

What is security?

Mainack Mondal

CS 60081
Autumn 2022



Roadmap

- Defining computer security
- CIA model
- How do security violations happen in practice?
- Basic security analysis

Security: Many definitions

- “The *protection of data* and resources from **accidental and malicious acts**, usually by taking appropriate actions ...These acts many be modification, destruction, access, disclosure or acquisition if not authorized.”

-- ISO/IEC, 1998

Security: Many definitions

- “The *protection of data* and resources from *accidental and malicious acts*, usually by taking appropriate actions ...These acts many be modification, destruction, access, disclosure or acquisition if not authorized.”

-- ISO/IEC, 1998

- Building Systems to remain dependable in the face of *malice, error or mischance*

-- Ross Anderson

Roadmap

- Defining computer security
- CIA model
- How do security violations happen in practice?
- Basic security analysis

Properties of a secure system (CIA model)

- Confidentiality
 - Non-public information should be accessible only to authorized parties (access control, encryption, policies)
- Integrity
 - System and data should remain unaltered, except for authorized parties (error correction code, sha3)
- Availability
 - Information and system should remain accessible for authorized use (protection against DDOS, related to usability)

CIA model needs a few more properties to function

- **Authentication**
 - Verifying that the identify of an entity is genuine relative to expectations arising from context (**Password**)
- **Authorization**
 - Ensuring that system and data are only accessible to intended entities (**access control**)
- **Accountability**
 - Identifying entities responsible for past actions (**blockchain, append-only logs**)

Roadmap

- Defining computer security
- CIA model
- How do security violations happen in practice?
- Basic security analysis

Security violations in practice

- Source: "A Summary of Computer Misuse Techniques," by Peter G. Neumann and Donn B. Parker, 1989
 - External misuse
 - Hardware misuse
 - Masquerading
 - Setting up subsequent misuse
 - Bypassing intended controls
 - Active misuse
 - Passive misuse
 - Inactive misuse
 - Indirect misuse

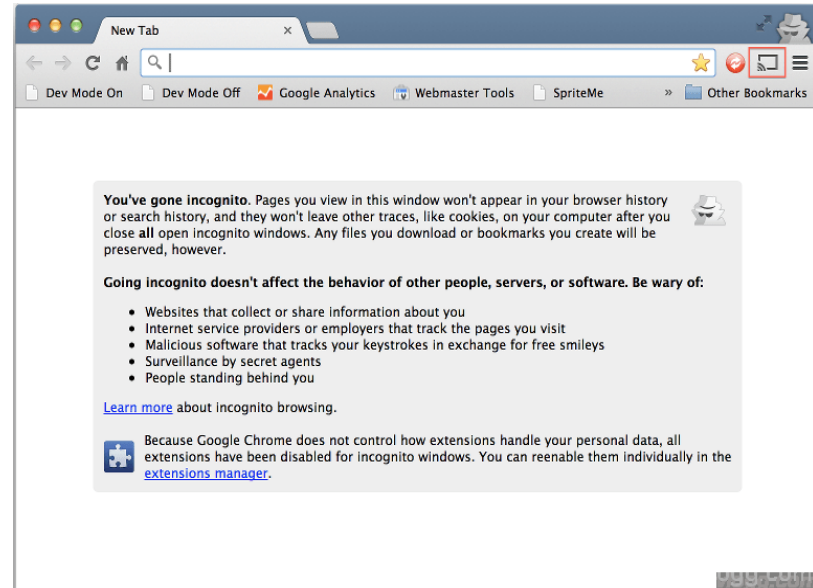
A brief look at these misuses

- External misuse

- Generally nontechnological (physical scavenging, visual spying, deception)

- Hardware misuse

- Passive (logical scavenging, eavesdropping)
- Active (trojan horse, introducing faults)



A brief look at these misuses

- **Masquerading**
 - Impersonation; playback and spoofing attacks; may be indistinguishable from legitimate activity
- **Setting up subsequent misuse**
 - Logic bombs, zero days, malicious worms, botnets, ransomwares, viruses
- **Bypassing intended controls**
 - Using trapdoors (e.g., known bugs), authorization attacks (cracking passwords)

A brief look at these misuses

- **Active misuse** : Modifying data, DoS attacks
- **Passive misuse**: Browsing, analyzing collected data without changing the system
- **Inactive misuse**: Misuse because user was too lazy (e.g. giving phone to repair shop without erasing data)
- **Indirect misuse**: Breaking cryptographic keys and then use it for listening to encrypted communications

Roadmap

- Defining computer security
- CIA model
- How do security violations happen in practice?
- Basic security analysis

How to do basic security analysis for a system?

- Question: Is a given system secure OR how do you secure the system?
 - *What* do we intend to protect? (system model)
 - *Who* is the attacker or the threat? (threat model)
 - What are the security requirements? (Security Goals)
 - What security approaches can be effective? (Solution)

1. System model

- **Understand** architecture of the system
- **Enumerate** asset and their value in the system
- Possible questions you should ask:
 - What are the exact assets? (be as specific as possible)
 - What is the operating value (can be \$, can be man hours)
 - What is the impact if this asset if breached?

Question: What is the **system model** for **protecting against password guessing attack** on a banking website?

2. Threat model

- **Identify** potential attackers (script-kiddies, hacker-for-hire, your ex, a nation state?)
- **Enumerate** attacker resources
- Estimate number of attacks, probability of attack

Common adversary types in threat models

- **Attacker action**
 - Passive (eavesdropping), Active (man-in-the-middle attack)
- **Attacker capability**
 - Script kiddies to nation states (decides how resilient your solution should be)
- **Attacker access**
 - External (can only observe the system), Internal (inside the system, e.g., compromised user account)

Common adversary types in threat models

- **Attacker action**
 - Passive (eavesdropping), Active (man-in-the-middle attack)
- **Attacker capability**
 - Script kiddies to nation states (decides how resilient your solution should be)
- **Attacker access**
 - External (can only observe the system), Internal (inside the system, e.g., compromised user account)

Question: What is the **threat model** for **protecting against password guessing attack** on a banking website?

3. Security goals

- What are your security requirements
 - Confidentiality (encryption)
 - Integrity (cryptographic hashes)
 - Authenticity (MAC or keyed hash)
 - Availability (DDoS)
 - Auditability (Blockchain, tamper-proof-logs)
 - Access control
 - Privacy
 - Plausible deniability ...

4. Designing systems

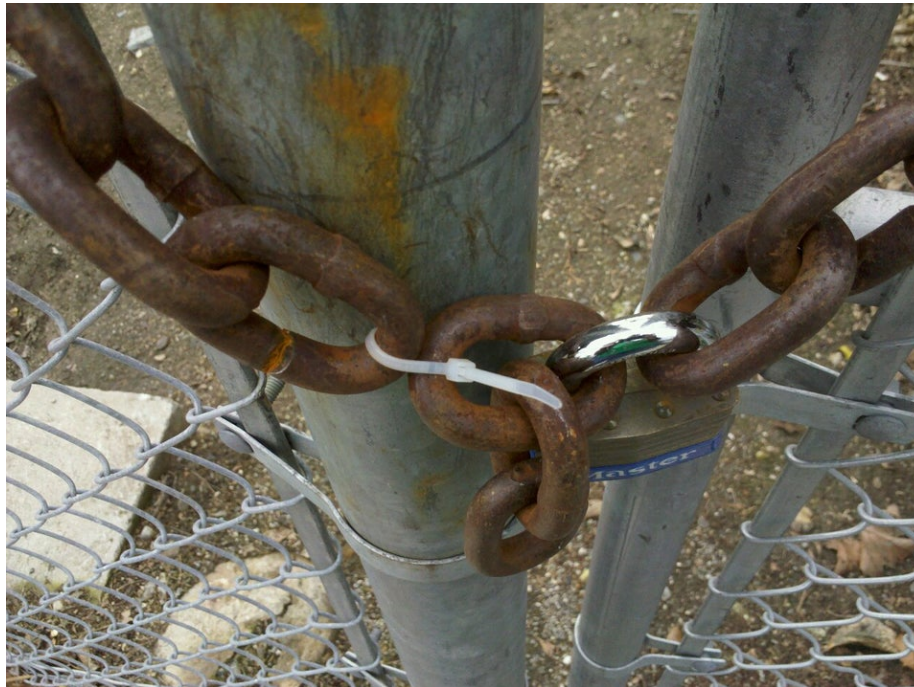
- Security via policy
 - Pass a law and make it illegal
- Use cryptography and security primitives
 - Encryption, hashes, VPNs, firewalls
- Make your system resilient to attack
 - Keep updated copies of systems (*hot standby*)
- Detection and recovery
 - Intrusion detection system, Redundancy etc.

Pitfalls of security

- Can't protect against everything
 - expensive and inconvenient
- Identify most likely avenues of attack
 - Identify *likely* attackers and their resources?
 - Identify *likely* consequences – financial loss or personal loss?
 - Accept your design **will not** defend against all attacks
 - Identify where will it not help? (is that reasonable)

You need to think like an attacker

- Adversary target *assets*, not defenses
 - Will try to exploit *weakest part* of the defenses (bribing, social engineering)



Summary

- Security is important AND difficult
- Security is NOT absolute
 - Your solution will depend on YOUR system model, threat/attacker model, security goals
 - Shoot for at least “raising the bar”
- Bonus: System and attack model of obtaining encrypted data
 - Security by obscurity
 - Kerckhoffs’s law/Shannon’s maxim (“Enemy knows the system”)