

Lecture 01

Introduction

CMPU-4008

Advanced Security 2

Module Contents

- Authentication Applications
- Electronic Mail Security
- Internet Protocol Security
- Web security
- Intruders, Crimeware, Firewalls
- Security Policies, Standards, Compliance

Module Contents

- Security Metrics and Auditing
- Penetration Testing
- Social Engineering
- Defences to security attacks
- The impact of Technological developments on Security
- Disaster Recovery, Business Continuity

Assessment Methods

- Written examination – 50%
- Continuous assessment – 50%

Continuous assessment – 50%

- Quiz 1 - 10%.
 - Theory Test in week 6.
- Quiz 2 - 10%.
 - Theory Test in week 12 (**All lecture material**).
- Assignment 1 - 15% (**Week7**).
 - Research on the skills, certifications and training for security expert.
 - Google hacking, Vulnerabilities and Exploits
- Assignment 2 - 15% (**Week13**).
 - Security Tools

Submission guidelines

- Submission guidelines
 - Use Brightspace, no email submission
 - naming files (Full-Name_Student-Number_Assignment-Name)
- Optional Report guidelines
 - Cover page, introduction, body, discussion, conclusion and references
- Marks will be deducted for late submission

Penetration Testing Tools

- **Resources**

- <http://www.darknet.org.uk/>
- <http://www.livehacking.com/>
- <http://www.hiren.info/>
- <http://holisticinfosec.org/>

Tools used for security training

- Seed - <http://www.cis.syr.edu/~wedu/seed/>
- Sweet - <http://csis.pace.edu/~lchen/sweet/>
- Security Shepherd -
https://www.owasp.org/index.php/OWASP_Security_Shepherd
- There are a lot of Security Gaming software

Essential Reading

- Computer Security: Principles and Practice, 3rd edition, William Stallings and Lawrie Brown (2015), Pearson.

Supplemental Reading

- Cryptography and Network Security : Principles and Practices, 6th Ed, Williams Stallings (2014) Prentice Hall.
- Network Security Essentials: Applications and Standards, 4th Ed, William Stallings (2011), Prentice Hall

References

- Seymour Bosworth and M.E. Kabay, 2009, Computer Security Handbook, John Wiley & Sons. Inc.
- Andrew Lockhart, 2004, Network Security Hacks 100 Industrial-Strength Tips & Tools, O'Reilly
- Markus Jakobsson, Zulfikar Ramzan, 2008, Crimeware: Understanding New Attacks and Defences, Symantec Press.
- Ed Skoudis and Tom Liston, 2006, Counter Hack Reloaded: A step-by-step Guide to Computer Attacks and Effective Defences, Prentice hall
- Bruce Schneier, 2012, Liars and Outliers: Enabling the Trust that Society Needs to Thrive, John Wiley & Sons ISBN: 978-1118143308

Software license

- This software is provided “as is” and any expressed or implied warranties, including, but not limited to, the implied warranties of merchantability and fitness for a particular purpose are disclaimed. In no event shall the contributor be liable for any direct, indirect, accidental, special, exemplary, or consequential damages (including, but not limited to, procurement of substitute goods or services; loss of use, data, or profits; or business interruption) however caused and on any theory of liability, or tort (including negligence or otherwise) arising in any way out of use of this software, even if advised of the possibility of such damage.
- In plain English what does the above information mean.

Software license

- We don't claim this software is good for anything— if you think it is, great, but it's up to you to decide.
- If this software doesn't work: tough. If you lose a million dollars because this software messes up, it's you that's out of million, not us.
- If you don't like this disclaimer: tough. We reserve the right to do the absolute minimum provided by law, up to and including nothing.

Software characteristics

- We interact with software on daily basis.
- How and when we touch software and how and when it touches us is less our choice everyday.
- The quality of software matters greatly.
- Software is insecure.
- Insecure software is everywhere interconnected and woven tightly into the fabric of civilisation.

Why Software is insecure

- Software is not necessarily designed and constructed with security in mind.
- Internet Explorer is one of many examples of insecure software.
- Lack of security training:
 - Many software developers do not understand the risks that they are exposing their users to by creating poorly written code.

Costs of Insecure Software

- Maintenance :
 - Network administrator has to spend a reasonable amount of his time installing security patches on the company's machines.
- Lack of productivity:
 - When a piece of software is compromised at work, everyone suffers.
- Reduce Bandwidth

Ongoing Platform Battlegrounds

- Web Search
 - Google vs. Bing/Yahoo, foreign engines
- Smart Phone
 - OS Apple vs. RIM, Nokia/Symbian, Android, Microsoft, Palm, Linux, ARM, Intel Atom)
- Digital Media
 - Apple (iPod, iPad & iTunes) vs. Microsoft (Media Player, Zune) vs. Real?
- Social Networking
 - Facebook, Twitter, LinkedIn, etc.

Ongoing Platform Battlegrounds

- Video Games
 - Sony, Nintendo, Microsoft
- Enterprise software
 - SAP vs. Oracle/Sun, Microsoft, IBM
- Micropayments
 - Sony Felica vs. PayPal, credit cards, Apple Pay,
 - Google Wallet, Softcard, CurrentC etc.
- Displays
 - Oled, 4k, Plasma vs. LCD (Sharp, Sony, Samsung, others)

The future of Security threats

- Cyberwar declared – Stuxnet a politically motivated attack (weaponized malware) :
Duqu, Flame, and Shamoons
- Advanced Persistent Threat (APT) – advanced malware attack
- VoIP attacks – brute force and directory traversal class attacks against VoIP servers

The future of Security threats

- Car hacking – cars are more connected with built-in Bluetooth, 3G internet, GPS, Onstar, and dashboard computers
- The Facebook challenge - users trust of web (Web 2.0, API etc)
- Manufactured-delivered malware – products arriving with infections out of the box

The future of Security threats

- Fighting internet crime does not come cheap.

For example, Inga Beale, the CEO of Lloyd's said that Lloyd's estimates that cyber attacks cost businesses as much as \$400 billion a year, including the damage itself and subsequent disruption to the normal course of business.

Cybercrime Knows No Borders

- Prosecuting cybercrime is no easy task.

One of the biggest problems lies with the scope of legislation within a particular country. “There is a tremendous range in the laws – with many countries not having laws covering such simple concepts as unauthorized access to a computer system or installation of malicious software”.

Cloud apps a click away

- Dropbox – <http://www.dropbox.com/>
- Google Docs- <https://docs.google.com/>
- Microsoft OneDrive <https://onedrive.live.com>
- Evernote - <http://www.evernote.com/>
- GoToMyPC - <http://www.gotomypc.co.uk/>
- And many more ...

Cloud Security Mechanism

- Take responsibility for your own security
- Ring fence your data
- Think about encryption
- Strong passwords for cloud services

Common Sense Security

- Security is not a specialist subject – it's everyone's responsibility
- The attackers only have to get lucky once and the defenders have to get it right 100% of the time

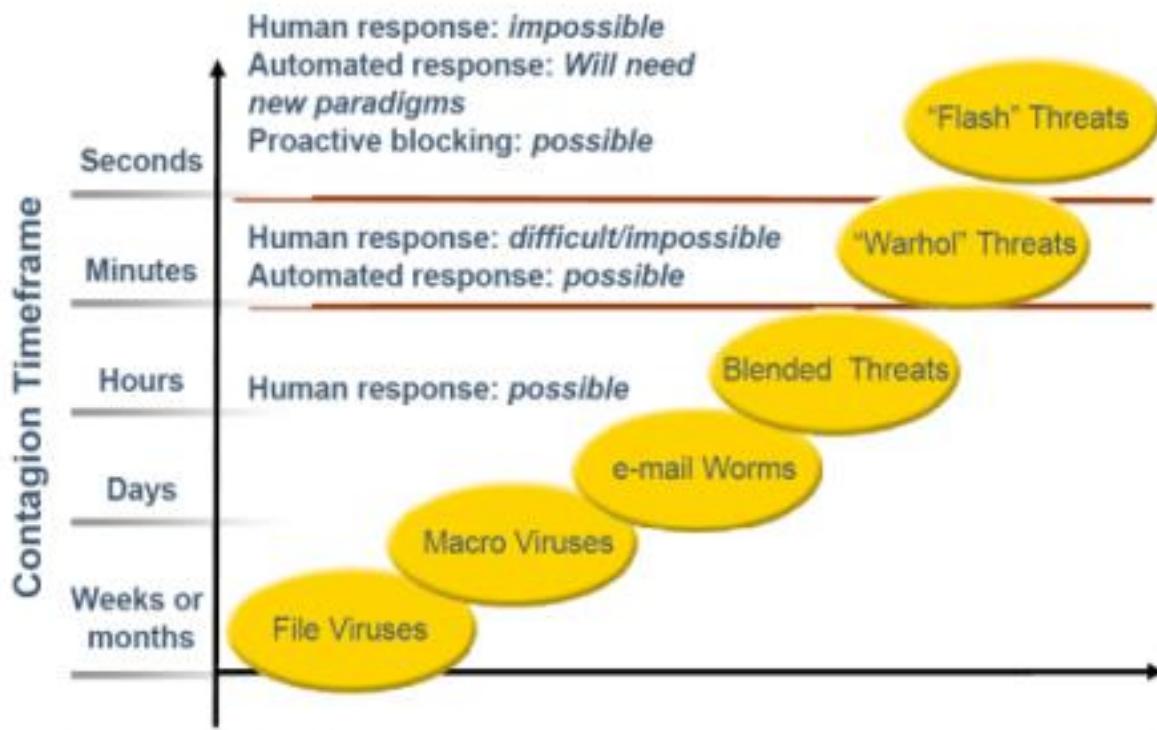
Some Resources on Cloud Security

1. Top Threats to Cloud Computing V1.0, Cloud Security Alliance, March, 2010.
2. Security Guidance for Critical Areas of Focus in Cloud Computing V3.0, Cloud Security Alliance, 2011.
3. Guidelines on Security and Privacy in Public Cloud Computing, Wayne Jansen and Timothy Grance, NIST, January 2011.
4. Cloud Computing Security: A Survey, Issa M. Khalil , Abdallah Khreishah,Muhammad Azeem, Computers 2014.
5. Overview of Attacks on Cloud Computing, Ajey Singh, Maneesh Shrivastava, IJEIT,2012
6. The Management of Security in Cloud Computing, Ramgovind S, Eloff MM, Smith E, IEEE, 2010

Intruders

- An Intruder is a person who attempts to gain unauthorized access to a system, to damage that system, or to disturb data on that system.
- Building technical knowledge and skills
- Gaining leverage through automation
- Exploiting network interconnections and moving easily through the infrastructure
- Becoming more skilled at masking their behaviour

Response Time



Vulnerability Trends

- Flaws can be found without source code
 - common: system call trace
 - new: subroutine call trace
 - protocols can be examined for vulnerabilities
 - program instabilities (buffer overflow, etc.)
- Good news — the public & vendors becoming
 - more security conscious
 - Patches now being released via Internet

I am a Developer

- 10 lines of code = 10 issues.
500 lines of code = "looks fine."
- Code reviews.
Recent source lines of code (SLOC) reviews and estimates suggest that a very conservative guess would place the number of bugs in most modern software at the rate of about one per 1000 lines of extremely well-written source code with great attention to security detail.
1000 SLOC = 1 bug (error)
- Source: <http://www.techrepublic.com/blog/it-security/thedanger-of-complexity-more-code-more-bugs>

Windows: Source Lines of Code (Sloc)

Year	Operating System	Sloc (Million)
1993	Windows 3.1	6
1994	Windows NT 3.5	10
1996	Windows NT 4.0	16
2000	Windows 2000	29
2001	Windows XP	40
2005	Windows Vista Beta 2	50

Linux: Source Lines of Code (Sloc)

Operating System	Sloc (Million)
Red Hat Linux 6.2	17
Red Hat Linux 7.1	30
Debian 2.2	55-59
Debian 3.0	104
Debian 3.1	215
Debian 4.0	283
OpenSolaris	9.

Graphics Programs: Source Lines of Code (Sloc)

Operating System	Sloc (Million)
Mac OS X	86
Linux Kernel 2.6.0	5.2
Graphics Programs	
OpenOffice.org	10
Blender 2.42	1
GIMP v2.3.8	0.65
Paint.NET 3.0	0.13

Air Domain Strategic Context

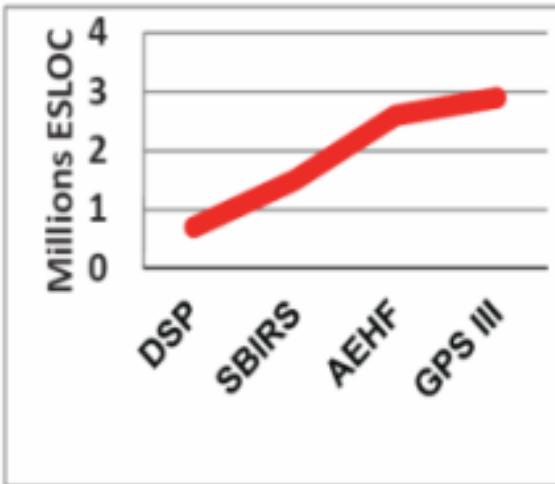


Figure 1b:
Space Systems Software Growth
Source: CMU/SEI

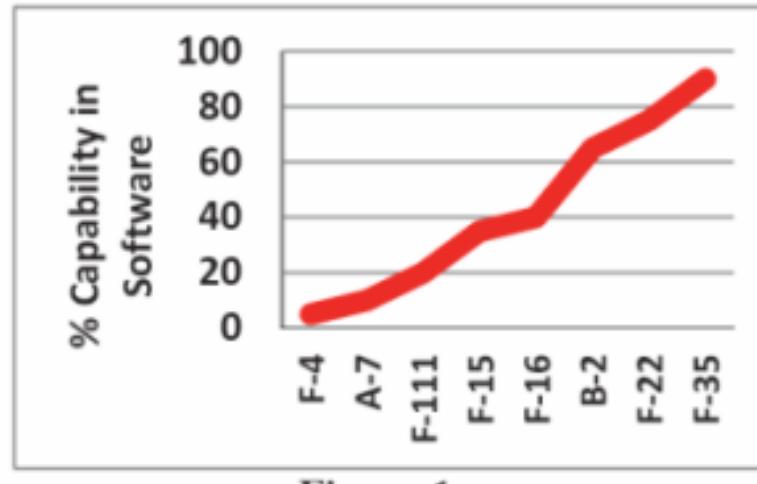


Figure 1a:
Air Platform Software Growth
Source: CMU/SEI and Lockheed Martin

Modernisation Centred Software

- Approximately ninety percent of the functionality in the Joint Strike Fighter (F-35) is dependent upon software (approximately 10 million lines of embedded code on the platform)
- 15 million on the ground-based Autonomic Logistics Information System (ALIS)).
- This contrasts with only five percent in a 1960-era F-4 fighter

Security Threats

- Spyware and Ad ware
- Viruses
- Phishing and Pharming
- Worms, Bots
- SQL injection
- Sophisticated targeted attacks
- Politically motivated attacks (Weaponized malware) - Stuxnet

Security Certification

- Certified Information System Security Professional (CISSP)

<https://www.isc2.org/Certifications/CISSP>

- Cisco Certified Security Professional (CCSP)

<https://www.cisco.com/c/en/us/training-events/training-certifications/certifications/security.html#~security-certifications>

- Certified Ethical Hacking (CEH)

<https://www.eccouncil.org/programs/certified-ethical-hacker-ceh/>

It's going to get worse - 1

- Explosive growth of the Internet continues
 - continues to double in size every 10-12 months
 - where will all the capable system administrators come from?
- Market growth will drive vendors
 - time to market, features, performance, cost are primary
 - “invisible” quality features such as security are secondary

It's going to get worse - 1

- The death of the firewall
 - traditional approaches depend on complete administrative control and strong perimeter controls
 - today's business practices and wide area networks violate these basic principles
 - no central point of network control
 - more interconnections with customers, suppliers, partners
 - more network applications

It's going to get worse - 1

- Beware of snake-oil
 - the market for security products and services is growing faster than the supply of *quality* product and service providers
 - sometimes the suppliers don't understand Consumer needs

Before it gets better - 1

- Strong market for security professionals will eventually drive graduate and certificate programs.
- Increased understanding by technology users will build demand for quality security products; vendors will pay attention to the market.
- Insurance industry will provide incentives for improved business security practices.

Before it gets better - 1

- Technology will continue to improve and we will figure out how to use it
 - Encryption
 - strong authentication
 - survivable systems
- Increased collaboration across government and industry.

Sensible Security

- All security involves trade-offs
- Security trade-offs depend on power and agenda
- Security is a process and not a product
- Security is a game a never ending one

How Security Works

- You need to know systems and how they fail.
- Know the attackers
- Attackers never change their tunes, just their instruments
- Technology creates security imbalances
- Security is a weakest-link problem
- Security evolves around people
- Detection is useless without response
- Identification, authentication and authorization
- All countermeasures have some value, but no countermeasure is perfect

Computer Security

- The process of preventing and detecting unauthorized use of your computer.
- Attain the integrity, availability and confidentiality of information system resources (includes hardware, software, firmware, information/data, and telecommunications)

Key Security Concepts

- Confidentiality
- Integrity
- Availability

Level of Impact

- can define 3 levels of impact from a security breach
- Low
- Moderate
- High

Examples of Security Requirements

- Confidentiality – **Student grades**, **Student enrolment**, **Staff Directory**
- Integrity – **patient information**, **Website Forum**, **Online poll.**
- Availability – **Bank authentication service**, **University Website**, **telephone directory**

Computer Security Challenges

- Not simple
- Must consider potential attacks
- Involve algorithms and secret info
- Must decide where to deploy mechanisms
- Battle of wits between attacker / admin
- Requires regular monitoring

Security Areas

- Consumerization :
 - consumer devices will become trendier, cheaper, and more integrated
- Decentralization
 - increase use of cloud computing
- Deconcentration
 - special purpose hardware like iPhone
- Decustomerization:
 - get more IT function without any business relationship: free Google, Bing, Social, Networking sites etc

Vulnerabilities of the Internet

- The addressing system that finds out where to go on the internet for a specific address DNS
- The routing among ISPs, a systems known as the Border Gateway Protocol
- Almost everything that makes it work is open, unencrypted
- Its ability to propagate intentionally malicious traffic designed to attack computers
- It is one big network with a decentralised design

Attack Surfaces

Consist of the reachable and exploitable vulnerabilities in a system

Examples:

Open ports on outward facing Web and other servers, and code listening on those ports

Services available on the inside of a firewall

Code that processes incoming data, email, XML, office documents, and industry-specific custom data exchange formats

Interfaces, SQL, and Web forms

An employee with access to sensitive information vulnerable to a social engineering attack

Attack Surface Categories

Network Attack Surface

Vulnerabilities over an enterprise network, wide-area network, or the Internet

Included in this category are network protocol vulnerabilities, such as those used for a denial-of-service attack, disruption of communications links, and various forms of intruder attacks

Software Attack Surface

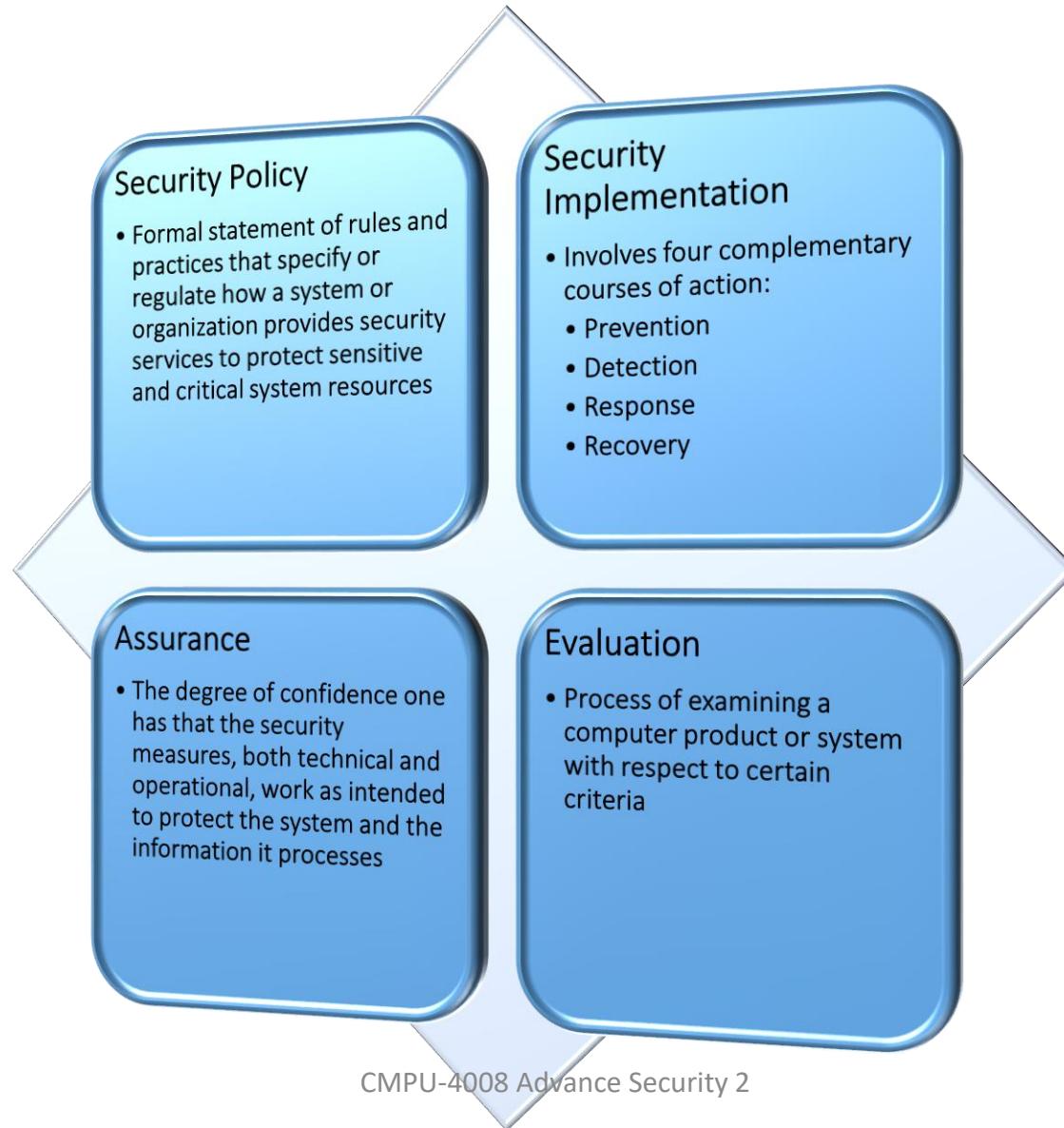
Vulnerabilities in application, utility, or operating system code

Particular focus is Web server software

Human Attack Surface

Vulnerabilities created by personnel or outsiders, such as social engineering, human error, and trusted insiders

Computer Security Strategy



Lecture 02

Google Hacking for Penetration Tester

CMPU-4008

Advance Security 2

Outline

- Google Introduction & Features
- Google Search Technique
- Google Basic Operators
- Google Advanced Operators

Google Hacking

- Google Search Technique
 - Just put the word and run the search
- You need to audit your Internet presence
 - One database, Google almost has it all!
- One of the most powerful databases in the world
- Usage:
 - Business ...
 - One stop shop for attack, maps, addresses, photos, technical information

Google Hacking

- Google Advance Search
 - A little more sophisticated
- Google hacking is the term used when a hacker tries to find vulnerable targets or sensitive data by using the Google search engine.



Advanced Search

[Advanced Search Tips](#) | [About Google](#)

Find results	with all of the words with the exact phrase with at least one of the words without the words	<input type="text"/> <input type="text"/> <input type="text"/> <input type="text"/>	<input type="button" value="10 results"/> <input type="button" value="Google Search"/>
Language	Return pages written in <input type="button" value="any language"/>		
File Format	<input type="checkbox"/> Only <input type="button" value="return results of the file format"/> <input type="button" value="any format"/>		
Date	Return web pages first seen in the <input type="button" value="anytime"/>		
Occurrences	Return results where my terms occur <input type="button" value="anywhere in the page"/>		
Domain	<input type="checkbox"/> Only <input type="button" value="return results from the site or domain"/> e.g. google.com, .org More info		
Usage Rights	Return results that are <input type="button" value="not filtered by license"/> More info		
SafeSearch	<input checked="" type="radio"/> No filtering <input type="radio"/> Filter using SafeSearch		

Google Operators

- Operators are used to refine the results and to maximize the search value.
They are your tools as well as hackers' weapons.
- Basic Operators:
 - +, -, ~, ., *, "", |, OR
- Advanced Operators:
 - allintext:, allintitle:, allinurl:, bphonebook:, cache:, define:, filetype:, info:, intext:, intitle:, inurl:, link:, phonebook:, related:, rphonebook:, site:, numrange:, daterange

Basic Operators

- (+) force inclusion of something common
- Google ignores common words (where, how, digit, single letters) by default:
 - Example: StarStar Wars Episode +I
- (-) exclude a search term
 - Example: apple -red
- (“) use quotes around a search term to search exact phrases:
 - Example: “Aneel Rahim”
 - Aneel Rahim without “” has the 35,900 results, but “Aneel Rahim” only has 742 results.
Reduce the 99% irrelevant results

Basic Operators

- **(~) search synonym:**
 - Example: ~food
 - Return the results about food as well as recipe, nutrition and cooking
- **(.) a single-character wildcard:**
 - Example: m.trix
 - Return the results of M@trix, matrix, metrix.....

Basic Operators

- **(*) any word wildcard**
 - For example, **invit*** returns both invitation and invite
- **(AND)** Searches for results that include both the term before and the term after the operator.
- **(OR)** Searches for results that include either the term before or the term after the operator (or both).



dublin



All

Images

Maps

News

Videos

More

Settings

Tools

About 217,000,000 results (0.97 seconds)



cork



All

Images

Maps

News

Videos

More

Settings

Tools

About 128,000,000 results (0.80 seconds)



Cork OR Dublin



All

Images

Maps

News

Videos

More

Settings

Tools

About 343,000,000 results (0.54 seconds)



Cork AND dublin



All

Maps

Images

News

Videos

More

Settings

Tools

About 42,500,000 results (0.57 seconds)

Advanced Operators at a Glance

Advanced operators can be combined in some cases.

In other cases, mixing should be avoided.

Operator	Purpose	Mixes with other operators?	Can be used alone?	Does search work in			
				Web	Images	Groups	News
intitle	Search page title	yes	yes	yes	yes	yes	yes
allintitle	Search page title	no	yes	yes	yes	yes	yes
inurl	Search URL	yes	yes	yes	yes	not really	like intitle
allinurl	Search URL	no	yes	yes	yes	yes	like intitle
filetype	Search specific files	yes	no	yes	yes	no	not really
allintext	Search text of page only	not really	yes	yes	yes	yes	yes
site	Search specific site	yes	yes	yes	yes	no	not really
link	Search for links to pages	no	yes	yes	no	no	not really
inanchor	Search link anchor text	yes	yes	yes	yes	not really	yes
numrange	Locate number	yes	yes	yes	no	no	not really
daterange	Search in date range	yes	no	yes	not really	not really	not really
author	Group author search	yes	yes	no	no	yes	not really
group	Group name search	not really	yes	no	no	yes	not really
insubject	Group subject search	yes	yes	like intitle	like intitle	yes	like intitle
msgid	Group msgid search	no	yes	not really	not really	yes	not really

Some operators can only be used to search specific areas of Google, as these columns show.

Advance Operators

- **Advance Operator: “Site:”**
- Get results from certain sites or domains.
 - Example: **olympics site:nbc.com**
- To get results from multiple sites or domains, combine with **OR**
 - Example: **Olympics site:nbc.com OR site:.gov**



Olympics site:nbc.com



All

Images

Videos

News

Maps

More

Settings

Tools

About 3,420 results (0.30 seconds)

[2016 Rio Olympics - NBC.com](#)

[www.nbc.com/olympics](#) ▾

Commonly known as Rio 2016, the Games of the XXXI Olympiad in Rio de Janeiro, Brazil, mark a historic first time that the Olympics are held in South America, ...

[2016 Rio Olympics: 2016 Olympic Trials Photo: 2908958 - NBC.com](#)

[www.nbc.com/olympics/photos/2016-olympic-trials/2908958](#) ▾

Aug 8, 2016 - View photos from 2016 Rio Olympics 2016 Olympic Trials on NBC.com.

[Monologue Image: 2016 Olympics - The Tonight Show - NBC.com](#)

[www.nbc.com/the-tonight-show/photo/monologue-image-2016-olympics/5871](#) ▾

The International Olympic Committee is now considering London as a backup host city for the 2016 Olympics if Rio isn't ready. So I'd like to officially congratulate ...

[Superstore: Olympics Photo: 2908360 - NBC.com](#)

[www.nbc.com/superstore/photos/olympics/2908360](#) ▾

View photos from Superstore Olympics on NBC.com.

Advance Operators

- Advance Operator: “Site:”
- Examples:
 - site:ie
 - site:tudublin.ie

The screenshot shows the Google search interface. At the top left is the Google logo. To its right is a search bar containing the query "site:ie". Below the search bar is a navigation bar with tabs: All (which is underlined in blue), Images, News, Shopping, Maps, More, Settings, and Tools. Below the navigation bar, the text "About 469,000,000 results (0.31 seconds)" is displayed.



site:tudublin.ie

X |

All Images News Shopping Maps More

Tools

About 61,100 results (0.24 seconds)

Google promotion

Try Google Search Console

www.google.com/webmasters/

Do you own **tudublin.ie**? Get indexing and ranking data from Google.

<https://tudublin.ie> › virtualug

⋮

TU Dublin Virtual UG

24 Jun 2020 — This webinar will also be hosted on the Technological University Dublin

Facebook page. **Note: the live chat below is for the Webinar events ...

<https://arrow.tudublin.ie> › bsn

⋮

Building Services Engineering | Journals - Arrow@TU Dublin

Building Services Engineering (formerly known as Building Services News, The Irish Plumber & Heating Contractor, Irish Plumbing & Heating Engineer and Irish ...

<https://arrow.tudublin.ie> › ijap

⋮

Irish Journal of Academic Practice | Current Publications

This journal publishes current research related to learning, teaching and assessment in higher education in Ireland, and also research by the participants ...

Advance Operators

- **Advanced Operators: “Filetype:”**
- Google searches more than just Web pages.
- Google can search many different types of files, including PDF (Adobe Portable Document Format) and Microsoft Office documents
- Filetype: extension_type

Advance Operators

The Main File Types Google Searches

File Type	File Extension
Adobe Portable Document Format	Pdf
Adobe PostScript	Ps
Lotus 1-2-3	wk1, wk2, wk3, wk4, wk5, wki, wks, wku
Lotus WordPro	Lwp
MacWrite	Mw
Microsoft Excel	Xls
Microsoft PowerPoint	Ppt
Microsoft Word	Doc
Microsoft Works	wks, wps, wdb
Microsoft Write	Wri
Rich Text Format	Rtf
Shockwave Flash	Swf
Text	ans, txt



security filetype: pdf



All

Images

News

Videos

Maps

More

Settings

Tools

About 638,000 results (0.29 seconds)

[PDF] **Introduction to Network Security - Interhack**

www.interhack.net/pubs/network-security.pdf ▾

by M Curtin - 1997 - Cited by 47 - Related articles

Introduction to Network Security. Matt Curtin". March 1997. Reprinted with the permission of Kent Information Services, Inc. Abstract. Network security is a ...

[PDF] **Introduction to Computer Security**

its.ucsc.edu/security/training/docs/intro.pdf ▾

4. Why is Computer Security Important? Computer Security allows the University to carry out its mission by: ◦ Enabling people to carry out their jobs, education ...

[PDF] **Network Security: History, Importance, and Future - MIT**

web.mit.edu/~bdaya/www/Network%20Security.pdf ▾

by B Daya - Cited by 27 - Related articles

The entire field of network security is vast and in an evolutionary stage. www.infosecwriters.com/text_resources/pdf/IPv6_SSot illo.pdf. [6] Andress J., "IPv6: ...

[PDF] **the NIST Handbook - NIST Computer Security Resource Center**

csrc.nist.gov/publications/nistpubs/800-12/handbook.pdf ▾

by A User - 1995 - Related articles

nist special Publication 800-12. An Introduction to Computer Security: The NIST Handbook. U.S. DEPARTMENT OF COMMERCE. Technology Administration.

[PDF] **security in-a-box**

<https://securityinabox.org/sites/securitybckp.ngoinabox.org/security/booklet-en.pdf> ▾

Remembering and recording secure passwords 35. 4. How to protect ... Advocates are increasingly concerned about their digital security, and with good reason.

Advance Operators

- *filetype:xls username password email*
- Microsoft Excel spreadsheets containing the words *username*, *password*, and *email*.
- Read Criminal Justice (Offences Relating to Information Systems) Bill 2016
(<http://www.oireachtas.ie/documents/bills28/bills/2016/1016/b1016d.pdf>)
- Please do not practice this one, This is just for learning purpose.

A screenshot of a Google search results page. The search query in the bar is "filetype:xls username password email". Below the search bar are navigation links: All (highlighted in blue), News, Images, Videos, Maps, More, Settings, and Tools. The main content area shows the search results with the following details:

About 4,950 results (0.22 seconds)

[XLS] Using the Social Media Account Tracker

cdn2.hubspot.net/hub/215313/file-499131210.xls ▾

For a lot of social media accounts the login is the email address. ... Why wouldnt you just give them the primary email and password to access your Facebook ...

[XLS] GUCCIFER-2016-cycle-passwords

<https://guccifer2.files.wordpress.com/2016/08/2016-cycle-passwords.xls> ▾

7, Login, Password, GO TO: www.tveyes.com. 8, Matsdorf@dccc.org ... 1, Customer ID, Login, Password. 2, 623040 ... 1, Email, Password. 2, padilla@dccc.org ...

[XLS] email address from username - Moodle

https://moodle.org/pluginfile.php/183/mod_forum/.../user-account-creation_2.xls ▾

1, username, password, firstname, lastname, email. 2, 0000111, changeme, john, smith, 0000111@citycol.com. 3. username from frame-lname. A, B, C, D, E.

[XLS] 17651_Copy of All Paid Accounts 07232007.xls - WikiLeaks

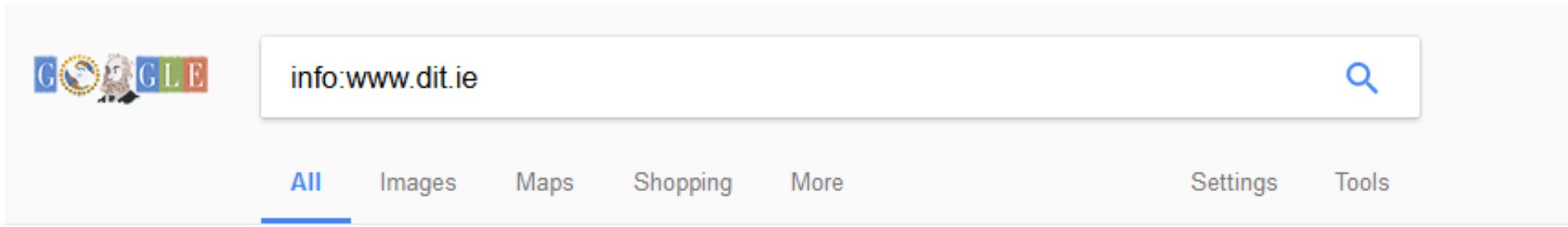
https://wikileaks.org/.../17651_Copy%20of%20All%20Paid%20Accounts%20072320... ▾

1, username, password, first_name, last_name, email, email_format, daily_email, address1, address2, city, state, province, country, postal_code, telephone ...

Advance Operators

- **Advanced Operators:** “info:website”
- Using this operator will tell Google to bring back information about a certain domain. It reveals:
 - Google’s cache of the site
 - Pages that are similar to the one you searched for
 - Pages that link to the domain you searched for
 - Other pages on the same domain
 - Pages that contain the domain text on their page

Advance Operators

A screenshot of a Google search results page. The search bar at the top contains the query "info:www.dit.ie". Below the search bar, there are navigation links for "All", "Images", "Maps", "Shopping", and "More", with "All" being underlined. To the right of these are "Settings" and "Tools" links. The main content area shows a single search result for DIT Dublin Institute of Technology. The result includes the URL "www.dit.ie/", a description stating "Features information on admissions, academic departments, and administration.", and a snippet of the website's content.

1 result (0.09 seconds)

DIT Dublin Institute of Technology -

www.dit.ie/

Features information on admissions, academic departments, and administration.

Google can show you the following information for this URL:

- Show Google's cache of [www.dit.ie](#)
- Find web pages that are [similar to](#) [www.dit.ie](#)
- Find web pages [from the site](#) [www.dit.ie](#)
- Find web pages that [contain the term](#) "www.dit.ie"

Advance Operators

- Advanced Operators “Intitle:”
- Intitle: search_term
 - Find search term within the title of a Webpage
- Allintitle: search_term1 search_term2 search_term3
 - Find multiple search terms in the Web pages with the title that includes all these words
- These operators are specifically useful to find the directory lists
- Example:
 - **intitle:Google** This query will return pages that have the word Google in their title
 - **Intitle: Index.of “parent directory”** It find the directory list



Intitle: Index.of “parent directory”

X |

All

Images

News

Videos

Shopping

More

Tools

About 189,000 results (0.29 seconds)

<https://www.ieee802.org> › files › public ...

[Index of /1/files/public - IEEE 802](#)

Index of /1/files/public. Icon Name Last modified Size Description. [PARENTDIR] **Parent Directory** - [DIR] 802-1-assigned-numbers/ 2021-07-20 14:34 - [DIR] ...

<https://www.ucd.ie> › phps ...

[Index of /phps](#)

Index of /phps. [ICO], Name · Last modified · Size · Description. [PARENTDIR], **Parent Directory**, - [DIR], CVD 1 PMC Cardiovascular Disease (1) Session 1 ...



intitle index of "parent directory" games



All Images News Videos Maps More Settings Tools

About 79,600 results (0.36 seconds)

[Index of /~archive/atari/Games](#)

[umich.edu/~archive/atari/Games/](#) ▾

Parent Directory - 0index 16-Mar-1997 01:30 32K Adventure/ 27-Nov-1995 15:49 - Arcade/ 28-Jan-1996 18:15 - Board/ 27-Jul-1995 12:43 - Cards/ 20-Jul-1995 ...

[Index of /Shareware/Games/ - Pacsteam.org](#)

[pacsteam.org/Shareware/Games/](#) ▾

Index of /Shareware/Games/ ... up Parent Directory 01-Nov-2017 11:05 - directory ... Farm Frenzy - Four Games In One Pack 18-Sep-2013 02:19 - directory ...

[Index of /games/](#)

[dl3.freengames.ir/games/](#) ▾

Parent directory/, -, -. 100ft-Robot-Golf-CODEX-www.FreeGames.iR.part1.rar, 1.0 GiB, 2017-Mar-30 01:01. 100ft-Robot-Golf-CODEX-www.FreeGames.iR.part2.

[Index of /pub4/sourceforge/a/ah/ahmedateeqzia/games - Last modified](#)

[download2.nust.na/pub4/sourceforge/a/ah/ahmedateeqzia/games/](#) ▾

[PARENTDIR], Parent Directory, -, [], Age of Empires 2 setup.exe, 2014-06-05 02:50, 185M. [], Age of Mythology Gold Edition setup.exe, 2014-07-14 05:44 ...

Advance Operators

- Advanced Operators “Inurl:”
 - Inurl: search_term
- Find search term in a Web address
 - Allinurl: search_term1 search_term2 search_term3
- Find multiple search terms in a Web address
- Examples:
 - Inurl:cgi-bin
 - Allinurl:cgi-bin password (It provides access of password file of web applications)



Allinurl:cgi-bin password



All

News

Videos

Images

Maps

More

Settings

Tools

About 9,800 results (0.46 seconds)

[Index of /staff/tydesjo/physics/workarea/cgi-password/cgi-bin](#)

www.hep.lu.se/staff/tydesjo/physics/workarea/cgi-password/cgi-bin/ ▾

Index of /staff/tydesjo/physics/workarea/cgi-password/cgi-bin. Icon Name Last modified Size Description. [DIR] Parent Directory - [] password.pl 09-Dec-2003 14:20 1.7K. Apache/2.2.15 (Linux/SUSE) Server at www.hep.lu.se Port 80.

[The definitive super list for "Google Hacking". · GitHub](#)

<https://gist.github.com/cmartinbaughman/5877945> ▾

inurl:/wwwboard. inurl:/yabb/Members/Admin.dat. inurl:ccbill filetype:log. inurl:cgi-bin
inurl:calendar.cfg. inurl:chap-secrets -cvs. inurl:config.php dbuname dbpass. inurl:filezilla.xml -cvs.
inurl:lilo.conf filetype:conf password -tatercounter2000 -bootpwd -man. inurl:nuke filetype:sql.
inurl:ospfd.conf intext:password -sample -test ...

[\[PDF\] Google Hacking \(Kind of\)](#)

fleming0.flemingc.on.ca/~blbrown/Google%20Hacking%20Lesson.pdf ▾

Advanced Operators "Inurl:". – Inurl: search_term. – Find search term in a Web address. – Allinurl: search_term1 search_term2 search_term3. – Find multiple search terms in a Web address. – Examples: Inurl: cgi-bin. Allinurl: cgi-bin password. . . Google Hacking ...

Advance Operators

- Advanced Operators “Intext;”
- **Intext: search_term**
 - Find search term in the text body of a document.
- **Allintext: search_term1 search_term2 search_term3**
 - Find multiple search terms in the text body of a document.
- Examples:
 - **Intext: Administrator login**



Intext:Administrator login



All Images Videos News Shopping More

Settings Tools

About 1,170,000 results (0.37 seconds)

Admin Login

<https://admin.lavu.com/> ▾

Forgot Password? | Terms of Service By continuing, you are agree to our Terms of Service. Forgot Password. Username. Back to Login | Terms of Service By continuing, you are agree to our Terms of Service. Reset Password. Username. New Password. Confirm Password. Back to Login | Terms of Service By continuing ...

Administration Login - Adobe Business Catalyst

<https://www.businesscatalyst.com/adminconsole/> ▾

Email Address: Password: Lost your password?

Admin Login

<https://www.iitk.ac.in/hall7/admin.php> ▾

Home · About Hall7; HEC. Wardens · Student HEC · Hall Office Staff · Hall Residents; Facilities. Mess · Canteen · Reading Room · TV Room · Computer Room · Games And Sports · Music Room · Gymnasium · Garden · Guest Room · Hall ShopC · Hall Bicycles. Events. Hall Day · Saraswati Puja · Diwali · Rush'08.

Admin - Login - phpSocial

<https://phpsocial.com/demo/index.php?a=admin> ▾

Admin Login. Username. Type in your Admin Username. Password. Type in your Admin Password. username: admin password: password (Note: no changes will be saved, this is just a demo). Share.

The screenshot shows a web browser window with the URL www.ijbed.org/admin/login.php in the address bar. The page itself has a dark blue header with the text "Admin Login" in white. In the top right corner, there is a small logo with the words "authentic software". Below the header, there are two input fields: one for "User ID" and one for "Password", both represented by blue rectangular boxes. To the right of these fields is a large blue button with the word "LOGIN" in white. At the bottom right of the form area, there is a link labeled "> Site Home".

Advance Operators

- Advanced Operators: “Cache:”
- cache: URL
- Find the old version of Website in Google cache
- Sometimes, even the site has already been updated, the old information might be found in cache
- Examples:
 - cache:www.tudublin.ie



cache:www.tudublin.ie



Google Search

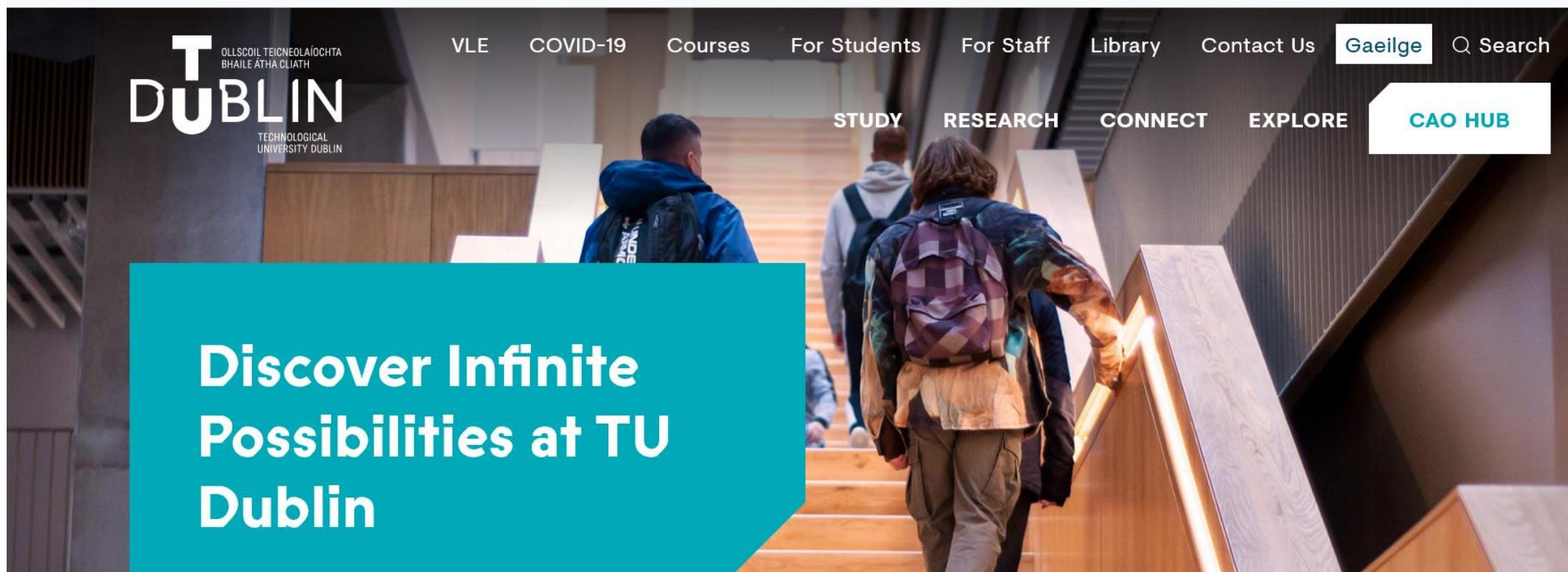
I'm Feeling Lucky

[Full version](#)

[Text-only version](#)

[View source](#)

Tip: To quickly find your search term on this page, press **Ctrl+F** or **⌘-F** (Mac) and use the find bar.



The image shows the homepage of the Technological University Dublin (TU Dublin). The header features the university's logo, "T DUBLIN", with the full name "TECHNICAL UNIVERSITY DUBLIN" below it. The navigation menu includes links for VLE, COVID-19, Courses, For Students, For Staff, Library, Contact Us, Gaeilge, and a search bar. Below the menu, four main categories are displayed: STUDY, RESEARCH, CONNECT, and EXPLORE. A prominent teal-colored call-to-action box on the left side contains the text "Discover Infinite Possibilities at TU Dublin". The background of the page shows students walking through a modern, well-lit building interior.

T OLLSCOIL TEICNEOLAÍOCHTA
BHAILE ÁTHA CLIATH

DUBLIN

TECHNICAL UNIVERSITY DUBLIN

VLE COVID-19 Courses For Students For Staff Library Contact Us Gaeilge Q Search

STUDY RESEARCH CONNECT EXPLORE CAO HUB

Discover Infinite Possibilities at TU Dublin

Advance Operators

- Advanced Operators
- <number1>..<number2>
- Conduct a number range search by specifying two numbers, separated by two periods, with no spaces. Be sure to specify a unit of measure or some other indicator of what the number range represents
- Examples:
 - Computer \$500..1000
 - DVD player \$250..350
 - boys clothes 2y..10



Computer \$500..1000



All

Images

Maps

News

Videos

More

Settings

Tools

Inspiron

For home and home office

Micro desktops, small desktops and desktops featuring Intel® Core™ processors and AMD processors and plenty of storage space for the latest entertainment and productivity features.

[Learn more](#)



Desktops Starting at \$279.99

[Small Desktop](#) | [Desktops](#)

With the large hard drives and expandability of the Inspiron Desktop, you'll never be pressed for storage space. Space-saving desktop design perfect for small spaces and ideal for expandability.



3000 Series All-in-One Starting at \$349.99

20" | New 22" | 24"

Space-saving all-in-one desktops with easy, all-in-one set-up. Featuring AMD or Intel® processors and wide-screen viewing.



5000 Series All-in-One Starting at \$699.99

24"

Powerful, 24-inch all-in-one desktop with rich multimedia features.



7000 Series All-in-One Starting at \$799.99

24"

Ultrathin 24-inch all-in-one is designed to impress with an Intel® RealSense™ Camera and Windows Hello.



boys clothes 2y..10



All Images News Videos Shopping More Settings Tools

About 9,080,000 results (0.66 seconds)

[Boys Clothes - 1½ - 10 years - Shop online | H&M](#)

www2.hm.com/en_ie/kids/shop-by-product/boys-size-18m-8y.html ▾

Comfy, practical and bursting with vibrant colours and charming prints – we have clothes and accessories for your boy's every need.

[Boys Clothes - 1½ - 10 years - Shop online](#)

www2.hm.com/en_ie/kids/shop-by.../boys-size-18m-8y.mobileapp.html?offset... ▾

Boys 1½-10 years. Back to top Back to start. Category. Boys 1½-10 years (). All. Accessories. Best Basics. Blazers & Waistcoats. Cartoons & Comics. Fancy dress.

[Children Pajamas Cotton Dinosaur Kids Clothes Boys Size 2Y-10Y ...](#)

amazin-movers-and-shakers.com/.../children-pajamas-cotton-dinosaur-kids-clothes-bo... ▾

Children Pajamas Cotton Dinosaur Kids Clothes Boys Size 2Y-10Y. \$27.99 (as of December 12, 2016, 2:49 pm). 100% cotton, soft and comfortable. Long sleeve ...

[Boys 2y-10y | Lola and the Boys](#)

<https://lolaandtheboys.com/product-category/boys/> ▾

Boys Ballin Paris Shirt. \$18.00 Select options · Boys Patchwork Jeans ... BOYS SHIRTS SIZE 8-10 · CUSTOM BOY CLOTHES · Custom Dresses · Featured Back ...

Advance Operators

- Advanced Operators: “Daterange:”
- Daterange: <start_date>-<end date>
- Find the Web pages between start date and end date
- Note: start_date and end date use the Julian date
- The Julian date is calculated by the number of days since January 1, 4713 BC. For example, the Julian date for August 1, 2001 is 2452122
- Examples:
2004.07.10=2453196
2004.08.10=2453258
- Vulnerabilities date range: 2453196-2453258

Google Search: Vulnerabilities daterange:2453196-2453258 - Microsoft Internet Explorer

File Edit View Favorites Tools Help

Back Forward Stop Home Search Favorites Media Print Find Copy Paste

Address http://www.google.ca/search?hl=en&ie=UTF-8&q=Vulnerabilities+daterange%3A2453196-2453258&btnG=Search&meta=

Google Vulnerabilities daterange:2453196-2453258 Search Web PageRank 2 blocked AutoFill Options

Web Images Groups News more » Vulnerabilities daterange:2453196-2453258 Search Advanced Search Preferences

Search: the web pages from Canada

Web Results 1 - 10 of about 880,000 for Vulnerabilities daterange:2453196-2453258. (0.50 seconds)

[Common Vulnerabilities and Exposures](#)
Common **Vulnerabilities** and Exposures (CVE) is a list or dictionary that provides common names for publicly known information security **vulnerabilities** and ...
www.cve.mitre.org/ - 13k - 8 Aug 2004 - [Cached](#) - [Similar pages](#)

[SANS Top 20 Vulnerabilities - The Experts Consensus](#)
... Pentagon hacking incident and the easy and rapid spread of the Code Red and NIMDA worms can be traced to exploitation of unpatched **vulnerabilities** on this list ...
www.sans.org/top20/ - 101k - 8 Aug 2004 - [Cached](#) - [Similar pages](#)

[{PivX Solutions, LLC}](#)
... It tries to exploit 7 different **vulnerabilities** to infect Windows machines, ranging from the Messenger Service buffer overrun, the uPnP overflow, LSASS as well ...
www.pivx.com/lehnlm/unpatched/ - 7k - 8 Aug 2004 - [Cached](#) - [Similar pages](#)

Sponsored Links

[Vulnerability Database](#)
Easy-to-use & validated info.
Free and updated daily.
www.secunia.com

[DIGEV 2004](#)
1st International Digital Evidence Web Conference. You're invited!
www.digev2004.com

[Network Security](#)
Free info on network security, software and enterprise solutions

Discussions Discussions not available on http://www.google.ca/ Internet

The image shows a Google search results page. In the top left corner is the Google logo. To its right is a search bar containing the query "dit daterange: 2457762-2457762". On the far right of the search bar is a blue magnifying glass icon. Below the search bar is a navigation bar with several tabs: "All" (which is highlighted with a blue underline), "Maps", "Videos", "News", "Images", and "More". To the right of these tabs are "Settings" and "Tools" buttons. The main content area below the navigation bar displays the message "Your search - dit daterange: 2457762-2457762 - did not match any documents." followed by a section titled "Suggestions:" with a bulleted list.

dit daterange: 2457762-2457762

All Maps Videos News Images More Settings Tools

Your search - **dit daterange: 2457762-2457762** - did not match any documents.

Suggestions:

- Make sure that all words are spelled correctly.
- Try different keywords.
- Try more general keywords.
- Try fewer keywords.

Advance Operators

- Advanced Operators “Link:”
- Link: URL
 - Find the Web pages having a link to the specified URL
- Related: URL
 - Find the Web pages that are “similar” to the specified Web page
- Define: search_term
 - Provide a definition of the words gathered from various online sources
- Examples:
 - Link:tudublin.ie
 - Related:dit.ie
 - Define:network security



link:tudublin.ie

X



<https://tudublin.ie> › for-students › student-login

[Student Login | TU Dublin](#)

As a student of TU Dublin you are entitled to the use of a wide range of services including email, Wi-Fi, print services, data storage, software and much ...

<https://tudublin.ie> › for-students › starting-at-tu-dublin › g...

[Getting Online | TU Dublin](#)

For access to Moodle, Tallaght students should use this link <https://elearning-ta.tudublin.ie> while those in Blanchardstown can visit the LMS here ...

6 Sept 2021 · Uploaded by IS Support

<https://tudublin.ie> › for-staff › city-centre

[City Centre Login | TU Dublin](#)

Staff Login · Username: firstname.lastname@tudublin.ie · Username: staffnumber · Business Apps · Useful Links · Privacy Preference Center.

<https://tudublin.ie> › how-to-apply › entry-pathways › a...

[Access TU Dublin](#)

Application Support from TU Dublin Access Service staff; Reduced points CAO ... The information in the link below is correct as of the 17th August 2021:

<https://www.tudublin.ie> › student-services-and-support

[Registration | TU Dublin](#)

Welcome to Registration for TU Dublin. We manage the registration and fee payment process for students on your programme and modules. Useful Links.



related:www.dit.ie



All Images Maps Shopping More

Settings Tools

About 46 results (0.13 seconds)

[University College Dublin](#)

www.ucd.ie/ ▾

This website uses cookies, by continuing you agree to their use. Learn more about cookies and how to manage them on cookie policy. Close. It appears JavaScript is disabled. To get the most out of the website we recommend enabling JavaScript in your browser. Home · Current Students · Alumni · Community · News and ...

[Waterford Institute of Technology](#)

<https://www.wit.ie/> ▾

Waterford Institute of Technology (WIT) is a university-level institution in the South-East of Ireland with over 10000 students and 1000 staff. WIT offers tuition and research programmes in various areas from Higher Certificate to Degree to PhD.

[Trinity College Dublin, the University of Dublin, Ireland](#)

<https://www.tcd.ie/> ▾

Cookies on the Trinity College Dublin website. By using this website you consent to the use of cookies in accordance with the Trinity cookie policy. OK. Skip to main content. Trinity College Dublin, The University of Dublin. Menu Search. Trinity Search. Your query. Search collection. All Trinity, Undergraduate Courses ...

[NUI Galway - NUI Galway](#)

www.nuigalway.ie/ ▾

Dr Elaine Toomey and Dr David Mothersill from the School of Psychology at NUI Galway, have both



Define:network security



All Images News Videos Shopping More

Settings Tools

About 2,760,000 results (0.45 seconds)

Network security is protection of the access to files and directories in a computer **network** against hacking, misuse and unauthorized changes to the system. An example of **network security** is an anti-virus system.



www.cisco.com

[Network security dictionary definition | network security defined](#)
www.yourdictionary.com/network-security

[About this result](#) [Feedback](#)

People also ask

What do you mean by network security? ▼

What are the different types of network security? ▼

What is the job of network security engineer? ▼

Why is Network Security? ▼

[Feedback](#)

Advance Operators

- Advanced Operators “phonebook:”
- Phonebook
 - Search the entire Google phonebook
- rphonebook
 - Search residential listings only
- bphonebook
 - Search business listings only
- Examples:
 - Phonebook: robert las vegas (robert in Las Vegas)
 - Phonebook: (702) 944-2001 (reverse search, not always work)
 - The phonebook is quite limited to U.S.A

Google Search: robert las vegas - Microsoft Internet Explorer

File Edit View Favorites Tools Help

Back Forward Stop Refresh Home Search Favorites Media Mail Print Find Copy Paste Address http://www.google.ca/search?hl=en&ie=UTF-8&pb=f&q=robert+las+vegas&pb=f Go Links

Google robert las vegas Search Web PageRank 2 blocked AutoFill Options

Web Images Groups News more »

Google PhoneBook Search PhoneBook Search the Web Preferences

Business Phonebook

Results 1 - 5 of about 219 for **robert las vegas**. (0.31 seconds)

Century Vision Center, **Robert Pearson** Od - (702) 944-2001 - , Las Vegas, NV 89101 - [Yahoo! Maps](#) - [MapQuest](#)

Eob, Head Start Centers, **Robert Jones** Gardens - (702) 438-3770 - 1750 Marion Dr, Las Vegas, NV 89115 - [Yahoo! Maps](#) - [MapQuest](#)

Clark County Of, Constable **Robert Bobby G Gronauer** - (702) 385-2436 - , Las Vegas, NV 89101 - [Yahoo! Maps](#) - [MapQuest](#)

Clark County Of, Constable **Robert Bobby G Gronauer**, Las Vegas Township - (702) 455-4099 - 309 S 3rd St, Las Vegas, NV 89101 - [Yahoo! Maps](#) - [MapQuest](#)

American Family Insurance, Career Opportunities, Harrison **Robert** - (702) 732-4708 - 3993 Howard Hughes Pkwy, Las Vegas, NV 89109 - [Yahoo! Maps](#) - [MapQuest](#)

[More business listings...](#) ([Removal Info](#))

Residential Phonebook

Results 1 - 5 of about 7 for **robert las vegas**. (0.31 seconds)

I **Robert** - (702) 433-6314 - 3890 S Nellis Blvd, Las Vegas, NV 89121 - [Yahoo! Maps](#) - [MapQuest](#)

Enrique **Robert** - (702) 792-9312 - 2700 S Valley View Blvd, Las Vegas, NV 89102 - [Yahoo! Maps](#) - [MapQuest](#)

F S **Robert** - (702) 631-2034 - , Las Vegas, NV 89101 - [Yahoo! Maps](#) - [MapQuest](#)

Howard **Robert** - (702) 260-8896 - , Las Vegas, NV 89101 - [Yahoo! Maps](#) - [MapQuest](#)

Discussions Discussions not available on http://www.google.ca/ Internet

Google Search: (702) 944-2001 - Microsoft Internet Explorer

File Edit View Favorites Tools Help

Back Stop Home Search Favorites Media Mail Print

Address <http://www.google.ca/search?hl=en&ie=UTF-8&pb=f&q=%28702%29+944-2001&pb=f&btnG=Search+PhoneBook> Go Links

Google [\(702\) 944-2001](#) Search Web PageRank 2 blocked AutoFill Options

Web [Images](#) [Groups](#) [News](#) [more »](#)

Google PhoneBook [Search PhoneBook](#) [Search the Web](#) [Preferences](#)

Business Phonebook Results 1 - 8 of 8 for (702) 944-2001 . (0.03 seconds)

Century Vision Center, Robert Pearson Od - **(702) 944-2001** - , Las Vegas, NV 89101 - [Yahoo! Maps](#) - [MapQuest](#)

Century Vision Center, Ronald Dutton Od - **(702) 944-2001** - , Las Vegas, NV 89101 - [Yahoo! Maps](#) - [MapQuest](#)

Century Vision Center - **(702) 944-2001** - 8230 W Sahara Ave, Las Vegas, NV 89117 - [Yahoo! Maps](#) - [MapQuest](#)

Century Vision Center, Michael Crutchfield Od - **(702) 944-2001** - 8230 W Sahara Ave, Las Vegas, NV 89117 - [Yahoo! Maps](#) - [MapQuest](#)

Cohen David B MD - **(702) 944-2001** - 8230 W Sahara Ave, Las Vegas, NV 89117 - [Yahoo! Maps](#) - [MapQuest](#)

Crutchfield Michael Od - **(702) 944-2001** - 8230 W Sahara Ave Infocus, Las Vegas, NV 89101 - [Yahoo! Maps](#) - [MapQuest](#)

Dutton Ronald Od - **(702) 944-2001** - 8230 W Sahara Ave, Las Vegas, NV 89117 - [Yahoo! Maps](#) - [MapQuest](#)

Somers William Od - **(702) 944-2001** - 8230 W Sahara Ave, Las Vegas, NV 89117 - [Yahoo! Maps](#) - [MapQuest](#)

Discussions Discussions not available on http://www.google.ca/

Done Internet

Advance Operators

- Advanced Operators “author:”
- author : name
 - It restrict the Google search results to show pages only about the author you specify.
- Examples:
 - author: william stalling
 - operating system author: william stalling
 - author: “aneel rahim”



author: william stalling



All Images News Videos Maps More

Settings Tools

About 457,000 results (0.72 seconds)

[William Stallings](#)

williamstallings.com/ ▾

BOOKS BY WILLIAM STALLINGS ... Welcome to the Web site for the computer science textbooks of William Stallings. He is an 12-time winner of the Texty Award ...

[ComputerOrganization](#) · [Cryptography](#) · [OperatingSystems](#) · [NetworkSecurity](#)

[Amazon.com: William Stallings: Books, Biography, Blog, Audiobooks ...](#)

<https://www.amazon.com/William-Stallings/e/B000APXR9Q> ▾

Dr. William Stallings is an American author. He has written textbooks on computer science topics such as operating systems, computer networks, computer ...

[William Stallings - Wikipedia](#)

https://en.wikipedia.org/wiki/William_Stallings ▾

Dr. William Stallings is an American author. He has written textbooks on computer science topics such as operating systems, computer networks, computer ...

[Books by William Stallings \(Author of Computer Organization and ...\)](#)

https://www.goodreads.com/author/list/47971.William_Stallings ▾

William Stallings has 77 books on Goodreads with 6203 ratings. William Stallings's most popular book is Computer Organization and Architecture: Designing...



operating system author: william stalling



All

Images

News

Videos

Shopping

More

Settings

Tools

About 382,000 results (0.61 seconds)

Operating Systems - William Stallings

[williamstallings.com/Operating Systems/](http://williamstallings.com/Operating%20Systems/) ▾

BOOKS BY WILLIAM STALLINGS. OPERATING ... A state-of-the art survey of operating system principles. Covers ... OPERATING SYSTEMS, EIGHTH EDITION.

OS8e-Student · OS8e-Instructor · OS7e-Instructor · OS7e-Student

Operating Systems, Sixth Edition - William Stallings

williamstallings.com/OS/OS6e.html ▾

Student Resources Operating Systems: Internals and Design Principles, Sixth Edition. Last updated: Thursday, November 11, 2010 ...

Operating Systems - William Stalling 6th edition.pdf - Google Drive

<https://docs.google.com/file/d/0ByWx.../edit> ▾

Sign in. Loading... Whoops! There was a problem loading more pages. Retrying... Whoops! There was a problem previewing this document. Retrying.

Operating Systems: Internals and Design Principles (8th Edition ...

<https://www.amazon.com/Operating-Systems-Internals-Design.../dp/0133805913> ▾

Operating Systems: Internals and Design Principles (8th Edition) [William ... Data and Computer Communications (10th Edition) (William Stallings Books on ...



author: "Aneel Rahim"



All

Images

News

Videos

Maps

More

Settings

Tools

About 1,430 results (0.50 seconds)

Aneel Rahim - Semantic Scholar

<https://www.semanticscholar.org/author/Aneel-Rahim/2548533> ▾

Semantic Scholar profile for Aneel Rahim, with fewer than 50 highly influential citations, fewer than 50 est. total ... Authors who most influenced Aneel Rahim:

STR member: Aneel Rahim publishes two papers: Intrusion Detection ...

<str.tssg.org/2013/12/27/str-member-aneel-rahim-publishes-two-papers/> ▾

Dec 27, 2013 - Paper Title:Intrusion Detection System for Wireless Nano Sensor Networks.
Authors:Aneel Rahim, Paul Malone. Conference:The 8th ...

Aneel Rahim - Articles - Scientific Research Publishing

<www.scirp.org> > Journals ▾

Aneel Rahim. ... Information for Authors · Paper Submission · Manuscript Tracking System · Join Peer-Review Program · Free SCIRP Newsletter · Call for Special ...

Aneel Rahim, Fahad Bin Muhaya - جامعة الملك سعود -

<search.ksu.edu.sa/ar/search?num=10&q=aneel+rahim+fahad+bin...site...> ▾

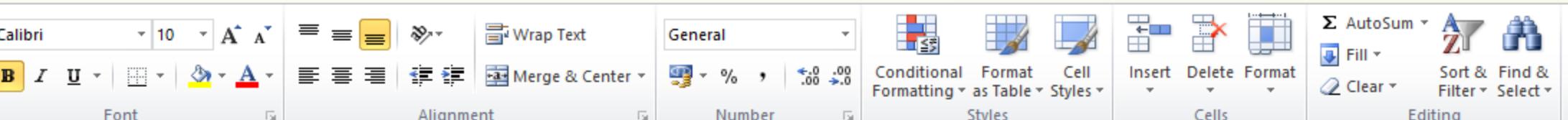
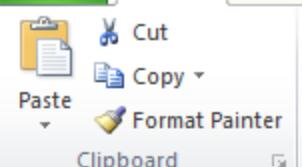
<http://pmc.ksu.edu.sa/ar/journals-papers> ... Authors: Aneel Rahim, Fahad Bin Muhaya, Zeeshan Shafii, MA Ansari, Muhammad Sher. Journal: Informatica.

Google Hacking

- What can google can do for a hacker?
 - Search sensitive information like payroll, even personal email box
 - Vulnerabilities scanner
 - Transparency proxy

Google Hacking

- Financial Information
 - sales filetype: xls site: ie



Google Hacking

- Personal Mailbox
 - intitle: index.of inurl:inbox

Index of /INBOX

	<u>Name</u>	<u>Last modified</u>	<u>Size</u>	<u>Description</u>
	Parent Directory		-	
	OLD/	05-Jan-2017 17:21	-	
	archivo.tar.gz	12-May-2009 10:58	1.4M	
	msg0000.WAV	05-Jan-2017 18:05	2.2K	
	msg0000.gsm	05-Jan-2017 18:05	2.2K	
	msg0000.txt	05-Jan-2017 18:05	249	
	msg0000.wav	05-Jan-2017 18:05	22K	
	msg0001.WAV	06-Jan-2017 11:26	34K	
	msg0001.gsm	06-Jan-2017 11:26	35K	
	msg0001.txt	06-Jan-2017 11:26	255	
	msg0001.wav	06-Jan-2017 11:26	337K	
	msg0002.WAV	06-Jan-2017 20:10	29K	
	msg0002.gsm	06-Jan-2017 20:10	29K	
	msg0002.txt	06-Jan-2017 20:10	250	
	msg0002.wav	06-Jan-2017 20:10	283K	
	msg0003.WAV	06-Jan-2017 20:12	23K	
	msg0003.gsm	06-Jan-2017 20:12	23K	
	msg0003.txt	06-Jan-2017 20:12	250	
	msg0003.wav	06-Jan-2017 20:12	223K	

Google Hacking

- Confidential Files
 - "not for distribution" confidential

About 325,000 results (0.25 seconds)

CONFIDENTIAL**NOT FOR
DISTRIBUTION****DOCUMENTARY SYNOPSIS:****UNACKNOWLEDGED: AN EXPOSE OF THE GREATEST SECRET IN HUMAN HISTORY**

Created by: Steven M. Greer MD Release Date: Fall 2016
Director: TBA Produced by: SiriusDisclosure.com

In the aftermath of the most successful crowd-funded documentary in history, Sirius, Dr. Greer and his team are producing "Unacknowledged : An Expose of the Greatest Secret in Human History".

Sirius reached number 1 on Netflix for documentaries and was acclaimed throughout the world. With virtually no marketing or P & A budget, Sirius reached millions of people and has had over \$1 million in revenue.

"Unacknowledged" will focus on the historic files of the Disclosure Project and how UFO secrecy has been ruthlessly enforced - and why. The best evidence for Extraterrestrial contact, dating back decades, will be presented with direct top-secret witness testimony, documents and UFO footage.

The behind-the-scenes research and high level meetings convened by Dr. Steven Greer will expose the degree of illegal, covert operations at the core of UFO secrecy. From meetings with Laurance Rockefeller and the Clintons, to briefings with the CIA Director, top Pentagon Generals and Admirals, to the briefing of President Obama via senior advisor John Podesta, current chairman of the Hillary Clinton Campaign - we will take the viewer behind the veil of secrecy and into the



GET CERTIFIED

Google Hacking Database

Filters

Reset All

Show Quick Search

Date Added

Dork

Category

Author

2019-01-30	intitle:QueryService Web Service	Various Online Devices	Miguel Santareno
2019-01-25	intitle:"index of /" ssh	Sensitive Directories	FlyingFrog
2019-01-21	"Please click here to download and install the latest plug-in. Close your browser before installation."	Various Online Devices	Sohail E.B.
2019-01-21	inurl:pwm/public/	Pages Containing Login Portals	Sohail E.B.
2019-01-18	inurl:login.zul	Pages Containing Login Portals	ManhNho
2019-01-18	intitle:FCKeditor - Uploaders Tests"	Footholds	Burov Konstantin
2019-01-18	intitle:FCKeditor - Connectors Tests"	Footholds	Burov Konstantin
2019-01-17	inurl:setup.cgi@next_file=	Various Online Devices	ManhNho
2019-01-14	intitle:Index of / inurl:passport	Sensitive Directories	Bl4kd43m0n

Latest Google Vulnerabilities 2018

- Finds Login Pages of CentOS
 - `inurl:/login/index.php intitle:CentOS`



inurl:/login/index.php intitle:CentOS



All Images Videos News Maps More

Settings Tools

4 results (0.20 seconds)

[Server CentOS powered by HTTP Test Page Apache -www ...](#)

www.microfin360.com/login/index.php/g700chorographical-cbrachymetropia17996/ ▾

This page is used to test the proper operation of the Apache HTTP server after it has been installed. If you can read this page it means that the Apache HTTP server installed at this site is working properly. If you are a member of the general public: The fact that you are seeing this page indicates that the website you just ...

[SSL login](#)

<https://128.199.170.195:2031/login/index.php>

Login to CentOS WebPanel. Fast Login (no stats and checks). You are using SSL login. Visit Website How to Install. © 2017 CentOS WebPanel control panel for linux.

[Login | CentOS WebPanel](#)

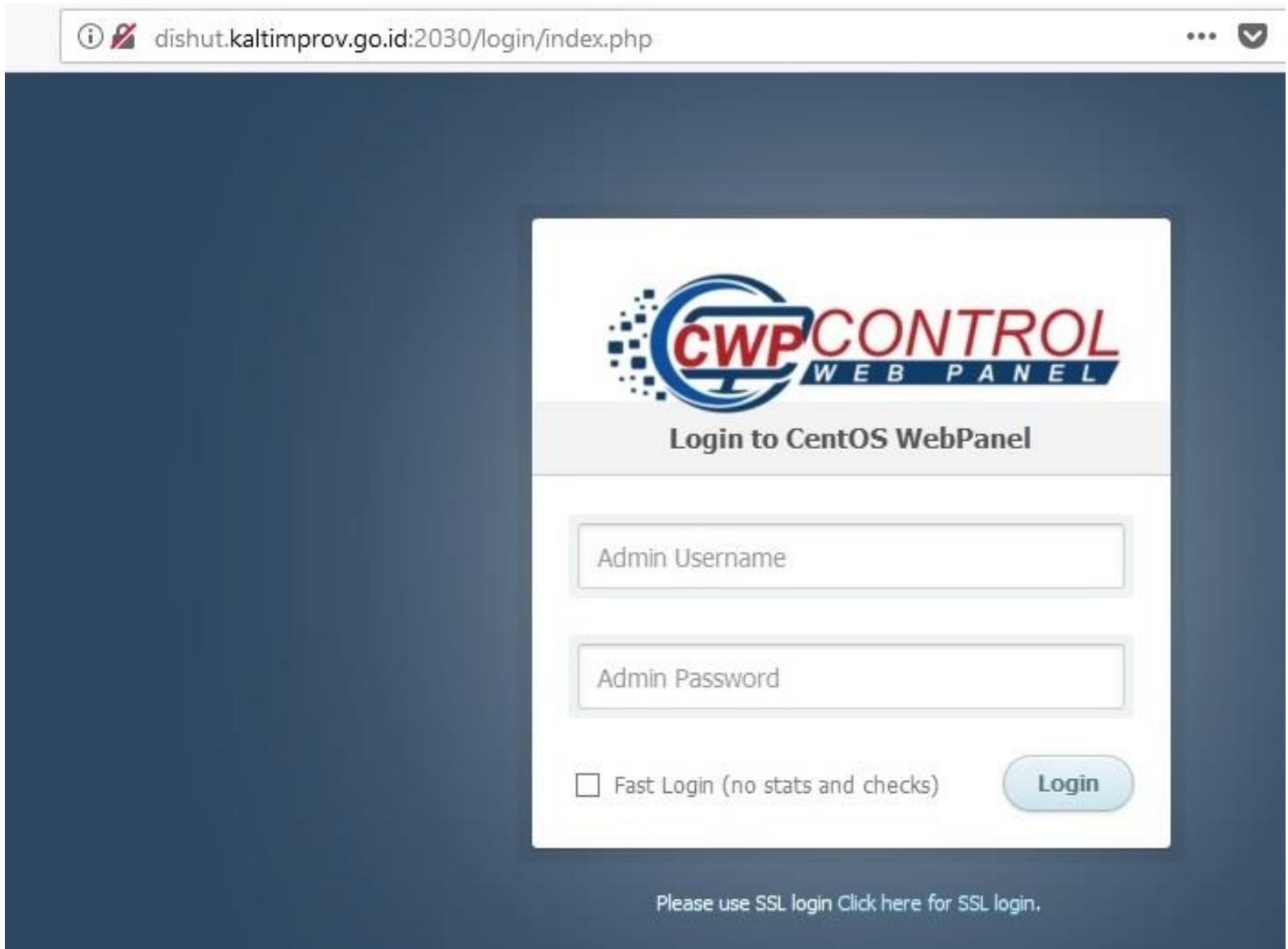
dishut.kaltimprov.go.id:2030/login/index.php ▾

Login to CentOS WebPanel. Fast Login (no stats and checks). Please use SSL login Click here for SSL login. Visit Website How to Install. © 2017 CentOS WebPanel control panel for linux.

[Login | CentOS WebPanel - Web Site Satpol PP Prov.Kaltim](#)

satpolpp.kaltimprov.go.id:2030/login/index.php ▾

Login to CentOS WebPanel. Fast Login (no stats and checks). Please use SSL login Click here for SSL login. Visit Website How to Install. © 2017 CentOS WebPanel control panel for linux.



Latest Google Vulnerabilities 2018

- List all server statistics , hardware and software details
 - intitle:"PHP Web Stat - Sysinfo" intext:php inurl:stat/sysinfo.php



intitle:"PHP Web Stat - Sysinfo" intext:php inurl:stat/sysinfo.php



All

Images

Videos

News

Shopping

More

Settings

Tools

About 27 results (0.40 seconds)

PHP Web Stat - Sysinfo - Haus Martin

hausmartin.org/stat/sysinfo.php ▾

Server Info. Server Host, alfa3011.alfahosting-server.de. Server OS, Apache. PHP Version, 5.2.17. Max Execution T. 30 sec. Memory Limit, 16MB. Session Support, enabled. Cookie Support, disabled ...

PHP Web Stat - Sysinfo

www.sorenm.com/stat/sysinfo.php ▾

Server Info. Server Host, dd39220.kasserver.com. Server OS, Apache. PHP Version, 5.5.38-nmm3. Max Execution T. 30 sec. Memory Limit, 128MB. Session Support, enabled. Cookie Support, disabled ...

PHP Web Stat - Sysinfo - Meteo Gouda

www.meteo-gouda.nl/stat/sysinfo.php

Stat Info. Script Version, 4.9.15. Script Activity, enabled. DB Active, OFF. Script Domain, http://www.meteo-gouda.nl. Script Path, stat/. Starting Page, index.php. Domain(s), weerstation-gouda-bloemendaal.nl meteo-gouda.nl. URL Parameter. Frames, enabled. IP Recount Time, 10 min. Update Check, enabled.

PHP Web Stat - Sysinfo

www.fv-dresden-sw.de/stat/sysinfo.php ▾

Stat Info. Script Version, 4.9.15. Script Activity, enabled. DB Active, OFF. Script Domain, http://www.fv-dresden-sw.de. Script Path, stat/. Starting Page, index.php. Domain(s), fv-dresden-sw.de. URL Parameter. Frames, OFF. IP Recount Time, 60 min. Update Check, enabled. Error Reporting, OFF. Log htaccess, enabled.



PHP Web Stat

SysInfo v2.4

[Stat](#)[Counter](#)[File Version](#)[Admin-Center](#)

Stat Info

Script Version	4.9.15
Script Activity	✓
DB Active	OFF
Script Domain	http://www.hausmartin.org
Script Path	stat/
Starting Page	index.html
Domain(s)	hausmartin.org
URL Parameter	
Frames	OFF
IP Recount Time	5 min.
Update Check	✓
Error Reporting	✓
Log htaccess	OFF
Creator Number	5.000
Referer Cut	0
Index Number	30.000
Cache Update	OFF
Country detection	08/2014
Last log entry	27.01.2018 08:44:24

File Check

File	Version
config/admin.php	✓
config/backup.php	✓
config/reset.php	✓
config/setup.php	✓
func/func_browser.php	✓
func/func_cache_write.php	✓
func/func_display.php	✓
func/func_load_creator.php	✓
func/func_operating_system.php	✓
func/func_pattern_matching.php	✓
func/func_pattern_reverse.php	✓
func/html_header.php	✓
./archive.php	✓
./cache_creator.php	✓
./cache_panel.php	✓
./cookie.php	✓
./counter.php	✓
./index.php	✓
./last_hits.php	✓
./plugin_loader.php	✓
./syscheck.php	✓
./sysinfo.php	✓
./track.php	✓
./track_file.php	✓

Server Info

Server Host	alfa3011.alfahosting-server.de
Server OS	Apache
PHP Version	5.2.17
Max Execution T.	30 sec.
Memory Limit	16MB
Session Support	✓
Cookie Support	✓

Server Info

Server Host	dd39220.kasserver.com
Server OS	Apache
PHP Version	5.5.38-nmm3
Max Execution T.	30 sec.
Memory Limit	128MB
Session Support	✓
Cookie Support	✓

./syscheck.php
./sysinfo.php
./track.php
./track_file.php

**File CHMOD Status**

File	Size	Rows	CHMOD	Status
backup/		755	666	!
log/		777	666	✓
log/archive/		777	666	✓
config/config.php		666	666	✓
config/config_db.php		666	666	✓
config/pattern_site_name.inc	222,88 KB	2685	666	✓
config/pattern_string_replace.inc	0,00 KB	0	666	✓
config/tracking_code.php	0,49 KB	15	666	!
cache_time_stamp.php	0,04 KB	1	666	✓
cache_time_stamp_archive.php	0,04 KB	1	666	✓
cache_visitors.php	2.091,00 KB	20.961	666	✓
cache_visitors_archive.php	28,24 KB	1.604	666	✓
logdb.dta	27,53 KB	605	666	✓
logdb_backup.dta	24.403,25 KB	534.909	666	✓
logdb_temp.dta	26,44 KB	580	666	✓
logdb_track_file.dta	0,28 KB	1	666	✓
pattern_browser.dta	7,13 KB	342	666	✓
pattern_operating_system.dta	0,27 KB	21	666	✓
pattern_referer.dta	2.165,20 KB	11.870	666	✓
pattern_resolution.dta	8,19 KB	659	666	✓
pattern_site_name.dta	375,58 KB	7.941	666	✓

Latest Google Vulnerabilities 2018

- Show live cams and tv
 - `inurl:embed.html inurl:dvr`



inurl:embed.html inurl:dvr



All

Videos

Images

News

Shopping

More

Settings

Tools

About 3,480 results (0.20 seconds)

d4fee077-1a44-47fb-a367-d15cad794a2a

langate.tv/d4fee077-1a44-47fb-a367-d15cad794a2a/embed.html?dvr=false ▾

brixer - AirMAX

<https://streaming.airmax.pl/brixer/embed.html?dvr=false> ▾

Dvorkino_1

5.189.243.162:8082/Dvorkino_1/embed.html?dvr=false ▾

Video is not available.

rysianka2

91.224.104.112:8181/rysianka2/embed.html?dvr=false ▾

Video is not available.

dvoracky-panorama

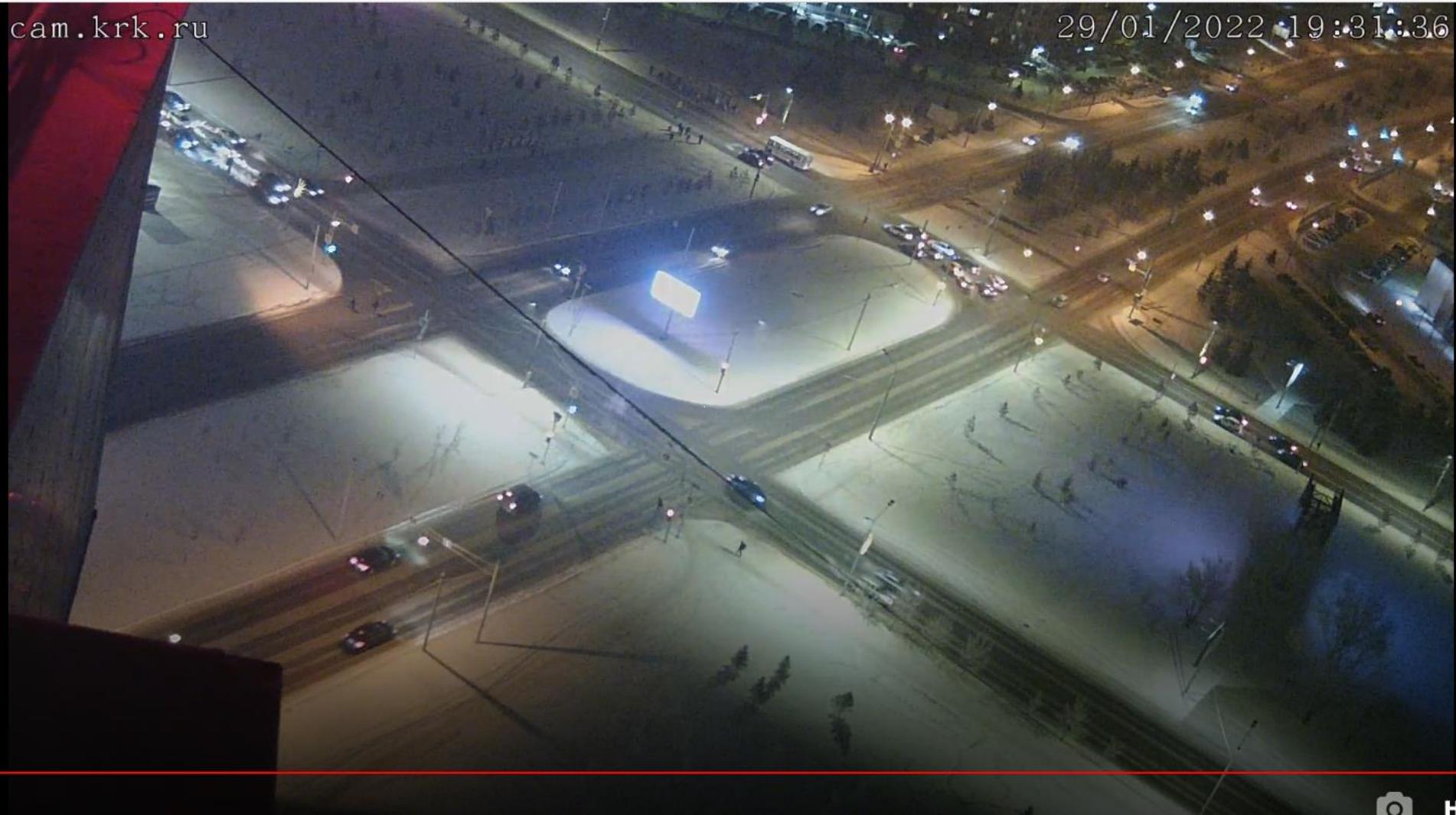
79.98.156.78:8080/dvoracky-panorama/embed.html?dvr=false&proto=hls ▾

live. back to live. Disabled.

BishopsLydeard_59234

mirlees.railcam.co.uk:8080/BishopsLydeard_59234/embed.html?dvr=false...rtmp ▾

live. back to live. Disabled.



Latest Google Vulnerabilities 2018

- list of FTP/SFTP passwords from the text.
 - intitle:"Index Of" intext:sftp-config.json



intitle:"Index Of" intext:sftp-config.json



All

Images

Videos

News

Shopping

More

Settings

Tools

About 160 results (0.23 seconds)

Index of /kitnes/cache.old/pages2/sftp/config.json - GBC Ghana

www.gbcghana.com/kitnes/cache.old/pages2/sftp/config.json/ ▾

Index of /kitnes/cache.old/pages2/sftp/config.json. Name · Last modified · Size · Description · Parent Directory, -., 1.htm, 2015-07-11 18:30, 0.

Index of /wp-includes - Bronx Lebanon Ophthalmology

bronx-lebanon-ophthalmology.org/wp-includes/ ▾

... post-template.php · post-thumbnail-template.php · post.php · query.php · random_compat/ · registration-functions.php · registration.php · rest-api.php · rest-api/ · revision.php · rewrite.php · rss-functions.php · rss.php · script-loader.php · session.php · sftp-config.json · shortcodes.php · taxonomy.php · template-loader.php ...

Index of /assets - PintaSuper

pintasuper.com/assets/ ▾

Name · Last modified · Size · Description · Parent Directory, -., cache/, 2015-04-02 13:20, -., css/, 2016-04-30 14:47, -., docs/, 2015-04-02 13:20, -., fonts/, 2016-04-30 14:47, -., images/, 2016-04-30 14:48, -., js/, 2016-04-30 14:49, -., pdf/, 2015-04-02 13:20, -., sftp-config.json, 2016-04-30 13:20, 1.4K, svg/, 2016-04-30 14:48, -.

intitle:"Index Of" intext:sftp-config.json - Exploit-DB

<https://www.exploit-db.com/ghdb/4657/> ▾

Jan 12, 2018 - 1. 2. 3. 4. 5. 6. 7. 8. Description : This dork returns list of FTP/SFTP passwords from sublime text. Dork : intitle:"Index Of" intext:sftp-config.json. Author : Vipin Joshi (@vocuzi) ...

The screenshot shows a browser window displaying the contents of a JSON file at the URL bronx-lebanon-ophthalmology.org/wp-includes/sftp-config.json. The browser interface includes standard navigation buttons (back, forward, search, home) and tabs for 'JSON', 'Raw Data' (which is selected), and 'Headers'. Below the tabs are 'Save' and 'Copy' buttons. The JSON code itself is presented in a monospaced font. A red rectangular box highlights the connection details (host, user, password, port) which are sensitive pieces of information.

```
{  
    // The tab key will cycle through the settings when first created  
    // Visit http://wbond.net/sublime\_packages/sftp/settings for help  
  
    // sftp, ftp or ftps  
    "type": "ftp",  
  
    "save_before_upload": true,  
    "upload_on_save": false,  
    "sync_down_on_open": false,  
    "sync_skip_deletes": false,  
    "sync_same_age": true,  
    "confirm_downloads": false,  
    "confirm_sync": true,  
    "confirm_overwrite_newer": false,  
  
    "host": "70.32.92.106",  
    "user": "mwt_ftp_user",  
    "password": "!11oRKCTX!",  
    // "port": "22",  
  
    "remote_path": "/htdocs",  
    "ignore_regexes": [  
        "\\.sublime-(project|workspace)", "sftp-config(-alt\\d?)?\\.json",  
        "sftp-settings\\.json", "/venv/", "\\.svn/", "\\.hg/", "\\.git/",  
        "\\.bzr", "_darcs", "CVS", "\\.DS_Store", "Thumbs\\.db", "desktop\\.ini"  
    ],  
    // "file_permissions": "664",  
    // "dir_permissions": "775",  
  
    // "extra_list_connections": 0,  
}
```

The screenshot shows a browser window with the URL `pintasuper.com/assets/sftp-config.json`. The tab bar includes icons for back, forward, refresh, and home. Below the URL, there are tabs for "JSON" (which is selected), "Raw Data", and "Headers". Underneath the tabs are "Save" and "Copy" buttons. The main content area displays a JSON object with the following structure:

```
{  
    // The tab key will cycle through the settings when first created  
    // Visit http://wbond.net/sublime_packages/sftp/settings for help  
  
    // sftp, ftp or ftps  
    "type": "sftp",  
  
    "save_before_upload": true,  
    "upload_on_save": false,  
    "sync_down_on_open": false,  
    "sync_skip_deletes": false,  
    "sync_same_age": false,  
    "confirm_downloads": false,  
    "confirm_sync": true,  
    "confirm_overwrite_newer": false,  
  
    "host": "ftp.pintasuper.com",  
    "user": "pintasuper",  
    "password": "KXRD00wjr9",  
    "port": "22",  
  
    // "remote_path": "/home/pintasuper/public_html/prueba",  
    // "remote_path": "/home/pintasuper/public_html/",  
    // "ignore_regexes": [  
    // ]  
}
```

Latest Google Vulnerabilities 2018

- Finds vulnerable printers
 - `inurl:"/websys/webArch/mainFrame.cgi" -hatana`



inurl:"/websys/webArch/mainFrame.cgi" -hatana



All Maps Images News Shopping More Settings Tools

About 60 results (0.36 seconds)

RNP002673A96CBA - Web Image Monitor - PRINTER-HACKED

[impsecfyp.us.es/web/guest/en/websys/webArch/mainFrame.cgi](#) ▾

Status. System: Status OK. Toner: Status OK. Waste Toner Bottle: Status OK. Input Tray: Status OK. Output Tray: Status OK. Check Details. Skip menu and go to the main content. Status/Information. Device Info - Status - Counter - Job - Inquiry. Device Management. Configuration - Device Home Management. Print Job/Stored ...

Web Image Monitor

[62.93.36.200/web/user/en/websys/webArch/mainFrame.cgi](#) ▾

SMB - System Log - Webpage. Top Page. Click [Refresh] to display current status. Help. Refresh. Web Image Monitor. Device Name, : RNP802EE8. Comment, : DRUKARKA-FIZYKA. Status. Printer, : Alert. Copier, : Alert. Scanner, : Energy Saver Mode. Detail. Point to each function with mouse pointer to display details.

192.168.1.101 /web/guest/en/websys/webarch ... - IPAddress.com

<https://www.ipaddress.com/search/192.168.1.../en/websys/webarch/mainframe.cgi> ▾

Your search for 192.168.1.101 /web/guest/en/websys/webarch/mainframe.cgi would give you better results when you put the query in the form of a domain name or IP address format. The term 192.168.1.101 /web/guest/en/websys/webarch/mainframe.cgi can be used in domains. Our suggested articles will help you put ...

[Home](#)

[Status/Information](#)

[Device Management](#)

[Print Job/Stored File](#)

[Convenient Links](#)

① impsecfyp.us.es/web/guest/en/websys/webArch/mainFrame.cgi

... [Bookmark](#) [Star](#) [Search](#)

RICOH MP C3003 Web Image Monitor

English [Switch](#) [Refresh](#)

Device Name : Ricoh MPC 3003
Location :
Comment :
Host Name : RNP002673A96CBA



Alert

- Alert
- Messages (0item(s))

Status

System	 Status OK
Toner	 Status OK
Waste Toner Bottle	 Status OK
Input Tray	 Almost Out of Paper
Output Tray	 Status OK

Latest Google Vulnerabilities 2019

- Access SAP Crystal report
- **inurl:apspassword**



inurl:apspassword



All Images Maps Videos News More

Settings Tools

About 36 results (0.22 seconds)

Crystal Reports Viewer

rz3.cubeserv.com:49000/BOE/OpenDocument/.../viewrpt.cwr?...apspassword... ▾

The viewer could not process an event. The object with ID 326660 does not exist in the CMS or you do not have the right to access it. [CRSDK00001182] ...

Crystal Reports Viewer

200.77.230.24/.../viewrpt.aspx?...apspassword... ▾ [Translate this page](#)

AV. ESPARTO NO. 1165. VALLE DEL PEDREGAL. (686)2-23-96-16. HIGUERA REYES
ALEJANDRO. HIRA-800430-4G1. HIRA800430HSLGYL06. 0. MÉXICO.

Crystal Reports Viewer

200.77.230.24/crystalreportviewers115/viewrpt.aspx?id...apspassword... ▾

@Annio, @Annio. Set to Null. @Mes, @Mes. Set to Null. @icveie, @icveie. Set to Null. @quincena, @quincena. Set to Null. OK.

Crystal Reports Viewer - ncdenr.org

<https://reports.ncdenr.org/BOE/.../viewrpt.cwr?id...U&apspassword...> ▾

Enter prompt values. Please enter Animal Operations Permit Number (must include NC or NCG prefix):, prm00_Permit_Number. OK.

ⓘ 200.77.230.24/crystalreportviewers115/HTMLViewerBridge.aspx?id=15114811

1 / 1+ Main Report | 100% | BusinessObjects

+3
 +2
 -1
 +3

INEA
S.A.S.A.
Fecha de Emisión : 2/3/2019
No de Página: 1
4:51:46AM

EXPEDIENTE DEL EDUCANDO

Inst Est: 02 BAJA CALIFORNIA **Coord de Zona :** 11 MEXICALI ORIENTE

HIGUERA REYES ALEJANDRO	RFE	HIRA-800430-4G1
F. Ingreso 28/02/1998	CURP	HIRA800430HSLGYL06
Nacionalidad MÉXICO	Vialidad	AV. ESPARTO NO. 1165
F. Nacimiento 30/04/1980	No.Ext	
Sexo MASCULINO	Asentamiento	VALLE DEL PEDREGAL
Edo Civil CASADO	Teléfono	(686)2-23-96-16
Ocupación AYUDANTE	Ent. Fed	BAJA CALIFORNIA
Hijos 3	Municipio	MEXICALI
Lengua No especificado	Localidad	MEXICALI
Documentos Entregados		

Etapa E.B.: AVANZADO	Modelo: MEVYT	F. Conclusión Nivel: 23/07/2011	Promedio: 9.5							
Subproyecto: INFONAVI	Situación: CONCLUYE NIVEL									
Grado	Módulo/Examen	Calif.	Acred.	F. Calif.	Tip. Eval	F. Aplic.	C.E.	Asesor	I.E.	C.Z.
	EDUCACION PARA LA VIDA LABOR	6	SI	A	EQVL	03/02/2003				
	FRACCIONES Y PORCENTAJES (FO	COM	SI	A	FORM	07/05/2011	20020002	PEREZ GONZALEZ DELIA BERTHA	02	11
	HABLANDO SE ENTIENDE LA GENT	COM	SI	A	FORM	09/04/2011	20020002	PUENTES SOLANO JULIA DOLORES	02	11
	INFORMACION Y GRAFICAS (FORM	COM	SI	A	FORM	09/04/2011	20020002	PUENTES SOLANO JULIA DOLORES	02	11
	LA EDUCACION DE NUESTROS HIJ	COM	SI	L	FORM	23/07/2011	20110002	REYES ESPINO MARIA LUISA	02	11
	MEXICO, NUESTRO HOGAR (FORMA	COM	SI	L	FORM	25/06/2011	20110002	PEREZ GONZALEZ DELIA BERTHA	02	11
	NUESTRO PLANETA, LA TIERRA (COM	SI	A	FORM	04/06/2011	20110002	PEREZ GONZALEZ DELIA BERTHA	02	11
	OPERACIONES AVANZADAS (FORMA	COM	SI	A	FORM	27/05/2011	20110002	PEREZ GONZALEZ DELIA BERTHA	02	11
	PARA SEGUIR APRENDIENDO (FOR	COM	SI	L	FORM	18/06/2011	20110002	PEREZ GONZALEZ DELIA BERTHA	02	11
	SER PADRES, UNA EXPERIENCIA	COM	SI	L	FORM	13/07/2011	20110002	REYES ESPINO MARIA LUISA	02	11
	UN HOGAR SIN VIOLENCIA (FORM	COM	SI	A	FORM	09/06/2011	20110002	PEREZ GONZALEZ DELIA BERTHA	02	11
	VAMOS A ESCRIBIR (FORMATIVA	COM	SI	A	FORM	14/05/2011	20020002	PEREZ GONZALEZ DELIA BERTHA	02	11
1	FRACCIONES Y PORCENTAJES	10	SI	A	FINAL	07/05/2011	20020002	PEREZ GONZALEZ DELIA BERTHA	02	11
1	HABLANDO SE ENTIENDE LA GENT	9	SI	A	FINAL	09/04/2011	20020002	PUENTES SOLANO JULIA DOLORES	02	11
1	INFORMACION Y GRAFICAS	10	SI	A	FINAL	09/04/2011	20020002	PUENTES SOLANO JULIA DOLORES	02	11
	LA EDUC. DE NUESTROS HIJOS E	10	SI	L	FINAL	23/07/2011	20110002	REYES ESPINO MARIA LUISA	02	11



Combined Distribution Management Pty Ltd

T/AS CDM LOGISTICS

ACN: 072 045 802

ABN: 50 072 045 802

Admin Office - PO Box 6264 Wetherill Park NSW 2164

Phone: 02 9773 2400 Fax: 02 9773 2440

email: accounts@cdmlogistics.com.au

WEEKLY TAX INVOICE - 45054 - 1/20/2019 to 1/26/2019

Customer - INTA

INTERTRADING AUSTRALIA P/L
PO BOX 256

NARELLAN NSW 2561

OK

TAX INVOICE

Consignment No.	SY03060225	Invoice Date	1/21/2019
Origin: SMEATON GRANGE	INTERTRADING AUSTRALIA 157 HARTLEY RD SMEATON GRANGE	Pick Up Date	1/21/2019
Destination: KEYSBOROUGH	IMS 4 FIVEWAYS BOULEVARD		
Customer References 224874+			
Rate type	Quantity	Description	Rate
Q	3.00	STANDARD PALLETS	109.0210
L		FUEL LEVY 6.85% 6.85%	327.0600
Net Invoice Amount \$317.69		GST Amount \$31.77	Amount
CIVIPU-4UU08 Advanced Security ↗			\$327.06
			\$22.40

Invoice Total (incl GST) \$349.46

Latest Google Vulnerabilities 2019

- Find Answer Keys
- **filetype:doc "Answer Key"**



filetype:doc "Answer Key"



All Images News Maps Books More Settings Tools

About 158,000 results (0.30 seconds)

[DOC] **Answer Key - Schoolnet**

<https://cleveland.schoolnet.com/Outreach/Content/ServeAttachment.aspx?...id...> ▾

Answer Key. Day 1. 1. C. 2. "The square root of a number is 15" can be represented by the equation .
To find x, students should realize that the inverse operation ...

[DOC] **Answer Key for Exercises**

<https://www.uvm.edu/~dhowell/.../SPSSAnswer%20Key%20for%20Exercises.doc> ▾

Answer Key for Exercises. Exercises-Chapter 1. 1.1 A variety of topics appear under ANOVA. A summary is below. You should look at some of the topics in more ...

[DOC] **Answer Key:**

https://mars.nasa.gov/mer/classroom/marsdial/downloads/Marsdial1_answers.doc ▾

Answer Key: Will the curve be the same throughout the year? Why or why not? The shape of the curve will be the same, but the exact positioning of the curve on ...

[DOC] **answer key - Cengage**

www.cengage.com/resource_uploads/downloads/elt.../0618789677_34117.DOC ▾

ANSWER KEY. TOP 20 STUDENT No answer key required for this exercise. 3. 1 ... NOTE:
Answer key applicable only for first part of each question. 1 ...

Latest Google Vulnerabilities 2019

- I found a lot of servers using SSH .
- intitle:"index of /" ssh

Data you find:

- Webserver Version
- SSH Version
- SSH Keys
- SSH Logins



intitle:"index of /" ssh



All

Images

Videos

News

Maps

More

Settings

Tools

About 38,300 results (0.33 seconds)

Index of /ssh/ccc

www.cs.tau.ac.il/ssh/ccc/ ▾

Index of /ssh/ccc. [ICO], Name · Last modified · Size · Description. [PARENTDIR], Parent Directory, -. [DIR], META-INF/, 2001-06-12 11:59, -. [DIR], mindbright ...

Index of ~/edmund/materials/ssh

enos.itcollege.ee/~edmund/materials/ssh/ ▾

Index of ~/edmund/materials/ssh ... ssh-fingerprint-server-bbd-oldssh.sh, 2018-01-24 12:02, 1.5K. [TXT] ... ssh-fingerprint-server.sh, 2018-01-21 06:37, 1.1K.

Index of /.ssh - Auberge d'Eygliers

auberge-eygliers.com/.ssh/ ▾

Index of /.ssh. Icon Name Last modified Size Description. [PARENTDIR] Parent Directory - [] authorized_keys2 2014-08-04 15:16 397.

Index of /.ssh - Weave Conference 2018

weaveconference.com/.ssh/ ▾

Index of /.ssh. Parent Directory. Apache Server at weaveconference.com Port 80.

Latest Google Vulnerabilities 2019

- Find NVR (Network Video Recorder) login portals.
- "Please click here to download and install the latest plug-in. Close your browser before installation."



"Please click here to download and install the latest plug-in. Close your browser 

All Videos News Shopping Images More Settings Tools

10 results (0.35 seconds)

"Please click here to download and install the latest plug-in. Close ...

<https://www.exploit-db.com/ghdb/5082> ▾

Jan 21, 2019 - Google Dork: "Please click here to download and install the latest plug-in. Close your browser before installation." # Description: Find NVR ...

NVR-ADM4P4

remote.cetechnology.net/ ▾

Please click here to download and install the latest plug-in. Close your browser before installation. Language. 简体中文, English, 繁體中文, にほんご, 한국의 ...

NVR304-32E

212.3.204.54/

Please click here to download and install the latest plug-in. Close your browser before installation. Language. 简体中文, English, 繁體中文, にほんご, 한국의 ...

NVR-ADM8P8

www.cgfaucher.com/ ▾

Please click here to download and install the latest plug-in. Close your browser before installation. Language. 简体中文, English, 繁體中文, にほんご, 한국의 ...

Latest Google Vulnerabilities 2020

- **allintext:"Index Of" "cookies.txt"**

- Show Valuable cookie information

- **inurl:check_mk/login.py**

- Show the login pages of admin

- **intitle:"index of" "ftp.log"**

- Show files that contains FTP logs

Latest Google Vulnerabilities 2021

- **allintext:@gmail.com filetype:log**
 - Show log files that contains emails and passwords
- **"password 7" ext:txt | ext:log | ext:cfg**
 - Show files containing passwords
- **inurl:authorization.ping**
 - Pages containing portals for login or employee account recovery

Google, Friend or Enemy?

- Google, Friend or Enemy?
- Google is everyone's best friend (yours or hackers)
- Information gathering and vulnerability identification are the tasks in the first phase of a typical hacking scenario
- Google can do more than search
- Have you used Google to audit your organization today?

Lecture 3

User Authentication

CMPU-4008

Advance Security 2

RFC 4949

RFC 4949 defines user authentication as:

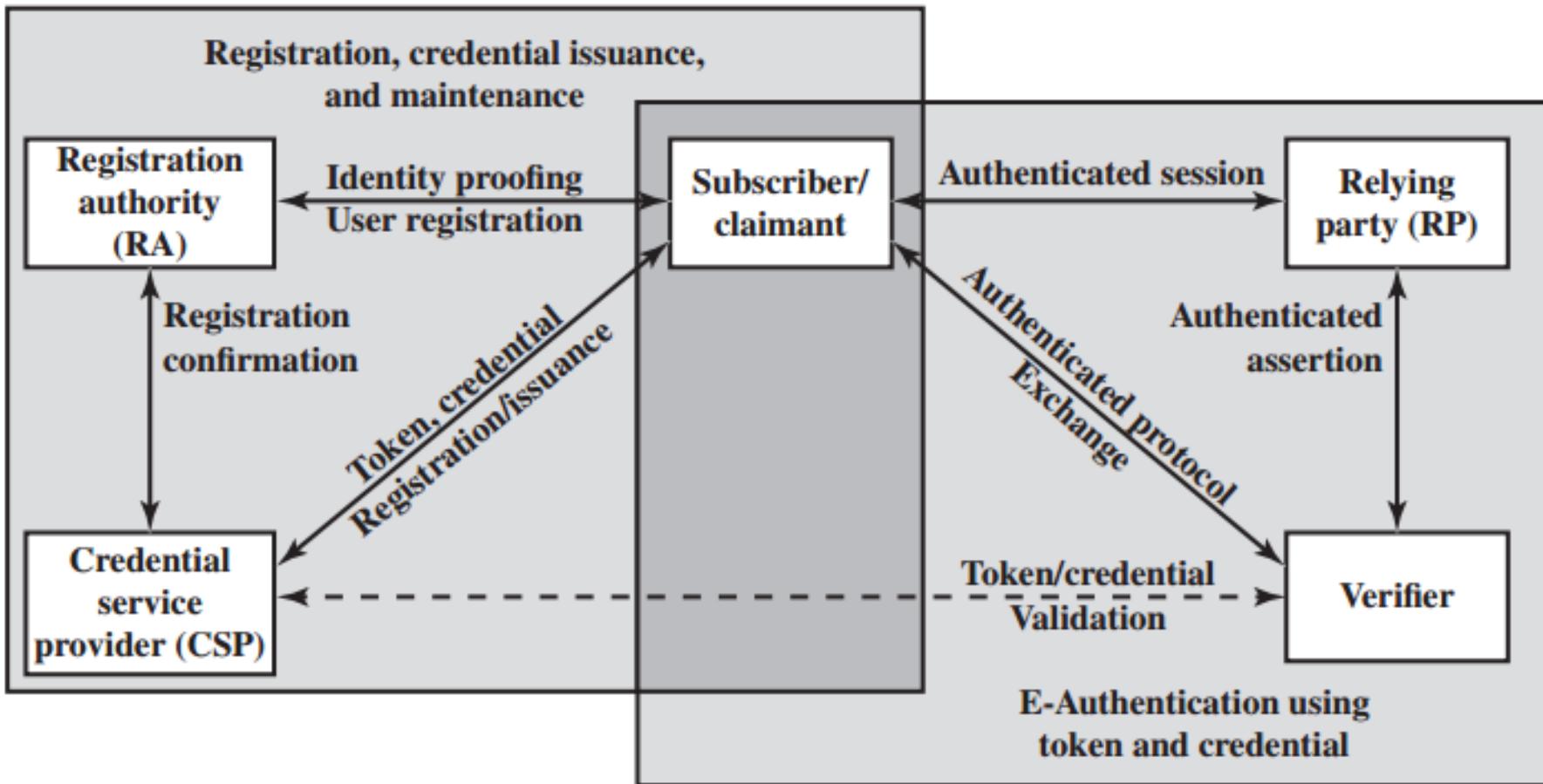
“The process of verifying an identity claimed by or for a system entity.”



Authentication Process

- Fundamental building block and primary line of defense
- Basis for access control and user accountability
- Identification step
 - Presenting an identifier to the security system
- Verification step
 - Presenting or generating authentication information that corroborates the binding between the entity and the identifier





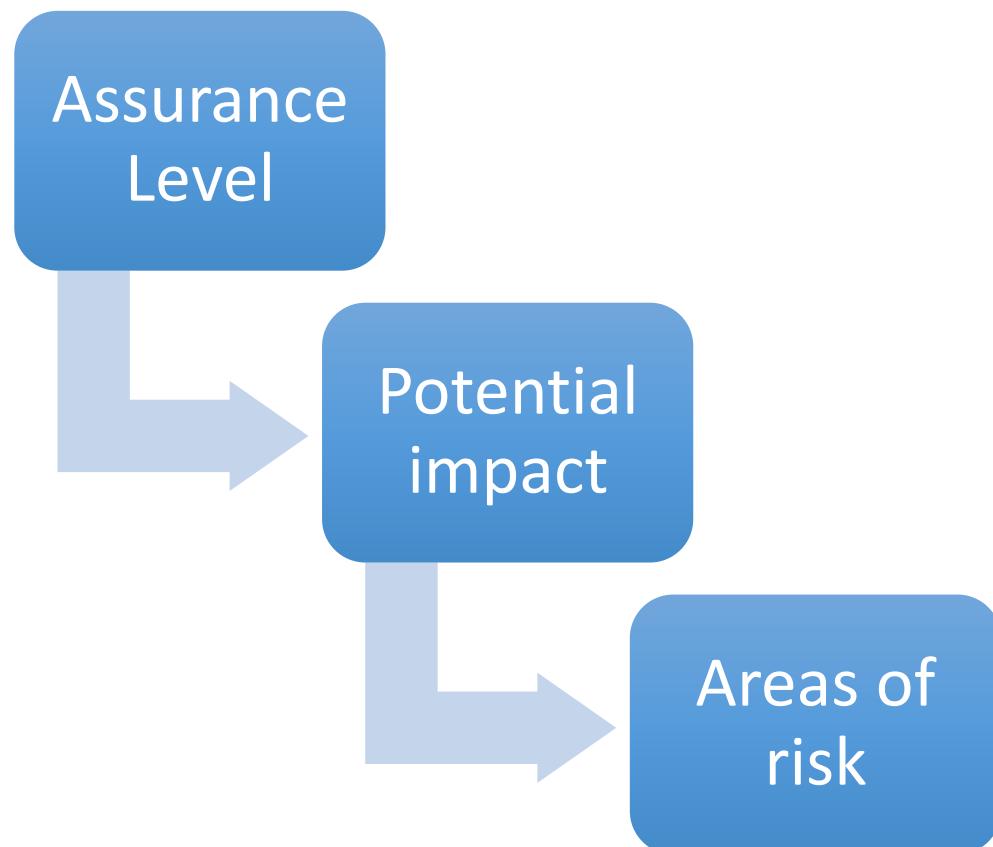
The NIST SP 800-63-2 E-Authentication Architectural Model

The four means of authenticating user identity are based on:

Something the individual knows	Something the individual possesses (token)	Something the individual is (static biometrics)	Something the individual does (dynamic biometrics)
<ul style="list-style-type: none">• Password, PIN, answers to prearranged questions	<ul style="list-style-type: none">• Smartcard, electronic keycard, physical key	<ul style="list-style-type: none">• Fingerprint, retina, face	<ul style="list-style-type: none">• Voice pattern, handwriting, typing rhythm

Risk Assessment for User Authentication

- There are three separate concepts:



Assurance Level

Describes an organization's degree of certainty that a user has presented a credential that refers to his or her identity

More specifically is defined as:

The degree of confidence in the vetting process used to establish the identity of the individual to whom the credential was issued

The degree of confidence that the individual who uses the credential is the individual to whom the credential was issued

Four levels of assurance

Level 1

- Little or no confidence in the asserted identity's validity

Level 2

- Some confidence in the asserted identity's validity

Level 3

- High confidence in the asserted identity's validity

Level 4

- Very high confidence in the asserted identity's validity

Potential Impact

- FIPS 199 defines three levels of potential impact on organizations or individuals should there be a breach of security:
 - Low
 - An authentication error could be expected to have a limited adverse effect on organizational operations, organizational assets, or individuals
 - Moderate
 - An authentication error could be expected to have a serious adverse effect
 - High
 - An authentication error could be expected to have a severe or catastrophic adverse effect

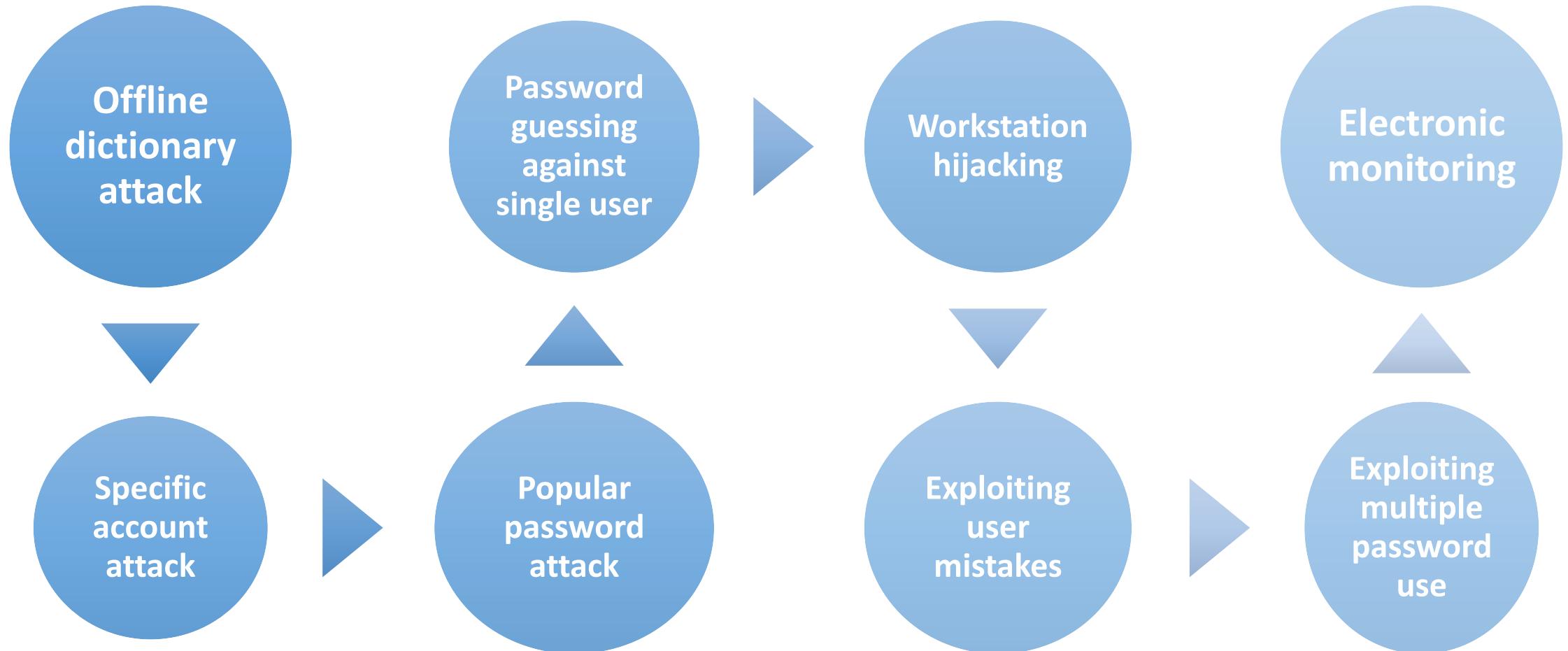
Maximum Potential Impacts for Each Assurance Level

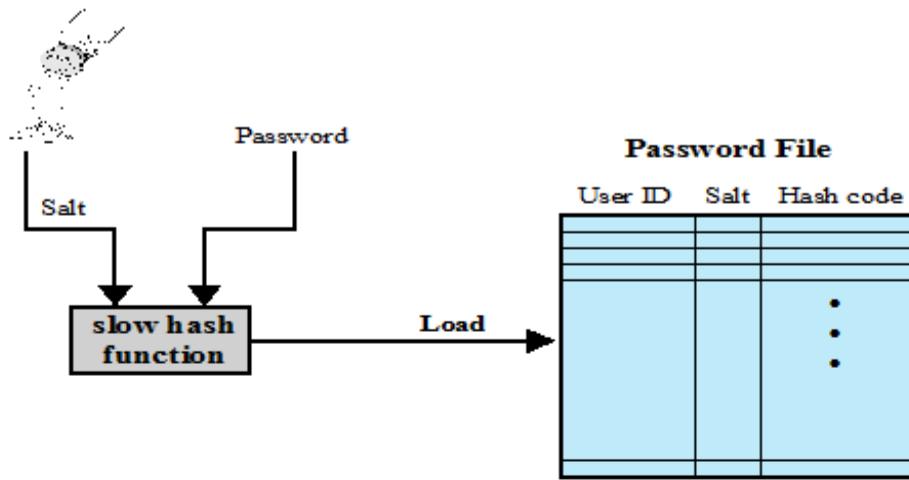
Potential Impact Categories for Authentication Errors	Assurance Level Impact Profiles			
	1	2	3	4
Inconvenience, distress, or damage to standing or reputation	Low	Mod	Mod	High
Financial loss or organization liability	Low	Mod	Mod	High
Harm to organization programs or interests	None	Low	Mod	High
Unauthorized release of sensitive information	None	Low	Mod	High
Personal safety	None	None	Low	Mod/ High
Civil or criminal violations	None	Low	Mod	High

Password Authentication

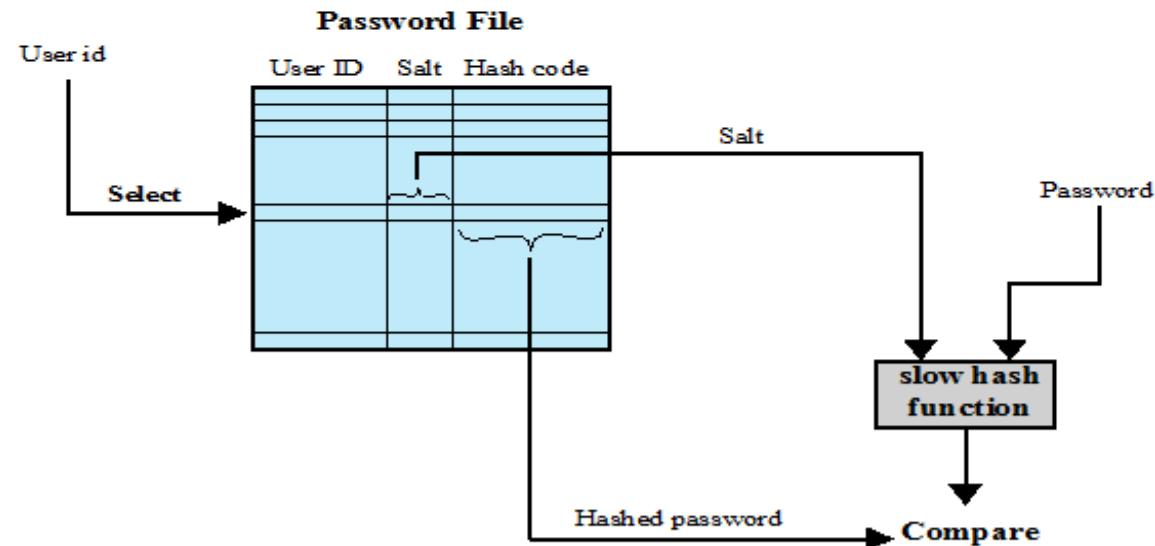
- Widely used line of defense against intruders
 - User provides name/login and password
 - System compares password with the one stored for that specified login
- The user ID:
 - Determines that the user is authorized to access the system
 - Determines the user's privileges
 - Is used in discretionary access control

Password Vulnerabilities





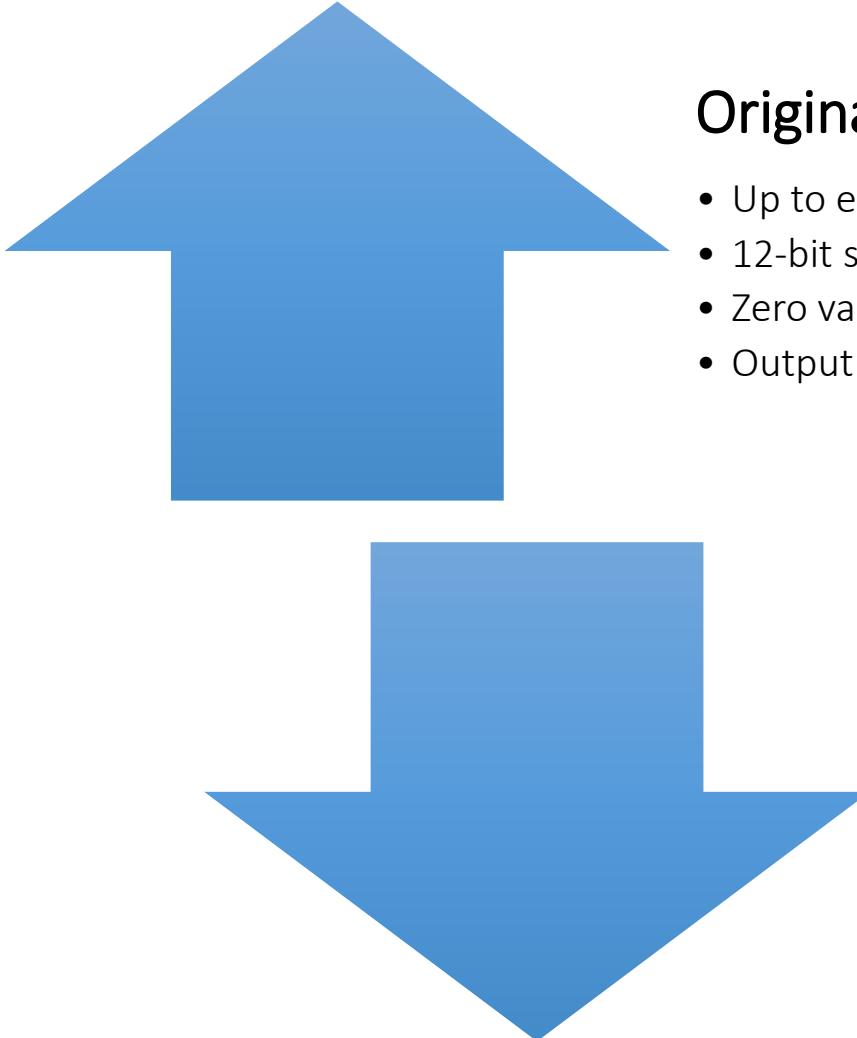
(a) Loading a new password



(b) Verifying a password

UNIX Password Scheme

UNIX Implementation



Original scheme

- Up to eight printable characters in length
- 12-bit salt used to modify DES encryption into a one-way hash function
- Zero value repeatedly encrypted 25 times
- Output translated to 11 character sequence

Now regarded as inadequate

- Still often required for compatibility with existing account management software or multivendor environments

Improved Implementations

Much stronger hash/salt schemes available for Unix

OpenBSD uses Blowfish block cipher based hash algorithm called Bcrypt

- Most secure version of Unix hash/salt scheme
- Uses 128-bit salt to create 192-bit hash value

Recommended hash function is based on MD5

- Salt of up to 48-bits
- Password length is unlimited
- Produces 128-bit hash
- Uses an inner loop with 1000 iterations to achieve slowdown

Password Cracking

Dictionary attacks

- Develop a large dictionary of possible passwords and try each against the password file
- Each password must be hashed using each salt value and then compared to stored hash values

Rainbow table attacks

- Pre-compute tables of hash values for all salts
- A mammoth table of hash values
- Can be countered by using a sufficiently large salt value and a sufficiently large hash length

Password crackers exploit the fact that people choose easily guessable passwords

- Shorter password lengths are also easier to crack

John the Ripper

- Open-source password cracker first developed in 1996
- Uses a combination of brute-force and dictionary techniques

Modern Approaches

- **Complex password policy**
 - Forcing users to pick stronger passwords
- **However password-cracking techniques have also improved**
 - The processing capacity available for password cracking has increased dramatically
 - The use of sophisticated algorithms to generate potential passwords
 - Studying examples and structures of actual passwords in use

Password File Access Control

Can block offline guessing attacks by denying access to encrypted passwords

Make available only to privileged users

Shadow password file

Vulnerabilities

Weakness in the OS that allows access to the file

Accident with permissions making it readable

Users with same password on other systems

Access from backup media

Sniff passwords in network traffic



Password Selection Strategies

User education

Users can be told the importance of using hard to guess passwords and can be provided with guidelines for selecting strong passwords



Computer generated passwords

Users have trouble remembering them



Reactive password checking

System periodically runs its own password cracker to find guessable passwords

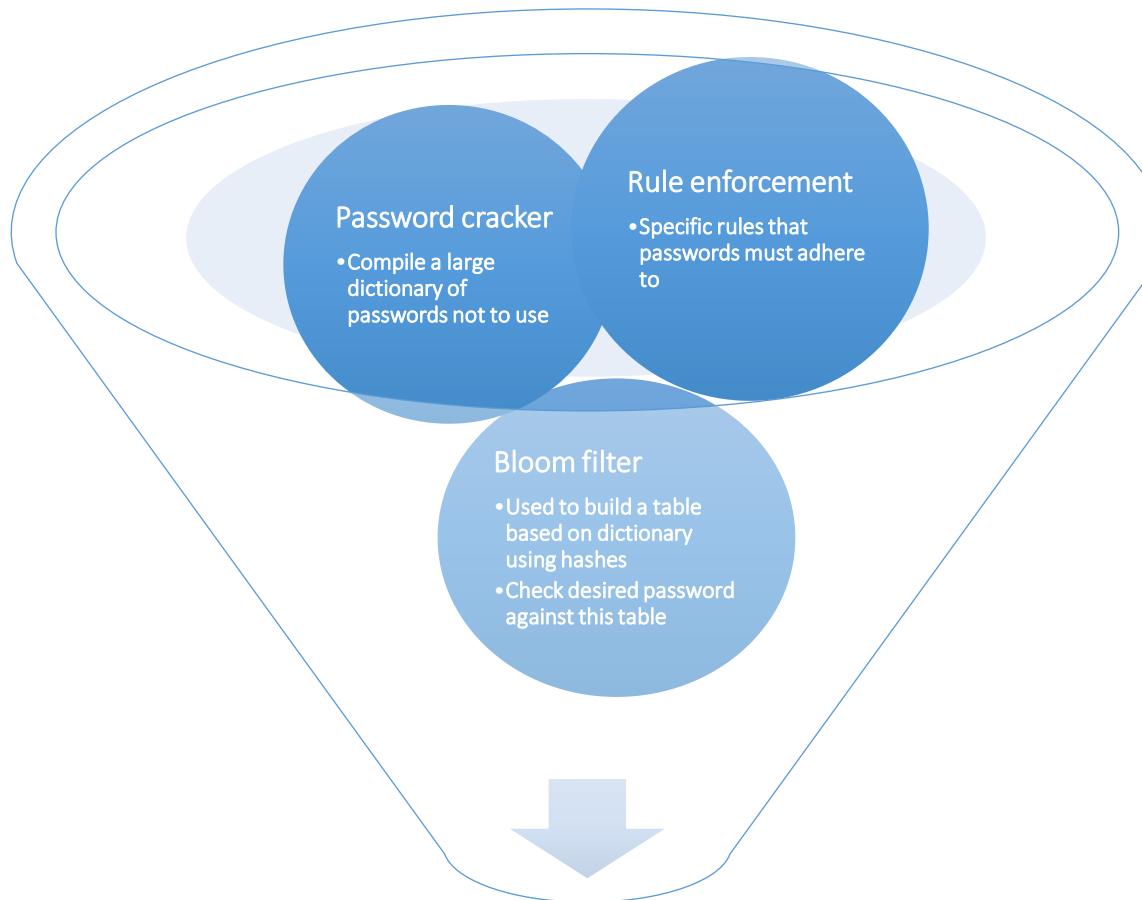


Complex password policy

User is allowed to select their own password, however the system checks to see if the password is allowable, and if not, rejects it

Goal is to eliminate guessable passwords while allowing the user to select a password that is memorable

Proactive Password Checking



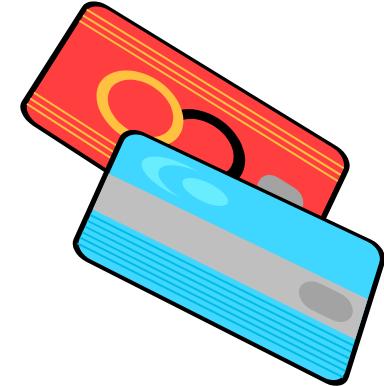
Token Based Authentication

Types of Cards Used as Tokens

Card Type	Defining Feature	Example
Embossed	Raised characters only, on front	Old credit card
Magnetic stripe	Magnetic bar on back, characters on front	Bank card
Memory	Electronic memory inside	Prepaid phone card
Smart Contact Contactless	Electronic memory and processor inside Electrical contacts exposed on surface Radio antenna embedded inside	Biometric ID card

Memory Cards

- Can store but do not process data
- The most common is the magnetic stripe card
- Can include an internal electronic memory
- Can be used alone for physical access
 - Hotel room
 - ATM
- Provides significantly greater security when combined with a password or PIN
- Drawbacks of memory cards include:
 - Requires a special reader
 - Loss of token
 - User dissatisfaction



Smart Tokens

- Physical characteristics:
 - Include an embedded microprocessor
 - A smart token that looks like a bank card
 - Can look like calculators, keys, small portable objects
- Interface:
 - Manual interfaces include a keypad and display for interaction
 - Electronic interfaces communicate with a compatible reader/writer
- Authentication protocol:
 - Classified into three categories:
 - Static
 - Dynamic password generator
 - Challenge-response



Smart Cards

- **Most important category of smart token**
 - Has the appearance of a credit card
 - Has an electronic interface
 - May use any of the smart token protocols
- **Contain:**
 - An entire microprocessor
 - Processor
 - Memory
 - I/O ports
- **Typically include three types of memory:**
 - Read-only memory (ROM)
 - Stores data that does not change during the card's life
 - Electrically erasable programmable ROM (EEPROM)
 - Holds application data and programs
 - Random access memory (RAM)
 - Holds temporary data generated when applications are executed

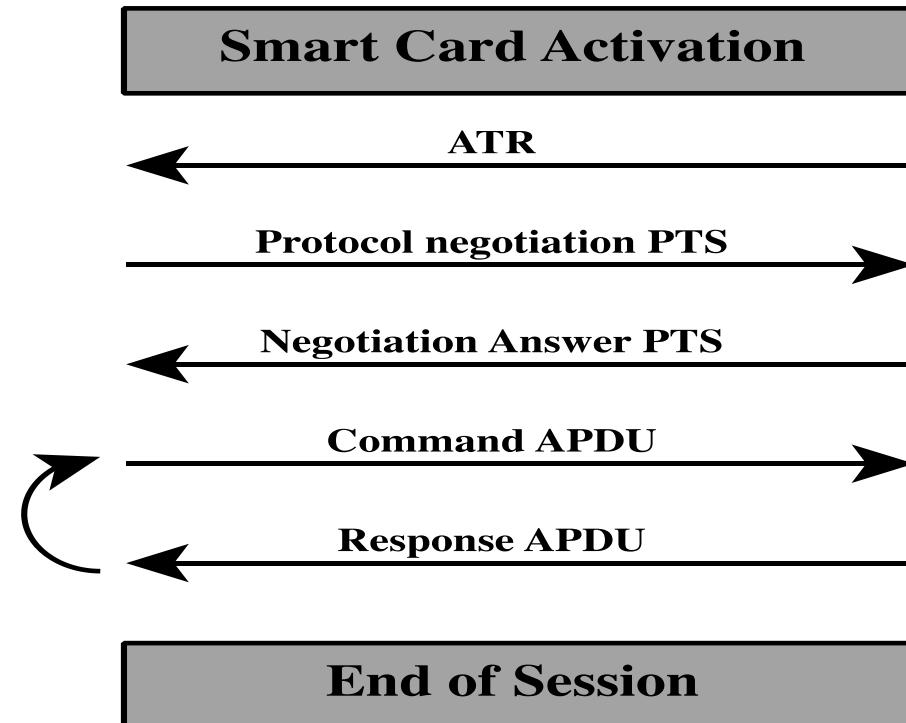




Smart card



Card reader



APDU = application protocol data unit

ATR = Answer to reset

PTS = Protocol type selection

Figure 3.5 Smart Card/Reader Exchange

Electronic Identity Cards (eID)

Use of a smart card as a national identity card for citizens

Most advanced deployment is the German card *neuer Personalausweis*

Can serve the same purposes as other national ID cards, and similar cards such as a driver's license, for access to government and commercial services

Has human-readable data printed on its surface

- Personal data
- Document number
- Card access number (CAN)
- Machine readable zone (MRZ)

Can provide stronger proof of identity and can be used in a wider variety of applications

In effect, is a smart card that has been verified by the national government as valid and authentic



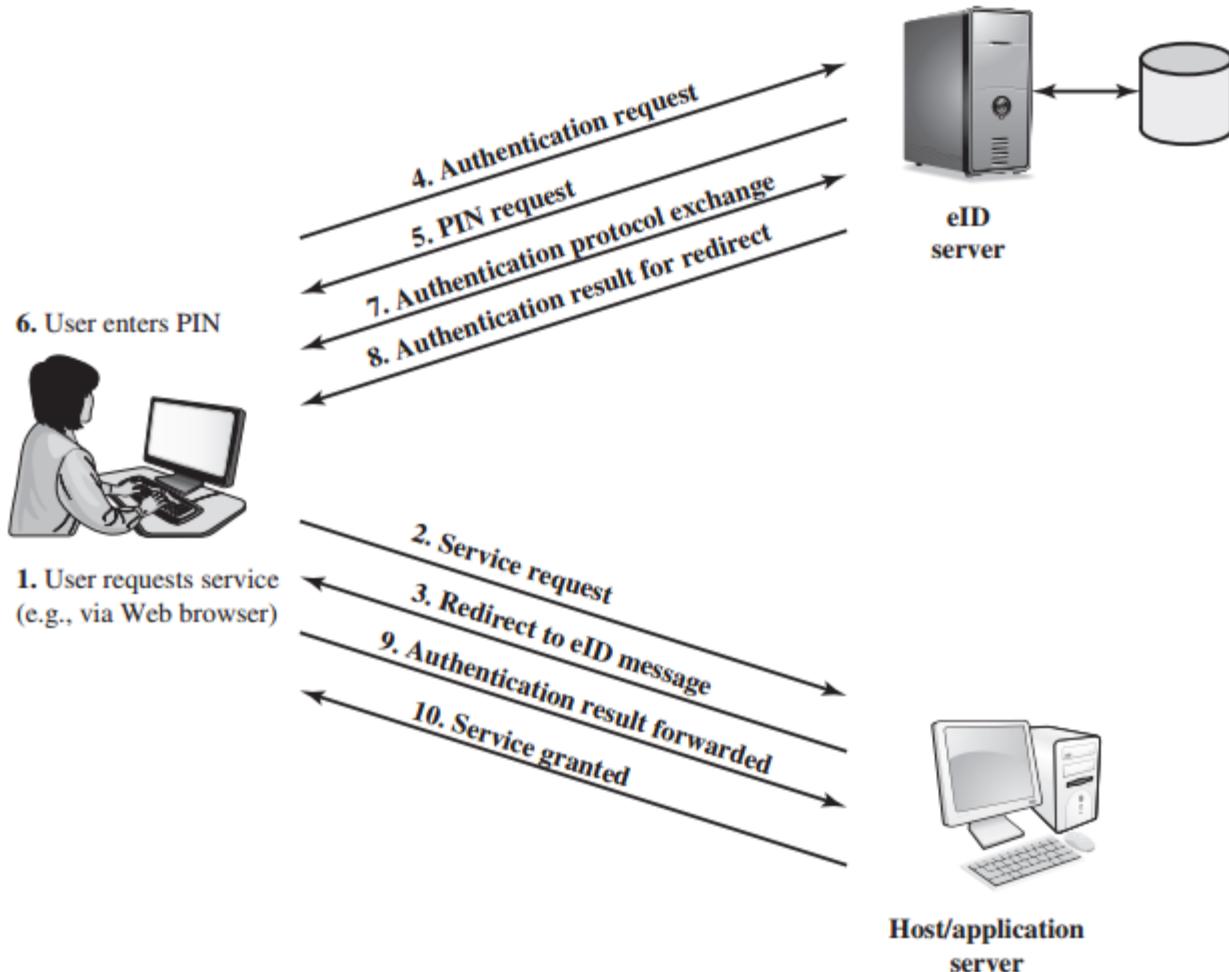
Function	Purpose	PACE Password	Data	Uses
ePass (mandatory)	Authorized offline inspection systems read the data	CAN or MRZ	Face image; two fingerprint images (optional), MRZ data	Offline biometric identity verification reserved for government access
eID (activation optional)	Online applications read the data or access functions as authorized	eID PIN	Family and given names; artistic name and doctoral degree; date and place of birth; address and community ID; expiration date	Identification; age verification; community ID verification; restricted identification (pseudonym); revocation query
	Offline inspection systems read the data and update the address and community ID	CAN or MRZ		
eSign (certificate optional)	A certification authority installs the signature certificate online	eID PIN	Signature key; X.509 certificate	Electronic signature creation
	Citizens make electronic signature with eSign PIN	CAN		

CAN = card access number

MRZ = machine readable zone

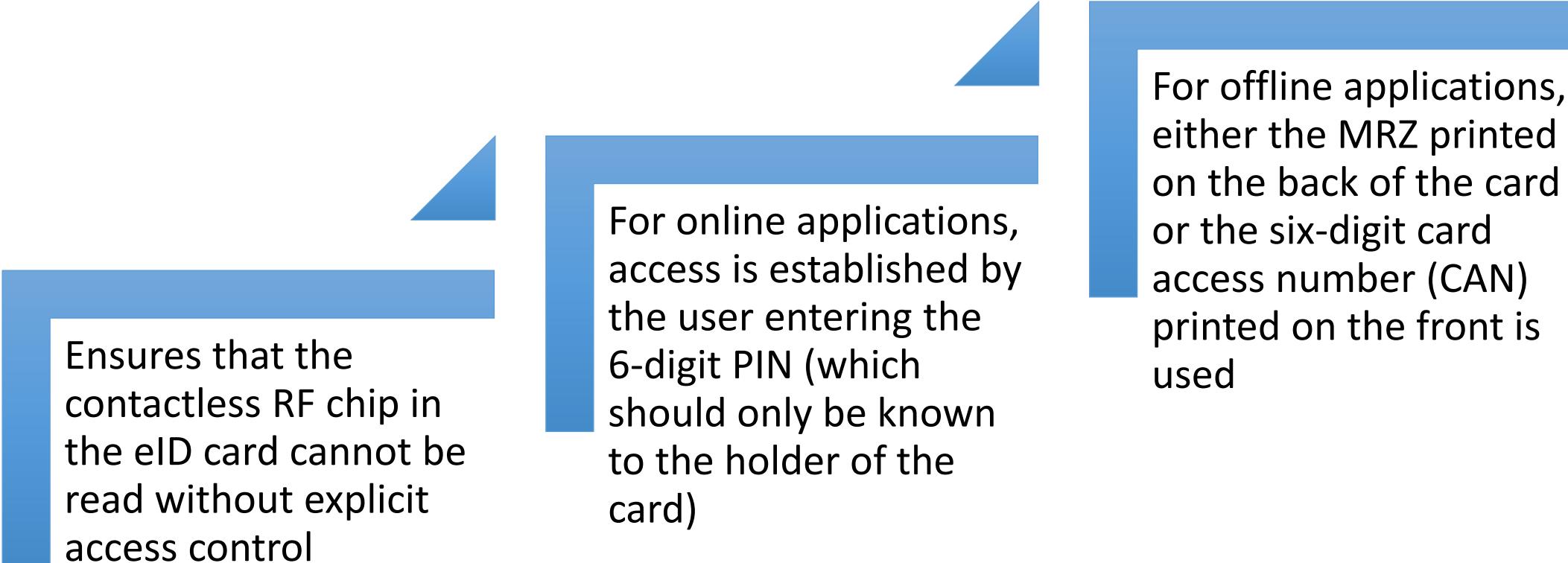
PACE = password authenticated connection establishment

PIN = personal identification number



User Authentication with eID

Password Authenticated Connection Establishment (PACE)



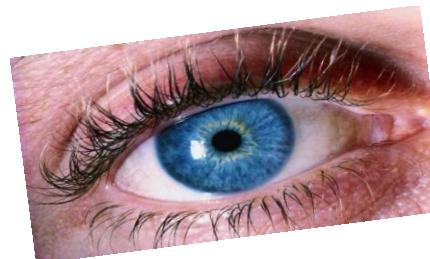
Ensures that the contactless RF chip in the eID card cannot be read without explicit access control

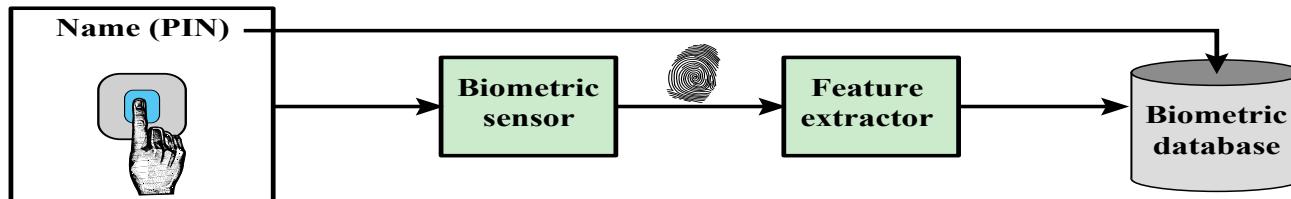
For online applications, access is established by the user entering the 6-digit PIN (which should only be known to the holder of the card)

For offline applications, either the MRZ printed on the back of the card or the six-digit card access number (CAN) printed on the front is used

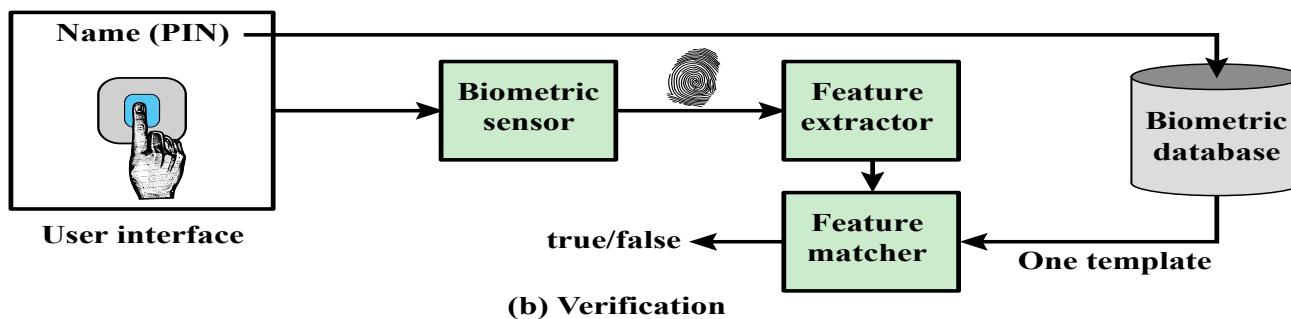
Biometric Authentication

- Attempts to authenticate an individual based on unique physical characteristics
- Based on pattern recognition
- Is technically complex and expensive when compared to passwords and tokens
- Physical characteristics used include:
 - Facial characteristics
 - Fingerprints
 - Hand geometry
 - Retinal pattern
 - Iris
 - Signature
 - Voice

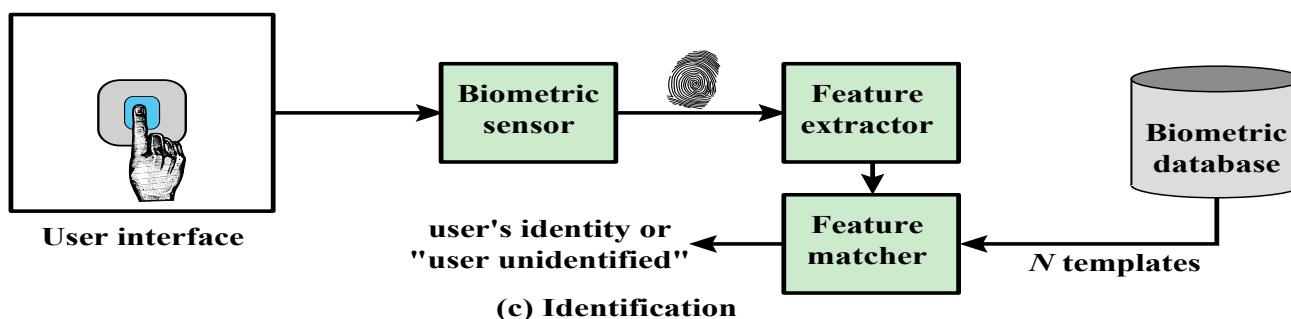




(a) Enrollment



(b) Verification



(c) Identification

Figure 3.8 A Generic Biometric System. Enrollment creates an association between a user and the user's biometric characteristics. Depending on the application, user authentication either involves verifying that a claimed user is the actual user or identifying an unknown user.

Remote User Authentication

- Authentication over a network, the Internet, or a communications link is more complex
- Additional security threats such as:
 - Eavesdropping, capturing a password, replaying an authentication sequence that has been observed
- Generally rely on some form of a challenge-response protocol to counter threats



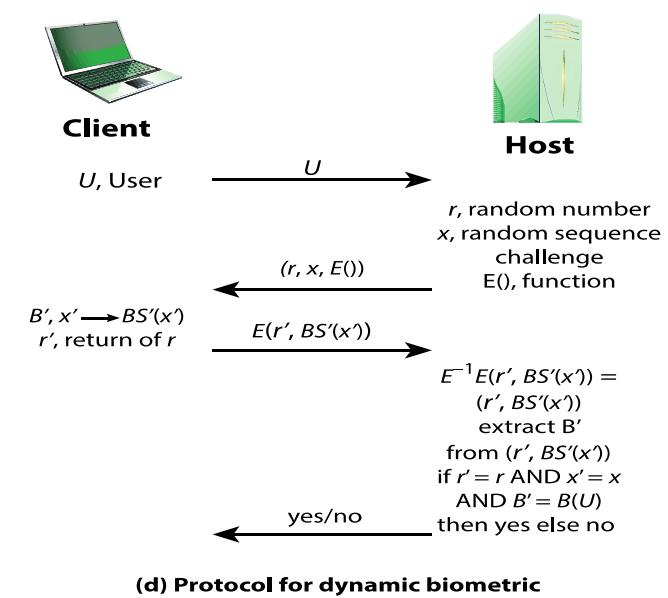
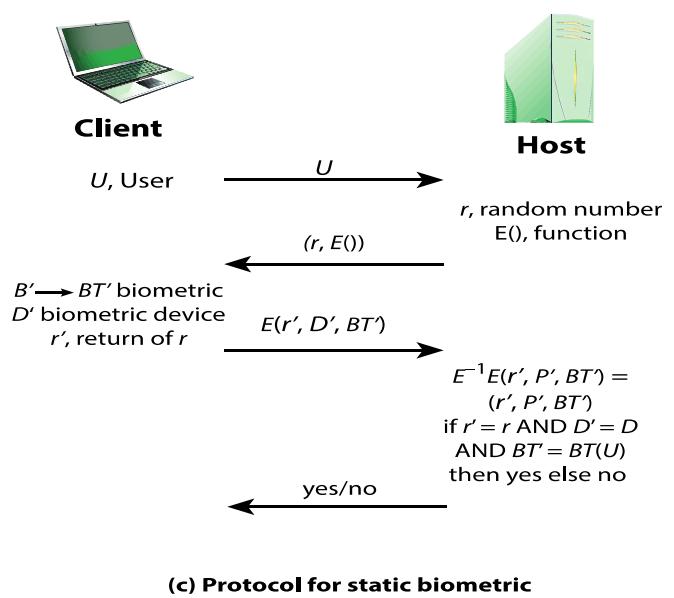
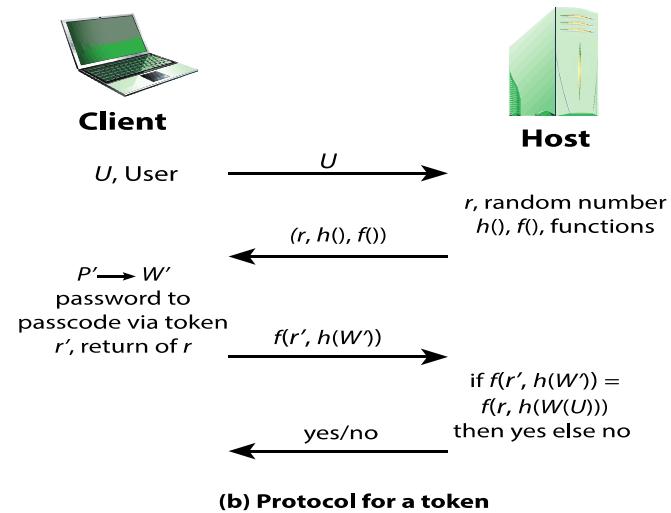
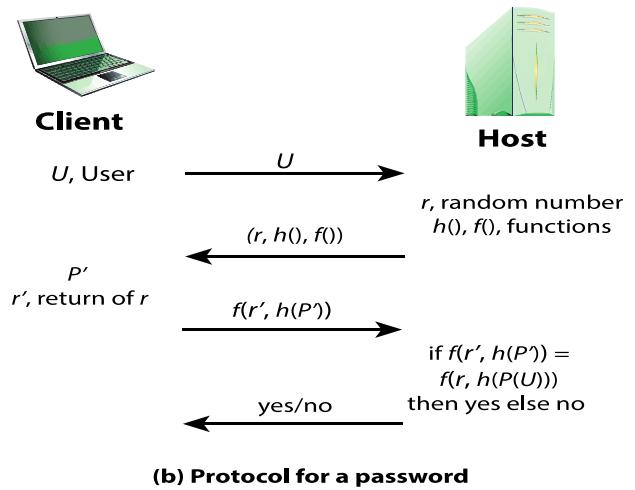


Figure 3.12 Basic Challenge-Response Protocols for Remote User Authentication

Attacks	Authenticators	Examples	Typical defenses
Client attack	Password	Guessing, exhaustive search	Large entropy; limited attempts
	Token	Exhaustive search	Large entropy; limited attempts, theft of object requires presence
	Biometric	False match	Large entropy; limited attempts
Host attack	Password	Plaintext theft, dictionary/exhaustive search	Hashing; large entropy; protection of password database
	Token	Passcode theft	Same as password; 1-time passcode
	Biometric	Template theft	Capture device authentication; challenge response
Eavesdropping, theft, and copying	Password	"Shoulder surfing"	User diligence to keep secret; administrator diligence to quickly revoke compromised passwords; multifactor authentication
	Token	Theft, counterfeiting hardware	Multifactor authentication; tamper resistant/evident token
	Biometric	Copying (spoofing) biometric	Copy detection at capture device and capture device authentication
Replay	Password	Replay stolen password response	Challenge-response protocol
	Token	Replay stolen passcode response	Challenge-response protocol; 1-time passcode
	Biometric	Replay stolen biometric template response	Copy detection at capture device and capture device authentication via challenge-response protocol
Trojan horse	Password, token, biometric	Installation of rogue client or capture device	Authentication of client or capture device within trusted security perimeter

Authentication Security Issues

Denial-of-Service

Attempts to disable a user authentication service by flooding the service with numerous authentication attempts

Eavesdropping

Adversary attempts to learn the password by some sort of attack that involves the physical proximity of user and adversary

Host Attacks

Directed at the user file at the host where passwords, token passcodes, or biometric templates are stored

Trojan Horse

An application or physical device masquerades as an authentic application or device for the purpose of capturing a user password, passcode, or biometric

Client Attacks

Adversary attempts to achieve user authentication without access to the remote host or the intervening communications path

Replay

Adversary repeats a previously captured user response

Lecture 4

Access Control

CMPU-4008

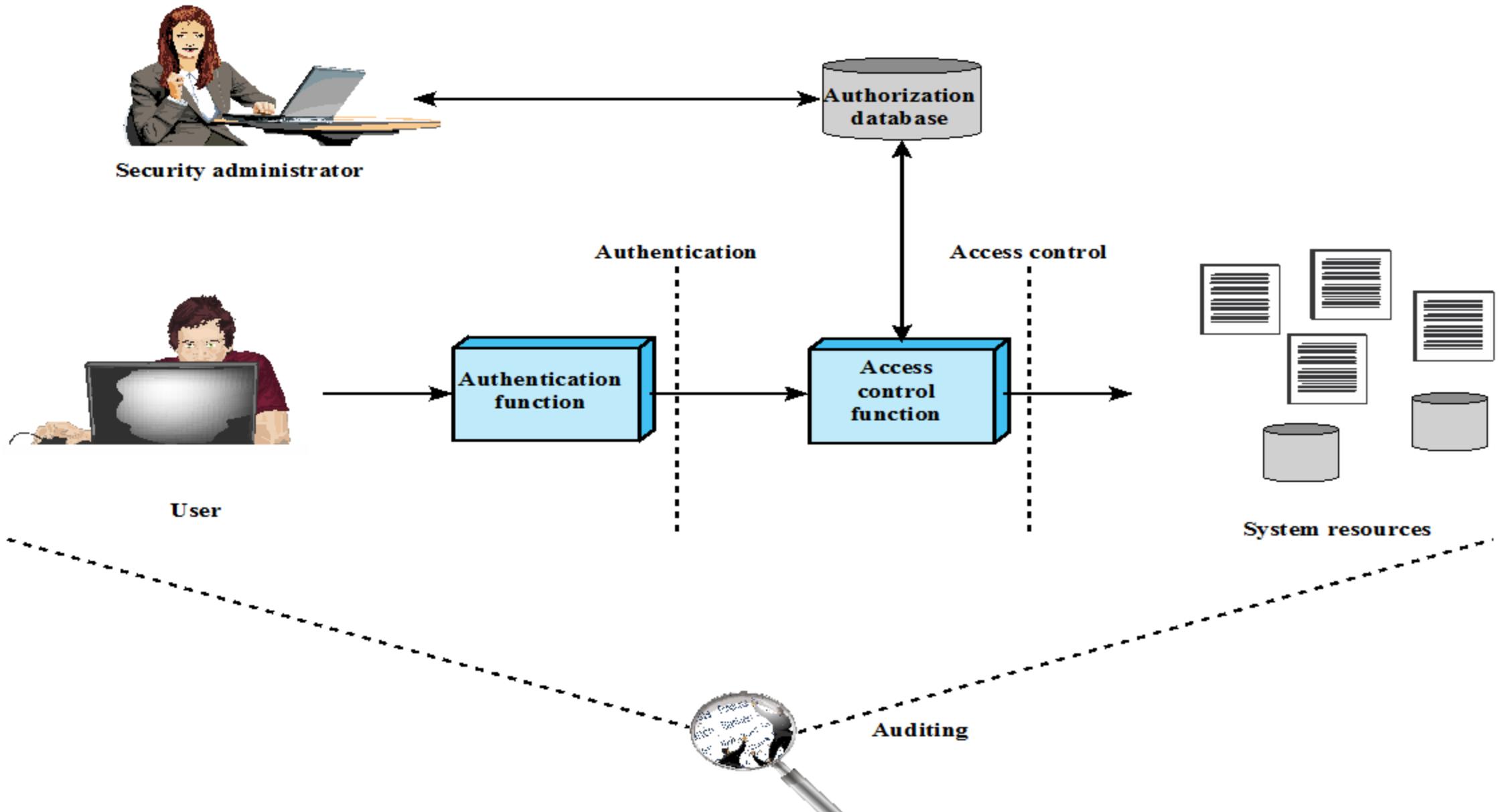
Advance Security 2

Access Control Principles

RFC 4949 defines computer security as:

“Measures that implement and assure security services in a computer system, particularly those that assure access control service.”





Relationship Among Access Control and Other Security Functions

Access Control Policies

- Discretionary access control (DAC)
 - Controls access based on the identity of the requestor and on access rules (authorizations) stating what requestors are (or are not) allowed to do
- Mandatory access control (MAC)
 - Controls access based on comparing security labels with security clearances
- Role-based access control (RBAC)
 - Controls access based on the roles that users have within the system and on rules stating what accesses are allowed to users in given roles
- Attribute-based access control (ABAC)
 - Controls access based on attributes of the user, the resource to be accessed, and current environmental conditions

Subjects, Objects, and Access Rights

Subject

An entity capable of accessing objects

- Three classes
- Owner
 - Group
 - World

Object

A resource to which access is controlled

Entity used to contain and/or receive information

Access right

Describes the way in which a subject may access an object

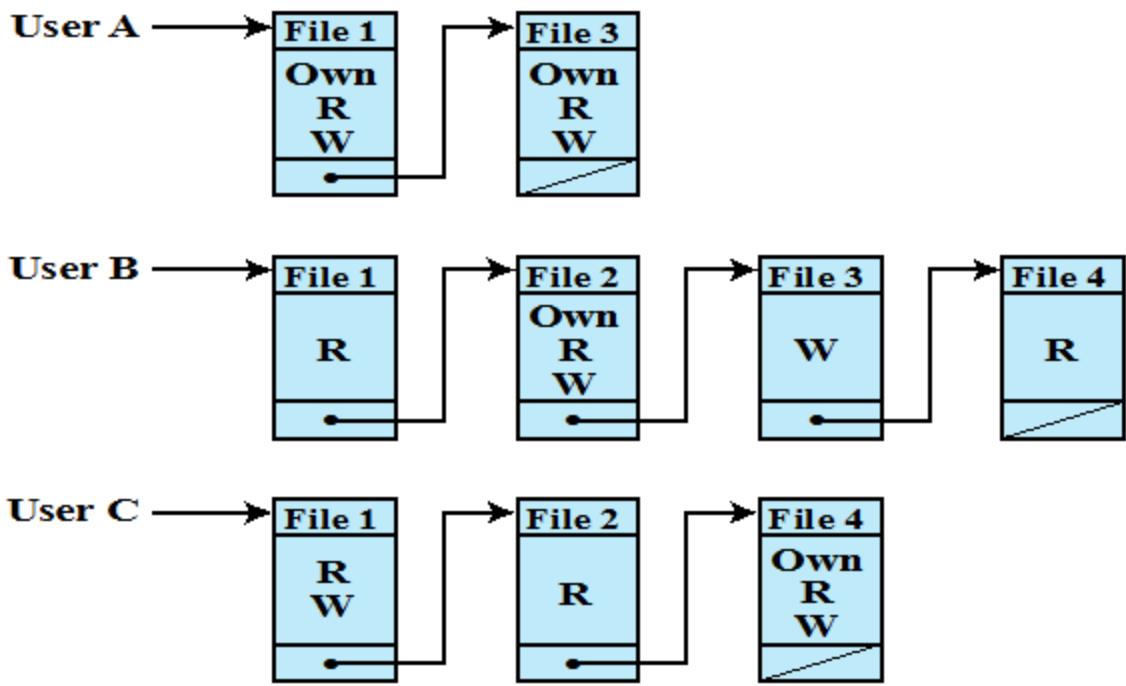
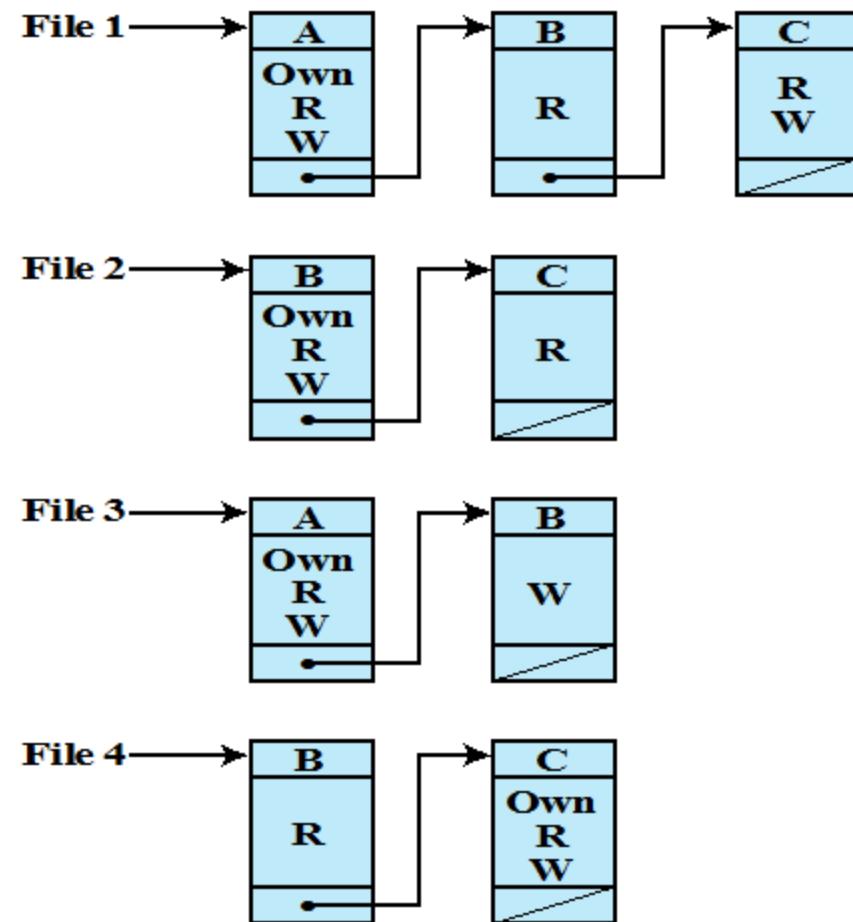
- Could include:
- Read
 - Write
 - Execute
 - Delete
 - Create
 - Search

Discretionary Access Control (DAC)

- Scheme in which an entity may enable another entity to access some resource
- Often provided using an access matrix
 - One dimension consists of identified subjects that may attempt data access to the resources
 - The other dimension lists the objects that may be accessed
- Each entry in the matrix indicates the access rights of a particular subject for a particular object

		OBJECTS			
		File 1	File 2	File 3	File 4
SUBJECTS	User A	Own Read Write		Own Read Write	
	User B	Read	Own Read Write	Write	Read
	User C	Read Write	Read		Own Read Write

(a) Access matrix



Example of Access Control Structures

Authorization Table for Files

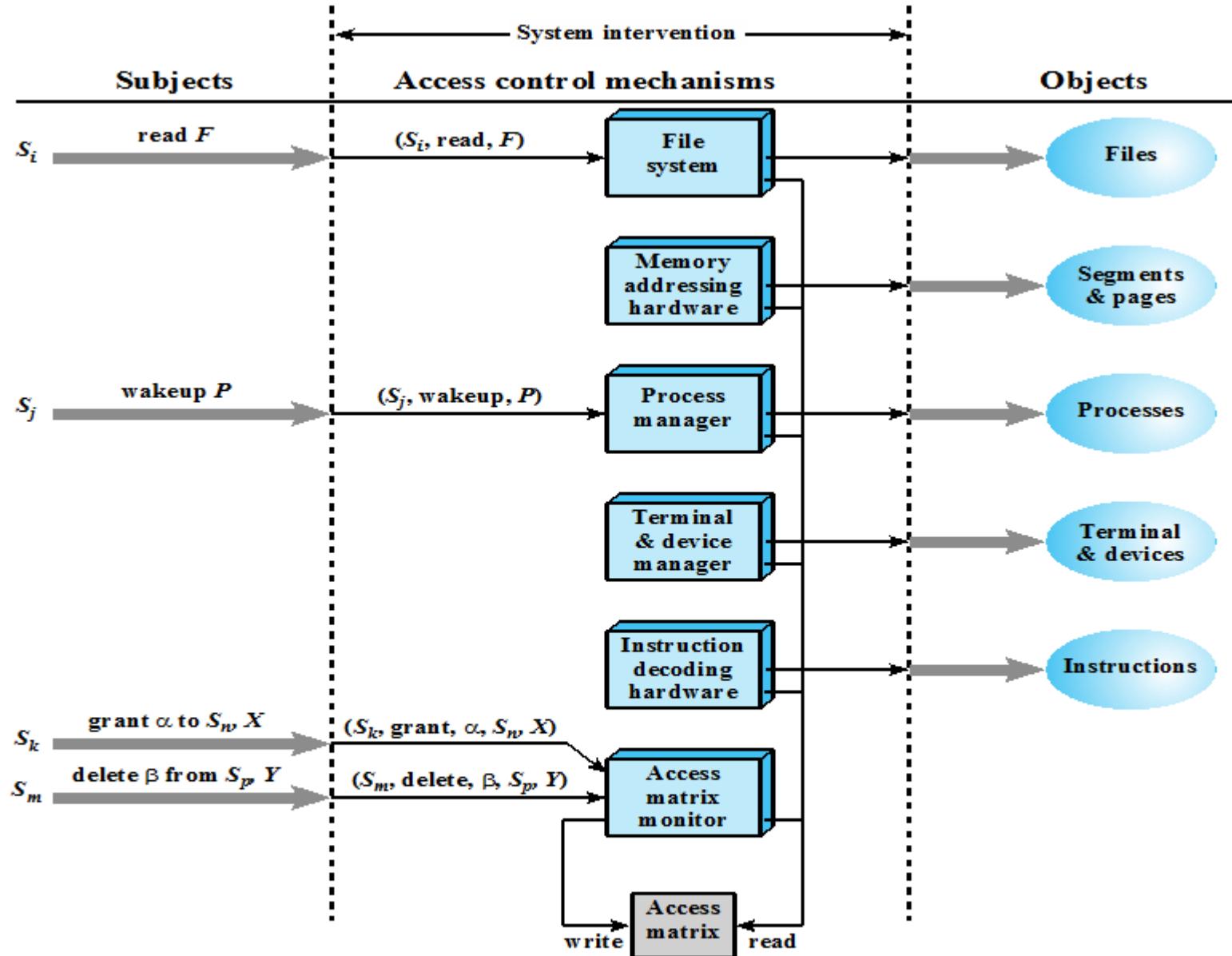
Subject	Access Mode	Object
A	Own	File 1
	Read	File 1
	Write	File 1
A	Own	File 3
	Read	File 3
	Write	File 3
B	Read	File 1
B	Own	File 2
	Read	File 2
	Write	File 2
B	Write	File 3
	Read	File 4
C	Read	File 1
C	Write	File 1
	Read	File 2
	Own	File 4
C	Read	File 4
	Write	File 4

OBJECTS

		subjects			files		processes		disk drives	
		S ₁	S ₂	S ₃	F ₁	F ₂	P ₁	P ₂	D ₁	D ₂
SUBJECTS	S ₁	control	owner	owner control	read *	read owner	wakeup	wakeup	seek	owner
	S ₂		control		write *	execute			owner	seek *
	S ₃			control		write	stop			

* – copy flag set

Extended Access Control Matrix



An Organization of the Access Control Function

UNIX File Access Control

UNIX files are administered using inodes (index nodes)

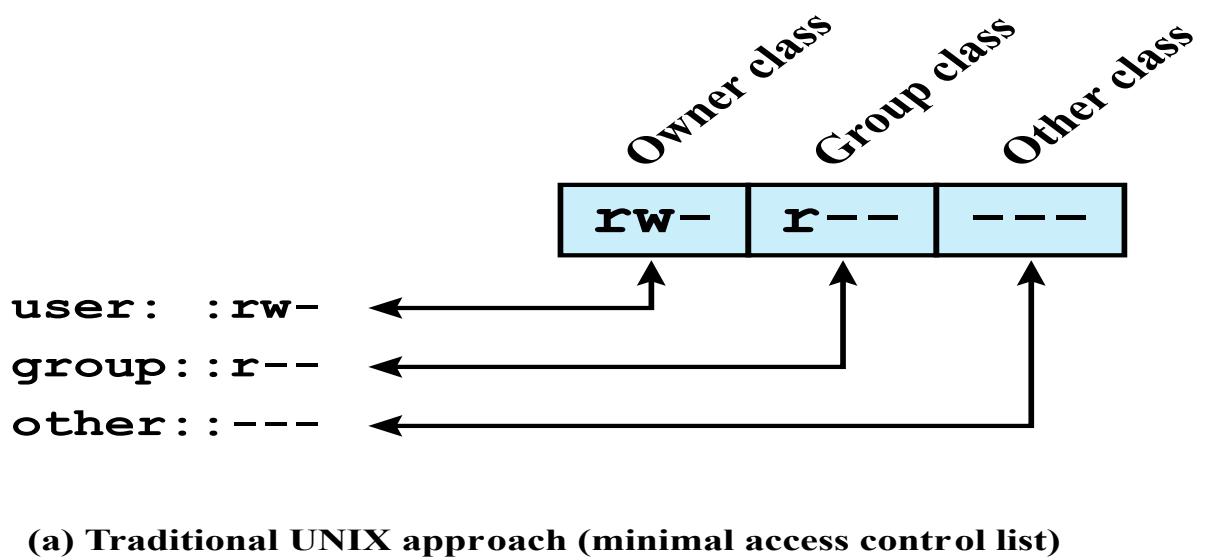
- Control structures with key information needed for a particular file
- Several file names may be associated with a single inode
- An active inode is associated with exactly one file
- File attributes, permissions and control information are sorted in the inode
- On the disk there is an inode table, or inode list, that contains the inodes of all the files in the file system
- When a file is opened its inode is brought into main memory and stored in a memory resident inode table

Directories are structured in a hierarchical tree

- May contain files and/or other directories
- Contains file names plus pointers to associated inodes

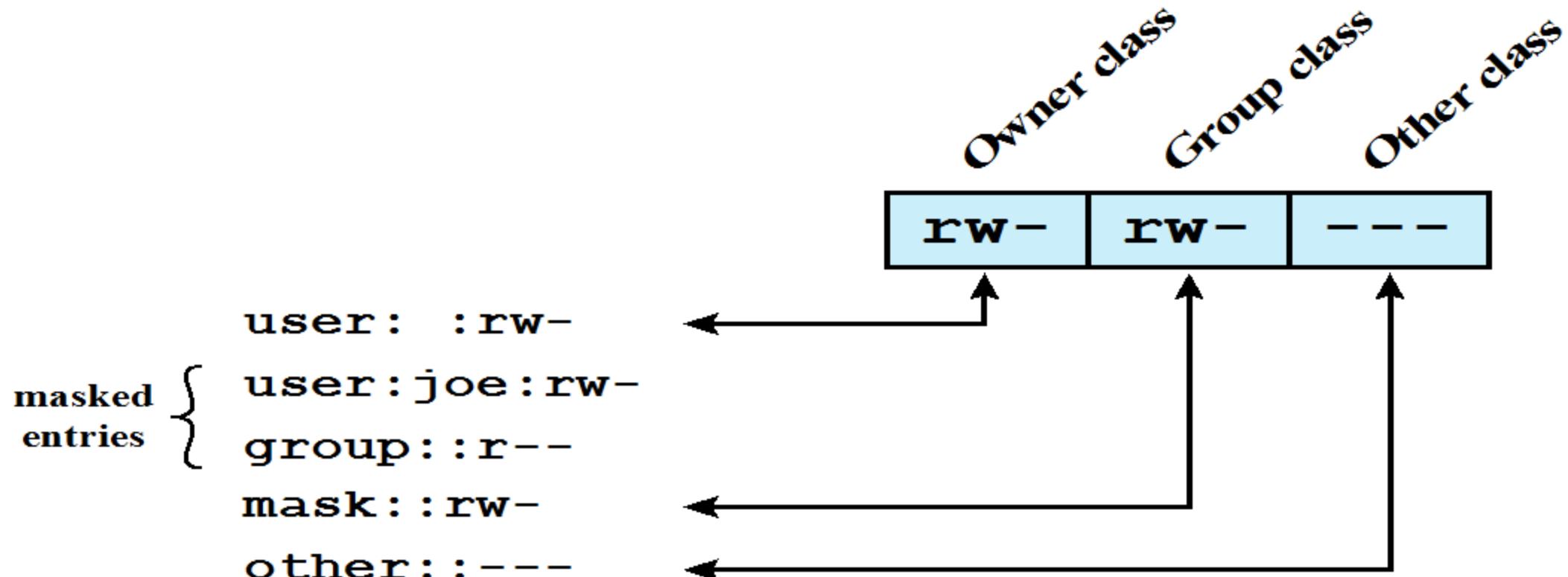
UNIX File Access Control

- Unique user identification number (user ID)
- Member of a primary group identified by a group ID
- Belongs to a specific group
- 12 protection bits
 - Specify read, write, and execute permission for the owner of the file, members of the group and all other users
- The owner ID, group ID, and protection bits are part of the file's inode



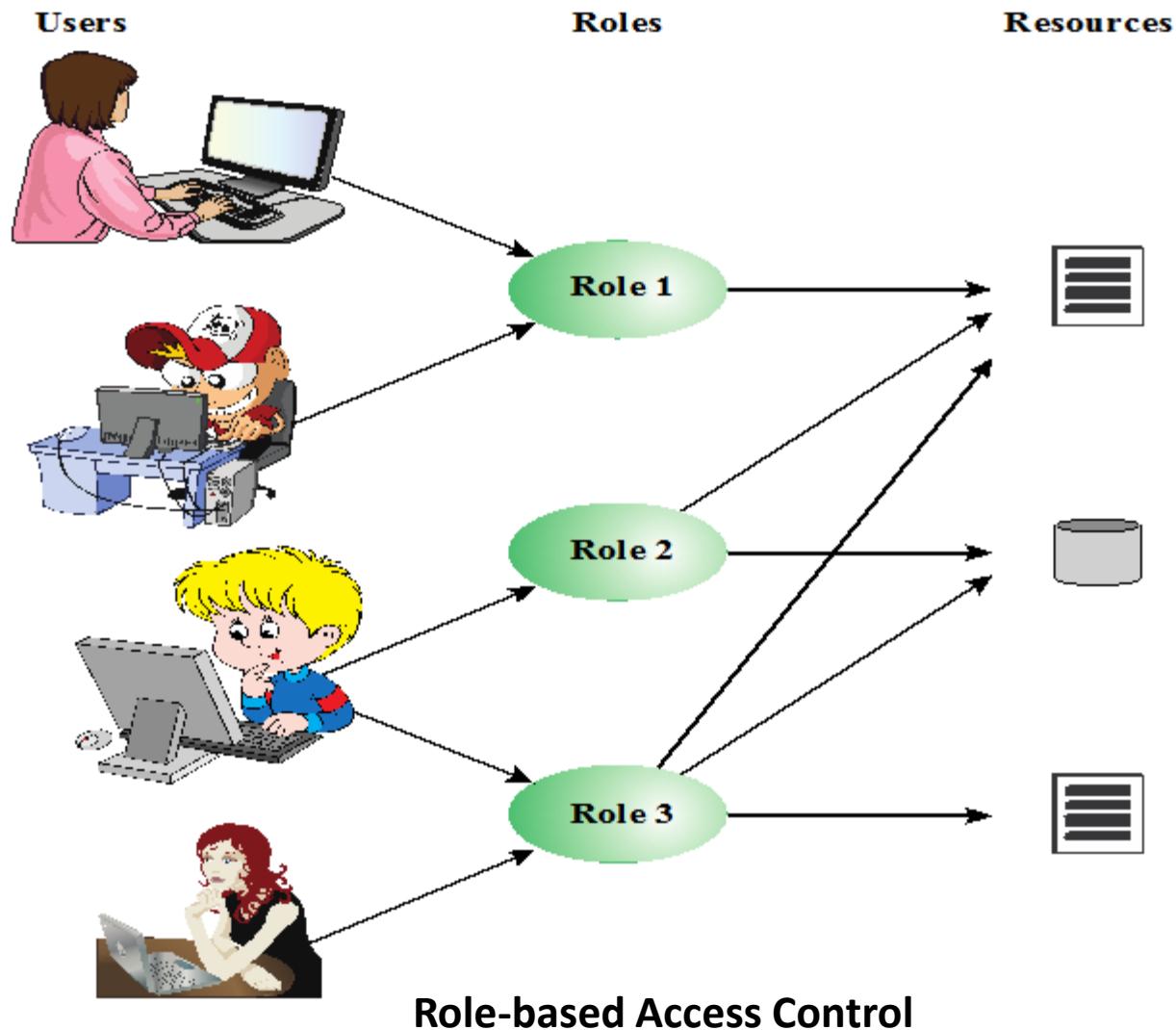
Traditional UNIX File Access Control

- “Set user ID”(SetUID)
 - “Set group ID”(SetGID)
 - System temporarily uses rights of the file owner/group in addition to the real user’s rights when making access control decisions
 - Enables privileged programs to access files/resources not generally accessible
- Sticky bit
 - When applied to a directory it specifies that only the owner of any file in the directory can rename, move, or delete that file
- Superuser
 - Is exempt from usual access control restrictions
 - Has system-wide access



(b) Extended access control list

UNIX File Access Control

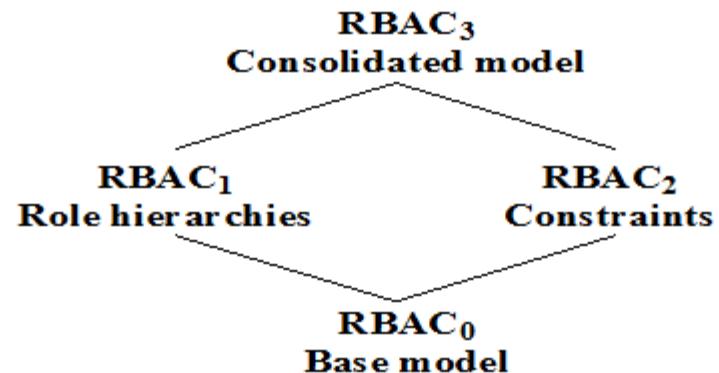


Users, Roles, and Resources

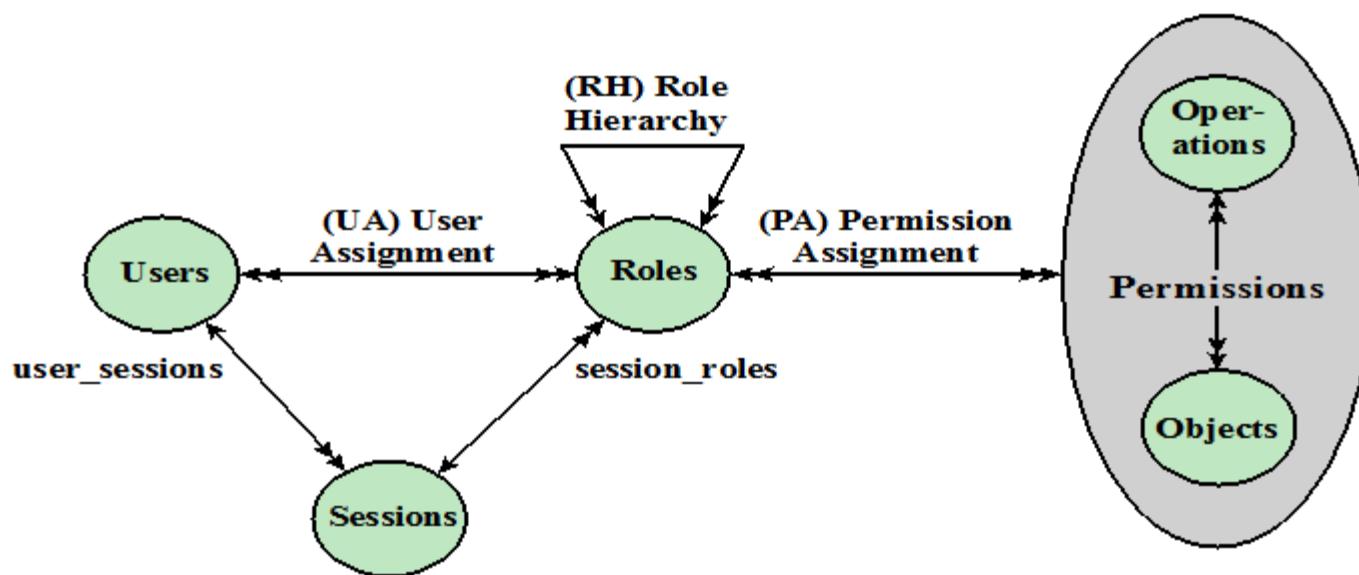
	R ₁	R ₂	• • •	R _n
U ₁	X			
U ₂	X			
U ₃		X		X
U ₄				X
U ₅				X
U ₆				X
•				
•				
•				
U _m	X			

		OBJECTS								
		R ₁	R ₂	R _n	F ₁	F ₁	P ₁	P ₂	D ₁	D ₂
ROLES	R ₁	control	owner	owner control	read *	read owner	wakeup	wakeup	seek	owner
	R ₂		control		write *	execute			owner	seek *
	•									
	•									
	R _n			control		write	stop			

Access Control Matrix Representation of RBAC



(a) Relationship among RBAC models

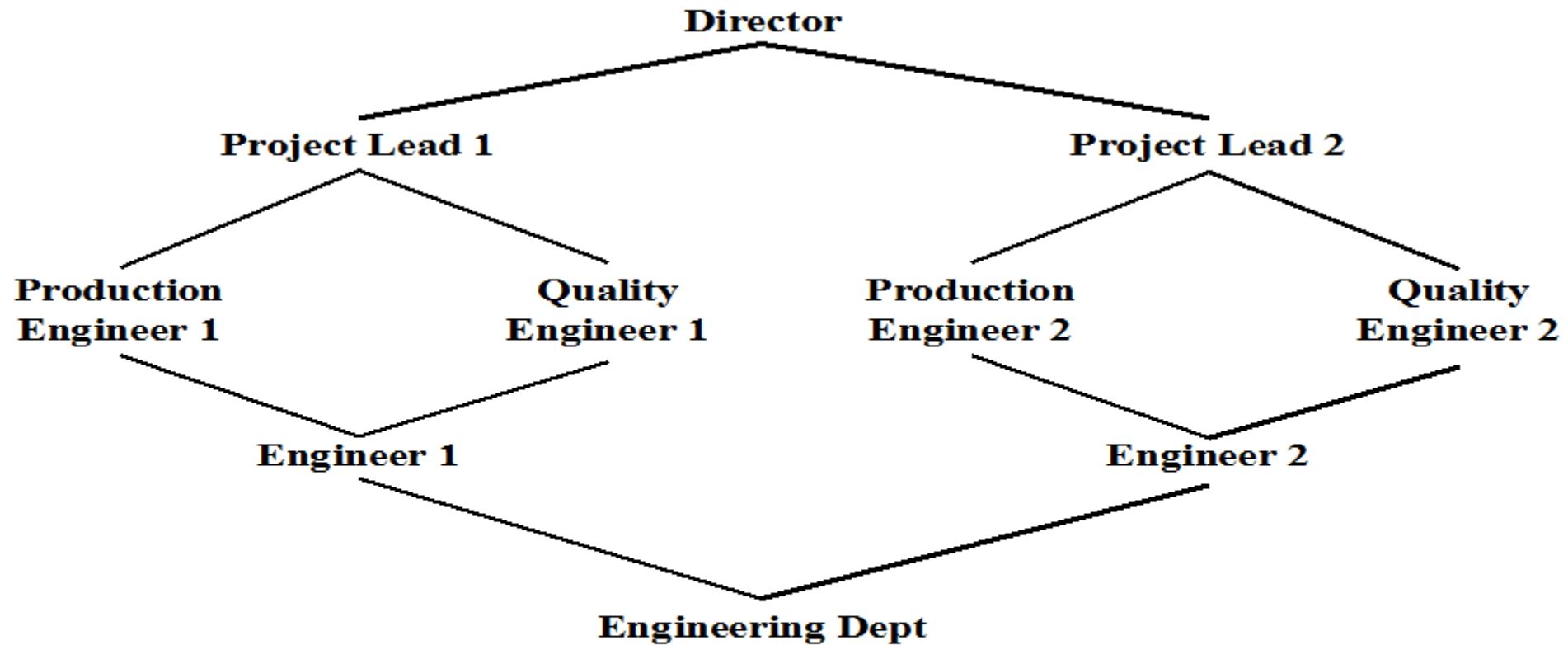


(b) RBAC models

A Family of Role-Based Access Control Models.

Scope RBAC Models

Models	Hierarchies	Constraints
RBAC_0	No	No
RBAC_1	Yes	No
RBAC_2	No	Yes
RBAC_3	Yes	Yes



Example of Role Hierarchy

Constraints - RBAC

- Provide a means of adapting RBAC to the specifics of administrative and security policies of an organization
- A defined relationship among roles or a condition related to roles
- Types:

Mutually exclusive roles
<ul style="list-style-type: none">• A user can only be assigned to one role in the set (either during a session or statically)• Any permission (access right) can be granted to only one role in the set

Cardinality
<ul style="list-style-type: none">• Setting a maximum number with respect to roles

Prerequisite roles
<ul style="list-style-type: none">• Dictates that a user can only be assigned to a particular role if it is already assigned to some other specified role

Attribute-Based Access Control (ABAC)

Can define authorizations that express conditions on properties of both the resource and the subject

Strength is its flexibility and expressive power

Main obstacle to its adoption in real systems has been concern about the performance impact of evaluating predicates on both resource and user properties for each access

Web services have been pioneering technologies through the introduction of the eXtensible Access Control Markup Language (XAMCL)

There is considerable interest in applying the model to cloud services

ABAC Model: Attributes

Subject attributes

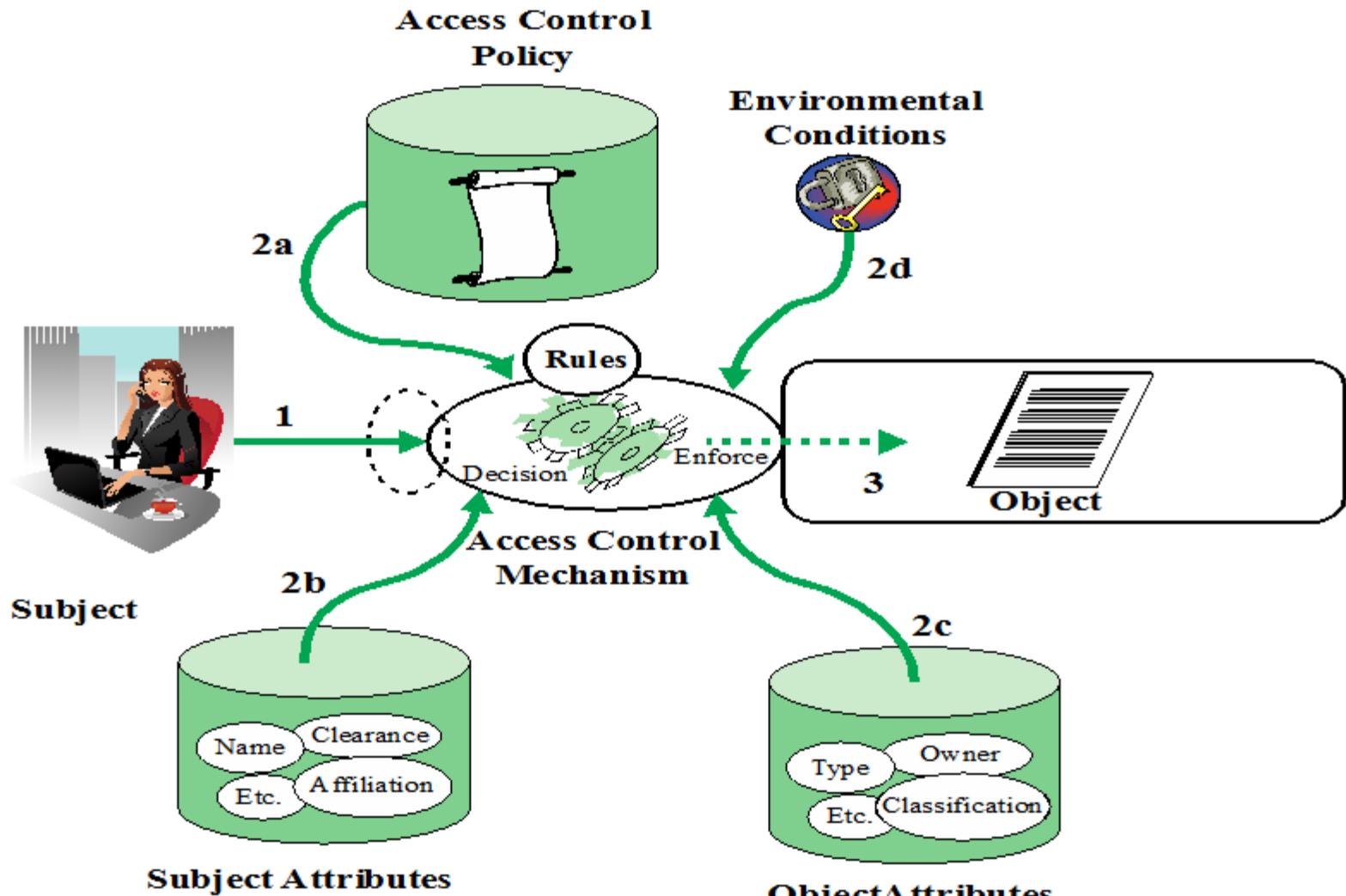
- A subject is an active entity that causes information to flow among objects or changes the system state
- Attributes define the identity and characteristics of the subject

Object attributes

- An object (or resource) is a passive information system-related entity containing or receiving information
- Objects have attributes that can be leveraged to make access control decisions

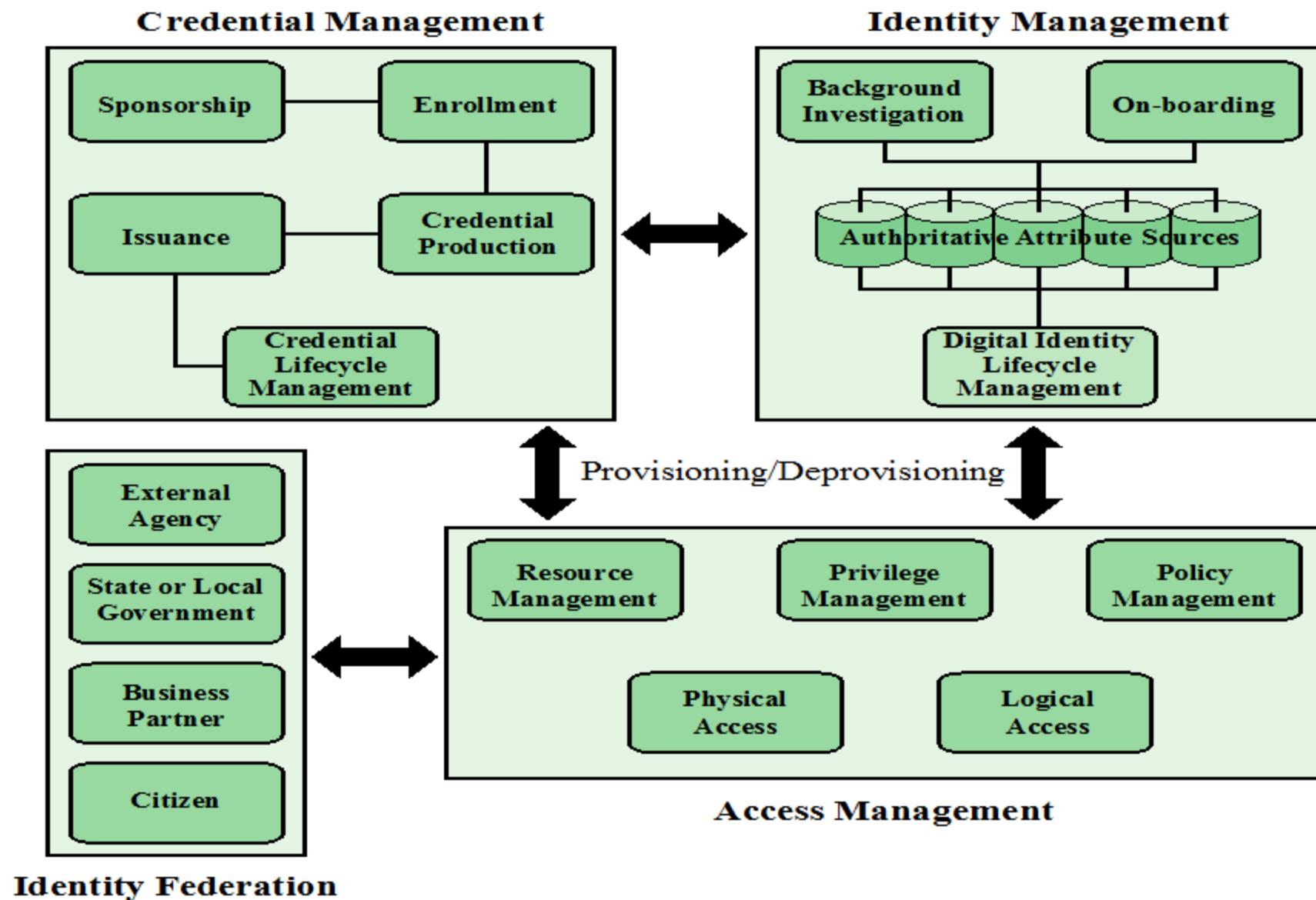
Environment attributes

- Describe the operational, technical, and even situational environment or context in which the information access occurs
- These attributes have so far been largely ignored in most access control policies



Identity, Credential, and Access Management (ICAM)

- A comprehensive approach to managing and implementing digital identities, credentials, and access control
- Developed by the U.S. government
- Designed to:
 - Create trusted digital identity representations of individuals and nonperson entities (NPEs)
 - Bind those identities to credentials that may serve as a proxy for the individual or NPE in access transactions
 - A credential is an object or data structure that authoritatively binds an identity to a token possessed and controlled by a subscriber
 - Use the credentials to provide authorized access to an agency's resources



Identity, Credential, and Access Management (ICAM)

Identity Management



Concerned with assigning attributes to a digital identity and connecting that digital identity to an individual or NPE

Goal is to establish a trustworthy digital identity that is independent of a specific application or context

Most common approach to access control for applications and programs is to create a digital representation of an identity for the specific use of the application or program

Maintenance and protection of the identity itself is treated as secondary to the mission associated with the application

Final element is lifecycle management which includes:

- Mechanisms, policies, and procedures for protecting personal identity information
- Controlling access to identity data
- Techniques for sharing authoritative identity data with applications that need it
- Revocation of an enterprise identity

Credential Management

The management of the life cycle of the credential

Examples of credentials are smart cards, private/public cryptographic keys, and digital certificates

Encompasses five logical components:

An authorized individual sponsors an individual or entity for a credential to establish the need for the credential

The sponsored individual enrolls for the credential

- Process typically consists of identity proofing and the capture of biographic and biometric data
- This step may also involve incorporating authoritative attribute data, maintained by the identity management component

A credential is produced

- Depending on the credential type, production may involve encryption, the use of a digital signature, the production of a smart card or other functions

The credential is issued to the individual or NPE

A credential must be maintained over its life cycle

- Might include revocation, reissuance/replacement, reenrollment, expiration, personal identification number (PIN) reset, suspension, or reinstatement

Access Management

Deals with the management and control of the ways entities are granted access to resources

Covers both logical and physical access

May be internal to a system or an external element

Purpose is to ensure that the proper identity verification is made when an individual attempts to access a security sensitive building, computer systems, or data

Three support elements are needed for an enterprise-wide access control facility:

- Resource management
- Privilege management
- Policy management

Three support elements are needed for an enterprise-wide access control facility:

Resource management

- Concerned with defining rules for a resource that requires access control
- Rules would include credential requirements and what user attributes, resource attributes, and environmental conditions are required for access of a given resource for a given function

Privilege management

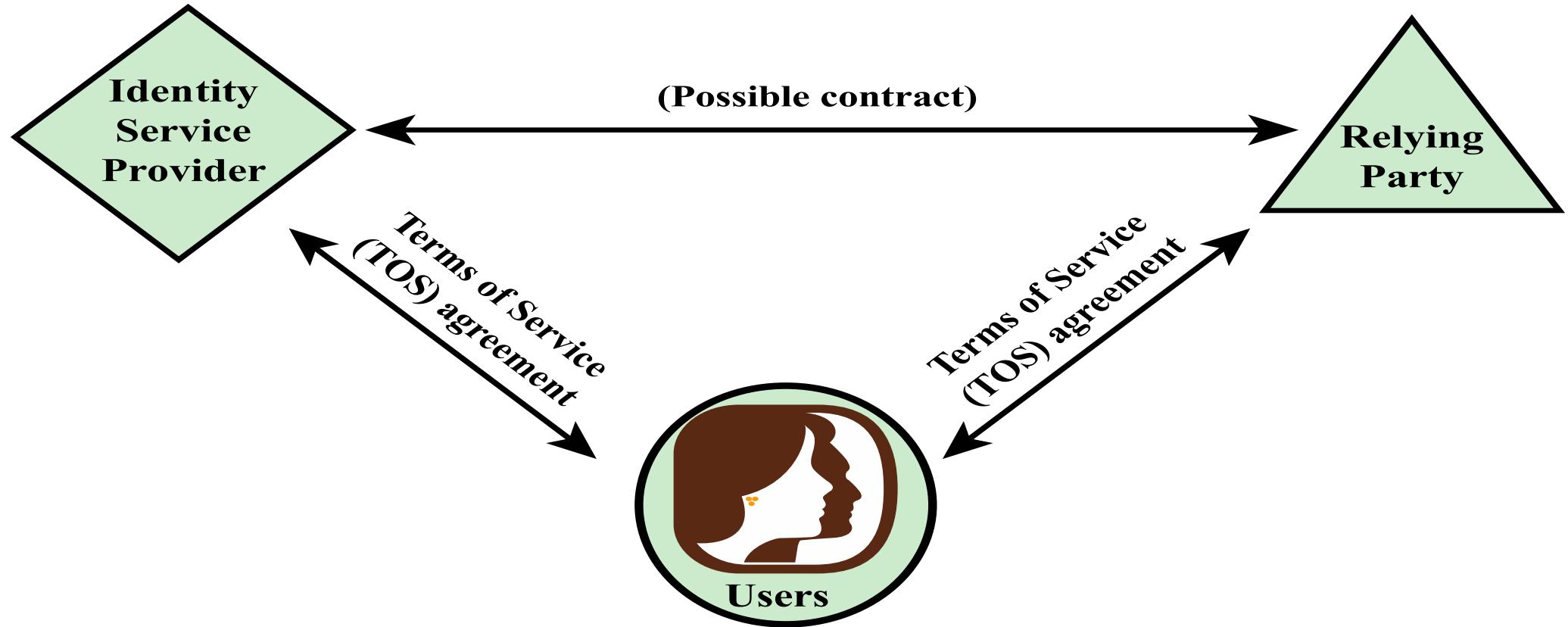
- Concerned with establishing and maintaining the entitlement or privilege attributes that comprise an individual's access profile
- These attributes represent features of an individual that can be used as the basis for determining access decisions to both physical and logical resources
- Privileges are considered attributes that can be linked to a digital identity

Policy management

- Governs what is allowable and unallowable in an access transaction

Identity Federation

- Term used to describe the technology, standards, policies, and processes that allow an organization to trust digital identities, identity attributes, and credentials created and issued by another organization
- Addresses two questions:
 - How do you trust identities of individuals from external organizations who need access to your systems
 - How do you vouch for identities of individuals in your organization when they need to collaborate with external organizations



(a) Traditional triangle of parties involved in an exchange of identity information

Identity Information Exchange Approaches

Open Identity Trust Framework

OpenID

- An open standard that allows users to be authenticated by certain cooperating sites using a third party service

OIDF

- OpenID Foundation is an international nonprofit organization of individuals and companies committed to enabling, promoting, and protecting OpenID technologies

ICF

- Information Card Foundation is a nonprofit community of companies and individuals working together to evolve the Information Card ecosystem

OITF

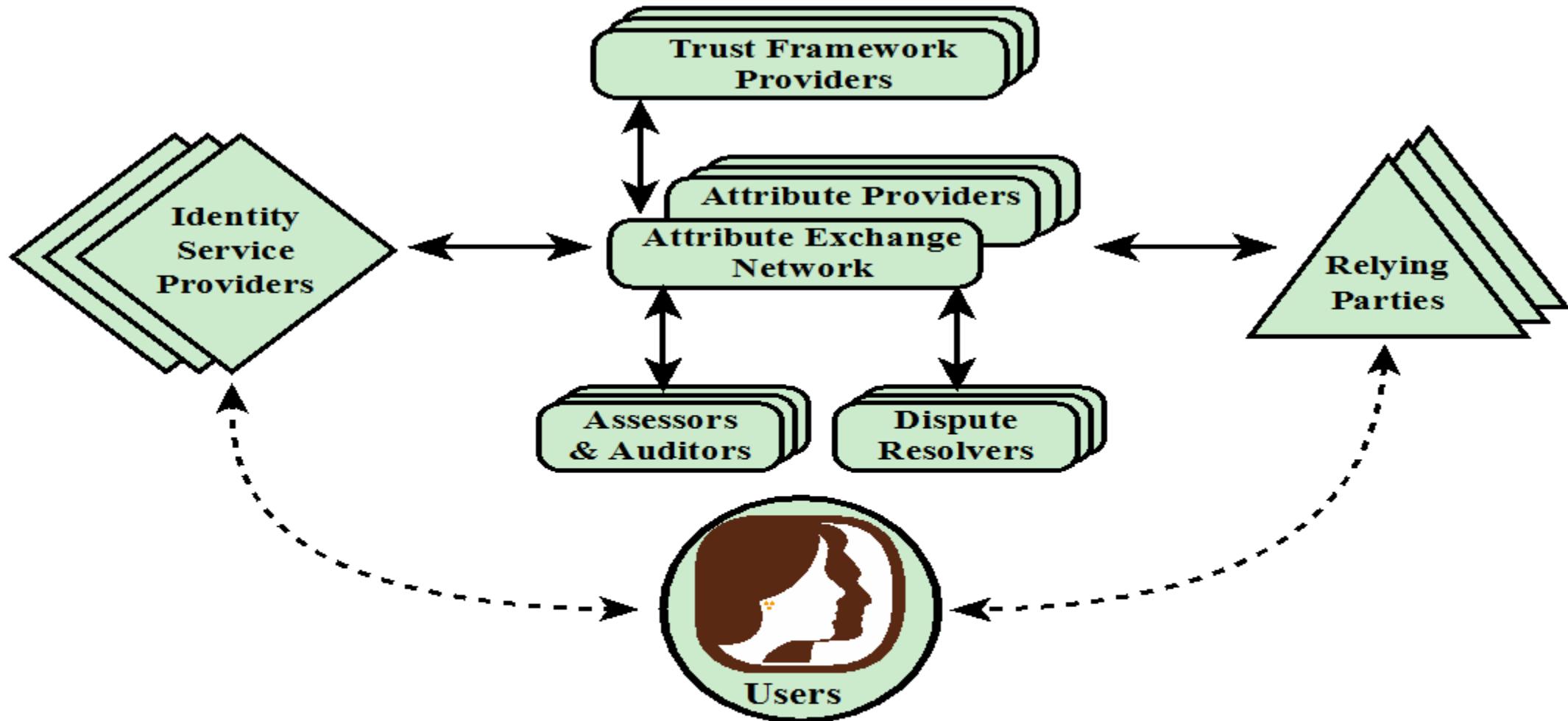
- Open Identity Trust Framework is a standardized, open specification of a trust framework for identity and attribute exchange, developed jointly by OIDF and ICF

OIX

- Open Identity Exchange Corporation is an independent, neutral, international provider of certification trust frameworks conforming to the OITF model

AXN

- Attribute Exchange Network is an online Internet-scale gateway for identity service providers and relying parties to efficiently access user asserted, permissioned, and verified online identity attributes in high volumes at affordable costs



(B) Identity attribute exchange elements

Identity Information Exchange Approaches

Lecture 5

Database and Cloud security

CMPU-4008

Advance Security 2

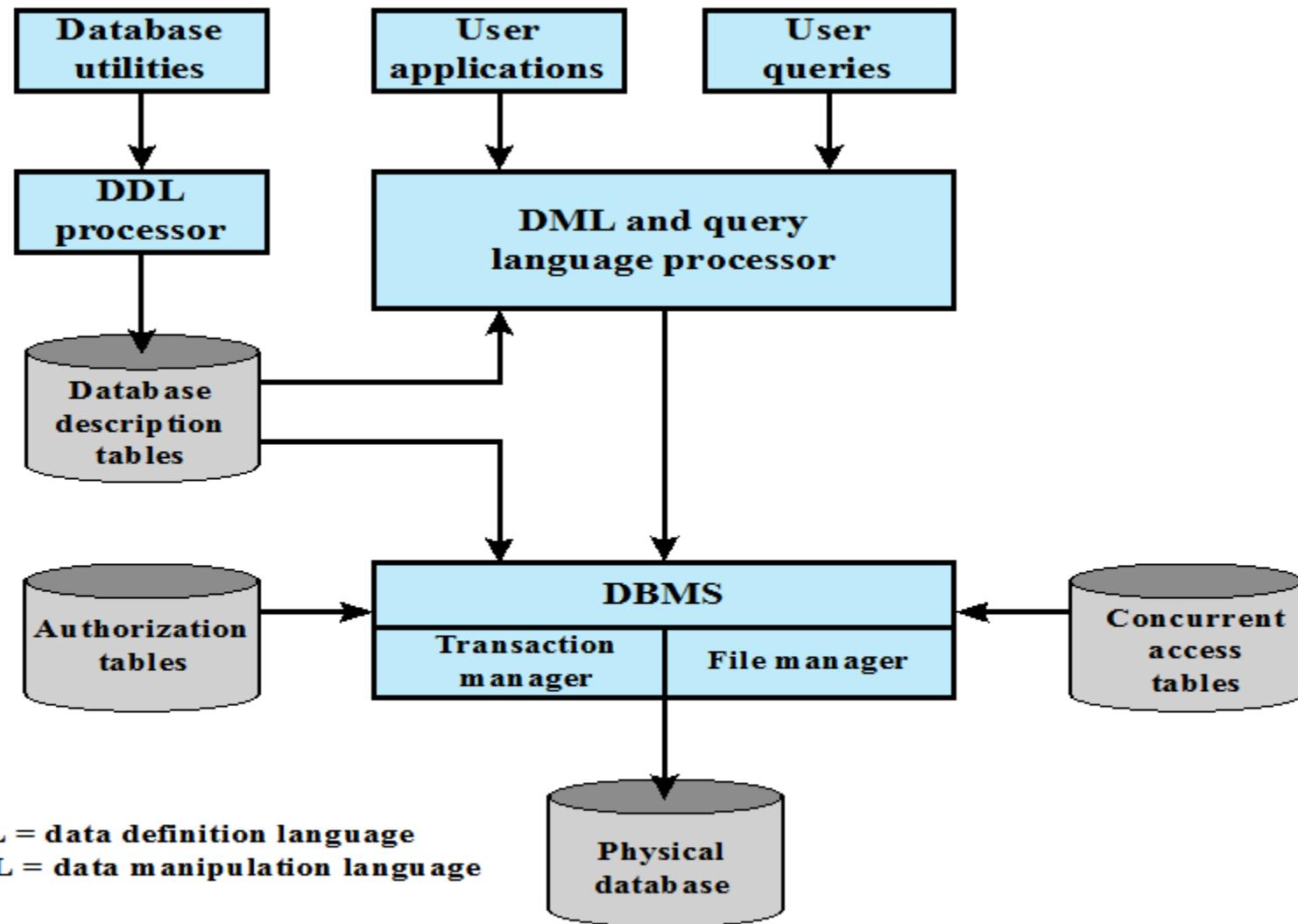


Databases

- Structured collection of data stored for use by one or more applications
- Contains the relationships between data items and groups of data items
- Can sometimes contain sensitive data that needs to be secured
- Query language
 - Provides a uniform interface to the database

Database management system (DBMS)

- Suite of programs for constructing and maintaining the database
- Offers ad hoc query facilities to multiple users and applications



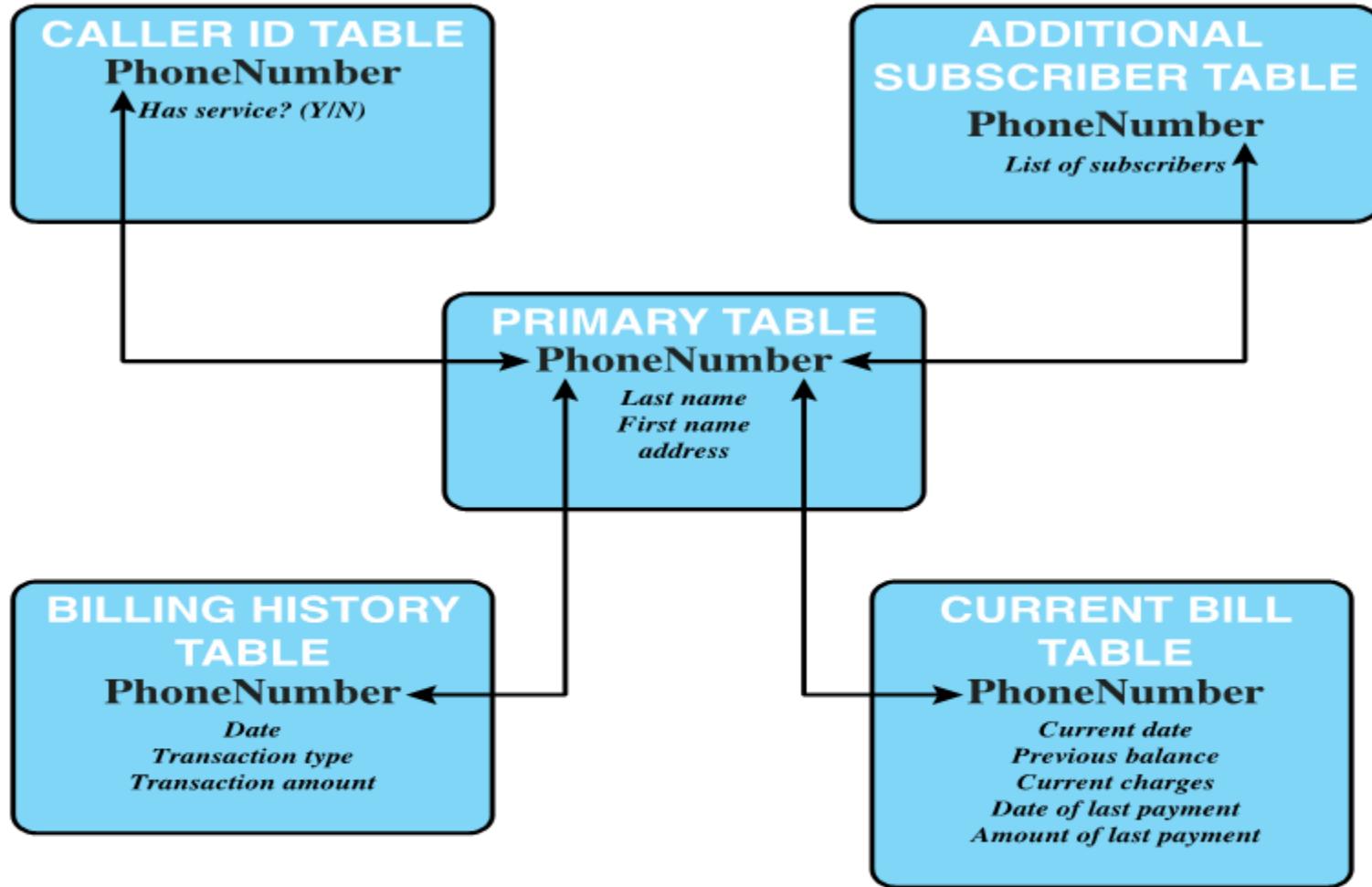
DDL = data definition language

DML = data manipulation language

DBMS Architecture

Relational Databases

- Table of data consisting of rows and columns
 - Each column holds a particular type of data
 - Each row contains a specific value for each column
 - Ideally has one column where all values are unique, forming an identifier/key for that row
- Enables the creation of multiple tables linked together by a unique identifier that is present in all tables
- Use a relational query language to access the database
 - Allows the user to request data that fit a given set of criteria



Example Relational Database Model. A relational database uses multiple tables related to one another by a designated key; in this case the key is the **PhoneNumber** field.

Relational Database Elements



- Relation/table/file
- Tuple/row/record
- Attribute/column/field

Primary key

- Uniquely identifies a row
- Consists of one or more column names

Foreign key

- Links one table to attributes in another

View/virtual table

- Result of a query that returns selected rows and columns from one or more tables

Basic Terminology for Relational Databases

Formal Name	Common Name	Also Known As
Relation	Table	File
Tuple	Row	Record
Attribute	Column	Field

Department Table

Did	Dname	Dacctno
4	human resources	528221
8	education	202035
9	accounts	709257
13	public relations	755827
15	services	223945

primary key

Employee Table

Ename	Did	Salarycode	Eid	Ephone
Robin	15	23	2345	6127092485
Neil	13	12	5088	6127092246
Jasmine	4	26	7712	6127099348
Cody	15	22	9664	6127093148
Holly	8	23	3054	6127092729
Robin	8	24	2976	6127091945
Smith	9	21	4490	6127099380

foreign key

primary key

(a) Two tables in a relational database

Dname	Ename	Eid	Ephone
human resources	Jasmine	7712	6127099348
education	Holly	3054	6127092729
education	Robin	2976	6127091945
accounts	Smith	4490	6127099380
public relations	Neil	5088	6127092246
services	Robin	2345	6127092485
services	Cody	9664	6127093148

(b) A view derived from the database

Relational Database Example

Structured Query Language (SQL)

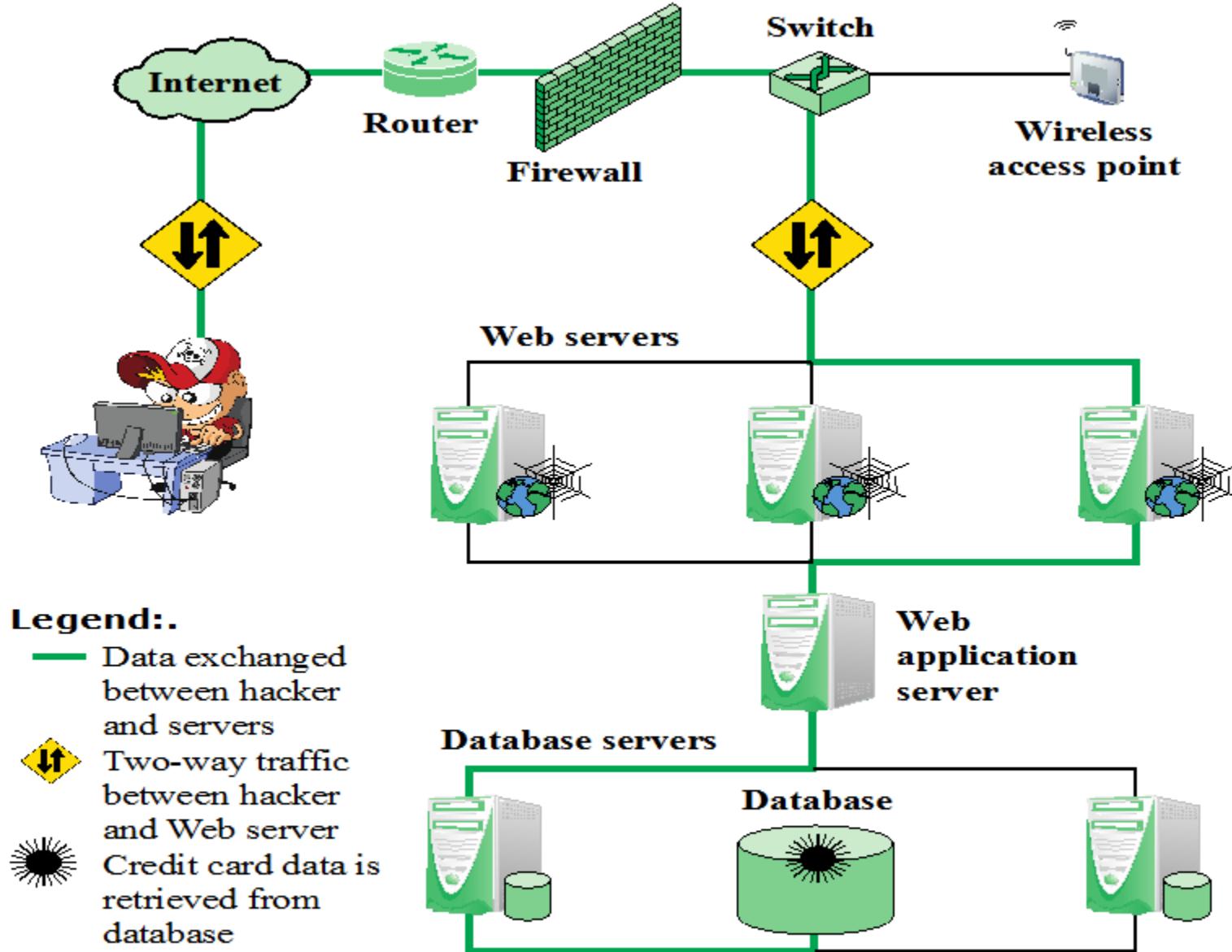
- Standardized language to define schema, manipulate, and query data in a relational database
- Several similar versions of ANSI/ISO standard
- All follow the same basic syntax and semantics

SQL statements can be used to:

- Create tables
- Insert and delete data in tables
- Create views
- Retrieve data with query statements

SQL Injection Attacks (SQLi)

- One of the most prevalent and dangerous network-based security threats
- Designed to exploit the nature of Web application pages
- Sends malicious SQL commands to the database server
- Most common attack goal is bulk extraction of data
- Depending on the environment SQL injection can also be exploited to:
 - Modify or delete data
 - Execute arbitrary operating system commands
 - Launch denial-of-service (DoS) attacks

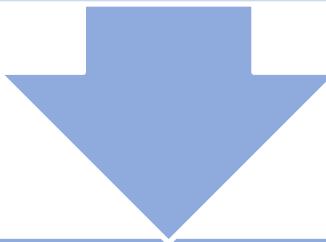


Typical SQL Injection Attack

Injection Technique

The SQLi attack typically works by prematurely terminating a text string and appending a new command

Because the inserted command may have additional strings appended to it before it is executed the attacker terminates the injected string with a comment mark “--”



Subsequent text is ignored at execution time

SQLi Attack Avenues

User input

- Attackers inject SQL commands by providing suitable crafted user input

Server variables

- Attackers can forge the values that are placed in HTTP and network headers and exploit this vulnerability by placing data directly into the headers

Second-order injection

- A malicious user could rely on data already present in the system or database to trigger an SQL injection attack, so when the attack occurs, the input that modifies the query to cause an attack does not come from the user, but from within the system itself

Cookies

- An attacker could alter cookies such that when the application server builds an SQL query based on the cookie's content, the structure and function of the query is modified

Physical user input

- Applying user input that constructs an attack outside the realm of web requests

Inband Attacks

- Uses the same communication channel for injecting SQL code and retrieving results
- The retrieved data are presented directly in application Web page
- Include:

Tautology

This form of attack injects code in one or more conditional statements so that they always evaluate to true

End-of-line comment

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

Piggybacked queries

The attacker adds additional queries beyond the intended query, piggy-backing the attack on top of a legitimate request

Inferential Attack

- There is no actual transfer of data, but the attacker is able to reconstruct the information by sending particular requests and observing the resulting behavior of the Website/database server
- Include:
 - Illegal/logically incorrect queries
 - This attack lets an attacker gather important information about the type and structure of the backend database of a Web application
 - The attack is considered a preliminary, information-gathering step for other attacks
 - Blind SQL injection
 - Allows attackers to infer the data present in a database system even when the system is sufficiently secure to not display any erroneous information back to the attacker

Out-of-Band Attack

- Data are retrieved using a different channel
- This can be used when there are limitations on information retrieval, but outbound connectivity from the database server is lax



SQLi Countermeasures

- Three types:

- Manual defensive coding practices
- Parameterized query insertion
- SQL DOM

Defensive coding

Detection

- Signature based
- Anomaly based
- Code analysis

Run-time prevention

- Check queries at runtime to see if they conform to a model of expected queries

Database Access Control

Database access control system determines:

If the user has access to the entire database or just portions of it

What access rights the user has (create, insert, delete, update, read, write)

Can support a range of administrative policies

Centralized administration

- Small number of privileged users may grant and revoke access rights

Ownership-based administration

- The creator of a table may grant and revoke access rights to the table

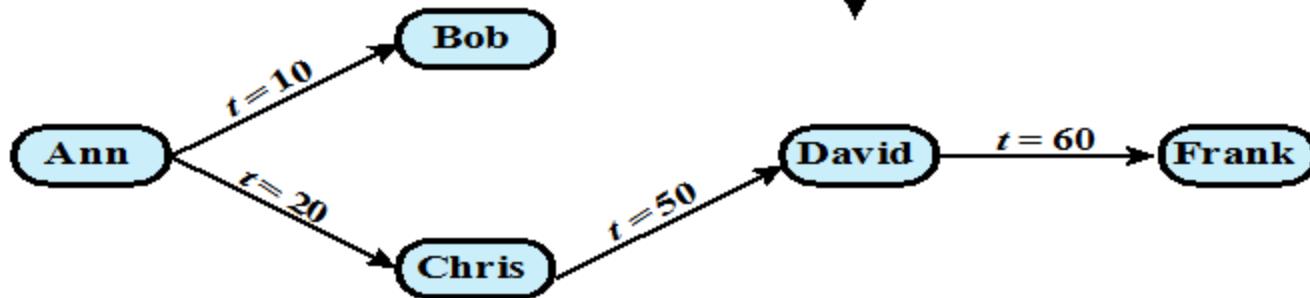
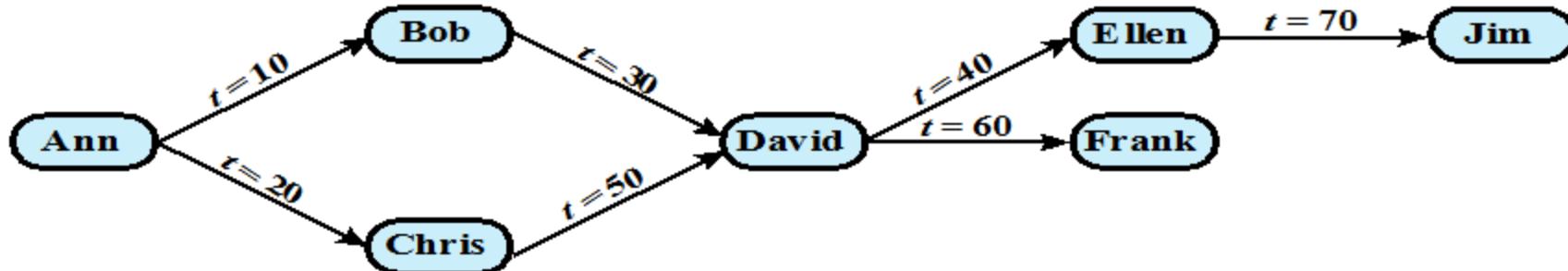
Decentralized administration

- The owner of the table may grant and revoke authorization rights to other users, allowing them to grant and revoke access rights to the table

SQL Access Controls

- Two commands for managing access rights:
 - Grant
 - Used to grant one or more access rights or can be used to assign a user to a role
 - Revoke
 - Revokes the access rights
- Typical access rights are:
 - Select
 - Insert
 - Update
 - Delete
 - References

Example of Cascading Authorizations



Bob Revokes Privilege from David

Role-Based Access Control (RBAC)

- Role-based access control eases administrative burden and improves security
- A database RBAC needs to provide the following capabilities:
 - Create and delete roles
 - Define permissions for a role
 - Assign and cancel assignment of users to roles
- Categories of database users:

Application owner

- An end user who owns database objects as part of an application

End user

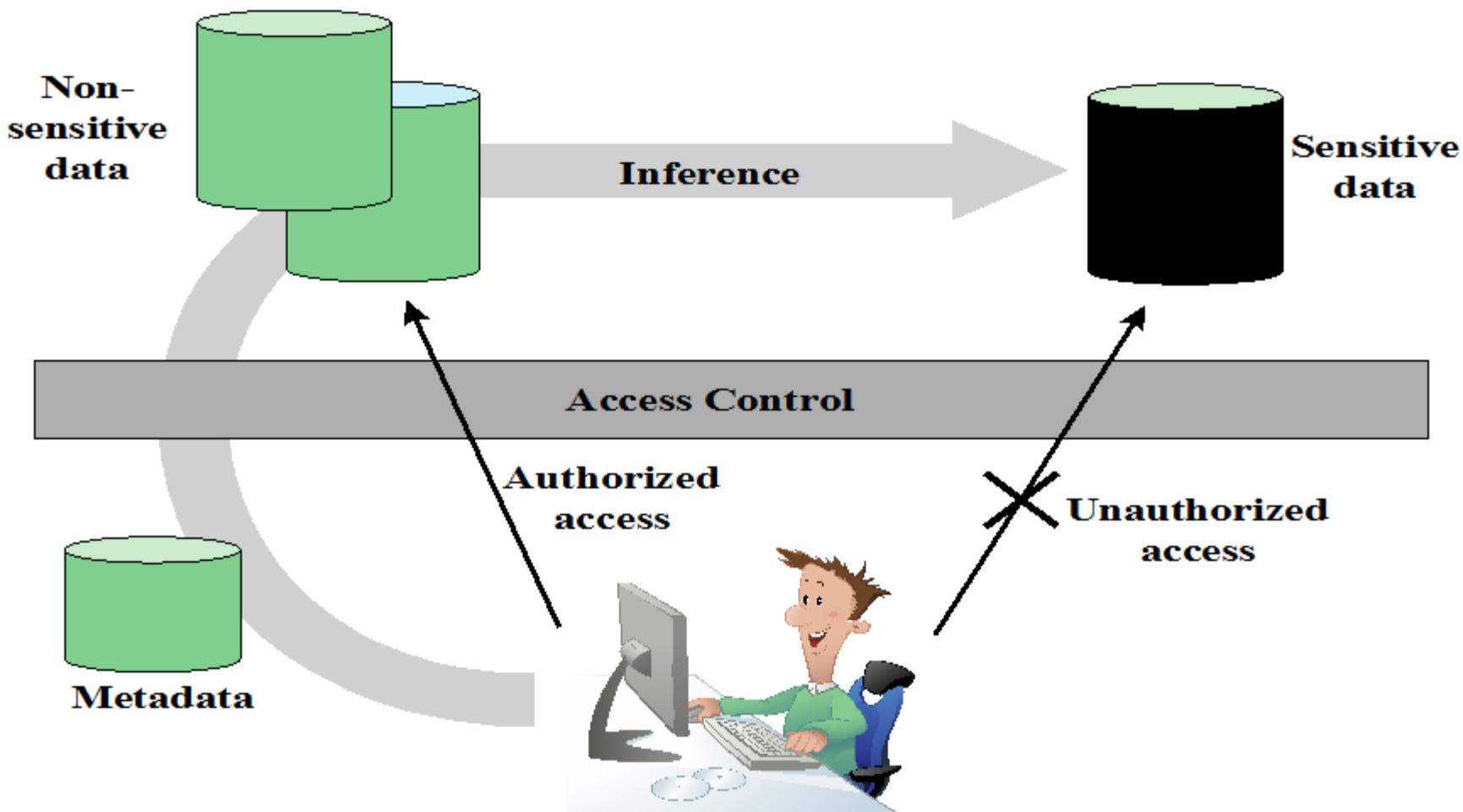
- An end user who operates on database objects via a particular application but does not own any of the database objects

Administrator

- User who has administrative responsibility for part or all of the database

Fixed Roles in Microsoft SQL Server

Role	Permissions
Fixed Server Roles	
sysadmin	Can perform any activity in SQL Server and have complete control over all database functions
serveradmin	Can set server-wide configuration options, shut down the server
setupadmin	Can manage linked servers and startup procedures
securityadmin	Can manage logins and CREATE DATABASE permissions, also read error logs and change passwords
processadmin	Can manage processes running in SQL Server
dbcreator	Can create, alter, and drop databases
diskadmin	Can manage disk files
bulkadmin	Can execute BULK INSERT statements
Fixed Database Roles	
db_owner	Has all permissions in the database
db_accessadmin	Can add or remove user IDs
db_datareader	Can select all data from any user table in the database
db_datawriter	Can modify any data in any user table in the database
db_ddladmin	Can issue all Data Definition Language (DDL) statements
db_securityadmin	Can manage all permissions, object ownerships, roles and role memberships
db_backupoperator	Can issue DBCC, CHECKPOINT, and BACKUP statements
db_denydatareader	Can deny permission to select data in the database
db_denydatawriter	Can deny permission to change data in the database



Indirect Information Access Via Inference Channel

Item	Availability	Cost (\$)	Department
Shelf support	in-store/online	7.99	hardware
Lid support	online only	5.49	hardware
Decorative chain	in-store/online	104.99	hardware
Cake pan	online only	12.99	housewares
Shower/tub cleaner	in-store/online	11.99	housewares
Rolling pin	in-store/online	10.99	housewares

(a) Inventory table

Availability	Cost (\$)
in-store/online	7.99
online only	5.49
in-store/online	104.99

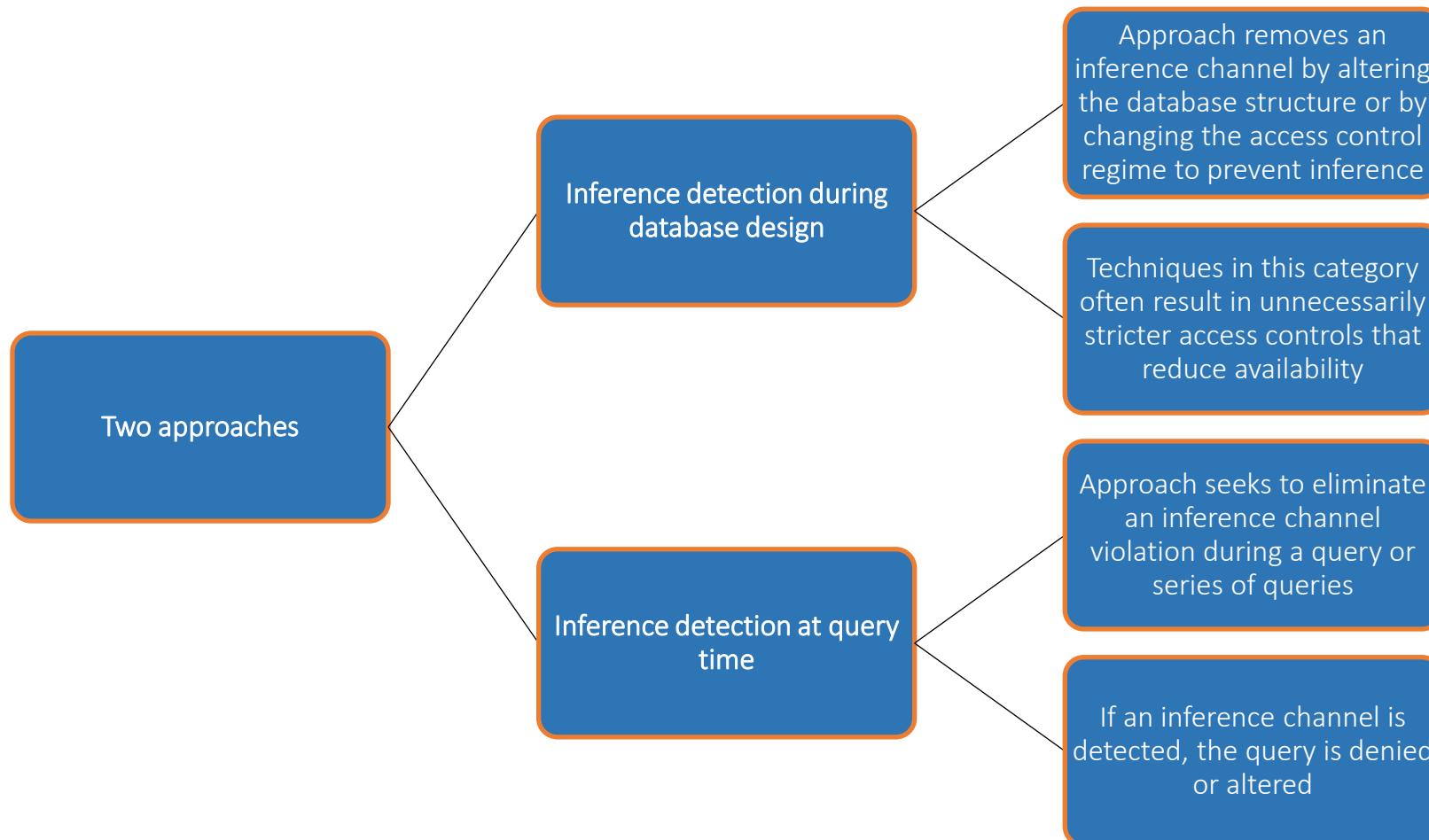
Item	Department
Shelf support	hardware
Lid support	hardware
Decorative chain	hardware

(b) Two views

Item	Availability	Cost (\$)	Department
Shelf support	in-store/online	7.99	hardware
Lid support	online only	5.49	hardware
Decorative chain	in-store/online	104.99	hardware

(c) Table derived from combining query answers

Inference Detection



- Some inference detection algorithm is needed for either of these approaches
- Progress has been made in devising specific inference detection techniques for multilevel secure databases and statistical databases

Database Encryption

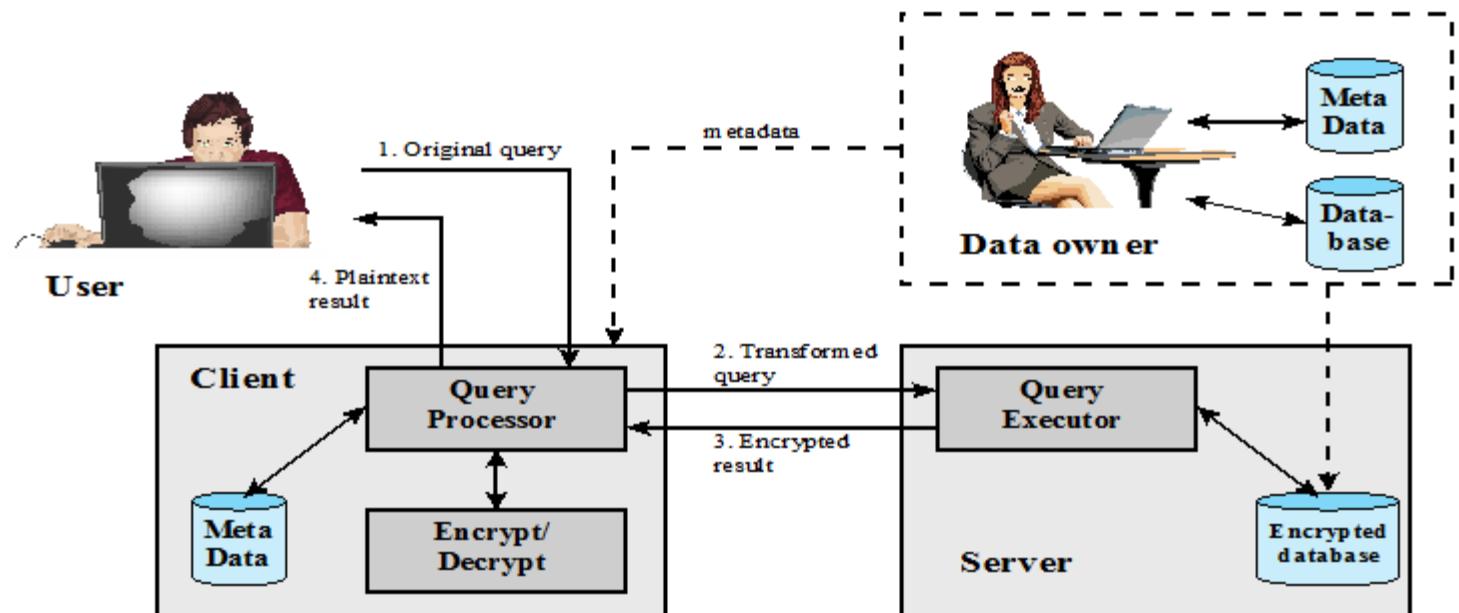
- The database is typically the most valuable information resource for any organization
 - Protected by multiple layers of security
 - Firewalls, authentication, general access control systems, DB access control systems, database encryption
 - Encryption becomes the last line of defense in database security
 - Can be applied to the entire database, at the record level, the attribute level, or level of the individual field
- Disadvantages to encryption:
 - Key management
 - Authorized users must have access to the decryption key for the data for which they have access
 - Inflexibility
 - When part or all of the database is encrypted it becomes more difficult to perform record searching

Data owner – organization that produces data to be made available for controlled release

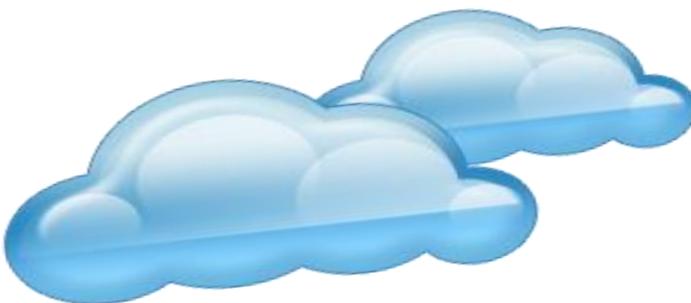
User – human entity that presents queries to the system

Client – frontend that transforms user queries into queries on the encrypted data stored on the server

Server – an organization that receives the encrypted data from a data owner and makes them available for distribution to clients



A Database Encryption Scheme

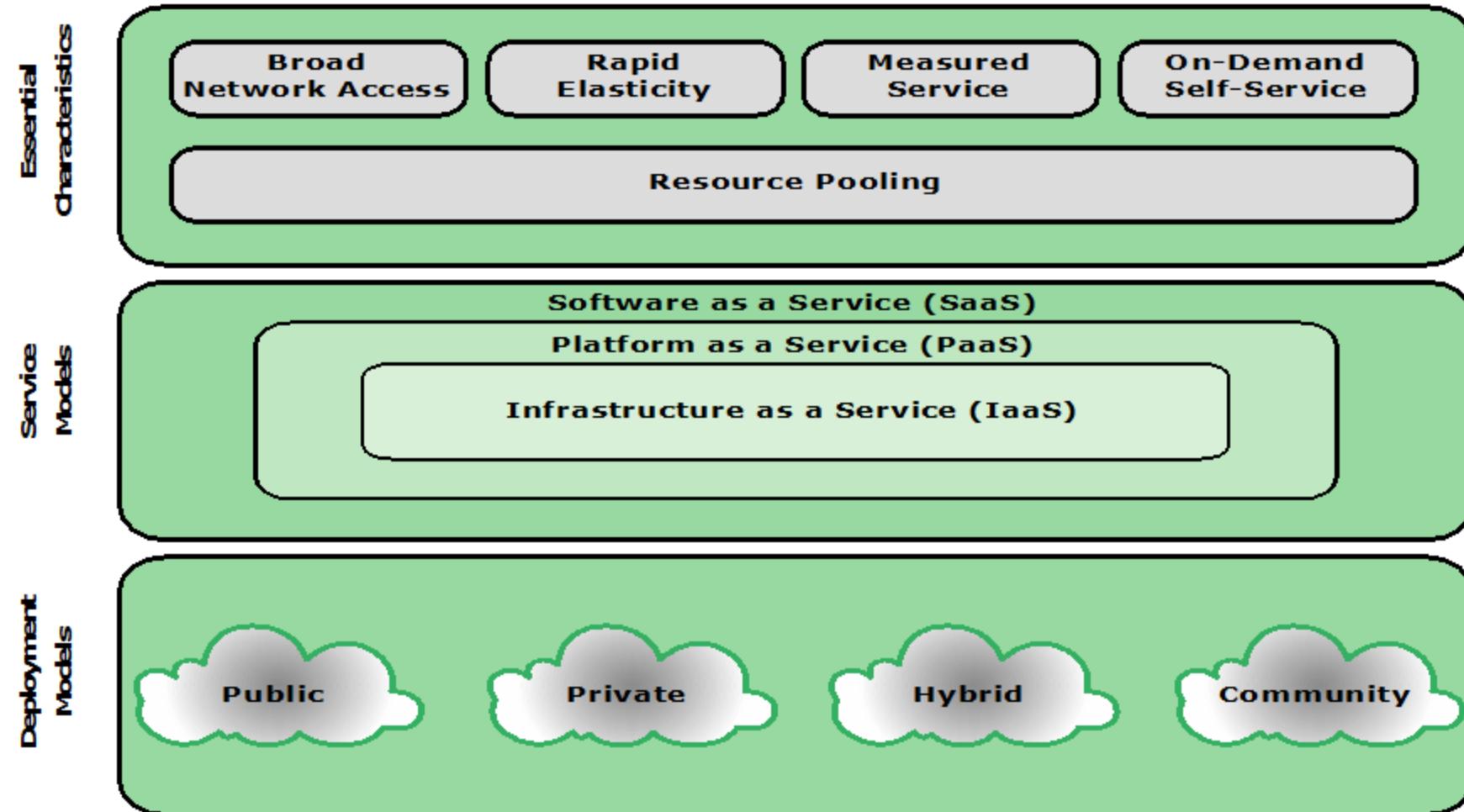


Cloud Security

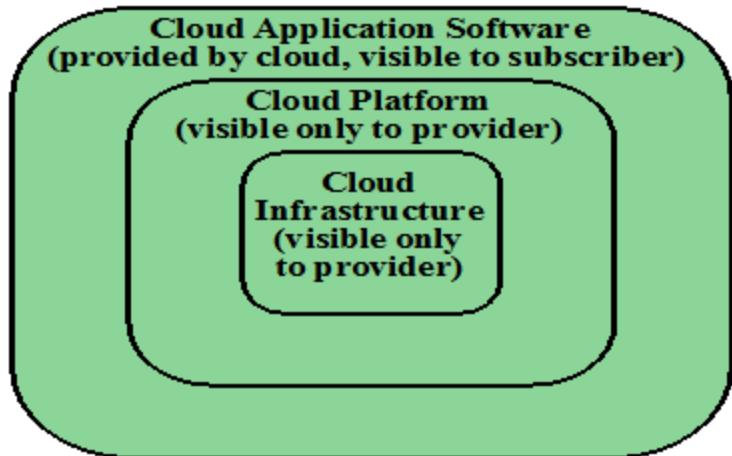


NIST SP-800-145 defines cloud computing as:

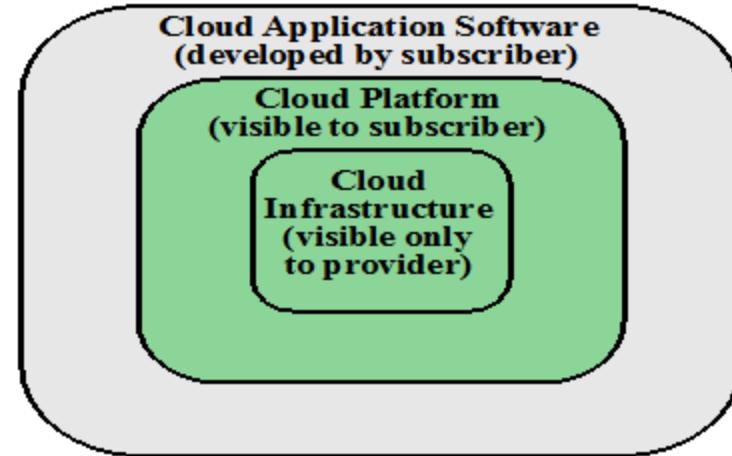
“A model for enabling ubiquitous, convenient, on-demand network access to a shared pool of configurable computing resources (e.g., networks, servers, storage, applications, and services) that can be rapidly provisioned and released with minimal management effort or service provider interaction. This cloud model promotes availability and is composed of five essential characteristics, three service models, and four deployment models.”



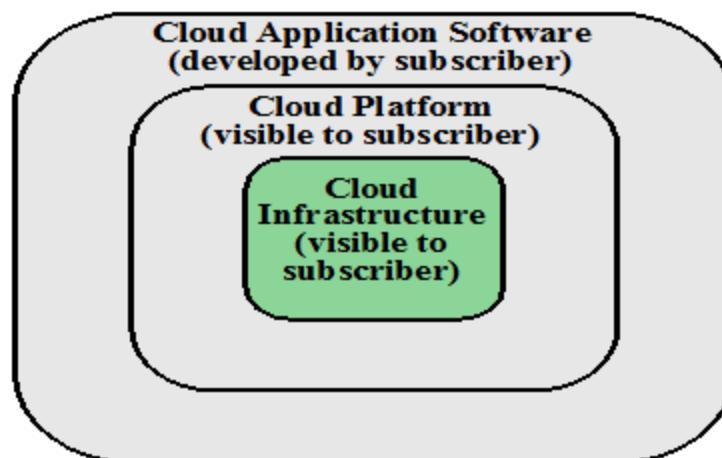
Cloud Computing Elements



(a) SaaS



(b) PaaS



(c) IaaS

Cloud Service Models

NIST Deployment Models

Public cloud

- The cloud infrastructure is made available to the general public or a large industry group and is owned by an organization selling cloud services
- The cloud provider is responsible both for the cloud infrastructure and for the control of data and operations within the cloud

Private cloud

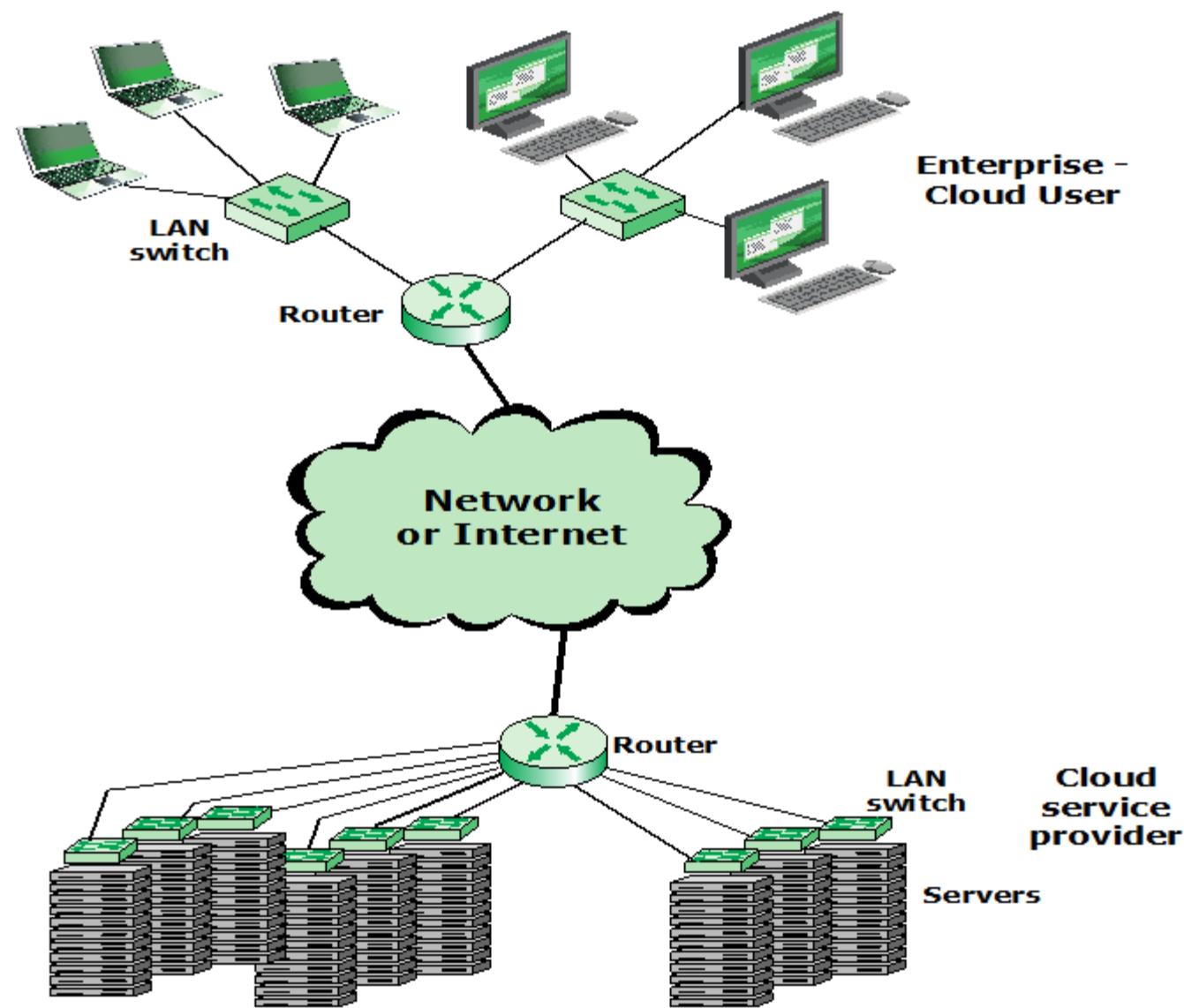
- The cloud infrastructure is operated solely for an organization
- It may be managed by the organization or a third party and may exist on premise or off premise
- The cloud provider is responsible only for the infrastructure and not for the control

Community cloud

- The cloud infrastructure is shared by several organizations and supports a specific community that has shared concerns
- It may be managed by the organizations or a third party and may exist on premise or off premise

Hybrid cloud

- The cloud infrastructure is a composition of two or more clouds that remain unique entities but are bound together by standardized or proprietary technology that enables data and application portability



Cloud Computing Context



Cloud Security Threats

The Cloud Security Alliance lists the following as the top cloud specific security threats:

Abuse and nefarious use of cloud computing

Insecure interfaces and APIs

Malicious insiders

Shared technology issues

Data loss or leakage

Account or service hijacking

Cloud Security As A Service

- SecaaS
- Is a segment of the SaaS offering of a CP
- Defined by The Cloud Security Alliance as the provision of security applications and services via the cloud either to cloud-based infrastructure and software or from the cloud to the customers' on-premise systems

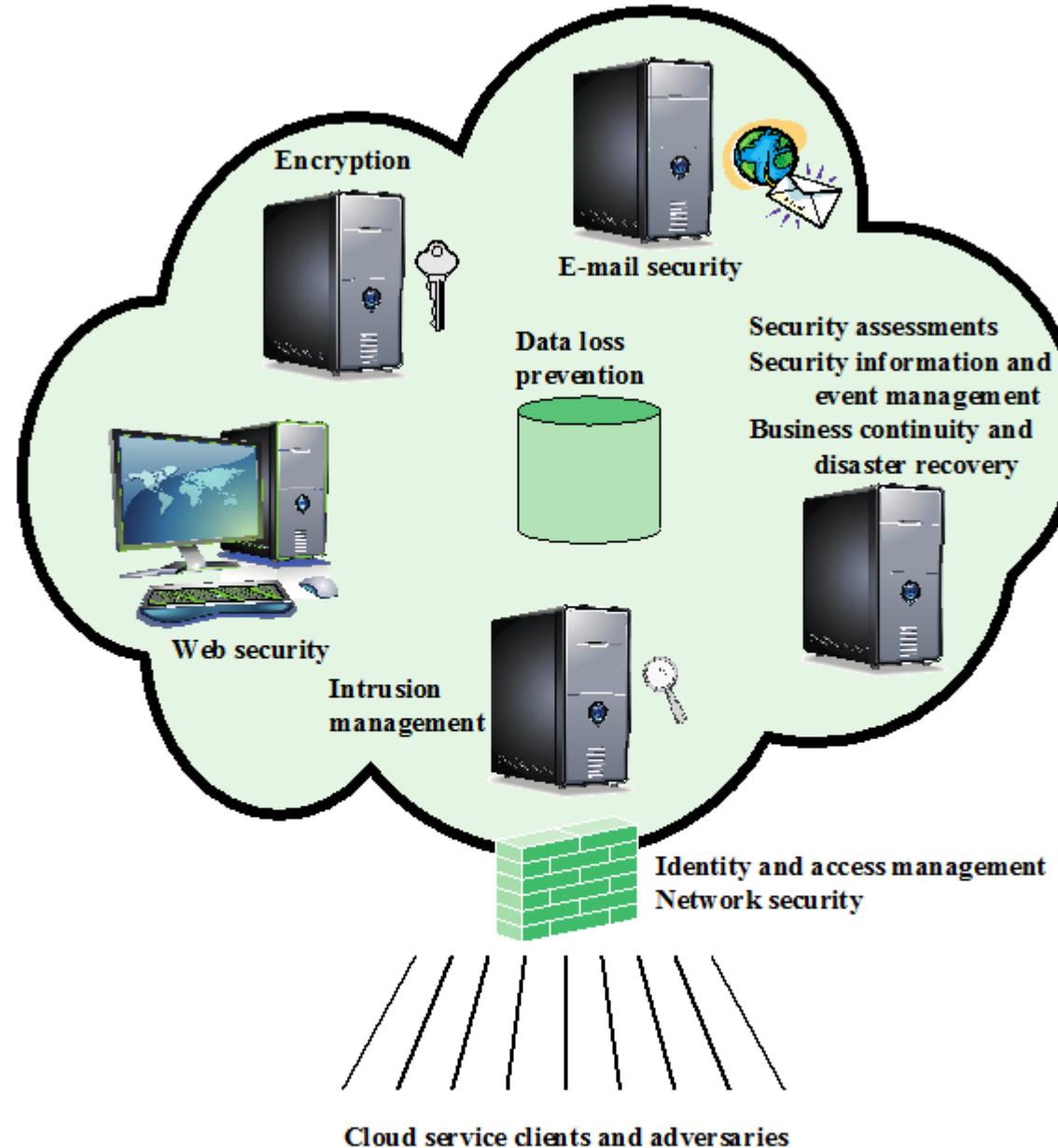


Figure Elements of Cloud Security as a Service

Cloud Security Attacks

- Denial of Service (DoS) attacks
- Malware Injection Attack
- Authentication Attacks
- Man In The Middle Attacks

Cloud Security Mechanisms

- Secure Operating System
- Strong Authentication
- Encrypt Store Data
- Intrusion Detection System

Cloud Security References

1. Top Threats to Cloud Computing V1.0, Cloud Security Alliance, March, 2010.
2. Security Guidance for Critical Areas of Focus in Cloud Computing V3.0, Cloud Security Alliance, 2011.
3. Guidelines on Security and Privacy in Public Cloud Computing, Wayne Jansen and Timothy Grance, NIST, January 2011.
4. Cloud Computing Security: A Survey, Issa M. Khalil , Abdallah Khreishah,Muhammad Azeem, Computers 2014.
5. Overview of Attacks on Cloud Computing, Ajey Singh, Maneesh Shrivastava, IJEIT,2012
6. The Management of Security in Cloud Computing, Ramgovind S, Eloff MM, Smith E, IEEE, 2010.

Lecture 6

Malicious Software

CMPU-4008
Advance Security 2

2015 Top Security Tools

Voted by ToolsWatch.org Readers

1. OWASP ZAP – Zed Attack Proxy Project
2. Lynis
3. Haka
4. Faraday
5. BeEF – The Browser Exploitation Framework
6. Burp Suite
7. PeStudio
8. Nmap
9. IDA
10. OWASP Offensive (Web) Testing Framework

Other Security Tools

- AlienVault OSSIM – The Open Source SIEM >>
 - <http://www.alienvault.com/open-threat-exchange/projects>
- oclHashcat – The Advanced Password Recovery >>
 - <http://hashcat.net/oclhashcat/>
- Metasploit – The Exploit Framework >>
 - <http://www.metasploit.com/>
- WATOBO – Web Application Toolbox >>
 - http://sourceforge.net/apps/mediawiki/watobo/index.php?title=Main_Page
- Drozer The Comprehensive security and attack framework for Android >>
 - <https://labs.mwrinfosecurity.com/tools/drozer/>
- SQLMap The Automatic SQL Injection and TakeOver Tool >>
 - <http://sqlmap.org/>
- Vega – The open source scanner and web testing platform >>
 - subgraph.com/products.html
- Nova - The Honeypot Configuration Tool and IDS >>
 - <https://github.com/DataSoft/Nova>

Other Security Tools

- Arachni – The Web Application Security Scanner Framework >> <http://www.arachniscanner.com/>
- Tunna Framework Bypass Firewalls Restrictions Tools >> <http://www.secforce.com/research/tunna.html>
- Veil – Anti Virus Evasion >> <https://www.veil-evasion.com/>
- Moloch – Large Scale PCAP Capturing and Indexing Database >><https://github.com/aol/moloch>
- Pipal – The Password Analyzer >> <http://www.digininja.org/projects/pipal.php>
- SimpleRisk The Enterprise Risk Management Simplified >> <http://www.simplerisk.org/>
- Security Research and Development Framework >> <https://github.com/AmrThabet/winSRDF>
- Hackbar Firefox extension for testing Application Security >> <https://addons.mozilla.org/en-US/firefox/addon/hackbar/>
- Python – The Programming Language >> <http://www.python.org/>
- Websecurify Web Application Security Toolkit >> <http://www.websecurify.com>

Malware

NIST defines malware as:

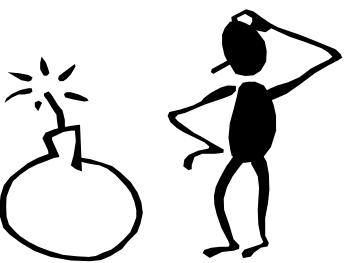
“a program that is inserted into a system, usually covertly, with the intent of compromising the confidentiality, integrity, or availability of the victim’s data, applications, or operating system or otherwise annoying or disrupting the victim.”



Name	Description	Trojan horse	A computer program that appears to have a useful function, but also has a hidden and potentially malicious function that evades security mechanisms, sometimes by exploiting legitimate authorizations of a system entity that invokes the Trojan horse program.
Advanced persistent threat	Cybercrime directed at business and political targets, using a wide variety of intrusion technologies and malware, applied persistently and effectively to specific targets over an extended period, often attributed to state-sponsored organizations.		
Adware	Advertising that is integrated into software. It can result in pop-up ads or redirection of a browser to a commercial site.		
Attack Kit	Set of tools for generating new malware automatically using a variety of supplied propagation and payload mechanisms.		
Auto-rooter	Malicious hacker tools used to break into new machines remotely.		
Backdoor (trapdoor)	Any mechanisms that bypasses a normal security check; it may allow unauthorized access to functionality in a program, or onto a compromised system.		
Downloaders	Code that installs other items on a machine that is under attack. It is normally included in the malware code first inserted on to a compromised system to then import a larger malware package.		
Drive-by download	An attack using code in a compromised web site that exploits a browser vulnerability to attack a client system when the site is viewed.		
Exploits	Code specific to a single vulnerability or set of vulnerabilities.		
Flooders (DoS client)	Used to generate a large volume of data to attack networked computer systems, by carrying out some form of denial-of-service (DoS) attack.		
Keyloggers	Captures keystrokes on a compromised system.		
Logic bomb	Code inserted into malware by an intruder. A logic bomb lies dormant until a predefined condition is met; the code then triggers an unauthorized act.		
Macro Virus	A type of virus that uses macro or scripting code, typically embedded in a document, and triggered when the document is viewed or edited, to run and replicate itself into other such documents.		
Mobile Code	Software (e.g., script, macro, or other portable instruction) that can be shipped unchanged to a heterogeneous collection of platforms and execute with identical semantics.		
Rootkit	Set of hacker tools used after attacker has broken into a computer system and gained root-level access.		
Spammer Programs	Used to send large volumes of unwanted e-mail.		
Spyware	Software that collects information from a computer and transmits it to another system by monitoring keystrokes, screen data and/or network traffic; or by scanning files on the system for sensitive information.		

Table

Malware Terminology



Classification of Malware

Classified into two broad categories:

Based first on how it spreads or propagates to reach the desired targets

Then on the actions or payloads it performs once a target is reached

Also classified by:

Those that need a host program (parasitic code such as viruses)

Those that are independent, self-contained programs (worms, trojans, and bots)

Malware that does not replicate (trojans and spam e-mail)

Malware that does replicate (viruses and worms)

Types of Malicious Software (Malware)

Propagation mechanisms include:

- Infection of existing content by viruses that is subsequently spread to other systems
- Exploit of software vulnerabilities by worms or drive-by-downloads to allow the malware to replicate
- Social engineering attacks that convince users to bypass security mechanisms to install Trojans or to respond to phishing attacks



Payload Actions include

Four broad categories of payloads that malware may carry

- Corruption of system or data files
- Theft of service/make the system a zombie agent of attack as part of a botnet
- Theft of information from the system/keylogging
- Stealthing/hiding its presence on the system

Attack Kits

- Initially the development and deployment of malware required considerable technical skill by software authors
 - The development of virus-creation toolkits in the early 1990s and then more general attack kits in the 2000s greatly assisted in the development and deployment of malware
- Toolkits are often known as “crimeware”
 - Include a variety of propagation mechanisms and payload modules that even novices can deploy
 - Variants that can be generated by attackers using these toolkits creates a significant problem for those defending systems against them
- Widely used toolkits include:
 - Zeus
 - Blackhole
 - Sakura
 - Phoenix

Advanced Persistent Threats (APTs)

- Well-resourced, persistent application of a wide variety of intrusion technologies and malware to selected targets (usually business or political)
- Typically attributed to state-sponsored organizations and criminal enterprises
- Differ from other types of attack by their careful target selection and stealthy intrusion efforts over extended periods
- High profile attacks include Aurora, RSA, APT1, and Stuxnet

APT Attacks

- Aim:
 - Varies from theft of intellectual property or security and infrastructure related data to the physical disruption of infrastructure
- Techniques used:
 - Social engineering
 - Spear-phishing email
 - Drive-by-downloads from selected compromised websites likely to be visited by personnel in the target organization
- Intent:
 - To infect the target with sophisticated malware with multiple propagation mechanisms and payloads
 - Once they have gained initial access to systems in the target organization a further range of attack tools are used to maintain and extend their access



Viruses



- Piece of software that infects programs
 - Modifies them to include a copy of the virus
 - Replicates and goes on to infect other content
 - Easily spread through network environments
- When attached to an executable program a virus can do anything that the program is permitted to do
 - Executes secretly when the host program is run
- Specific to operating system and hardware
 - Takes advantage of their details and weaknesses

Virus Components



Infection mechanism

- Means by which a virus spreads or propagates
- Also referred to as the *infection vector*

Trigger

- Event or condition that determines when the payload is activated or delivered
- Sometimes known as a *logic bomb*

Payload

- What the virus does (besides spreading)
- May involve damage or benign but noticeable activity



Virus Phases

Dormant phase

Virus is idle

Will eventually be activated by some event

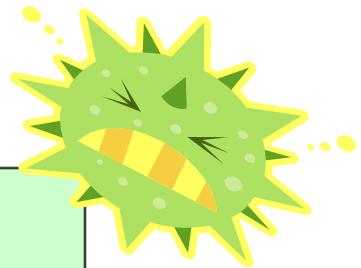
Not all viruses have this stage

Triggering phase

Propagation phase

Execution phase

Virus Structure



```
program V
1234567;

procedure attach-to-program;
begin
repeat
    file := get-random-program;
until first-program-line ≠ 1234567;
prepend V to file;
end;

procedure execute-payload;
begin
    (* perform payload actions *)
end;

procedure trigger-condition;
begin
    (* return true if trigger condition is true *)
end;

begin (* main action block *)
    attach-to-program;
    if trigger-condition then execute-payload;
    goto main;
end;
```

(a) A simple virus

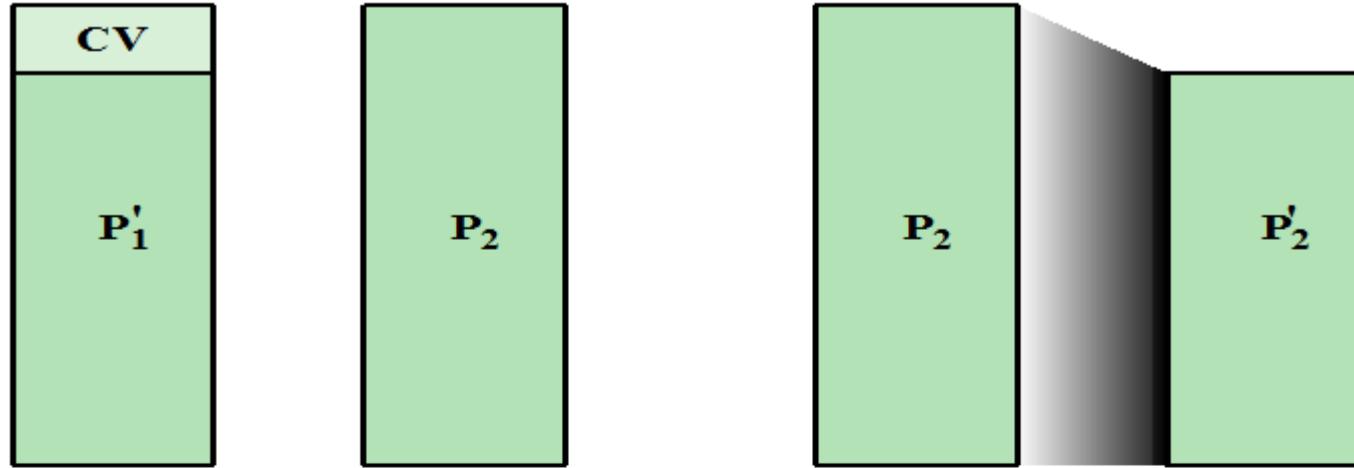
```
program CV
1234567;

procedure attach-to-program;
begin
repeat
    file := get-random-program;
until first-program-line ≠ 1234567;
compress file; (* t1 *)
prepend CV to file; (* t2 *)
end;

begin (* main action block *)
    attach-to-program;
    uncompress rest of this file into tempfile; (* t3 *)
    execute tempfile; (* t4 *)
end;
```

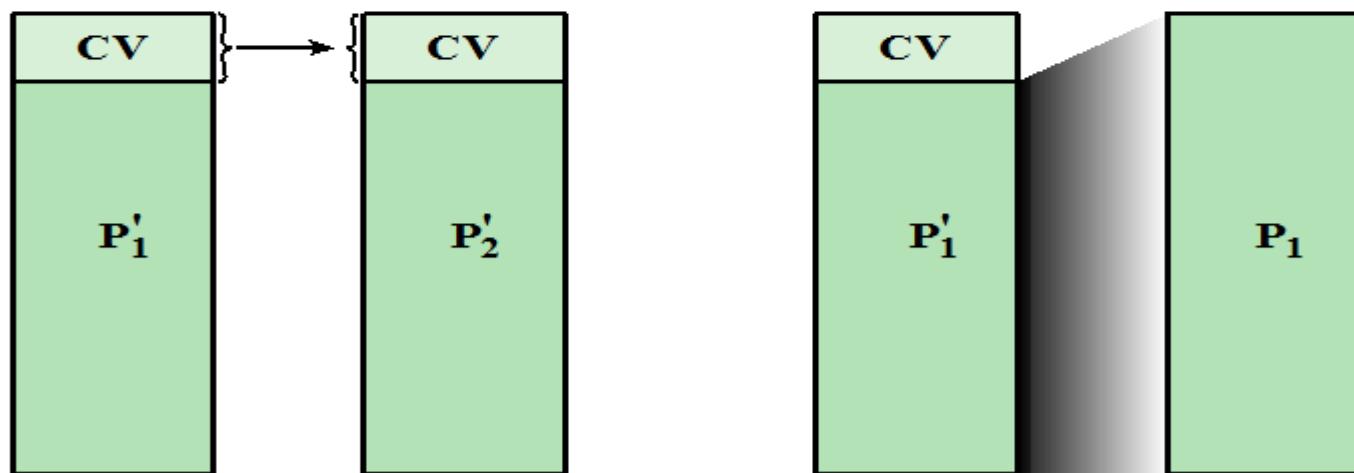
(b) A compression virus

Example Virus Logic



t_0 : P'_1 is infected version of P_1 ;
 P_2 is clean

t_1 : P_2 is compressed into P'_1



t_2 : CV attaches itself to P'_1

t_3 : P'_1 is decompressed into the
original program P_1



Virus Classifications

Classification by target

- Boot sector infector
 - Infects a master boot record or boot record and spreads when a system is booted from the disk containing the virus
- File infector
 - Infects files that the operating system or shell considers to be executable
- Macro virus
 - Infects files with macro or scripting code that is interpreted by an application
- Multipartite virus
 - Infects files in multiple ways

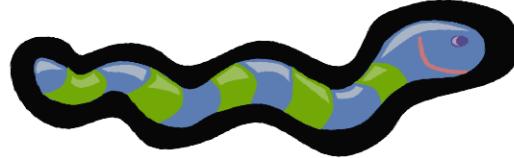
Classification by concealment strategy

- Encrypted virus
 - A portion of the virus creates a random encryption key and encrypts the remainder of the virus
- Stealth virus
 - A form of virus explicitly designed to hide itself from detection by anti-virus software
- Polymorphic virus
 - A virus that mutates with every infection
- Metamorphic virus
 - A virus that mutates and rewrites itself completely at each iteration and may change behavior as well as appearance

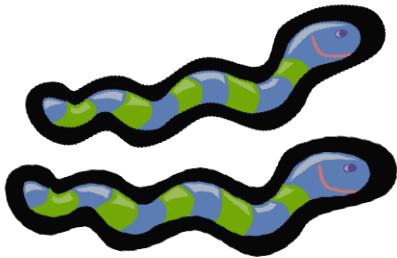
Macro and Scripting Viruses

- Very common in mid-1990s
 - Platform independent
 - Infect documents (not executable portions of code)
 - Easily spread
- Exploit macro capability of MS Office applications
 - More recent releases of products include protection
- Various anti-virus programs have been developed so these are no longer the predominant virus threat

Worms



- Program that actively seeks out more machines to infect and each infected machine serves as an automated launching pad for attacks on other machines
- Exploits software vulnerabilities in client or server programs
- Can use network connections to spread from system to system
- Spreads through shared media (USB drives, CD, DVD data disks)
- E-mail worms spread in macro or script code included in attachments and instant messenger file transfers
- Upon activation the worm may replicate and propagate again
- Usually carries some form of payload
- First known implementation was done in Xerox Palo Alto Labs in the early 1980s



Worm Replication

Electronic mail or instant messenger facility

- Worm e-mails a copy of itself to other systems
- Sends itself as an attachment via an instant message service

File sharing

- Creates a copy of itself or infects a file as a virus on removable media

Remote execution capability

- Worm executes a copy of itself on another system

Remote file access or transfer capability

- Worm uses a remote file access or transfer service to copy itself from one system to the other

Remote login capability

- Worm logs onto a remote system as a user and then uses commands to copy itself from one system to the other

Target Discovery

- Scanning (or fingerprinting)
 - First function in the propagation phase for a network worm
 - Searches for other systems to infect

Scanning strategies that a worm can use:

- Random

- Each compromised host probes random addresses in the IP address space using a different seed
 - This produces a high volume of Internet traffic which may cause generalized disruption even before the actual attack is launched

- Hit-list

- The attacker first compiles a long list of potential vulnerable machines
 - Once the list is compiled the attacker begins infecting machines on the list
 - Each infected machine is provided with a portion of the list to scan
 - This results in a very short scanning period which may make it difficult to detect that infection is taking place

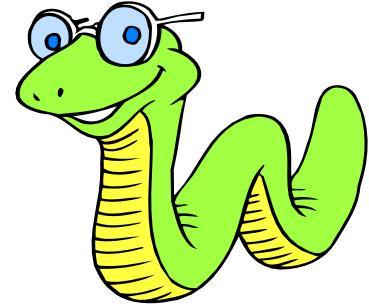
- Topological

- This method uses information contained on an infected victim machine to find more hosts to scan

- Local subnet

- If a host can be infected behind a firewall that host then looks for targets in its own local network
 - The host uses the subnet address structure to find other hosts that would otherwise be protected by the firewall

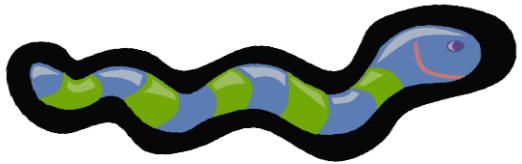
Morris Worm



- Earliest significant worm infection
- Released by Robert Morris in 1988
- Designed to spread on UNIX systems
 - Attempted to crack local password file to use login/password to logon to other systems
 - Exploited a bug in the finger protocol which reports the whereabouts of a remote user
 - Exploited a trapdoor in the debug option of the remote process that receives and sends mail
- Successful attacks achieved communication with the operating system command interpreter
 - Sent interpreter a bootstrap program to copy worm over

Recent Worm Attacks

Melissa	1998	e-mail worm first to include virus, worm and Trojan in one package
Code Red	July 2001	exploited Microsoft IIS bug probes random IP addresses consumes significant Internet capacity when active
Code Red II	August 2001	also targeted Microsoft IIS installs a backdoor for access
Nimda	September 2001	had worm, virus and mobile code characteristics spread using e-mail, Windows shares, Web servers, Web clients, backdoors
SQL Slammer	Early 2003	exploited a buffer overflow vulnerability in SQL server compact and spread rapidly
Sobig.F	Late 2003	exploited open proxy servers to turn infected machines into spam engines
Mydoom	2004	mass-mailing e-mail worm installed a backdoor in infected machines
Warezov	2006	creates executables in system directories sends itself as an e-mail attachment can disable security related products
Conficker (Downadup)	November 2008	exploits a Windows buffer overflow vulnerability most widespread infection since SQL Slammer
Stuxnet	2010	restricted rate of spread to reduce chance of detection targeted industrial control systems



Worm Technology

Multiplatform

Metamorphic

Multi-exploit

Polymorphic

Ultrafast
spreading

Mobile Code

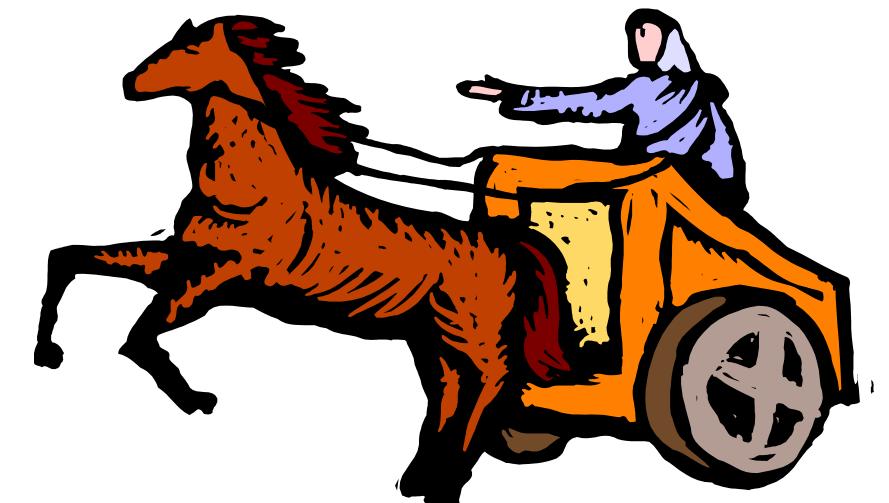
- Programs that can be shipped unchanged to a variety of platforms
- Transmitted from a remote system to a local system and then executed on the local system
- Often acts as a mechanism for a virus, worm, or Trojan horse
- Takes advantage of vulnerabilities to perform its own exploits
- Popular vehicles include Java applets, ActiveX, JavaScript and VBScript

Mobile Phone Worms

- First discovery was Cabir worm in 2004
- Then Lasco and CommWarrior in 2005
- Communicate through Bluetooth wireless connections or MMS
- Target is the smartphone
- Can completely disable the phone, delete data on the phone, or force the device to send costly messages
- CommWarrior replicates by means of Bluetooth to other phones, sends itself as an MMS file to contacts and as an auto reply to incoming text messages

Drive-By-Downloads

- Exploits browser vulnerabilities to download and installs malware on the system when the user views a Web page controlled by the attacker
- In most cases does not actively propagate
- Spreads when users visit the malicious Web page



Clickjacking

- Also known as a user-interface (UI) redress attack
- Using a similar technique, keystrokes can also be hijacked
 - A user can be led to believe they are typing in the password to their email or bank account, but are instead typing into an invisible frame controlled by the attacker
- Vulnerability used by an attacker to collect an infected user's clicks
 - The attacker can force the user to do a variety of things from adjusting the user's computer settings to unwittingly sending the user to Web sites that might have malicious code
 - By taking advantage of Adobe Flash or JavaScript an attacker could even place a button under or over a legitimate button making it difficult for users to detect
 - A typical attack uses multiple transparent or opaque layers to trick a user into clicking on a button or link on another page when they were intending to click on the top level page
 - The attacker is hijacking clicks meant for one page and routing them to another page

Social Engineering

- “Tricking” users to assist in the compromise of their own systems

Spam

Unsolicited bulk e-mail

Significant carrier of malware

Used for phishing attacks

Trojan horse

Program or utility containing harmful hidden code

Used to accomplish functions that the attacker could not accomplish directly

Mobile phone trojans

First appeared in 2004 (Skuller)

Target is the smartphone

Payload System Corruption



Chernobyl virus

- First seen in 1998
- Windows 95 and 98 virus
- Infects executable files and corrupts the entire file system when a trigger date is reached



Klez

- Mass mailing worm infecting Windows 95 to XP systems
- On trigger date causes files on the hard drive to become empty

Ransomware

- Encrypts the user's data and demands payment in order to access the key needed to recover the information
- PC Cyborg Trojan (1989)
- Gpcode Trojan (2006)



Payload System Corruption

- Real-world damage
 - Causes damage to physical equipment
 - Chernobyl virus rewrites BIOS code
 - Stuxnet worm
 - Targets specific industrial control system software
 - There are concerns about using sophisticated targeted malware for industrial sabotage
- Logic bomb
 - Code embedded in the malware that is set to “explode” when certain conditions are met

Payload – Attack Agents Bots

- Takes over another Internet attached computer and uses that computer to launch or manage attacks
- *Botnet* - collection of bots capable of acting in a coordinated manner
- Uses:
 - Distributed denial-of-service (DDoS) attacks
 - Spamming
 - Sniffing traffic
 - Keylogging
 - Spreading new malware
 - Installing advertisement add-ons and browser helper objects (BHOs)
 - Attacking IRC chat networks
 - Manipulating online polls/games



Remote Control Facility

- Distinguishes a bot from a worm
 - Worm propagates itself and activates itself
 - Bot is initially controlled from some central facility
- Typical means of implementing the remote control facility is on an IRC server
 - Bots join a specific channel on this server and treat incoming messages as commands
 - More recent botnets use covert communication channels via protocols such as HTTP
 - Distributed control mechanisms use peer-to-peer protocols to avoid a single point of failure

Payload – Information Theft, Key loggers and Spyware

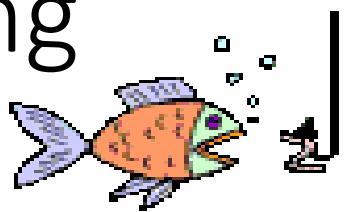
Keylogger

- Captures keystrokes to allow attacker to monitor sensitive information
- Typically uses some form of filtering mechanism that only returns information close to keywords (“login”, “password”)

Spyware

- Subverts the compromised machine to allow monitoring of a wide range of activity on the system
 - Monitoring history and content of browsing activity
 - Redirecting certain Web page requests to fake sites
 - Dynamically modifying data exchanged between the browser and certain Web sites of interest

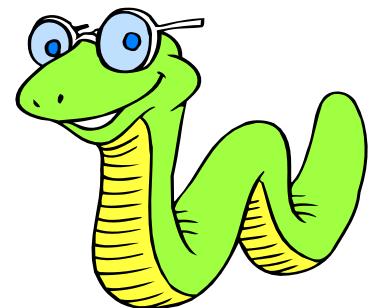
Payload – Information Theft Phishing



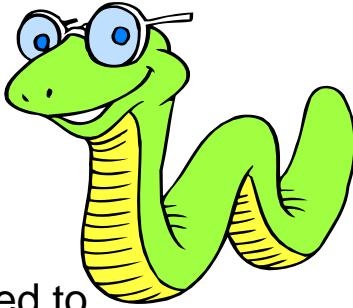
- Exploits social engineering to leverage the user's trust by masquerading as communication from a trusted source
 - Include a URL in a spam e-mail that links to a fake Web site that mimics the login page of a banking, gaming, or similar site
 - Suggests that urgent action is required by the user to authenticate their account
 - Attacker exploits the account using the captured credentials
- Spear-phishing
 - Recipients are carefully researched by the attacker
 - E-mail is crafted to specifically suit its recipient, often quoting a range of information to convince them of its authenticity

Worm Countermeasures

- Considerable overlap in techniques for dealing with viruses and worms
- Once a worm is resident on a machine anti-virus software can be used to detect and possibly remove it
- Perimeter network activity and usage monitoring can form the basis of a worm defense
- Worm defense approaches include:
 - Signature-based worm scan filtering
 - Filter-based worm containment
 - Payload-classification-based worm containment
 - Rate limiting
 - Rate halting

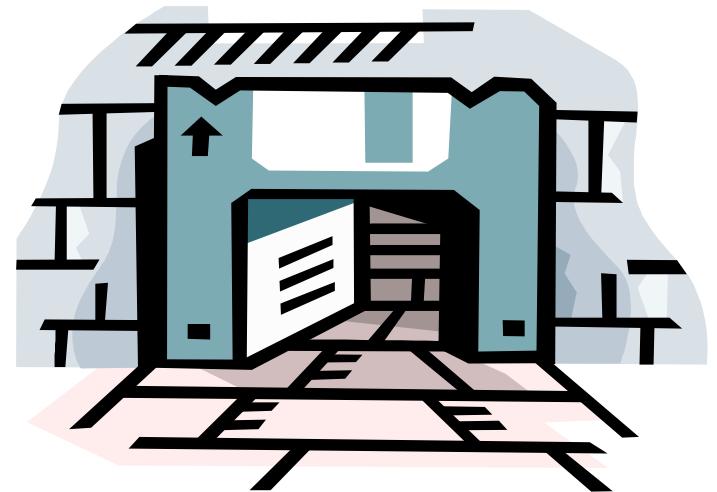


Worm Countermeasures



- **Signature-based worm scan filtering:** This type of approach generates a worm signature, which is then used to prevent worm scans from entering/leaving a network/host.
- **Filter-based worm containment:** This approach focuses on worm content rather than a scan signature. The filter checks a message to determine if it contains worm code.
- **Payload-classification-based worm containment:** These network-based techniques examine packets to see if they contain a worm. Various anomaly detection techniques can be used, but care is needed to avoid high levels of false positives or negatives.
- **Rate limiting:** Various strategies can be used, including limiting the number of new machines a host can connect to in a window of time, detecting a high connection failure rate, and limiting the number of unique IP addresses a host can scan in a window of time.
- **Rate halting:** This approach immediately blocks outgoing traffic when a threshold is exceeded either in outgoing connection rate or in diversity of connection attempts.

Payload – Stealthing Backdoor



- Also known as a *trapdoor*
- Secret entry point into a program allowing the attacker to gain access and bypass the security access procedures
- *Maintenance hook* is a backdoor used by Programmers to debug and test programs
- Difficult to implement operating system controls for backdoors in applications

Payload – Stealthing Rootkit

- Set of hidden programs installed on a system to maintain covert access to that system
- Hides by subverting the mechanisms that monitor and report on the processes, files, and registries on a computer
- Gives administrator (or root) privileges to attacker
 - Can add or change programs and files, monitor processes, send and receive network traffic, and get backdoor access on demand

Rootkit Classification Characteristics

Persistent

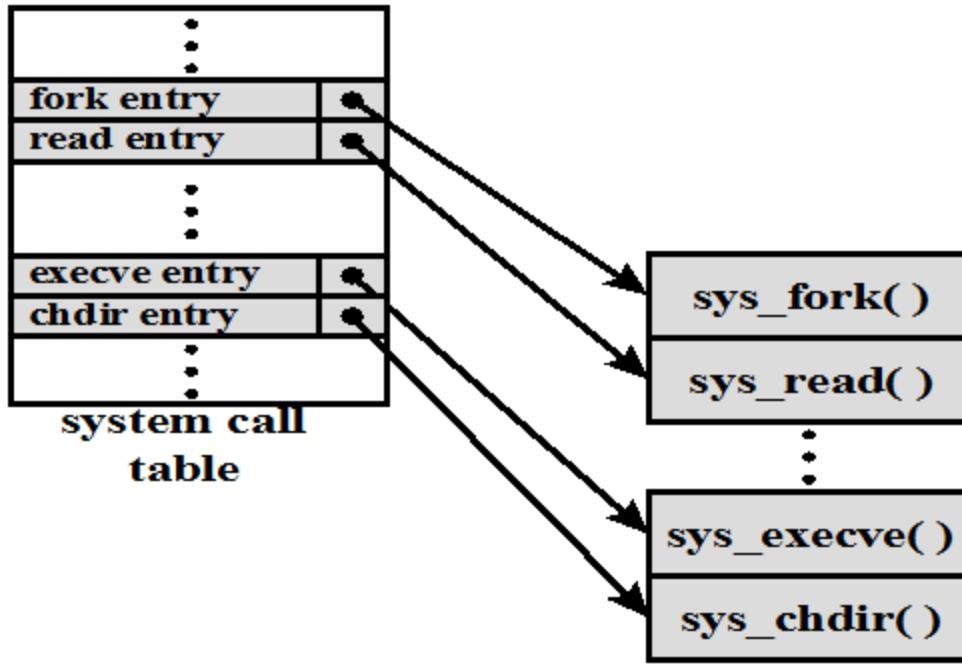
Memory
based

User mode

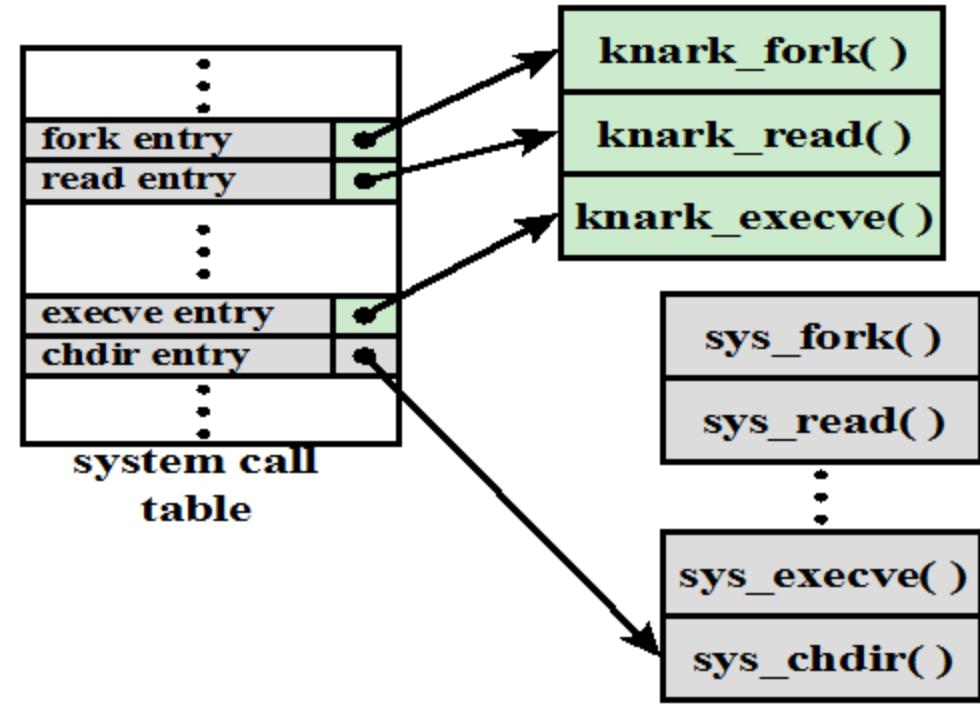
Kernel mode

Virtual
machine
based

External
mode



(a) Normal kernel memory layout



(b) After nkark install

System Call Table Modification by Rootkit

Malware Countermeasure Approaches

- Ideal solution to the threat of malware is prevention

Four main elements of prevention:

- Policy
- Awareness
- Vulnerability mitigation
- Threat mitigation

- If prevention fails, technical mechanisms can be used to support the following threat mitigation options:
 - Detection
 - Identification
 - Removal

Generations of Anti-Virus Software

First generation: simple scanners

- Requires a malware signature to identify the malware
- Limited to the detection of known malware

Second generation: heuristic scanners

- Uses heuristic rules to search for probable malware instances
- Another approach is integrity checking

Third generation: activity traps

- Memory-resident programs that identify malware by its actions rather than its structure in an infected program

Fourth generation: full-featured protection

- Packages consisting of a variety of anti-virus techniques used in conjunction
- Include scanning and activity trap components and access control capability

Generic Decryption (GD)

- Enables the anti-virus program to easily detect complex polymorphic viruses and other malware while maintaining fast scanning speeds
- Executable files are run through a GD scanner which contains the following elements:
 - CPU emulator
 - Virus signature scanner
 - Emulation control module
- The most difficult design issue with a GD scanner is to determine how long to run each interpretation

Host-Based Behavior-Blocking Software

- Integrates with the operating system of a host computer and monitors program behavior in real time for malicious action
 - Blocks potentially malicious actions before they have a chance to affect the system
 - Blocks software in real time so it has an advantage over anti-virus detection techniques such as fingerprinting or heuristics

Limitations

- Because malicious code must run on the target machine before all its behaviors can be identified, it can cause harm before it has been detected and blocked

Lecture 7

Denial-of-Service Attack

CMPU-4008

Advance Security 2

Denial-of-Service (DoS) Attack

The NIST Computer Security Incident Handling Guide defines a DoS attack as:

“An action that prevents or impairs the authorized use of networks, systems, or applications by exhausting resources such as central processing units (CPU), memory, bandwidth, and disk space.”



Denial-of-Service (DoS)

- A form of attack on the availability of some service
- Categories of resources that could be attacked are:

Network bandwidth

Relates to the capacity of the network links connecting a server to the Internet

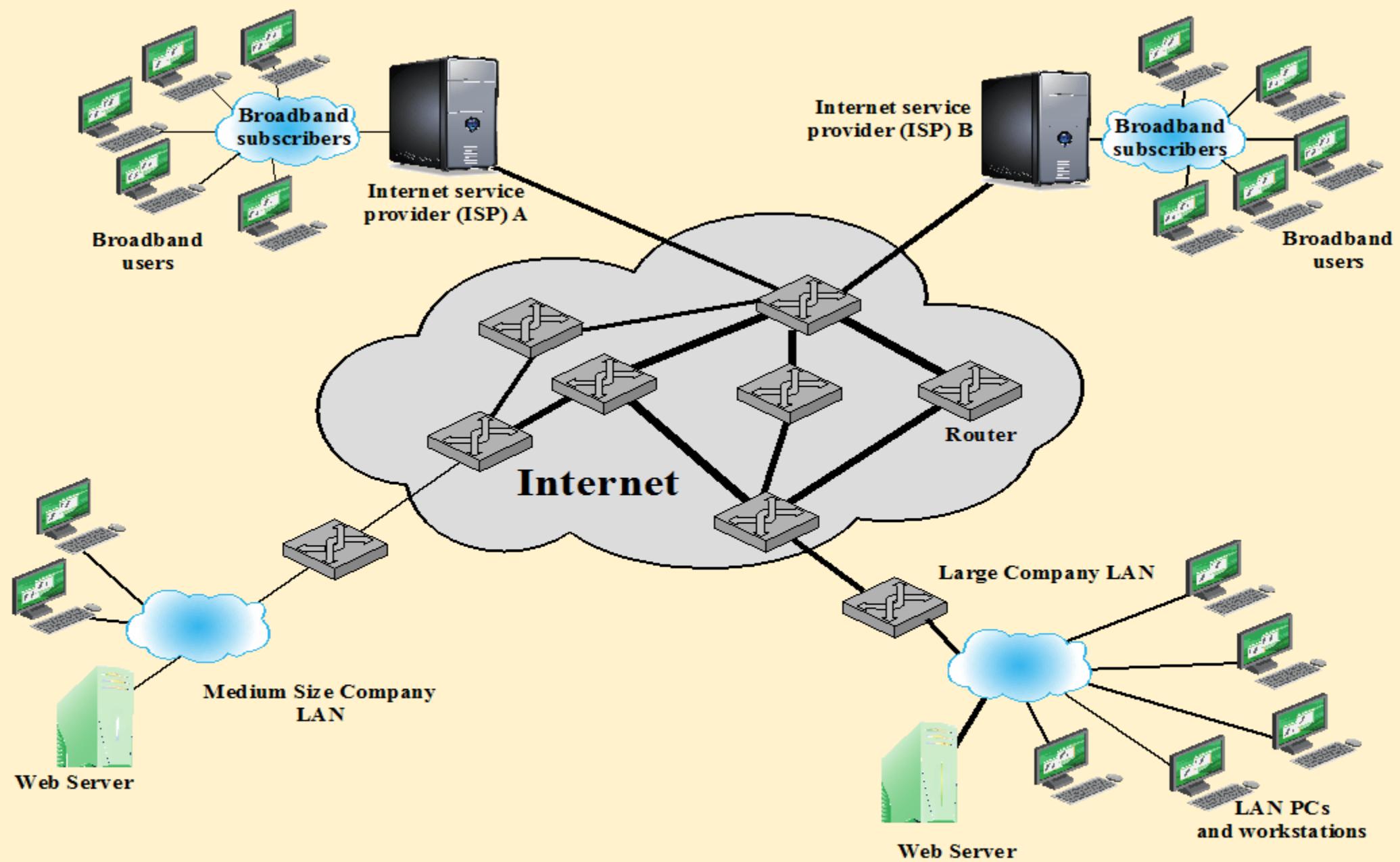
For most organizations this is their connection to their Internet Service Provider (ISP)

System resources

Aims to overload or crash the network handling software

Application resources

Typically involves a number of valid requests, each of which consumes significant resources, thus limiting the ability of the server to respond to requests from other users

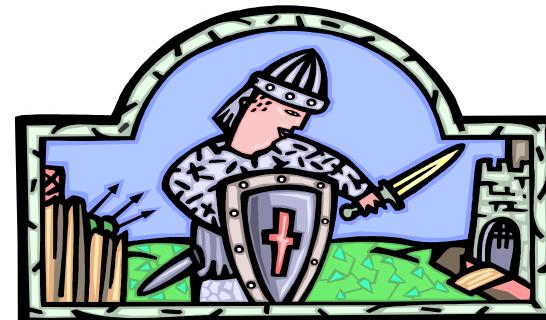


Example Network to Illustrate DoS Attacks

Classic DoS Attacks

- Flooding ping command

- Aim of this attack is to overwhelm the capacity of the network connection to the target organization
- Traffic can be handled by higher capacity links on the path, but packets are discarded as capacity decreases
- Source of the attack is clearly identified unless a spoofed address is used
- Network performance is noticeably affected

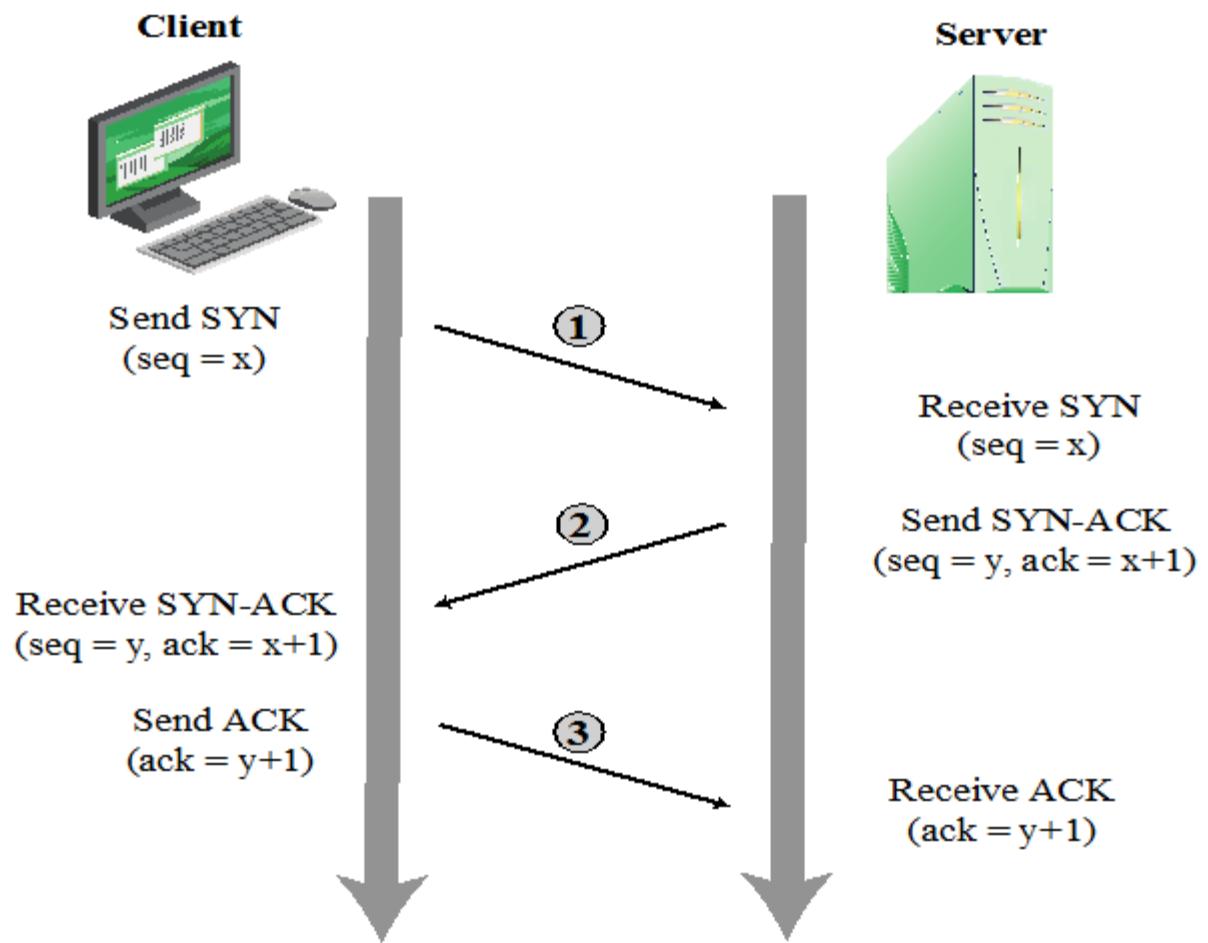


Source Address Spoofing

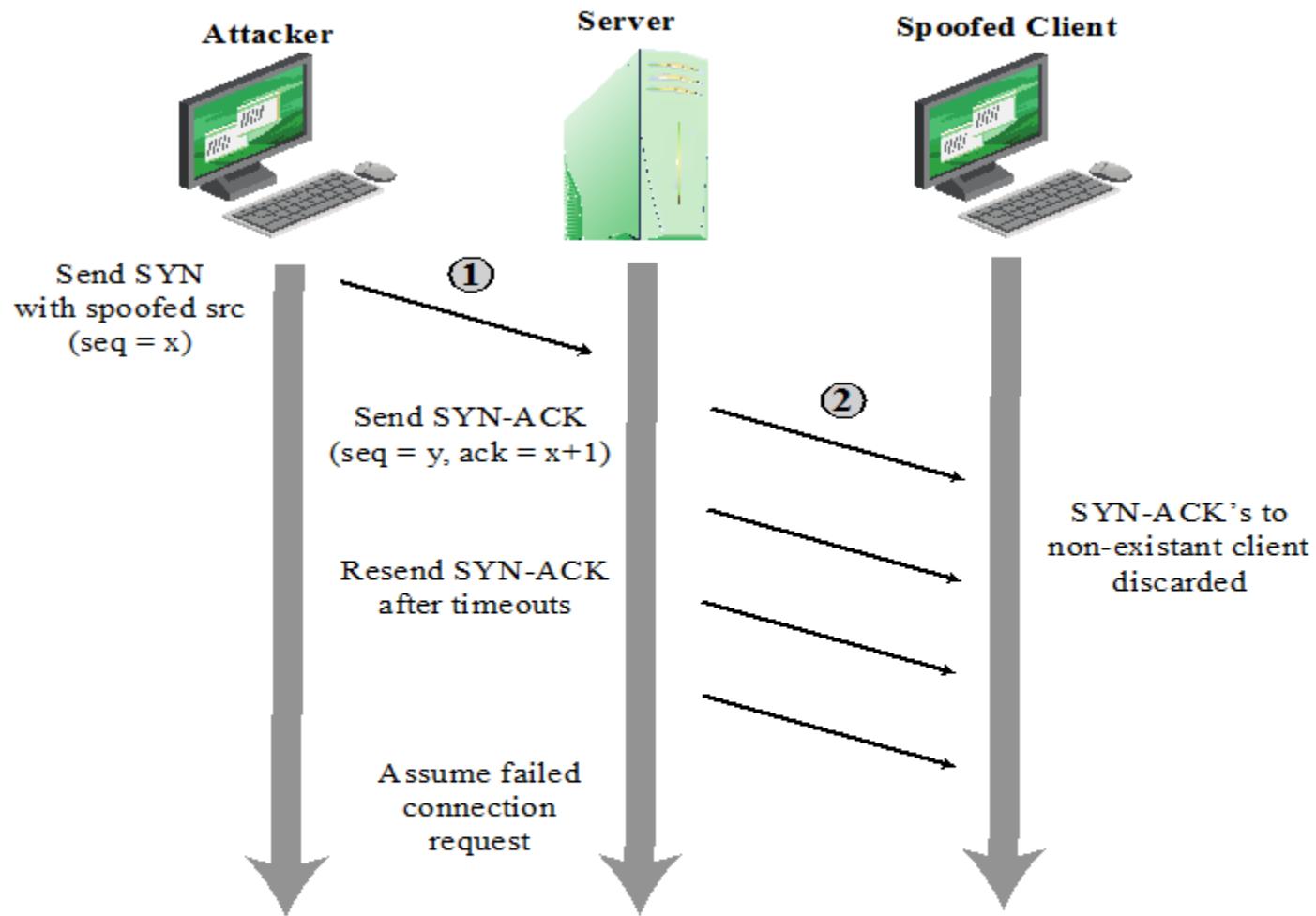
- Use forged source addresses
 - Usually via the raw socket interface on operating systems
 - Makes attacking systems harder to identify
- Attacker generates large volumes of packets that have the target system as the destination address
- Congestion would result in the router connected to the final, lower capacity link
- Requires network engineers to specifically query flow information from their routers
- *Backscatter traffic*
 - Advertise routes to unused IP addresses to monitor attack traffic

SYN Spoofing

- Common DoS attack
- Attacks the ability of a server to respond to future connection requests by overflowing the tables used to manage them
- Thus legitimate users are denied access to the server
- Hence an attack on system resources, specifically the network handling code in the operating system



TCP Three-Way Connection Handshake



TCP SYN Spoofing Attack

Flooding Attacks

- Classified based on network protocol used
- Intent is to overload the network capacity on some link to a server
- Virtually any type of network packet can be used

ICMP flood

- Ping flood using ICMP echo request packets
- Traditionally network administrators allow such packets into their networks because ping is a useful network diagnostic tool

UDP flood

- Uses UDP packets directed to some port number on the target system

TCP SYN flood

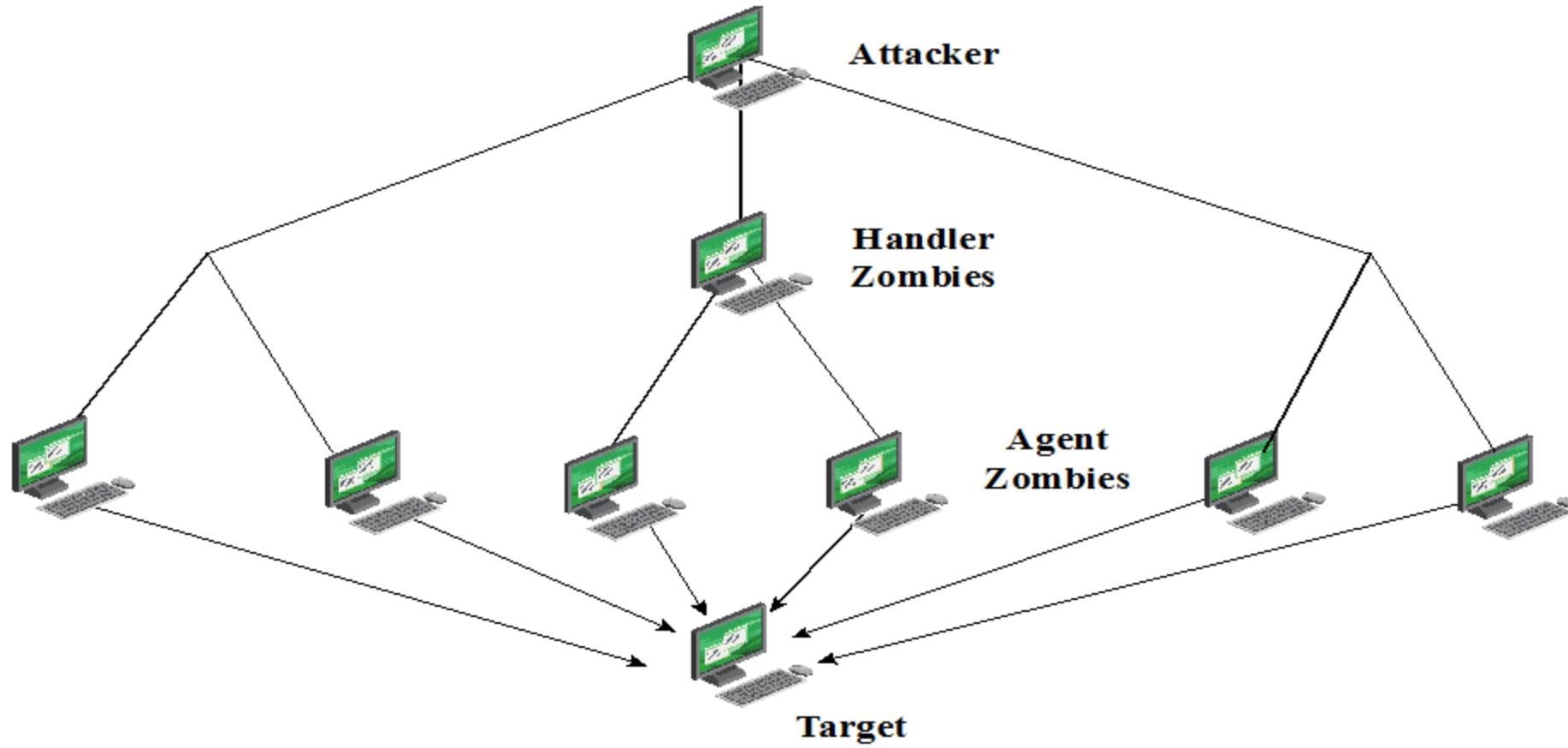
- Sends TCP packets to the target system
- Total volume of packets is the aim of the attack rather than the system code

Distributed Denial of Service DDoS Attacks

Use of multiple systems to generate attacks

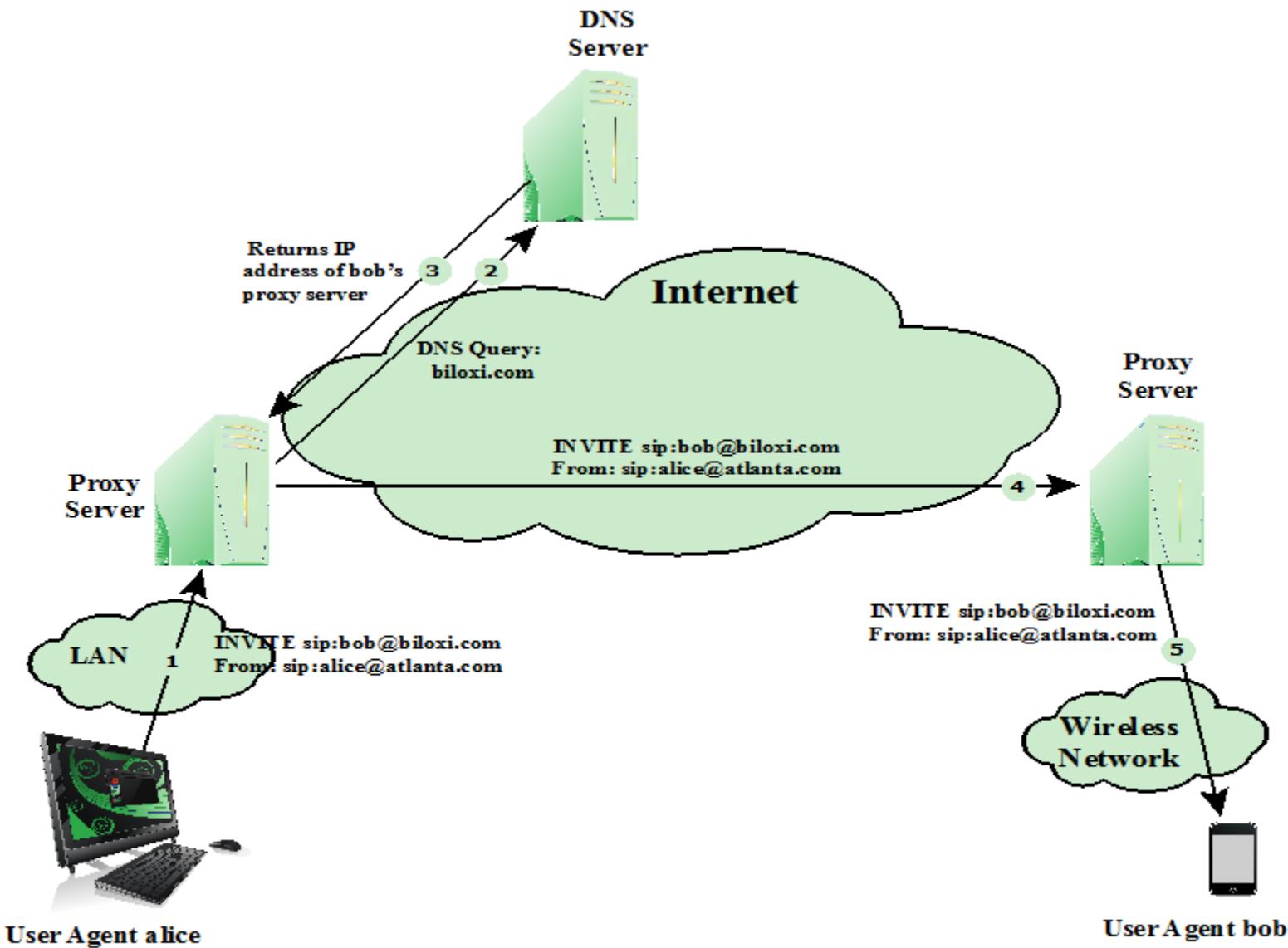
Attacker uses a flaw in operating system or in a common application to gain access and installs their program on it (zombie)

Large collections of such systems under the control of one attacker's control can be created, forming a botnet



DDoS Attack Architecture

Application Based Bandwidth Attacks



SIP INVITE Scenario

Application Based Bandwidth Attacks

(HTTP) Based Attacks

HTTP flood

- Attack that bombards Web servers with HTTP requests
- Consumes considerable resources
- Spidering
 - Bots starting from a given HTTP link and following all links on the provided Web site in a recursive way

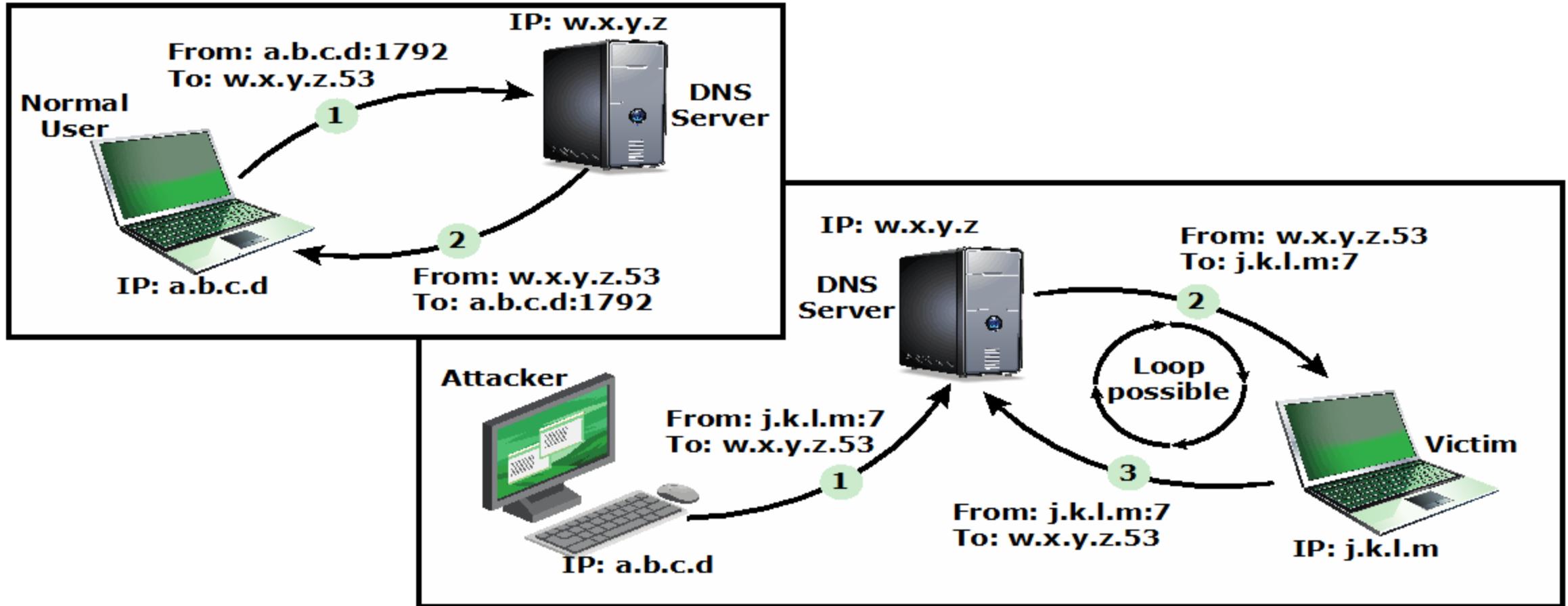
Slowloris

- Attempts to monopolize by sending HTTP requests that never complete
- Eventually consumes Web server's connection capacity
- Utilizes legitimate HTTP traffic
- Existing intrusion detection and prevention solutions that rely on signatures to detect attacks will generally not recognize Slowloris

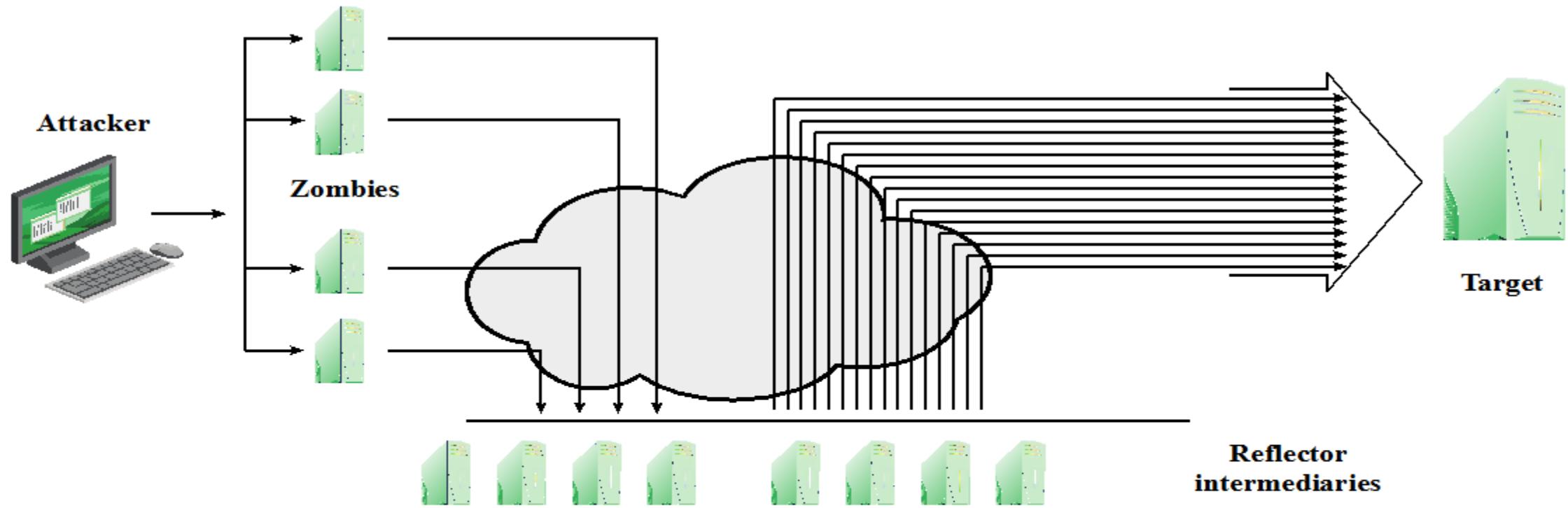
Reflection Attacks



- Attacker sends packets to a known service on the intermediary with a spoofed source address of the actual target system
- When intermediary responds, the response is sent to the target
- “Reflects” the attack off the intermediary (reflector)
- Goal is to generate enough volumes of packets to flood the link to the target system without alerting the intermediary
- The basic defense against these attacks is blocking spoofed-source packets



DNS Reflection Attack



Amplification Attack

DNS Amplification Attacks

- Use packets directed at a legitimate DNS server as the intermediary system
- Attacker creates a series of DNS requests containing the spoofed source address of the target system
- Exploit DNS behavior to convert a small request to a much larger response (amplification)
- Target is flooded with responses
- Basic defense against this attack is to prevent the use of spoofed source addresses

DoS Attack Defenses

- These attacks cannot be prevented entirely
- High traffic volumes may be legitimate
 - High publicity about a specific site
 - Activity on a very popular site
 - Described as *slashdotted, flash crowd, or flash event*

Four lines of defense against DDoS attacks

Attack prevention and preemption

- Before attack

Attack detection and filtering

- During the attack

Attack source traceback and identification

- During and after the attack

Attack reaction

- After the attack

DoS Attack Prevention

- Block spoofed source addresses

- On routers as close to source as possible

- Filters may be used to ensure path back to the claimed source address is the one being used by the current packet

- Filters must be applied to traffic before it leaves the ISP's network or at the point of entry to their network

- Use modified TCP connection handling code

- Cryptographically encode critical information in a cookie that is sent as the server's initial sequence number
 - Legitimate client responds with an ACK packet containing the incremented sequence number cookie
 - Drop an entry for an incomplete connection from the TCP connections table when it overflows

DoS Attack Prevention

- Block IP directed broadcasts
- Block suspicious services and combinations
- Manage application attacks with a form of graphical puzzle (captcha) to distinguish legitimate human requests
- Good general system security practices
- Use mirrored and replicated servers when high-performance and reliability is required

Responding to DoS Attacks

Good Incident Response Plan

- Details on how to contact technical personal for ISP
- Needed to impose traffic filtering upstream
- Details of how to respond to the attack

- Antispoofing, directed broadcast, and rate limiting filters should have been implemented
- Ideally have network monitors and IDS to detect and notify abnormal traffic patterns

Responding to DoS Attacks

- Identify type of attack
 - Capture and analyze packets
 - Design filters to block attack traffic upstream
 - Or identify and correct system/application bug
- Have ISP trace packet flow back to source
 - May be difficult and time consuming
 - Necessary if planning legal action
- Implement contingency plan
 - Switch to alternate backup servers
 - Commission new servers at a new site with new addresses
- Update incident response plan
 - Analyze the attack and the response for future handling



Lecture 8

Intrusion Detection

CMPU-4008

Advance Security 2

Classes of Intruders – Cyber Criminals

- Individuals or members of an organized crime group with a goal of financial reward
- Their activities may include:
 - Identity theft
 - Theft of financial credentials
 - Corporate espionage
 - Data theft
 - Data ransoming
- Typically they are young, often Eastern European, Russian, or southeast Asian hackers, who do business on the Web
- They meet in underground forums to trade tips and data and coordinate attacks



Classes of Intruders – Activists

- Are either individuals, usually working as insiders, or members of a larger group of outsider attackers, who are motivated by social or political causes
- Also known as hacktivists
 - Skill level is often quite low
- Aim of their attacks is often to promote and publicize their cause typically through:
 - Website defacement
 - Denial of service attacks
 - Theft and distribution of data that results in negative publicity or compromise of their targets

Classes of Intruders – State-Sponsored Organizations

- Groups of hackers sponsored by governments to conduct espionage or sabotage activities
- Also known as Advanced Persistent Threats (APTs) due to the covert nature and persistence over extended periods involved with any attacks in this class
- Widespread nature and scope of these activities by a wide range of countries from China to the USA, UK, and their intelligence allies



Classes of Intruders – Others

- Hackers with motivations other than those previously listed
- Include classic hackers or crackers who are motivated by technical challenge or by peer-group esteem and reputation
- Many of those responsible for discovering new categories of buffer overflow vulnerabilities could be regarded as members of this class
- Given the wide availability of attack toolkits, there is a pool of “hobby hackers” using them to explore system and network security

Intruder Skill Levels – Apprentice

- Hackers with minimal technical skill who primarily use existing attack toolkits
- They likely comprise the largest number of attackers, including many criminal and activist attackers
- Given their use of existing known tools, these attackers are the easiest to defend against
- Also known as “script-kiddies” due to their use of existing scripts (tools)



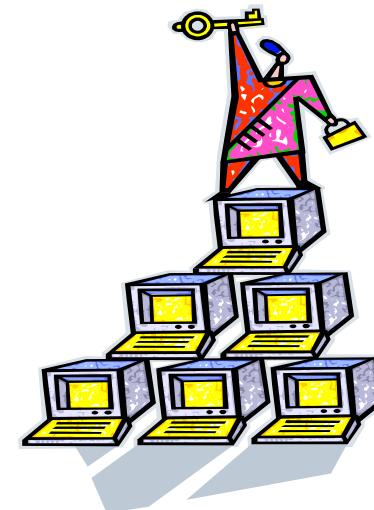
Intruder Skill Levels – Journeymen

- Hackers with sufficient technical skills to modify and extend attack toolkits to use newly discovered, or purchased, vulnerabilities
- They may be able to locate new vulnerabilities to exploit that are similar to some already known
- Hackers with such skills are likely found in all intruder classes
- Adapt tools for use by others



Intruder Skill Levels – Master

- Hackers with high-level technical skills capable of discovering brand new categories of vulnerabilities
- Write new powerful attack toolkits
- Some of the better known classical hackers are of this level
- Some are employed by state-sponsored organizations
- Defending against these attacks is of the highest difficulty



Examples of Intrusion

- Remote root compromise
- Web server defacement
- Guessing/cracking passwords
- Copying databases containing credit card numbers
- Viewing sensitive data without authorization
- Running a packet sniffer
- Distributing pirated software
- Using an unsecured modem to access internal network
- Impersonating an executive to get information
- Using an unattended workstation



Intruder Behavior

Target acquisition
and information
gathering

Initial access

Privilege
escalation

Information
gathering or
system exploit

Maintaining
access

Covering tracks

(a) Target Acquisition and Information Gathering

- Explore corporate website for information on corporate structure, personnel, key systems, as well as details of specific web server and OS used.
- Gather information on target network using DNS lookup tools such as dig, host, and others; and query WHOIS database.
- Map network for accessible services using tools such as NMAP.
- Send query email to customer service contact, review response for information on mail client, server, and OS used, and also details of person responding.
- Identify potentially vulnerable services, eg vulnerable web CMS.

(b) Initial Access

- Brute force (guess) a user's web content management system (CMS) password.
- Exploit vulnerability in web CMS plugin to gain system access.
- Send spear-phishing email with link to web browser exploit to key people.

(c) Privilege Escalation

- Scan system for applications with local exploit.
- Exploit any vulnerable application to gain elevated privileges.
- Install sniffers to capture administrator passwords.
- Use captured administrator password to access privileged information.

(d) Information Gathering or System Exploit

- Scan files for desired information.
- Transfer large numbers of documents to external repository.
- Use guessed or captured passwords to access other servers on network.

(e) Maintaining Access

- Install remote administration tool or rootkit with backdoor for later access.
- Use administrator password to later access network.
- Modify or disable anti-virus or IDS programs running on system.

(f) Covering Tracks

- Use rootkit to hide files installed on system.
- Edit logfiles to remove entries generated during the intrusion.

Table 8.1

Examples of Intruder Behavior



Definitions from RFC 2828 (Internet Security Glossary)

Security Intrusion: A security event, or a combination of multiple security events, that constitutes a security incident in which an intruder gains, or attempts to gain, access to a system (or system resource) without having authorization to do so.

Intrusion Detection: A security service that monitors and analyzes system events for the purpose of finding, and providing real-time or near real-time warning of, attempts to access system resources in an unauthorized manner.

Intrusion Detection System (IDS)

- Host-based IDS (HIDS)
 - Monitors the characteristics of a single host for suspicious activity
- Network-based IDS (NIDS)
 - Monitors network traffic and analyzes network, transport, and application protocols to identify suspicious activity
- Distributed or hybrid IDS
 - Combines information from a number of sensors, often both host and network based, in a central analyzer that is able to better identify and respond to intrusion activity



Comprises three logical components:

- Sensors - collect data
- Analyzers - determine if intrusion has occurred
- User interface - view output or control system behavior

Characteristics of an IDS

Run continually

Be fault tolerant

Resist subversion

Impose a minimal overhead on system

Configured according to system security policies

Adapt to changes in systems and users

Scale to monitor large numbers of systems

Provide graceful degradation of service

Allow dynamic reconfiguration

Analysis Approaches

Anomaly detection

- Involves the collection of data relating to the behavior of legitimate users over a period of time
- Current observed behavior is analyzed to determine whether this behavior is that of a legitimate user or that of an intruder

Signature/Heuristic detection

- Uses a set of known malicious data patterns or attack rules that are compared with current behavior
- Also known as misuse detection
- Can only identify known attacks for which it has patterns or rules

Anomaly Detection

Three broad categories of classification for Anomaly Detection are

Statistical

- Analysis of the observed behavior using univariate, multivariate, or time-series models of observed metrics

Knowledge based

- Approaches use an expert system that classifies observed behavior according to a set of rules that model legitimate behavior

Machine-learning

- Approaches automatically determine a suitable classification model from the training data using data mining techniques

Signature or Heuristic Detection

Signature approaches

Match a large collection of known patterns of malicious data against data stored on a system or in transit over a network

The signatures need to be large enough to minimize the false alarm rate, while still detecting a sufficiently large fraction of malicious data

Widely used in anti-virus products, network traffic scanning proxies, and in NIDS

Rule-based heuristic identification

Involves the use of rules for identifying known penetrations or penetrations that would exploit known weaknesses

Rules can also be defined that identify suspicious behavior, even when the behavior is within the bounds of established patterns of usage

Typically rules used are specific

SNORT is an example of a rule-based NIDS

Host-Based Intrusion Detection (HIDS)

- Adds a specialized layer of security software to vulnerable or sensitive systems
- Can use either anomaly or signature and heuristic approaches
- Monitors activity to detect suspicious behavior
 - Primary purpose is to detect intrusions, log suspicious events, and send alerts
 - Can detect both external and internal intrusions



Data Sources and Sensors



A fundamental component of intrusion detection is the sensor that collects data

Common data sources include:

- System call traces
- Audit (log file) records
- File integrity checksums
- Registry access

(a) Ubuntu Linux System Calls

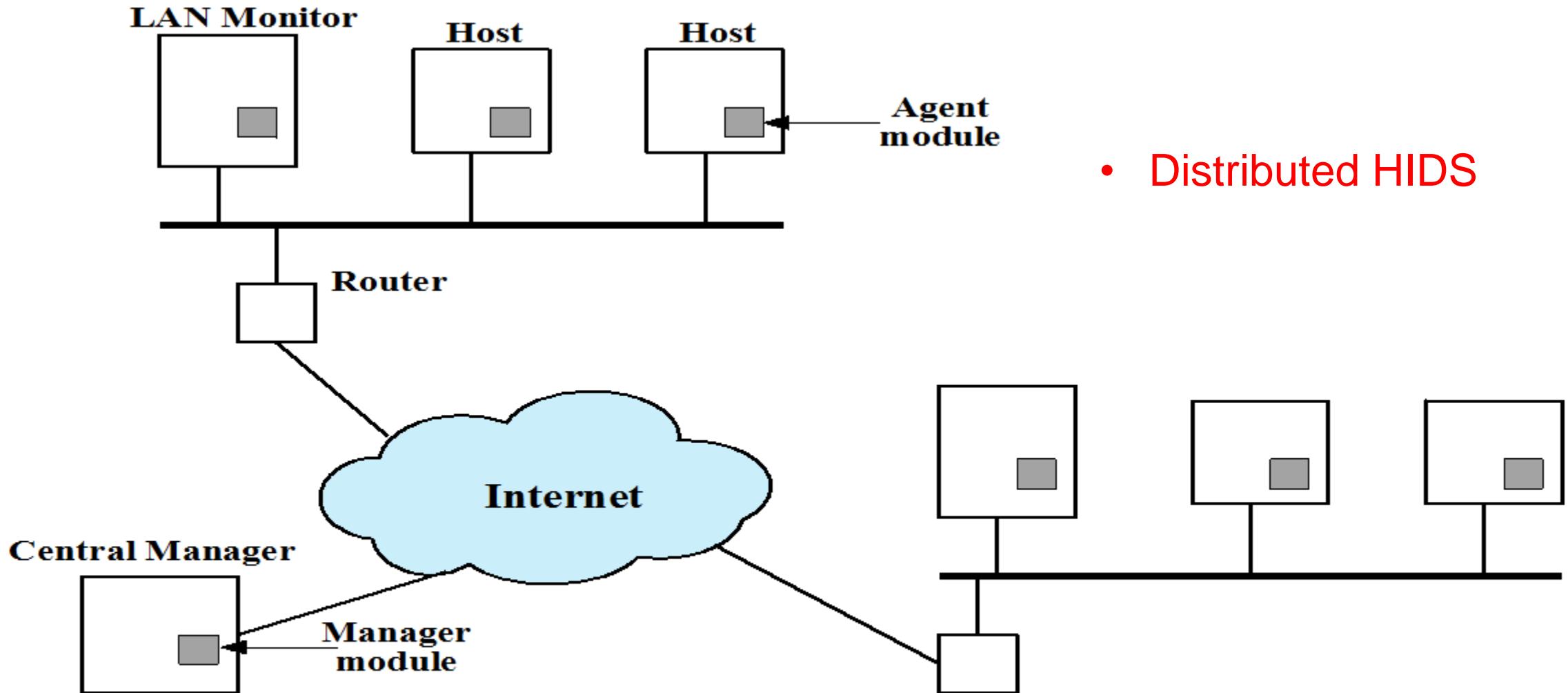
```
accept, accept, acct, adjtime, aiocancel, aioread, aiowait, aiowrite, alarm, async_daemon,  
auditsys, bind, chdir, chmod, chown, chroot, close, connect, creat, dup, dup2, execv, execve,  
exit, exportfs, fchdir, fchmod, fchown, fchroot, fcntl, flock, fork, fpathconf, fstat, fstat,  
fstatfs, fsync, ftime, ftruncate, getdents, getdirentries, getdomainname, getdopt, getdtablesize,  
getfh, getgid, getgroups, gethostid, gethostname, getitimer, getmsg, getpagesize,  
getpeername, getpgrp, getpid, getpriority, getrlimit, getrusage, getsockname, getsockopt,  
gettimeofday, getuid, gtty, ioctl, kill, killpg, link, listen, lseek, lstat, madvise, mctl, mincore,  
mkdir, mknod, mmap, mount, mount, mprotect, mpxchan, msgsys, msync, munmap,  
nfs_mount, nfssvc, nice, open, pathconf, pause, pcfs_mount, phys, pipe, poll, profil, ptrace,  
putmsg, quota, quotactl, read, readlink, readv, reboot, recv, recvfrom, recvmsg, rename,  
resuba, rfssys, rmdir, sbreak, sbrk, select, semsys, send, sendmsg, sendto, setdomainname,  
setdopt, setgid, setgroups, sethostid, sethostname, setitimer, setpgid, setpgrp, setpgrp,  
setpriority, setquota, setregid, setreuid, setrlimit, setsid, setsockopt, gettimeofday, setuid,  
shmsys, shutdown, sigblock, sigpause, sigpending, sigsetmask, sigstack, sigsys, sigvec,  
socket, socketaddr, socketpair, sstk, stat, stat, statfs, stime, stty, swapon, symlink, sync,  
sysconf, time, times, truncate, umask, umount, uname, unlink, unmount, ust, utime, utimes,  
vadvise, vfork, vhangup, vlimit, vpixsys, vread, vtimes, vtrace, vwrite, wait, wait3, wait4,  
write, writev
```

(b) Key Windows DLLs and Executables

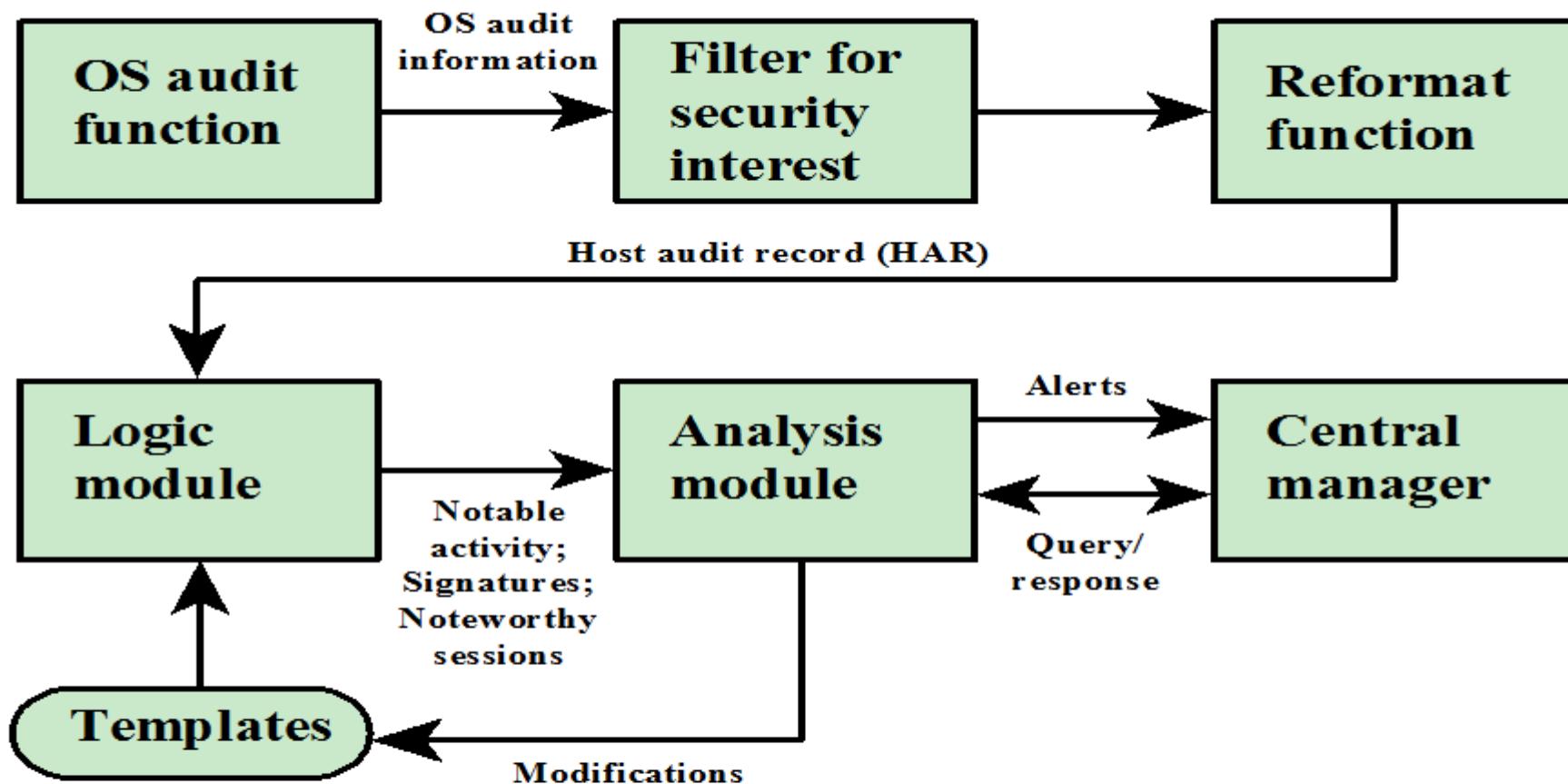
```
comctl32  
kernel32  
msvcpp  
msvcrt  
mswsock  
ntdll  
ntoskrnl  
user32  
ws2_32
```

Linux System Calls and Windows DLLs Monitored

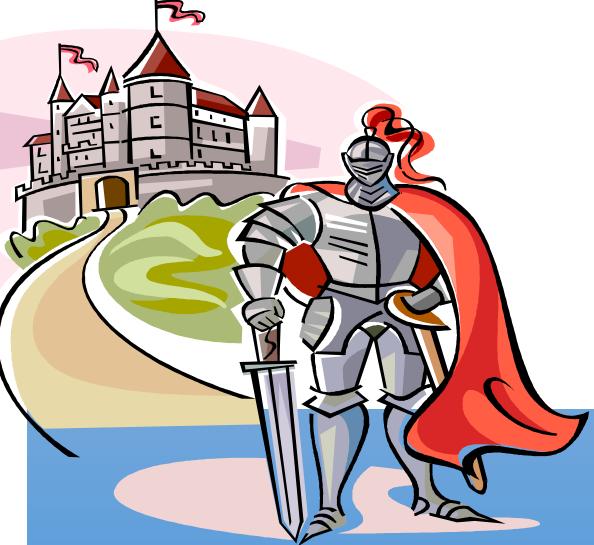
- Anomaly based HIDS
- Signature based HIDS



Architecture for Distributed Intrusion Detection



Agent Architecture



Monitors traffic at selected points on a network

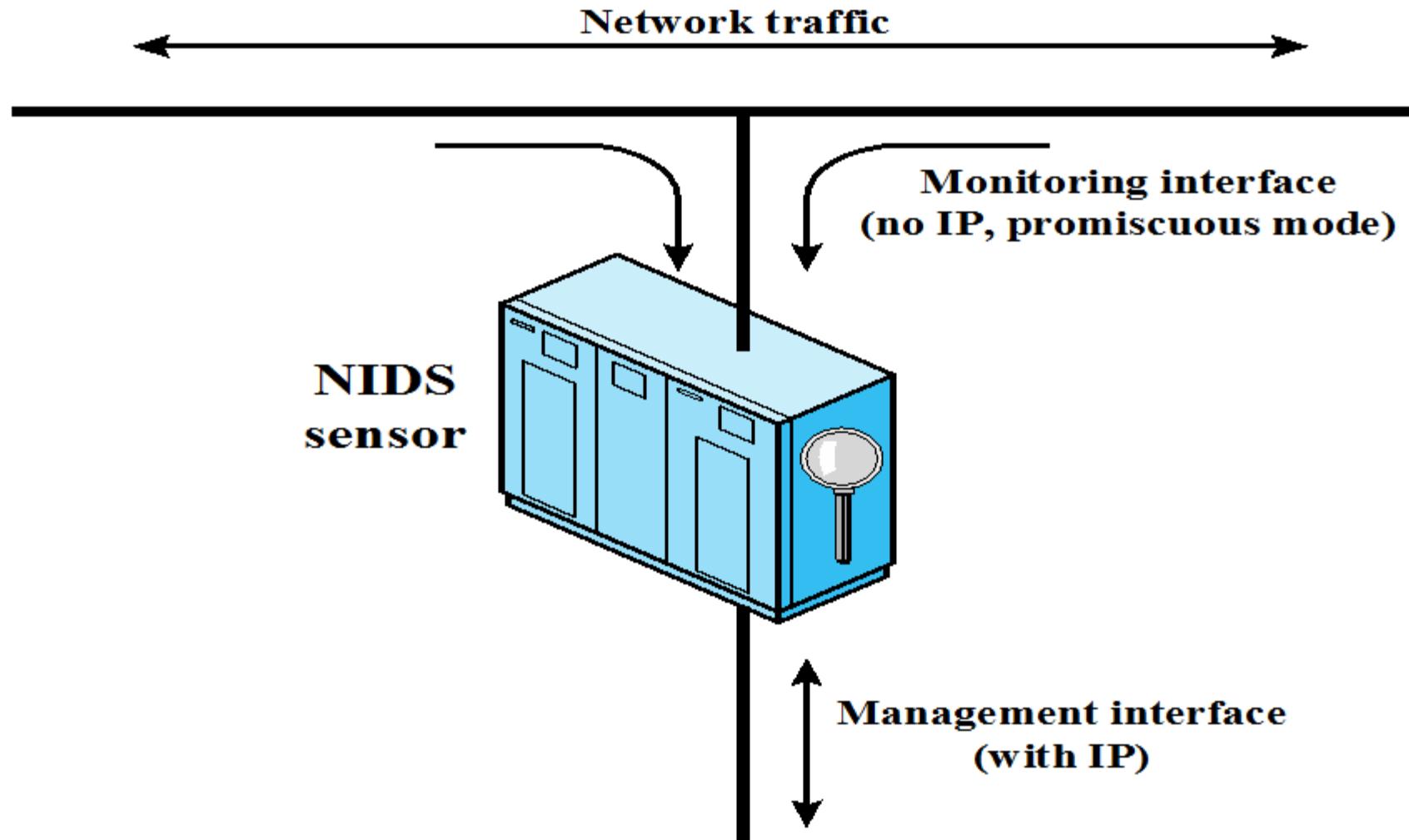
Network-Based IDS (NIDS)

Examines traffic packet by packet in real or close to real time

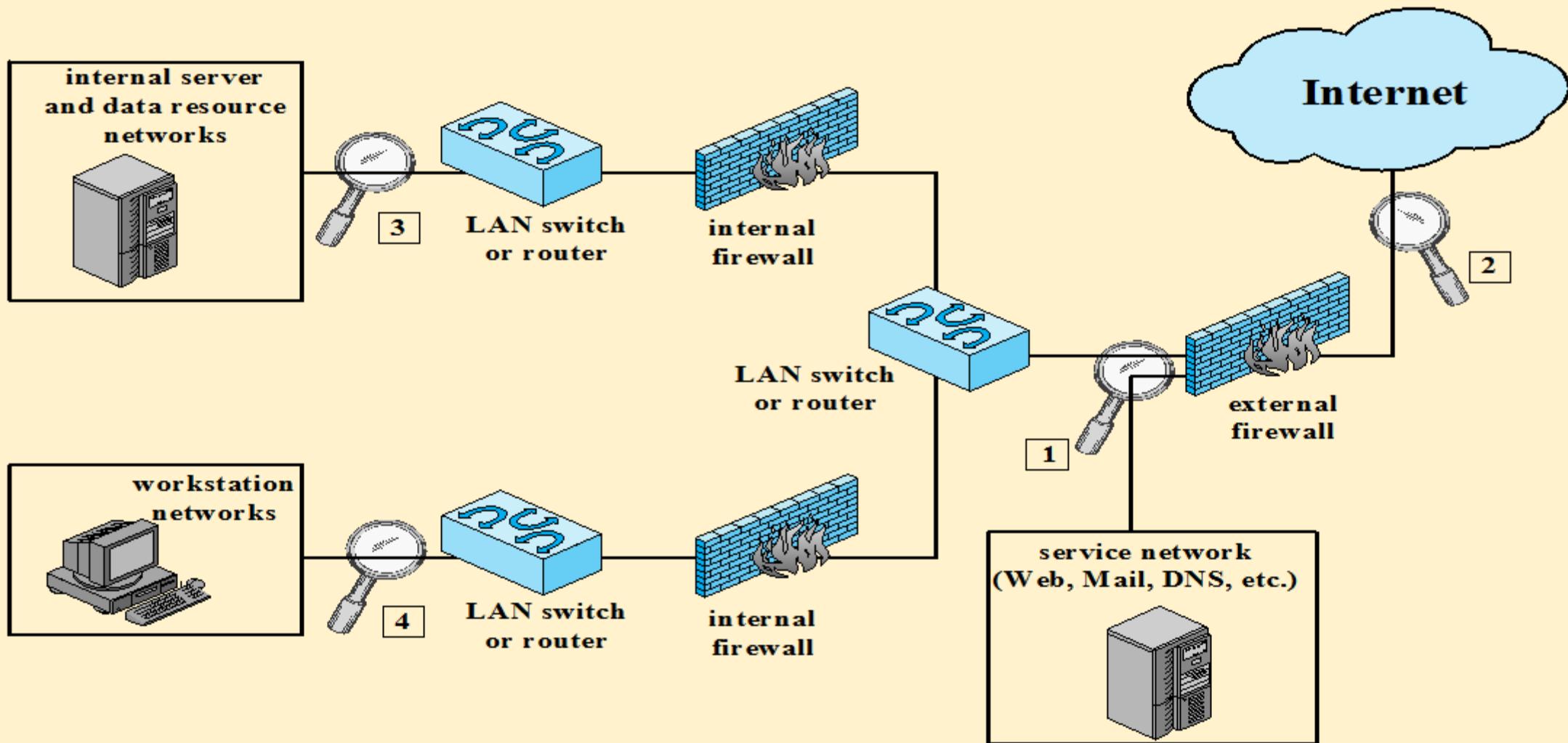
May examine network, transport, and/or application-level protocol activity

Comprised of a number of sensors, one or more servers for NIDS management functions, and one or more management consoles for the human interface

Analysis of traffic patterns may be done at the sensor, the management server or a combination of the two



Passive NIDS Sensor



Example of NIDS Sensor Deployment

Intrusion Detection Techniques

Attacks suitable for Signature detection

- Application layer reconnaissance and attacks
- Transport layer reconnaissance and attacks
- Network layer reconnaissance and attacks
- Unexpected application services
- Policy violations

Attacks suitable for Anomaly detection

- Denial-of-service (DoS) attacks
- Scanning
- Worms

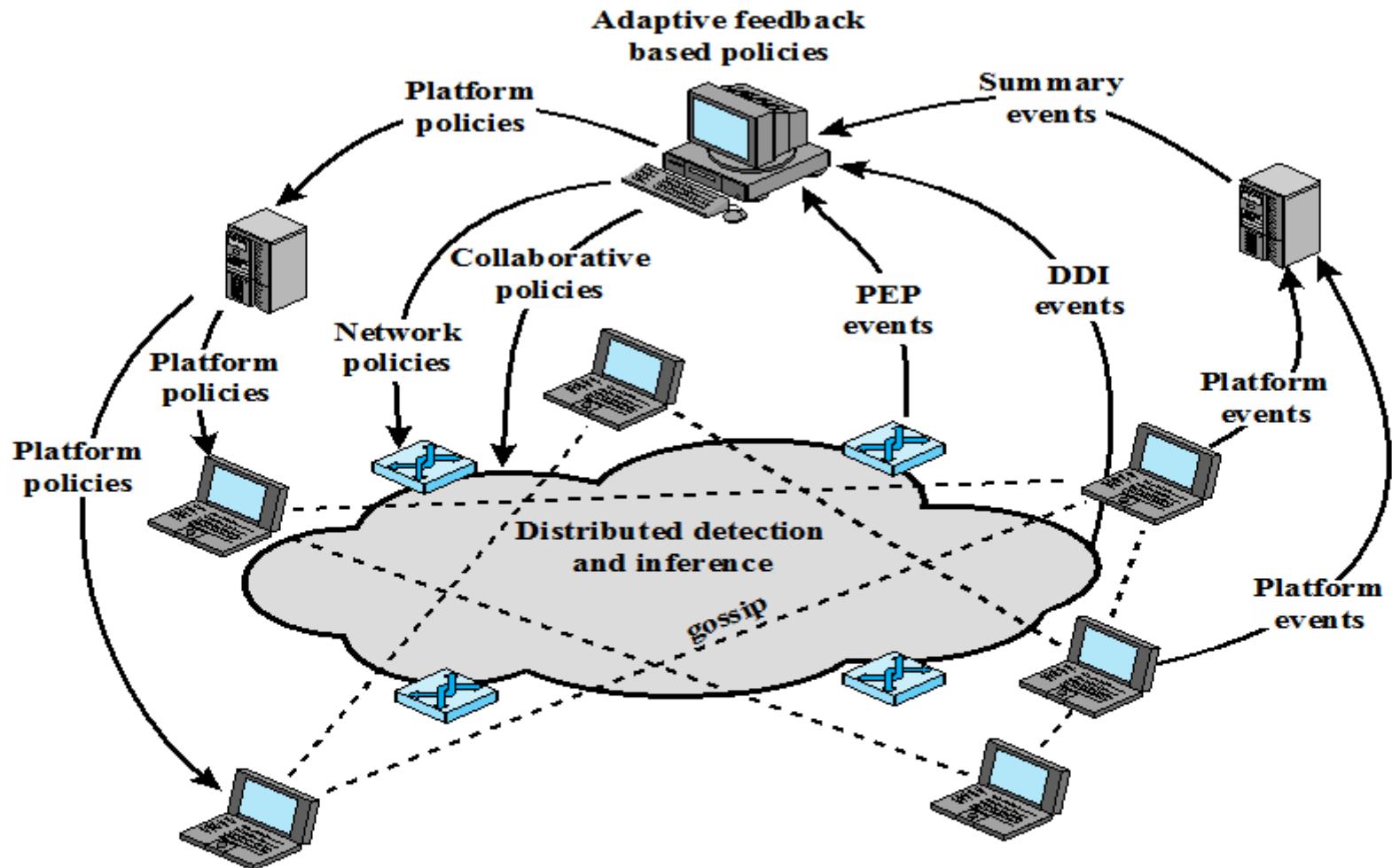
Stateful Protocol Analysis (SPA)

- Subset of anomaly detection that compares observed network traffic against predetermined universal vendor supplied profiles of benign protocol traffic
 - This distinguishes it from anomaly techniques trained with organization specific traffic protocols
- Understands and tracks network, transport, and application protocol states to ensure they progress as expected
- A key disadvantage is the high resource use it requires

Logging of Alerts

- Typical information logged by a NIDS sensor includes:

- Timestamp
- Connection or session ID
- Event or alert type
- Rating
- Network, transport, and application layer protocols
- Source and destination IP addresses
- Source and destination TCP or UDP ports, or ICMP types and codes
- Number of bytes transmitted over the connection
- Decoded payload data, such as application requests and responses
- State-related information



PEP = policy enforcement point

DDI = distributed detection and inference

- **Distributed IDS**

Overall Architecture of an Autonomic Enterprise Security System

IETF Intrusion Detection Working Group

- Purpose is to define data formats and exchange procedures for sharing information of interest to intrusion detection and response systems and to management systems that may need to interact with them
- The working group issued the following RFCs in 2007:

Intrusion Detection Message Exchange Requirements (RFC 4766)

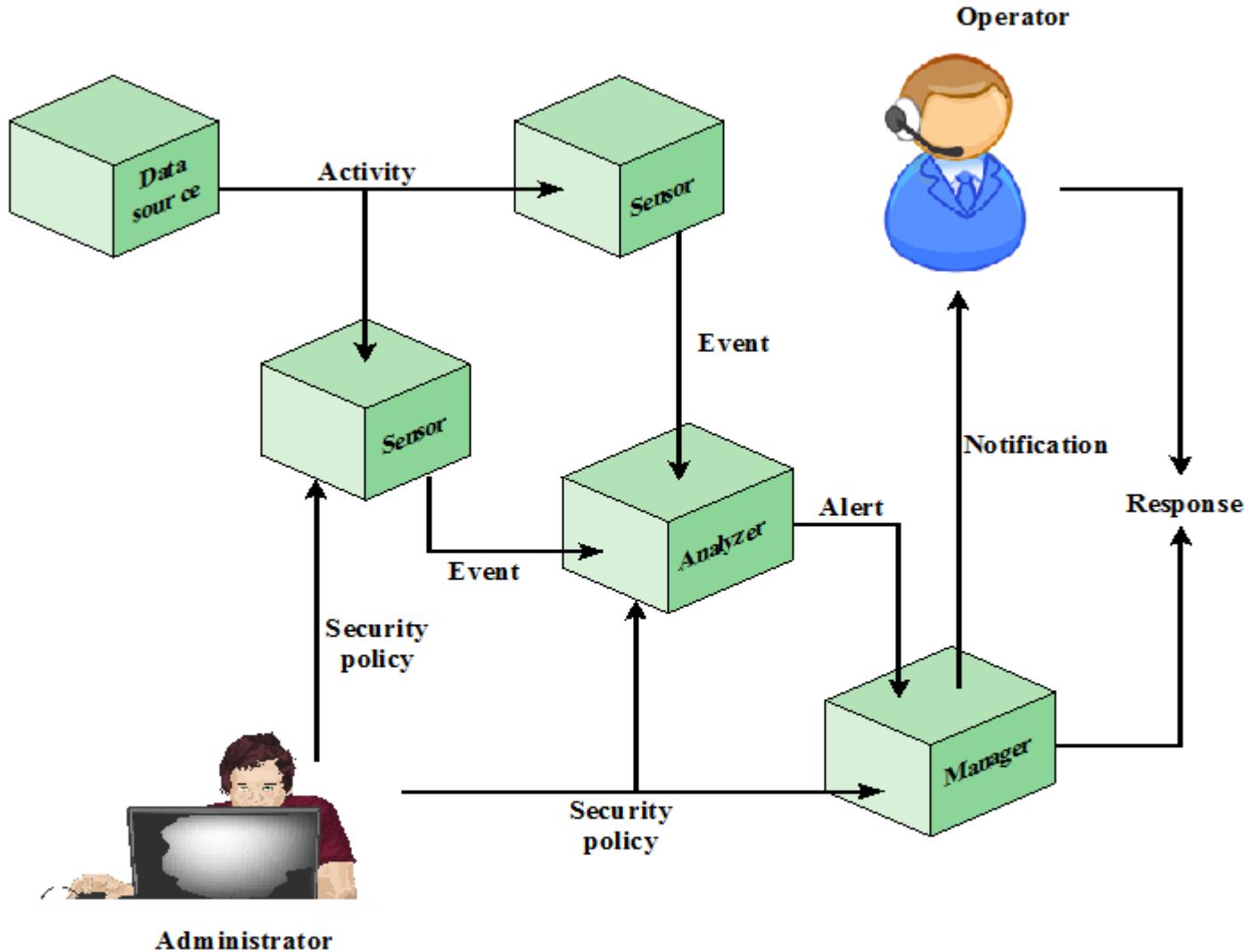
- Document defines requirements for the Intrusion Detection Message Exchange Format (IDMEF)
- Also specifies requirements for a communication protocol for communicating IDMEF

The Intrusion Detection Message Exchange Format (RFC 4765)

- Document describes a data model to represent information exported by intrusion detection systems and explains the rationale for using this model
- An implementation of the data model in the Extensible Markup Language (XML) is presented, and XML Document Type Definition is developed, and examples are provided

The Intrusion Detection Exchange Protocol (RFC 4767)

- Document describes the Intrusion Detection Exchange Protocol (IDXP), an application level protocol for exchanging data between intrusion detection entities
- IDXP supports mutual authentication, integrity, and confidentiality over a connection oriented protocol

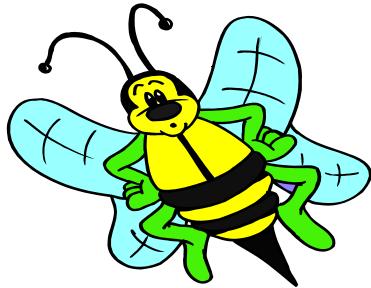


Model For Intrusion Detection Message Exchange

Honeypots



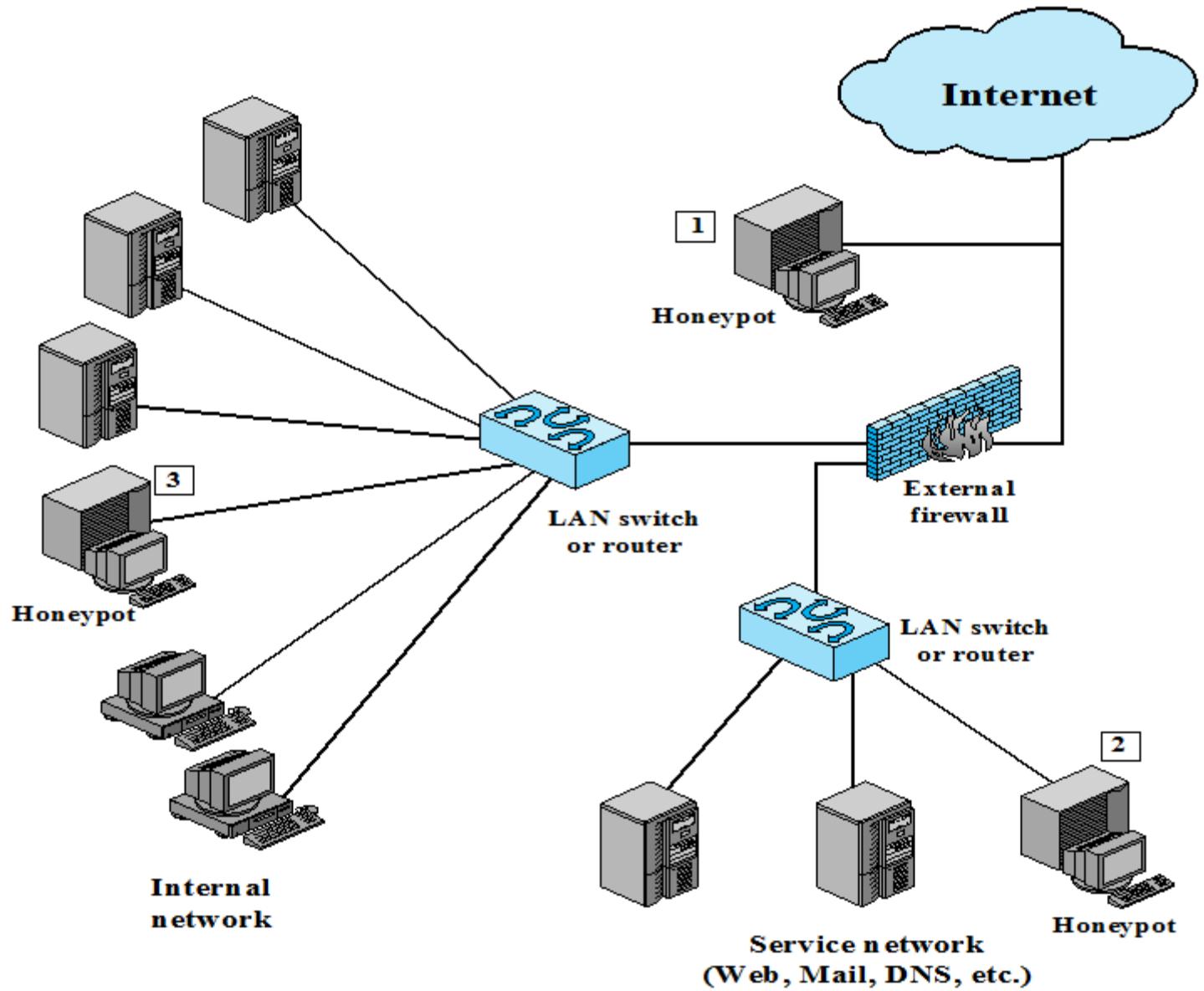
- Decoy systems designed to:
 - Lure a potential attacker away from critical systems
 - Collect information about the attacker's activity
 - Encourage the attacker to stay on the system long enough for administrators to respond
- Systems are filled with fabricated information that a legitimate user of the system wouldn't access
- Resources that have no production value
 - Therefore incoming communication is most likely a probe, scan, or attack
 - Initiated outbound communication suggests that the system has probably been compromised



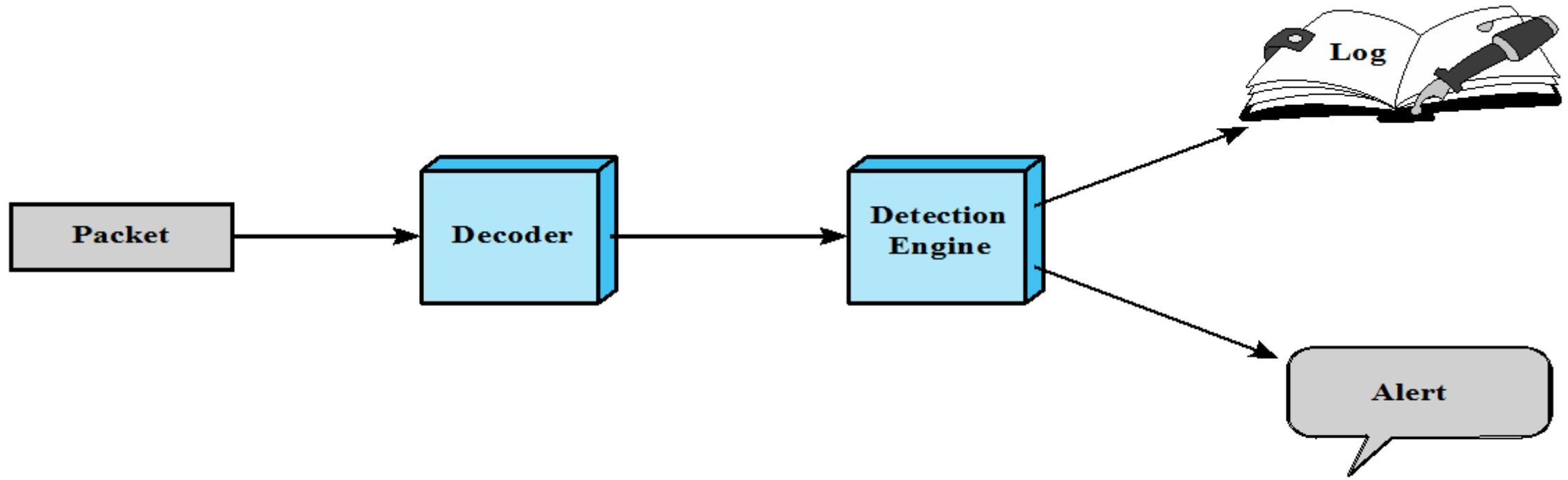
Honeypot Classifications



- Low interaction honeypot
 - Consists of a software package that emulates particular IT services or systems well enough to provide a realistic initial interaction, but does not execute a full version of those services or systems
 - Provides a less realistic target
 - Often sufficient for use as a component of a distributed IDS to warn of imminent attack
- High interaction honeypot
 - A real system, with a full operating system, services and applications, which are instrumented and deployed where they can be accessed by attackers
 - Is a more realistic target that may occupy an attacker for an extended period
 - However, it requires significantly more resources
 - If compromised could be used to initiate attacks on other systems



Example of Honeypot Deployment



Snort Architecture

Action	Protocol	Source IP address	Source Port	Direction	Dest IP address	Dest Port
--------	----------	-------------------	-------------	-----------	-----------------	-----------

(a) Rule Header

Option Keyword	Option Arguments	• • •
----------------	------------------	-------

(b) Options

Snort Rule Formats

Snort Rule Actions

Action	Description
alert	Generate an alert using the selected alert method, and then log the packet.
log	Log the packet.
pass	Ignore the packet.
activate	Alert and then turn on another dynamic rule.
dynamic	Remain idle until activated by an activate rule , then act as a log rule.
drop	Make iptables drop the packet and log the packet.
reject	Make iptables drop the packet, log it, and then send a TCP reset if the protocol is TCP or an ICMP port unreachable message if the protocol is UDP.
sdrop	Make iptables drop the packet but does not log it.

meta-data

msg Defines the message to be sent when a packet generates an event.

reference Defines a link to an external attack identification system, which provides additional information.

classtype Indicates what type of attack the packet attempted.

payload

content Enables Snort to perform a case-sensitive search for specific content (text and/or binary) in the packet payload.

depth Specifies how far into a packet Snort should search for the specified pattern. Depth modifies the previous content keyword in the rule.

offset Specifies where to start searching for a pattern within a packet. Offset modifies the previous content keyword in the rule.

nocase Snort should look for the specific pattern, ignoring case. Nocase modifies the previous content keyword in the rule.

non-payload

ttl Check the IP time-to-live value. This option was intended for use in the detection of traceroute attempts.

id Check the IP ID field for a specific value. Some tools (exploits, scanners and other odd programs) set this field specifically for various purposes, for example, the value 31337 is very popular with some hackers.

dsize Test the packet payload size. This may be used to check for abnormally sized packets. In many cases, it is useful for detecting buffer overflows.

flags Test the TCP flags for specified settings.

seq Look for a specific TCP header sequence number.

icmp-id Check for a specific ICMP ID value. This is useful because some covert channel programs use static ICMP fields when they communicate. This option was developed to detect the stacheldraht DDoS agent.

post-detection

logto Log packets matching the rule to the specified filename.

session Extract user data from TCP Sessions. There are many cases where seeing what users are typing in telnet, rlogin, ftp, or even web sessions is very useful.

Examples of Snort Rule Options

Summary

- Intruders
 - Intruder behavior
- Intrusion detection
 - Basic principles
 - The base-rate fallacy
 - Requirements
- Analysis approaches
 - Anomaly detection
 - Signature or heuristic detection
- Distributed or hybrid intrusion detection
- Intrusion detection exchange format
- Honeypots
- Host-based intrusion detection
 - Data sources and sensors
 - Anomaly HIDS
 - Signature or heuristic HIDS
 - Distributed HIDS
- Network-based intrusion detection
 - Types of network sensors
 - NIDS sensor deployment
 - Intrusion detection techniques
 - Logging of alerts
- Example system: Snort
 - Snort architecture
 - Snort rules



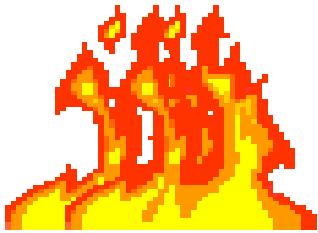
Lecture 9

Firewalls and

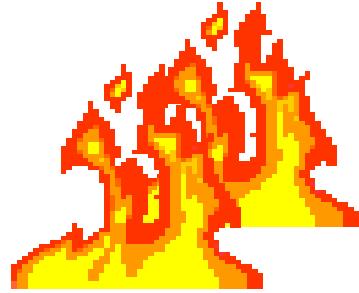
Intrusion Prevention Systems

CMPU-4008

Advance Security 2



The Need For Firewalls



- Internet connectivity is essential
 - However it creates a threat
- Effective means of protecting LANs
- Inserted between the premises network and the Internet to establish a controlled link
 - Can be a single computer system or a set of two or more systems working together
- Used as a perimeter defense
 - Single choke point to impose security and auditing
 - Insulates the internal systems from external networks

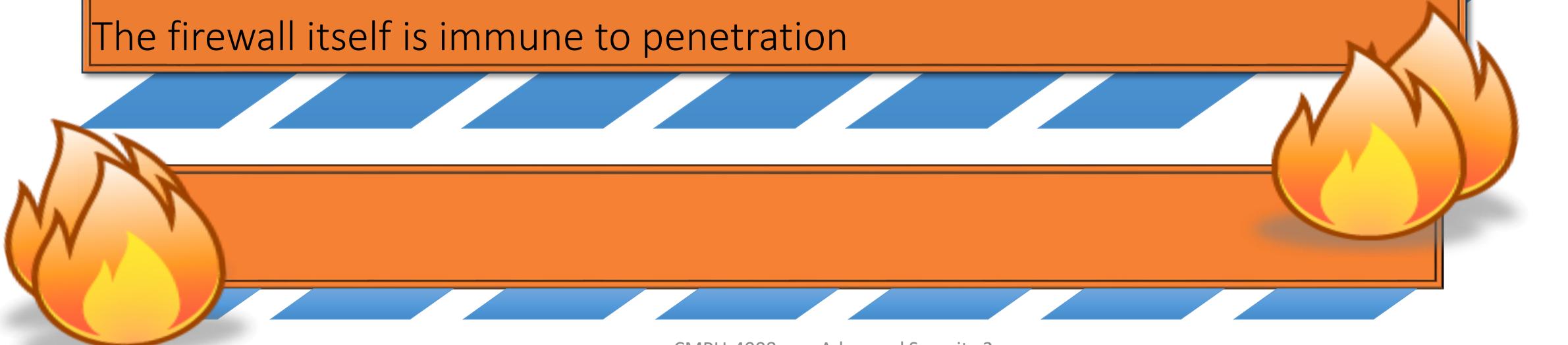
Firewall Characteristics

Design Goals

All traffic from inside to outside, and vice versa, must pass through the firewall

Only authorized traffic as defined by the local security policy will be allowed to pass

The firewall itself is immune to penetration



Firewall Access Policy

- A critical component in the planning and implementation of a firewall is specifying a suitable access policy
 - This lists the types of traffic authorized to pass through the firewall
 - Includes address ranges, protocols, applications and content types
- This policy should be developed from the organization's information security risk assessment and policy
- Should be developed from a broad specification of which traffic types the organization needs to support
 - Then refined to detail the filter elements which can then be implemented within an appropriate firewall topology

Firewall Filter Characteristics

- Characteristics that a firewall access policy could use to filter traffic include:

IP address and protocol values

This type of filtering is used by packet filter and stateful inspection firewalls

Typically used to limit access to specific services

Application protocol

This type of filtering is used by an application-level gateway that relays and monitors the exchange of information for specific application protocols

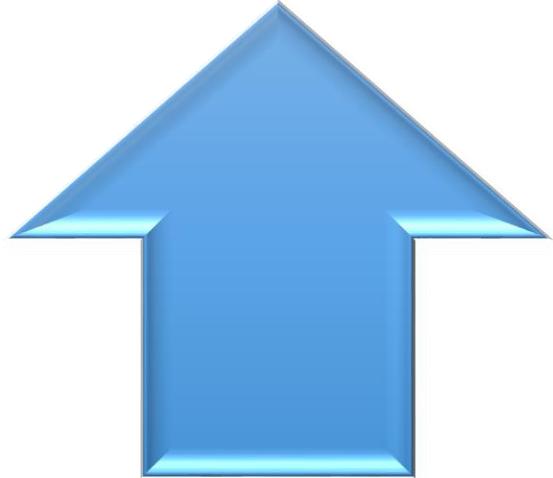
User identity

Typically for inside users who identify themselves using some form of secure authentication technology

Network activity

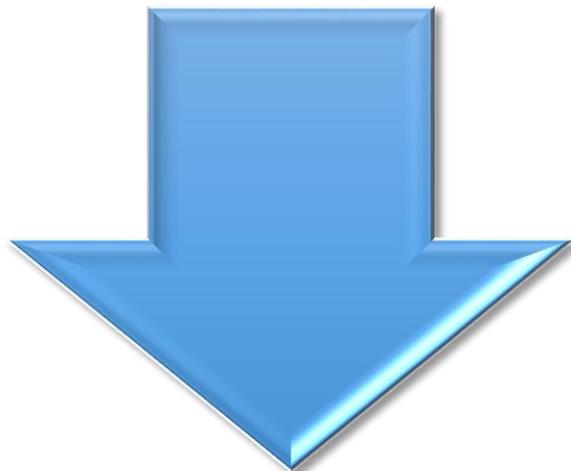
Controls access based on considerations such as the time or request, rate of requests, or other activity patterns

Firewall Capabilities And Limits



Capabilities:

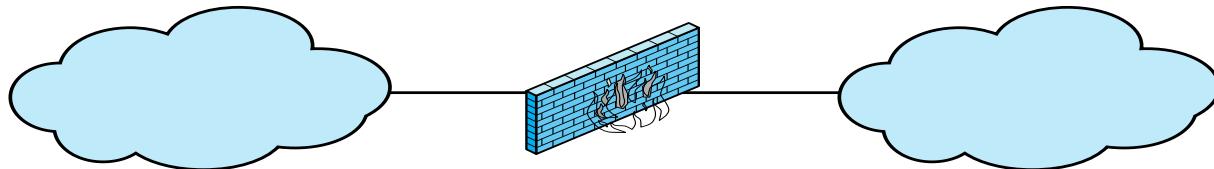
- Defines a single choke point
- Provides a location for monitoring security events
- Convenient platform for several Internet functions that are not security related
- Can serve as the platform for IPSec



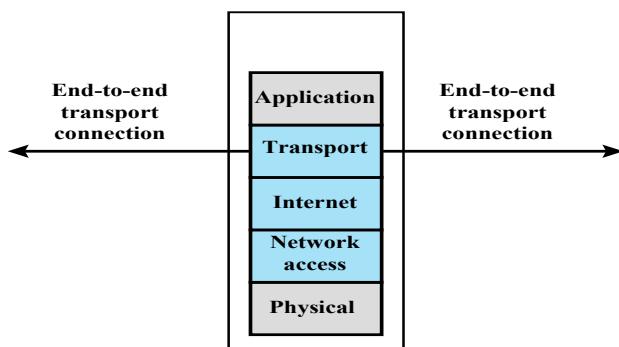
Limitations:

- Cannot protect against attacks bypassing firewall
- May not protect fully against internal threats
- Improperly secured wireless LAN can be accessed from outside the organization
- Laptop, PDA, or portable storage device may be infected outside the corporate network then used internally

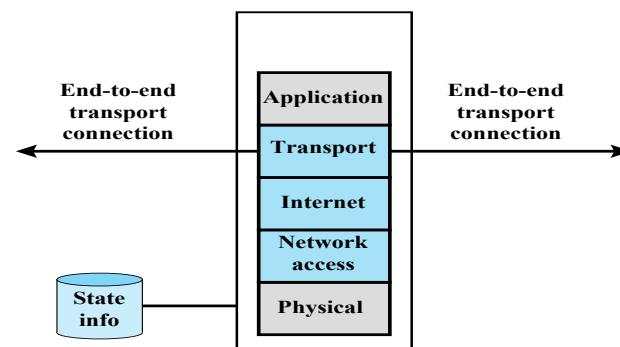
**Internal (protected) network
(e.g. enterprise network)** **Firewall** **External (untrusted) network
(e.g. Internet)**



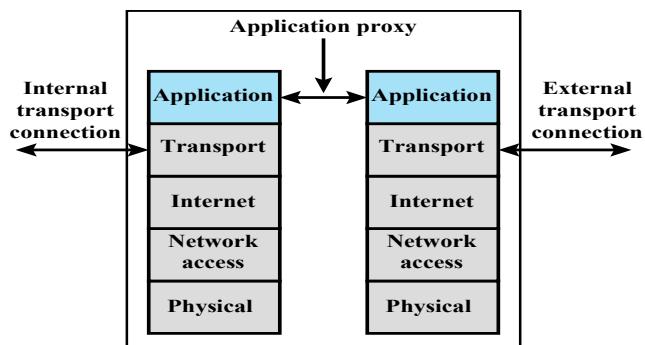
(a) General model



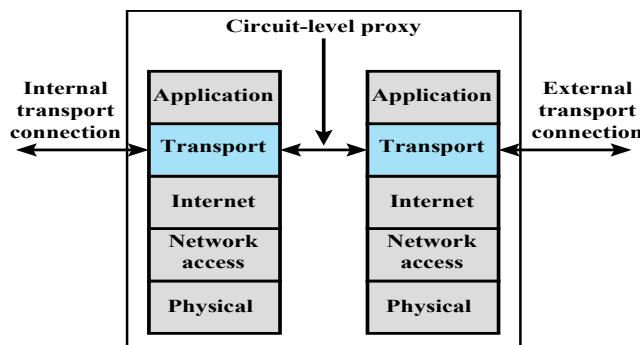
(b) Packet filtering firewall



(c) Stateful inspection firewall



(d) Application proxy firewall



(e) Circuit-level proxy firewall

Figure 9.1 Types of Firewalls

Packet Filtering Firewall

- Applies rules to each incoming and outgoing IP packet
 - Typically a list of rules based on matches in the IP or TCP header
 - Forwards or discards the packet based on rules match

Filtering rules are based on information contained in a network packet

- Source IP address
- Destination IP address
- Source and destination transport-level address
- IP protocol field
- Interface

- Two default policies:
 - Discard - prohibit unless expressly permitted
 - More conservative, controlled, visible to users
 - Forward - permit unless expressly prohibited
 - Easier to manage and use but less secure

Table 9.1

Packet-Filtering Examples

Rule	Direction	Src address	Dest addresss	Protocol	Dest port	Action
1	In	External	Internal	TCP	25	Permit
2	Out	Internal	External	TCP	>1023	Permit
3	Out	Internal	External	TCP	25	Permit
4	In	External	Internal	TCP	>1023	Permit
5	Either	Any	Any	Any	Any	Deny

Packet Filter Advantages And Weaknesses

- **Advantages**
 - Simplicity
 - Typically transparent to users and are very fast
- **Weaknesses**
 - Cannot prevent attacks that employ application specific vulnerabilities or functions
 - Limited logging functionality
 - Do not support advanced user authentication
 - Vulnerable to attacks on TCP/IP protocol bugs
 - Improper configuration can lead to breaches

Stateful Inspection Firewall

Tightens rules for TCP traffic by creating a directory of outbound TCP connections

- There is an entry for each currently established connection
- Packet filter allows incoming traffic to high numbered ports only for those packets that fit the profile of one of the entries in this directory

Reviews packet information but also records information about TCP connections

- Keeps track of TCP sequence numbers to prevent attacks that depend on the sequence number
- Inspects data for protocols like FTP, IM and SIPS commands

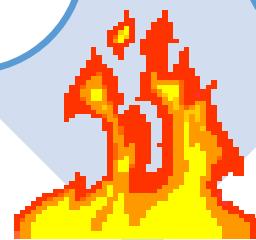


Table 9.2

Example Stateful Firewall

Connection State Table

Source Address	Source Port	Destination Address	Destination Port	Connection State
192.168.1.100	1030	210.9.88.29	80	Established
192.168.1.102	1031	216.32.42.123	80	Established
192.168.1.101	1033	173.66.32.122	25	Established
192.168.1.106	1035	177.231.32.12	79	Established
223.43.21.231	1990	192.168.1.6	80	Established
219.22.123.32	2112	192.168.1.6	80	Established
210.99.212.18	3321	192.168.1.6	80	Established
24.102.32.23	1025	192.168.1.6	80	Established
223.21.22.12	1046	192.168.1.6	80	Established

Application-Level Gateway

- Also called an application proxy
- Acts as a relay of application-level traffic
 - User contacts gateway using a TCP/IP application
 - User is authenticated
 - Gateway contacts application on remote host and relays TCP segments between server and user
- Must have proxy code for each application
 - May restrict application features supported
- Tend to be more secure than packet filters
- Disadvantage is the additional processing overhead on each connection

Circuit-Level Gateway

Circuit level proxy

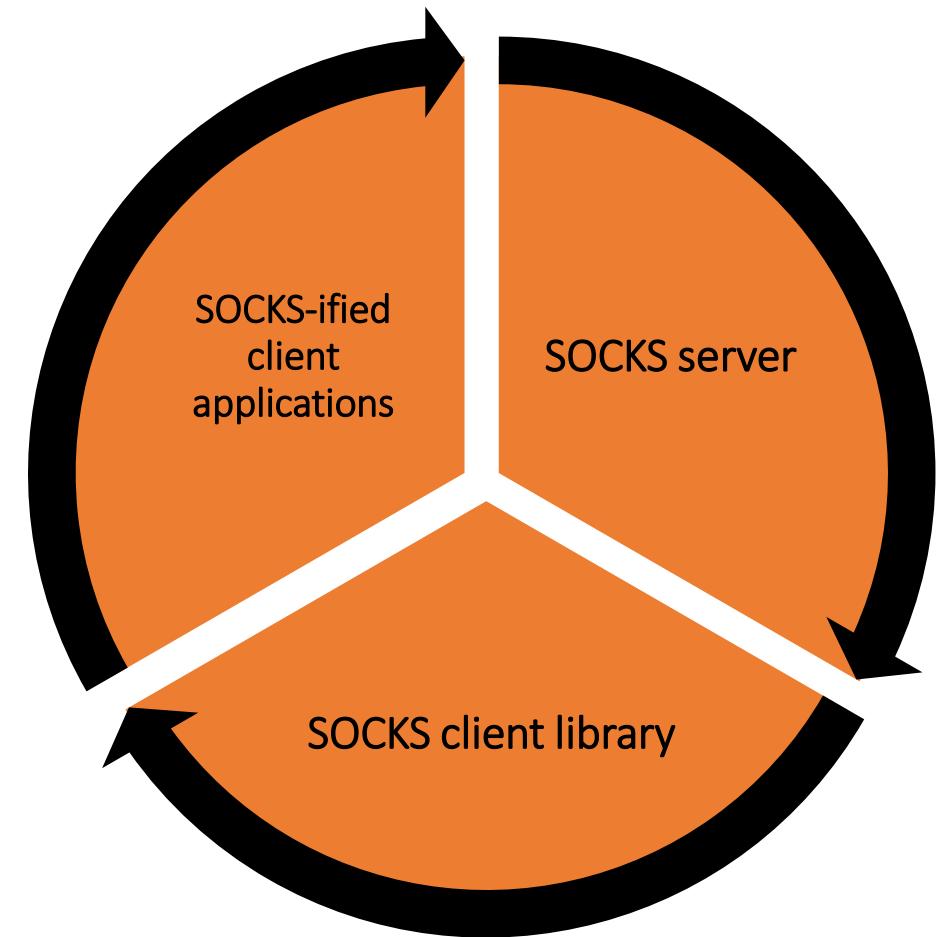
- Sets up two TCP connections, one between itself and a TCP user on an inner host and one on an outside host
- Relays TCP segments from one connection to the other without examining contents
- Security function consists of determining which connections will be allowed

Typically used when inside users are trusted

- May use application-level gateway inbound and circuit-level gateway outbound
- Lower overheads

SOCKS Circuit-Level Gateway

- SOCKS v5 defined in RFC1928
- Designed to provide a framework for client-server applications in TCP/UDP domains to conveniently and securely use the services of a network firewall
- Client application contacts SOCKS server, authenticates, sends relay request
 - Server evaluates and either establishes or denies the connection



Components

Bastion Hosts

- System identified as a critical strong point in the network's security
- Serves as a platform for an application-level or circuit-level gateway
- Common characteristics:
 - Runs secure O/S, only essential services
 - May require user authentication to access proxy or host
 - Each proxy can restrict features, hosts accessed
 - Each proxy is small, simple, checked for security
 - Each proxy is independent, non-privileged
 - Limited disk use, hence read-only code

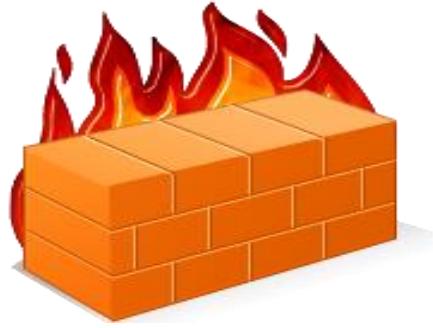


Host-Based Firewalls

- Used to secure an individual host
- Available in operating systems or can be provided as an add-on package
- Filter and restrict packet flows
- Common location is a server

Advantages:

- Filtering rules can be tailored to the host environment
- Protection is provided independent of topology
- Provides an additional layer of protection



Personal Firewall

- Controls traffic between a personal computer or workstation and the Internet or enterprise network
- For both home or corporate use
- Typically is a software module on a personal computer
- Can be housed in a router that connects all of the home computers to a DSL, cable modem, or other Internet interface
- Typically much less complex than server-based or stand-alone firewalls
- Primary role is to deny unauthorized remote access
- May also monitor outgoing traffic to detect and block worms and malware activity

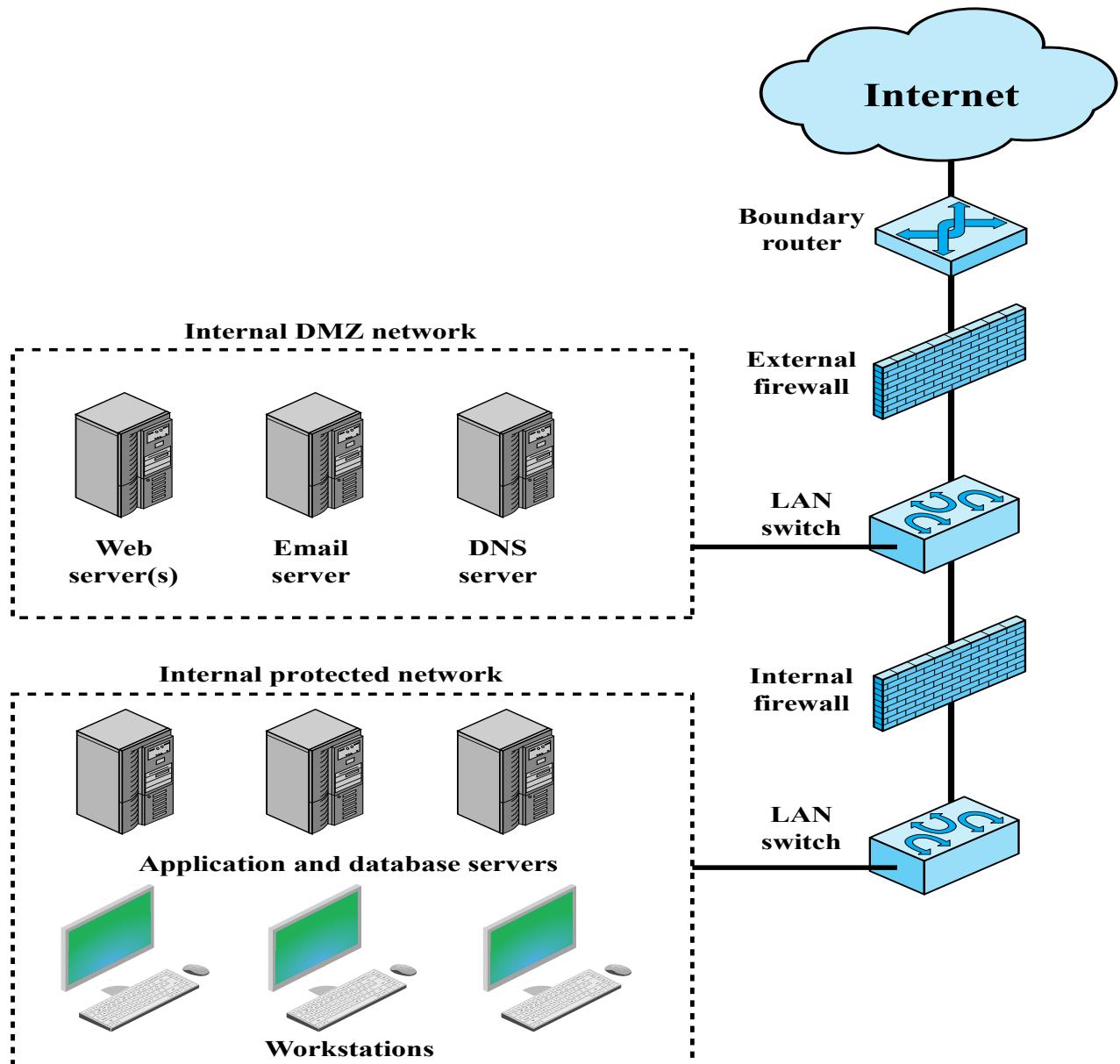


Figure 9.2 Example Firewall Configuration

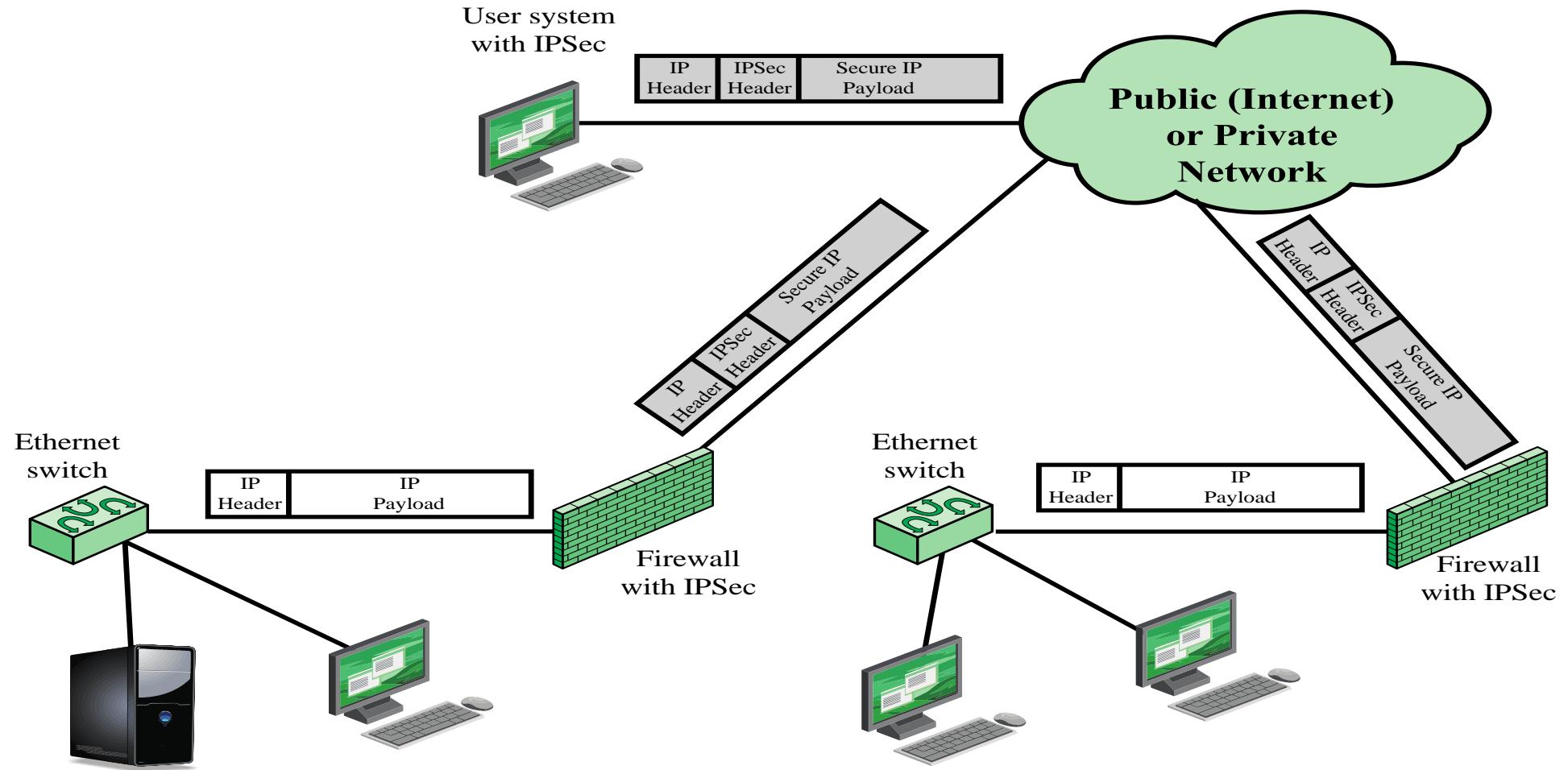


Figure 9.3 A VPN Security Scenario

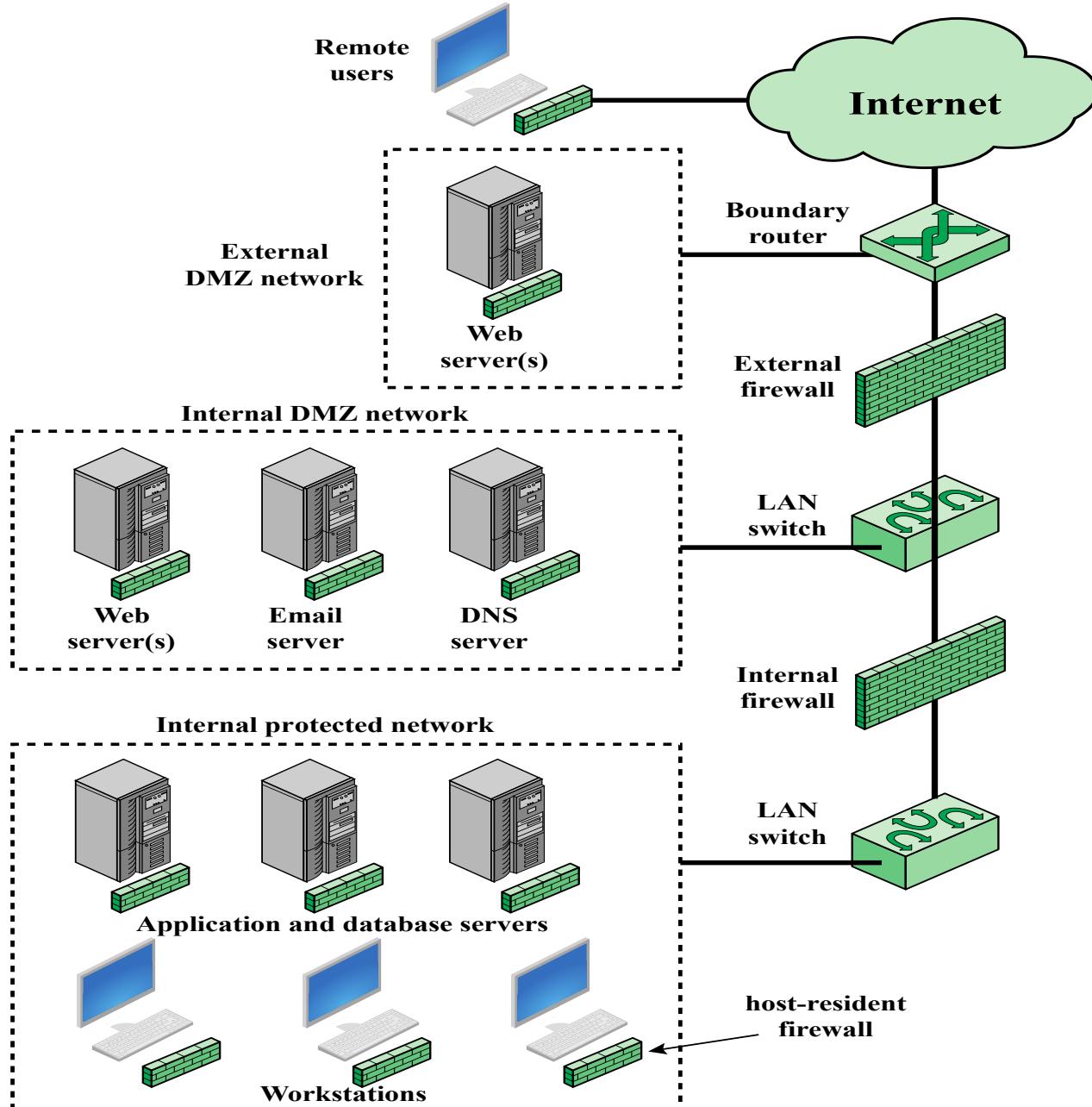


Figure 9.4 Example Distributed Firewall Configuration

Firewall Topologies

Host-resident firewall

- Includes personal firewall software and firewall software on servers

Screening router

- Single router between internal and external networks with stateless or full packet filtering

Single bastion inline

- Single firewall device between an internal and external router

Single bastion T

- Has a third network interface on bastion to a DMZ where externally visible servers are placed

Double bastion inline

- DMZ is sandwiched between bastion firewalls

Double bastion T

- DMZ is on a separate network interface on the bastion firewall

Distributed firewall configuration

- Used by large businesses and government organizations

Intrusion Prevention Systems (IPS)

- Also known as Intrusion Detection and Prevention System (IDPS)
- Is an extension of an IDS that includes the capability to attempt to block or prevent detected malicious activity
- Can be host-based, network-based, or distributed/hybrid
- Can use anomaly detection to identify behavior that is not that of legitimate users, or signature/heuristic detection to identify known malicious behavior can block traffic as a firewall does, but makes use of the types of algorithms developed for IDSs to determine when to do so

Host-Based IPS (HIPS)

- Can make use of either signature/heuristic or anomaly detection techniques to identify attacks
 - Signature: focus is on the specific content of application network traffic, or of sequences of system calls, looking for patterns that have been identified as malicious
 - Anomaly: IPS is looking for behavior patterns that indicate malware
- Examples of the types of malicious behavior addressed by a HIPS include:
 - Modification of system resources
 - Privilege-escalation exploits
 - Buffer-overflow exploits
 - Access to e-mail contact list
 - Directory traversal

HIPS

- Capability can be tailored to the specific platform
- A set of general purpose tools may be used for a desktop or server system
- Some packages are designed to protect specific types of servers, such as Web servers and database servers
 - In this case the HIPS looks for particular application attacks
- Can use a sandbox approach
 - Sandboxes are especially suited to mobile code such as Java applets and scripting languages
 - HIPS quarantines such code in an isolated system area then runs the code and monitors its behavior
- Areas for which a HIPS typically offers desktop protection:
 - System calls
 - File system access
 - System registry settings
 - Host input/output

The Role of HIPS

- Many industry observers see the enterprise endpoint, including desktop and laptop systems, as now the main target for hackers and criminals
 - Thus security vendors are focusing more on developing endpoint security products
 - Traditionally, endpoint security has been provided by a collection of distinct products, such as antivirus, antispyware, antispam, and personal firewalls
- Approach is an effort to provide an integrated, single-product suite of functions
 - Advantages of the integrated HIPS approach are that the various tools work closely together, threat prevention is more comprehensive, and management is easier
- A prudent approach is to use HIPS as one element in a defense-in-depth strategy that involves network-level devices, such as either firewalls or network-based IPSs

Network-Based IPS(NIPS)

- Inline NIDS with the authority to modify or discard packets and tear down TCP connections
- Makes use of signature/heuristic detection and anomaly detection
- May provide flow data protection
 - Requires that the application payload in a sequence of packets be reassembled
- Methods used to identify malicious packets:

Pattern matching

Stateful matching

Protocol anomaly

Traffic anomaly

Statistical anomaly

Distributed or Hybrid IPS (Digital Immune System)

- Comprehensive defense against malicious behavior caused by malware
- Developed by IBM and refined by Symantec
- Motivation for this development includes the rising threat of Internet-based malware, the increasing speed of its propagation provided by the Internet, and the need to acquire a global view of the situation
- Success depends on the ability of the malware analysis system to detect new and innovative malware strains

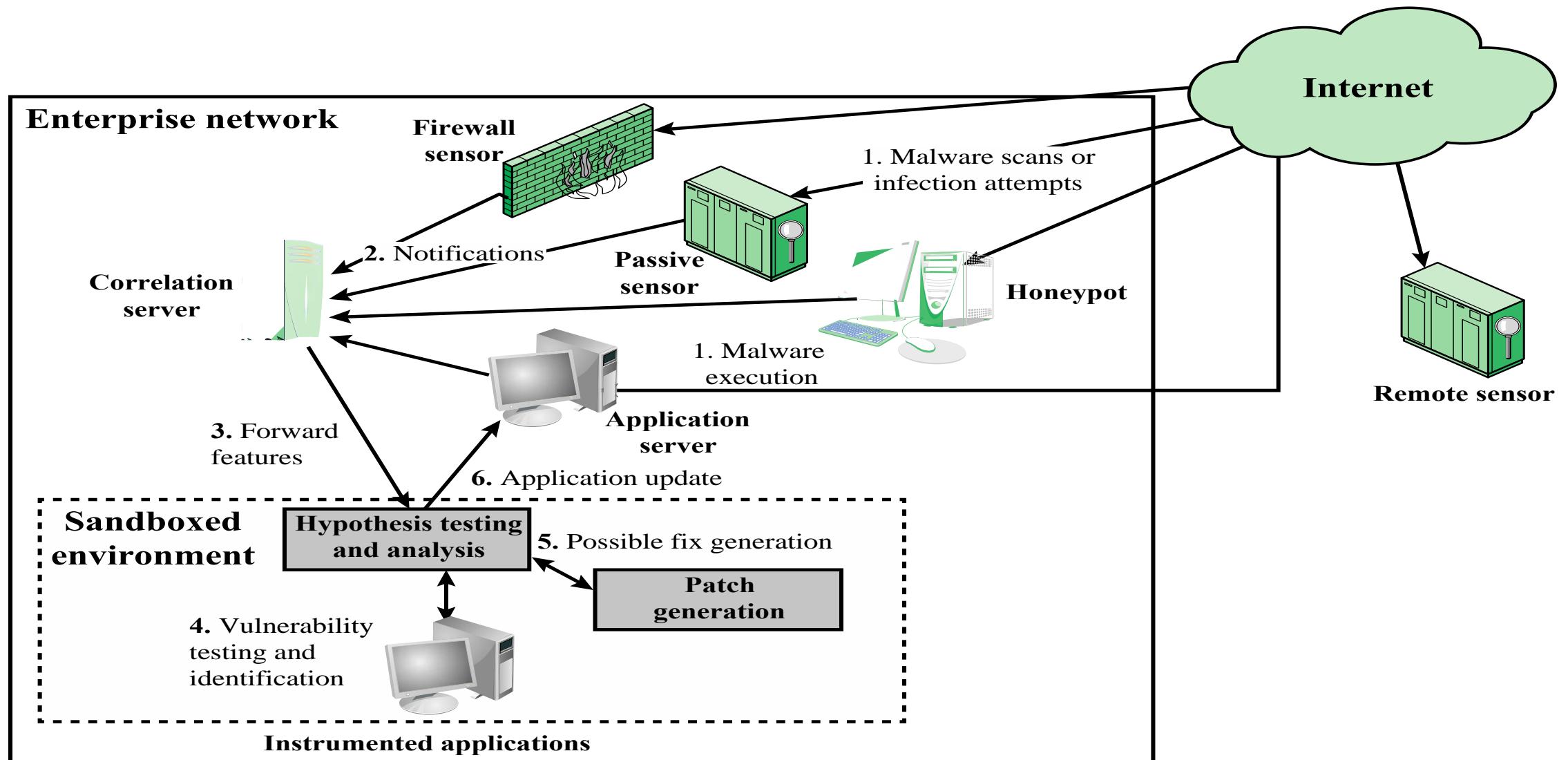


Figure 9.5 Placement of Worm Monitors

Snort Inline

- Enables Snort to function as an intrusion prevention system
- Includes a replace option which allows the Snort user to modify packets rather than drop them
 - Useful for a honeypot implementation
 - Attackers see the failure but cannot figure out why it occurred

Drop

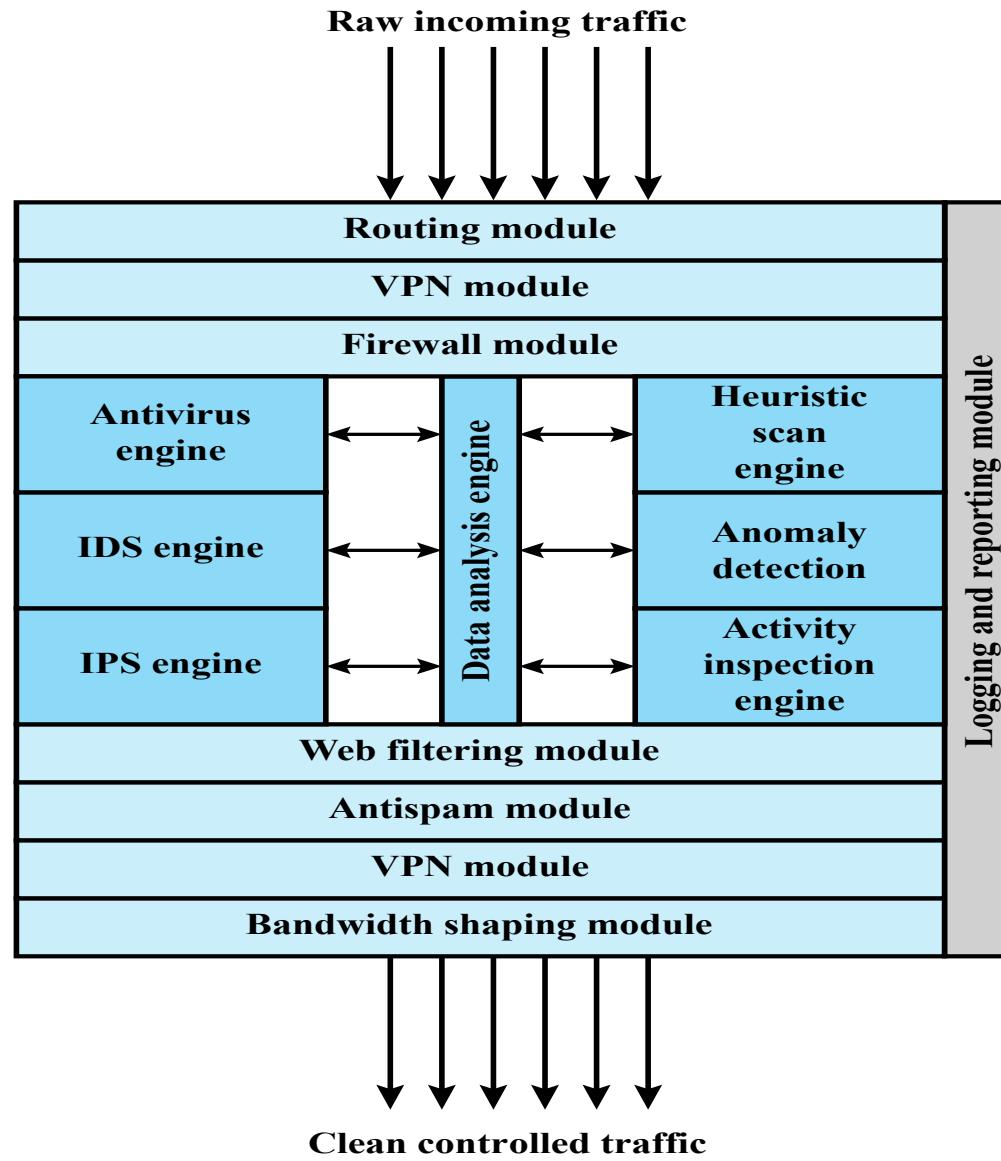
Snort rejects a packet based on the options defined in the rule and logs the result

Reject

Packet is rejected and result is logged and an error message is returned

Sdrop

Packet is rejected but not logged



**Figure 9.6 Unified Threat Management Appliance
(based on [JAME06])**

Table 9.3
Sidewinder G2 Security Appliance Attack Protections
Summary Transport Level Examples

Attacks and Internet Threats	Protections
TCP	
<ul style="list-style-type: none"> • Invalid port numbers • Invalid sequence numbers • SYN floods • XMAS tree attacks • Invalid CRC values • Zero length • Random data as TCP header 	<ul style="list-style-type: none"> • TCP hijack attempts • TCP spoofing attacks • Small PMTU attacks • SYN attack • Script Kiddie attacks • Packet crafting: different TCP options set <ul style="list-style-type: none"> • Enforce correct TCP flags • Enforce TCP header length • Ensures a proper 3-way handshake • Closes TCP session correctly • 2 sessions, one on the inside and one on the outside • Enforce correct TCP flag usage • Manages TCP session timeouts • Blocks SYN attacks
UDP	
<ul style="list-style-type: none"> • Invalid UDP packets • Random UDP data to bypass rules 	<ul style="list-style-type: none"> • Connection prediction • UDP port scanning <ul style="list-style-type: none"> • Verify correct UDP packet • Drop UDP packets on ports not open

Table 9.4

Sidewinder G2 Security Appliance Attack Protections Summary - Application Level Examples (page 1 of 2)

Attacks and Internet Threats	Protections	
DNS		
Incorrect NXDOMAIN responses from AAAA queries could cause denial-of-service conditions.	<ul style="list-style-type: none"> •Does not allow negative caching •Prevents DNS Cache Poisoning 	
ISC BIND 9 before 9.2.1 allows remote attackers to cause a denial of service (shutdown) via a malformed DNS packet that triggers an error condition that is not properly handled when the rdataset parameter to the dns_message_findtype() function in message.c is not NULL.	<ul style="list-style-type: none"> •Sidewinder G2 prevents malicious use of improperly formed DNS messages to affect firewall operations. •Prevents DNS query attacks •Prevents DNS answer attacks 	
DNS information prevention and other DNS abuses.	<ul style="list-style-type: none"> •Prevent zone transfers and queries •True split DNS protect by Type Enforcement technology to allow public and private DNS zones. •Ability to turn off recursion 	
FTP		
<ul style="list-style-type: none"> •FTP bounce attack •PASS attack •FTP Port injection attacks •TCP segmentation attack 	<ul style="list-style-type: none"> •Sidewinder G2 has the ability to filter FTP commands to prevent these attacks. •True network separation prevents segmentation attacks. 	
SQL		
SQL Net man in the middle attacks	<ul style="list-style-type: none"> •Smart proxy protected by Type Enforcement Technology •Hide Internal DB through nontransparent connections 	
Real-Time Streaming Protocol (RTSP)		
<ul style="list-style-type: none"> •Buffer overflow •Denial of service 	<ul style="list-style-type: none"> •Smart proxy protected by Type Enforcement technology •Protocol validation •Denies multicast traffic 	<ul style="list-style-type: none"> •Checks setup and teardown methods •Verifies PNG and RTSP protocol, discards all others •Auxiliary port monitoring
SNMP		
<ul style="list-style-type: none"> •SNMP flood attacks •Default community attack •Brute force attack •SNMP put attack 	<ul style="list-style-type: none"> •Filter SNMP version traffic 1, 2c •Filter Read, Write, and Notify messages •Filter OIDs •Filter PDU (Protocol Data Unit) 	

SSH			
<ul style="list-style-type: none"> •Challenge-Response buffer overflows •SSHD allows users to override “Allowed Authentications” •OpenSSH buffer_append_space buffer overflow •OpenSSH/PAM challenge Response buffer overflow •OpenSSH channel code offer-by-one 		<p>Sidewinder G2 v6.x’s embedded Type Enforcement technology strictly limits the capabilities of Secure Computing’s modified versions of the OpenSSH daemon code.</p>	
SMTP			
<ul style="list-style-type: none"> •Sendmail buffer overflows •Sendmail denial of service attacks •Remote buffer overflow in sendmail 	<ul style="list-style-type: none"> •Sendmail address parsing buffer overflow •SMTP protocol anomalies 	<ul style="list-style-type: none"> •Split Sendmail architecture protected by Type Enforcement technology •Sendmail customized for controls 	<ul style="list-style-type: none"> •Prevents buffer overflows through Type Enforcement technology •Sendmail checks SMTP protocol anomalies
<ul style="list-style-type: none"> •SMTP worm attacks •SMTP mail flooding •Relay attacks •Viruses, Trojans, worms 	<ul style="list-style-type: none"> •E-mail Addressing spoofing •MIME attacks •Phishing e-mails 	<ul style="list-style-type: none"> •Protocol validation •Anti-spam filter •Mail filters – size, keyword •Signature antivirus 	<ul style="list-style-type: none"> •Anti-relay •MIME/Antivirus filter •Firewall antivirus •Anti-phishing through virus scanning
Spyware Applications			
<ul style="list-style-type: none"> •Adware used for collecting information for marketing purposes •Stalking horses •Trojan horses 	<ul style="list-style-type: none"> •Malware •Backdoor Santas 	<ul style="list-style-type: none"> •SmartFilter® URL filtering capability built in with Sidewinder G2 can be configured to filter Spyware URLs, preventing downloads. 	

Lecture 10

Operating System Security and Security Assessment Tools

CMPU-4008

Advance Security 2

Introduction

- Linux is used to power many of the servers found around the world.
- It is a robust, full-featured operating system.
- It is a hacker's favorite because it is easy to develop programs, and it is a great platform for building and testing security tools.

Introduction

- Linux is an operating system that is based on UNIX.
- Linux was originally created by Linus Torvalds with help from programmers from around the world.
- The benefits to using Linux are that it is economical, well-designed, and offers good performance.
- Linux distributions are easily available and can be downloaded onto any system.

Introduction

- Linux comes in many flavors, including Red Hat, Ubuntu, Debian, Mandrake, SUSE, and MINIX.
- Some specialized versions of Linux have been developed for a specific purpose such as Knoppix, FreeNAS, BackTrack and Scientific Linux.
- The best way to learn Linux is just by using it.

Introduction

- Other versions of Linux that have been customized for security work and penetration testing are available at this website:
 - <http://livecdlist.com/>
- Linux is open source, which means that it can be freely distributed and you have the right to modify the source code.

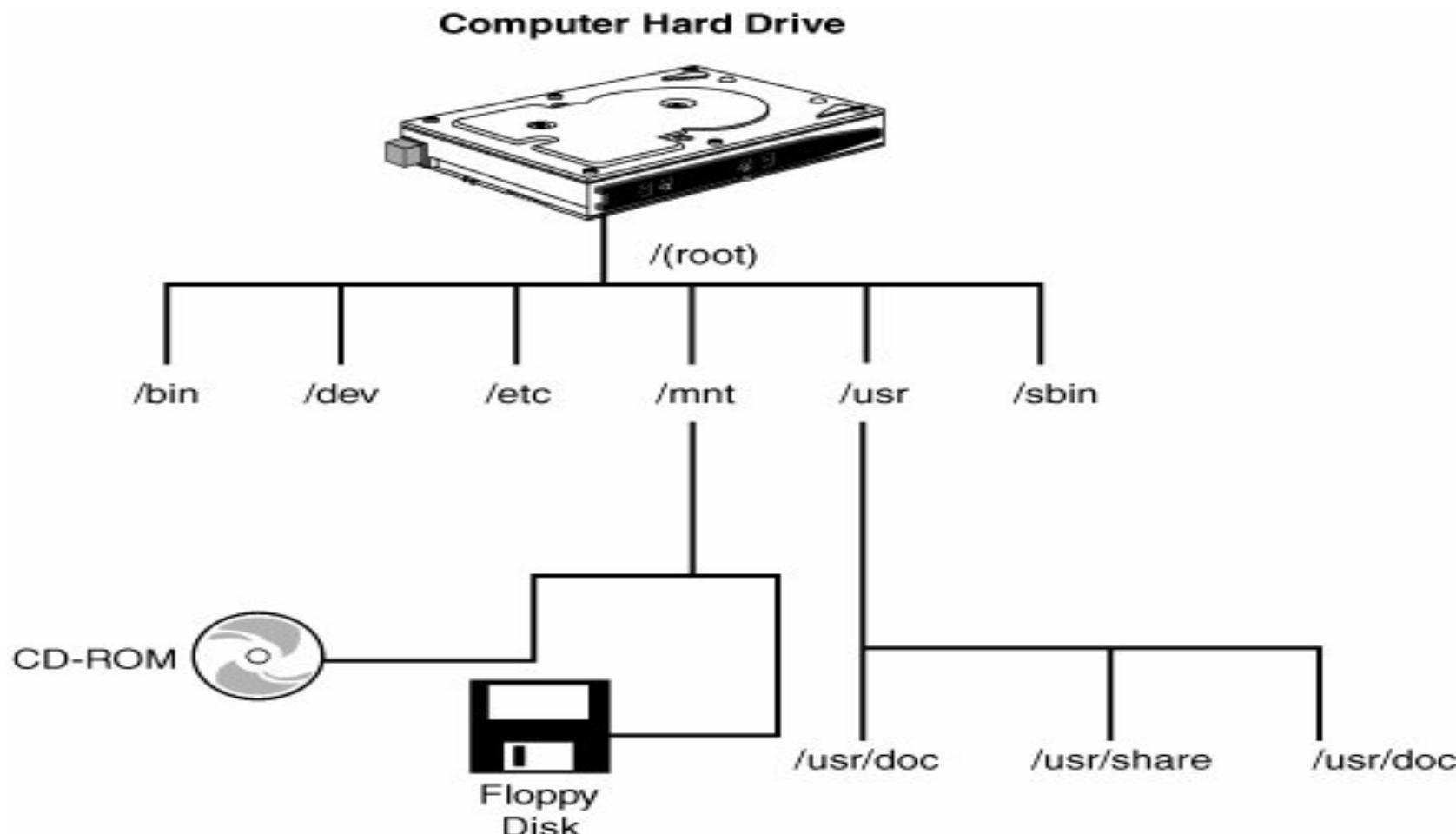
Introduction

- Linux is also easy to develop your own programs on.
- This is one of the reasons that you will see many security tools released on Linux well before they ever make a debut in the Windows world.

Linux File Structure

- The Linux file system is the structure in which all the information on the computer is stored.
- Files are stored within a hierarchy of directories. Each directory can contain other directories and files.

Linux File Structure



Linux File Structure

Some of the more common directories found on a Linux system are described here:

- `/` Represents the root directory.
- `/bin` Contains common Linux user commands, such as `ls`, `sort`, `date`, and `chmod`.
- `/dev` Contains files representing access points to devices on your systems. These can include floppy disks, hard disks, and CD-ROMs.
- `/etc` Contains administrative configuration files, the `passwd` file, and the `shadow` file.
- `/home` Contains user home directories.
- `/mnt` Provides a location for mounting devices, such as CD-ROMs and floppy disks.
- `/sbin` Contains administrative commands and daemon processes.
- `/usr` Contains user documentation, graphical files, libraries, as well as a variety of other user and administrative commands and files.

Linux File Structure

- Directories and files on a Linux system are set up so that access can be controlled.
- When you log in to the system, you are identified by a user account. In addition to your user account, you might belong to a group or groups.
- Therefore, files can have permissions set for a user, a group, or others.

Linux File Structure

- Access for each of these groups has three options:
 - Read
 - Write
 - Execute
- To see the current permissions, owner, and group for a file or directory, type the `ls -l` command. This will display the contents of the directory you are in with the privileges for the user, group, and all others.

Linux File Structure

- The *chmod* command is used by a file owner or administrator to change the definition of access permissions to a file or set of files.
- *Chmod* can be used in symbolic and absolute modes.
- Symbolic deals with symbols such as rwx, whereas absolute deals with octal values.

File Access Permissions

- \$ chmod u+x filename
- \$ chmod u+r,g+x filename
- \$ chmod u-rx filename
- \$ chmod a+x filename
- \$ chmod -R 755 directory-name/

Linux Basics

- The # sign is most important here as it denotes that you are root.
- Root in Linux has total control of the system and maintains the highest level of privilege.
- You will want to make sure that you properly execute commands while working as root because unlike Windows, Linux might not offer you prompts or warnings before it executes a critical command.

Linux Commands Basics

Command	Description
cat	Lists the contents of a file
cd	Changes directory
chmod	Changes file and folder rights and ownership
cp	The copy command
history	Shows the history of up to 500 commands
ifconfig	Similar to ipconfig in Windows
kill	Kills a running process by specifying the PID
ls	Lists the contents of a folder
man	Opens manual pages

Linux Commands Basics

Command	Description
mv	Command to move file and directories
passwd	The command to change your password
ps	The process status command
pwd	Prints the working directory path
rm	Removes a file
rm -r	Removes a directory and all its contents
ctrl-p	Pauses a program
ctrl-b	Puts the current program into the background
ctrl-z	Puts the current program to sleep

Linux Basics

- Linux users must be managed in an organized way.
- Access for users and system processes are assigned a User ID (UID) and a Group ID (GID).
- Groups are the logical grouping of users that have similar requirements.
- This information is contained in the /etc/passwd file.

Linux Basics

- If you execute this command # cat /etc/passwd
- You will notice that root is the first account in the list.
- Root is always assigned the UID 0 and the GID 0.
- Other special users and accounts associated with services and daemons are listed after root and have values below 100.

The /etc/passwd fields

- The **username** is the first field.
- The second field holds the **encrypted password**. If you notice that the field is marked by an x that is because this particular Linux system is using shadow passwords, which are held in /etc/shadow.
- The third field is the **UID**.
- The fourth field is the **GID**. You will notice that the GID and UID are the same.
- The fifth field is the **user description**. Information from this field can be reported by the finger utility.
- The sixth field is the **User's Home Directory**.
- The seventh and final field is the **User's Login Shell**.

The /etc/passwd fields

- To add users to Linux issue the ***useradd*** command.
- Of all the users, the one requiring the most protection is the root account because it must be secure.
- Although files such as ***passwd*** are world readable, the ***shadow file*** is only readable by root.
- If an attacker can gain access to the root account, he has essentially taken control of the computer from you.
- For this reason, the root account must be protected at the highest level.

Passwords and shadow file

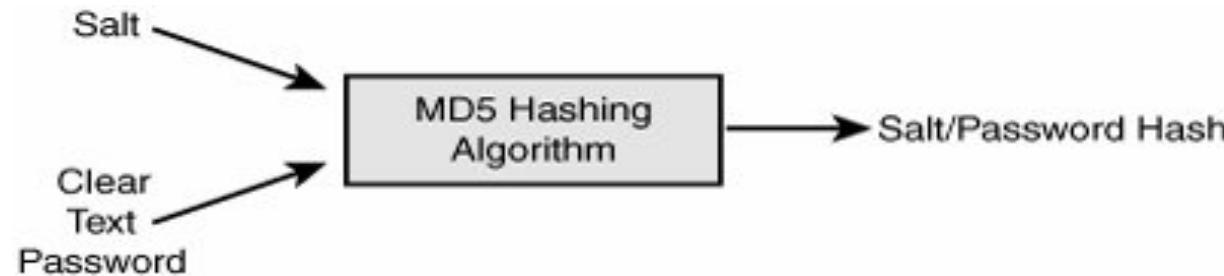
- Linux requires that user accounts have a password, but by default, it will not prevent you from leaving one set as blank.
- Most versions of Linux, use MD5 by default or if you choose not to use MD5, you can choose DES.
- Linux also includes the /etc/shadow file for additional password security.

Passwords and shadow file

- You must be logged as a root to see the contents shadow passwords by using the following command:
 - `more /etc/shadow`
- Linux systems passwords use **salts**.
- Salts are needed to add a layer of randomness to the passwords. Because MD5 is a hashing algorithm, this means that if I used "secret" for my password and another user used "secret" for his password, encrypted values would look the same.

Passwords and shadow file

- A salt can be one of 4,096 values and helps further scramble the password.
- Under Linux, the MD5 password is 32 characters long and begins with \$1\$. The characters between the second and third \$ represent the salt.



Passwords and shadow file

- Linux also has a host of password cracking tools available. John the Ripper is one of these tools (<http://www.openwall.com/John/>).
- It is probably the most well-known, most versatile, and fastest password cracking program around.
- You can verify that John works by running it in test mode. It will generate a baseline cracking speed for your system.
 - `./john -h`
 - `./john -test`

Compressing, Installing, and Compiling Linux

- In Linux, files are packaged and compressed in various ways.
- One of the most common compression formats is the Tape Archiving program (**Tar**).
 - **Tar** is a standard archive and was originally developed as backup software for UNIX.
 - It collects several files to a single file. It does-n't do file compression
- A program called **gzip** is one of the most common file compression programs.

Compressing, Installing, and Compiling Linux

- Compiling a package from a source tarball is not always a simple procedure.
 - After uncompressed the package, you should search for a file called README, INSTALL, CONFIGURE, or something similar.
 - This file will usually describe the configuration and installation process.
 - Frequently, the source package includes a script called configure, which you execute to have the package auto detect your computer's installed libraries and configure itself appropriately.

Compressing, Installing, and Compiling Linux

- If so, the process includes three commands:
 - `./configure`
 - `Make`
 - `make install`
- Linux comes with the GNU C compiler (GCC). This capability also comes in handy when you download a C program from a security site or would like to check out a piece of exploit code.

Compressing, Installing, and Compiling Linux

- \$vi hello.c

```
#include <stdio.h>
int main(int argc, char ** argv)
{
    printf("Hello world!\n");
    return 0;
}
```

- \$gcc -o hello hello.c
- \$./hello Hello world!
- Notice the ./ in front of the command. This ensures that Linux looks in the local directory for the specified executable.

Hacking Linux

- Hacking Linux follows the same basic methodology. The steps are broadly divided into six phases:
 - Reconnaissance
 - Scanning and enumeration
 - Gaining access
 - Escalation of privilege
 - Maintaining access
 - Cover tracks and placing backdoors

Reconnaissance

- Reconnaissance is about passive and active information gathering.
- This might be scanning the organizational website, reviewing job postings, social engineering etc.
- The same basic techniques used to attack Linux systems can also be used to attack Windows computers.

Scanning

- Scanning finds the hosts and determines what ports and applications they might be running.
- Here, you can see results that will begin to differentiate Windows and Linux systems.
- Port scanners and OS fingerprinting software will be the tools of the trade.
 - \$ nmap -O 192.168.13.10

Enumeration

- After any type of Linux or UNIX system is found, it will still require further probing to determine what's running.
- More importantly, if you think that the target is some flavor of UNIX, you have access to some programs not found in the world of Windows.
- For example, Finger, rwho - rpcinfo p, rusers, and Simple Mail Transfer Protocol (SMTP) - vrfy (verify) and expn (expand) can all be used to further leverage your knowledge.

Gaining Access

- Attempts to gain access can occur remotely or locally. Remote attacks are primarily carried out through one of four methods.
 - Exploit a process or program.
 - Exploit a Transmission Control Protocol (TCP) or User Datagram Protocol (UDP) listening service.
 - Exploit vulnerabilities in a system that is supplying routing services and providing security between two or more networks.
 - Exploit the user by having him initiate some type of action such as running an email attachment or visiting a hostile website.

Gaining Access

- Regardless of what method is used, the idea is to get some type of shell of the victim's machine.
- This can be as mindless as guessing usernames and passwords to more advanced backchannel attacks that rely on the victim's system to push the shell out to the attacker.

Gaining Access

- If the victim is found to be running TFTP, you can try to get the victim to hand over critical files.

```
[root@fs /root]# tftp 192.168.13.50
tftp> get /etc/passwd /root/passwdhack.txt
Received 1015 bytes in 0.0 seconds
tftp> quit
[root@fs /root]#more passwdhack.txt
```

- Although you could get the passwd file, you might have noticed that the passwords have been shadowed. This was not a complete success; however, the attacker was able to recover a list of users on the system.
- It is important to specify a destination directory when using TFTP to get the remote host's /etc/passwd file. Otherwise, you will overwrite your own /etc/passwd file.

Privilege Escalation

- Privilege escalation can best be described as the act of leveraging a bug or vulnerability in an application or operating system to gain access to resources, which normally would have been protected from an average user.
- These are attacks that are usually run locally and are concerned with increasing privilege.

Privilege Escalation

- The objective is to force an application to perform actions that are running within a higher security context than intended by the designer, and the hacker is granted full local access and control.
 - For example, this exploit here will escalate your privilege in Linux Kernel <= 2.6.36-rc8 RDS privilege escalation exploit:
 - <https://www.exploit-db.com/exploits/15285/>

Maintaining Access and Covering Tracks

- After an attacker is on a Linux system and has made himself root, he will be concerned with maintaining access and covering his tracks.
- One of the best ways to maintain access is with a rootkit.
- A rootkit contains a set of tools and replacement executables for many of the operating system's critical components.
- Once installed, a rootkit can be used to hide evidence of the attacker's presence and to give the attacker backdoor access to the system.
- Rootkits can contain log cleaners that attempt to remove all traces of an attacker's presence from the log files.

Maintaining Access and Covering Tracks

- Rootkits can be divided into two basic types: traditional, which replace binaries, and loadable kernel modules, which corrupt the kernel.
- Traditionally, rootkits replaced binaries, such as ls, ifconfig, inetd, killall, login, netstat, passwd, pidof, or ps with trojaned versions.
- These trojaned versions have been written to hide certain processes or information from the administrators.
 - Tools, like MD5sum and Tripwire, can help in uncovering these types of hacks.

Maintaining Access and Covering Tracks

- The second type of rootkit is the loadable kernel module (LKM).
- A kernel rootkit is loaded as a driver or kernel extension. Because kernel rootkits corrupt the kernel, they can do basically anything, including detection by many software methods.
- The best way to avoid these rootkits is simply to recompile the kernel without support for LKMs.
- Examples include: Flea and Adorm

Maintaining Access and Covering Tracks

- All rootkits allow an attacker to:
 - Run packet sniffers covertly to capture passwords.
 - Trojan the login binary to open a backdoor for anytime access.
 - Replace utility programs that can be used to detect the hacker's activity.
 - Provide utilities for installing Trojans with the same attributes as legitimate programs.

Maintaining Access and Covering Tracks

- Two major tools can be used to audit suspected rootkit attacks:
 - **Chkrootkit:** An excellent tool that can be used to search for signs of a rootkit. It has the capability to examine system binaries for modification.
 - **Rootkit Hunter:** Another tool that scans file and system binaries for known and unknown rootkits.
- Finding the rootkit is not the same as seeing justice done. The overwhelming majority of individuals who attack systems go unpunished. The global nature of the Internet makes it hard to track hackers and bring them to justice.

Linux Hardening

- This can mean patching, removing, or hardening those services.
- Placing a firewall in front of critical servers is also an important step. Programs, such as ipchains and iptables, can also be used to filter and control traffic.
- Another easy solution is to remove programs and services if they aren't needed.
- This is known as the principle of least privilege.

Linux Hardening

- Some of the programs and services that are considered nonessential might include:
 - Wget, Finger, Lynx, Curl, SCP, FTP, Telnet, Trivial FTP and Ping.
 - Turning off unneeded services, removing unnecessary programs, and applying the latest security patches is known as hardening a system. When trying to harden your Linux system, one good source of information is the NSA hardening guidelines; they can be found at http://www.nsa.gov/ia/mitigation_guidance/security_configuration_guides/operating_systems.shtml.

Linux Hardening

- Chroot basically puts a program in a sandbox.
- The term sandbox refers to the concept of limiting the activity of a program and applying boundaries.
- Because of this lockdown, it is important to remember that any files a chrooted program needs for proper functionality must be present inside the jail.
- Chroot is commonly used by programs such as FTP, BIND, mail, and Apache.

Linux Hardening

- TCP Wrapper is another tool that can be used to harden Linux.
- For many years, this was one of the default methods used to harden Linux. It's now being replaced by xinetd.d, which is considered more granular. Network services such as Finger, FTP, Rlogin, Telnet, and TFTP can be configured for TCP Wrapper use.

Linux Hardening

- More information about TCP Wrapper follows:
 - TCP Wrapper allows you to specify which hosts are allowed access.
 - TCP Wrapper is activated by having inetd call the TCP Wrapper daemon.
 - TCP Wrapper can be used with TCP or UDP.
 - Two files are used to verify access host.allow and host.deny.
 - **hosts.allow** Lists all hosts with connectivity to the system that can connect to a specific service.
 - **hosts.deny** Works in the same fashion as most ACLs because if it is not expressly permitted, access is then denied.

Linux Hardening

- Tripwire is another valuable tool that can be used to secure Linux systems.
- Tripwire is the most commonly used file integrity program. It performs integrity checking by using cryptographic checksums. Tripwire can help you identify if any file tampering has occurred.
- It is commonly used with IDS systems because it can be used to maintain a snapshot of the system while in a known good state.

Linux Hardening

- If rootkits or other changes are made, Tripwire can detect it. Tripwire performs its magic by creating a one-way hash value for files and directories.
- This hash is stored, and then periodically new scans are performed. The new scanned value is compared against the stored ones.

Linux Hardening

- Finally, there is logging. Although logging will not prevent an attack, it is a useful tool for determining what happened. Linux will allow you to log systems, applications, and protocols.
- The output of most logs are kept in the /var/log directory. If you are curious about who has logged in to the system, you can use the lastlog file. The /var/log/lastlog file tracks the last login of user accounts into the system.

Automated Assessment Tools

- It's not always possible to perform every security test manually.
- Many checks, scans, and fixes are best performed by automated tools. So many new vulnerabilities are discovered daily that it's hard to keep up.
- If you're not using an automated patch management system, how do you know if all the patches that should have been installed actually have been?

Automated Assessment Tools

- Automated tools allow the ethical hacker to cover a lot of ground quickly and use the results for further manual inspection.
- An entire range of security assessment tools are available.
- Some look at source code, others look at applications, and still others are developed to look at entire systems or networks.

Automated Assessment Tool Categories

- All these tools can be broken into three basic categories, including
 - Source code scanners examine the source code of an application.
 - Application scanners examine a specific application or type of application.
 - System scanners examine entire systems or networks for configuration or application-level problems.
- These tools can be open source, commercial or available through subscription.

Source Code Scanners

- Source code scanners can be used to assist in auditing security problems in source code.
- Source code scanners can detect problems, such as buffer overflows, race conditions, privilege escalation, and tainted input.

Source Code Scanners

- Buffer overflows enable data to be written over portions of your executable, which can allow a malicious user to do just about anything.
- Race conditions can prevent protective systems from functioning properly, or deny the availability of resources to their rightful users.

Source Code Scanners

- Privilege escalation occurs when code runs with higher privileges than that of the user who executed it.
- Tainting of input allows potentially unchecked data through your defenses, possibly qualified as already error-checked information.

Source Code Scanners

- Examples of source code scanners:
- Flawfinder , Rough Auditing Tool for Security (RATS), StackGuard and Libsafe

Application Level Scanners

- Application scanners provide testing against completed applications or components rather than the source code.
- This type of assessment tool looks at vulnerabilities as the program is running.
- Scanners can examine their configuration and look for problems.

Application Level Scanners

- Examples of application-level scanners include:
- Whisker, N-stealth, WebInspect, AppDetective and Nikto

System-level Scanners

- These types of scanners are versatile in that they can probe entire systems and their components rather than individual applications.
- A system-level scanner can be run against a single address or a range of addresses and can also test the effectiveness of layered security measures, such as a system running behind a firewall.

System-level Scanners

- Examples of system-level scanners include:
- Nessus, (Nessus Windows Technology) NeWT, Saint, Sara, Internet Security Systems (ISS) internet scanner, Netrecon, Retina, LANguard and Vlad