Security mindset

Security threats, vulnerability; risk and security controls

Debdeep Mukhopadhyay
Mainack Mondal

CS 60065
Autumn 2020

Roadmap

- Defining computer security
- Goals of computer security: CIA model
- Security policy in a system
- How do security violations happen in practice?
- Basic risk 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
- Goals of computer security: CIA model
- Security policy in a system
- How do security violations happen in practice?
- Basic risk analysis

Properties of a secure system (CIA model)

- Confidentiality
    - Non-public information should be accessible only to authorized parties (access control, encryption, *procedural means*)
- Integrity
    - System and data should remain unaltered, except by authorized parties (error correction code, cryptographic hashes or checksums)
- Availability
    - Information and system should remain accessible for authorized use (protection against DDOS, related to usability)

Properties of a secure system (CIA model)

- Confidentiality
  - Non-public information should be accessible only to authorized parties (access control, encryption, *procedural means*)
- Integrity
  - System and data should remain unaltered, except by authorized parties (error correction code, cryptographic hashes or checksums)
- 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

- Authorization
    - Ensuring that system and data are only accessible to intended entities

CIA model needs a few more properties to function

- Authorization
    - Ensuring that system and data are only accessible to intended entities == called “principals” in security

CIA model needs a few more properties to function

- Authorization
  - Ensuring that system and data are only accessible to intended entities

CIA model needs a few more properties to function

- Authorization
  - Ensuring that system and data are only accessible to intended entities
- Authentication
  - Verifying that the identify of an entity is genuine relative to expectations arising from context, Authentication also enable Attribution (Password, cryptographic keys)

CIA model needs a few more properties to function

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

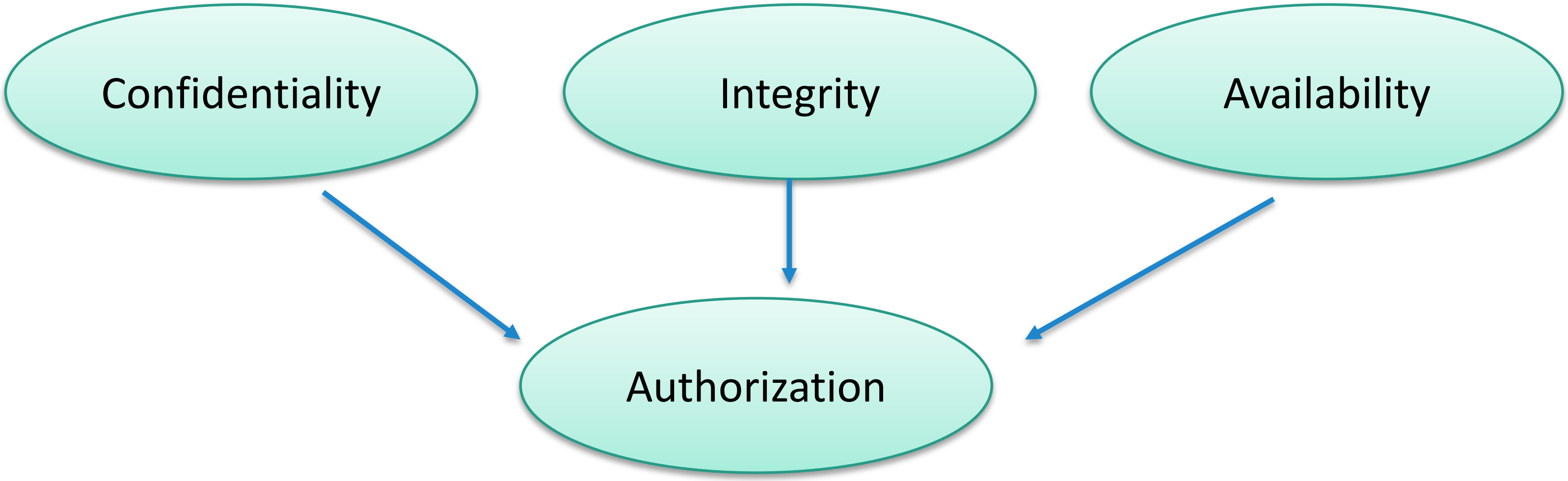
Putting it all together

Confidentiality

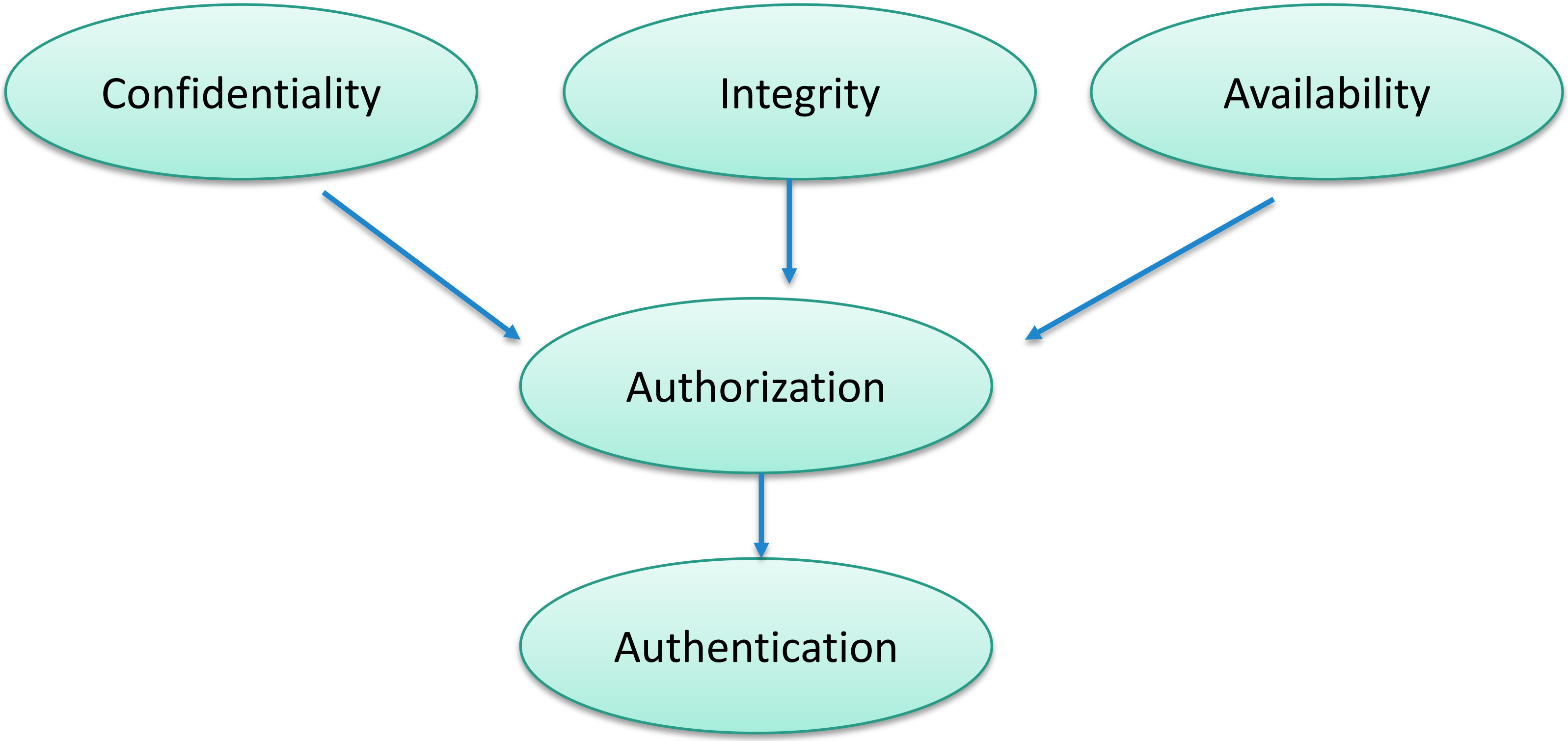
Integrity

Availability

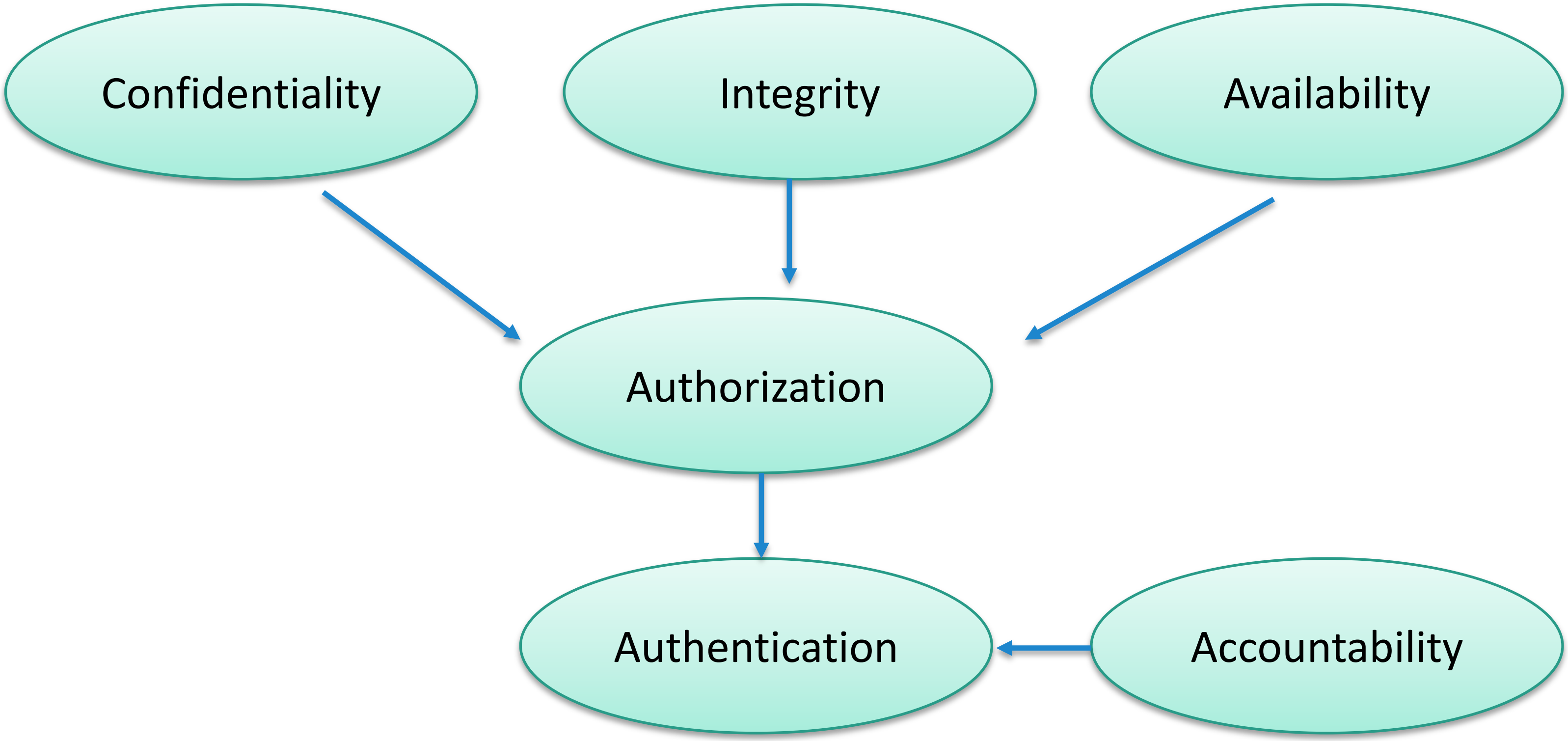
Putting it all together



Putting it all together



Putting it all together



Roadmap

- Defining computer security
- Goals of computer security: CIA model
- Security policy in a system
- How do security violations happen in practice?
- Basic risk analysis

Security policy

- Key question: Who is authorized to access what?
  - Authentication, enumerating assets
  - Violated if there is unauthorized access/modification

Security policy

- Key question: Who is authorized to access what?
  - Authentication, enumerating assets
  - Violated if there is unauthorized access/modification

Used to find Security violations

Threat and control

- Threats: Entities performing steps/methods which will violate security (enable unauthorized access)
  - Steps/methods == Attack vector
- Controls and Countermeasures: Prevent / detect unauthorized access

Roadmap

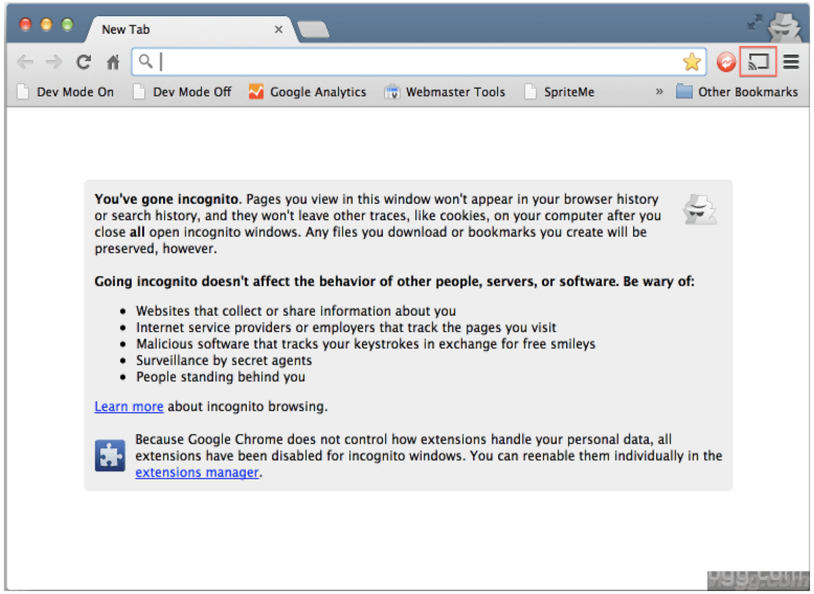
- Defining computer security
- Goals of computer security: CIA model
- Security policy in a system
- How do security violations happen in practice?
- Basic risk analysis

Security violations / threats / vulnerabilities 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)



You've gone incognito. Pages you view in this window won't appear in your browser history or search history, and they won't leave other traces, like cookies, on your computer after you close **all** open incognito windows. Any files you download or bookmarks you create will be preserved, however.

Going incognito doesn't affect the behavior of other people, servers, or software. Be wary of:

- Websites that collect or share information about you
- Internet service providers or employers that track the pages you visit
- Malicious software that tracks your keystrokes in exchange for free smileys
- Surveillance by secret agents
- People standing behind you

Learn more about incognito browsing.

Because Google Chrome does not control how extensions handle your personal data, all extensions have been disabled for incognito windows. You can reenable them individually in the extensions manager.

- 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
- Goals of computer security: CIA model
- Security
- How do security violations happen in practice?
- Basic risk analysis

Why risk analysis?

- You need to focus on protecting the most important and most vulnerable resources
  - How?

Why risk analysis?

- You need to focus on protecting the most important and most vulnerable resources
    - How? calculate approximate loss using Risk Equation

Why risk analysis?

- You need to focus on protecting the most important and most vulnerable resources
  - How? calculate approximate loss using Risk Equation

Risk due to an attack

=

Probability That an attack will happen

Why risk analysis?

- You need to focus on protecting the most important and most vulnerable resources
  - How? calculate approximate loss using Risk Equation

Risk due to an attack

=

Probability That an attack will happen

X

Probability that the vulnerability exists

Why risk analysis?

- You need to focus on protecting the most important and most vulnerable resources
  - How? calculate approximate loss using Risk Equation

Risk due to an attack

=

Probability That an attack will happen

X

Probability that the vulnerability exists

X

Value of the targeted asset (tangible + intangible)

Fundamental questions for building any secure system

1. What assets are most valuable, and what are their values?

2. What system vulnerabilities exist?

3. What are the relevant threat agents and attack vectors?

4. What are the associated estimates of attack probabilities, or frequencies?

Next class

- Basic security analysis
  - Threat modelling
  - Adversary modelling
- Design principles for security