UMP
اونيۏرسيتي مليسيا ڤهڠ
UNIVERSITI MALAYSIA PAHANG
FAKULTI KOMPUTERAN

Data & Network Security

Chapter 1 - Foundational Concepts in Security

Outline

1.1 Introduction

1.2 CIA (Confidentiality, Integrity, Availability)

1.3 Concepts of Risk, Threat, Vulnerability, and Attack.

1.4 Authentication, Authorization, and Access Control

1.5 Responsible Disclosure

Learning Outcome

At the end of this chapter the students able to

- Define security concepts CIA.
- Explain the authentication, authorization and access control concepts.
- Define the concepts of trust and trustworthiness and analyse their influences on data and network security.
- Understand the concept of ethics.

Introduction

- Information Security - “The protection afforded to an automated information system in order to attain the applicable objectives of preserving the integrity, availability and confidentiality of information system resources” (William 2015)
- Network security - " refers to any activity designed to protect the usability and integrity of your network and data. It includes both hardware and software technologies. Effective network security manages access to the network. It targets a variety of threats and stops them from entering or spreading on your network.” (CISCO)

The History of Information Security

- Computer security began immediately after the first mainframe was develop.
  - Group developing code-breaking computation during World war II created the first modern computers.
  - Multiple level of security was implemented
- Physical controls to limit access to sensitive military location to authorized personal.
- Rudimentary/fundamentally in defending against, physical theft, espionage and sabotage

The Enigma : The courtesy from National Security Agent

Earlier versions of the German code machine Enigma were first broken by the Poles in the 1930s. The British and Americans managed to break later, more complex versions during World War II. The increasingly complex versions of the Enigma, especially the submarine or *Unterseeboot* version of the Enigma, caused considerable anguish to Allied forces before finally being cracked. The information gained from decrypted transmissions was used to anticipate the actions of German armed forces. "Some ask why, if we were reading the Enigma, we did not win the war earlier. One might ask, instead, when, if ever, we would have won the war if we hadn't read it."[1]

Figure 1-1 The Enigma

Source: Courtesy of National Security Agency

What Is Security?

"The Committee on National Security Systems (CNSS) defines information security as the protection of information and its critical elements, including the systems and hardware that use, store, and transmit that information."

- The quality or state of being secure.
- Free from danger.
- Protection against adversaries.
- Needs multiple layers of protection in place:
  - √ Physical security
  - √ Personnel security
  - √ Operations security
  - √ Communications security
  - √ Network security
  - √ Information security

Components of Information Security

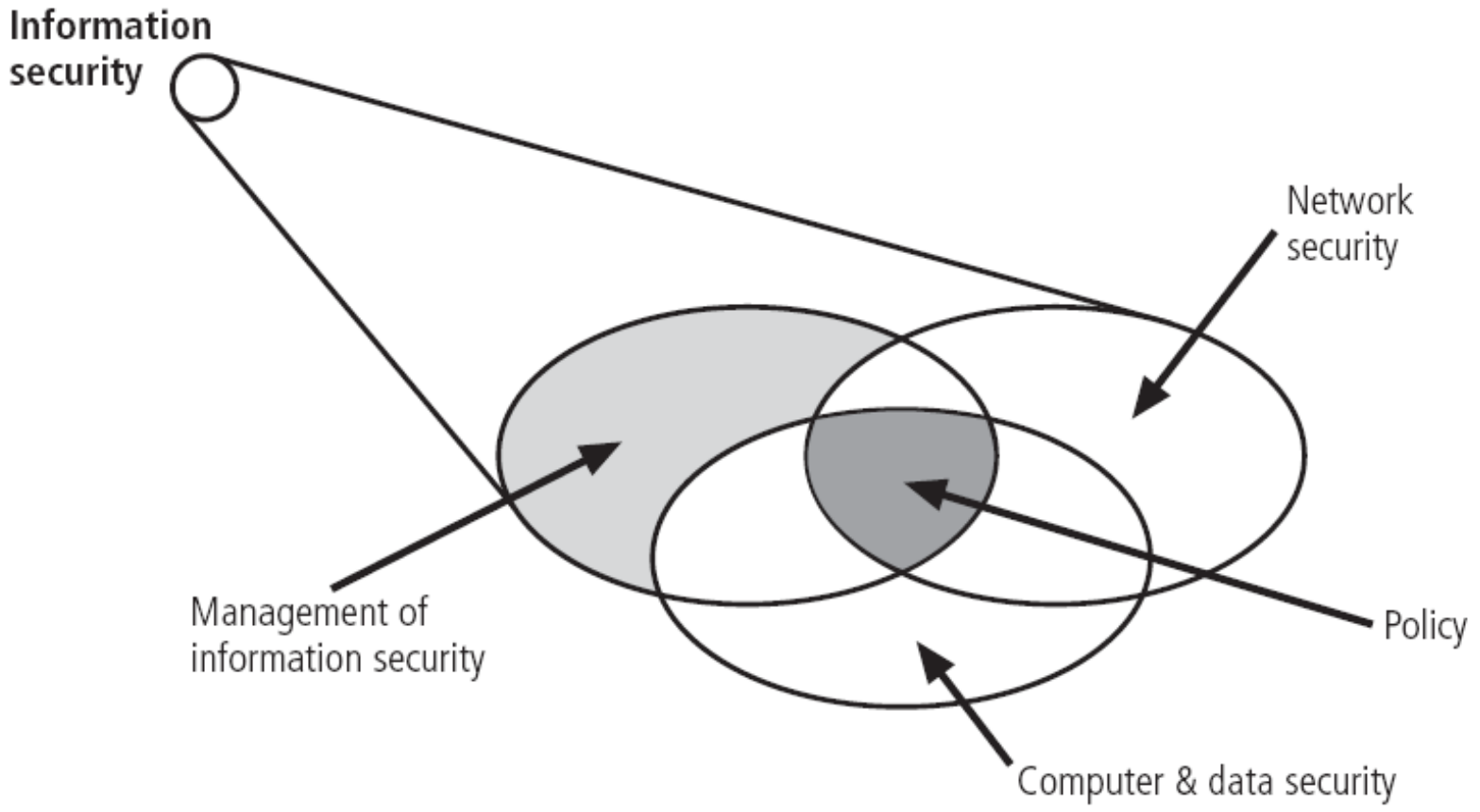

FIGURE 1-1 Components of Information Security

Key Information Security Concepts

Concepts•	Access•	Asset•	Attack
Control,Safeguard	Exploit	Exposure	Loss
Protection Profile	Risk	Subjects and Objects	Threat
	Threat Agent	Vulnerability	

CIA Triad

- Confidentiality
  - √ Confidentiality is the protection of information from unauthorized access
  - √ Data confidentiality and privacy.
  - √ Preserving authorized restrictions on information access and disclosure, in protecting personal privacy and proprietary information.
  - √ A loss of confidentiality is the unauthorized disclosure of information.

Confidentiality, Integrity, Availability (CIA)

- Integrity
  - √ Integrity is the condition where information is kept accurate and consistent unless authorized changes are made.
  - √ Data and system integrity.
  - √ Guarding against improper information modification or destruction and includes ensuring information non-repudiation and authenticity.
  - √ A loss of integrity is the unauthorized modification or destruction of information.
- Availability
  - √ Availability is the situation where information is available when and where it is rightly needed.
  - √ Ensuring timely and reliable access to and use of information.
  - √ A loss of availability is the disruption of access to or use of information or an information system.

NSTISSC Security Model

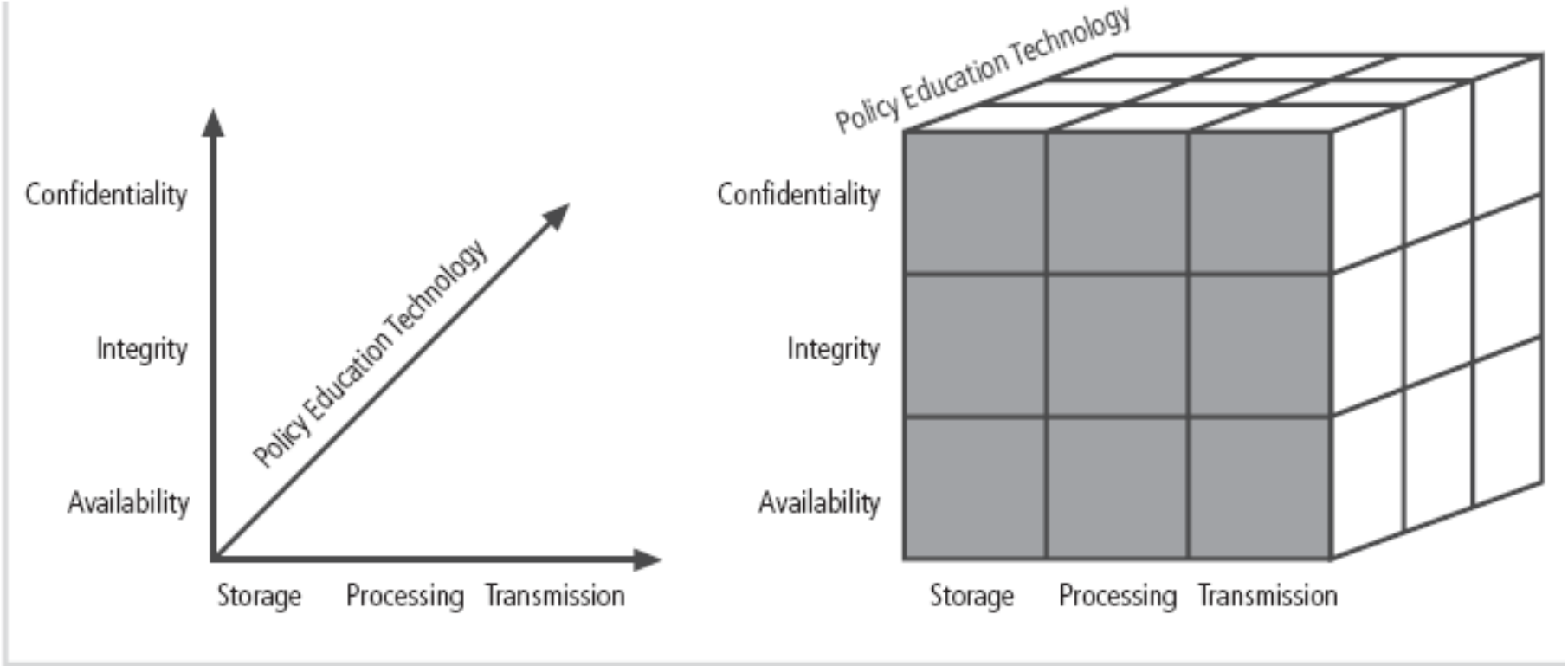

FIGURE 1-2 NSTISSC Security Model

Concepts of Risk, Threat, Vulnerability and Attack

Risk – someone or something that is a risk to safety Any package left unattended will be deemed a security risk.

Threat – The people eager, willing, and qualified to take advantage of each security weakness, and they continually search for new exploits and weaknesses.

Vulnerability – A weakness that is inherent in every network and device. This includes routers, switches, desktops, servers, and even security devices themselves.

Attack – The threats use a variety of tools, scripts, and programs to launch attacks against networks and network devices. Typically, the network devices under attack are the endpoints, such as servers and desktops.

Risk

- Risk is defined as the **potential** for loss or damage when a threat exploits a vulnerability. Examples of risk include financial losses, loss of privacy, reputational damage, legal implications, and even loss of life.
- Risk can also be defined as follows:

  Risk = *Threat* X *Vulnerability*

Threat

- A threat refers to a new or newly discovered **incident that has the potential to harm a system** or your company overall. There are three main types of threats:
- **Natural threats**, such as floods, hurricanes, or tornadoes
- **Unintentional threats**, like an employee mistakenly accessing the wrong information
- **Intentional threats**, such as spyware, malware, adware companies, or the actions of a disgruntled employee
- **Worms and viruses** are categorized as threats because they could cause harm to your organization

Vulnerability

- A vulnerability refers to a **known** weakness of an asset (resource) that can be exploited by one or more attackers. In other words, it is a known issue that allows an attack to succeed.
- For example, when a team member resigns and you forget to disable their access to external accounts, change logins, or remove their names from company credit cards, this leaves your business open to both intentional and unintentional threats.

Attack

- The main difference between threat and attack is a threat can be either intentional or unintentional whereas an attack is intentional.
- Threat is a circumstance that has potential to cause loss or damage whereas attack is attempted to cause damage
- **Attack vector:** A method or way an attacker can gain unauthorized access to a network or computer system.

Concepts of Risk, Threat, Vulnerability and Attack

Attack Vectors - (Ligier, 2016)

- Network
- User
- Email
- Web Application
- Remote Access
- Mobile

Attacks (threats carried out)

- Passive – does not affect system resources
- Active – attempt to alter system resources or affect their operation
- Insider – initiated by an entity inside the security parameter
- Outsider – initiated from outside the perimeter

Authentication, Authorization, and Access control

A framework for controlling access to computer resources, enforcing policies, auditing usage, and providing the information necessary

Authentication

- A process to identify a user.
- Typically, by having the user enter a valid username and valid password before access is granted.

Authorization

- Levels of granting permission.
- Process determines whether the user has the authority to issue such commands.
- Authorization is the process of enforcing policies: determining what types or qualities of activities, resources, or services a user is permitted.

Access Control

- Access control is a security term used to refer to a set of policies for restricting access to information, tools, and physical locations.
- Measures the resources a user consumes during access.
- Authorization control, billing, trend analysis, resource utilization, and capacity planning activities.

Concept in a Story

- One of the popular security concepts is the CIA. The term CIA stands for Confidentiality, Integrity and Availability.
- Another security concept is AAA which stands for Authentication, Authorization and Accounting, some refer to the last A as Auditing.
- We could classify AAA as five different levels as listed below:

  1: Identification

  2: Authentication

  3: Authorization

  4: Accounting

  5: Auditing

Concept in a Story

- We will look at both terms for an example. Suppose there is a military base where there are obviously army people and military operations going on. One fine day the boss of our hero ordered him to take a file to the military base which is highly confidential. (This classification of information as secret or similar prioritized events dealing with information is what is dealt with in **confidentiality**).
- Until our hero reaches his destination, the data inside the document should not be altered or changed (This is what **Integrity** Deals with).
- Now our hero reached the military base, and a person came out of the room, now the document should be delivered to the person who came out (This is what **availabilit**y is about).

Concept in a Story

- Now we will see about AAA, so the person who came out asked our hero to show proof like an identification card or dependent ID and he showed the same.
- This is what **Identification** is, we verify the identity of a person or a machine. Now the person asks our hero to provide a secret passcode which is given by his boss to let him inside the base. This is what **authentication** is, we have a user and a unique identification key to ensure identity.
- Now our hero is inside the base, and he sees so many rooms and the person says that he can only go to these rooms because they are out of the privileges given to him. This is what **authorization** is.

Concept in a Story

- Now in this secret operation, our hero's actions are always being recorded, for further reference. This is what **Auditing** is. Auditing refers to the record-keeping and tracking of user activities. And now when carrying out all these activities our hero should also realize that he is responsible for the information he carries. This is what we term as **Accountability**.

Responsible Disclosure

Responsible disclosure is the process of inviting security researchers to find and report security issues in the systems.

Step to create responsible disclosure:

- Prepare your organization
- Create a public disclosure policy
- Publish your policy
- Be responsive and communicate clearly
- Be transparent
- Don’t Panic
- Acknowledge and credit
- Fix fast

Other Terms in Information Security

- Accuracy
- Authenticity
- Privacy
- Non-repudiation
- Trustworthiness
- 6 D’s of Cyber Security

Conclusion

- Security concept
- CIA triad
- Different of risk, threat, vulnerability and attack
- Concept of 3 A’s and responsible disclosure

References

Stallings, W. and L. Brown, *Computer Security: Principles and Practice*. 2015, Pearson Education.

CISCO. *What Is Network Security?* [cited 2017 22 August 2017]; Available from: https://www.cisco.com/c/en/us/products/security/what-is-network-security.html.

Techopedia. *Computer Ethics*. [cited 2017 22 August 2017]; Available from: https://www.techopedia.com/definition/5499/computer-ethics.

Larson, S.F.S. *The uncertain future of Internet privacy*. 2017 [cited 2017 22 August 2017]; Available from: http://money.cnn.com/2017/04/05/technology/internet-privacy-future/index.html.

Ligier, S. *Threat vectors – what are they and why do you need to know them?* 2016 17 Nov 2016 [cited 2017 4 Sep 2017]; Available from: https://blog.barracuda.com/2016/11/17/threat-vectors-what-are-they-and-why-do-you-need-to-know-them/.