# Lecture 1

1. Introduction
2. Basic Security Concepts

Dr. Hatim Alsuwat

# Course Information

https://hatimalsuwat.github.io/computersecurity-summer2024.html

Hatim Alsuwat, Ph.D.

HOME
RESEARCH
LAB
TEACHING
PUBLICATIONS
CONTACT

(14013602-1) COMPUTER SECURITY

HOMEPAGE AND SYLLABUS

Disclaimer

This is the best information available as of today, **Sunday July 31, 2022** at **3:30 a.m. KSA time**. Changes will appear in this web page as the course progresses.

Meeting time and place

- **Section 1:** Monday and Wednesday 1:00 p.m. - 2:50 p.m. Room: H07

Instructor: Dr. Hatim Alsuwat

Course Homepage: https://hatimalsuwat.github.io/computersecurity-summer2024.html
Office: 1148
Office hours: TBD
Phone: NA
Email: hssuwat@uqu.edu.sa

Course Overview

This course is the first level of computer and network security. The course will cover various topics related to computer security, data privacy, network protection against various attacks. The course gives students enough knowledge and a reasonable background to understand network security, active and passive attacks, Internet privacy, secure communications. Students are expected to practice biweekly homework, develop critical thinking about computer and network security, and apply learned materials in different contexts of various attacks, wireless and Internet security.

- Communication:
  - Announcements on webpage/ emails/ blackboard
  - Questions? Email me.
  - Staff email: hssuwat@uqu.edu.sa
- Course technology:
  - Website
  - UQU Blackboard
  - Regular homework
  - Help us make it awesome!

# Course Information

- Course Website https://hatimalsuwat.github.io/computersecurity-summer2024.html
- Discussion:
  - Please ask any question during the lecture (don't be shy)
  - There is no such thing as a stupid question.
  - Answer others' questions - if you know the answer ;-)
  - Learn from others' questions and answers

# Course Information

- **Assignments:**
  - ***Quizzes:*** there will be several quizzes randomly given
  - ***Homework assignments*:** there will be several homework assignments during the semester.
  - ***Exams*:** One Midterm Exam and One Final Exam. Closed book tests will cover the course material.
  - Assignments are always due on the announced day and time. Exams must be taken as scheduled except in cases of extenuating circumstances such as a documented emergency.
- Participation can help on margins

# Course Information

- **Grading:**
  - **Midterm Exam: 20%**
  - **Practical: 20%**
  - **Homework Assignments: 10%**
  - **Participation and Quizzes: 10%**
  - **Final Exam: 40%**

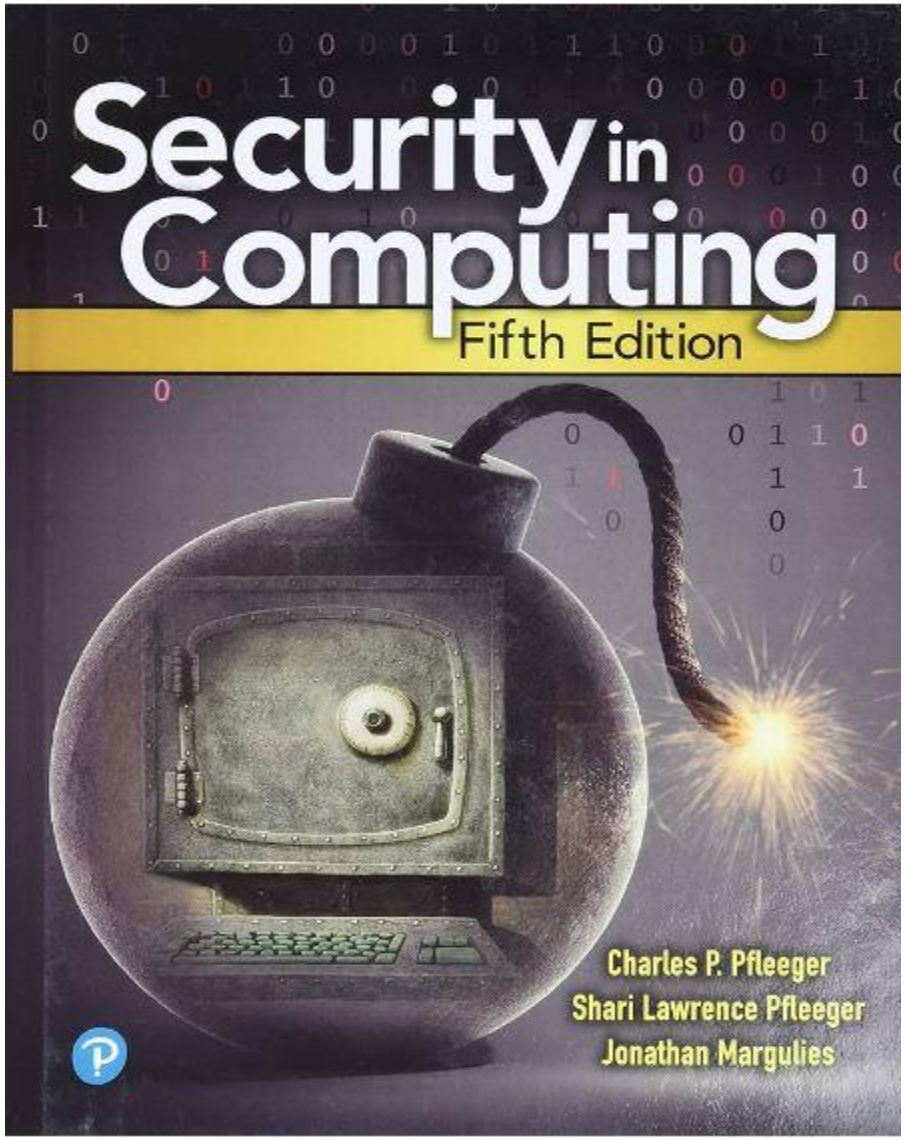
- **Total score that can be achieved: 100**

# Course Information

- **Meeting time and place:**
  - **Office:** Department of Computer Science (office #1148)
  - **Office hours:** Please email me if you have any question. If necessary, I will arrange a phone call or in-person meeting
  - **Email:** Hssuwat@uqu.edu.sa

# Textbook

Charles P. Pfleeger and Shari Lawrence Pfleeger, Security in Computing (5th Edition) (Hardcover), Prentice Hall PTR; ISBN: 9780134085043



# Course Information: Feedback

- Please give feedback positive or negative as early as you can via email.

# Reading Assignment

- **Reading assignments for this class**:
  - Pfleeger: Ch 1
- **Reading assignments for next class**:
  - Pfleeger: Ch 2

# TENTATIVE SCHEDULE

- Basic security concepts
- Cryptography, Secret Key
- Cryptography, Public Key
- Identification and Authentication, key-distribution centers, Kerberos
- Security Policies -- Discretionary Access Control, Mandatory Access Control
- Access control -- Role-Based, Provisional, and Logic-Based Access Control
- The Inference Problem
- Network and Internet Security, E-mail security, User Safety
- Program Security -- Viruses, Worms, etc.
- Firewalls
- Intrusion Detection, Fault tolerance and recovery
- Information Warfare
- Security Administration, Economic impact of cyber attacks

# What is Computer Security?

- Computer security is the protection of the items you value, called the **assets** of a computer or computer system.
- E.g. HW, SW, Data,

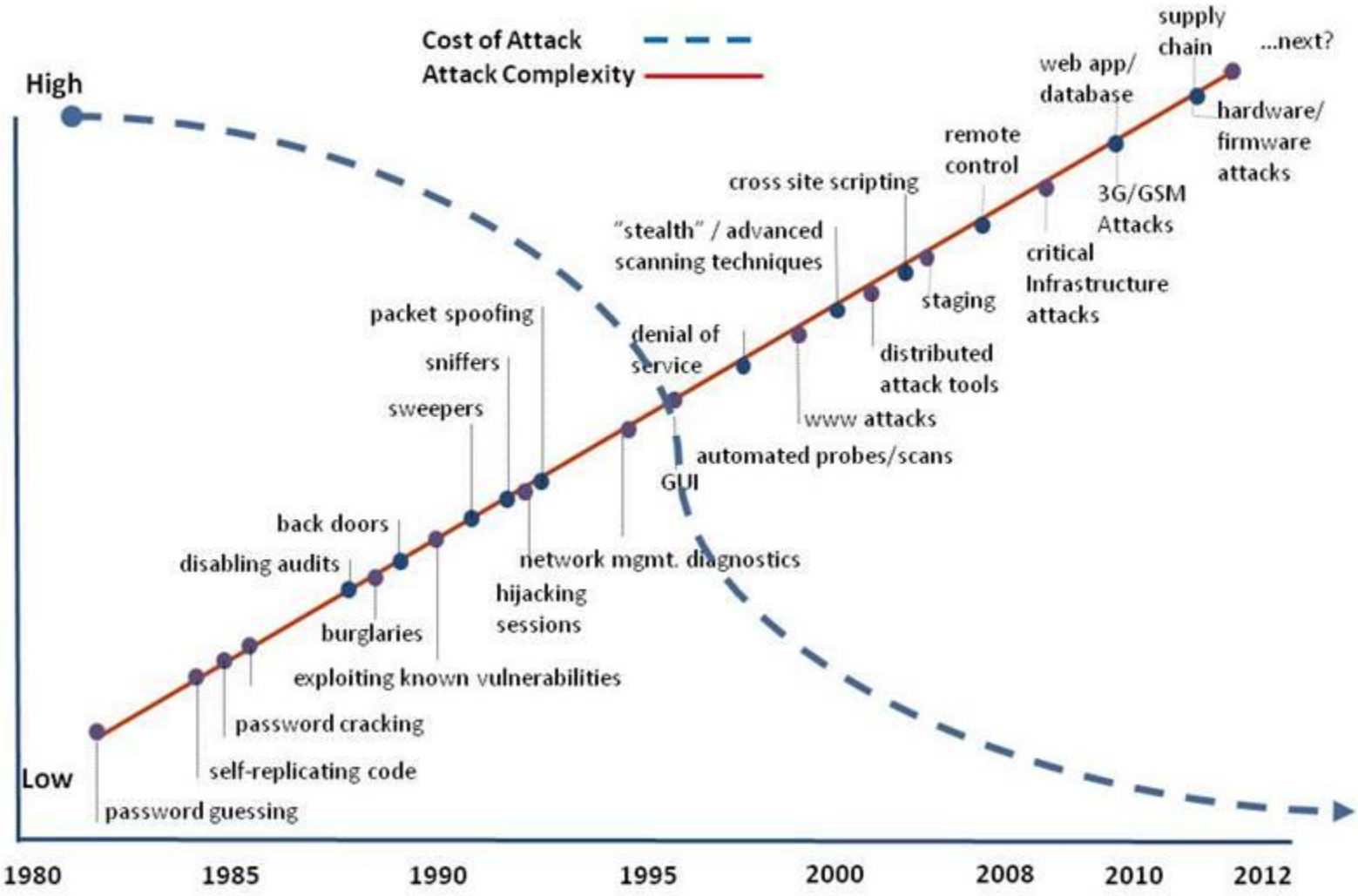
- There are many types of assets, involving hardware, software, data, people, processes, or combinations of these.

# Values of Assets

- After identifying the assets to protect, we next determine their value.
- We make value-based decisions frequently, even when we are not aware of them.
- For example, when you go for a swim, you can leave a bottle of water and a towel on the beach, but not your wallet or cell phone. The difference relates to the value of the assets.

# Diminishing Attack Costs & Increasing Complexity

*Increased network complexity & dependence means more attacks succeed with high payoffs*
*Technology advances mean lower cost for a successful attack*



# What Can I Do?

# Security Objectives

- **Confidentiality**: prevent/detect/deter improper **disclosure** of information
- **Integrity**: prevent/detect/deter improper modification of information
- **Availability**: prevent/detect/deter improper **denial of access** to services

# Military Example

- **Confidentiality**: target coordinates of a missile should not be improperly disclosed
- **Integrity**: target coordinates of missile should be correct
- **Availability**: missile should fire when proper command is issued

# Commercial Example

- **Confidentiality**: patient's medical information should not be improperly disclosed
- **Integrity**: patient's medical information should be correct
- **Availability**: patient's medical information can be accessed when needed for treatment

# Fourth Objective

- Securing **computing resources**: prevent/detect/deter improper **use** of computing resources
  - Hardware
  - Software
  - Data
  - Network

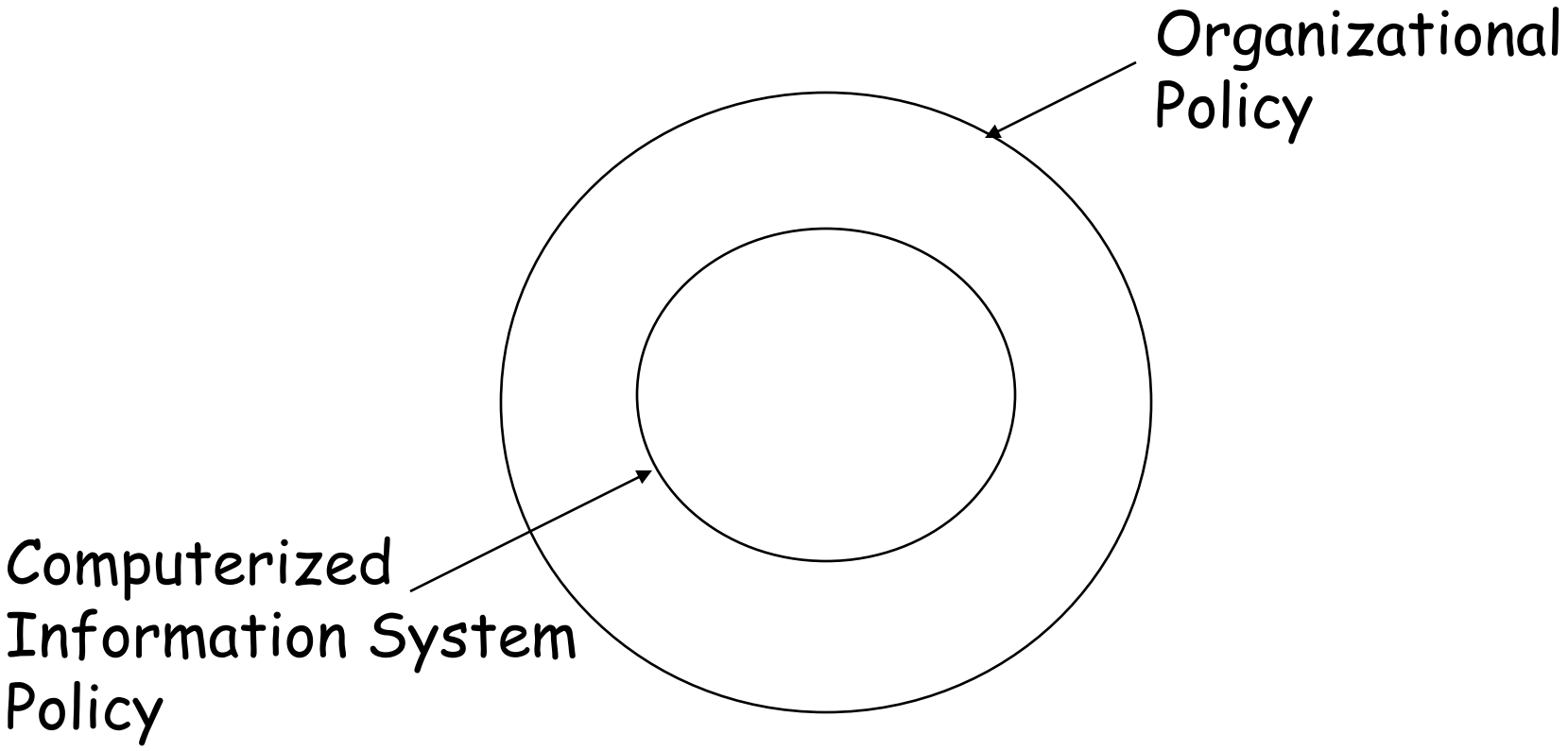
# Question 1: What is the trade off between the security objectives?

a) Confidentiality reduces integrity because secret data is higher quality
b) Integrity requires that the data is kept in an isolated location and cannot be accessed
c) Increased confidentiality may reduce availability
d) Confidential and correct data has high trade off availability

# Achieving Security

- **Organizational Goals**
  - Why to invest in security protection?
- **Policy**
  - What to protect?
- **Mechanism**
  - How to protect?
- **Assurance**
  - How good is the protection?

# Security Policy



# Question 2: Why do we need to fit the security policy into the organizational policy?

a) Because the management would not pay for it otherwise
b) Because security policy should support and protect organizational goals
c) Because this will make the implementation easier
d) Because it is mandated by law and regulation

# Security Mechanism

- Prevention
- Detection
- Tolerance/Recovery

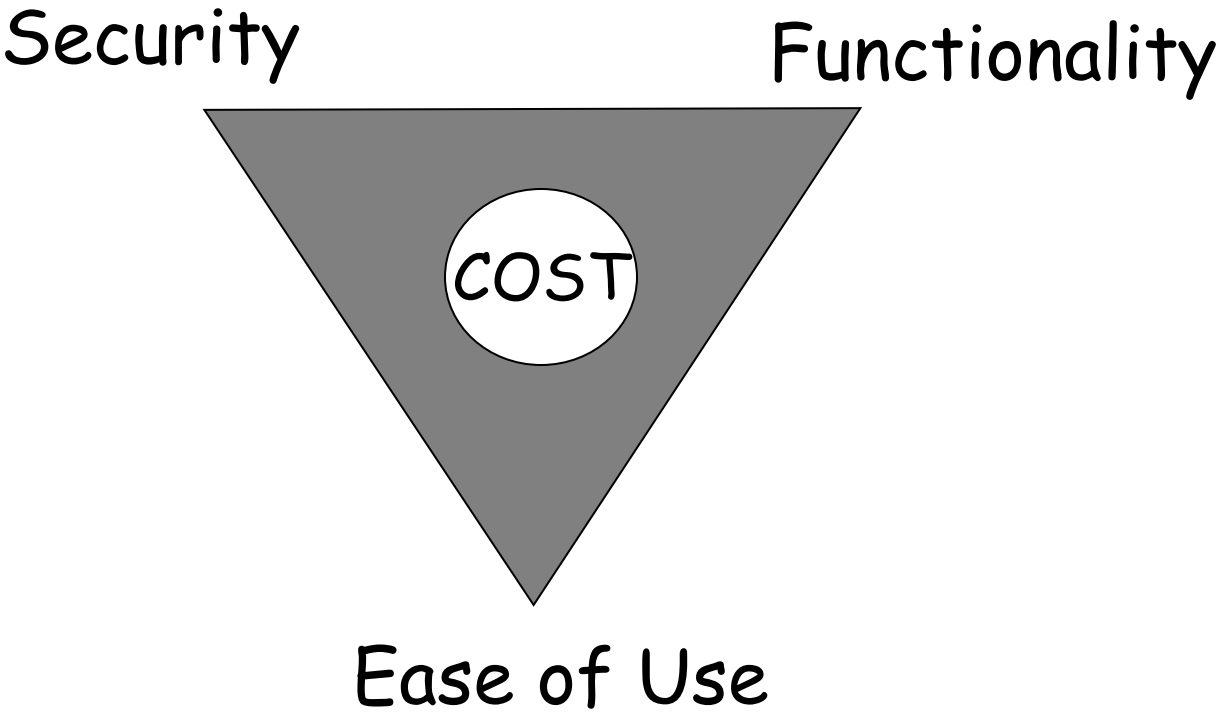
# Security by Obscurity

- Hide inner working of the system
- Bad idea!
  - Vendor independent open standard
  - Widespread computer knowledge

# Security by Legislation

- Instruct users how to behave
- Not good enough!
  - Important
  - Only enhance security
  - Targets only some of the security problems

# Security Tradeoffs



# Threat, Vulnerability, Risk

- **Threat**: potential occurrence that can have an undesired effect on the system
- **Vulnerability**: characteristics of the system that makes is possible for a threat to potentially occur
- **Attack**: action of malicious intruder that exploits vulnerabilities of the system to cause a threat to occur
- **Risk**: measure of the possibility of security breaches and severity of the damage

# Types of Threats (1)

- Errors of users
- Natural/man-made/machine disasters
- Dishonest insider
- Disgruntled insider
- Outsiders

# Types of Threats (2)

- **Disclosure** threat – dissemination of unauthorized information
- **Integrity** threat – incorrect modification of information
- **Denial of service** threat – access to a system resource is blocked

# Types of Attacks (1)

- **Interruption** – an asset is destroyed, unavailable or unusable (*availability*)
- **Interception** – unauthorized party gains access to an asset (*confidentiality*)
- **Modification** – unauthorized party tampers with asset (*integrity*)
- **Fabrication** – unauthorized party inserts counterfeit object into the system (*authenticity*)
- **Denial** – person denies taking an action (*authenticity*)

# Types of Attacks (2)

- **Passive attacks:**
  - Eavesdropping
  - Monitoring
- **Active attacks**:
  - **Masquerade** – one entity pretends to be a different entity
  - **Replay** – passive capture of information and its retransmission
  - **Modification** of messages – legitimate message is altered
  - **Denial of service** – prevents normal use of resources

# Computer Crime

- Any crime that involves computers or aided by the use of computers
- U.S. Federal Bureau of Investigation: reports uniform crime statistics

# Malicious Attacks

- A malicious attacker must have three things to ensure success:
- Method: skills, knowledge, tools, information, etc.
- Opportunity: time and access
- Motive: reason to perform the action

How can defense influence these aspects of attacks?

# Computer Criminals

- **Amateurs**: regular users, who exploit the vulnerabilities of the computer system
  - Motivation: easy access to vulnerable resources
- **Crackers**: attempt to access computing facilities for which they do not have the authorization
  - Motivation: enjoy challenge, curiosity
- **Career criminals**: professionals who understand the computer system and its vulnerabilities
  - Motivation: personal gain (e.g., financial)

# Methods of Defense

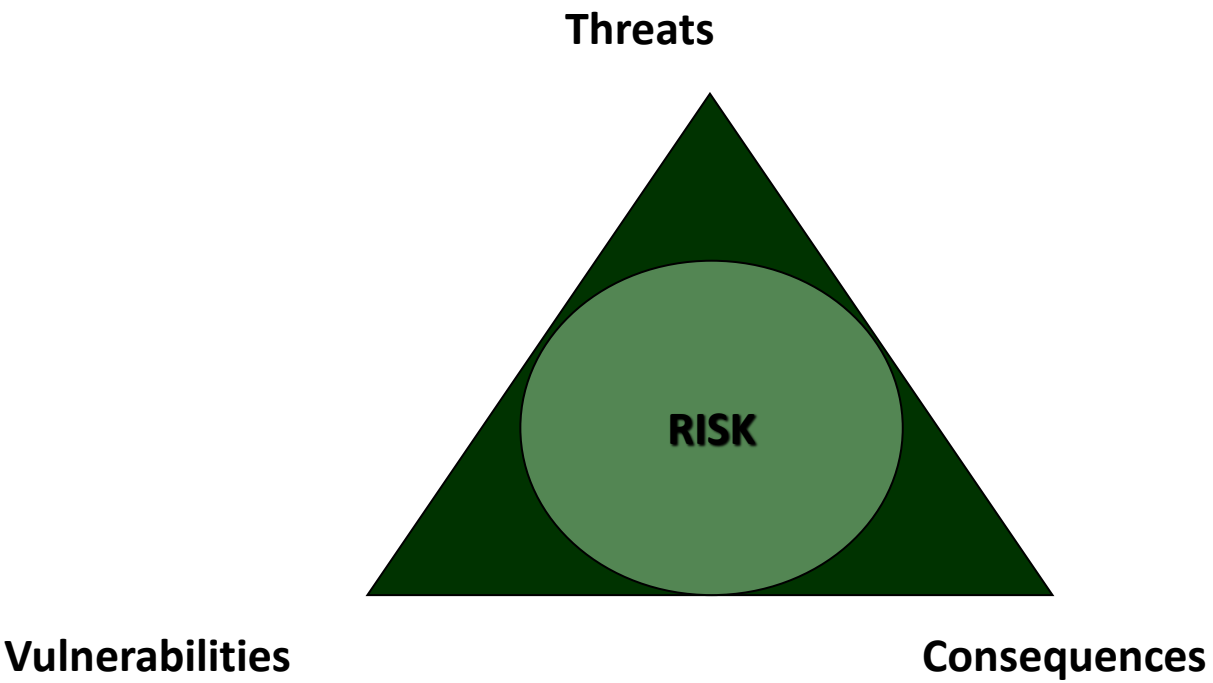
- **Prevent**: block attack
- **Deter**: make the attack harder
- **Deflect**: make other targets more attractive
- **Detect**: identify misuse
- **Tolerate**: function under attack
- **Recover**: restore to correct state

# Information Security Planning

- Organization Analysis
- Risk management
- Mitigation approaches and their costs
- Security policy
- Implementation and testing
- Security training and awareness

# Risk Management

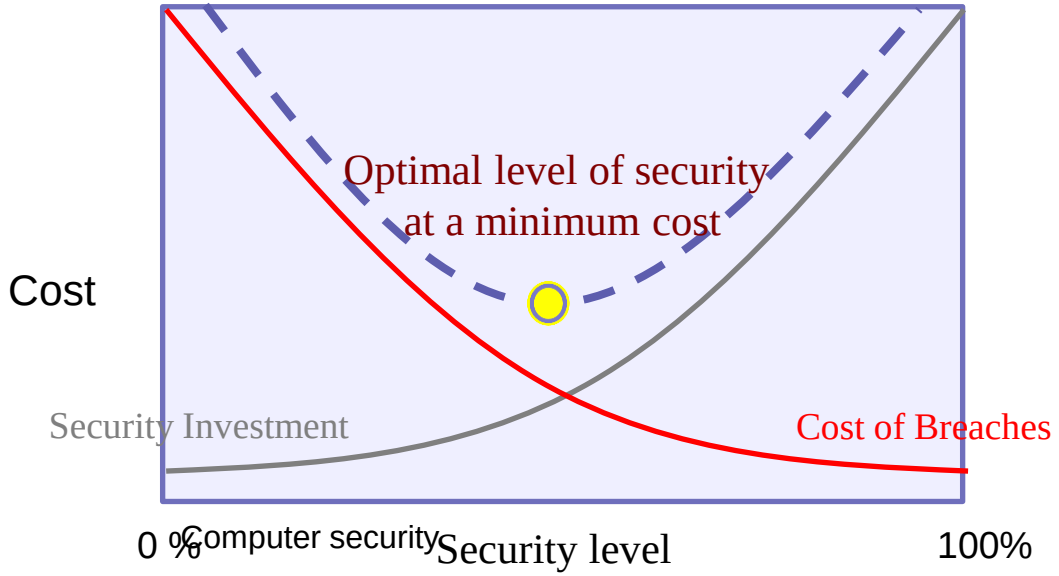
# Risk Assessment



# Risk Assessment

- Business Policy Decision
  - Communication between technical and administrative employees
  - Internal vs. external resources
  - Legal and regulatory requirements

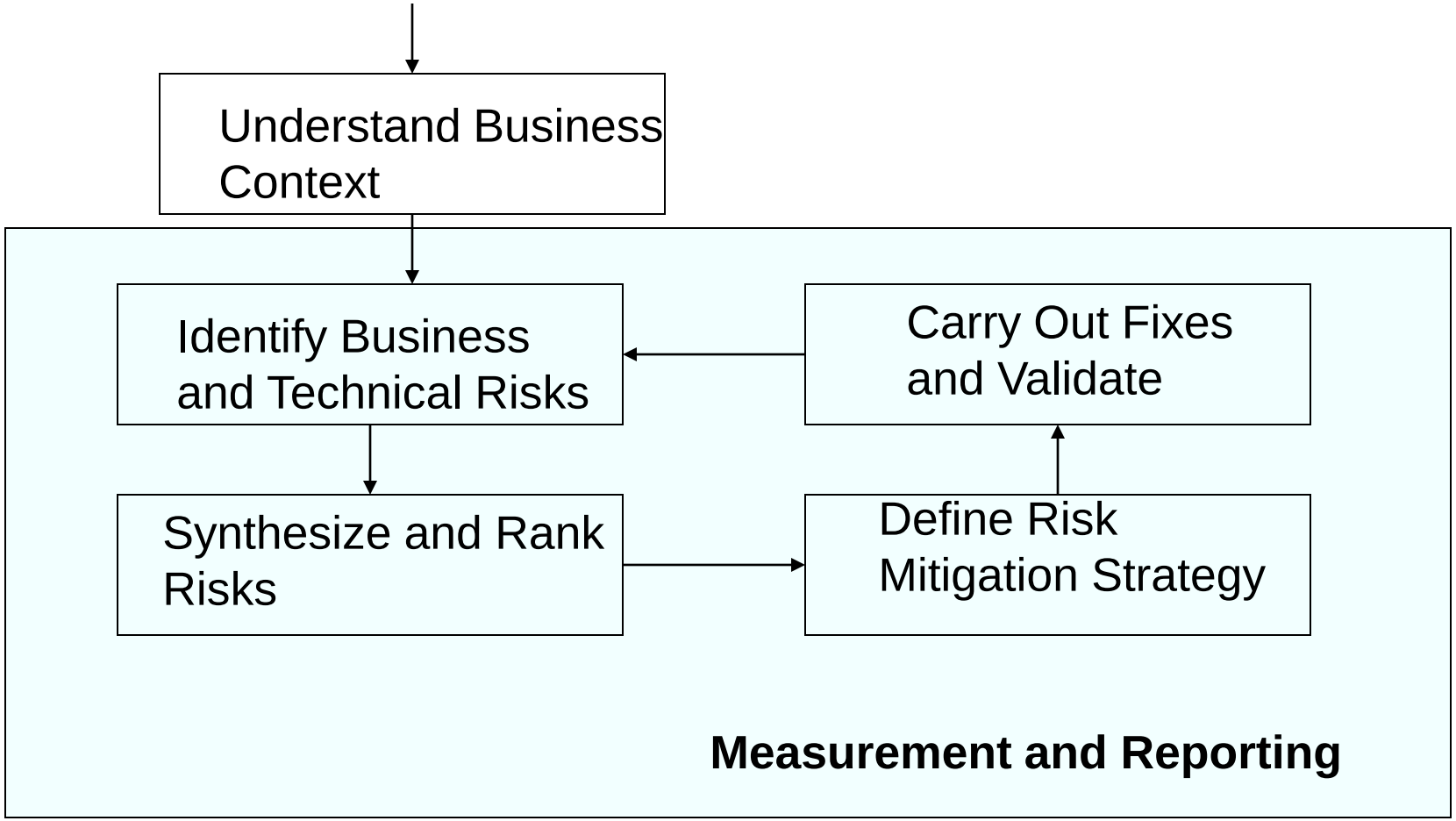
- Developing security capabilities



# Real Cost of Cyber Attack

- Damage of the target may not reflect the real amount of damage
- Services may rely on the attacked service, causing a cascading and escalating damage
- Need: support for decision makers to
  - Evaluate risk and consequences of cyber attacks
  - Support methods to prevent, deter, and mitigate consequences of attacks

# Risk Management Framework (Business Context)



# Next Class

## Cryptography

The science and study of secret writing