Attack Types

Documented by:
Mr. Ahmed Khan
Mr. Dipak
Mr. Kannan
Mr. Kiran
Mr. Kulkarni
Madunix
Mr. Mohamed Iqbal
Mr. Nitai
Mr. Sagar
Mr. Shrikanth

Draft Copy : 01.03

Attacks

- An **attack** is any attempt to destroy, expose, alter, disable, steal or gain unauthorized access to or make unauthorized use of an asset.
- Without proper security measures and controls in place, our data might be subjected to an attack. Some attacks are passive, meaning information is monitored; others are active, meaning the information is altered with intent to corrupt or destroy the data or the network itself.
- Attacks can be Insider or via external

Attacks

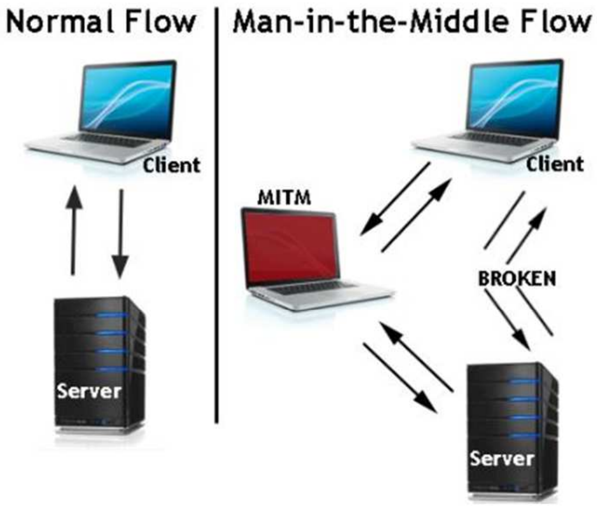
Active Attacks: An active attack is a network exploit ation in which a hacker attempts to make changes to data on the target or data en route to the target.

Passive Attacks: A passive attack is a network attack in which a system is monitored and sometimes scanned for open ports and vulnerabilities. The purpose is solely to gain information about the target and no data is changed on the target.

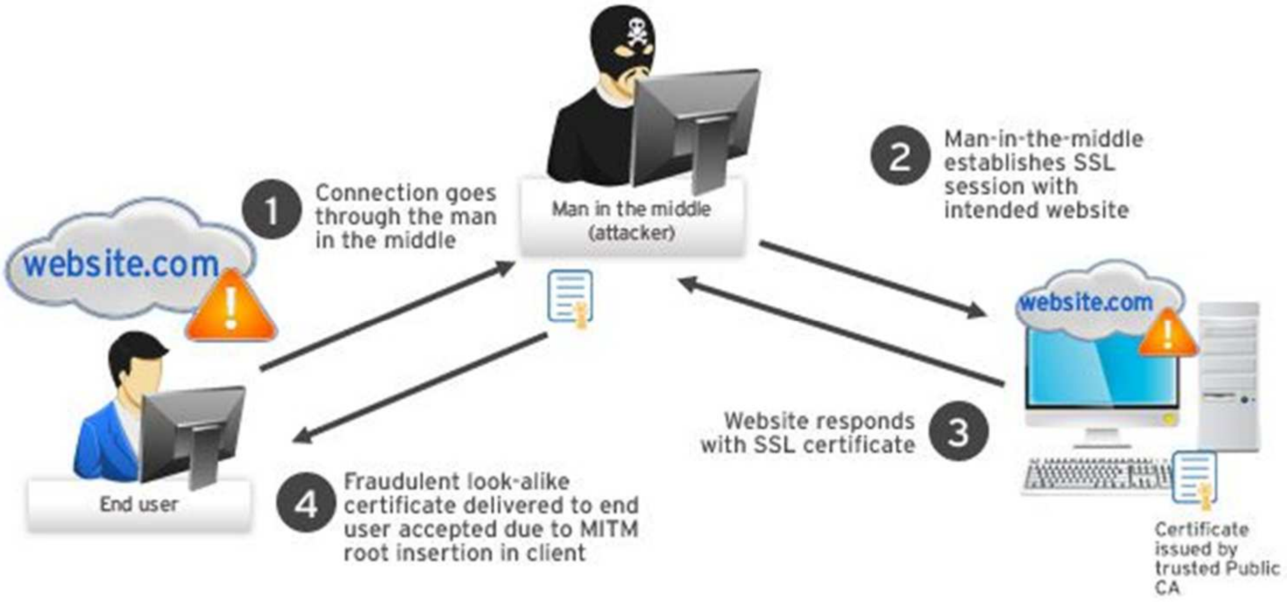
Active :Listens **Passive : Modifies**

Man-In-The-Middle AKA MITM

- It is an attack where the attacker secretly relays and possibly alters the communication between two parties who believe they are directly communicating with each other.



Countermeasures
- Digital signature
- Mutual authentication



website.com
Man in the middle (attacker)
End user
website.com
Certificate issued by trusted Public CA

1 Connection goes through the man in the middle

2 Man-in-the-middle establishes SSL session with intended website

3 Website responds with SSL certificate

4 Fraudulent look-alike certificate delivered to end user accepted due to MITM root insertion in client

Brute Force

- A brute-force attack consists of an attacker trying many passwords or passphrases with the hope of eventually guessing correctly
- The attacker systematically checks all possible passwords and passphrases until the correct one is found.
- When password guessing, this method is very fast when used to check all short passwords.
- Hackers knows the passwords saved in database
- Once we request the page, request sends from server to client machine. Hackers are active to access our account
- They start trying passwords to login
- There is a computer program run automatically to get the password

Countermeasures

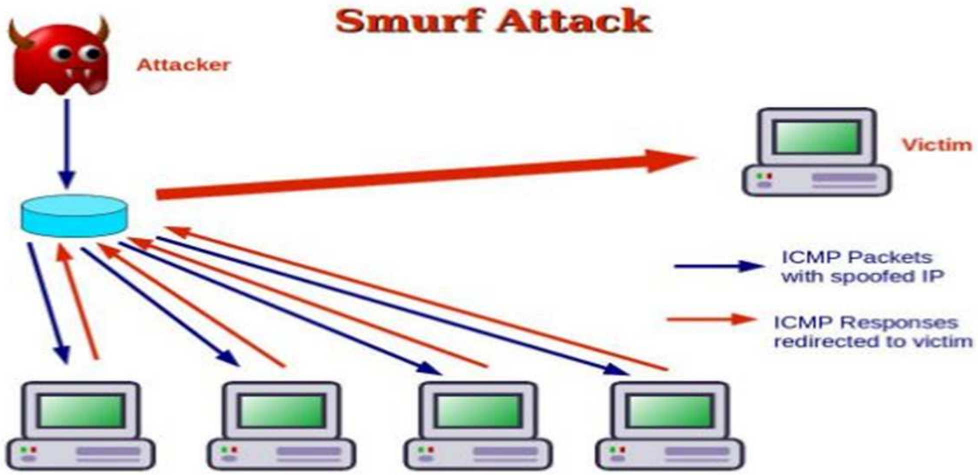
- Account Lockout (Clipping Levels)
- Strong Passwords

Smurf Attacks

- Is a form of a DDOS that renders computer networks inoperable
- Huge numbers of ICMP requests are sent to the victim's IP address
- The source destination IP address is spoofed
- The hosts on the victim's network respond to the ICMP requests
- This creates a significant amount of traffic on the victim’s network, resulting in consumption of bandwidth and ultimately causing the victim’s server to crash.

Countermeasures

- Configure individual hosts and routers to not respond to ICMP requests or broadcasts; or
- Configure routers to not forward packets directed to broadcast addresses.


Smurf Attack
Attacker
Victim
ICMP Packets with spoofed IP
ICMP Responses redirected to victim

Fraggle Attacks

- A Fraggle attack is exactly the same as a smurf attack, except that it uses the user datagram protocol, or UDP, rather than the more common transmission control protocol, or TCP. Fraggle attacks, like smurf attacks, are starting to become outdated and are commonly stopped by most firewalls or routers.

- It is also a denial-of-service (DoS) **attack** that involves sending a large amount of spoofed UDP traffic to a router's broadcast address within a network.

Countermeasures

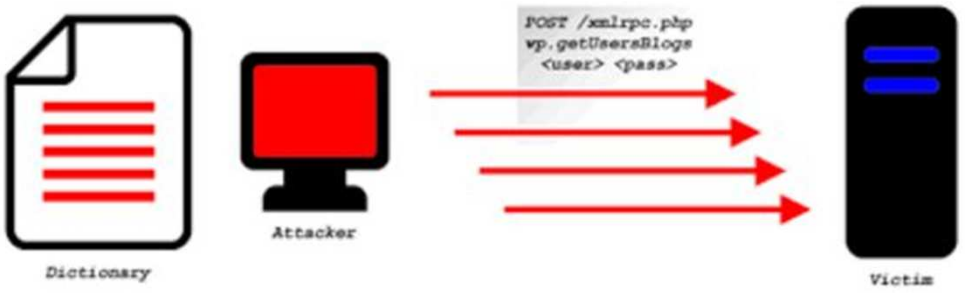
- Close unneeded ports

Dictionary Attacks

- Most people use real words as passwords.
- Trying all dictionary words and makes the attack much faster.
- Hackers and spammers attempt to log in to a computer system by trying all possible passwords until the correct one is found.

Countermeasures

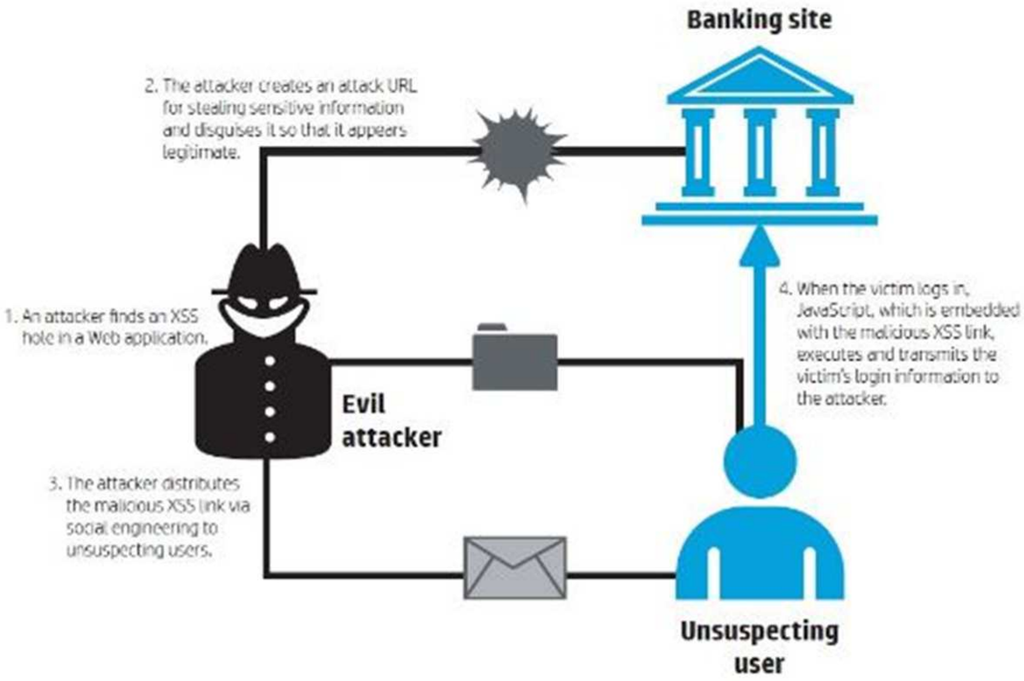
- Lock out a user after X failed login attempts
- Not using Dictionary words as passwords



```
POST /xmlrpc.php
wp.getUsersBlogs
  <user> <pass>
```

Cross Site Scripting

Cross Site Scripting- Attackers inserts malicious code into an application, when regular user request the webpage it returns the malicious page and attacker gains control over user data via code he injects


Banking site
2. The attacker creates an attack URL for stealing sensitive information and disguises it so that it appears legitimate.
1. An attacker finds an XSS hole in a Web application.
4. When the victim logs in, JavaScript, which is embedded with the malicious XSS link, executes and transmits the victim's login information to the attacker.
Evil attacker
3. The attacker distributes the malicious XSS link via social engineering to unsuspecting users.
Unsuspecting user

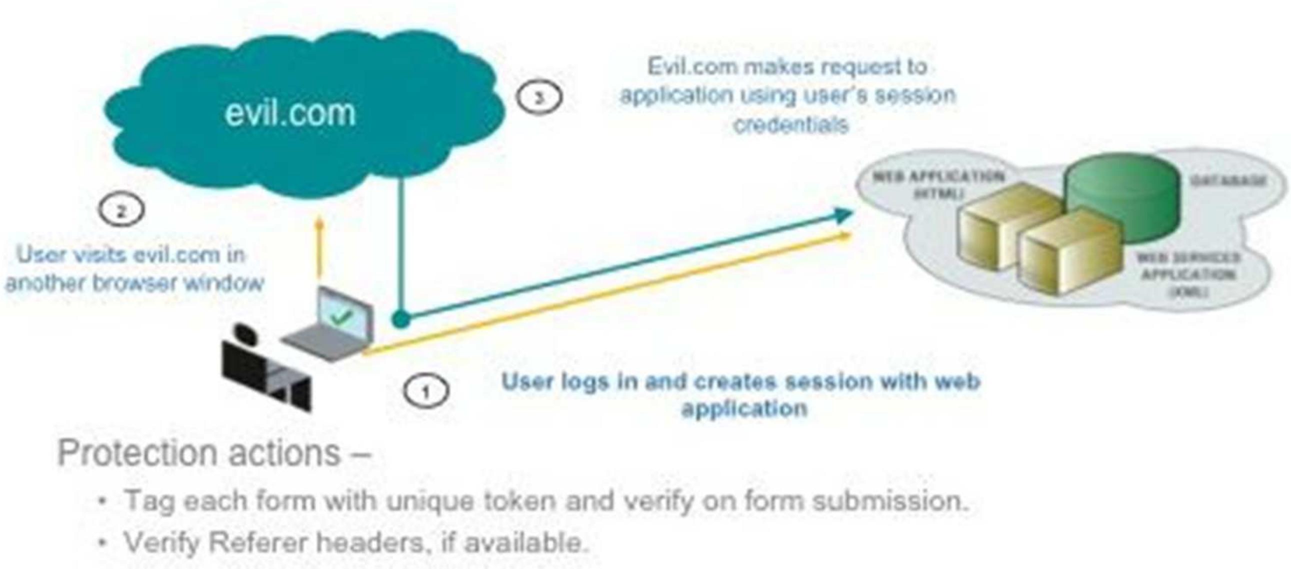
Countermeasure

- Safely validating untrusted HTML input
- Cookie security
- Disabling scripts

Cross Site Request Forgery

CSRF- Cross Site Request Forgery

A cross-site request forgery is an attack that involves forcing a victim to send an HTTP request to a target destination without their knowledge or intent in order to perform an action as the victim.


evil.com
3
Evil.com makes request to application using user's session credentials
WEB APPLICATION (HTML)
DATABASE
WEB SERVICES APPLICATION (XML)
2
User visits evil.com in another browser window
1
User logs in and creates session with web application

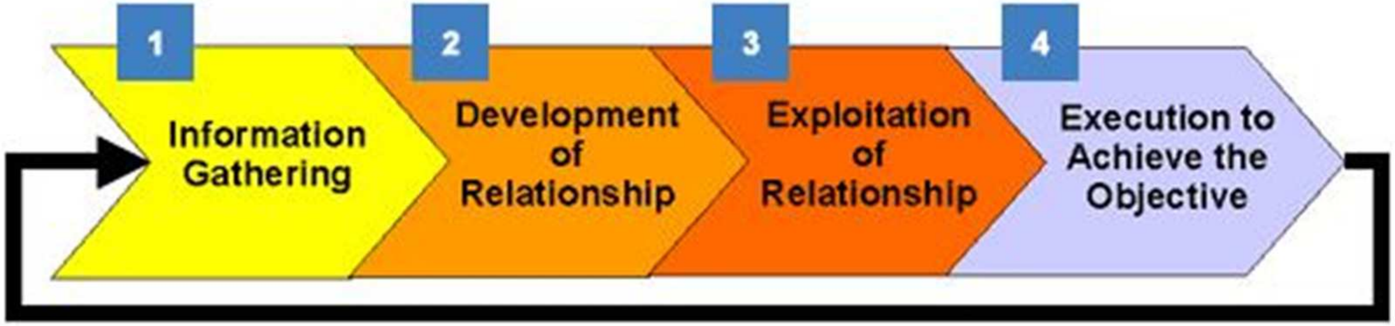
Protection actions –

- Tag each form with unique token and verify on form submission.
- Verify Referer headers, if available.

Social Engineering Attack

Social engineering is the art of manipulating people so they give up confidential information

Criminals usually trying to trick you into giving them your passwords or bank information, or access your computer to secretly install malicious software


1
Information Gathering
2
Development of Relationship
3
Exploitation of Relationship
4
Execution to Achieve the Objective

Countermeasures

- **NEVER** provide confidential information or, for that matter, even non-confidential data and credentials via email, chat messenger, phone or in person to unknown or suspicious sources.
- **BEFORE** clicking on links both in emails and on websites keep an eye out for for misspellings, @ signs and suspicious sub-domains.
- Don’t Open mails from untrusted sources
- Employee Awareness
- **USE** 2-factor authentication

Spoofing /Masquerading Attack

These attacks are carried out when someone(or something) try to introduce himself as another person (or another object), this called spoofing

Changing person’s identity

Masquerading:

A **masquerade attack** is an **attack** that uses a fake identity, such as a network identity, to gain unauthorized access to personal computer information through legitimate access identification.

Countermeasures

- Use authentication based on key exchange
- Use an access control list
- Implement filtering of both inbound and outbound

traffic.

- Enable encryption sessions

Dumpster Diving

- Collecting information from trash like access codes or passwords written down on sticky notes
- Information like a phone list, calendar, or organizational chart can be used to assist an attacker using social engineering techniques to gain access to the network.

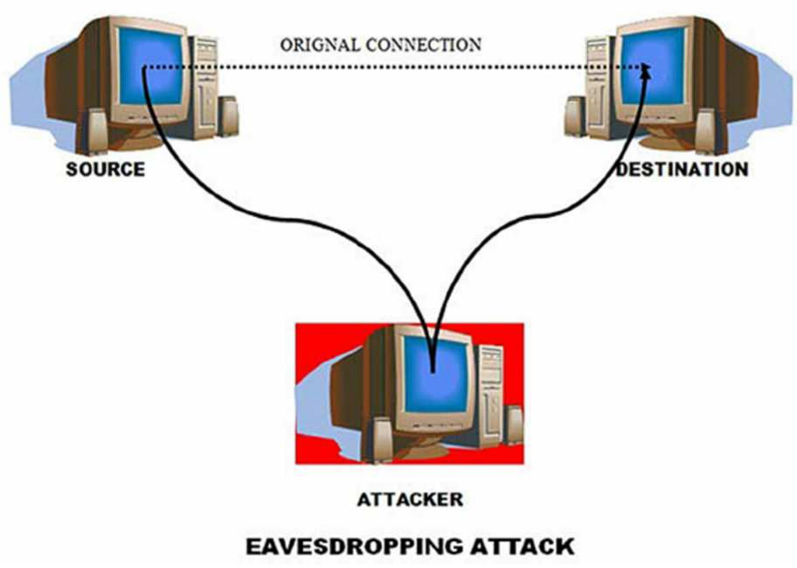
Countermeasures

- Shred personal documents and credit card offers before throwing them away, and wipe hard drives clean before you get rid of computers or smartphones.

Eavesdropping Attack

EAVESDROPPING ATTACK:

- Network Eavesdropping or network sniffing is an attack that aims to capture information transmitted over a network by other computers.
- The objective is to acquire sensitive information like passwords, session tokens, or any kind of confidential information.

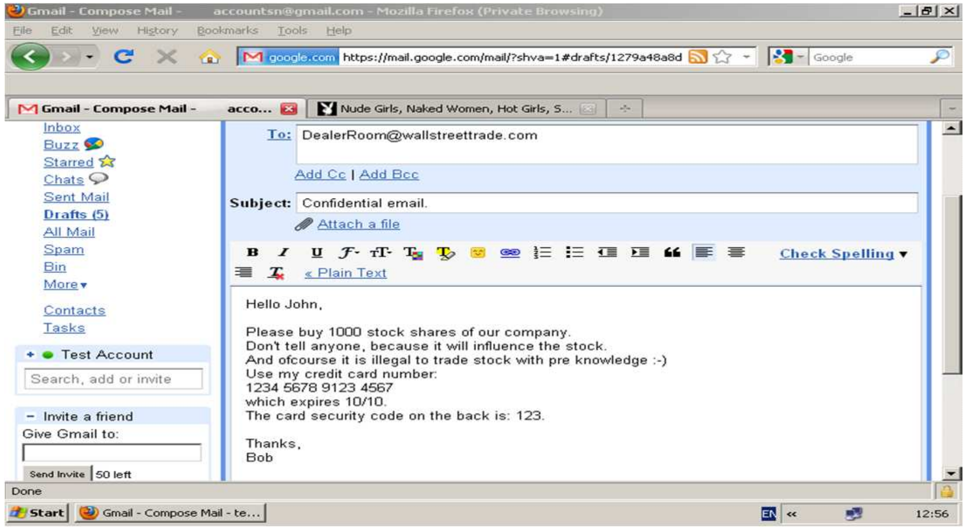


Countermeasures

- Encryption
- Awareness
- Network Segmentation
- NAC
- Physical Security

Keystroke Logging

- **Keystroke logging** often referred to as keylogging or keyboard capturing, is the action of recording (logging) the keys struck on a keyboard, typically covertly, so that the person using the keyboard is unaware that their actions are being monitored.


Gmail - Compose Mail - accountsn@gmail.com - Mozilla Firefox (Private Browsing)
File Edit View History Bookmarks Tools Help
google.com https://mail.google.com/mail/?shva=1#drafts/1279a48a8d
Google
Gmail - Compose Mail - acco...
Nude Girls, Naked Women, Hot Girls, S...
Inbox
Buzz
Starred
Chats
Sent Mail
Drafts (5)
All Mail
Spam
Bin
More
Contacts
Tasks
Test Account
Search, add or invite
Invite a friend
Give Gmail to:
Send Invite
50 left
Add Cc | Add Bcc
Attach a file
Check Spelling
« Plain Text
Done
Start
Gmail - Compose Mail - te...
EN
12:56

To: DealerRoom@wallstreettrade.com

Subject: Confidential email.

Hello John,

Please buy 1000 stock shares of our company.
Don't tell anyone, because it will influence the stock.
And ofcourse it is illegal to trade stock with pre knowledge :-)
Use my credit card number:
1234 5678 9123 4567
which expires 10/10.
The card security code on the back is: 123.

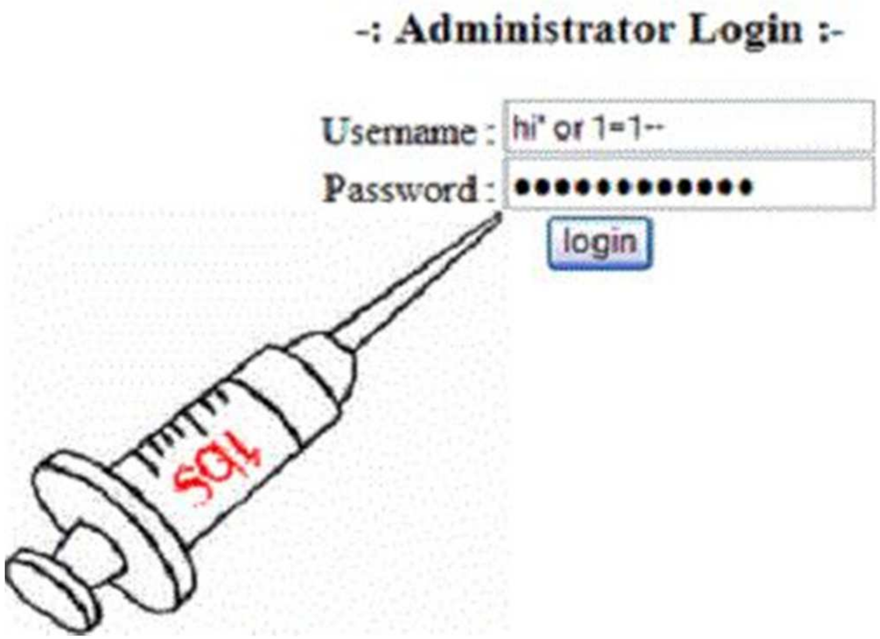
Thanks,
Bob

Countermeasures

Anti – Key Logger

Sqli Attack

- An SQL query is a request for some action to be performed on a database and statements are inserted into an entry field for execution.
- SQL injection is a type of security exploit in which the attacker adds Structured Query Language (SQL) code to a Web form input box to gain access to resources or make changes to data.



-: Administrator Login :-

Username : hi' or 1=1--

Password : ●●●●●●●●●●●●●

Countermeasures
Trust no-one
Don't use dynamic SQL when it can be avoided
Update and patch
Firewall
Reduce your attack surface
Use appropriate privileges
Keep your secrets secret
Don't divulge more information than you need to

Competitive intelligence

Competitive Intelligence involves the use of public sources to develop data on competition, competitors, and the market environment. It then transforms, by analysis, that data into intelligence. Public, in CI, means all information you can legally and ethically identify, locate, and then access. “Competitive intelligence” is known by a litany of other names: competitor intelligence, business intelligence, strategic intelligence, marketing intelligence, competitive technical intelligence, technology intelligence, and technical intelligence.

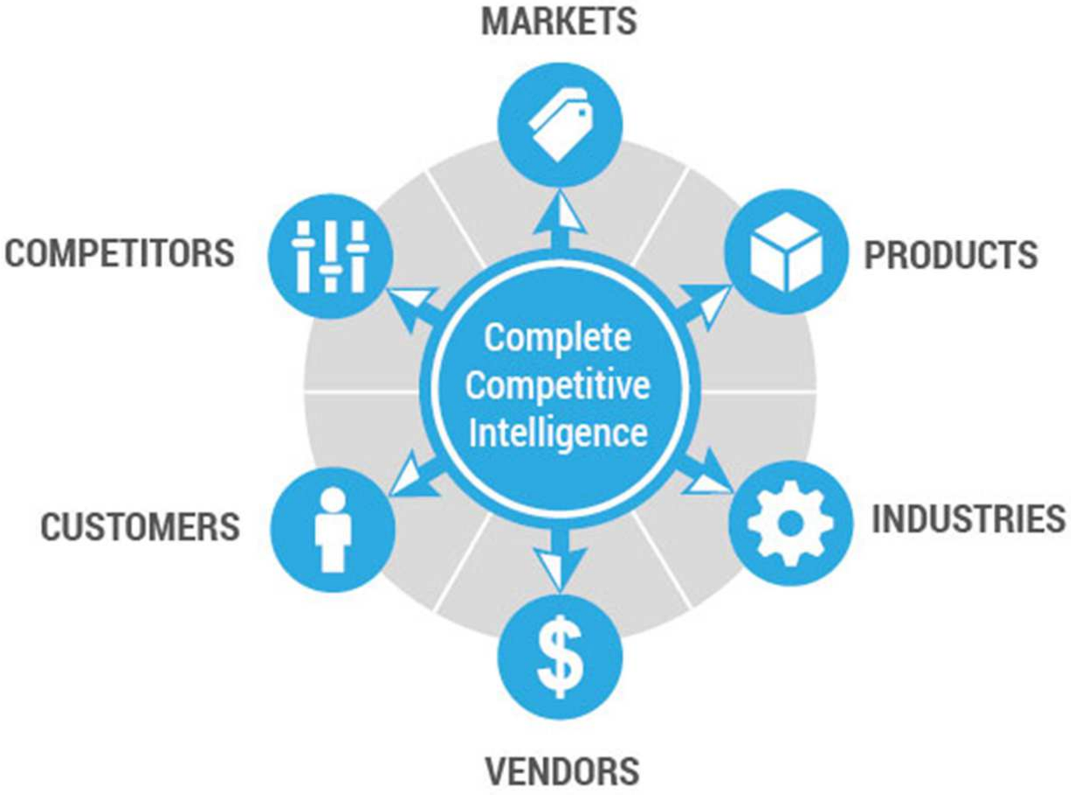
However, whatever name is goes by, it all refers to the same practice:

- Identifying the information that a decision-maker needs on the competition, or the competitive environment
- Collecting raw data, using legal and ethical means, from public sources
- Analyzing that data, using any one of a wide variety of tools, converting it into intelligence that is actionable
- Communicating the finished intelligence to key decision-maker for their internal use

Countermeasures:

- Full Radio Frequency (RF) Spectrum Analysis
- Infrared Spectrum Analysis (IR)
- Detecting transmitting devices in the electrical system/wiring
- Computer forensics (for example, searching for emails that mention a sensitive topic after a meeting has taken place to look for leaks).
- Disrupting laser frequencies with static “white noise” and or window coatings to prevent laser listening systems from gathering micro-vibrations from the surface of a window to listen in on conversations from outside of a room.
- Conducting a physical search looking for:
- Idle surveillance equipment that may be turned off or out of batteries.
- Cameras or microphones in the ceiling.
- Reflections from camera lenses.
- Radio transmitters that could broadcast to an external radio.
- Bugged telephones. Polycom phone systems are easy to turn into listening devices.
- Easily found passwords left on desks or under keyboards.
- Computers left on and logged in.
- Document disposal and inadequate document shredders

Competitive intelligence

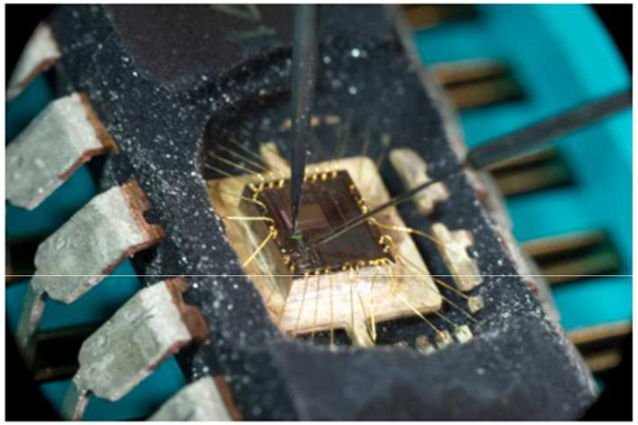


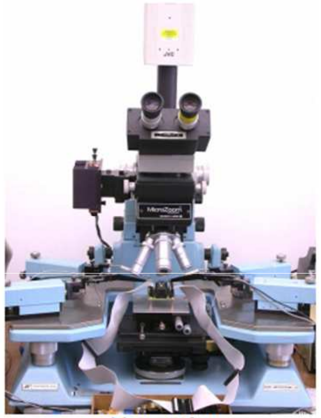
Invasive attacks: Micro-probing

Micro probing means attaching microscopic needles onto the internal wiring of a chip; this can be used to either read out internal secrets that are not intended to leave the chip, or it can be used for fault attacks.

Micro probing with fine electrodes

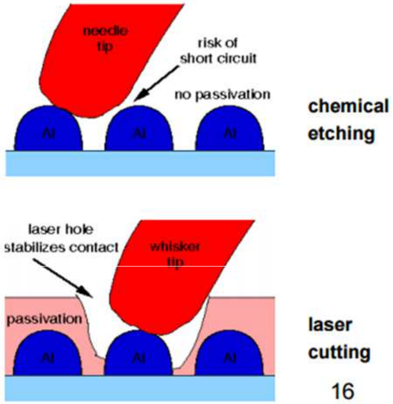
- eavesdropping on signals inside a chip
- injection of test signals and observing the reaction
- can be used for extraction of secret keys and memory contents
- laser cutter can be used to remove passivation and cut metal wires
- limited use for 0.35µm and smaller chips





probing station

laser cutter



Picture courtesy of Dr Markus Kuhn

FAULT GENERATION

Fault generation is a smart card attack that allows a hacker to uncover the encryption key using reverse engineering. This is accomplished by introducing an input voltage, clock rate, or temperature fluctuation error into the card. Comparison between the encryption functions that are produced when the error occurs versus when no error occurs helps with the reverse engineering process.

RFID SKIMMING/EAVESDROPPING

A new breed of digital pickpocket has been discovered lurking in stations and shopping centers.They come armed with technology that can effortlessly steal credit and debit card details without so much as touching your wallet.Standing just six inches (15cm) away, these criminals use radio-frequency identification (RFID) readers to harvest bank details in a practice known as ‘digital skimming’.A low power Embedded Linux Computer, and an easily purchasable RFID reader.‘This was then powered by a USB Battery, and stuck into a backpack.’As well as a device, digital pickpockets can download an RFID app onto their phone.If a reader or RFID-app enabled smartphone is within range, it can pick up the wireless signals transmitted when that card is being used to buy a product. The information can then be input into a machine that can be purchased for $300-$400 to replicate the card.

RFID SKIMMING/EAVESDROPPING

SAFEGUARD

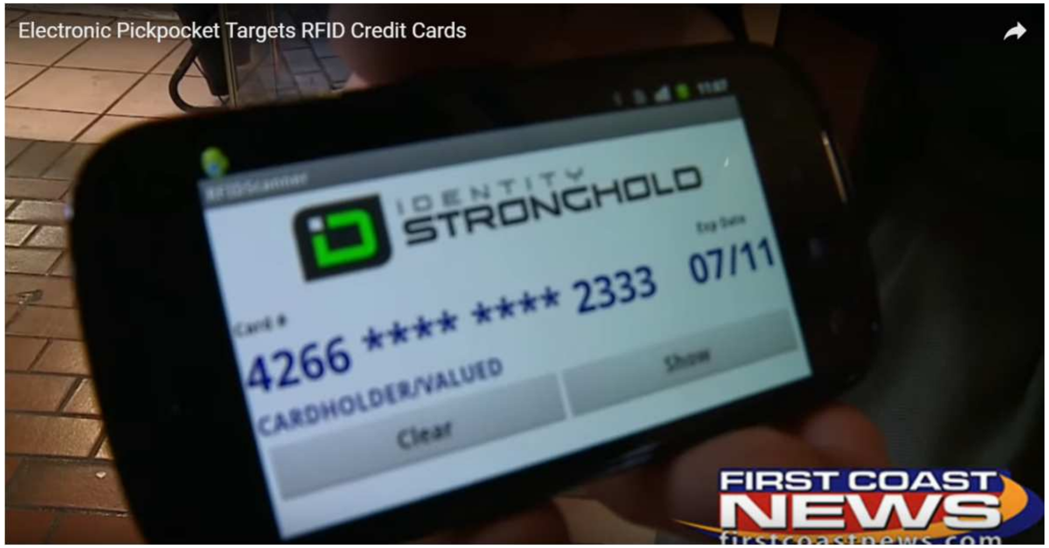
Cards can be protected from RFID skimmers by being wrapped in tin foil

COUNTERMEASURES

Mutual authentication between Tag and Reader

Encryption of the data transfer between Tag and Reader

Software countermeasures do exist (e.g., derived keys, use of session keys, periodical key updates)



RFID ROGUE READER

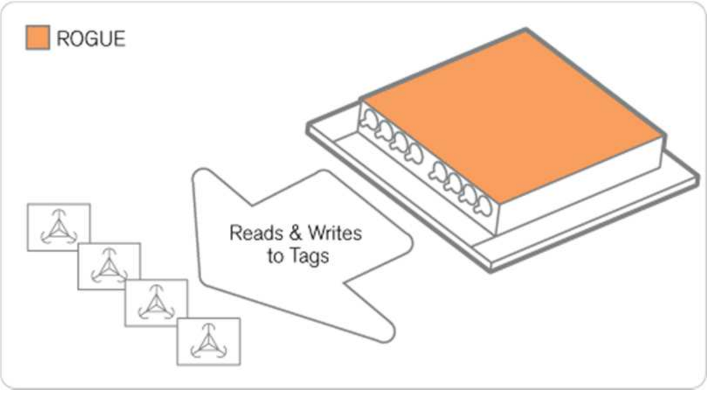
Tags are evolving quickly in complexity, power, and flexibility. However, all types of tag share a critical vulnerability to rogue RFID readers. A rogue reader can read a tag, recording information that may be confidential. It can also write new, potentially damaging information to the tag. Or it can kill the tag. In each of these cases, the tags respond as if the RFID reader was authorized, since the rogue reader appears like any other RFID reader. This capability has broad implications, since tags may contain data that should not be shared with unauthorized devices.

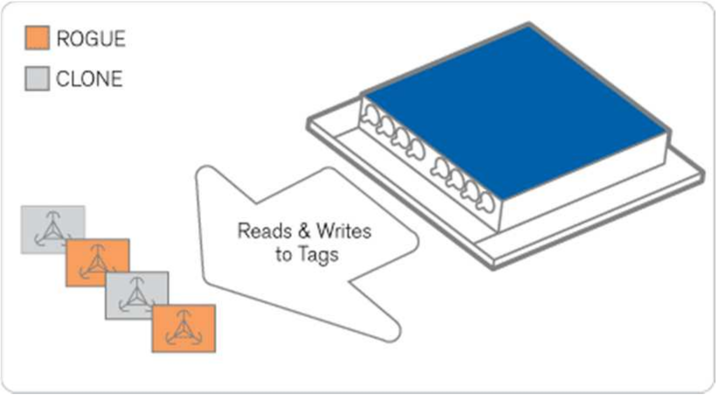
A rogue RFID reader might be able to measure the inventory on a store shelf and chart sales of certain items—providing critical sales data to a rival product manufacturer. This unauthorized information could play a key role in developing a competitive strategy informed by corporate espionage—e.g., negotiating more shelf space or better product placement.

RFID ROGUE READER

Rogue and Clone Tags On the other end of the tag-reader connection, consider the threat of rogue and clone tags. Rogue tags are tags from unauthorized sources, while clone tags are unauthorized copies of real tags. These tags connect with the RFID reader via RF and send false data.

Example: Rogue and Clone Tags A bootleg product could appear to be an actual product if it bears a clone tag. A rogue tag placed within proximity to a RFID reader could contribute false data to the reader. In both cases, these tags affect the integrity of the system, and undermine security for both consumers and the companies that rely on RFID.





RFID MALWARE

Low level misuse of improperly formatted RFID tag data.

What are RFID Exploits?

An RFID exploit is malicious RFID tag data that "exploits" some part of the RFID system that encounters it. RFID systems are susceptable to hacker attacks, just like conventional computing systems. When an RFID reader scans a tag, it expects to get back information in a certain format. However, a malicious person can write carefully crafted data whose format and content is so unexpected that it can corrupt the RFID reader's software and potentially its database as well.

What are RFID Worms?

An RFID worm is an RFID-based exploit that abuses a network connection to achieve self-replication. RFID worms may propagate by exploiting online RFID services, but can also spread via RFID tags. The RFID worm code causes unsuspecting RFID servers to download and execute some file from a remote location. This file then proceeds to compromise the RFID middleware server in the same fashion as most Internet-based malware. The worm infected RFID software can then "infect" new RFID tags by overwriting their data with a copy of the RFID worm code.

RFID MALWARE

What are RFID Viruses?

An RFID virus is an RFID-based exploit that autonomously self-replicates its code to new RFID tags, without requiring a network connection. RFID viruses may or may not have a payload, which modifies or disrupts the workings of the back-end RFID system. Once the newly-infected RFID tags are sent on their way, they infect other RFID systems (assuming use of the same software system). These RFID systems then infect other RFID tags, which infect other RFID software systems, etc..

COUNTERMEASURES

Sanitize input
Error/ Bounds Checking
Disable Unnecessary facilities
Segregate Users
Use parameter binding
Code review
Limit permission

RFID REPLAY ATTACK

Eavesdropping, like it sounds, occurs when an unauthorized RFID reader listens to conversations between a tag and reader then obtains important data. It is still necessary for the hacker to know the specific protocols and tag and reader information for this technique to work.

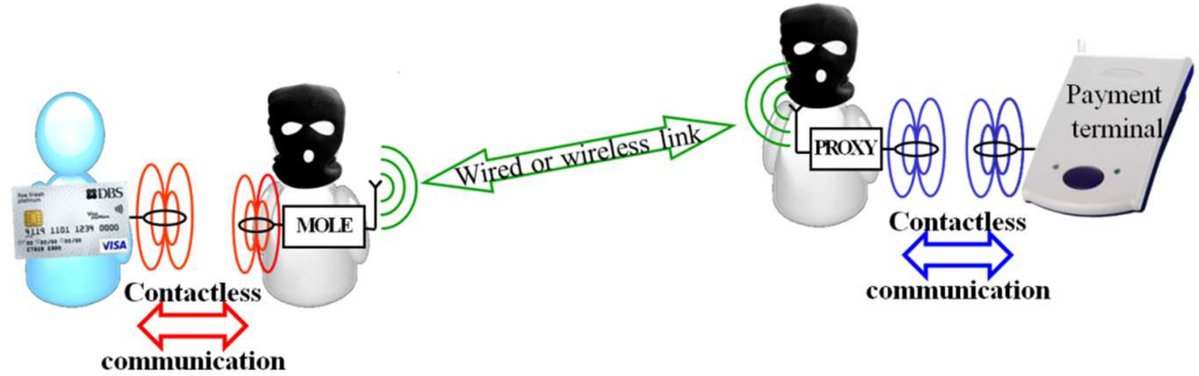
Replay attacks builds on eavesdropping and specifically occur when one part of communication in an RFID system is recorded and then ‘replayed’ at a later time to the receiving device in order to steal information or gain access.

COUNTERMEASURES:

To deal with replay attacks the tag’s response must be unique for every server challenge. To achieve this, the values of the server challenges and the tag responses must be unpredictable. One way to achieve this is to enforce that the answers be (cryptographically) pseudo-random.

Time Stamping the messages between the reader and tags are one viable countermeasure

RFID REPLAY ATTACK



RFID SPOOFING

Technically two specific events, cloning and spoofing are usually done back to back. Cloning is duplicating data from a pre-existing tag, and spoofing is then using the cloned tag to gain access to a secured area or item. Because the hacker has to know the data on the tag to clone it, this type of attack is mainly seen in access or asset management operations.

In relation to RFID technology, spoofing occurs when a forged tag masquerades as a valid tag and thereby gains an illegitimate advantage. Tag cloning is a spoofing attack where the attacker captures the data from a valid tag and creates a copy of the captured sample on a blank tag. Another example is an attacker reading a tag's data from a cheap item in a store and then uploading the data onto another tag attached to a similar but more expensive item. Mr. Lukas Grunwald, a German security expert, said “I was at a hotel that used smartcards, so I copied one and put the data into my computer, … Then I used RF Dump to upload the room key card data to the price chip on a box of cream cheese from the Future Store. And I opened my hotel room with the cream cheese!” (Newitz, 2006)

RFID SPOOFING

Countermeasures

A common way to defeat a spoofing attack is to implement an RFID authentication protocol and data encryption, which increases the cost and technology complexity needed for a successful attack.

Purpose: Gain Access

RFID Eavesdropping

Since an RFID tag is a wireless device that emits data, usually a unique identifier, when interrogated by an RFID reader, there exists a risk that the communication between tag and reader can be eavesdropped. Eavesdropping occurs when an attacker intercepts data with a compliant reader—one for the correct tag family and frequency—while a tag is being read by an authorized RFID reader. Since most RFID systems use clear text communication, due to tag memory capacity or cost, eavesdropping is a simple but efficient means for the attacker to obtain information on the collected tag data. The information picked up during the attack can have serious implications—it can be used in subsequent attacks against the RFID system. It is necessary to point out that in passive RFID systems readers have significantly longer transmission ranges than tags. When passive tags modulate and backscatter the signal from the reader to communicate, they have only a fraction of the transmission power of the reader. Therefore, passive tags have a more limited transmission range and are less susceptible to eavesdropping (Karygiannis et al., 2007). However, it is necessary to keep in mind that even if the eavesdropper is out of the range of the tag signal, he or she may still be able to listen to the commands sent out from the reader (Figure 5).

Countermeasures

Countermeasures against eavesdropping include establishing a secure channel and/or encrypting the communication between tag and reader. Another approach is to only write the tag with enough information to identify the object. The identity is used to look up relevant information about the object in a back end database, thus requiring the attacker to have access to both the tag and the database to succeed in the attack.

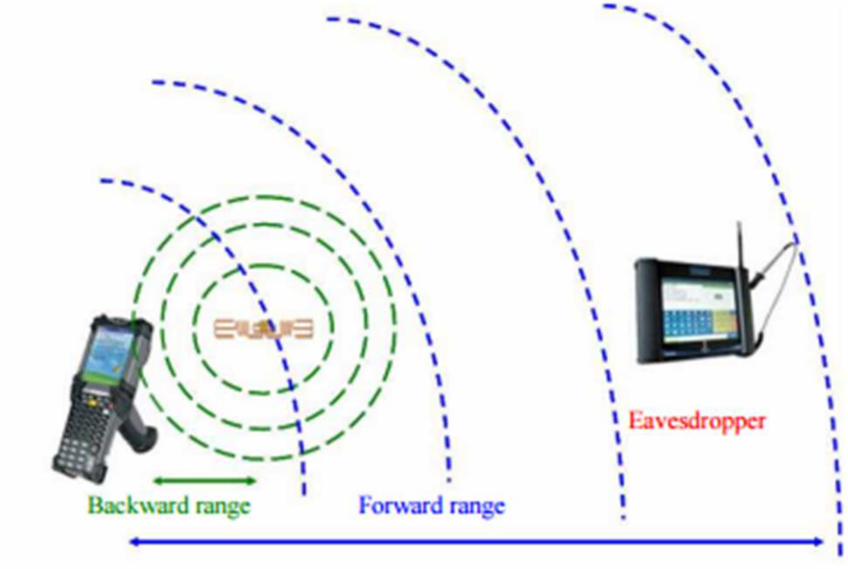


Fig. 5. Eavesdropping on reader-tag communication

RFID TRACKING

Unlike the previously discussed RFID attacks, tracking is a threat directed against an individual. Within the next few years, manufacturers may put item-level RFID tags into many more household products. There is a privacy concern because instead of tracking books and consumer products such as clothing, RFID systems can be used to track people’s movements and even create a precise profile of their purchases.

Countermeasures

An easy method to disable tracking is to deactivate the RFID tags, which is known as “killing” the tag that will be introduced in the following section.

RFID MITM

Depending on the system configuration, a man-in-the-middle (MITM) attack is possible while the data is in transit from one component to another. An attacker can interrupt the communication path and manipulate the information back and forth between RFID components (Figure 6). This is a real-time threat. The attack reveals the information before the intended device receives it and can change the information en route (Welch & Lathrop, 2003). Even if it received some invalid data, the system being attacked might assume the problem was caused by network errors and would not recognize that an attack occurred. An RFID system is particularly vulnerable to MITM attacks because the tags are small in size and low in price, all of which means that there is generally a lack of sophisticated protection circuitry

Countermeasures

Several technologies can be implemented to reduce MITM threats, such as encrypting communications, sending information through a secure channel, and providing an authentication protocol.

RFID MITM

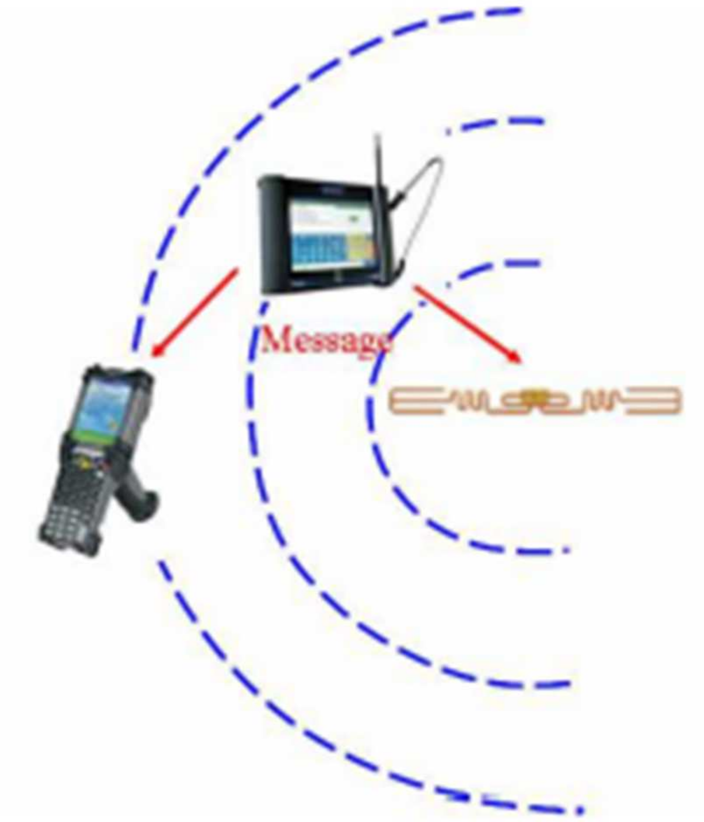


Fig. 6. Man-in-the-middle attack

RFID DOS ATTACK

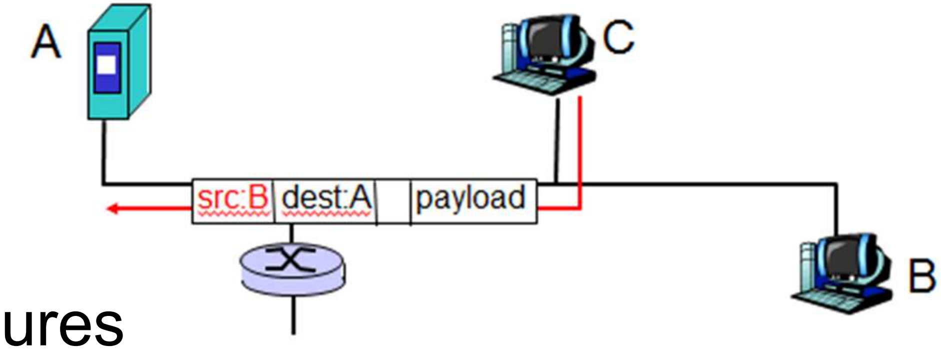
DoS attacks can take different forms by attacking the RFID tag, the network, or the backend. The purpose is not to steal or modify information, but to disable the RFID system so that it cannot be used. When talking about DoS attacks on wireless networks, the first concern is physical layer attacks, such as jamming and interference. Jamming using noise in the RFID system's frequency range can reduce the throughput of the network and ruin network connectivity resulting in overall supply chain failure (Egli, 2006). Jamming happens when a device that actively broadcasts radio signals can block and disrupt the operation of any and all nearby RFID readers. Interference with other radio transmitters can also launch a DoS attack to obscure the communications between the tags and reader. Another form of DoS is to destroy or disable RFID tags by removing them from the items, washing out their contents completely, or wrapping them with metal foil.

Countermeasures

In general, it is easier to detect DoS attacks than prevent them from happening. However, once detected, the attacks can generally be stopped before they do too much harm. For example, countermeasures against jamming can use passive listening to detect the tags whose transmission exceeds a predefined volume, and then use block functions to thwart them. Countermeasures against detaching the tags from the targeted items could be either through enhancing the mechanical connection between the tags and items, or adding an alarm function to active tags.

IP Spoofing

- can generate “raw” IP packets directly from application, putting any value into IP source address field
- receiver can’t tell if source is spoofed
- e.g.: C pretends to be B

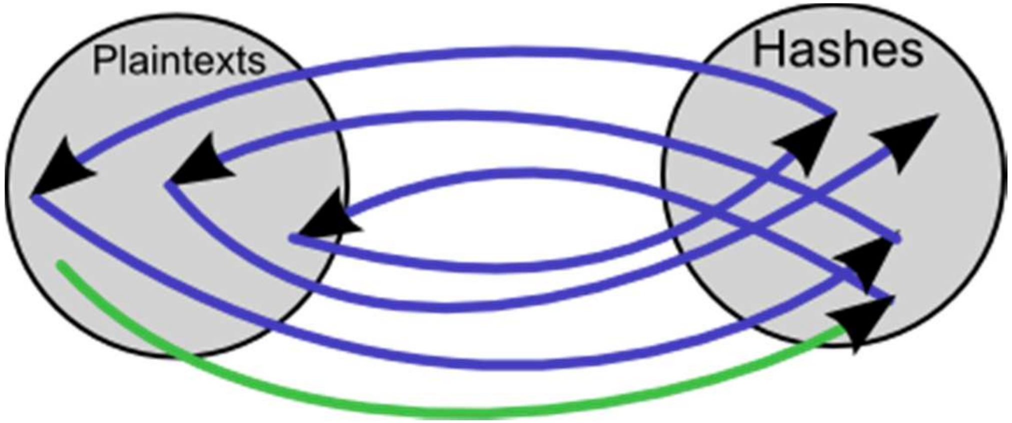


Countermeasures

- routers should not forward outgoing packets with invalid source addresses (e.g., datagram source address not in router’s network)
- great, but ingress filtering can not be mandated for all networks

RAINBOW TABLE

A rainbow table is a precomputed table for reversing cryptographic hash functions, usually for cracking password hashes. Tables are usually used in recovering a plaintext password up to a certain length consisting of a limited set of characters. It is a practical example of a space/time trade-off, using less computer processing time and more storage than a brute-force attack which calculates a hash on every attempt, but more processing time and less storage than a simple lookup table with one entry per hash. Use of a key derivation function that employs a salt makes this attack infeasible.



Countermeasures

A rainbow table is ineffective against one-way hashes that include large salts. For example, consider a password hash that is generated using the following function (where "+" is the concatenation operator):

saltedhash(password) = hash(password + salt)

Or

saltedhash(password) = hash(hash(password) + salt)

The salt value is not secret and may be generated at random and stored with the password hash. A large salt value prevents precomputation attacks, including rainbow tables, by ensuring that each user's password is hashed uniquely. This means that two users with the same password will have different password hashes (assuming different salts are used). In order to succeed, an attacker needs to precompute tables for each possible salt value.

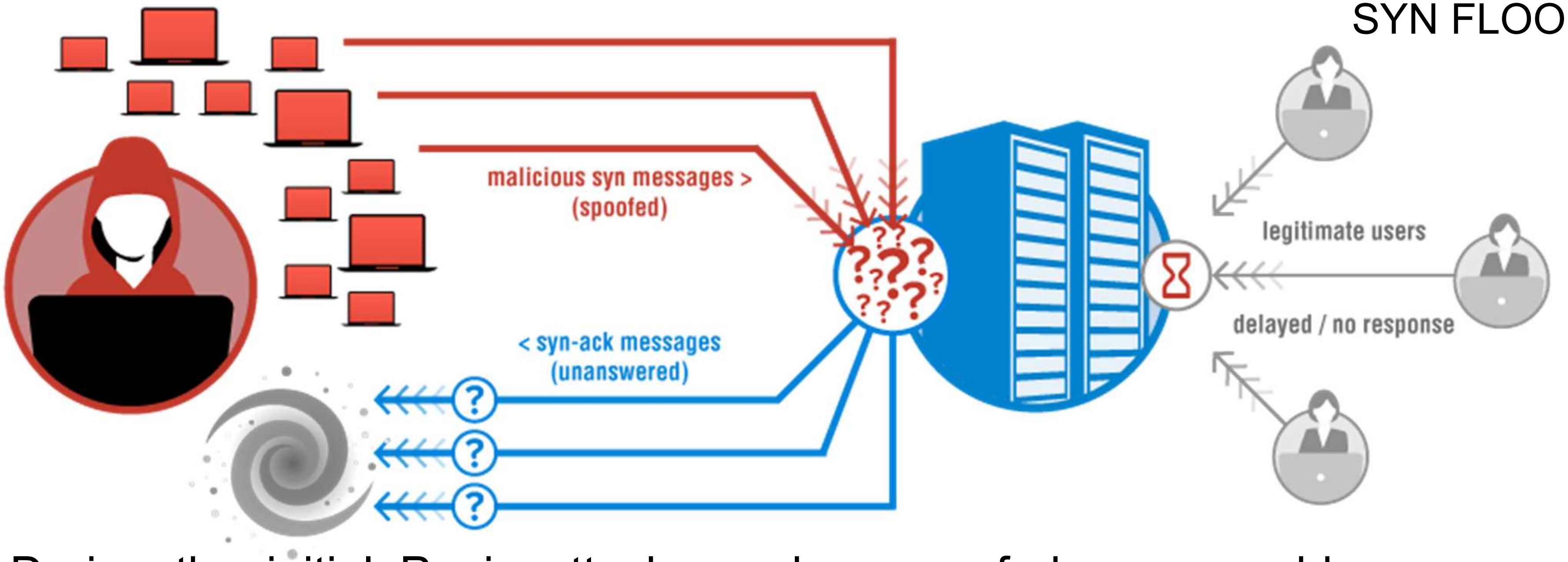
SYN flood

A SYN flood is a layer 4 DDoS attack method that exploits a server’s TCP connection capability. Typically, a client and server establish a TCP connection using a ‘three-way’ handshake:

- Client requests to connect to the server, and sends a SYN (synchronize) message
- Server acknowledges the SYN message and sends back a SYN-ACK (synchronize-acknowledge) message
- Client responds back with an ACK (acknowledge message), establishing the connection

During a SYN flood attack, an attacker’s client sends numerous SYN messages to the target server. The server creates an entry in its connection table for each SYN received and responds to each with a SYN-ACK message. The attacker then either doesn’t send the ACK message, or many times, has spoofed its client IP address in the SYN packets so that the target server’s SYN-ACK responses are never received. As the attacker continues to send SYN messages, the target server’s connection tables become full and the server can no longer respond to any more connection requests. With all of its resources consumed, the target server is unable to connect with legitimate clients, creating a denial of service.

SYN FLOOD



During the initial Panix attack, random spoofed source addresses were being used, but it was noted that the attack TCP SYNs all used the same source port number. A filter that denied incoming packets from this port was temporarily effective, but easy for the attacker to adapt to, and the attack segments began using random ports. Panix was able to isolate which of its ingress routers the attack was coming from and null-route packets destined for its servers coming through that router, but this solution was obviously a heavy-handed one, and seems to have also been overcome when the attacker started sending packets that were routed through a different upstream provider. Panix had mixed success in getting its providers to assist in tracing and blocking the attack, and the networking community was spurred into devising other solutions.

SYN FLOOD

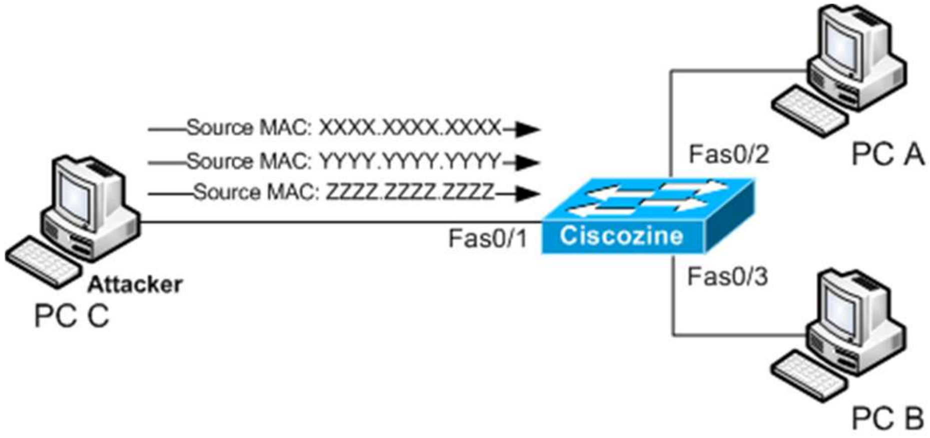
Two broad classes of solutions to SYN flooding attacks have evolved, corresponding to where the defenses are implemented. The first class of solutions involves hardening the end-host TCP implementation itself, including altering the algorithms and data structures used for connection lookup and establishment, as well as some solutions that diverge from the TCP state machine behavior during connection establishment, as described in RFC 793.

The second class involves hardening the network, either to lessen the likelihood of the attack preconditions (an army of controlled hosts or the propagation of IP packets with spoofed source addresses), or to insert middleboxes that can isolate servers on the networks behind them from illegitimate SYNs.

MAC FLOODING

In a typical MAC flooding attack, a switch is flooded with packets, each containing different source MAC addresses. The intention is to consume the limited memory set aside in the switch to store the MAC address-to-physical port translation table.

The result of this attack causes the switch to enter a state called failopen mode, in which all incoming packets are broadcast out on all ports (as with a hub), instead of just down the correct port as per normal operation. A malicious user could then use a packet sniffer running in promiscuous mode to capture sensitive data from other computers, which would not be accessible were the switch operating normally.


Source MAC: XXXX.XXXX.XXXX
Source MAC: YYYY.YYYY.YYYY
Source MAC: ZZZZ.ZZZZ.ZZZZ
Fas0/1
Ciscozine
Fas0/2
Fas0/3
PC A
PC B
Attacker
PC C

COUNTERMEASURES

To prevent MAC flooding attacks, network operators usually rely on the presence of one or more features in their network equipment:

With a feature often called "port security" by vendors, many advanced switches can be configured to limit the number of MAC addresses that can be learned on ports connected to end stations. A smaller table of "secure" MAC addresses is maintained in addition to (and as a subset to) the traditional "MAC address table."

Many vendors allow discovered MAC addresses to be authenticated against an authentication, authorization and accounting (AAA) server and subsequently filtered.

Implementations of IEEE 802.1X suites often allow packet filtering rules to be installed explicitly by an AAA server based on dynamically learned information about clients, including the MAC address.

MAC FLOODING COUNTERMEASURES

Security features to prevent ARP spoofing or IP address spoofing in some cases may also perform additional MAC address filtering on unicast packets, however this is an implementation-dependent side-effect.

Additional security measures are sometimes applied along with the above to prevent normal unicast flooding for unknown MAC addresses.This feature usually relies on the "port security" feature to retain all "secure" MAC addresses for at least as long as they remain in the ARP table of layer 3 devices. Hence, the aging time of learned "secure" MAC addresses is separately adjustable. This feature prevents packets from flooding under normal operational circumstances, as well as mitigating the effects of a MAC flood attack.

Keystroke logging

Keystroke logging, often referred to as keylogging or keyboard capturing, is the action of recording (logging) the keys struck on a keyboard, typically covertly, so that the person using the keyboard is unaware that their actions are being monitored.Keylogging can also be used to study human–computer interaction. Numerous keylogging methods exist: they range from hardware and software-based approaches to acoustic analysis.

Countermeasures

- Anti keyloggers
- Live CD/USB
- Anti-spyware / Anti-virus programs
- Network monitors
- Automatic form filler programs
- One-time passwords (OTP)
- Security tokens
- On-screen keyboards
- Keystroke interference software
- Speech recognition
- Handwriting recognition and mouse gestures
- Macro expanders/recorders
- Non-technological methods

DOS ATTACK

A denial-of-service attack (DoS attack) is a cyber-attack where the perpetrator seeks to make a machine or network resource unavailable to its intended users by temporarily or indefinitely disrupting services of a host connected to the Internet. Denial of service is typically accomplished by flooding the targeted machine or resource with superfluous requests in an attempt to overload systems and prevent some or all legitimate requests from being fulfilled.[1] A DoS attack is analogous to a group of people crowding the entry door or gate to a shop or business, and not letting legitimate parties enter into the shop or business, disrupting normal operations.

Countermeasures

- Intrusion Detection Systems (IDS) and an Intrusion Protection Systems (IPS).
- Strong anti-virus and anti-spyware software on all systems with Internet connectivity.
- File and folder hashes on system files and folders to identify if they have been compromised.
- Reverse DNS lookup to verify the source address.
- External firewalls with the following filters:
- Ingress filters that specify any inbound frame must have a public IP address from outside of the organization's LAN.
- Egress filters that specify any outbound frame must have a private IP address within the organization's LAN.
- Address filter to prevent traffic from specific attackers (if known).
- Once a DoS attack begins, you can minimize its effects by implementing filters to block unwanted traffic. You can also contact your ISP to implement filtering closer to the source and reduce the bandwidth used by the attack.
- Hardening practices on all machines, especially publicly exposed servers and directory and resource servers.

Sniffer Attack

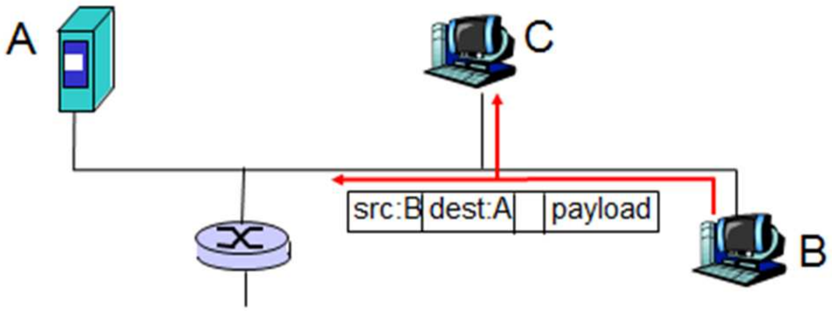
A *sniffer* is an application or device that can read, monitor, and capture network data exchanges and read network packets. If the packets are not encrypted, a sniffer provides a full view of the data inside the packet. Even encapsulated (tunneled) packets can be broken open and read unless they are encrypted *and* the attacker does not have access to the key.

Using a sniffer, an attacker can do any of the following:

- Analyze your network and gain information to eventually cause your network to crash or to become corrupted.
- Read your communications.

Countermeasures

- all hosts in organization run software that checks periodically if host interface in promiscuous mode (or try to remotely detect this)
- one host per segment of broadcast media (switched Ethernet at hub)



Session Hijacking

Session Hijacking by the name only it suggests that we are hacking someone’s active session and trying to exploit it by taking the unauthorized access over their computer system or Network. So Session Hijacking is the exploitation of valid computer or network session. Sometimes technical guys also call this HTTP cookie theft or more correctly Magic Cookie Hack. Now you guys surely be thinking what is Magic Cookie.

Magic cookie is simply a cookie that is used to authenticate the user on remote server or simply computer. In general, cookies are used to maintain the sessions on the websites and store the remote address of the website. So in Session Hijacking what Hacker does is that he tries to steal the Magic cookies of the active session that’s why its called HTTP cookie Theft. Nowadays several websites has started using HTTPS cookies simply called encrypted cookies. But we all know If encrypter exits so its decrypter also.

Session Hijacking

Session Hijacking is the process of taking over a existing active session. One of the main reason for Hijacking the session is to bypass the authentication process and gain the access to the machine. Since the session is already active so there is no need of re-authenticating and the hacker can easily access the resources and sensitive information like passwords, bank details and much more.

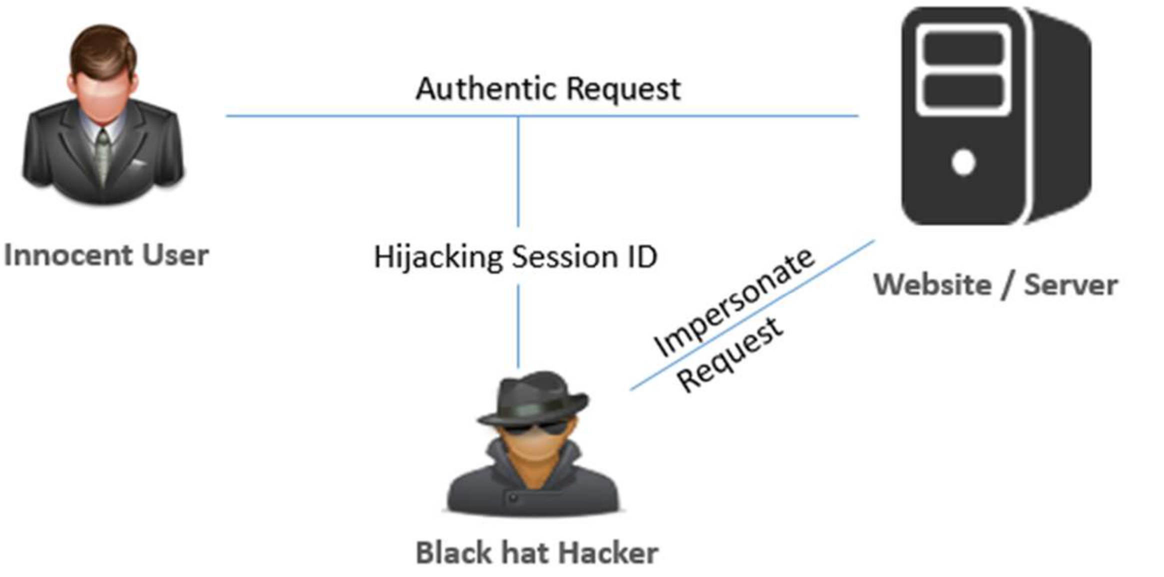


Image created by Sarvesh Kushwaha

Buffer Overflow

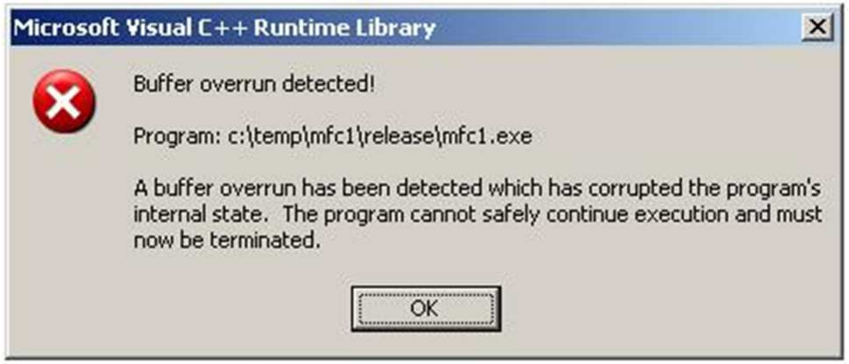
A buffer overflow, or buffer overrun, is an anomaly where a program, while writing data to a buffer, overruns the buffer's boundary and overwrites adjacent memory locations.

Buffers are areas of memory set aside to hold data, often while moving it from one section of a program to another, or between programs. Buffer overflows can often be triggered by malformed inputs; if one assumes all inputs will be smaller than a certain size and the buffer is created to be that size, if an anomalous transaction produces more data it could cause it to write past the end of the buffer. If this overwrites adjacent data or executable code, this may result in erratic program behavior, including memory access errors, incorrect results, and crashes.

A buffer overflow occurs when data written to a buffer also corrupts data values in memory addresses adjacent to the destination buffer due to insufficient bounds checking. This can occur when copying data from one buffer to another without first checking that the data fits within the destination buffer.

Countermeasures

- Deploy on systems capable of using non-executable stacks
- Use higher-level programming languages that are strongly typed and that disallow direct memory access.
- Validate input to prevent unexpected data from being processed, such as being too long, of the wrong data type, containing "junk" characters, etc.
- If relying upon operating system functions or utilities written in a vulnerable language, ensure that they:
  - use the principle of least privilege
  - use compilers that protect against stack and heap overflows
  - are current in terms of patches



Buffer overrun detected!

Program: c:\temp\mfc1\release\mfc1.exe

A buffer overrun has been detected which has corrupted the program's internal state. The program cannot safely continue execution and must now be terminated.

Relay Attack

Replay attacks are form of traditional man-in-the middle attacks. Communication with both parties is initiated by the attacker who merely relays the messages between the two parties without manipulating them or even necessarily reading them.
Example: An attacker could circumvent an authentication protocol by relaying a challenge to a legitimate token, which will provide him with the correct response, which could be relayed back to the verifier.

Countermeasures:

- Encrypt all the message communications between client and the server.
- Use SSL/TLS as the communication protocol.

Kernel Flaws

Kernel flaws are problems that are seen mainly within the Operating System (OS) of the machine.
These problems occur below the user’s interface. Any flaw in the kernel can be reached by an attacker and thus make it exploitable.

Countermeasures:

- Ensure that security patches are reviewed and tested first.
- Also, the deployment of the patches should be performed promptly to OS.
- For bigger patches, monitoring of the system is beneficial.

Authorization Creep

If a user gets a set of access rights after joining the organisation and soon he gets transferred/ promoted to other departments. Thus, getting more set of access rights and also major productivity classes.

Countermeasures:

- Ensure that security patches are reviewed and tested first.
- Also, the deployment of the patches should be performed promptly to OS.
- For bigger patches, monitoring of the system is beneficial.

Single Point of Failure (SPOF)

A single point of failure (SPOF) is a critical system component with the ability to cease system operations during failover. SPOF’s are undesirable to systems requiring reliability and availability, such as software applications, networks or supply chains.
In simple words, SPOF is caused when one critical system/device fails that it results in an entire system/architecture failure.

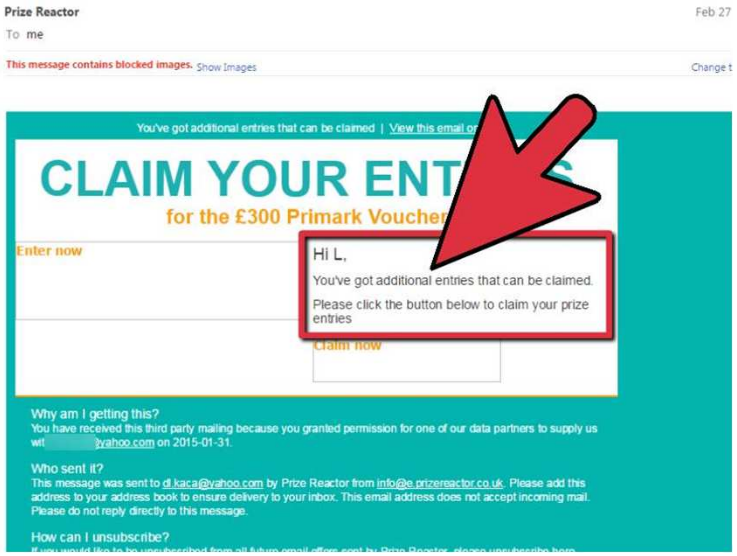
Countermeasures:

- At system levels, multiple machines or systems could provide required redundancy.
- Replication can be used at the site level, where another site or location is prepared to take over in the event of sudden site access failure.

Spamming

Spamming is the use of electronic messaging systems to send an unsolicited message (spam), especially advertising, as well as sending messages repeatedly on the same site. While the most widely recognized form of spam is email spam, the term is applied to similar abuses in other media.

Spam has become a constant fixture in our online lives. While it's easy to gloss over spam in your inbox, accidentally clicking a spam link can lead to virus infection and identity theft. Take the fight to the spammers by actively blocking the spam that you receive, as well as preventing future spam. Your inbox will thank you.



Prize Reactor
To me

Feb 27

This message contains blocked images. Show Images

Change t

You've got additional entries that can be claimed | View this email o

CLAIM YOUR ENT

for the £300 Primark Voucher

Enter now

Hi L,

You've got additional entries that can be claimed.

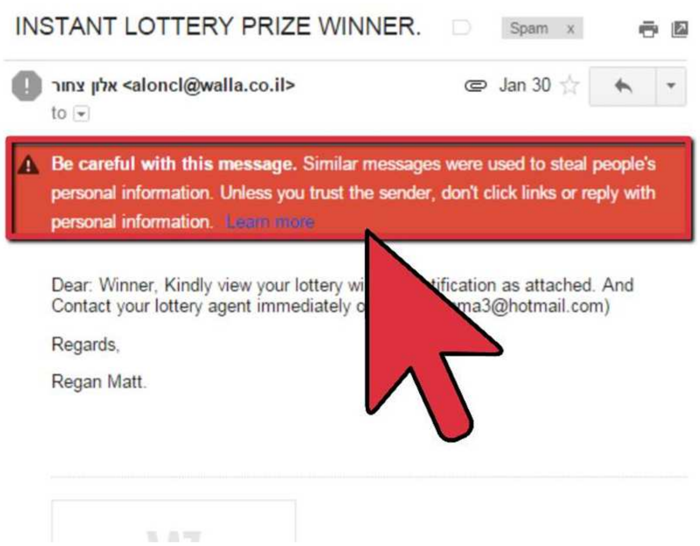
Please click the button below to claim your prize entries

Claim now

Why am I getting this?
You have received this third party mailing because you granted permission for one of our data partners to supply us wit[redacted]yahoo.com on 2015-01-31.

Who sent it?
This message was sent to dl.kaca@yahoo.com by Prize Reactor from info@e.prizereactor.co.uk. Please add this address to your address book to ensure delivery to your inbox. This email address does not accept incoming mail. Please do not reply directly to this message.

How can I unsubscribe?



INSTANT LOTTERY PRIZE WINNER.

Spam x

אלון צחור <aloncl@walla.co.il>
to

Jan 30

Be careful with this message. Similar messages were used to steal people's personal information. Unless you trust the sender, don't click links or reply with personal information. Learn more

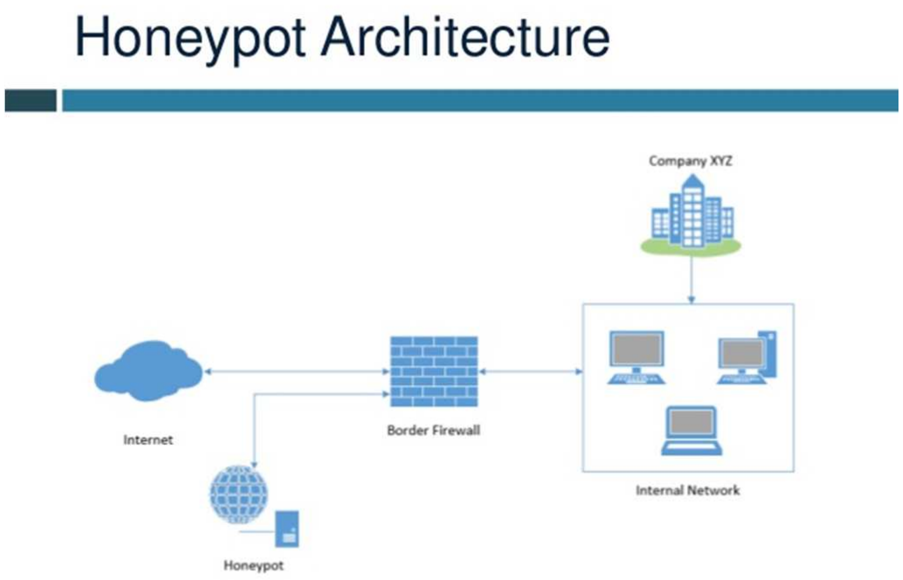
Dear: Winner, Kindly view your lottery wi tification as attached. And Contact your lottery agent immediately o ma3@hotmail.com)

Regards,

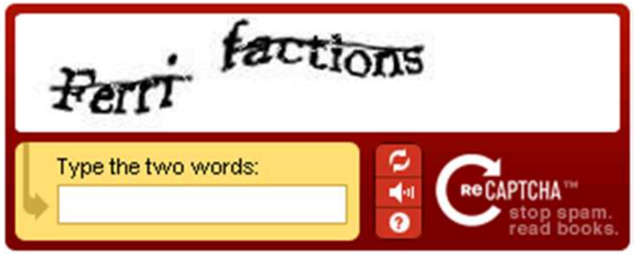
Regan Matt.

Countermeasures

CAPTCHAs
Filters
Honeypots



Honeypot Architecture



A watering hole attack

A watering hole attack is a malware attack in which the attacker observes the websites often visited by a victim or a particular group, and infects those sites with malware. A watering hole attack has the potential to infect the members of the targeted victim group. Although uncommon, a watering hole attack does pose a significant threat to websites, as these attacks are difficult to diagnose.

In watering hole attacks, the goal is not to serve malware to as many systems possible. Instead, the attackers run exploits on well-known and trusted sites likely to be visited by their targeted victims. This makes the watering hole technique effective in delivering its intended payload.

Aside from carefully choosing sites to compromise, watering hole attacks are known to incorporate zero-day exploits that target unpatched vulnerabilities. Thus, the targeted entities are left with little or no defense against these exploits.

This doesn’t mean that attackers don’t target patched system vulnerabilities. Because of patch management difficulties in an enterprise setting, IT administrators may delay deploying critical updates. This window of exposure may lead to a targeted attack leveraging old, but reliable vulnerabilities.

A watering hole attack

Who are the targets?
The watering hole technique is used in targeted attacks that aim to gather confidential information and intelligence from the following organizations:

- Various businesses
- Human rights groups
- Government offices

The stolen information, in turn, may be used to initiate more damaging attacks against the affected organization

Countermeasures

Timely software updating. For watering hole attacks that employ old vulnerabilities, an organization’s best defense is to update systems with the latest software patches offered by vendors.
Vulnerability shielding. Also known as “virtual patching,” it operates on the premise that exploits take a definable network path in order to use a vulnerability. Vulnerability shielding helps administrators scan suspicious traffic as well as any deviations from the typical protocols used. Thus, this monitoring empowers system administrators to prevent exploits.

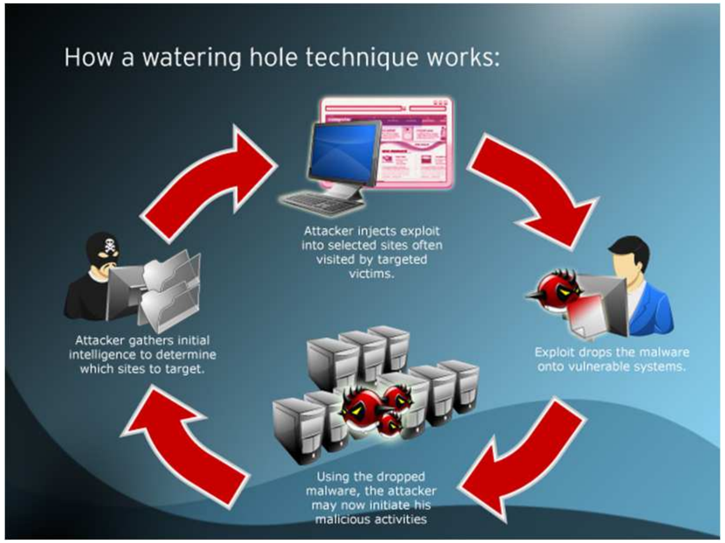
Countermeasures - Contd

A watering hole attack

Network traffic detection. Though attackers may incorporate different exploits or payloads in their attack, the traffic generated by the final malware when communicating with the command-and-control servers remains consistent. By detecting these communications, organizations can readily implement security measures to prevent the attack from further escalating. Technologies such as Trend Micro Deep Discovery can aid IT administrators in detecting suspicious network traffic.

Correlating well-known APT activities. Using big data analytics, organizations can gain insight on whether they are affected by a targeted attack by correlating and associating in-the-wild cybercrime activities with what is happening on an enterprise' network.

Organizations should also consider building their own local intelligence to document previous cases of targeted attacks within the company. These enable organizations to spot possible correlations and insights needed to create an effective action or recovery plan.



How a watering hole technique works:

Attacker gathers initial intelligence to determine which sites to target.

Attacker injects exploit into selected sites often visited by targeted victims.

Exploit drops the malware onto vulnerable systems.

Using the dropped malware, the attacker may now initiate his malicious activities

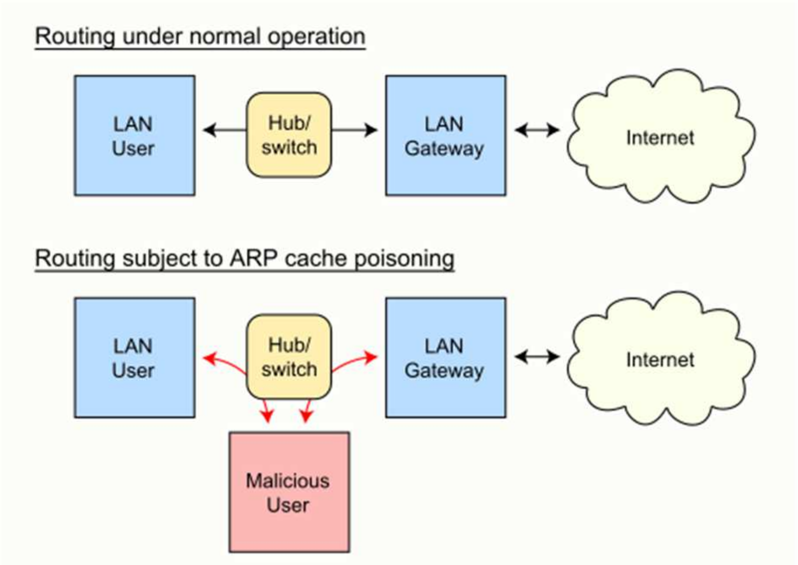
ARP poisoning

Address Resolution Protocol poisoning (ARP poisoning) is a form of attack in which an attacker changes the Media Access Control (MAC) address and attacks an Ethernet LAN by changing the target computer's ARP cache with a forged ARP request and reply packets. This modifies the layer -Ethernet MAC address into the hacker's known MAC address to monitor it. Because the ARP replies are forged, the target computer unintentionally sends the frames to the hacker's computer first instead of sending it to the original destination. As a result, both the user's data and privacy are compromised. An effective ARP poisoning attempt is undetectable to the user.

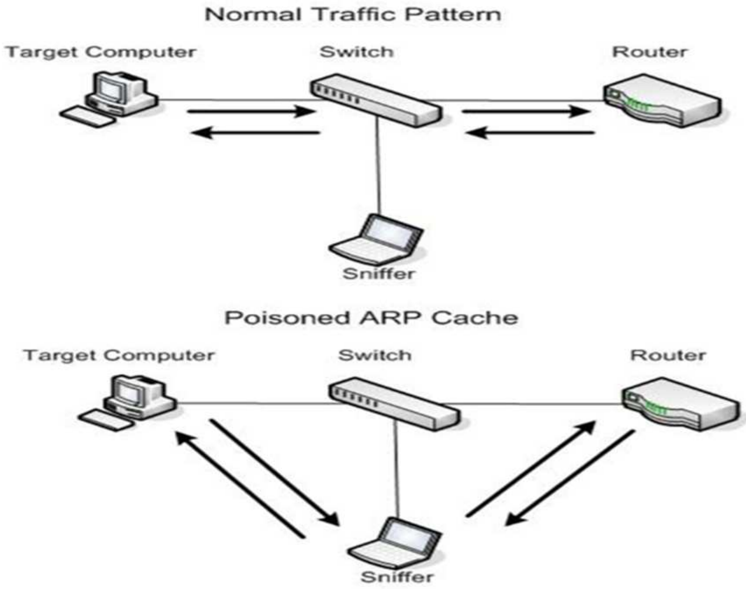
ARP poisoning is also known as ARP cache poisoning or ARP poison routing (APR).

ARP poisoning is very effective against both wireless and wired local networks. By triggering an ARP poisoning attack, hackers can steal sensitive data from the targeted computers, eavesdrop by means of man-in-the-middle techniques, and cause a denial of service on the targeted computer. In addition, if the hacker modifies the MAC address of a computer that enables Internet connection to the network, access to Internet and external networks may be disabled.

For smaller networks, using static ARP tables and static IP addresses is an effective solution against ARP poisoning. Another effective method for all kinds of networks is implementing an ARP monitoring tool.



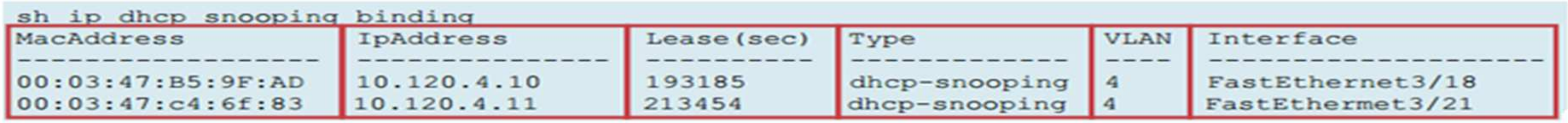
ARP poisoning



Countermeasures

Dynamic ARP inspection in cisco systems helps prevent the man-in-the-middle attacks by not relaying invalid or gratuitous ARP replies out to other ports in the same VLAN. Dynamic ARP inspection intercepts all ARP requests and all replies on the untrusted ports. Each intercepted packet is verified for valid IP-to-MAC bindings via DHCP snooping. Denied ARP packets are either dropped or logged by the switch for auditing so ARP poisoning attacks are stopped. Incoming ARP packets on the trusted ports are not inspected. Dynamic ARP inspection cans also rate-limit ARP requests from client ports to minimize port scanning mechanisms. Dynamic arp poisonings uses the information from DHCP Snooping table.

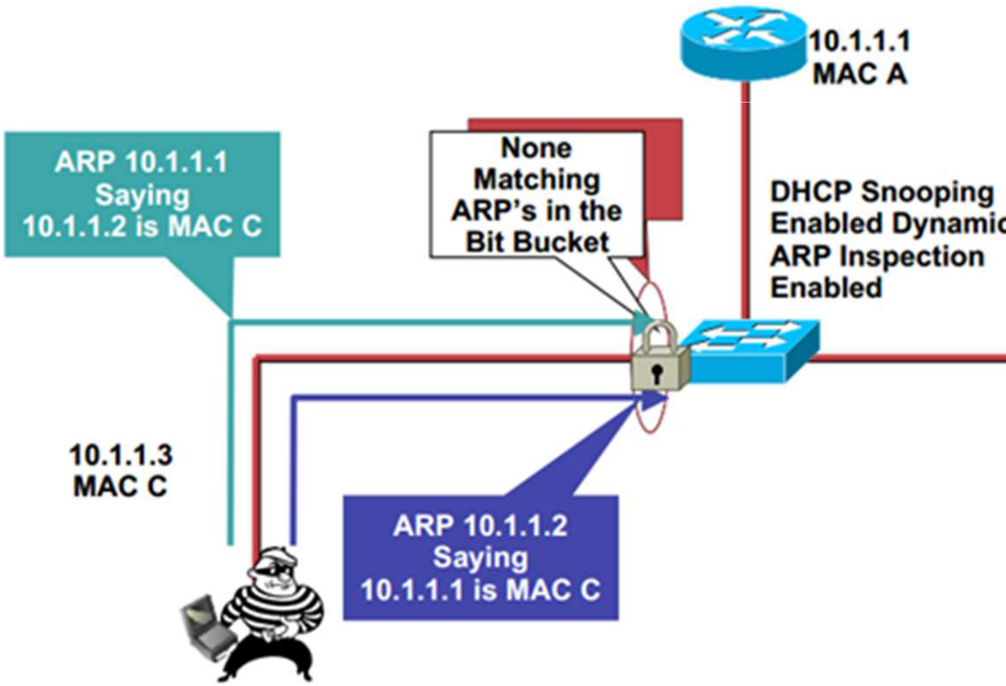
ARP poisoning



```
sh ip dhcp snooping binding
MacAddress          IpAddress        Lease(sec)  Type           VLAN  Interface
------------------  ---------------  ----------  -------------  ----  --------------------
00:03:47:B5:9F:AD   10.120.4.10      193185      dhcp-snooping  4     FastEthernet3/18
00:03:47:c4:6f:83   10.120.4.11      213454      dhcp-snooping  4     FastEthernet3/21
```

It Looks at the MacAddress and IpAddress fields to see if the ARP from the interface is in the binding, it not, traffic is blocked.

Dynamic ARP INSPECTION USES DHCP Snooping Table


10.1.1.1
MAC A
ARP 10.1.1.1 Saying 10.1.1.2 is MAC C
None Matching ARP's in the Bit Bucket
DHCP Snooping Enabled Dynamic ARP Inspection Enabled
10.1.1.3
MAC C
ARP 10.1.1.2 Saying 10.1.1.1 is MAC C
10.1.1.2
MAC B

- Uses the DHCP Snooping Binding table information
- Dynamic ARP Inspection
  - All ARP packets must match the IP/MAC Binding table entries
  - If the entries do not match, throw them in the bit bucket

Black hole attack

Black hole attack is a type of denial-of-service attack in which a router that is supposed to relay packets instead discards them. This usually occurs from a router becoming compromised from a number of different causes.

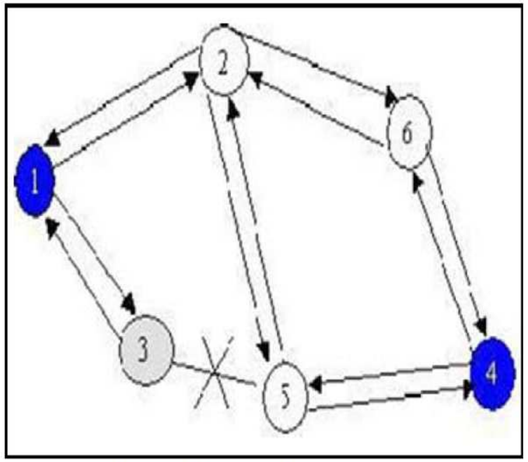


Fig. 2: Example of black hole attack

In the above diagram there is a Source node 1 want to transfer the packets to the destination node 4, other nodes are intermediate nodes. First of all source node sends the route request for sending the packets, that is called RREQ(3). When intermediate nodes receive RREQ then they will send reply of request that is called RREP. After the collecting of RREP from all the nodes, then it will send the packets based on their heights sequence number. Sequence number would generate on based of its algorithm which previously saved in nodes.

So source node will send the packets to the node having highest sequence number. The node which receive the packet it further transfer to other nodes, by this way packet should be reach up to the destination, but not necessary it should happen all the time. Sometimes a black hole node come in to existence which only receives the packet and not transfer it further to any other nodes. That node is called black hole node, and this attack is called black hole attack. In the above diagram we can watch node 3 is black hole node which further not transferring data to any other node.

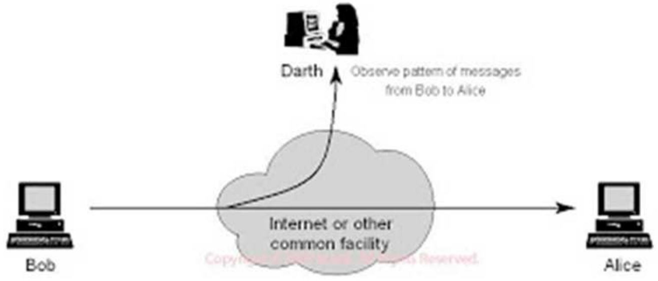
Countermeasure

- A DPRAODV (Detection, Prevention, and Reactive AODV) protocol is designed to prevent the black hole attack.
- Authentication mechanisms, based on the hash function are proposed to identify multiple black holes cooperating with each other.
- Wait and check the replies mechanism is also proposed to find a safe route for packets.
- Security-aware ad hoc routing protocol (SAR), is also proposed that can be used for protection against black hole attacks.
- Introduce route confirmation request CREQ and route confirmations reply CREP can also prevent black hole attacks.

Traffic analysis

Traffic analysis is a special type of inference attack technique that looks at communication patterns between entities in a system.

"Traffic analysis is the process of intercepting and examining messages in order to deduce information from patterns in communication. It can be performed even when the messages are encrypted and cannot be decrypted. In general, the greater the number of messages observed, or even intercepted and stored, the more can be inferred from the traffic. Traffic analysis can be performed in the context of military intelligence or counter-intelligence, and is a concern in computer security." Knowing who's talking to whom, when, and for how long, can sometimes clue an attacker in to information of which you'd rather she not be aware.


Darth
Observe pattern of messages from Bob to Alice
Internet or other common facility
Bob
Alice

Traffic Analysis (Passive Attacks)

Impact

- Disclosure about the identity of the communicating parties.
- Disclosure about the frequency of communication between two parties.
- Disclosure about the volume of communication between two parties.
- Disclosure about (some) content of the communication.
- Disclosure about the protocols in use, which allows an attacker to determine possible attack vectors.

Countermeasures

Protocol design for protection against traffic analysis is a very complicated process, equivalent to designing cryptographic algorithms, and possibly more difficult. Applications that require this level of secure communication should use an existing traffic-analysis resistant transport, like Tor, and take care to use it in ways which preserve its security properties.

Source routing Attack

Attackers use IP source route attacks to find the route that packets take through your network.

The attacker sends an IP packet and uses the response from your network to get information about the operating system of the target computer or network device.

Packet sender specifies precise path used for network troubleshooting and on token rings.

Ex. Trace route utility maps route through network

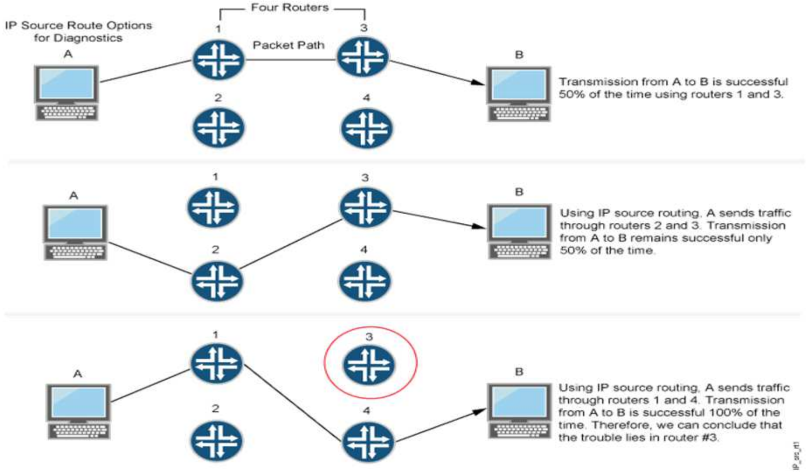
Benefits to attacker:

Trust (misplaced) on the network

Access to privately configured network

- May use Network Address Translation (NAT)
- NAT translates IP private address to public form

Countermeasure



Transmission from A to B is successful 50% of the time using routers 1 and 3.

Using IP source routing, A sends traffic through routers 2 and 3. Transmission from A to B remains successful only 50% of the time.

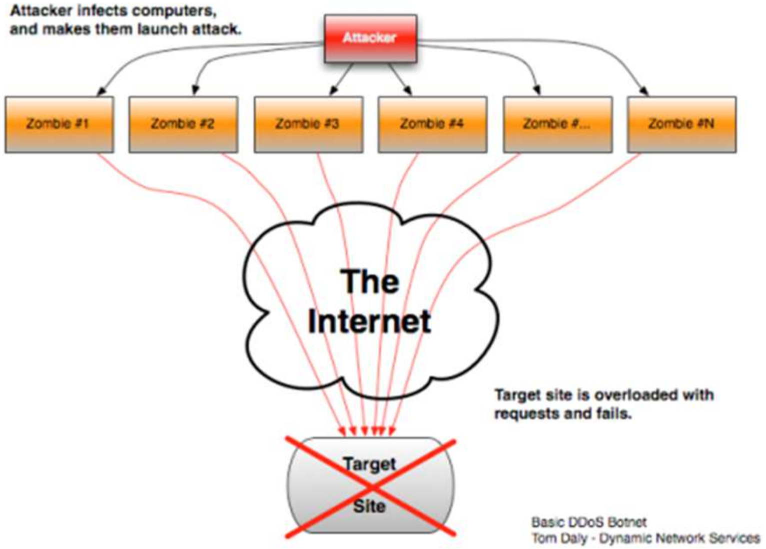
Using IP source routing, A sends traffic through routers 1 and 4. Transmission from A to B is successful 100% of the time. Therefore, we can conclude that the trouble lies in router #3.

DNS reflection

A DNS reflection DoS attack is an application-layer DoS attack that exploits vulnerabilities in DNS servers and insecurely configured networks.
In a DNS reflection DoS attack, a client, like a desktop, makes a forged DNS request from the distributed DoS (DDoS) target's IP and the DNS server sends a DNS response to a spoofed IP. The DNS response is relatively large, resulting in a large amount of traffic sent to a targeted host and thereby creating a denial of service. DNS reflection attacks differ from DDoS attacks by botnets in that the DNS servers are not responsible for maintaining secure networks.

Countermeasure

Restricting external access to open DNS resolvers could help reduce the impact of a DNS reflection DoS attack, along with throttling inbound and outbound DNS traffic at ISPs.
Organizations can also monitor their DNS servers and network. Spikes in bandwidth, a high number of queries for a specified name or IP, or malformed DNS packets may indicate that the organization is participating in an attack.



Attacker infects computers, and makes them launch attack.

Target site is overloaded with requests and fails.

Basic DDoS Botnet
Tom Daly - Dynamic Network Services

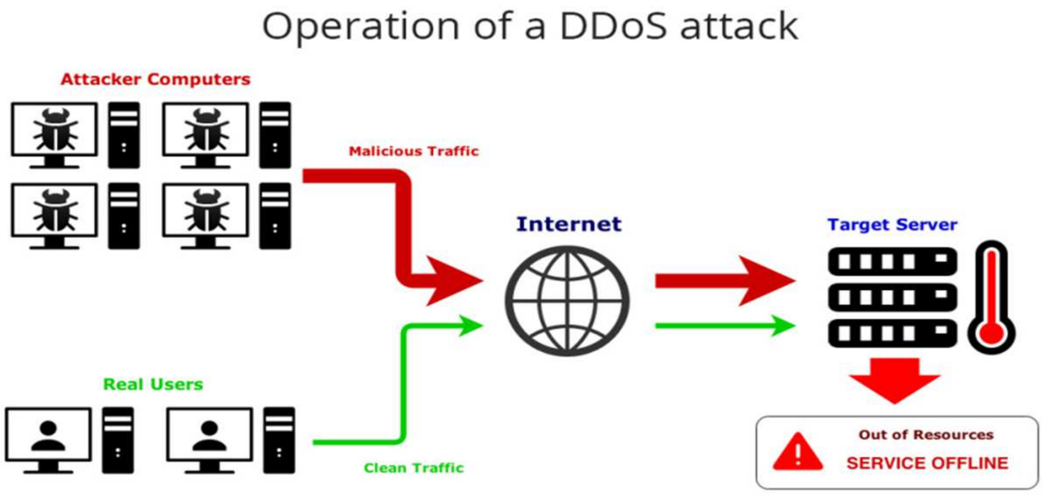
DDoS

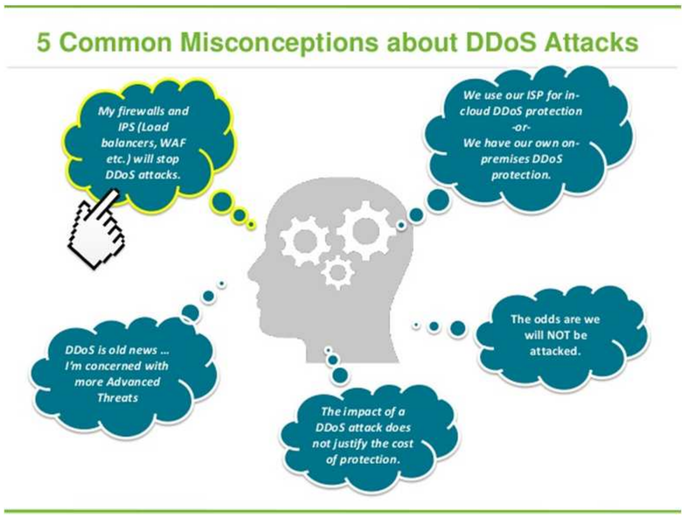
DDoS is a type of DOS attack where multiple compromised systems, which are often infected with a Trojan, are used to target a single system causing a Denial of Service (DoS) attack.

Victims of a DDoS attack consist of both the end targeted system and all systems maliciously used and controlled by the hacker in the distributed attack.

How it works:

In a DDoS attack, the incoming traffic flooding the victim originates from many different sources – potentially hundreds of thousands or more. This effectively makes it impossible to stop the attack simply by blocking a single IP address; plus, it is very difficult to distinguish legitimate user traffic from attack traffic when spread across so many points of origin.




5 Common Misconceptions about DDoS Attacks
My firewalls and IPS (Load balancers, WAF etc.) will stop DDoS attacks.
We use our ISP for in-cloud DDoS protection -or- We have our own on-premises DDoS protection.
DDoS is old news ... I'm concerned with more Advanced Threats
The odds are we will NOT be attacked.
The impact of a DDoS attack does not justify the cost of protection.

The Difference between DoS and DDos Attacks

A Denial of Service (DoS) attack is different from a DDoS attack.

- The DoS attack typically uses one computer and one Internet connection to flood a targeted system or resource.
- The DDoS attack uses multiple computers and Internet connections to flood the targeted resource. DDoS attacks are often global attacks, distributed via botnets.

Types of DDoS Attacks

- Traffic attacks: Traffic flooding attacks send a huge volume of TCP, UDP and ICPM packets to the target. Legitimate requests get lost and these attacks may be accompanied by malware exploitation.
- Bandwidth attacks: This DDos attack overloads the target with massive amounts of junk data. This results in a loss of network bandwidth and equipment resources and can lead to a complete denial of service.
- Application attacks: Application-layer data messages can deplete resources in the application layer, leaving the target's system services unavailable.

DDoS

You can’t prevent DoS assaults. The fact is that cybercriminals are going to attack. Some are going to hit their targets, regardless of the defenses in place.

However, there are steps you can take to spot a brewing storm, including:

- Monitoring your traffic to look for abnormalities, including unexplained traffic spikes and visits from suspect IP address and geolocations. All of these could be signs of attackers performing “dry runs” to test your defenses before committing to a full-fledged attack. Recognizing these for what they are can help you prepare for the onslaught to follow.
- Keep an eye on social media (particularly Twitter) and public waste bins (e.g., Pastebin.com) for threats, conversations and boasts that may hint on an incoming attack.
- Consider using third-party DDoS testing (i.e., pen testing) to simulate an attack against your IT infrastructure so you can be prepared when the moment of truth arrives. When you undertake this, test against a wide variety of attacks, not just those with which you are familiar.
- Create a response plan and a rapid response team, whose job is to minimize the impact of an assault. When you plan, put in place procedures for your customer support and communication teams, not just for your IT professionals.

What is Cyber Squatting?

Cybersquatting and Typo squatting (URL hijacking) attacks are aimed at exploiting human inattentiveness: one or two spelling mistakes when you type in a URL address and you might end at a phishing web site specifically created to steal your log in, personal or bank information. While this case is harmful to individual internet users, typo squatting (and its more recent variety, bit squatting) is also a sensitive issue for big brands and well-known organizations, including the government, educational, and healthcare institutions. A “confusingly similar” website can host untrue information and damage the company`s or person`s reputation as well as mislead a potential customer or a service user.

The key threats of Cybersquatting include, Phishing / password stealing, Client Malware infection, Information Stealing /Man in the Middle attacks (MTM), Spam, Malicious content publishing

Countermeasures and or Safeguards!?

- Implement mandatory usage of Digital signatures and Certificates in digital communication like mail, instant messaging, demo systems, etc.
- Create a list of possible malicious domains
- Implement filtering and logging of all attempts that are made to connect to or from similar domains
- Block suspicious domains on routers and mail-gateway
- Install antivirus software on mail-gateway
- Buy similar domains
- Use SSL on every public resource of Cybersquatting victims
- Use redirectors to secure the port and inform all clients that all Cybersquatting victim resources operate and are protected with SSL
- One of the solutions that`s been in practice for years is registering numerous domain names to protect your brand
- You can always file a complaint the downside of this particular approach, though, is the cost of filing a case and time it would take to win the case as well as implement the court decision.

What does Pharming mean?

Pharming refers to redirecting website traffic through hacking, whereby the hacker implements tools that redirect a search to a fake website. Pharming may cause users to find themselves on an illegitimate website without realizing they have been redirected to an impostor site, which may look exactly like the real site.

Pharming occurs when hackers locate vulnerabilities in domain name server (DNS) software. Pharming can also occur by rearranging the host’s file on the targeted computer. Online banking websites as well as e-commerce organizations have become popular pharming targets. Desktops are also vulnerable to pharming threats due to their lack of security administration. Pharming and phishing threats have been used simultaneously and these can cause the most potential for online identity theft.

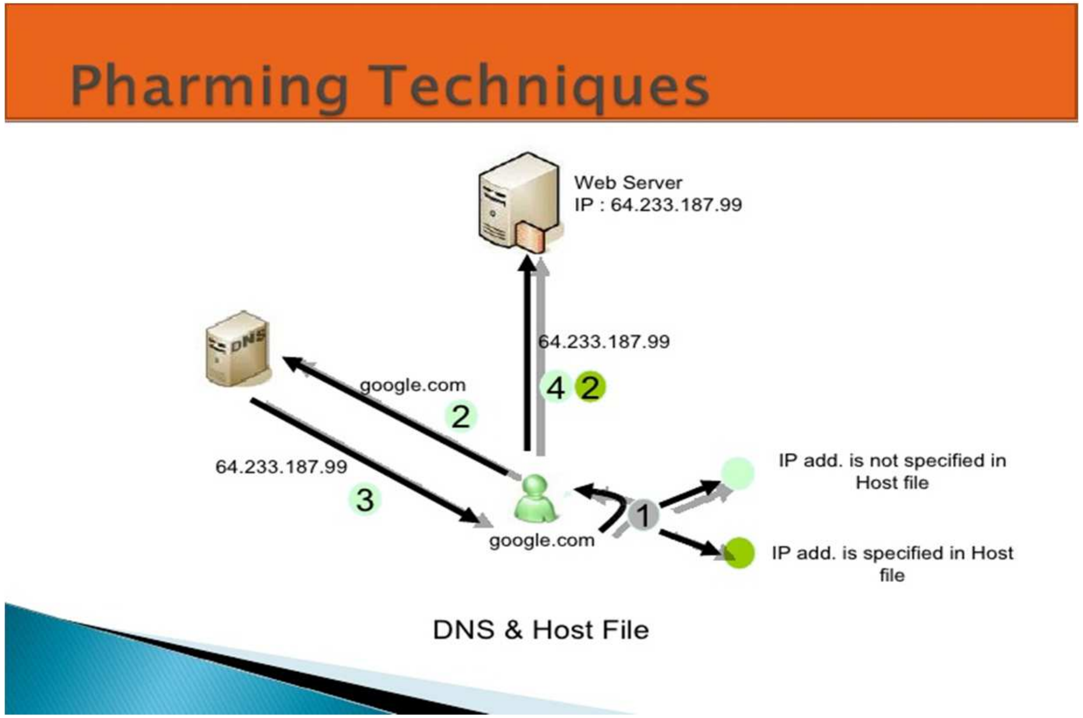
Countermeasures and or Safeguards!?

Internet service providers (ISPs) are working hard on their end to filter out pharmed sites. The main thing you can do to protect yourself on your end is to make sure the Web site is authentic. You need to use more than one method to stay ahead of the pharmers. Remember, most of these authentication methods are set up to work only on the pages where you're asked to enter your personal information.

- Use a trusted, legitimate Internet Service Provider. Rigorous security at the ISP level is your first line of defense against pharming.
- The attacker obscures the actual URL by overlaying a legitimate looking address or by using a similarly spelled URL. Check the Web browser's address bar to make sure the spelling is correct. For example, when you type http://www.google.com, you should see that address. But the address for a pharmed site might be http://www.nsgoogle.com.
- Check the http address. When you get to the page where you're asked to enter personal information, the http should change to https. The "s" stands for secure.
- Verify the certificate of the site. It takes just a few seconds to tell if a site you land on is legitimate. On the latest version of Internet Explorer and on many other commonly available Web browsers, go to "File" in the main menu and select "Properties," or right-click your mouse anywhere on the browser screen and, from the menu that pops up, click "Properties." When the "Properties" box opens, click "Certificates," and check if the site carries a secure certificate from its legitimate owner.

Pharming

- Look for a padlock or key on the bottom of your browser or your computer task bar. A locked padlock, or a key, indicates a secure, encrypted connection and an unlocked padlock, or a broken key, indicates an unsecured connection.
- Install an antivirus program from a trusted security software provider to reduce your exposure to pharming scams. Use a personal firewall to protect your data from hackers, viruses, worms, and Trojan horses.
- Download the latest security updates (or patches) for your Web browser and operating system.

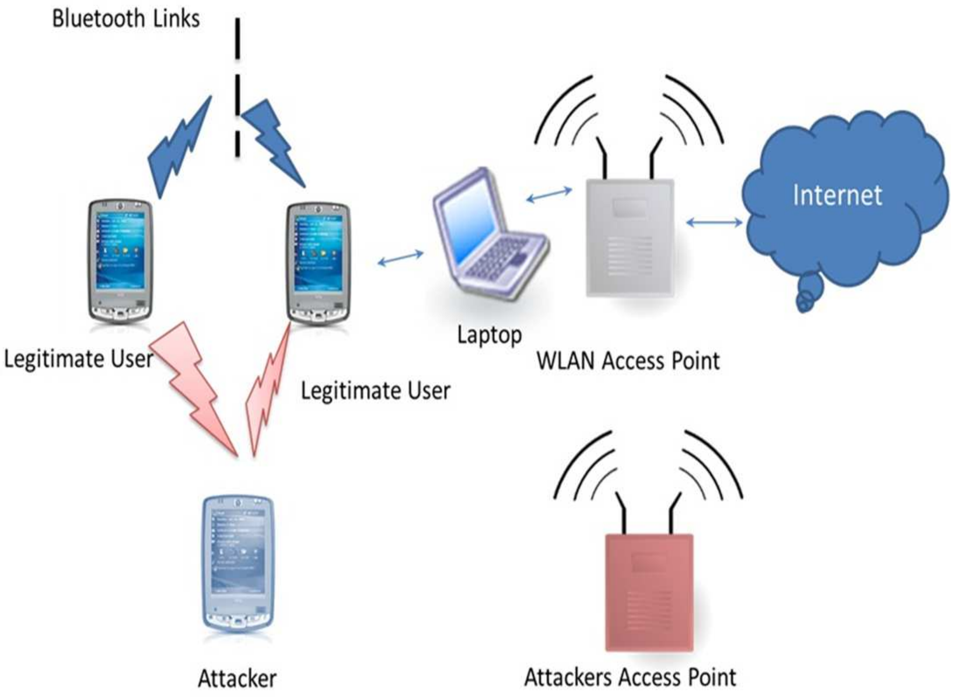


Pharming Techniques

DNS & Host File

What is Blue Jacking attack?

Blue jacking is the process of sending an anonymous message from a Bluetooth enabled phone to another, within a particular range without knowing the exact source of the received message to the recipient. Bluejacker will most likely comp out in crowded areas like shopping malls, airports- places with a potentially high percentage of people with Bluetooth enabled devices. Bluejacking is also known as bluehacking.



Countermeasures and Safeguards!?

The best way to protect a device, obviously, is to simply turn Bluetooth off. A device cannot be hacked via a Bluetooth attack vector if other Bluetooth devices cannot see it. Some devices come with Bluetooth turned on by default so users need to check this setting. If Bluetooth must be enabled, the user can set the device to be hidden .Setting a device to be invisible will still allow Bluetooth communications to function but will only allow connections to trusted devices that have been previously configured. This protection is not perfect, however; if an attacker finds out that a particular device is trusted, they can use their own Bluetooth device as the trusted device and will then be able to connect to the target phone If a user must use Bluetooth, they should also only turn it on as needed. In addition, users should change their Bluetooth personal identification number (PIN) every month or so. Changing the PIN requires that any Bluetooth devices that the user regularly employs will need to be re-paired, but it also makes it a bit harder for attackers. Attacks succeed because many users will balk at constantly turning their Bluetooth port on and off, or changing the PIN, but at the very least users should change the default PIN when they first get their Bluetooth enabled device.

User must use updated software and drivers to take advantage of product improvements and security fixes .It's also recommended to stop using a non supported or not secure Bluetooth-enabled devices or module, e.g. Bluetooth 1.0 and 1.2 For Android devices there are many Application available in Play store, for protecting device from Bluetooth hacking, some are mentioned below:- 1. BLUETOOTH

FIREWALL: Mobile Bluetooth Firewall protects our android device against all sort of Bluetooth attack from devices around us. It displays alerts when Bluetooth activities take place. You can also scan your device and detect apps with Bluetooth capabilities. So if you have installed a malicious app unknowingly this is the time to detect and uninstall it. 2. BLUETOOTH FILE TRANSFER: It provides custom security management for incoming BT connections, only authorized devices can connect, if you accept. If you refuse, no access is granted on your servers, personal data files and privacy are safe against hackers.

What does Blue Snarfing mean?

The term ”snarf” means grabbing a large document or file and using it without the author’s permission. Blue snarfing is considered a serious compromise in the category of Bluetooth hacking especially if the information vulnerable, is quite critical, as such attacks can allow the hacker access to victims; contact list, text messages, emails and even private photos and videos. Any device with its Bluetooth connection turned on and set to "discoverable" (able to be found by other Bluetooth devices in range) may be susceptible to Bluesnarfing if there is vulnerability in the vendor's software. By turning off this feature, the potential victim can be safer from the possibility of being Blue Snarfed; although a device that is set to "hidden" may be Blue Snarfable by guessing the device's MAC address via a brute force attack. As with all brute force attacks, the main obstacle to this approach is the sheer number of possible MAC addresses. Bluetooth uses a 48-bit unique MAC Address, of which the first 24 bits are common to a manufacturer. The remaining 24 bits have approximately 16.8 million possible combinations, requiring an average of 8.4 million attempts to guess by brute force.

Countermeasures and or Safeguards!?

The best way to protect a device, obviously, is to simply turn Bluetooth off. A device cannot be hacked via a Bluetooth attack vector if other Bluetooth devices cannot see it. Some devices come with Bluetooth turned on by default so users need to check this setting. If Bluetooth must be enabled, the user can set the device to be hidden .Setting a device to be invisible will still allow Bluetooth communications to function but will only allow connections to trusted devices that have been previously configured. This protection is not perfect, however; if an attacker finds out that a particular device is trusted, they can use their own Bluetooth device as the trusted device and will then be able to connect to the target phone If a user must use Bluetooth, they should also only turn it on as needed. In addition, users should change their Bluetooth personal identification number (PIN) every month or so. Changing the PIN requires that any Bluetooth devices that the user regularly employs will need to be re-paired, but it also makes it a bit harder for attackers. Attacks succeed because many users will balk at constantly turning their Bluetooth port on and off, or changing the PIN, but at the very least users should change the default PIN when they first get their Bluetooth enabled device.

Blue snarfing

User must use updated software and drivers to take advantage of product improvements and security fixes .It’s also recommended to stop using a nonsupported or not secure Bluetooth-enabled devices or module, e.g. Bluetooth 1.0 and 1.2 For Android devices there are many Application available in Play store, for protecting device from Bluetooth hacking, some are mentioned below:-

1. BLUETOOTH FIREWALL: Mobile Bluetooth Firewall protects our android device against all sort of Bluetooth attack from devices around us. It displays alerts when Bluetooth activities take place. You can also scan your device and detect apps with Bluetooth capabilities. So if you have installed a malicious app unknowingly this is the time to detect and uninstall it.
2. BLUETOOTH FILE TRANSFER: It provides custom security management for incoming BT connections, only authorized devices can connect, if you accept. If you refuse, no access is granted on your servers, personal data files and privacy are safe against hackers.

What does Blue bugging mean?

The third type of hacking mechanism is blue bugging. It goes well beyond Blue jacking and Blue snarfing in which the hacker uses sophisticated attacks to gain control of victim's mobile i.e. virtually complete takeover of a victims mobile. In this hacker can manipulate the users phone the way he desires by executing commands on the victims phone. The hacker could forward mobile calls from the victim's mobile to his own device and can even manipulate the mobile to follow a Bluetooth headset instructions like; receive call, send messages etc. They can even alter the call list, read the phone call list to see who their victims called or who called them.

Countermeasures and or Safeguards!?

The best way to protect a device, obviously, is to simply turn Bluetooth off. A device cannot be hacked via a Bluetooth attack vector if other Bluetooth devices cannot see it. Some devices come with Bluetooth turned on by default so users need to check this setting. If Bluetooth must be enabled, the user can set the device to be hidden .Setting a device to be invisible will still allow Bluetooth communications to function but will only allow connections to trusted devices that have been previously configured. This protection is not perfect, however; if an attacker finds out that a particular device is trusted, they can use their own Bluetooth device as the trusted device and will then be able to connect to the target phone. If a user must use Bluetooth, they should also only turn it on as needed.

Blue bugging

In addition, users should change their Bluetooth personal identification number (PIN) every month or so. Changing the PIN requires that any Bluetooth devices that the user regularly employs will need to be re-paired, but it also makes it a bit harder for attackers. Attacks succeed because many users will balk at constantly turning their Bluetooth port on and off, or changing the PIN, but at the very least users should change the default PIN when they first get their Bluetooth enabled device.

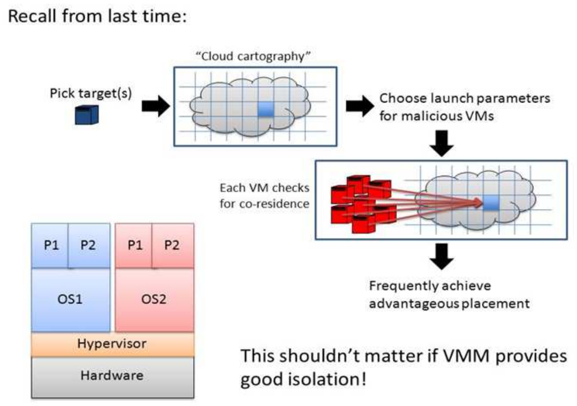
User must use updated software and drivers to take advantage of product improvements and security fixes .It’s also recommended to stop using a nonsupported or not secure Bluetooth-enabled devices or module, e.g. Bluetooth 1.0 and 1.2 For Android devices there are many Application available in Play store, for protecting device from Bluetooth hacking, some are mentioned below:-

1. BLUETOOTH FIREWALL: Mobile Bluetooth Firewall protects our android device against all sort of Bluetooth attack from devices around us. It displays alerts when Bluetooth activities take place. You can also scan your device and detect apps with Bluetooth capabilities. So if you have installed a malicious app unknowingly this is the time to detect and uninstall it.
2. BLUETOOTH FILE TRANSFER: It provides custom security management for incoming BT connections, only authorized devices can connect, if you accept. If you refuse, no access is granted on your servers, personal data files and privacy are safe against hackers.

What does Side Channel Attack (aka Cloud Cartography) mean?

Cloud cartography refers to figuring out the physical locations of hardware installations used by cloud computing service providers. Mapping a service provider’s hardware can help identify the most likely locations for a virtual machine, or help viewers to generally understand where the service provider deploys hardware.

While cloud cartography can help legitimate users make the services of a cloud provider more efficient, critics of this kind of mapping tend to point out that cloud cartography can leave service providers vulnerable to some types of liabilities from outside hackers or attackers. In theory, hackers could use cloud cartography approaches to figure out where virtual machines are and then create what are called side channel attacks. In this type of attack, an outside party would identify a location for virtual machines, and then place their own virtual machines co-resident with those being operated by the cloud service provider. This could result in the exploitation of specific vulnerabilities in service provider software, and could lead to data theft or similar outcomes.



Recall from last time:

“Cloud cartography”
Pick target(s)
Choose launch parameters for malicious VMs
Each VM checks for co-residence
Frequently achieve advantageous placement
P1
P2
P1
P2
OS1
OS2
Hypervisor
Hardware

This shouldn’t matter if VMM provides good isolation!

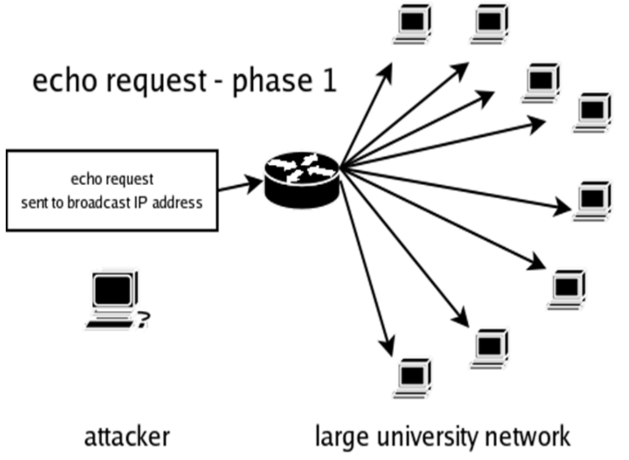
What is Ping Flood attack mean?

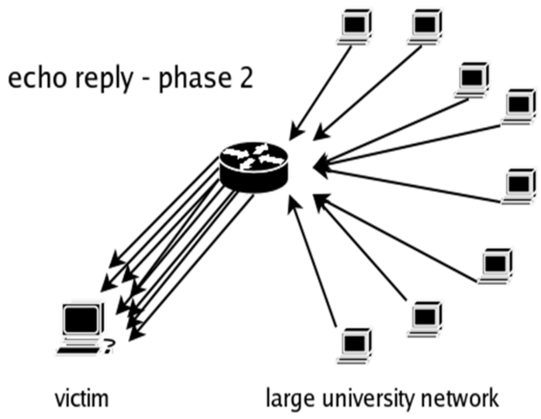
Ping flood, also known as ICMP flood, is a common Denial of Service (DoS) attack in which an attacker takes down a victim's computer by overwhelming it with ICMP echo requests, also known as pings.

The attack involves flooding the victim's network with request packets, knowing that the network will respond with an equal number of reply packets. Additional methods for bringing down a target with ICMP requests include the use of custom tools or code, such as hping and scapy.

This strains both the incoming and outgoing channels of the network, consuming significant bandwidth and resulting in a denial of service.

Normally, ping requests are used to test the connectivity of two computers by measuring the round-trip time from when an ICMP echo request is sent to when an ICMP echo reply is received. During an attack, however, they are used to overload a target network with data packets.





Ping flood

Executing a ping flood is dependent on attackers knowing the IP address of their target. Attacks can therefore be broken down into three categories, based on the target and how its IP address is resolved.

A targeted local disclosed ping flood targets a single computer on a local network. An attacker needs to have physical access to the computer in order to discover its IP address. A successful attack would result in the target computer being taken down.

A router disclosed ping flood targets routers in order to disrupt communications between computers on a network. It is reliant on the attacker knowing the internal IP address of a local router. A successful attack would result in all computers connected to the router being taken down.

A blind ping flood involves using an external program to uncover the IP address of the target computer or router before executing an attack.

Note that in order for a ping flood to be sustained, the attacking computer must have access to more bandwidth than the victim. This limits the ability to carry out a DoS attack, especially against a large network.

Countermeasures and or Safeguards !?

Reconfiguring your perimeter firewall to disallow pings will block attacks originating from outside your network, albeit not internal attacks. Still, the blanket blocking of ping requests can have unintended consequences, including the inability to diagnose server issues.

What does Smurf Attack (ICMP) mean?

Smurf is named after the DDoS Smurf malware that enables it execution.

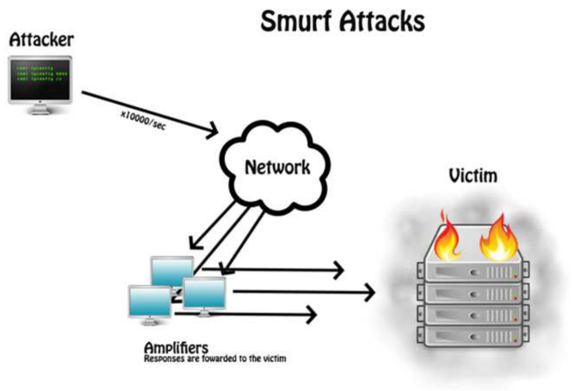
Smurf attacks are somewhat similar to ping floods or ICMP floods, as both are carried out by sending a slews of ICMP Echo request packets.

Unlike the regular ping flood, however, Smurf is an amplification attack vector that boosts its damage potential by exploiting characteristics of broadcast networks.

In a standard scenario, host A sends an ICMP Echo (ping) request to host B, triggering an automatic response. The time it takes for a response to arrive is used as a measure of the virtual distance between the two hosts.

In an IP broadcast network, a ping request is sent to every host, prompting a response from each of the recipients. With Smurf attacks, perpetrators take advantage of this function to amplify their attack traffic.

Smurf attack occurs in network layer of OSI Model.



Smurf attack

Countermeasures and or Safeguards!?

In addition to showing good internet citizenship, this should incentivize operators to prevent their networks from being unwitting Smurf attack participants.

To accomplish this you can:

Disable IP-directed broadcasts on your router.

Reconfigure your operating system to disallow ICMP responses to IP broadcast requests.

Reconfigure the perimeter firewall to disallow pings originating from outside your network.

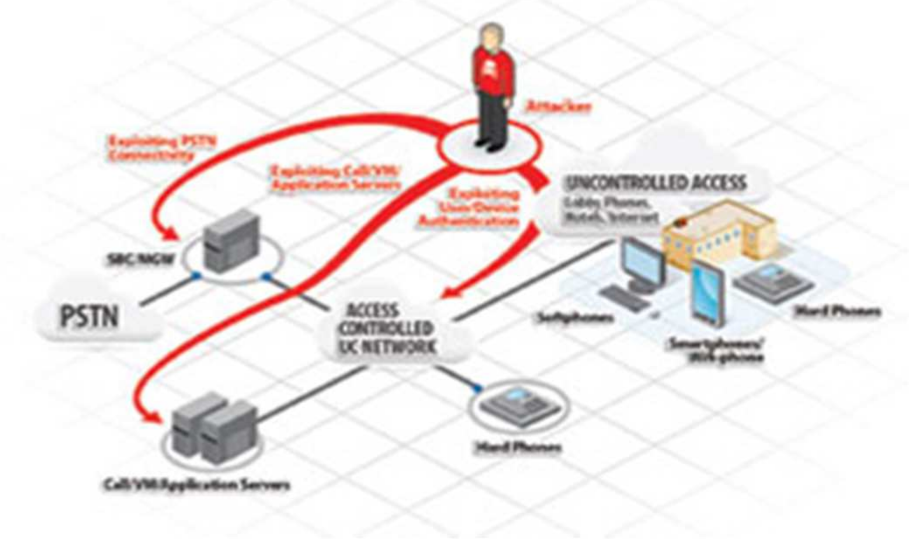
Smurf attack mitigation relies on a combination of capacity over provisioning (CO) and an existence of filtering services to identify and block illegal ICMP responses.

Through inspection of incoming traffic, all illegal packets—including unsolicited ICMP responses—are identified and blocked outside of your network.

What does Phreaking mean?

Phreaking is an old term to describe the activity of gaining access to a corporate telecom infrastructure. Phreakers would generally explore telecommunications systems for fun, or to get free long distance service. With the rise of VOIP technology, phreaking has gained a new dimension of threat to the enterprise, as well as a new generation of devotees. Successful phreaking of an enterprise voice network can yield access not only to critical voice infra, but to data networks as well, from which phreakers can pretty much have their way with the electronic infra of an enterprise.

Phreaking occurs at Datalink Layer of OSI Model


Attacker
Exploiting PSTN Connectivity
Exploiting Call/VM/ Application Servers
Exploiting User/Device Authentication
UNCONTROLLED ACCESS
Lobby Phones, Hotels, Internet
SBC/MGW
PSTN
ACCESS CONTROLLED UC NETWORK
Softphones
Smartphones/ Wifi phone
Hard Phones
Hard Phones
Call/VM/Application Servers

Countermeasures and or Safeguards !?

The best solution to prevent phreaking is an integrated approach that combines security, management and performance tools.

Telecom managers can use the Voice Firewall to protect the perimeter of the voice network from phreaking attacks. The voice network can automatically terminate any calls that fit pre-determined policies identifying call patterns that are likely phreaking attacks. Telecom managers should get visibility both into calling patterns across the network and into the current health-and-status of the voice network by using specialized tools, helping to identify phreaking activity as well as areas in the network that may be vulnerable to attack.

Scavenging Attack

Data-Scavenging Attacks : Data scavenging is the technique of piecing together information from found bits of data. There are two common types of data-scavenging attacks:

Keyboard Attacks :- Data scavenging through the resources that are available to normal system users who are sitting at the keyboard and using normal utilities and tools to glean information.

Laboratory Attacks:- Data scavenging by using very precise electronic equipment; these are planned, orchestrated attacks.

Countermeasures

Establish a disposal.
Prevent eavesdropping.

Data Diddling

Data diddling involves alteration of existing data and is extremely common. It is one of the easiest types of crimes to prevent by using access and accounting controls, supervision, auditing, separation of duties, and authorization limits. It is a form of active attack.

Countermeasures for all Data Diddling attacks are:

Disable all services that are not explicitly required.

Install security patches for applications as soon as they are available.

Audit logs and audit log review to identify unauthorized activity especially in databases.

Install anti-virus and anti-spyware.

Scan for malware code.

For developer-installed backdoors, disable them, change the defaults, or block access.

For malicious, user-installed backdoors, use access control management and controlled software deployment.

For device backdoors, maintain physical access control.

Implement strict coding standards to eliminate the potential for weaknesses.

Salami Attack

•A *salami attack* is collecting small amounts of data in order to build something of greater value and involves an attacker changing the information in a database. The attacker steals a little bit at a time over a long period of time from a large number of transactions. In a salami attack, the attacker:

•Gains access to the database.

•Modifies a calculation to round down.

•Sends the remainder to the attacker's account.

Countermeasures for all Salami attacks are:

Disable all services that are not explicitly required.

Install security patches for applications as soon as they are available.

Audit logs and audit log review to identify unauthorized activity especially in databases.

Install anti-virus and anti-spyware.

Scan for malware code.

For developer-installed backdoors, disable them, change the defaults, or block access.

For malicious, user-installed backdoors, use access control management and controlled software deployment.

For device backdoors, maintain physical access control.

Implement strict coding standards to eliminate the potential for weaknesses

LAND Attack

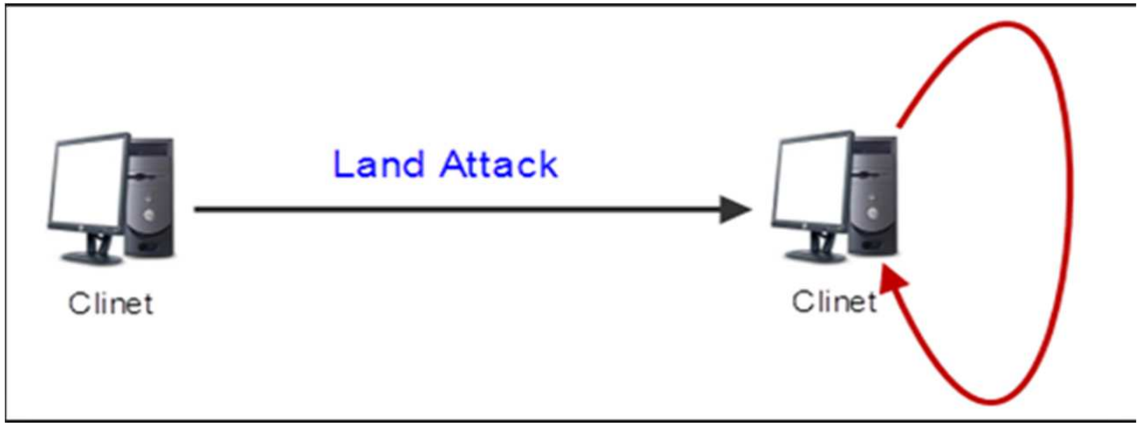
•A *Land* attack is one in which the attacker floods the victim's system with packets that have forged headers. In a Land attack:

•The packets have the same source and destination address (the victim's).

•The victim's system has no procedure to deal with these packets.

•The victim's system holds the packets in RAM.

•As the victim's system continues to hold more and more packets in RAM, it is unable to process legitimate requests.



Land attack

Countermeasures for DoS and DDoS attacks are:

- Intrusion Detection Systems (IDS) and an Intrusion Protection Systems (IPS).
- Strong anti-virus and anti-spyware software on all systems with Internet connectivity.
- File and folder hashes on system files and folders to identify if they have been compromised.
- Reverse DNS lookup to verify the source address.
- External firewalls with the following filters:
  - Ingress filters that specify any inbound frame must have a public IP address from outside of the organization's LAN.
  - Egress filters that specify any outbound frame must have a private IP address within the organization's LAN.
  - Address filter to prevent traffic from specific attackers (if known).
- Once a DoS attack begins, you can minimize its effects by implementing filters to block unwanted traffic. You can also contact your ISP to implement filtering closer to the source and reduce the bandwidth used by the attack.
- Hardening practices on all machines, especially publicly exposed servers and directory and resource servers.

War Driving

Wardriving is the act of searching for Wi-Fi wireless networks by a person in a moving vehicle, using a portable computer, smartphone or personal digital assistant (PDA).

Countermeasure

- Disable SSID
- Use strong Encryption
- Secure the Wifi with Password

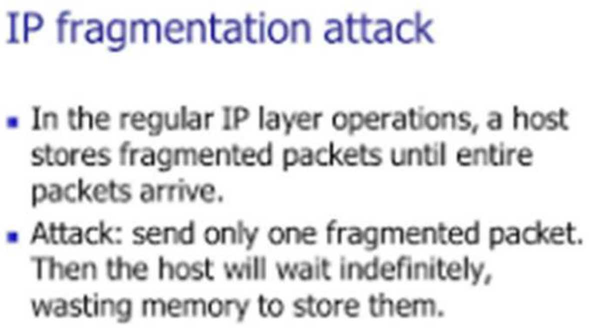
A free public Wi-Fi access point

IP Fragmentation Attack

- IP fragmentation is the process of breaking up a single Internet Protocol (IP) datagram into multiple packets of smaller size. Every network link has a characteristic size of messages that may be transmitted, called the maximum transmission unit (MTU).
- TYPES OF ATTACKS :-
  - UDP and ICMP fragmentation attacks.
  - TCP fragmentation attacks (a.k.a. Teardrop)

Countermeasures :

- Inspecting incoming packets for violations of fragmentation rules (e.g., using a router or a secured proxy).



IP fragmentation attack

- In the regular IP layer operations, a host stores fragmented packets until entire packets arrive.
- Attack: send only one fragmented packet. Then the host will wait indefinitely, wasting memory to store them.

Vishing Attack

The term is a combination of “voice” and phishing. Vishing is the criminal act of using voice email, VoIP (Voice Over Internet Protocol), landline or cellular telephone to gain access to private, personal and financial information from the public for the purpose of financial reward by committing identity theft. It is typically used to steal credit card numbers by a scammer who usually pretends to be in legitimate business

Typically attackers use a technique called caller ID spoofing to make it look like calls are coming from a legitimate or known phone number. It's a very similar technique to email spoofing, which makes e-mail addresses look like they are coming from a trusted source. But because people typically trust the phone service and caller ID, spoofing phone numbers can be particularly damaging.

And just like with online phishing attacks, which direct consumers to phony Web sites, vishing attacks usually have a recorded message that tells users to call a toll-free number. The caller is then typically asked to punch in a credit card number or other personal information. In the case of the warranty scams, users are asked to buy a bogus extended warranty for their car, which can cost anywhere between $2,000 and $3,000.

Countermeasures

Be suspicious of all unknown callers. People should be just as suspicious of phone calls as they are of e-mails asking for personal information. And some experts suggest letting all calls from unknown callers go to voicemail.

Don't trust caller ID. Just because your caller ID displays a phone number or name of a legitimate company you might recognize, it doesn't guarantee the call is really coming from that number or company. As explained earlier, caller ID spoofing is easy.

Ask questions. If someone is trying to sell you something or asking for your personal or financial information, ask them to identify who they work for, and then check them out to see if they are legitimate.

Call them back. Again if someone is selling you something or asking for information, tell them you will call them back and then either verify the company is legitimate, or if it's a bank or credit card company, call them back using a number from your bill or your card. Never provide credit card information or other private information to anyone who calls you.

TOC/TOU

Time-of-check-to-time-of-use (TOCTTOU - pronounced TOCK-too) is a file-based race condition that occurs when a resource is checked for a particular value, such as whether a file exists or not, and that value then changes before the resource is used, invalidating the results of the check.

Countermeasure

- Software lock

DNS/ **Cache** Poisoning

With DNS poisoning, the DNS server is given information that it thinks is legitimate when it isn't.

Domain Name Service(DNS)

Purpose

➢Translates URLs to IP Address

Creates mapping of IP address to URLs . So users need only to remember URLs not IP addresses.

TYPES

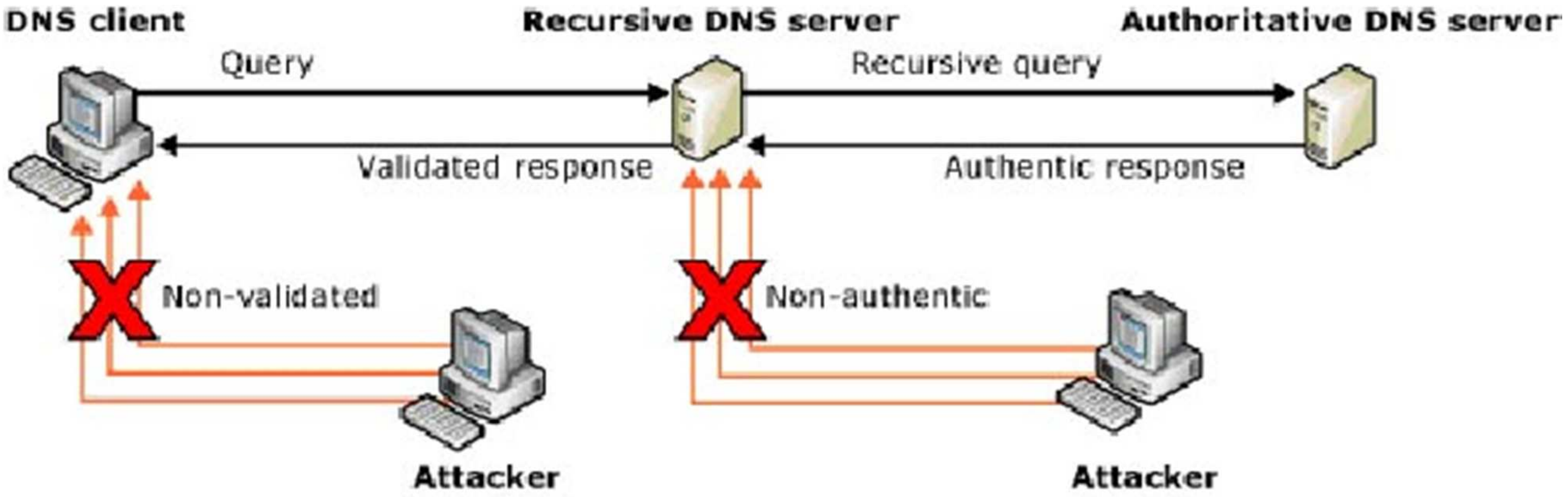
- **DNS Poisoning**
  - ➢DNS servers store its information (resource records) either in database files or as cached data. This information can be falsified or 'poisoned'.

This can send users to a website other than the one they wanted to go to, reroute mail, or do any other type of redirection wherein data from a DNS server is used to determine a destination.

- **DNS Cache Poisoning**
  - ➢Attach DNS Server and Inject poison record into cache

DNS Cache - Query Operation

- User types URL address say “cnn.com” in browser. The local DNS Server check for it in cache and ‘A’ records list. If not available this issue query to recursive(Go and Search for answer continuously) DNS server. It checks “cnn.com” mapped IP address in cache. If not exist then it will ask for answers with the authoritative servers(most dependable for certain zones). Once it receive the mapped IP address will store data in local cache and also send to the User. Translates URLs to IP Address



DNS Cache Attack consist of following

- Querying target (recursive) DNS Server for certain Domain, while it searching for answer
- Attacker will flood target the DNS Server with spoof replies with the queries that it is currently searching
- Goal - The idea is to get one of the spoof reply is accepted by DNS server. Attacker answer the query with spoof the reply before legitimate response reaches target DNS Server

- So the DNS server will end up caching the incorrect entries locally and serve them to users
- A user whose computer has referenced the poisoned DNS server could be tricked into accepting content coming from a non-authentic server and unknowingly download malicious content

Mitigation / Counter Measure

- **DNS poisoning** is difficult to defend against due to the attacks being mostly passive by nature. Typically, you will never know your DNS is being poisoned or spoofed until it has happened. That being said, there are still a few things that can be done to defend against these types of attacks:

  Secure your internal machines

  ▪Defending against internal threats and having a good internal security posture is always good

  ▪Don’t rely on DNS for secure systems – use local hosts file for sensitive name resolution data

  ▪Use IDS – monitor your network/host

  ▪Use DNSSEC – an updated and more secure version of DNS

Mitigation / Counter Measure

- **DNS Cache Poisoning** attack also be mitigated at the transport layer or application layer by performing end-to-end validation once a connection is established. A common example of this is the use of Transport Layer Security and digital signatures. For example, by using HTTPS (the secure version of HTTP), users may check whether the server's digital certificate is valid and belongs to a website's expected owner. Similarly, the secure shell remote login program checks digital certificates at endpoints (if known) before proceeding with the session. For applications that download updates automatically, the application can embed a copy of the signing certificate locally and validate the signature stored in the software update against the embedded certificate
- Secure modes of operation for DNS servers, such as switching to a TCP connection when potential attacks are detected, are another useful defense.

Typo squatting/URL hijacking

Cybersquatting or **URL Hijacking** simply means squatting or sitting on the cyber or domain name of someone else. It involves buying website URLs of popular business names or trademarks so that they can resell it at a cost. People started cybersquatting for personal gains, often monetary. Following a URL, if it leads to a parked website, site under construction and ‘site for sale’ web page, it is definitely a case of cybersquatting

Typo-squatting, is one of the variation of URL hijacking and most dangerous of its kind – often used for Phishing. Typos and misspellings are so common on the Internet that when a typical Internet user makes a mistake in the address bar when searching for a website, a typosquatter can take advantage of this opportunity to receive traffic for their own websites. He or she will buy domains looking like the genuine URL but actually contains a typo.

Typo squatting/URL hijacking

For example, to fool people, someone might buy linkdin.com or linked.in because linkedin.com already exists and is popular amongst career-minded people.

The intention in typosquatting is always harming people – stealing their identities and making profits while with cybersquatting, some of the cases might be genuine. Users might not have known about a company in some other part of the world and might have bought related URL. But For example, to fool people, someone might buy linkdin.com or linked.in because linkedin.com already exists and is popular amongst career-minded people. Though typosquatting is deliberate planning to skim Internet users.

Countermeasure

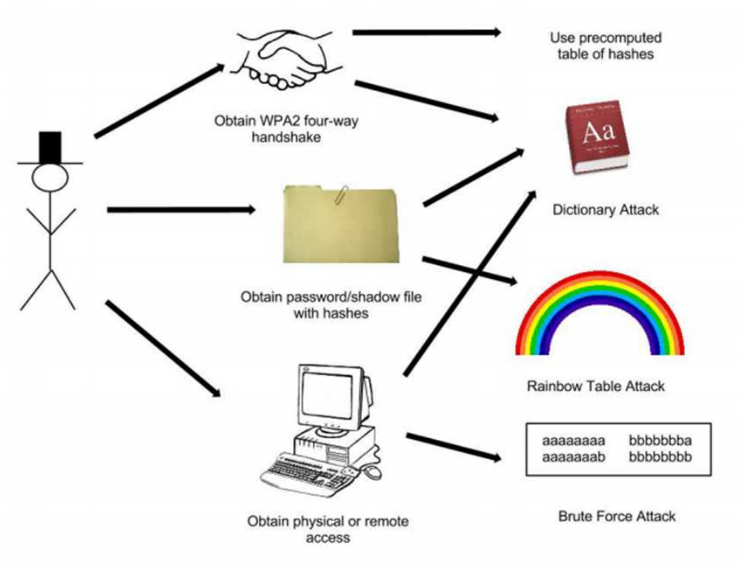
The best available solution to ensure protection against typosquatting involves identifying the most common typographical errors of that specific domain name and purchase them.

It is sometimes hard to prove that the person who is owning a cyber squatted domain actually did it with the intention to misuse your business name and reputation. You can either contact the site owner by sending cease letter and make him an offer or you may contact lawyers in your area and go ahead and file a case against cyber criminals. This is a decision you have to take. A legal proceeding takes up both time and money and as such, some people avoid that route and prefer to pay up. It also depends on the mindset of the other person. If he indeed is a cybersquatter, he is sure not to give in without a legal fight.

HYBRID ATTACK

A hybrid attack is a mixture of both a dictionary and brute force attack. That means that like a dictionary attack, you would provide a wordlist of passwords and a brute-force attack would be applied to each possible password in that list.

Both a dictionary and brute force attack are guessing attacks; they are not directly looking for a flaw or bypass. Either can be an offline attack or an online attack.


Obtain WPA2 four-way handshake
Obtain password/shadow file with hashes
Obtain physical or remote access
Use precomputed table of hashes
Aa
Dictionary Attack
Rainbow Table Attack
aaaaaaaa
aaaaaaab
bbbbbbba
bbbbbbbb
Brute Force Attack

HYBRID ATTACK

Brute Force Attack

Is an attempt to discover a password by systematically trying every possible combination of letters, numbers, and symbols until you discover the one correct combination that works.

Dictionary Attack

Typically, a guessing attack which uses precompiled list of options. Rather then trying every option, only try complete options which are likely to work.

It is a kind of brute force attack where the attacker is able to rate keys in order of most probable ... least probable, compile a list of the most probable (the dictionary), and test them in that order.

Trade Off

The main trade off between the two attacks is coverage versus time to complete. If you have a reasonable thought about what the password will be, you can skip unlikely answers and get a response in a faster amount of time.

Hybrids

Hybrids attacks which leverage both techniques in the interest of balancing the tradeoff.

Counter Measure

Following Techniques can be considered:

- For advanced users who want to protect their accounts from attack, give them the option to allow login only from certain IP addresses.
- Assign unique login URLs to blocks of users so that not all users can access the site from the same URL.
- Use a CAPTCHA to prevent automated attacks-presents the user with an obscured word that the user must type to pass the test.
- A completely automated public Turing test to tell computers and humans apart, or CAPTCHA, is a program that allows you to distinguish between humans and computers.
- Lock out accounts after a defined number of incorrect password attempts. Also instead of completely locking out an account, place it in a lockdown mode with limited capabilities.

Malicious Insider Threat

A security threat that originates from within the organization being attacked or targeted.

Types of Insider Threats
Insider threats can be organized into one of two general categories:

- **Deliberate/malicious insider.** When most people think of an insider threat, they immediately think of the malicious insider. This is someone who deliberately causes harm to an organization. Examples include Edward Snowden and Aldrich Ames, who were deliberate, malicious insiders working as a contractor and employee, respectively, for the United States government.

- **Accidental insider.** An accidental insider is someone who is tricked or manipulated into doing something that ultimately harms the organization. Some people further categorize the accidental insider threats into “the infiltrator” and “the ignorant insider.” The infiltrator situation occurs when an adversary accesses a user’s system or steals credentials to gain access to a system. The ignorant insider is a situation that occurs when an adversary convinces the user to click on a link or open an attachment, which ultimately causes the user’s system to be compromised. Since both cases are caused by a user action that ultimately results in a system or account being compromised, we group these types of threats together.

An employee can become a **malicious insider threat** when there is job frustration, persuasion by a competitor who is trying to hire him or a financial motive. Based on the lack of security and control around critical information, the malicious insider will often copy large amounts of proprietary data either to the cloud, a USB device or a personal device. While this seems very simple and basic, it is extremely effective and happens on a regular basis.

Malicious Insider Threat

When concerned about the insider threat, ask yourself these questions:

- Do you know all locations where your critical data resides?
- Do you know who has access to your critical data?
- What is the probability that critical data resides on personal devices?
- What is the probability that critical data resides on employees' home devices?

A second type **of insider attack** can occur when an adversary finds a target within the organization. The adversary performs extensive research to discover specific details about the insider's job and personal life that can be used in a well-crafted email that looks legitimate and contains an embedded link or an attachment. When the user clicks on the link or opens the attachment, the user's system becomes infected or the credentials are stolen. Once again, the attack vectors are simple, but very effective.

To prevent it is critical to understand how the adversary works and operates

STEP 1 : Reconnaissance or information gathering

Using social media to find out details about the target's personal life

STEP 2 : Develop attack model

Design the attack by understanding how people respond and react in a given situation, which is known as predictable response

STEP 3 : Determination of attack method

Sending Email that has an embedded link or an attachment.

STEP 4 : Attack/exploitation

The ultimate goal of an attack is to gain access and compromise critical data by data aggregation and exploitation(modify, delete or copy etc)

STEP 5 : Longevity/maintaining access

Will create backdoors or additional methods for readily gaining access to the organization, providing multiple points of entry and alternatives

STEP 6 : Pivoting and internal reconnaissance

Once inside the network, use that to pivot deeper and deeper until he ultimately finds the target system

STEP 7 : Hiding/covering their tracks

Delete logs and modifying files so there is no evidence of the attack left on any system within the network.

Prevention and Mitigation

- Enforce clear security policies and guidelines to minimize the risk posed by both intentional and unintentional security incidents.
- Implement the rule of least privilege which indicates that employees should only have access to information resources necessary to perform their daily tasks.
- Access control mechanisms enable companies to specify and implement monitoring and auditing requirements

By monitoring the analytics behind the behavior, organizations can do a more effective job detecting and minimizing the damage caused by the adversary. The best analytics focus in on metrics around the successful and failed access attempts to critical information.
In performing these types of analysis, there are three behavioral patterns that drastically change when an insider becomes an insider threat:

- Number of objects accessed
- Number of failed access attempts
- Amount of data accessed

Security is all about understanding managing and mitigating risks to your critical assets and how those risks could impact your organization.

Client Side Attack

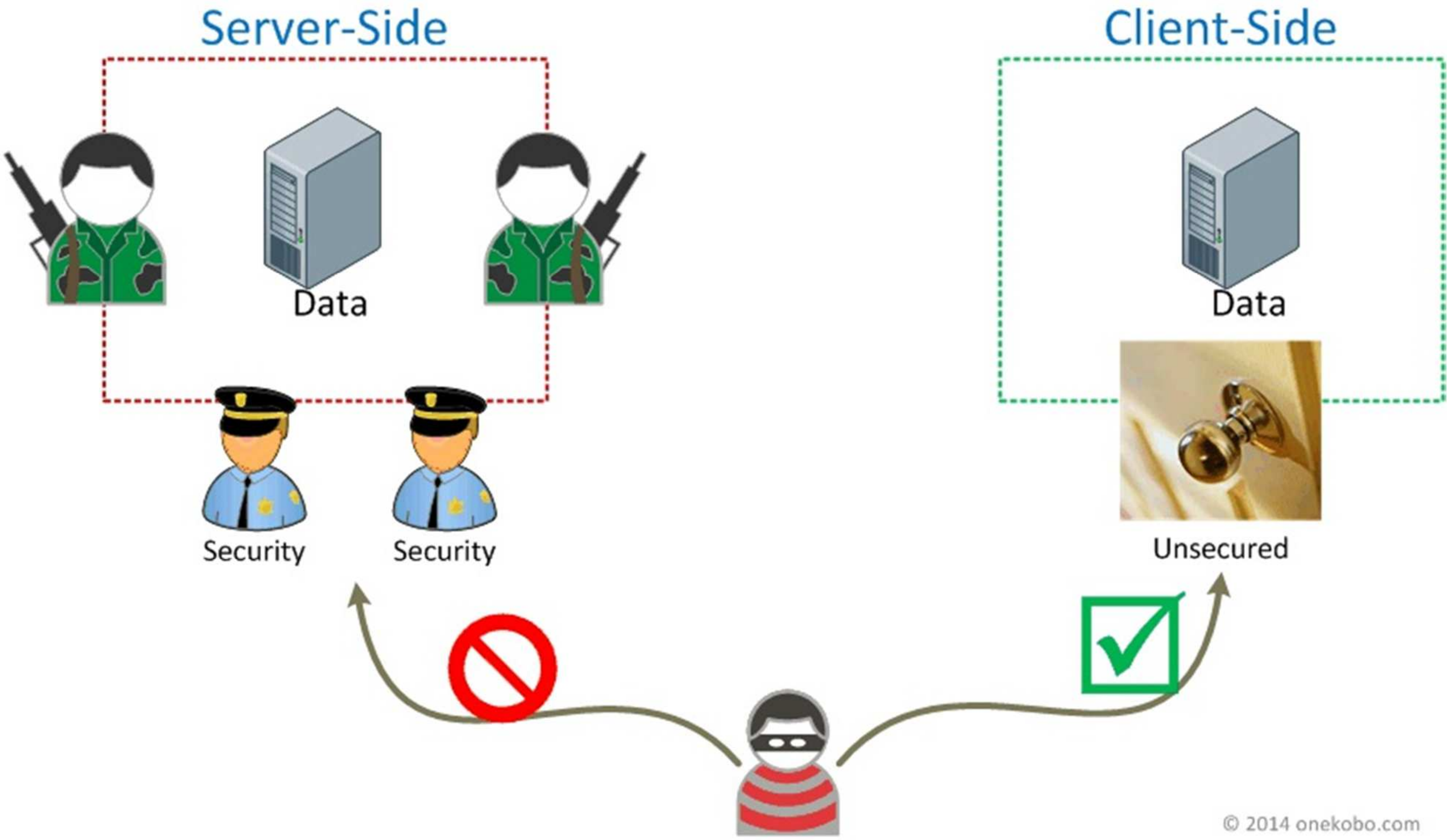
Attacks targeted at individual client computers are called client-side attacks. These are usually directed at web browsers and instant-messaging applications

In traditional Client/Server architecture, the “client” is usually an operating system(Windows, Linux etc) the corporate end-user (employee) interacts with on a daily basis. Unfortunately, client software can also be targeted with attacks from compromised servers accessed by the clients, and some client software actually listens for connections.

Type 1 - Traditional Client-side Exploits

These type of client-side exploits being used to create botnets and target specific organizations via a combination of social engineering and content with malicious payloads. These exploits target browsers, browser plugins, and email clients. Today, there is a fine line between email and web applications since many email applications share libraries when viewing emails that have been formatted with HTML content. We won’t spend any more time on this type of client-side exploit since this is the most commonly known type.

Client Side Attack



Type 2 – Clients with Exposed Services

Many types of client software will actually open up a socket and run a service that communicates on the network.

If it has a socket open on the network and connections can be made to it, it may be exploitable. If the host is directly connected to the Internet or to mobile broadband networks and it does not have a firewall, it may be attacked directly without any need for user interaction such as opening an email.

Type 3 – Clients Exposed to Hostile Servers

In this type of client exploit the server itself can be manipulated to attack a client directly. A classic example is CVE-2005-0467, which identifies a vulnerability in the PuTTY SSH and SCP clients that can be exploited by a malicious SSH server to execute code on connecting host.

Counter Measure

The three types of client-side exploits described here can be detected with

- Credentialed Nessus auditing,
- Some uncredentialed Nessus scans, and
- By monitoring traffic in real time with the Passive Vulnerability Scanner.
- Continuous update of end point patches.
- If you can’t patch all of your client vulnerabilities in a timely manner and have to perform a risk analysis in order to prioritize, knowing how the client software is used and what type of exploits it may be exposed to can help you rank which issues you need to mitigate first.

Transitive Access Attack

Transitive – Passing over to or affecting something else.

Transitive access is a problem when inadvertent (and possibly unauthorized) access results for a set of related and authorized access.

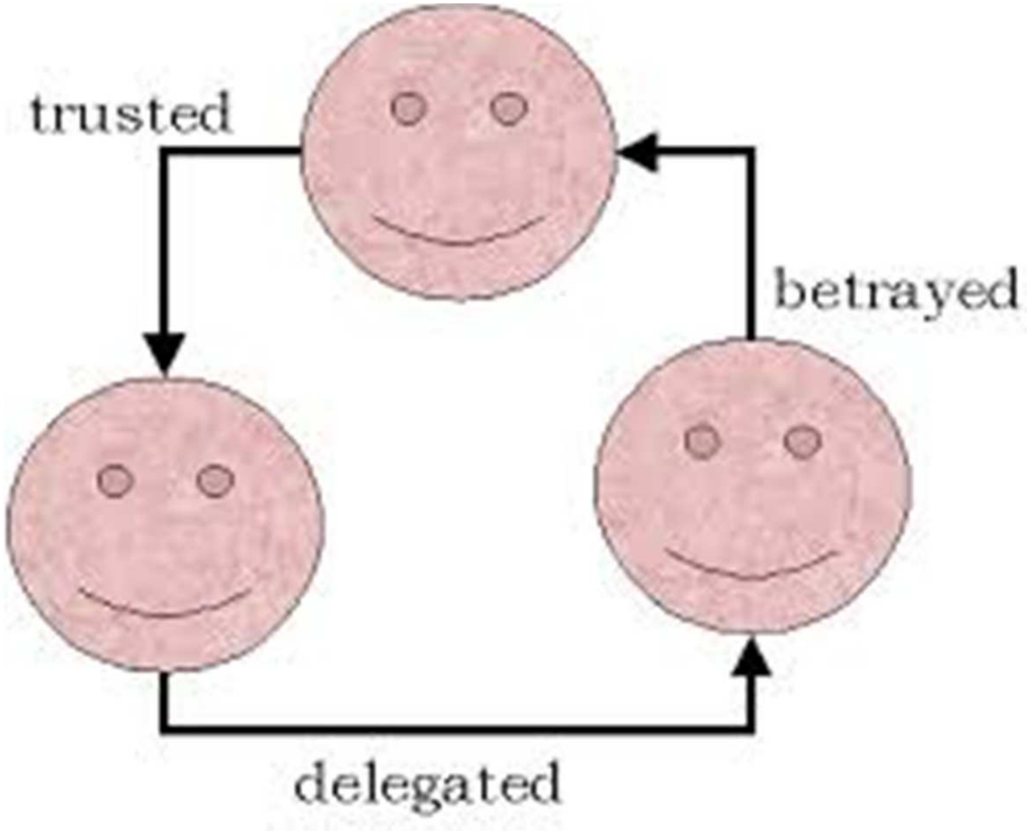
With transitive access, A trusts B, if B then trusts C, then a relationship can exist where C is trusted by A).

In a transitive trust relationship, the relationship between A and B flows through such that A now trusts C.

In all versions of Active Directory, the default is that all domains in a forest trust each other with two-way transitive trust relationships.

While this process makes administration much easier when you add a new child domain (no administrative intervention is required to establish the trusts), it leaves open the possibility of a hacker acquiring more trust than they should by virtue of joining the domain.

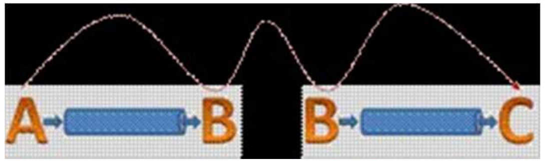
Transitive access Attack



Counter Measure

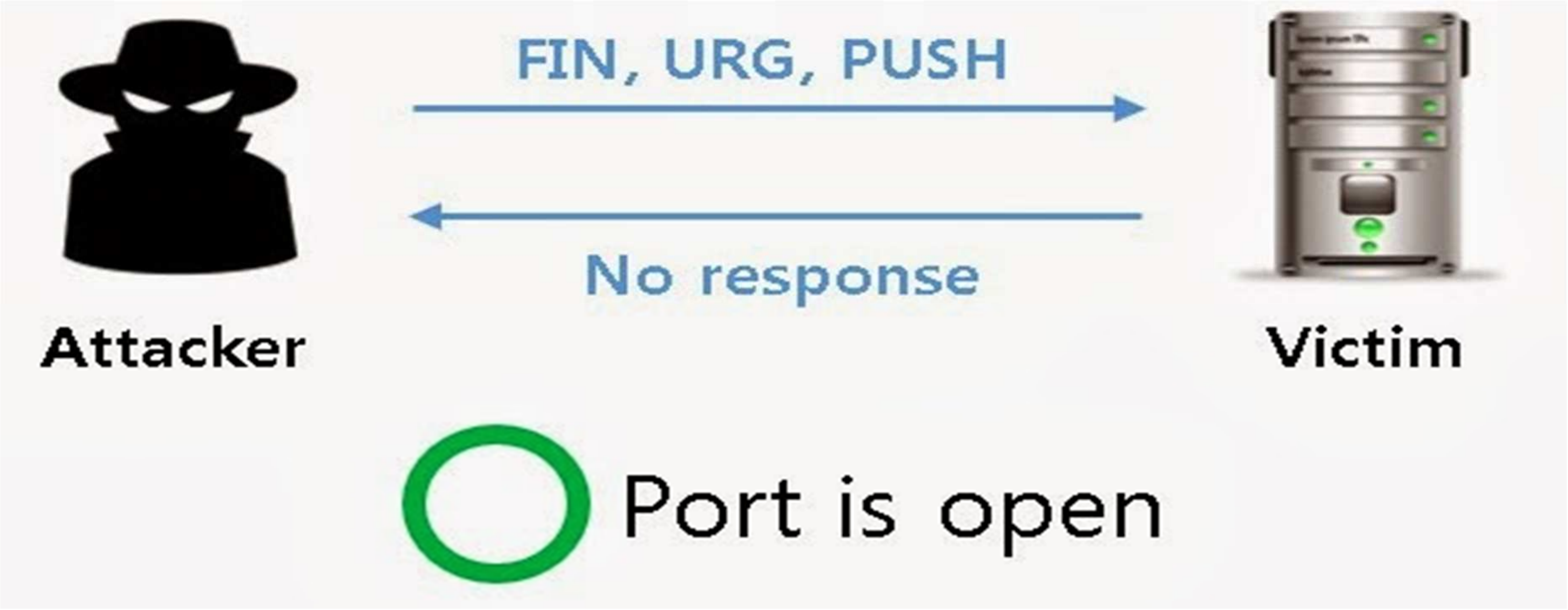
This attack arises from a poor choice of access control mechanism. Transitive attacks are attacks that become very, very difficult to prevent. This may be something that's occurring just because the series of trust that's been set up. Maybe in reality you really did not want a trusting C, but because of this transitive nature of trust in operating systems it's something that may be there already.

(i) Make sure that you're keeping your operating system updated,
(ii)You're keeping your applications updated.
(iii)You want to avoid that single vulnerability so by staying up to date with all of these patches and all of these updates
(iv)Enforce authentication at every critical point of operation.



X-MAS ATTACK

A Christmas tree packet is a type of packet that has a number of special settings applied, call "universal" or "default" settings. Christmas tree packets are set up in specific ways to be information heavy. This makes the data packet harder to pass through an average system and requires more processing power by a recipient. This type of packet is called a "Christmas tree packet" because of the metaphorical idea that the flags on the packet "shine" different colors and that the packet is "decked out like a Christmas tree."



Xmas Attack

Xmas scan is a port scan technique with URG, PSH and FIN flags set to send a TCP frame to a remote device. If the target port is closed, then you will receive a remote system reply with a RST. You can use this port scan technique to scan large networks and find which host is ip and what services it is offering. It is a technique to describe all TCP flag sets. When all flags are set, some systems hang.

Christmas tree packets can be used in "Christmas tree attacks," where a large number of these data-heavy packets can slow down or overload a network. They can also be used in certain types of hacker "reconnaissance," where outsiders send these packets to get a better idea of the network they are trying to infiltrate. For example, Christmas tree packets sent to a certain recipient can cause a piece of hardware to shut down or reboot, which can indicate to the sender that there is an older or obsolete piece of equipment, or a piece of equipment with less processing power, that might be a vulnerability in a system.

So it’s very unusual having so many of them there and having these 1s and 0s there, mean that this particular section of the flags of a TCP packet are lit up like a Christmas tree. And that’s where the name comes from.

Counter Measure

Following Two tools can be used to detect this attack:

1. The first one is Nmap which you can download from nmap.org or insecure.org. That will be the scanning tool that I use to perform the Christmas tree scan, the Christmas tree attack against this router that I have in my environment.

2. Use Wireshark packet capture protocol analysis device. We can capture packets in real time. Check whether the packet/frame is part of the Christmas tree scan.

3. To prevent need to get updated firmware and hardware

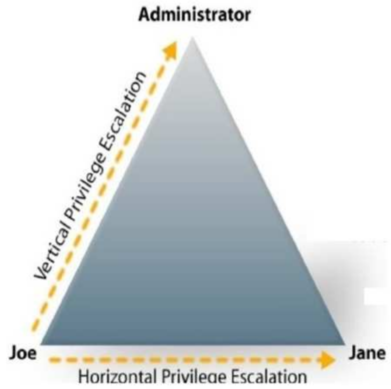
Privilege Escalation

Attacker look for vulnerabilities that they can exploit to gain control over a computer system or application by compromising user accounts. Through such initial exploit paths, an attacker will obtain certain access privileges.

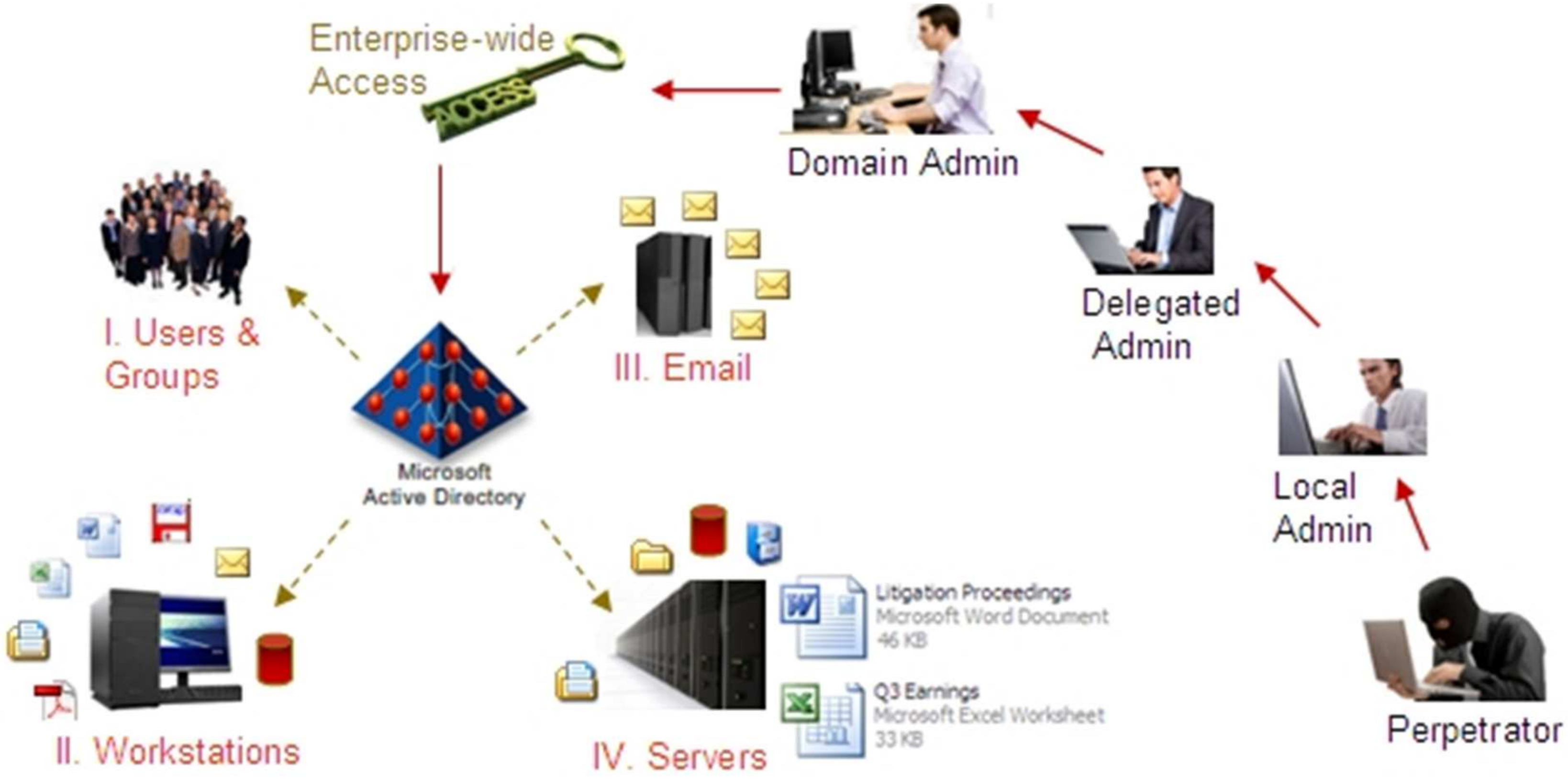
Next, the attacker will progressively probe the system he compromised to gain more privileges than what he initially gained, hoping to access sensitive information from other accounts, or even to obtain complete administrative control over a system. When an attacker expands his initial unauthorized access in this manner, we call the his efforts a privilege escalation attack.

Types

- Horizontal Privilege Escalation
- Vertical Privilege Escalation


Administrator
Vertical Privilege Escalation
Joe
Jane
Horizontal Privilege Escalation

Privilege Escalation



Horizontal Privilege Escalation

Let's suppose that an attacker has gained access to an online banking account. She's looking to steal money and the money she's stolen from this one account is not enough. She'll probe for information or try various exploits to gain access to other accounts. This is called horizontal privilege escalation because our attacker is moving laterally across accounts of similar privileges.

How does she move laterally? Our attacker may examine the hyperlinks this bank returns after she's logged in to see if they reveal any information about the way content is organized at the banking site. She may discover that the bank encodes a customer's account number in a particular way in hyperlinks. She'll compose and inject hyperlinks to the web site to test whether the banking system's security is flawed and whether the flaw allows her to view other customer account data or (better) to transfer funds. If successful, she may access several accounts before the bank detects her activities or a customer reports a theft. This is called a direct object reference technique.

Vertical Privilege Escalation

Attackers are often motivated to gain complete control over a computer system so that they can put the system to whatever use they choose. When an attacker begins with a compromised user account and is able to expand or elevate the single user privileges he has to where he gains complete administrative privileges or "root", we call such attacks vertical privilege escalation.

Let's consider a scenario where our attacker has gained unauthorized access to a user account on a computer system. He'll conduct local reconnaissance to see what the compromised user can do and what information he can access, whether he can write scripts or compile programs from this account, and more. If he's able to download and execute software on the compromised computer, he may run exploit software. He'll poke around until he finds a vulnerability or configuration error that he can exploit to become an administrator on the targeted computer, or he'll abandon this system and move on to another computer.

An attacker can also bypass access to protected or sensitive information through remote paths. For example, by carefully crafting queries that take advantage of a vulnerability in a web application deployed at a targeted site, an attacker can insert instructions directly to the site's database application that allow him to access ostensibly protected records or dump the entire contents of a database (see SQL injection). Attackers have an abundance of exploits to try but attackers often simply take advantage of the web application lacking any validation of the type of data that a user submits: in such situations, the web application passes anything the attacker enters into a web submission form to the database and the database executes what it receives, with often disastrous consequences including full database disclosure, data alteration or corruption.

Mitigation / Counter Measure

Enforce authorization policies and the methods (access controls, user permissions or privileges) are intended to protect sensitive information against unauthorized viewing, sharing, modification, or deletion. Such policies can also protect against unauthorized execution of applications on a computer.

Beef Up Authentication and Validate All Data!

Three simple remedies to reduce privilege escalation attacks are

- have your users or customers use the strongest authentication method possible, and use them intelligently (e.g., long, strong, complex passwords),
- scan your web applications for known vulnerabilities to minimize exploit attacks, and
- validate data in every submission form your web site uses. Apply these and you'll reduce your organization's exposure to privilege escalation attacks.

Non-Blind Spoofing

- This attack takes place when the attacker is on the same subnet as the target that could see sequence and acknowledgement of packets.

- The threat of this type of spoofing is session hijacking and an attacker could bypass any authentication measures taken place to build the connection.

- This is accomplished by corrupting the DataStream of an established connection, then re-establishing it based on correct sequence and acknowledgement numbers with the attack machine.

Banana Attack

- A "banana attack" is another particular type of DoS.
- It involves redirecting outgoing messages from the client back onto the client, preventing outside access, as well as flooding the client with the sent packets. A LAND attack is of this type.

The Banana attack uses a router to change the destination address of a frame. In the Banana attack:

- A compromised router copies the source address on an inbound frame into the destination address.
- The outbound frame bounces back to the sender.
- This sender is flooded with frames and consumes so many resources that valid service requests can no longer be processed.

Pulsing Zombie Attack

- A pulsing zombie is a computer whose security has been compromised without its owner's knowledge by a cracker so that it intermittently carries out a denial-of-service attack on target computers in a network.

- Unlike a regular zombie, the pulsing zombie doesn't completely paralyze its targets, but merely weakens them, in what some call degradation-of-service attacks.

- Whereas the usual zombie attack consists of a steady (and therefore more easily traced) stream of attack traffic intended to overwhelm one or more target computers, the pulsing zombie attack consists of irregular bursts of traffic intended to hamper service.

- It is more difficult to locate the source of an attack from a pulsing zombie, or even to know that an attack has taken place

Information Warfare

- Information warfare (IW) is a concept involving the use and management of information and communication technology in pursuit of a competitive advantage over an opponent.
- Information warfare may involve collection of tactical information, assurance(s) that one's own information is valid, spreading of propaganda or disinformation to demoralize or manipulate.

Countermeasure

Information Protection