Cryptography

Introduction

M S Vilkhu

21 / 23/ 24 Aug 2024 (C1/C3/C5)

High Level Course Topic

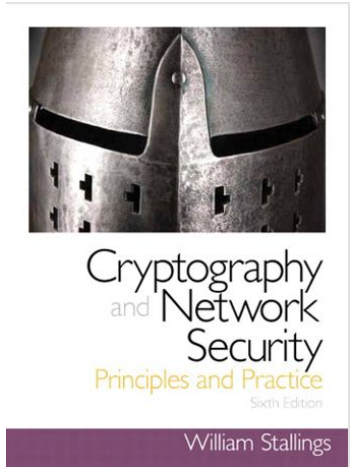
- Computer and network security
- Cryptography fundamentals
- Type of cryptographic algorithms
  - Symmetric key cryptography
  - Asymmetric key cryptography
  - Data integrity algorithms
  - Authentication protocols
- Digital Signature – concepts
- Integrity
- Trust

Agenda

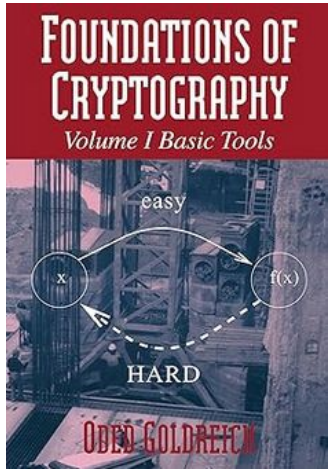
Fundamentals

- Overview
- Course contents
- Books

Textbooks



William Stallings, Cryptography And Network Security, Principles And Practice Sixth Edition, Pearson



Oded Goldreich, Fundations Of Cryptography, VOI•I Edition-I , ISBN-13: 978-0521119917

Intro

- students' level of understanding

Examples of security breach

1. Equifax Data Breach (2017)

- **Description**: One of the **largest data breaches** in history, Equifax, a **major credit reporting agency**, suffered a breach due to a vulnerability in a web application framework. Attackers exploited this vulnerability to gain **access to sensitive personal information** of approximately 147 million people.
- **Impact**: The breach **exposed personal data** including Social Security numbers, birth dates, and addresses, leading to identity theft risks and financial losses for affected individuals. Equifax faced significant legal and financial repercussions as a result.

2. Target Data Breach (2013)

- **Description**: Cybercriminals gained **access to Target's network through a third-party vendor's compromised credentials.** They **installed malware** on Target's point-of-sale systems, capturing credit and debit card information from millions of customers.
- **Impact**: The breach **affected around 40 million credit and debit card accounts** and led to significant **financial** losses and **reputational** damage for Target. The incident also prompted increased scrutiny and improvements in payment card security standards.

Example of Security breach

3. WannaCry Ransomware Attack (2017)

- **Description**: The WannaCry ransomware attack spread rapidly across the globe, **encrypting files** on infected computers and demanding ransom payments in Bitcoin. It **exploited a vulnerability in Microsoft Windows** that had been leaked by the **Shadow Brokers** hacker group.
- **Impact**: The attack affected hundreds of thousands of computers in over 150 countries, including critical infrastructure and healthcare organizations. The disruption caused financial losses and operational challenges for many organizations.

4. Sony PlayStation Network (PSN) Hack (2011)

- **Description**: Sony's PlayStation Network was hacked, leading to a massive data breach where attackers gained access to personal information, including names, addresses, and payment details of approximately 77 million accounts.
- **Impact**: The breach resulted in a **23-day outage of the PlayStation Network**, significant **financial** losses, and **reputational** damage for Sony. The company also faced **legal actions** and had to enhance its security measures and offer compensation to affected users.

Example of Security breach

5. Stuxnet Worm (2010)

- **Description:** The Stuxnet worm was a sophisticated piece of malware designed to **sabotage Iran's nuclear enrichment facilities**. It specifically targeted and disrupted **industrial control systems** used in the enrichment process.
- **Impact:** Stuxnet caused physical damage to Iran's centrifuges and highlighted the vulnerabilities in critical infrastructure systems. It was a landmark case demonstrating how cyberattacks could be used for geopolitical objectives.

Stuxnet, **a computer worm**, discovered in June 2010, that was specifically written to take over certain programmable industrial control systems and cause the equipment run by those systems to malfunction, all the while feeding false data to the systems monitors indicating the equipment to be running as intended

What do we infer from all these examples?

Cryptography

Computer Security & CIA Triad

M S Vilkhu

Aug 2024)

Reasons for increased data breaches

- Increased dependence on IT
- Hyper connected world
- Weakness in Software development - vulnerabilities
- Misconfiguration
- People weakness / Human errors
- Process weakness
- Access control

Computer Security

Definition of Computer Security

The NIST Computer Security Handbook [NIST95] defines the term computer security as follows:

Computer 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 (includes hardware, software, firmware, information/data, and telecommunications).

preserving **the integrity, availability, and confidentiality** of information system

Three key terms at the heart of Computer security

- These terms are Confidentiality, Integrity & Availability

- Called as CIA triad.

CIA Triad


CONFIDENTIALITY
INTEGRITY
Data
protected
by CIA Triad
AVAILABILITY

CIA Triad

The **CIA Triad is a foundational** concept in information security, representing **three key principles** that are essential for protecting data and systems. These principles are:

1. **Confidentiality**:

- Ensures that information is **not disclosed** to **unauthorized i**ndividuals, entities, or processes. Only those with the correct permissions should access sensitive data.

- **Methods** to achieve confidentiality include **encryption**, **access control** mechanisms (like passwords or biometrics), and **secure communication channels**.

Confidentiality 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.

CIA Triad

The **CIA Triad is a foundational** concept in information security, representing **three key principles** that are essential for protecting data and systems. These principles are:

2. **Integrity**:

- Ensures that information is **accurate, consistent, and unaltered** unless **modified by authorized personnel**. It **prevents unauthorized** modifications, tampering, or corruption of data.

- **Techniques** like **hashing, checksums, and digital signatures** are often used to maintain integrity.

Integrity 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.

CIA Triad

The **CIA Triad is a foundational** concept in information security, representing **three key principles** that are essential for protecting data and systems. These principles are:

3. **Availability**:

- Ensures that information and resources are **available to authorized users** when needed. Systems should be up and running, accessible without undue delay or downtime.

- Availability is maintained **through redundancy**, **fault tolerance**, regular maintenance, and **effective disaster recovery plans.**

CIA Triad

The CIA Triad		
What Is the CIA?		
Confidentiality	**Integrity**	**Availability**
The information is safe from accidental or intentional disclosure.	The information is safe from accidental or intentional modification or alteration.	The information is available to authorized users when needed.
Example		
I send you a message, and no one else knows what that message is.	I send you a message, and you receive exactly what I sent you (without any modification)	I send you a message, and you are able to receive it.
What's The Purpose of the CIA?		
Data is not disclosed	Data is not tampered	Data is available
How Can You Achieve the CIA?		
e.g., Encryption	e.g., Hashing, Digital signatures	e.g., Backups, redundant systems
Opposite of CIA		
Disclosure	Alteration	Destruction

CIA Triad

- **Additional concept** required apart from CIA, these are

- **Authenticity**: The property of
  - **being genuine** and
  - being able to be **verified and trusted**; T
  - his means verifying 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 of an entity to be **traced uniquely** to that entity.
  - This **supports nonrepudiation, deterrence, fault isolation, intrusion detection and prevention**, and after action **recovery and legal action**.
  - Because truly secure systems are not yet an achievable goal, we must be able to **trace a security breach** to a responsible party.
  - Systems must **keep records of their activities** to permit later forensic analysis to trace security breaches or to aid in transaction disputes**.**

Impact due to breach of security

- **three levels of impact** on organizations or individuals should there be a **breach of security** (i.e., a loss of confidentiality, integrity, or availability). (as per FIPS PUB 199 – (Federal information processing standards)
- Low
- Medium
- High

Impact due to breach of security

- **three levels of impact** on organizations or individuals should there be a **breach of security** (i.e., a loss of confidentiality, integrity, or availability). (as per FIPS PUB 199 – (Federal information processing standards)
- **Low**.
- **limited adverse effect on organizational operations, organizational assets, or individuals**. A limited adverse effect means that, for example, the loss of confidentiality, integrity, or availability might

  (i) cause a **degradation in mission capability** to an extent and duration that the organization is **able to perform its primary functions**, but the effectiveness of the functions is noticeably reduced;

  (ii) result in minor damage to organizational assets;

  (iii) result in minor financial loss; or

  (iv) result in minor harm to individuals.
- Medium
- High

Impact

- **three levels of impact** on organizations or individuals should there be a **breach of security** (i.e., a loss of confidentiality, integrity, or availability). (as per FIPS PUB 199 – (Federal information processing standards)
- Low.
- **Medium**
- The loss could be expected to have a **serious adverse effect on organizational operations, organizational assets, or individuals**. A serious adverse effect means that, for example, the loss might

  (i) cause a **significant degradation** in mission capability to an extent and duration that the organization is **able to perform its primary** functions, but the **effectiveness of the functions is significantly reduced**;

  (ii) result in **significant damage** to organizational assets;

  (iii) result in **significant financial loss**; or

  (iv) result in **significant harm to individuals** that does not involve loss of life or serious, life-threatening injuries
- High

Impact

- **three levels of impact** on organizations or individuals should there be a **breach of security** (i.e., a loss of confidentiality, integrity, or availability). (as per FIPS PUB 199 – (Federal information processing standards)
- Low.
- Medium
- **High**
- **High:** The loss could be expected to **have a severe or catastrophic adverse effect on organizational operations, organizational assets, or individuals**. A severe or catastrophic adverse effect means that, for example, the loss might
  - (i) cause a **severe degradation** in or loss of mission capability to an extent and duration that the organization is **not able to perform one or more of its primary functions**;
  - (ii) result in **major damage** to **organizational assets**;
  - (iii) result in **major financial** loss; or
  - (iv) result in severe or **catastrophic harm to individuals** involving loss of life or serious, life-threatening injuries.

Examples

- **Confidentiality**
- **High**
- Student grades
  - – High for the students and should be available to students, parents and the employees working on it
- **Moderate**
- Student enrolment information
  - Moderate – seen by more people and less likely to be targeted than grades, less damage
- **Low**
- Students Directory information
  - – it is available on internet or school / university website

Examples

- **Integrity**
- **High**
- Hospital patient's allergy stored in database
  - – Doctor should be able to trust the information is correct and current
- an employee (e.g., a nurse) who is authorized to view and update this information deliberately falsifies the data to cause harm to the hospitalModerate
- The database needs to be restored to a trusted basis quickly, and it should be possible to trace the error back to the person responsible
- Patient allergy information is an example of an **asset with a high requirement for integrity**.
- **Inaccurate information** could result in **serious harm or death** to a patient and **expose the hospital to massive liability.**

Examples

- **Integrity**
- **Moderate**
- **Web site** that offers a forum to **registered users** to **discuss** some specific topic. Either a registered user or a hacker could falsify some entries or deface the Web site.
- If the forum exists only for the enjoyment of the users, brings in little or no advertising revenue, and is not used for something important such as research, then potential **damage is not severe**.
- The Web master may experience **some data, financial, and time loss**.

Examples

- **Integrity**
- **low**
- An example of a low integrity requirement is an **anonymous online poll**. Many Web sites, such as news organizations, offer these polls to their users with very few
- safeguards. However, the inaccuracy and unscientific nature of such polls is well understood.

Examples

- **Availability**
- **High**
- The **more critical a component or service**, the higher is the level of availability required.
- **authentication services** for critical systems, applications, and devices.
- **An interruption** of service results in the **inability for customers** to access computing resources and staff to access the resources they need **to perform critical tasks**.
- The **loss of the service** translates into a
  - **large financial loss** in
  - lost employee productivity and
  - potential customer loss.

Examples

- **Availability**
- **Moderate**
- availability requirement is a **public Web site for a university**; the Web site provides
- information for current and prospective students and donors.
- Such a site is **not a critical component** of the university's information system, but its unavailability will **cause some embarrassment**.

Examples

- **Availability**
- **Low**
- An **online telephone directory** lookup application would be classified as
- Although the temporary loss of the application may be an annoyance

Challenges of Computer Security

- Field of computer and network security quite challenging and complex. Reason are

1. **Simple terms and complex implementation**. Terms are simple (confidentiality, integrity, availability, non-reputation & authentication) self-explanatory but the implementation is complex.
2. **Developing services by looking at potential attacks**. In developing a particular security mechanism or algorithm, one must always consider **potential attacks on those security features**.
   - In many cases, **successful attacks are designed by looking at the problem in a completely different way**, therefore **exploiting an unexpected weakness** in the mechanism.
3. **Procedure are complex and counterintuitive**. Because of point 2, the procedures used to provide particular services are often counterintuitive.
   - various aspects of the **threat are considered** that **elaborate security mechanisms make sense**.
4. **Decide where to place security mechanism**– physically & logically
   - At what layer or layers of TCP/IP should the mechanism should be placed.

Challenges of Computer Security

- Field of computer and network security quite challenging and complex. Reason are

5. **Security mechanism involves more than one algorithms and protocols**. Interworking of these parts in perfect fashion only leads to security of the entire IT ecosystem. There is communication element which adds to more complexity.
6. Computer security is the **battle between defender and attacker.** Defender must block **all the weakness however attack need to find one weakness.**
7. Get funding is difficult justify till a security failure happens
8. Security requires **continuous monitoring**
9. Security is still an **afterthought** rather than part of the design
10. **Security vs ease of working**. System admin finds security an impediment in their work.

Thank You