Network Security

Pengwenlong GU
Associate Professor

Centre d'études et de recherche en informatique et communications (CEDRIC)
CNAM Paris

Mail: gup@cnam.fr
Office: 33.1.9B

16/10/2024

Overview

1. Introduction
2. Security and Network Security
3. Security Mindset

Prerequisites

- Basic knowledge of computer networks: TCP/IP, Wireless networks and operation systems (Will help gain deeper understanding of security mechanisms and where they fit in the big picture)
- We can have a brief recall on computer networks especially the TCP/IP if needed
- Basic knowledge of programming languages (Needed in practical works)

Course Objectives

- **Develop a "security" mindset:** Security isn't just about technology; it's about mindset, culture, and continuous improvement
- **Explore Network Security Technologies:** Learn about firewalls, intrusion detection/prevention systems (IDS/IPS), VPNs, and other security tools
- **Develop Practical Skills:** Implement security measures through hands-on labs involving real-world scenarios
- **Analyse Security Protocols:** Study and critique existing network security protocols and understand the design of secure network protocols
- **Threat and Vulnerability Assessment:** Identify, analyse, and mitigate network vulnerabilities and threats

What This Course is Not About

- We are **Not** going to be able to cover everything (It is impossible)
- You will **Not** be a security expert after this class
- It is **Not** a course on ethical, legal, or economic issues

Main Themes of the Course

- Vulnerabilities of computer networks
    - Insecure protocols, Insufficient access controls, Lack of encryption, Poorly designed network architecture, Malware, etc.
- Defensive techniques
    - Cryptography, Firewalls, Intrusion detection systems (IDS), Access control, Authentication, Certificates, etc.
- Several security protocols
    - Application- and transport-layer security protocols, Virtual Private Network (VPN), etc.

Course Logistics

- Teaching Assistant: Yasmine CHAOUCHE (email: yasmine.chaouche@lecnam.net)
- Lectures: 9 sessions
- Practical work (50% of the final grade): 6 sessions
- Group project (50% of the final grade): 2 sessions for presentation (20 minuites each group: 15 minuites presentation and 5 minuites for questions)

Group Project Report

- Length: 3 pages each person (E.g. A group of 3: 9 pages of content and one more page of references)
- **Must be done with Latex** (Overleaf is very easy to use)
- Format $\backslash documentclass[12pt, draftclsnofoot, onecolumn]\{IEEEtran\}$
- Content: Select a use case of your choice, perform an in-depth vulnerability analysis against a particular type of attack, and outline a detailed attack model. Then, research and identify multiple countermeasures by referencing published research papers. Evaluate these countermeasures to discuss how the attack could be effectively detected or prevented within the chosen scenario.
- Submission deadline: 12/12/2024

Course Materials

- Textbook:
  - "Network Security: Private Communication in a Public World 3rd Edition" by Charlie Kaufman
  - "Introduction to Modern Cryptography Second Edition" by Jonathan Katz and Yehuda Lindell
- Online research database:
  - IEEE Xplore: `https://ieeexplore.ieee.org/Xplore/home.jsp`
  - ACM Digital Library: `https://dl.acm.org/`
  - Google Scholar `https://scholar.google.com/`

Overview

1. Introduction

2. Security and Network Security

3. Security Mindset

Security in General

Security broadly refers to the measures taken to protect against various threats, ensuring safety and preservation from harm or damage. It encompasses:

- **Physical Security:** Protection of personnel, hardware, programs, networks, and data from physical actions and events that could cause serious loss or damage.
- **Personal Security:** Measures to ensure the safety of individuals from threats like violence, theft, or harassment.
- **Financial Security:** Safeguarding one's financial assets from fraud, theft, or economic instability.
- **National Security:** Protecting a nation from external and internal threats, which includes defense, intelligence, and homeland security.

Why do we need security?

- Protect vital information while still allowing access to those who need it
- Provide authentication and access control for resources
- Guarantee availability of resources

What is Network Security?

- Network security refers to any activities designed to protect your network, which protect the usability, reliability, integrity, and safety of your network and data.
- Effective network security targets a variety of threats and stops them from entering or spreading on your network.

Why "Security" is Special in Computer Networks

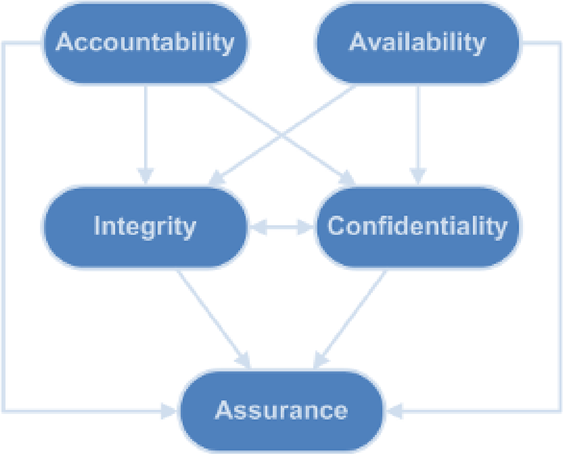
- The majority of engineering efforts are focused on designing systems to achieve desired behaviours.
- But security efforts are focused on preventing undesired behaviours.
- Is it possible to anticipate what is undesirable before it actually occurs?
- Adversaries are actively and maliciously trying to circumvent protective measures you put in place. (human intelligence against both human intelligence and human errors)

Information Security Triad: CIA

- Confidentiality: (Authentication, Encryption, etc.)
  - Protecting information from disclosure to unauthorized parties
  - Access to information should be granted only on a need-to-know basis
- Integrity: (Hashing, Digital Signatures, etc.)
  - Protecting information from being modified by unauthorized parties
  - Ensuring that the information is not tampered whenever it travels from source to destination or even stored at rest
- Availability: (Fault Tolerance, Anti-jamming, etc.)
  - Ensuring that authorised parties are able to access information when needed
  - Ensuring that the services of an organization are available

Model CIA^3

Renewed in 2016 (`https://www.cia-cubed.org`)



Model CIA^3

- Accountability:
  - Depends on controls and plausible deniability to make it "stick"
  - Accountability also may encompass segregation of duties
- Assurance:
  - Assurance is a continuous activity
  - Periodic controls assure that all security measures (both technical and operational) work as intended to protect the system and the information that it processes

Overview

1. Introduction
2. Security and Network Security
3. Security Mindset

Absolute security

An absolute security in computer networks would imply a state where a network is completely secure against all forms of unauthorised access, data breaches, and cyber threats under any circumstances.

Absolute security

It means:

- Zero Vulnerabilities
- Perfect Encryption
- Infallible Authentication
- Complete Isolation or Perfect Monitoring
- Predictive Threat Mitigation
- Human Error Elimination

Absolute security

Is Absolute Security Achievable?

In Theory:

- The concept of absolute security can be imagined, much like a mathematical ideal or a perfect vacuum in physics. It serves as a goal to strive towards.

Absolute security

In Practice: No, absolute security is not achievable in real-world scenarios for several reasons:

- Complexity: Modern computer networks are incredibly complex, with numerous interacting components, each potentially introducing vulnerabilities.
- Evolving Threats: Cyber threats evolve rapidly; what's secure today might not be secure tomorrow due to new attack vectors.
- Human Factor: People can be tricked or make mistakes, leading to security breaches (e.g., through social engineering).

Good security

- Good security is about risk management (Understanding what risks are acceptable, implementing flexible security measures)
- The goal is not always “to make the system as secure as possible”, but “to make the system as secure as possible within certain constraints”.
- Security can be considered as a trade-off in several dimensions like: Security vs. Usability, Security vs. Cost, Security vs. Performance, Security vs. Functionality.

Cost-benefit analysis [Jonathan Katz]

- Important to evaluate what level of security is necessary/appropriate
  - Cost of mounting a particular attack vs. value of attack to an adversary
  - Cost of damages from an attack vs. cost of defending against the attack
  - Likelihood of a particular attack
- Sometimes the best security is to make sure you are not the easiest target for an attacker. . .

Understanding Constraints

- Usability:
  - Key Point: Security measures should not impede the user's ability to perform their tasks effectively.
  - Example: Overly complex password policies might lead users to write down passwords or choose easily guessable patterns, thus reducing security.
- Performance:
  - Key Point: There must be a balance between security protocols and system performance to ensure operations remain efficient.
  - Example: Excessive encryption layers or real-time scanning can slow down systems to the point where they become impractical for use.

Understanding Constraints

- Cost:
  - Key Point: Security investments should align with risk assessments; not all assets require the same level of protection.
  - Example: Implementing the highest level of security for all aspects of an organization might be prohibitively expensive, especially for small to medium enterprises.
- Functionality:
  - Key Point: Security should enhance, not hinder, the primary functions of the systems or networks it protects.
  - Example: A network firewall configured with overly restrictive rules might block legitimate traffic, hindering business operations.

Definition of Risk

- **Risk:** Potential for loss, damage, or destruction of an asset as a result of a threat exploiting a vulnerability
- **Threat:** Any circumstance or event with the potential to adversely impact organisational operations, organizational assets or individuals through an information system via unauthorised access, destruction, disclosure, modification of information, and/or denial of service
- **Vulnerability:** A weakness in system security procedures, design, implementation, or internal controls that could be exploited by a threat

Risk Management Process

- **Risk Identification:** Asset Inventory, Threat Assessment, Vulnerability Analysis, etc.
- **Risk Assessment:**
  - Likelihood Determination: Estimate the probability that a given threat will exploit a vulnerability
  - Impact Analysis: Evaluate the potential impact if the risk materialises, often quantified in terms of financial loss, downtime, damage to reputation, etc.
- **Risk Response:** Mitigate, Avoid, Accept, etc.

Risk Appetite and Tolerance

- **Risk Appetite:** The amount and type of risk that an organization is willing to pursue or retain
- **Risk Tolerance:** The acceptable level of variance in performance relative to the achievement of objectives. Organisations might tolerate higher risks for greater potential returns

Examples

- A company might use biometric authentication for access to its server room but use simpler key card access for general office areas. Discuss why this makes sense.
- Software Development: In secure coding, not every function needs to be fortified against SQL injection if some functions don't interact with databases or user input.

Conclusion

- **Balanced Approach:** Optimal security involves finding a balance where the system or network is secure enough to protect against likely threats without unnecessary overhead or restrictions.
- **Continuous Evaluation:** Security needs are not static; they should be regularly reviewed and adjusted as threats evolve, technology advances, and business needs change.

Network security is not just about security [Jonathan Katz]

- Detection, response, audit:
  - How do you know when you are being attacked?
  - How quickly can you stop the attack?
  - Can you identify the attacker(s)?
  - Can you prevent the attack from recurring?
- Recovery (Can be much more important than prevention)
- Economics, insurance, risk management...
- Security is a process, not a product...

Thanks