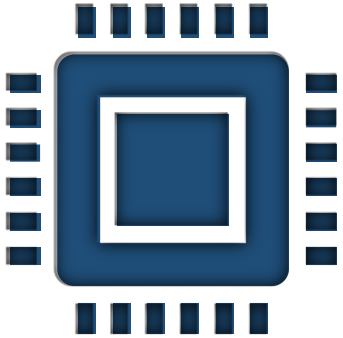
Introduction to Information Security

Network and Security (INFO8965)



Pawan Soobhri
Professor,
Applied CS and IT,
Conestoga College
Email: psoobhri@conestogac.on.ca

Lecture layout

- What is Information security and why?
- Threat actors
- Types of vulnerabilities and attacks
- Impact of attacks

References and acknowledgement

References

[CIAM] “CompTIA® Security+ Guide to Network Security Fundamentals” by Mark Ciampa, 7th edition, Publisher: Cengage Learning

Acknowledgement

Some of the material presented is based on:

- The recommended textbook [CIAM] by Cengage Learning.
- Other references are cited individually.

Is network and computer security important?

Why is it important for all computer users, not just IT professionals, to understand the **importance** of network and computer security?

"Contribute to Disaster Relief here"

"Donations for World Health Community"

Download AI Corona Antivirus

"Vaccine Registration: Click for available appointments"

"You are instructed to immediately read this list of cases to avoid potential hazards"

"Verify your account details to avoid suspension"

"Win a free N95 mask here"

"Apply for Canada Emergency Response Benefit (CERB) here"

https://www.sonicwall.com/phishing-iq-test/

https://www.av-test.org/en/statistics/malware/

Difficulties in defending against cyber security attacks

- Universally connected devices
- Increased internet speed
- Greater sophisticated attacks
- Availability of attack tools
- Delays in patching
- Weak patch distribution
- Distributed attacks
- Lacks of awareness

What is Information Security?

- Information security describes the tasks of securing digital information, whether it is:
  - Stored on storage hardware
  - Manipulated by microprocessor
  - Transmitted over a network
- There are three types of information protection (often called the CIA Triad):
  - Confidentiality: Only approved individuals may access information
  - Integrity: Ensures information is correct and unaltered
  - Availability: Ensures information is accessible to authorized users

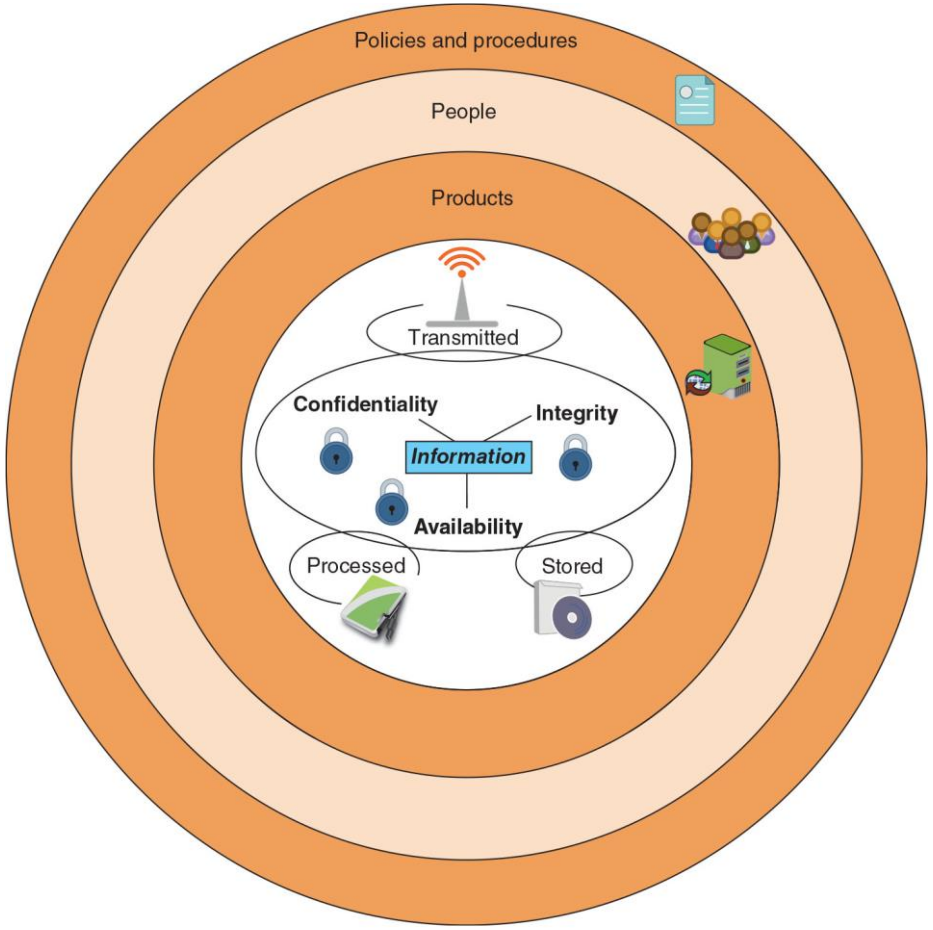


Figure 1-2 Information security layers

"CompTIA® Security+ Guide to Network Security Fundamentals" by Mark Ciampa, 7th edition, Publisher: Cengage Learning, © 2022 Cengage

What is Information Security?

- Information security cannot prevent successful attacks or guarantee that a system is totally secure.

- Goal of information security:
  - Implement protective measure, prevent collapse, and recover
  - Protect information of value
  - Protect devices that store, manipulate and transmit information

- Security and convenience are inversely proportional to each other.

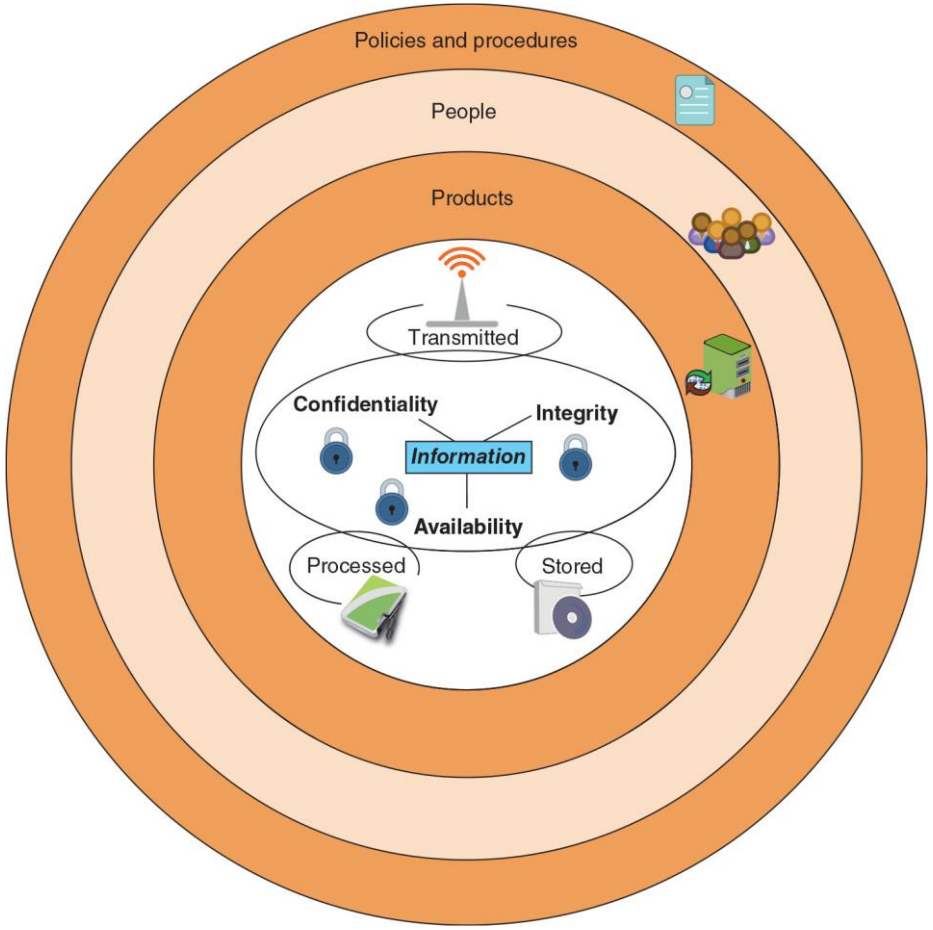


Figure 1-2 Information security layers

"CompTIA® Security+ Guide to Network Security Fundamentals" by Mark Ciampa, 7th edition, Publisher: Cengage Learning, © 2022 Cengage

Threat, Risk and Vulnerability

- **Threat** is anything that can exploit a vulnerability – intentionally or accidentally – and obtain, damage or destroy an asset.

- **Vulnerability** is a system flaw that can be exploited by threats to gain unauthorized access to an asset.

- **Risk** is the potential for loss or damage of assets, when a threat exploits a vulnerability.

RISK = THREAT X VULNERABILITY

Who are threat actors?

- A threat (or malicious) actor is an individual or entity responsible for cyber incidents against the technology equipment of enterprises and users

Categories of threat actors

- **Script kiddies**: are relatively unskilled attackers who use automated programs (or scripts) written by other threat actors.
- **Hacktivists**: are individuals that are strongly motivated by ideology (for the sake of their principles or beliefs)
  - Motivated socially or politically
  - Many work through disinformation campaigns by spreading fake news and supporting conspiracy theories.

Figure: Menu of Sniffing and Spoofing tools in Kali Linux

Categories of threat actors

- Governments are increasingly employing their own state-sponsored attackers for launching cyberattacks against their foes
  - These attackers are known as **state actors** and are considered the deadliest.
- State actors are often involved in multiyear intrusion campaigns targeting highly sensitive economic, proprietary, or national security information
  - A new class of attacks called advanced persistent threat (**APT**)
  - APTs are most commonly associated with state actors
  - Stages: Gain access, Establish a foothold, Deepen access, Move Laterally, Look-Learn-Remain

APT Groups: https://www.fireeye.com/current-threats/apt-groups.html

Categories of threat actors

- **Insider** threat actors are individuals working within an organization (employees, contractors, business partners etc.) that pose threat of manipulating data due to their trusted position.
  - Harder to recognize
  - Intellectual property theft, sabotage, espionage

- **Brokers** are financially motived threat actors that profit through sale of their knowledge of a weakness to other attackers or governments
  - Uncover weakness but do not report it. Instead sell it to the highest bidder who is willing to pay a high price for the unknown vulnerability.

Vulnerabilities

- According to National Institute of Standards and Technology (NIST), **vulnerability** is *"A weakness in the computational logic (e.g., code) found in software and hardware components that, when exploited, results in a negative impact to confidentiality, integrity, or availability.*
- National Vulnerability Database (NVD) is a comprehensive database of reported known vulnerabilities which are assigned Common Vulnerabilities and Exposures (CVEs).
  - https://nvd.nist.gov/
  - Cybersecurity vulnerabilities can be categorized into platforms, configurations, third parties, patches, and zero-day vulnerabilities

Vulnerabilities

- Several vulnerabilities are the result of the **platform** (hardware and OS that runs applications, programs or processes) being used.
  - Legacy platforms - outdated computing software and/or hardware that is still in use.
  - On-premises platforms – software and technology located within the physical confines of an enterprise.
  - Cloud platform – pay per use computing model. Computing resources can be scaled to cater requirements.

- **Configuration** settings are often not properly implemented
  - Results in weak configurations like default settings, open ports and services, unsecured root accounts, open permissions, unsecured protocols, weak encryption, errors due to human factor etc.

Vulnerabilities

- Almost all businesses use external entities known as **third parties**.
  - Organizations outsource code development.
  - Many rely on third party data storage facilities.
  - Helps to reduce CAPEX and OPEX.
  - System integration (connectivity between third party and the organization) can create vulnerabilities.
  - One of the major risks of third-party system integration involves the principle of the weakest link (Chain is as strong as its weakest link).

Vulnerabilities

- **Patches**: an officially released software security update intended to repair a vulnerability.
  - As important as patches are, they can create vulnerabilities:
    - Difficulty patching firmware
    - Few patches for application software
    - Delays in patching OSs
- **Zero Day**
  - Vulnerabilities can be exploited by attackers before anyone else even knows it exists. Called a zero day because it provides zero days of warning
  - Zero-day vulnerabilities are considered extremely serious

Zero Day Attacks Explained:
https://www.crowdstrike.com/cybersecurity-101/zero-day-exploit/

Attack vector

- In cyber security, **attack vector** is a method or pathway used by an adversary to access or breach the target system/network.
  - Compromised credentials, malicious insiders, missing encryption, misconfiguration and phishing are common attack vectors.
  - Significant percentage of all malware are delivered through malicious emails.
  - Physical nature of wireless transmission – anyone can intercept.
  - Physical (direct) access to computing and networking devices.
  - Supply chain attacks – threat actors tamper with the manufacturing process of a product.
  - Removable media like USB is also a common attack vector.

Impacts of attacks

- A successful attack always results in several negative impacts
- These impacts can be classified as:

Impact	Description
Data loss	Destroying data that cannot be recovered
Data exfiltration	Stealing data to distribute it to other parties
Data breach	Accessing, stealing, and using data without authorization
Identity theft	Taking personally identifiable information to impersonate someone

- Effects on the organization
  - Availability loss – system/data becomes inaccessible
  - Financial loss
  - Reputation – affects the public perception of the enterprise

World’s biggest data breaches & hacks

https://www.informationisbeautiful.net/visualizations/worlds-biggest-data-breaches-hacks/

https://en.wikipedia.org/wiki/List_of_data_breaches

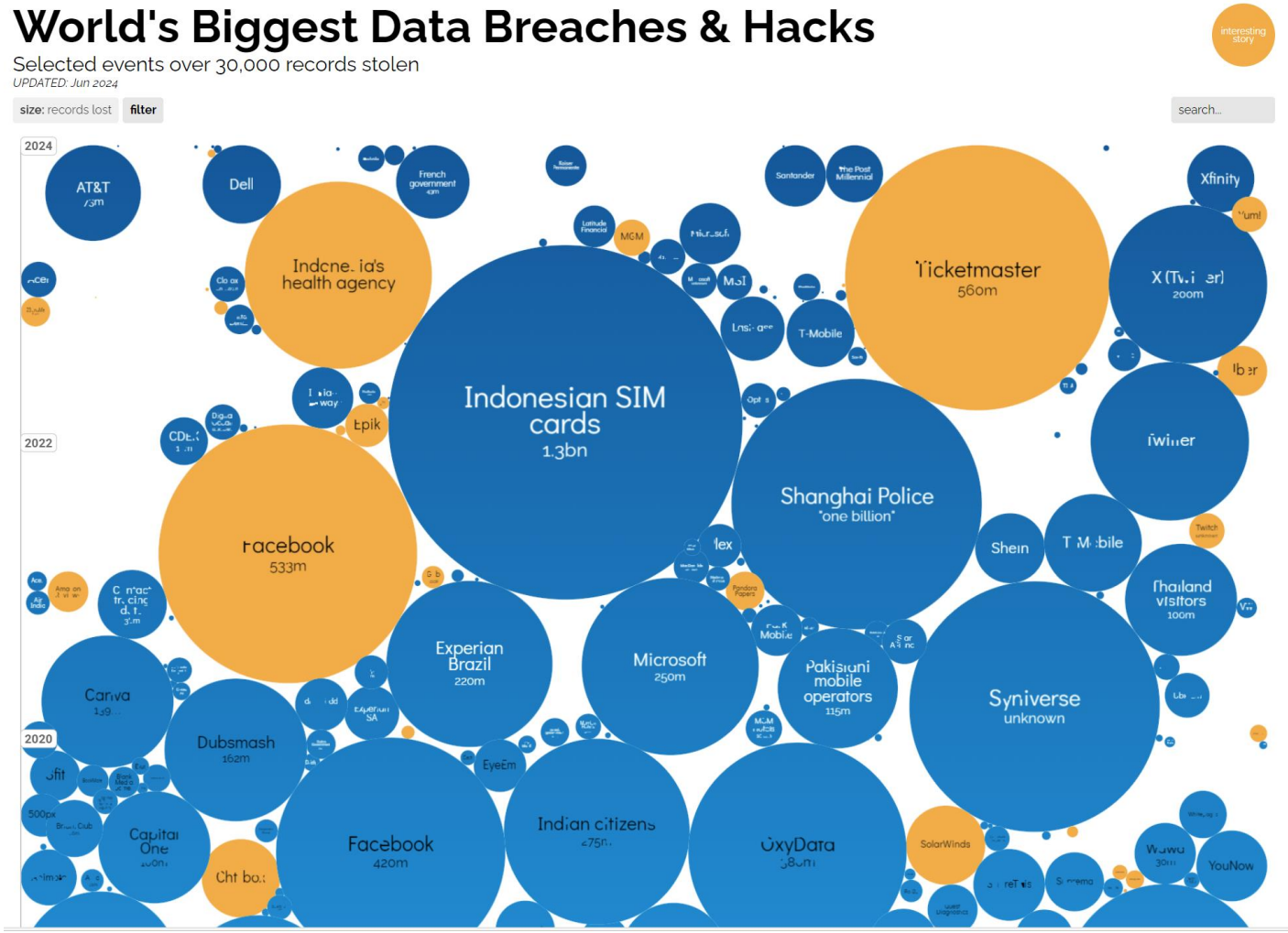


Figure: World’s biggest data breaches and Hacks website

Questions?