COSC130

Fundamentals of Cybersecurity and Privacy

LECTURE 1: SECURITY ATTACKS, MECHANISMS AND SERVICES

Lecture Overview

1. Food for thought
2. Cybersecurity landscape in Australia
3. What can go wrong?
4. What is cybersecurity?
5. Security Services
6. Security Mechanisms
7. Security Attacks
8. Vulnerabilities
9. Case Studies

Food for Thought

The art of war teaches us to rely not on the likelihood of the enemy's not coming, but on our own readiness to receive him; not on the chance of his not attacking, but rather on the fact that we have made our position unassailable."

— "*The Art of War*", Sun Tzu, 544 – 496 BC

"It is easy to run a secure computer system. You merely have to disconnect all dial-up connections and permit only direct-wired terminals, put the machine and its terminals in a shielded room, and put a guard at the door."

— "UNIX Operating System Security ", F. T. Grampp and R. H. Morris, 1984

"Amateurs hack systems, professionals hack people."

" If something is free, you're not the customer; you're the product."

"If you think technology can solve your security problems, then you don't understand the problems and you don't understand the technology."

— Bruce Schneier

"Ultimately, saying that you don't care about privacy because you have nothing to hide is no different from saying you don't care about freedom of speech because you have nothing to say."

— "Permanent Record", Edward Snowden, 2019

Cybersecurity Landscape in Australia

In 2020, Australians spent 5.6 billion dollars on cybersecurity products and services.

In 2021-2022 financial year, 76,000 cybercrimes were reported in Australia (13% increase from the previous year) – on average, a cybercrime is reported every 7 minutes. In 2022-2023, we had 94,000 cybercrime reports, or one report every 5.6 minutes.

The Australian Government has

- legislated cyber security obligations for over 2,000 'critical infrastructure' businesses that will be required to develop a cybersecurity risk management program, and
- increased penalties for businesses that do not sufficiently protect customer data.

Cybersecurity Landscape in Australia

60% of the Australian companies surveyed in 2022 said they would increase their cybersecurity budget in 2023.

That implies a growing need for cybersecurity professionals in Australia (and worldwide).

"The average cyber security salary in Australia is $120,056 per year or $61.57 per hour. Entry-level positions start at $100,000 per year, while most experienced workers make up to $159,206 per year." (au.talent.com)

What can go wrong?

- Ransome attack
- Identity theft
- Digitally disappearing
- Deepfake
- ancestry.com shares your DNA data with researchers

What is Cybersecurity?

- Security requirements have changed drastically in recent times.
  - Traditionally, security was provided by physical and administrative methods.
  - The widespread use of Information and Communication Technologies (ICT) introduced new security challenges.
    - Computer use requires automated software tools to protect data and other resources (assets).
    - Use of networks and communications links requires measures to protect data during transmission.

In most general terms, we define ***cybersecurity*** as keeping cyberspace safe from harm.

We distinguish between 'safety' and 'security'.

Safety is concerned with natural disasters including earthquakes, floods and fires, and unintentional human errors (also referred to as 'benign threats').

Security is concerned with malicious actions designed to cause harm ('intentional harm').

Definitions

Cybersecurity is notorious for its inconsistent terminology. Therefore, it is very important that we understand all the important concepts and not get confused by inconsistent terminology. We will start by giving some informal definitions.

- **Computer security** - generic name for the collection of tools designed to protect data and other resources (also referred to as 'assets'), and to thwart hackers.
- **Network (Internet) security** - measures to deter, prevent, detect and correct violations that involve transmission of data.
- **Data security** refers to the protection of data from unauthorised disclosure, destruction and alternation. In recent decades, ***data*** is recognised as one of the most valuable resources of governments, companies and organisation, and, to some extent, even individuals.

When defining cybersecurity concepts, most authors and documents rely on industry standards and recommendations. We next list some of the most important standards.

Recommendations and Standards

ITU-T (International Telecommunication Union, Telecommunication Standardization Sector)

- The X.800 *Security Architecture for Open Systems Interconnection (OSI)* http://www.itu.int/rec/T-REC-X.800-199103-I/e

The Requests for Comments (RFC) document series is a set of technical and organizational notes about the Internet; published by the Internet Engineering Task Force which develops Internet standards

- RFC4949 *Internet Security Glossary* - obsoletes RFC2828 https://www.rfc-editor.org/info/rfc4949

National Institute of Standards and Technology (NIST)

- FIPS 199 – *Standards for Security Categorization of Federal Information and Information Systems.* http://nvlpubs.nist.gov/nistpubs/FIPS/NIST.FIPS.199.pdf

- NIST SP 800-12 *An Introduction to Information Security* – obsoletes NIST95 https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-12r1.pdf

Exercise 1.1.

Do X.800, RFC 4949, FIPS 199, and NIST SP 800-12 define each of the following concepts:

- cyberspace
- cybersecurity
- computer security
- information security
- data security
- network security

If yes, are the definitions consistent?

If not, is there a similar concept defined in the document in question?

Security Services, Mechanisms, Attacks and Vulnerabilities

We need a systematic way to identify security requirements and how they can be satisfied.

We consider the following four aspects of cybersecurity:

- **Security services (goals, objectives)** – what we want to achieve
- **Security mechanisms** – how we can achieve that
- **Security attacks** – ways in which adversaries can harm the system
- **Security vulnerabilities** – weaknesses in the system that facilitate attacks

Cybersecurity is about **preventing** security attacks, or failing that, **detecting** and **mitigating** attacks, and **recovering** from them**.**

X.800 Security Architecture for OSI

The X.800 Security Architecture for OSI (Open Systems Interconnection Reference Model) focuses on security attacks, mechanisms, and services. These can be defined briefly as follows.

- **Security attack:** Any action that compromises the security of information owned by an organization.
- **Security mechanism:** A process (or a device incorporating such a process) that is designed to detect, prevent, or recover from a security attack.
- **Security service:** A processing or communication service that enhances the security of the data processing systems and the information transfers of an organization. The services are intended to counter security attacks, and they make use of one or more security mechanisms to provide the service.

Exercise 1.2.

Do RFC 4949, FIPS 199, and NIST SP 800-12 define security services, mechanisms, and attacks?

If yes, are the definitions consistent with X.800?

Security Services

Security services imitate services normally available in the context of physical documents, for example, protection from disclosure, tampering, or destruction, notarized or witnessed, and so on. They are meant to counter security attacks and are realised by one or more security mechanisms.

CIA Triad:

- Confidentiality - data should be accessible only by authorised users
- Integrity - data can be modified only by authorised users
- Availability - computer assets are available to authorised users when needed

We also need:

- Authenticity - the origin of an electronic document/user can be correctly identified
- Non-repudiation - neither the sender nor the receiver of the message can deny the transition
- Anonymity – individuals whose personal data is used for research etc., can remain anonymous (if they choose to do so); in other words, personal data cannot be linked back to the individuals, unless they agree with that

Security Services

Security services are inconsistently defined in the literature. For example:

- A. Menezes , P. van Oorschot, and S. Vanstone in "Handbook of Applied Cryptography", CRC Press, 1996, list confidentiality, integrity, authentication, and non-repudiation

- M. Bishop in "Computer Security: Art and Science", Addison Wesley, 2003, list confidentiality, integrity, and availability (CIA).

Security Services

Stallings in "Cryptography and Network Security" defines CIA Triad as follows:

Confidentiality: This term covers two related concepts:

- Data confidentiality: Assures that private or confidential information is not made available or disclosed to unauthorized individuals.
- Privacy: Assures that individuals control or influence what information related to them may be collected and stored and by whom and to whom that information may be disclosed.

Integrity: This term covers two related concepts:

- Data integrity: Assures that information (both stored and in transmitted packets) and programs are changed only in a specified and authorized manner.
- System integrity: Assures that a system performs its intended function in an unimpaired manner, free from deliberate or inadvertent unauthorized manipulation of the system.

Availability: Assures that systems work promptly and service is not denied to authorized users.

Security Services

He defines two additional security services:

Authenticity: The property of bring genuine and being able to be verified and trusted; confidence in the validity of a transmission, a message, or message originator. This means that users are who they say they are and that each input arriving at the system came from a trusted source.

Accountability: The security goal that generates the requirement for actions to be traced uniquely to that entity. This supports, nonrepudiation, deterrence, fault isolation, intrusion detection and prevention and after action recovery and legal action. Systems must keep records of their activities to permit later forensic analysis to trace security breaches or to aid in transaction disputes.

Exercise 1.3.

What security services are specified in X.800, RFC 4949, FIPS 199, and NIST SP 800-12 ?

Security Mechanisms

There is no single security mechanism that can support all the required security services.

However, one particular suite of techniques underlies many of the security mechanisms in use: **cryptographic techniques.**

Other security mechanisms include:

- access control,
- backups,
- traffic padding

and so on.

Security Mechanisms

We can divide security mechanisms/approach into proactive and reactive (Pfleeger et al, 2015).

Proactive approaches:

- Preventive controls, e.g., firewall
- Deterrence, e.g., two-factor authentication
- Deflection, e.g., deploying honeypots

Reactive approaches:

- Detection, e.g., logs
- Mitigation, e.g., network segmentation
- Recovery, e.g., backups

Exercise 1.4.

What security mechanisms are specified in X.800, RFC 4949, FIPS 199, and NIST SP 800-12?

Security Design Principles

According to Smith, 2012, the following generic security design principles are helpful for designing secure systems:

- Continuous improvement.
- Least privilege.
- Defence in depth.
- Open design.
- Chain of control.
- Transitive trust.
- Deny by default.
- Trust but verify.
- Separation of duty.
- The principle of least astonishment.

Threats and Attacks

Threat

- A potential for violation of security, which exists when there is a circumstance, capability, action or event that could breach security and cause harm. That is, a threat is a possible danger that might exploit a vulnerability.

Attack

- An assault on system security that derives form an intelligent threat; that is, an intelligent act that is a deliberate attempt to evade security services and violate the security policy of a system.

RFC4949, Internet Security Glossary

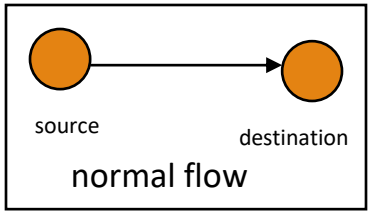
Security Attacks

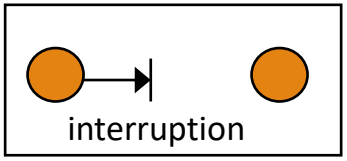
Security attack is any action that compromises the assets owned by an organization or an individual.

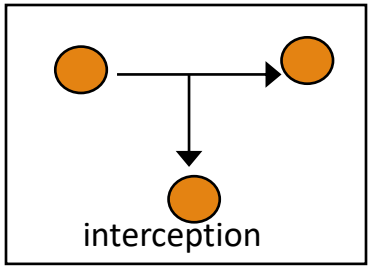
We distinguish between:

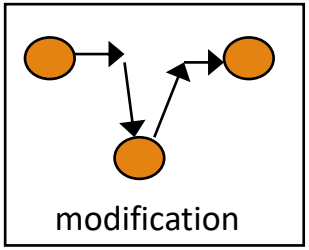
- **Passive attacks** - eavesdropping on, or monitoring of, transmissions to obtain message contents, or monitor traffic flows
- **Active attacks** – modification of data stream to:
  - masquerade of one entity as some other
  - replay previous messages
  - modify messages in transit
  - denial of service

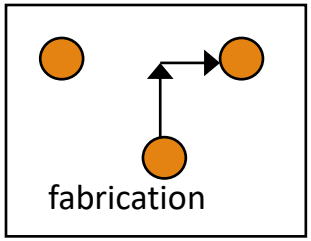
Security Attacks

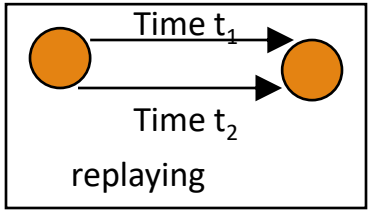












Exercise 1.5.

What security attacks are specified in X.800, RFC 4949, FIPS 199, and NIST SP 800-12?

Who are the Attackers?

According to Pfleeger et al., 2015, for an attack to succeed, an attacker needs a working method, an opportunity to attack, and a motive.

We next look at common types of attackers and their motives.

Amateur attackers:

1. Scrip Kiddies – usually have limited or no programming skills, use readily available tools to identify and exploit weaknesses; may not understand the effect of their actions; usually motivated by the feeling of 'thrill' and desire for reputation among their peers
2. Hacktivists – motivated by ideology and a desire to create publicity and further their cause
3. Rouge Hackers – motivated by curiosity
4. Hacking for personal gain – motivated by financial gain

Who are the Attackers?

Professional attackers:

1. White Hats – want to expose weaknesses and improve the security of the system
2. Corporate Spies – want to obtain commercial secrets
3. Cyber Criminals – motivated by financial gain
4. Nation States – want to influence other states and/or extend their power; well-resourced and capable of creating Advanced Persistent Threat (APT)

Who are the Attackers?

Another way of looking at attackers:

- unauthorised users
- authorised users having unauthorised access
- authorised users using authorised access to obtain access to data they should not access

Vulnerabilities

There are two pre-conditions for a successful attack:

1) exposure – if an attacker cannot reach a system, they cannot launch an attack

2) exploitability – if a system contains no vulnerability, it cannot be successfully attacked

A ***vulnerability*** is a flaw or weakness in a system that can be exploited to cause harm. The weakness can be in the system design, implementation, or operation and management.

Risk Management

'Exposure' and 'exploitability' together determine the 'likelihood' of the attack.

Another important parameter is the 'impact' of the attack.

'Likelihood' and 'impact' together determine the severity of the 'risk'.

Risk Matrix

		Likelihood		
		Low	Med	High
Impact	Low			
	Med			
	High			

Risk Management

Risks can be

1. avoided
2. mitigated by reducing the likelihood and/or impact
3. transferred by, for example, purchasing an insurance, or externalising the costs (passing it onto users of the system)
4. accepted by, for example, covering the cost of the risk

Stages of an Attack

A framework proposed by Lockheed Martin specifies attackers' actions when breaking into a secured network:

- ❑ Reconnaissance
- ❑ Weaponisation
- ❑ Delivery
- ❑ Exploitation
- ❑ Installation
- ❑ Command and Control
- ❑ Actions

Case Studies

(Markus et al., 2020)

- HTTP
- Buffer Overflow
- SQL Injection
- Reconnaissance
- Firewalls
- DDoS
- NIDS

References

C. P. Pfleeger, S. L. Pfleeger, and J. Margulies. *Security in Computing*, 5th Edition, Pearson Education, 2015.

C. Markus, B. Gordijn, and M. Loi (Eds.). *Ethics of cybersecurity*, The The International Library of Ethics, Law and Technology, Vol. 21, Springer, 2020.

W. Stallings. *Cryptography and Network Security: Principles and Practice*, Global Ed, Pearson, 2022.

R. Smith. A contemporary look at Saltzer and Schroeder's 1975 design principles. *IEEE Secur Priv* 10(6):20–25, 2012.