Introduction to Computer Security

Special Topic: Practical Computer Security

CSCI-GA.3033-019

Spring 2018

Housekeeping

Spring 2018

Special Topic: Practical Computer Security

CSCI-GA.3033-019

CIWW 201 Tuesdays 7:10-9:00PM

Instructor: Thitima Srivatanakul, Ph.D.

Email: thitima@cs.nyu.edu

Office hour: after class and by appointment

Grader: Le Wang (Cody) lw2341@nyu.edu

Security

“The state of being free from danger or threat.”

[Oxford dictionary]

“Protection of a person, building, organization or country against threats such as crime or attacks by foreign countries.”

[Cambridge dictionary]

“Security is all about protecting your computer system and the items you value”

[Pfleeger et al., 2015]

“Security is the quality or state of being *cost-effectively* protected from undue losses”

[Longley and Shain 1987]

What is Computer Security?

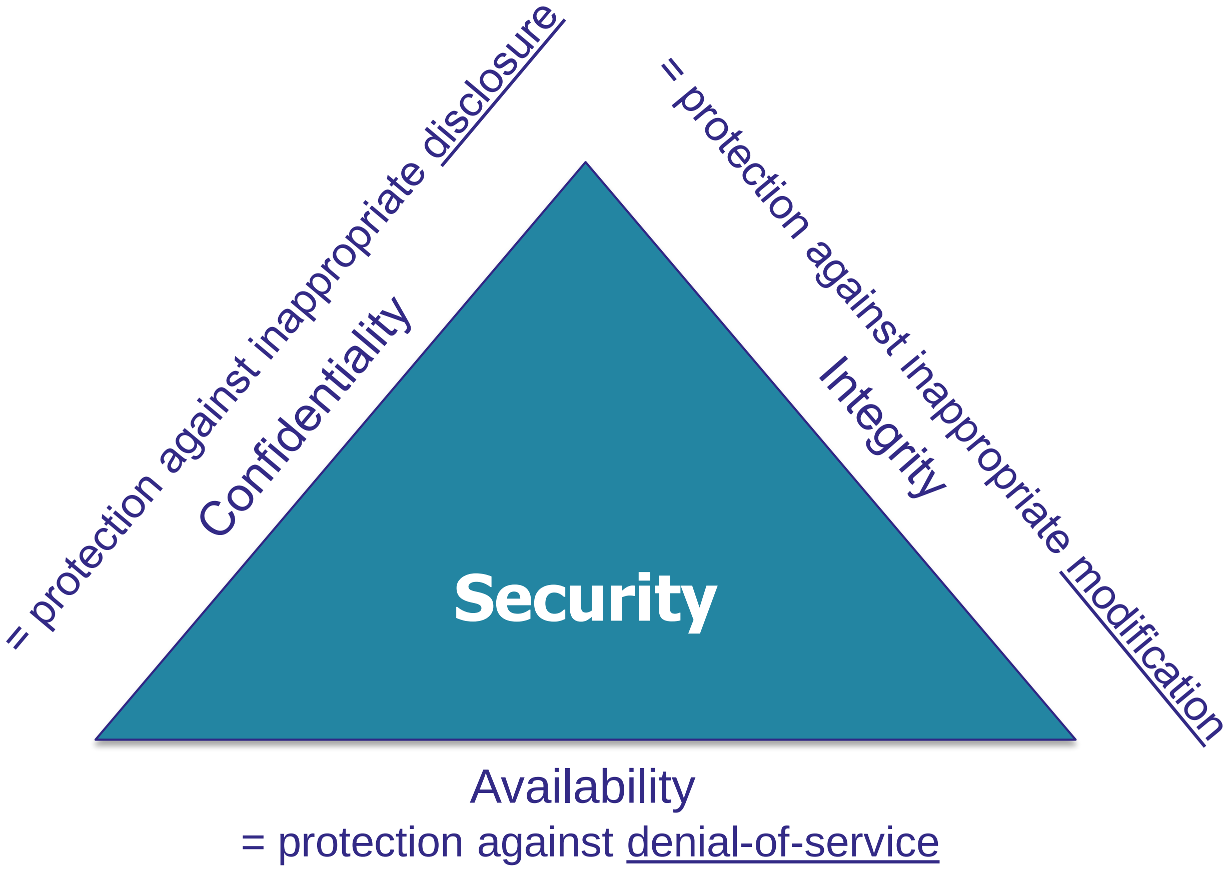
- **Software Engineering**
  - Ensuring that certain things happen
  - Achieving desired behavior
  - e.g., Alice can download the file.

- **Security**
  - Ensuring that certain things don't happen
  - Preventing undesired behavior
  - E.g., Chuck cannot modify the file.

> "Security is all about protecting your computer system and the items you value, which is called **assets."** – Pfleeger et al.

> Computer systems – hardware, software and data – have value and deserve security protection.

CIA Triad

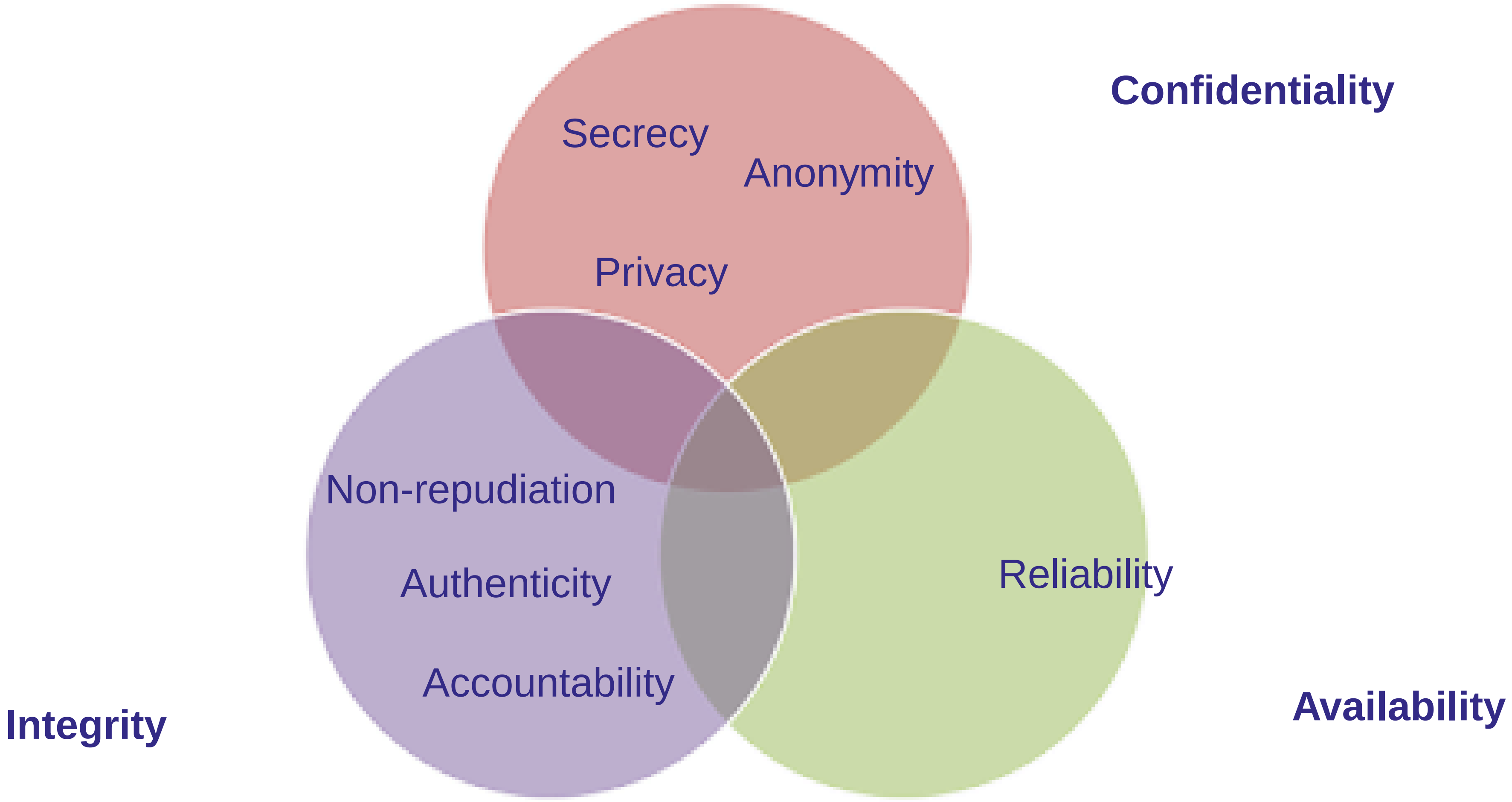

= protection against inappropriate disclosure
Confidentiality
= protection against inappropriate modification
Integrity
Security
Availability
= protection against denial-of-service

- **Confidentiality** - assets of the computer system should be accessible only by authorized parties.

- **Integrity** - assets can be modified only by authorized parties or in authorized ways.

- **Availability** - authorized parties should not be prevented from accessing objects to which they have legitimate access.

Sub properties



Confidentiality

Secrecy

Anonymity

Privacy

Non-repudiation

Authenticity

Accountability

Reliability

Integrity

Availability

Security concepts : some definitions

- **Vulnerability**
  - A weakness in the system
  - A vulnerability can be exploited to cause loss or harm
  - E.g. unpatched applications/OS, unrestricted wireless access point, an open port on a firewall.

- **Threat**
  - A set of circumstances that has the potential to cause loss or harm.
  - Any potential danger that is associated with the exploitation of a vulnerability.
  - E.g. *threat agent* – intruder accessing the network, a process accessing confidential data, an employee copying confidential information.

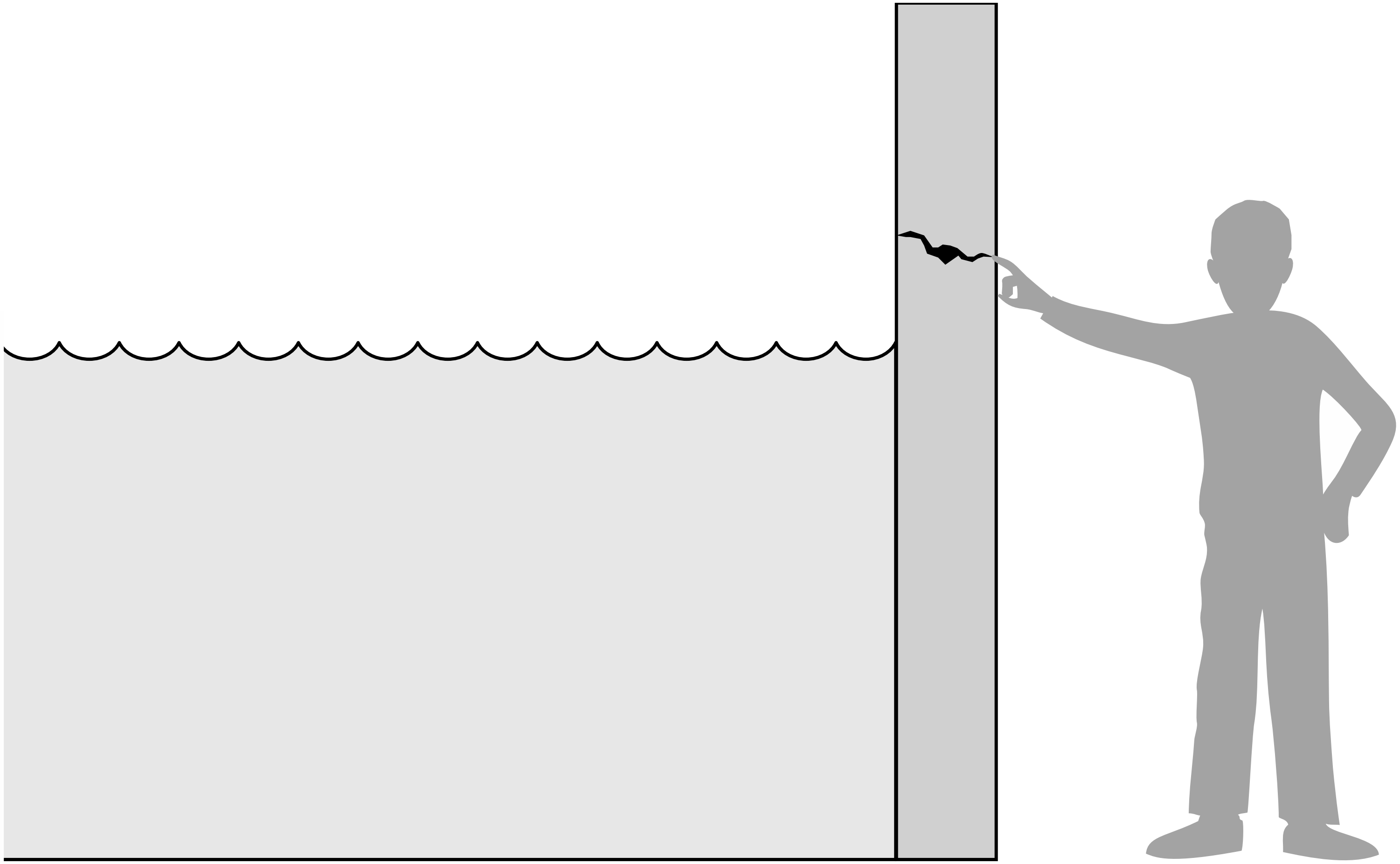
Security concepts : some definitions

- **Risk**
  - The likelihood of a threat source exploiting a vulnerability and the corresponding business impact.

- **Control**
  - An action, device, procedure, or technique that eliminates/reduces a vulnerability and/or to counter threats.

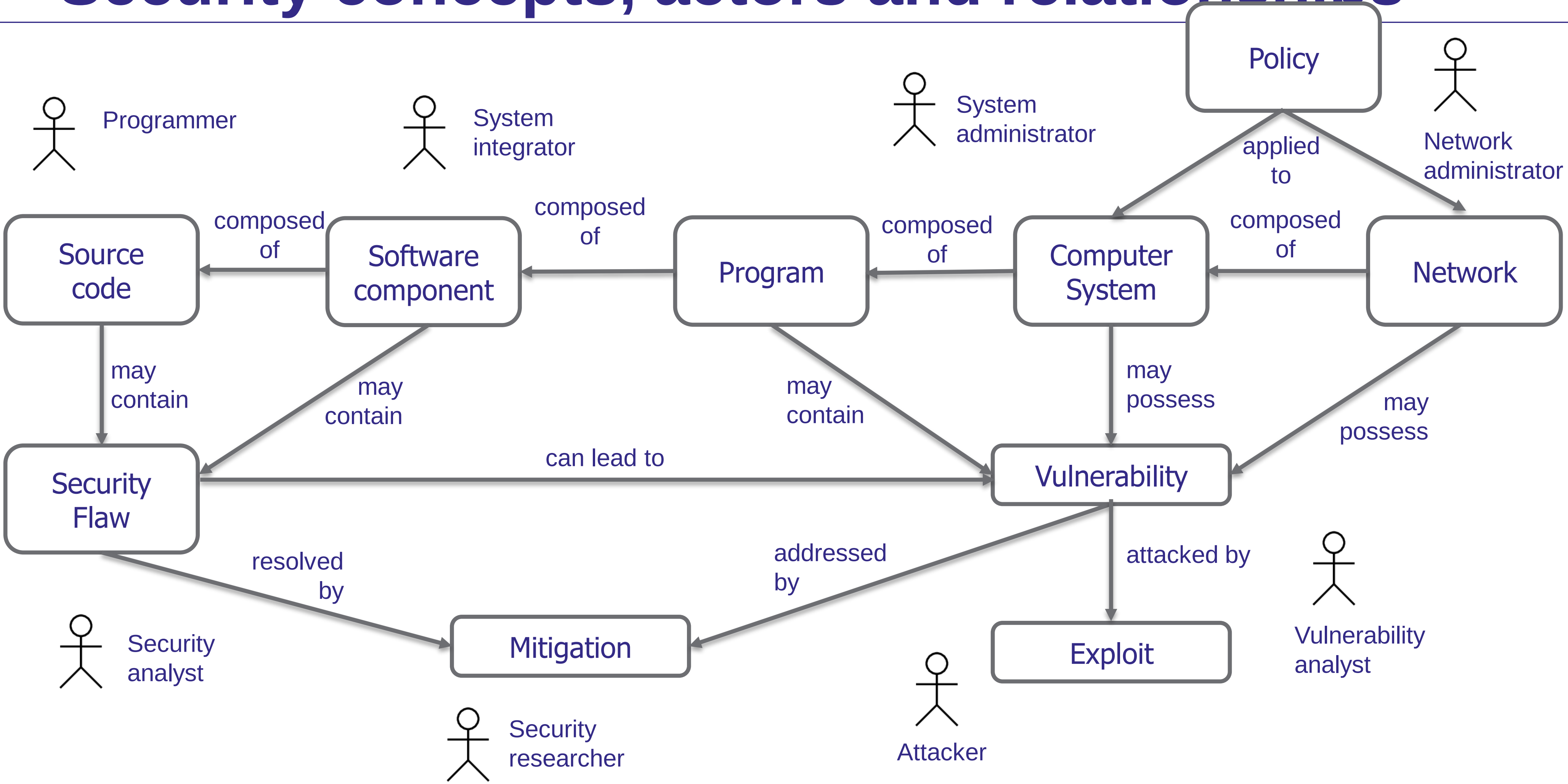
    -> mitigate/reduce the potential risk.
  - Also called a countermeasure / safeguard

Vulnerability-Threat-Control



From *Security in Computing, Fifth Edition*, by Charles P. Pfleeger, et al.

Security concepts, actors and relationships



Seacord, R. C. (2005)

Functionalities of Security Controls

- **Preventive** – to avoid an incident from occurring

  by blocking the attack or removing the vulnerability
- **Detective** – identifies an incident's activities (either as it happens or some time after the fact)
- **Corrective** – fixes systems after an incident has occurred
- **Deterrent** – to discourage a potential attacker

  by making the attack harder but not impossible
- **Recovery** – to bring the environment back to regular operations

Security Controls

- Identification & Authentication
  - Identification – is the act of asserting who a person is.
  - Authentication – is the act of proving that asserted identity.
    - ✓ (1) something you know
    - ✓ (2) something you have
    - ✓ (3) something you are
  - Authentication, however, need not be a ‘one-off’ activity
  - Two factor authentication/multi factor authentication

- Access Control
  - Limits who can access what in what ways
  - ensures that only authorized users can gain access to protected resources
  - Example: the unix’s control list, role-based access control, password protection

Security Controls

- Communication Security
  - Cryptography – conceals data against unauthorized access
    - An *encryption* mechanism transforms plain into unreadable text (called *cipher* text).
    - *Decryption* then transforms back to the original plain text
  - Security Protocols - a sequence of steps to allow communication
    - Transport Layer Security (TLS) & Secure Sockets Layer (SSL) - an example of protocol for allowing users to send information to web sites.
- Physical Controls
  - Detective measures – CCTV, alarm, personnel ID system, and metal or movement detectors.
  - Preventive measures – locks on doors, guards, fencing and strong constructions.
- Administrative Controls – “soft controls”
  - screening and management of personnel, password management, information house keeping and media handling, security documentation, training

Controls mapped to the CIA triad

Confidentiality	Integrity	Availability
Encryption for data at rest	Hashing (data integrity)	Redundant array or independent disks (RAID)
Encryption for data in transit (IPSec, TLS, PPTP, SSH)	Configuration management (system integrity)	Clustering
Access control	Change control (process integrity)	Load balancing
	Access control	Redundant data/power lines
	Software digital signing	Software and data backups
	CRC functions	

Basic Principles

J. H. Saltzer and M. D. Schroeder. The protection of information in computer systems. In *Proceedings of the IEEE*, volume 63, pages 1278–1308, 1975.

- Economy of Mechanism (Simplicity) –
  - The security mechanisms should be as simple as possible.
  - Implementation of unnecessary security mechanisms should be avoided.
- Fail-safe Defaults –
  - When a system fails, it should do so securely.
  - default should be no access; explicit grant access.
  - e.g. if a firewall fails, no packets will be forwarded.

Basic Principles

- Complete Mediation
  - All requests/access to objects should be checked to ensure that they are allowed.
  - e.g. computer memory enforces checks on every memory access requests.
- Open Design
  - the security of a system should not depend on the secrecy of its protection mechanisms, i.e. don’t rely on security through obscurity
  - e.g. cryptography should still be secure if everything, except for the keys, is not kept secret.

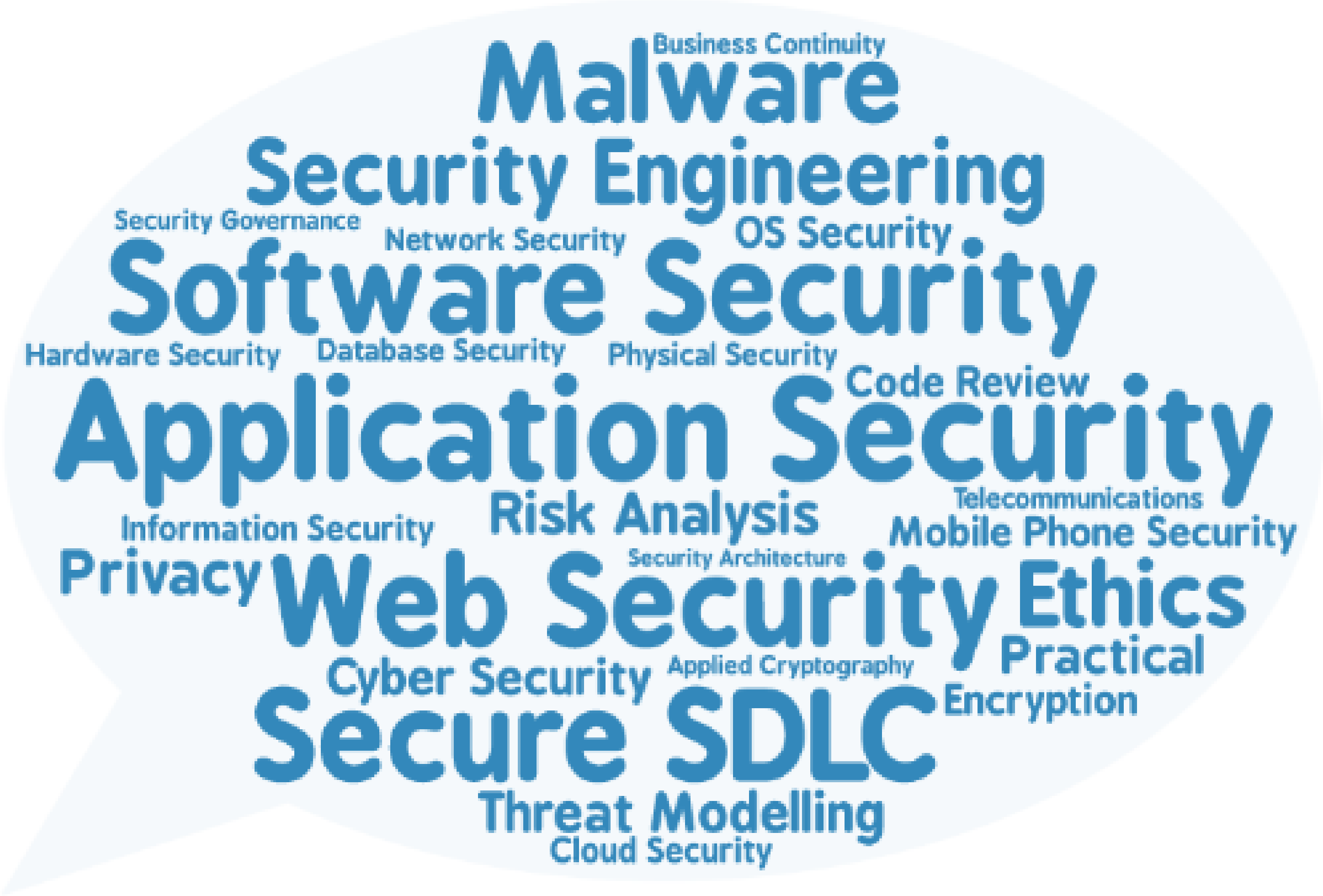
Basic Principles (2)

- Separation of Privilege –
  - no complete power – security should not reply only on a single mechanism
  - two or more conditions must be met before access should be permitted.
  - e.g. the use of token ID in web requests instead of relying only on cookies.
- Least Privilege – “need-to-know” rule.
  - Any component and user of a system should operate using the least set of privileges to complete its job
  - e.g. do not allow web applications to use sa or other privileged db account.

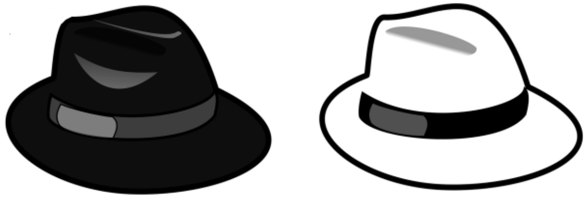
Basic Principles (3)

- Least common mechanism –
  - avoid having multiple subjects sharing mechanisms to grant access to a resource
  - mechanisms used to access resources should not be shared.
  - e.g. sharing of the network with an attacker allows him to eavesdrop packets.
- Psychological acceptability –
  - design usable security mechanisms
  - security mechanisms should be transparent to the users of the system
  - e.g. using of root account to circumvent restrictions

Course Overview



Topics Covered in the Course



PART1 – Understanding Threats/Attacks/Defenses

- Human Factors & Usability
  - Insider Attacks, Attacks on Passwords, Phishing
- Application Attacks
  - Buffer Overflows Exploits Format String Vulnerabilities
- Web Security
  - SQL Injection, XSS, CSRF, Broken authentication
- Malware
- Threat Modelling/Risk Management

PART2 – Building a Secure Software

- Requirements for Secure Software
- Secure Programming Techniques
- Penetration Testing / Security Testing

Also

- Legal & Ethical Issues

Grading

- Individual Homework Assignments – 30%
- Quizzes, Midterm Exam & Final Exam - 50%
    - Quizzes & Midterm Exam – 20%
    - Final Exam – 30%
- Course Project (team) + Participation – 20% *(*this is will be confirmed again)*

- All questions regarding assignments & project will be handled by Le Wang (Cody) lw2341@nyu.edu

At the end of the course…

- As a user
  - make better decisions
- As a software developer / IT manager
  - design and implement more secure system
- As a security researcher & professional
  - Identify new security issues
  - contribute solutions to security problems

Security Mindset - be more aware of security issues

References

- C.P. Pfleeger, S.L. Pfleeger and J. Margulies. *Security in computing* (5th ed.). Prentice Hall, 2015.
- S. Harris, *CISSP all-in-one exam guide*. McGraw-Hill, Inc., 2016.
- D. Longley and M. Shain. *Data and Computer Security, Dictionary of Standards, Concepts and Terms*. MacMillan Publishers Ltd., 1987.
- J. H. Saltzer and M. D. Schroeder. The protection of information in computer systems. In *Proceedings of the IEEE*, volume 63, pages 1278–1308, 1975
- R.C. Seacord, *Secure Coding in C and C*++. Pearson Education. 2005
- US-Cert. *Principles*. https://www.us-cert.gov/bsi/articles/knowledge/sdlc-process