Network and System Security

Dr. Gaurav Varshney

Learning Objectives

- Why are we learning Network and System Security
  - We have already learned basics of Networks in Computer Networks
    - We learned how data flows on the Internet
      - Now we will learn how data **securely** flows over the Internet
    - When we have data flowing on the Internet there will be
      - **Attacks**
        - We will hence try to learn the attacks at various layers of TCP/IP protocol stack
        - Obviously we need to study the **countermeasures** too to safeguard systems.
  - We did learned the basics of operating systems
    - We will now see how systems and software can be attacked in a variety of different ways and how they can be safeguarded.
      - Malwares, viruses
      - Buffer overflows
      - Reverse engineering of software, cracking
      - Windows and Linux internals

Week 1: Introduction to Security Concepts

- Highlights
  - Cyber Security, Cyber Threats, Types of Hackers, Lingo, Pen Testing, Hacking Methodology
  - CIA Triad, Authentication, Authorization and Accountability
    - Bella La Padula Model
    - Biba Model
  - Security Design Concepts
  - OSI Security Architecture Concepts

What is Cyber Security ?

- **Cybersecurity** is the practice of protecting systems, networks, and programs from digital attacks. **(Cisco)**
  - *These attacks are usually aimed at accessing, changing, or destroying sensitive information; extorting money from users; or interrupting normal business processes.*

- **Cyber Security** is: **(Department of Education, United States of America)**
  - ***Protection*** *of information systems* ***against unauthorized*** *access to or* ***modification*** *of information, whether in storage, processing or transit, and*
  - *against the* ***denial*** *of service to authorized users, including those measures necessary to detect, document, and counter such threats."*

- **Cybersecurity** refers to a set of techniques used to protect the integrity of networks, programs and data from attack, damage or unauthorized access. **(Palo Alto Networks)** https://www.paloaltonetworks.com/cyberpedia/what-is-cyber-security
  - *The core functionality of cybersecurity involves:*
    - protecting information and systems from major cyberthreats.
    - These cyberthreats take many forms
    - (e.g., application attacks, malware, ransomware, phishing, exploit kits).

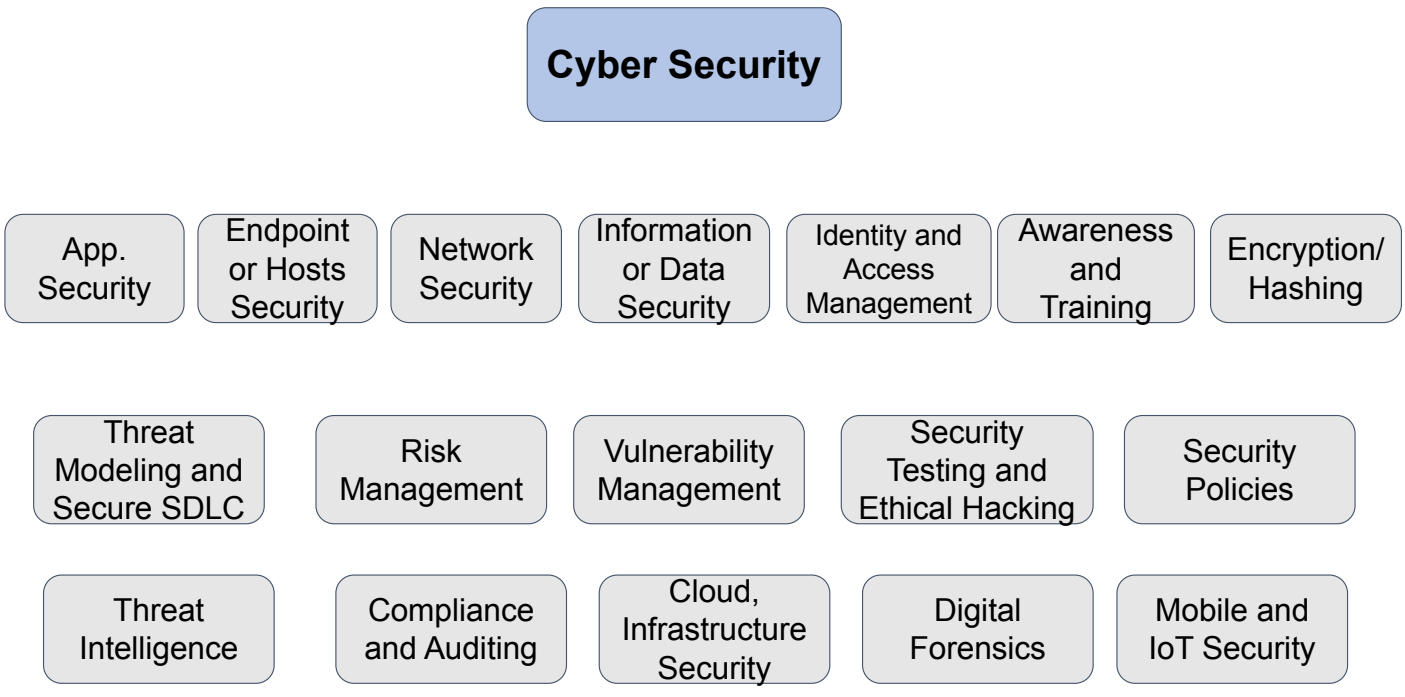
- **Cyber-safety** is a common term used to describe a set of practices, measures and/or actions you can take to protect personal information and your computer from attacks. **(UC Davis)**

Ransomware is a type of malware that threatens to publish the victim's personal data or permanently block access to it unless a ransom is paid off[1]. It encrypts the victim's files, making them inaccessible, and demands a ransom payment to decrypt them[1]. Ransomware attacks are typically carried out using a Trojan disguised as a legitimate file that the user is tricked into downloading or opening when it arrives as an email attachment[1].

Cybersecurity/Network & Systems Security

- **Cybersecurity** refers to a set of techniques used to protect the integrity of networks, programs and data from attack, damage or unauthorized attacks. [paloaltonetworks.com]
  - **Network and System Security**
    - Collectively It pertains to efforts through which you protect your network and systems from attacks.
    - Cybersecurity is a bigger and general term which encompasses almost everything required to secure the digital world as a whole.
    - Though when we say Network Security we try to see the attacks over TCP/IP protocol stack and the corresponding countermeasures.
    - When we say Systems Security we try to see how the hosts/end systems are affected by attacks [malwares, worms, Trojans, buffer overflows etc.] and how various countermeasures can be developed to thwart them.

Dr. Gaurav Varshney, IIT Jammu



Cyber Threats

- There can be two angles to defining cyber threats
  - You can define It in a broader scope such as
    - Cyberterrorism
    - Cyberwarfare
    - Cyberespionage
  - Or you can define it more granularly
    - Ransomware
    - Malware
    - Social Engineering
    - Phishing etc.

Vulnerability, Threat, Exploit and Attack

1. Weakness is Vulnerability
2. Threat is potential danger from a Vulnerability
3. Exploit is a specific code or technique through which the threat from a vulnerability can be realized
4. Attack is when an exploit successfully realize a vulnerability.

Cyber Threats (Palo Alto Networks)

- Some of the common threats are outlined below in more detail.
  - ***Cyberterrorism*** *is the disruptive use of information technology by terrorist groups to further their ideological or political agenda.*
  - ***Cyberwarfare*** *involves nation-states using information technology to penetrate another nation's networks to cause damage or disruption.*
    - Fifth domain of warfare (following land, sea, air and space)
  - ***Cyberespionage*** *is the practice of using information technology to obtain secret information without permission from its owners or holders.*

Cyber Threats ? (CISCO)

- **Ransomware :** Ransomware is a type of malicious software. It is designed to extort money by blocking access to files or the computer system until the ransom is paid. Paying the ransom does not guarantee that the files will be recovered or the system restored.
- **Malware:** Malware is a type of software designed to gain unauthorized access or to cause damage to a computer.
- **Social engineering:** Social engineering is essentially the art of gaining access to buildings, systems or data by exploiting human psychology, rather than by breaking in or using technical hacking techniques.
  - *For example, instead of trying to find a software vulnerability, a social engineer might call an employee and pose as an IT support person, trying to trick the employee into divulging his password.*
- **Phishing:** Phishing is the practice of sending fraudulent emails that resemble emails from reputable sources. The aim is to steal sensitive data like credit card numbers and login information. It's the most common type of cyber attack.
  - *https://www.cisco.com/c/en/us/products/security/what-is-cybersecurity.html*

Security Principles: CIA Triad

CIA stands for Confidentiality, Integrity and Availability. This is a model which is designed for guiding policies for information security within an organization.

Confidentiality: Rules to limit access to information.

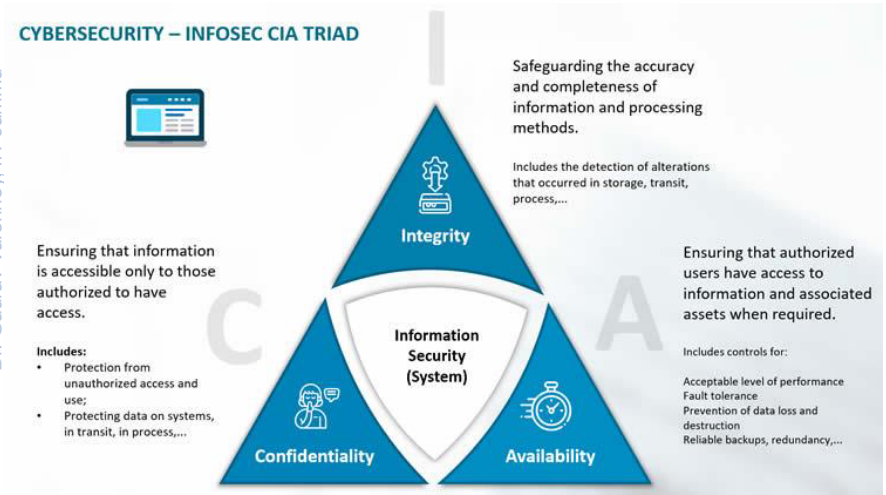
Integrity: Assurance that the information is correct and trustworthy

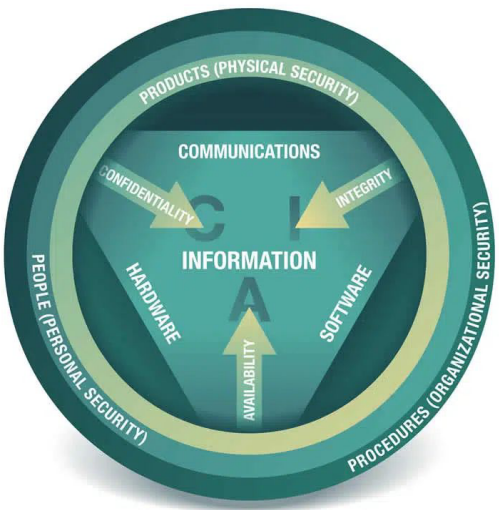
Availability: Uninterrupted on demand access to information whenever desired by authorized entities

[Which one is more important ? Depends on organization goals]

1. Whenever you design a product or a service you should make sure that CIA is satisfied
2. Facebook ? Think About It….
   1. When two people talk over chat or even when you browser Facebook data gets encrypted so that no one can see what you are doing and what you are chatting
   2. No one can edit your previous chats or a real time chat you send from your messenger to your friend.
   3. You can access your chats, browse Facebook, access your profile almost anytime on demand from anywhere with access to Internet.
   4. What if you miss CIA?
      1. You will find security problems in your product or service….

Dr. Gaurav Varshney, IIT Jammu





https://www.i-scoop.eu/cybersecurity/cia-confidentiality-integrity-availability-security/

Dr. Gaurav Varshney, IIT Jammu

OSI Security Architecture Understanding

You have three important classifications

1. Security Attack
   a. Passive [Release of message contents, Traffic Analysis]
   b. Active [Masquerade, Replay, Modification, DoS]
2. Security Mechanism
3. Security Service

Security services uses one or more security mechanism to counter security attacks.

OSI Security Architecture Understanding

Security Service

Authentication

- Peer Entity Authentication
- Data Origin Authentication

Access Control

Data Confidentiality

- Connection Confidentiality
- Connectionless Confidentiality
- Selective Field Confidentiality
- Traffic Flow Confidentiality

Data Integrity

- Connection Integrity with Recovery
- Connection Integrity without Recovery
- Selective Field Connection Integrity
- Connectionless Integrity
- Selective Field Connectionless Integrity

Non Repudiation

- Non repudiation source
- Non repudiation destination

Dr. Gaurav Varshney, IIT Jammu

OSI Security Architecture Understanding

Security Mechanisms

- Enchipherment
- Digital Signature
- Access Control
- Data Integrity
- Traffic Padding
- Routing Control
- Notarization

Encipherment is the process of converting a message into cipher or code[1]. It deals with hiding and covering of data which helps data to become confidential[2]. It is achieved by applying mathematical calculations or algorithms which reconstruct information into not readable form[2].

A digital signature is a mathematical scheme for verifying the authenticity of digital messages or documents[2]. It is an electronic, encrypted, stamp of authentication on digital information such as email messages, macros, or electronic documents[3]. A signature confirms that the information originated from the signer and has not been altered[3]. You can use a digital signature to comply with the most demanding legal and regulatory requirements because it provides the highest level of assurance about each signer's identity and the authenticity of the documents they sign.

Here are some security mechanisms that can be used to secure data and resources in a computing environment:
- **Data Integrity**: Ensures that data is not modified or corrupted during transmission or storage.
- **Traffic Padding**: Adds extra data to a message to make it more difficult to intercept or decode.
- **Routing Control**: Determines the path that data takes through a network to prevent unauthorized access or interception.
- **Notarization**: Provides a trusted third-party verification of the authenticity of a document or message.

Penetration testing is a type of security testing that is used to identify vulnerabilities in a system or network. It involves simulating an attack on a system to identify weaknesses that could be exploited by an attacker. Penetration testing can be used to test the effectiveness of security measures and to identify areas where improvements can be made.
Gray box and white box are terms used to describe testing approaches where the tester has some knowledge of the internal workings of the software being tested. In gray box testing, the tester has limited knowledge of the internal workings of the software being tested, while in white box testing, the tester has full knowledge of the internal workings of the software being tested.
Black box is a term used to describe a system or device that can be viewed in terms of its inputs and outputs without any knowledge of its internal workings. It is often used in the context of software testing to describe a testing approach where the tester has no knowledge of the internal workings of the software being tested.

Hacking / Attacking

Types of Hackers	Lingo of the Trade	Penetration Testing
Script Kiddies	Hack Value	Black Box
White Hat	Target of Evaluation	Gray Box
Gray Hat	Exploit	White Box
Black Hat	Zero Day	
Suicide Hackers	Daisy Chaining	

Hacking Methodology: It is a step by step approach used by an attacker to compromise a system

1. Footprinting - Google Hacking, Netcraft.com, Link Extractor, People Search (Spokeo), Social Engineering, Maltego, Whois, Nslookup
2. Scanning - Port Scan, Network Scan, Vulnerability Scan, Nmap, TCP Scans, OS Fingerprinting
3. Enumeration - NetBIOS, SMTP enumeration
4. System Hacking - Password Cracking, Session Hijacking, Phishing, Injection Attacks, Spywares
5. Escalation of Privilege
6. Covering Attacks
7. Planting Backdoors

Hacking methodology is a step-by-step approach used by an attacker to compromise a system. The following are the steps that most hackers follow:

1. **Footprinting**: Footprinting is the process of gathering information about a target system that can be used to execute a successful cyber attack. This information is the first road for the hacker to crack a system. There are two types of footprinting: Active Footprinting and Passive Footprinting. Active footprinting means performing footprinting by getting in direct touch with the target machine, while passive footprinting means collecting information about a system located at a remote distance from the attacker [2]. Different kinds of information that can be gathered from Footprinting are as follows: The operating system of the target machine, Firewall, IP address, Network map, Security configurations of the target machine, Email id, password, Server configurations, URLs, VPN [2].

2. **Scanning**: Scanning is a network exploration technique used to identify the systems connected to an organization's network. It provides information about the accessible systems, services, and resources on a target system. Scanning allows you to identify open ports on the target system and can be used for port mapping, performing an interactive session with the operating system via those ports, or even redirecting traffic from these open ports. There are many tasks that can be performed with a scanning tool. Scanning can be as simple as creating a list of IP addresses and netmasks to scan all the active addresses on the network .

3. **Enumeration**: Enumeration is extracting a system's valid usernames, machine names, share names, directory names, and other information. It is a key component of ethical hacking and penetration testing, as it can provide attackers with a wealth of information that can be used to exploit vulnerabilities. Enumeration can be used in both an offensive and defensive manner [1].

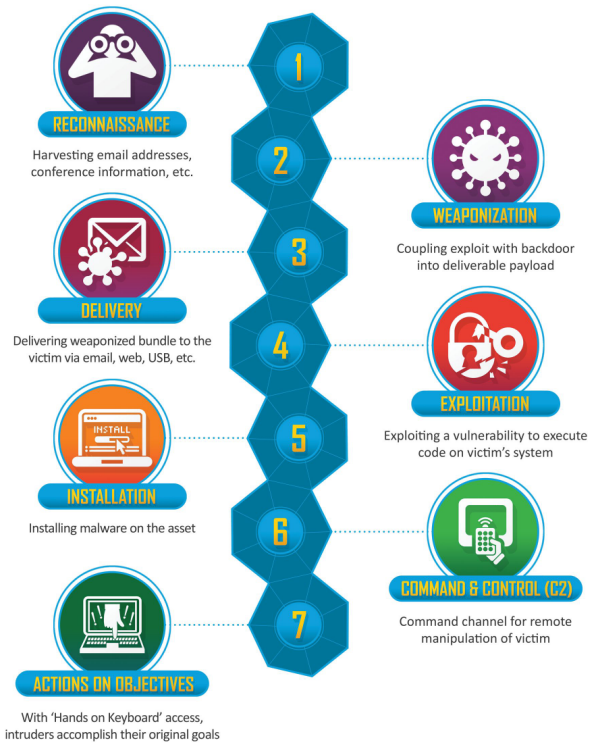
4. **System Hacking**: System hacking is the process of exploiting vulnerabilities in electronic systems for the purpose of gaining unauthorized access to those systems. Hackers use a variety of techniques and methods to access electronic systems, including phishing, social engineering, and password guessing [1].

5. **Escalation of Privilege**: Privilege escalation is a cyberattack technique where an attacker gains unauthorized access to higher privileges by leveraging security flaws, weaknesses, and vulnerabilities in an organization's system. It is the attempt to elevate access permissions by exploiting bugs, system flaws, human behaviors, configuration oversights or weak access controls .

6. **Covering Attacks**: Covering attacks are techniques used by hackers to hide their tracks and evade detection. It involves manipulating system logs and other records to make it appear as though nothing has been compromised [2][2].

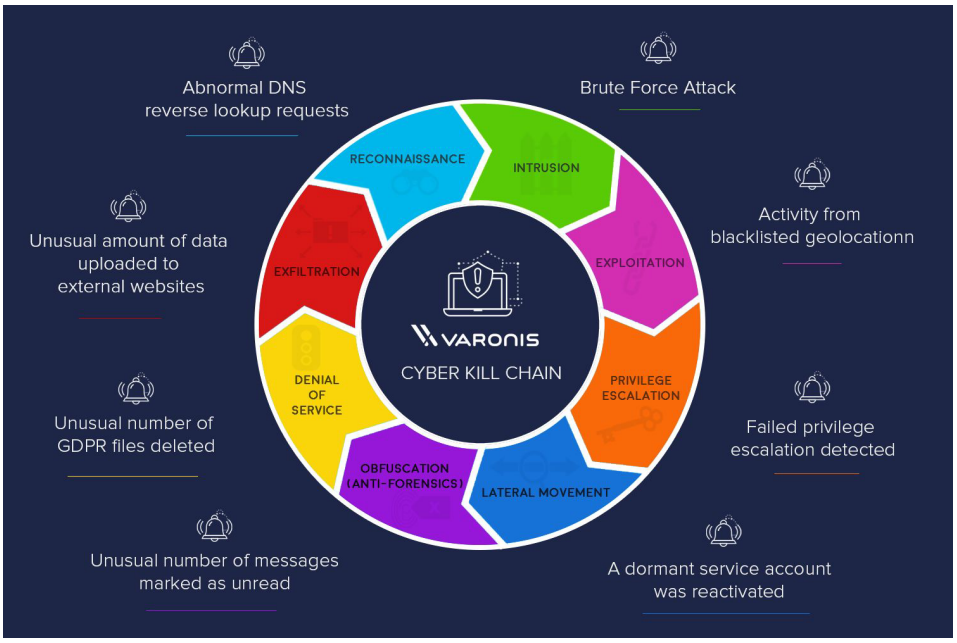
7. **Planting Backdoors**: Planting backdoors is leaving an entry point to a compromised system for easy access in further attack activities [1][2].

Dr. Gaurav Varshney, IIT Jammu



https://www.computer.org/publications/tech-news/trends/what-is-the-cyber-kill-chain-and-how-it-can-protect-against-attacks

https://www.lockheedmartin.com/en-us/capabilities/cyber/cyber-kill-chain.html



https://www.varonis.com/blog/cyber-kill-chain

Access Control: Authentication and Authorization Concepts

- Authentication
  - Checks whether you are authentic?
    - What is authentic and what is not?
      - Actually authentication is nothing but verification of an entity.
        - Entity can be a person can be a process can be a device etc.
- Authorization
  - Checks whether you are allowed to do an operation over data or resource [Access, Create, Delete]
    - Are you allowed to do an operation you are doing?
      - Resource can be data, device or service.

- Authentication allows you to login to ERP but what all you can do on ERP is based on whether you are authorized to do that or not.
  - Students can see a form to file a request
  - Faculty can see student requests and approve/disapprove a request
  - Dean can see request of faculties and students and approve/disapprove it.

  - We do have one more term as Accounting where we try to monitor if things are going well in authentication and authorization implementation by capturing the events and analyzing them.
  - When combined we call it as AAA [Authentication, Authorization and Accounting]

Access Control: Authentication and Authorization Concepts

- Authentication
  - Identification
    - User Id, TLS Certificates
  - Verification
    - Password, TLS Certificate Chain Validation and Key Exchange
  - We will learn this deeply in coming lectures
  - Humans can be verified by
    - Something they know - Password, PIN
    - Something they have - Smart Card/Token, BLE Watch
    - Something they are - Fingerprint, Iris, Palm, Face

- Security Assertion Markup Language [SAML] and Single Sign On [**We will take it up later**]
- Web Cookies for login token [Let us try and do a login via login session cookie]

Security Assertion Markup Language (SAML) is an open standard for exchanging authentication and authorization data between parties, in particular, between an identity provider and a service provider. SAML is an XML-based markup language for security assertions. It is also a set of XML-based protocol messages, a set of protocol message bindings, and a set of profiles (utilizing all of the above). An important use case that SAML addresses is web-browser single sign-on (SSO) [1].

SSO-: an identification system that allows users to access multiple applications and website with one set of login credentials.

Access Control: Authentication and Authorization Concepts

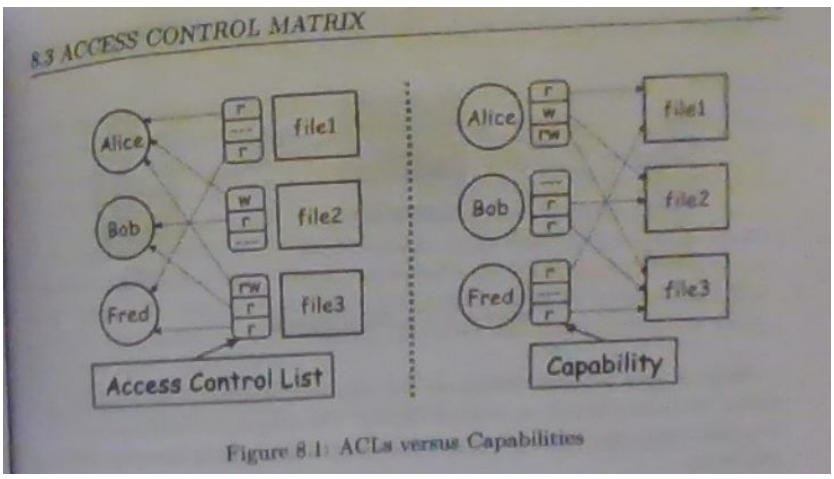
- Authorization
  - Begins with Lampson's access control matrix. [Butler W. Lampson in 1971]
    - The matrix contain all information needed by an operating system to decide which users can do what operations on system resources
    - There is a classification of
      - Subject: A user of the system
      - Object: A system resource.
    - Two fundamental constructs are
      - Access Control Lists
      - Capabilities List
    - Both are derived from Lampson's access control matrix where subject are represented by rows and objects are represented as columns.

	OS	**Accounting Program**	**Payroll Data**
Bob	rx	rx	--
Ram	rwx	rx	rw

Access Control Lists for Payroll Data [Taking out the column from the access control matrix]
(Bob --),(Ram, rw)
File permissions in Linux systems [ls -l \home\user]
Routers also use ACLs like this ACL on a CISCO router [see that the netmask is inverted]
access-list 101 permit ip 192.168.10.0 0.0.0.255 192.168.200.0 0.0.0.255

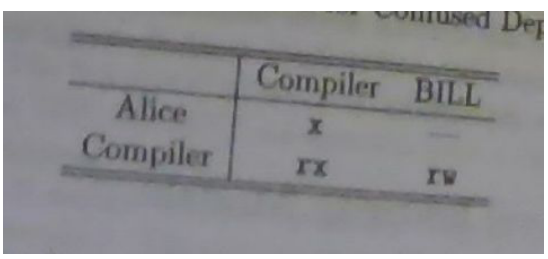
Access Control: Authentication and Authorization Concepts

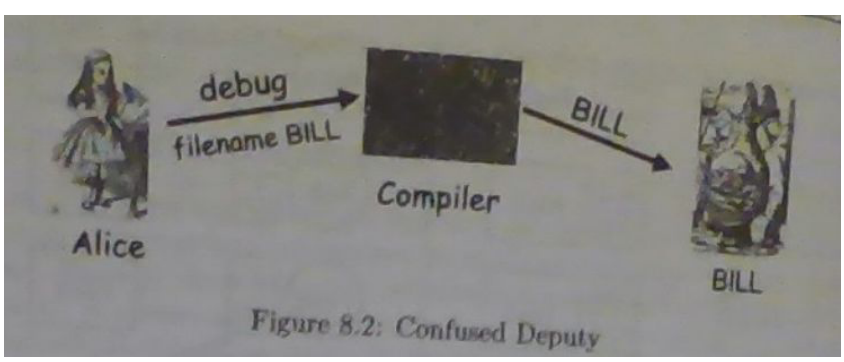
- Authorization
  - What if we store the contents of ACL in row format
    - Then we call it as capabilities as we are referring to what a subject can do on an object
    - For example Ram's C list will be
      - (OS, rwx), (Accounting Program, rx), (Payroll data, rw)



Access Control: Authentication and Authorization Concepts

- Confused Deputy Problem





Access Control Types

- Discretionary Access Control
  - The owner decides who should get access to a resource and who should not.
- Role Based Access Control
  - The role of a subject decides the operations permitted on objects
- Mandatory Access Control
  - The subjects have a security clearance and the object has a security classification as decided by the system administrator.
    - The operations are permitted based on the security clearance of the subject [level 1-5] and security classification of the object [secret/top secret]

confidentiality of the system

Multilevel Security: Bell LaPadula Model [Mark Stamp, Wiley]

- The purpose of multilevel security system is to enforce a form of access control by restricting subjects so that they only access objects for which they have necessary security clearance.
- The U.S. Department of Defense or DoD employs four level of classifications which are:
  - Top Secret > Secret > Confidential > Unclassified
- If O denotes an object and S denotes a subject we can denote L(O), L(S) as the security level of O and security clearance of S respectively.
- Objects have a security classification and Subjects have security clearances.
- Bell LaPadula Model capture minimal requirements for ensuring confidentiality of data in an MLS.
  - Simple Security Condition: Subject S can read object O if and only if L(O) <= L(S)
  - *_Property (Star Property): Subject S can write object O if an only if L(S)<=L(O)
  - Tranquility Property [Solution to McLean question which states that administrator can reclassify objects temporarily at which point they can be modified]
    - Weak and Strong Tranquility Property

No read up and No Write Down

Security clearance:- an authorization that allows access to information that would otherwise be forbidden

strong tranquility: security levels do not change during the normal operation of the system
weak tranquility: security levels may never change in such a way as to violate a defined security policy.

Top secret can't write in secret, and secret can't read Top-secret.

Biba Model (No Read Down No Write Up)

BLP deals with Confidentiality while Biba deals with Integrity

Let I(O) and I(S) denote integrity of object O and subject S then

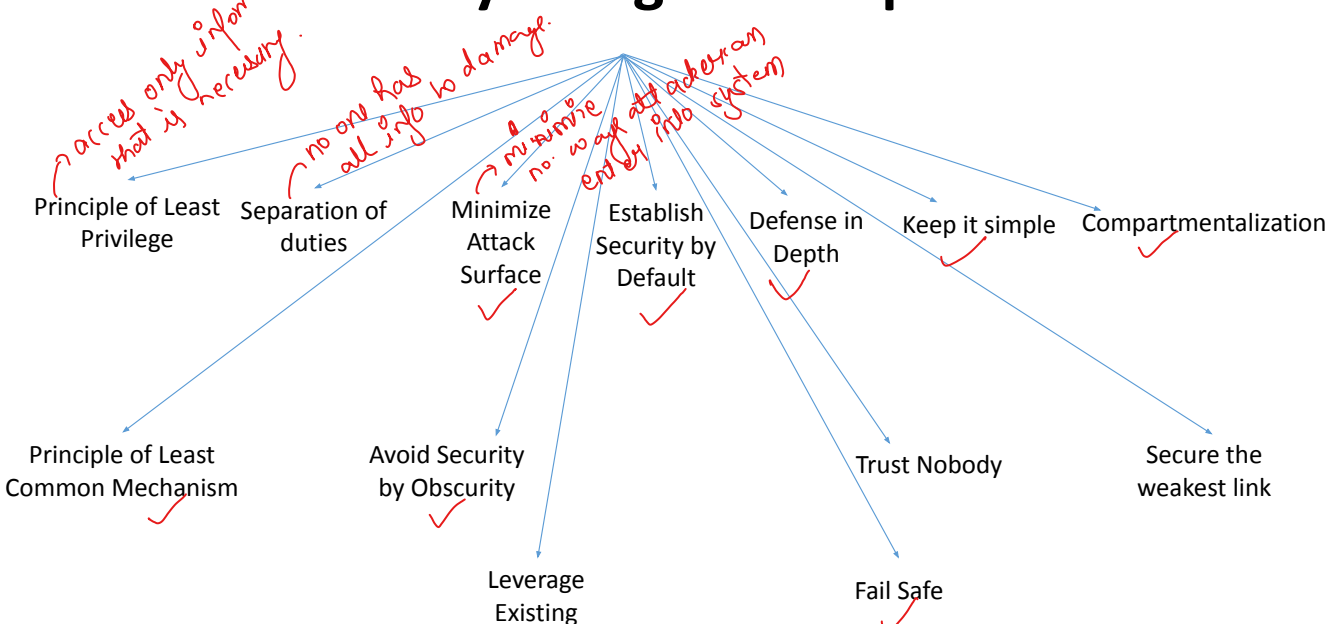
Write Access Rule: Subject S can write object O if and only if I(O)<=I(S)
Read Access: A subject S can read the object O if and only of I(S)<=I(O)

Low Water Mark Policy: If subject S reads object O, the I(S)= min(I(S), I(O))

Low water mark policy states that, subject S can ready anything under the condition that the integrity of subject S is downgraded after accessing an object at a lower level

The Biba integrity model protects information from unauthorized changes.

Security Design Concepts



1. **Minimize attack surface area**: Reduce the number of ways an attacker can enter a system.
2. **Establish security by default**: Ensure that security is enabled by default and not as an afterthought.
3. **Defense in depth**: Use multiple layers of security to protect against attacks.
4. **Keep it simple**: Avoid complexity in security mechanisms and designs.
5. **Compartmentalization**: Separate different parts of a system to prevent unauthorized access.
6. **Fail safe**: Ensure that a system fails securely when something goes wrong.
7. **Avoid security by obscurity**: Do not rely on secrecy to provide security.
8. **Principle of least common mechanism**: Use different mechanisms for different parts of a system to prevent attacks from spreading.
9. **Secure the weakest link**: Identify and secure the weakest part of a system to prevent attacks from exploiting it.

Web Security Policies: HTTP Strict Transport Security

- Strict Transport Security is a response header from the server and it informs the browser to always open the site over an HTTPS connection.
  - One may say that website can connect over HTTP and redirect the user to HTTPS connections

```
HTTP/1.1 301 Moved Permanently
Server: Server
Date: Sun, 30 Aug 2020 14:24:58 GMT
Content-Type: text/html
Content-Length: 179
Connection: keep-alive
Location: https://amazon.in/
```

  - Then what is the benefit of HSTS?
    - Can an attacker in between modify the HTTP response from the server and add 301 moved permanently
      - He can also add location of redirect as a Phishing site?
    - HSTS is for rescue in this situation. It does not let the browser initiate any connection over HTTP even if user wants it to be [mistakenly typing HTTP etc.]
  - Browser only honor Strict-Transport-Security response header from a server if communicated over HTTPS

Web Security Policies: HTTP Strict Transport Security

- The Header whenever returned by the server over HTTPS updates the previous values stored for a particular site in the browser
  - What if the server want the connections to fall back to HTTP.
  - It can set the max-age field to 0.
  - You can also add preload in the options. Browsers has a preloaded list of websites which should always be opened on HTTPS as submitted by website owners and accepted by browser community. Google maintains a preload list.

```
GET /runtime.26209474bfa8dc87a77c.js HTTP/1.1
Host: iitjammu.ac.in
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:79.0) Gecko/20100101 Firefox/79.0
Accept: */*
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Referer: https://iitjammu.ac.in/
Connection: close
```

```
HTTP/1.1 200 OK
X-Powered-By: Express
Access-Control-Allow-Origin: *
X-Frame-Options: SAMEORIGIN
Strict-Transport-Security: max-age=864000; includeSubDomains
X-Content-Type-Options: nosniff
X-XSS-Protection: 1; mode=block
Referrer-Policy: same-origin
Content-Security-Policy: default-src 'self'; style-src 'self' 'unsafe-inline' https://fonts.goo
Accept-Ranges: bytes
Cache-Control: public, max-age=0
Last-Modified: Tue, 21 Jul 2020 10:20:48 GMT
ETag: W/"5a0-17370e3df98"
Content-Type: application/javascript; charset=UTF-8
Vary: Accept-Encoding
Date: Sun, 30 Aug 2020 14:00:11 GMT
Connection: close
Content-Length: 1440
```

Web Security: Securing Cookies

- We use cookies for session management, personalization and tracking.
  - Server send a Set-Cookie header in the HTTP response and browser saves the information
  - Browser revert back with the cookie information whenever the website is revisited allowing webserver to do the necessary pre processing for the client [auto login, setting preferences etc.]
  - **Set Cookie: auto_login=X7xkbakbd….; cookiename2=cookievalue2….**

```
HTTP/1.1 200 OK
Server: Server
Date: Sun, 30 Aug 2020 14:27:38 GMT
Content-Type: text/html;charset=ISO-8859-1
Content-Length: 651
Connection: close
Cache-Control: max-age=0, no-cache, no-store, private, must-revalidate, s-maxage=0
Pragma: no-cache
Expires: Thu, 01 Jan 1970 00:00:00 GMT
p3p: policyref="https://www.amazon.com/w3c/p3p.xml", CP="PSAo PSDo OUR SAM OTR DSP COR"
Set-Cookie: ad-id=A0ka2b8hUk0VjmJEwJilQcM; Domain=.amazon-adsystem.com; Expires=Thu, 01-Apr-2021 14:27:37 GMT; Path=/; HttpOnly
Set-Cookie: ad-privacy=0; Domain=.amazon-adsystem.com; Expires=Wed, 01-Oct-2025 14:27:38 GMT; Path=/; HttpOnly
Vary: Accept-Encoding,User-Agent
```

Web Security: Securing Cookies

- **Secure Cookies:**
  - Set a lifetime for cookies. **Expires** as soon as the session ends, other cookies expires after the time as mentioned in Set Cookie Header expires.
  - A cookie with **Secure** attribute set is sent over HTTPS connection only.
  - A cookie with **HttpOnly** attribute set is only sent to server and not to client side Java Scripts [document.cookie API] thwarting XSS.
  - **Domain** attribute if set explicit which domains and subdomains are allowed to receive the cookie. Browser sends the cookies only to the specified domains and its subdomains. If the attribute is not present defaults to domain excluding subdomains.

```
HTTP/1.1 200 OK
Server: Server
Date: Sun, 30 Aug 2020 14:27:38 GMT
Content-Type: text/html;charset=ISO-8859-1
Content-Length: 651
Connection: close
Cache-Control: max-age=0, no-cache, no-store, private, must-revalidate, s-maxage=0
Pragma: no-cache
Expires: Thu, 01 Jan 1970 00:00:00 GMT
p3p: policyref="https://www.amazon.com/w3c/p3p.xml", CP="PSAo PSDo OUR SAM OTR DSP COR"
Set-Cookie: ad-id=A0ka2b8hUk0VjmJEwJilQcM; Domain=.amazon-adsystem.com; Expires=Thu, 01-Apr-2021 14:27:37 GMT; Path=/; HttpOnly
Set-Cookie: ad-privacy=0; Domain=.amazon-adsystem.com; Expires=Wed, 01-Oct-2025 14:27:38 GMT; Path=/; HttpOnly
Vary: Accept-Encoding,User-Agent
```

Web Security: Securing Cookies

- **Secure Cookies:**
  - If **Path** attribute is set the browser send the cookies to the website only when they are requested through a URL having the matching path component.
    - /
    - /rootdirectory or /rootdirectory/subdirectory
  - **SameSite** attribute : Strict, Lax, None
    - Strict: Sent to only the first party when visited directly by the user
    - Lax: Sent when the request is GET and top level
    - None: The cookies have no restrictions to be sent to third parties

```
HTTP/1.1 200 OK
Server: Server
Date: Sun, 30 Aug 2020 14:27:38 GMT
Content-Type: text/html;charset=ISO-8859-1
Content-Length: 651
Connection: close
Cache-Control: max-age=0, no-cache, no-store, private, must-revalidate, s-maxage=0
Pragma: no-cache
Expires: Thu, 01 Jan 1970 00:00:00 GMT
p3p: policyref="https://www.amazon.com/w3c/p3p.xml", CP="PSAo PSDo OUR SAM OTR DSP COR"
Set-Cookie: ad-id=A0ka3b8hUk0VjmJEwJilQcM; Domain=.amazon-adsystem.com; Expires=Thu, 01-Apr-2021 14:27:37 GMT; Path=/; HttpOnly
Set-Cookie: ad-privacy=0; Domain=.amazon-adsystem.com; Expires=Wed, 01-Oct-2025 14:27:38 GMT; Path=/; HttpOnly
Vary: Accept-Encoding,User-Agent
```

	First-Party Cookies	Third-Party Cookies
Setting and Reading the Cookie	Can be set by the publisher's web server or any JavaScript loaded on the website.	Can be set by a third-party server (e.g. an AdTech platform) via code loaded on the publisher's website.
Availability	A first-party cookie is only accessible via the domain that created it.	A third-party cookie is accessible on any website that loads the third-party server's code.
Browser Support, Blocking and Deletion	Supported by all browsers and can be blocked and deleted by the user, but doing so may provide a bad user experience.	Supported by all browsers, but many are now blocking the creation of third-party cookies by default. Many users also delete third-party cookies on a regular basis.

https://clearcode.cc/blog/difference-between-first-party-third-party-cookies/

Dr. Gaurav Varshney, IIT Jammu

Web Security Policies: Same Origin Policy [SOP]

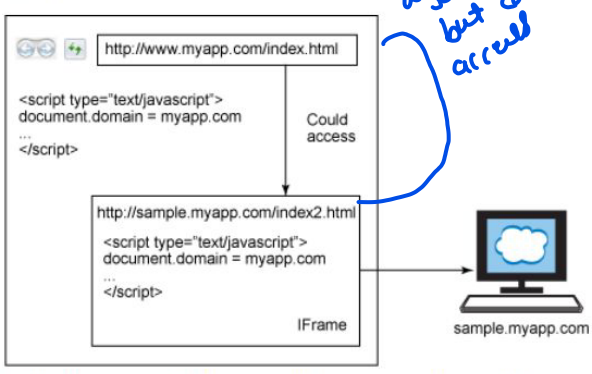
- Two URLs are said to be having the same origin if the Protocol, Port and Host are the same.
- http://example.com and http://example.com/form.html are from same origin
- https://www.example.com and http://www.example.com are from different origin [see the protocol difference]
- Browser enforce same origin policy which if does not get applied any domain can access data of any other domain through the browser via the DOM.
- A subdomain can ask for same origin policy checks over its parent domain by setting the document.domain property as the parent domain name.
  - This relax communication between two subdomains of a domain.
  - In such a case port is set to Null while applying same origin checks.

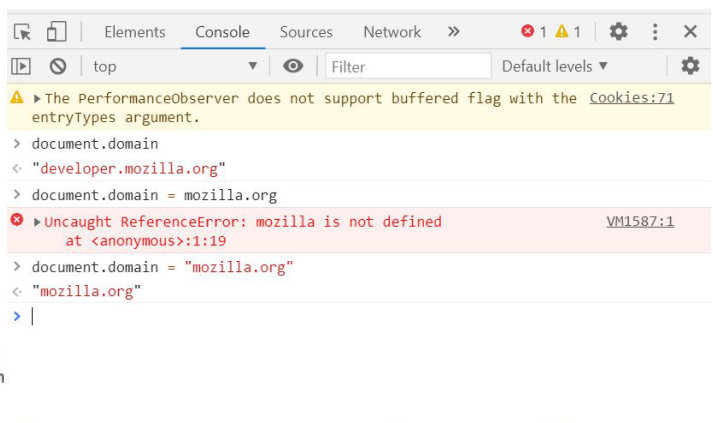
Dr. Gaurav Varshney, IIT Jammu

Cross-subdomain solution

If origin A and B share the same super domain, it's easy to let two documents access each other with the change of the `document.domain` property. `document.domain` is a read-only property in the HTML specification; most modern browsers allow it to be set to super domain (not top level). For example, a document with the URL www.myapp.com/index.html could set its own domain as `myapp.com`, while another document from sample.myapp.com/index2.html could also set its own domain as `myapp.com`. Figure 1 shows how `document.domain` works.

Figure 1. document.domain





With this cross-subdomain solution, origins from different subdomains could communicate under the same super domain, which is not an SOP restriction. But, strictly speaking, cross-subdomain solutions are most suitable for intranet applications.