Information Security CS3002 (Sections BDS-7A/B, BSE-7A) Lecture 01

Instructor: Dr. Syed Mohammad Irteza

Assistant Professor, Department of Computer Science

19, 20 August, 2024

Administrative Information

- Office: 036, 1st Floor, Block F / New Building

- Email-01: m.irteza@nu.edu.pk
- Email-02: mohammad.irteza@lhr.nu.edu.pk

- Office Hours:
  - Tues/Thursday 11:30 am ~ 12:30 pm

Office Hours

You are welcome to visit and discuss things related to the course, or general academic and/or research interests!

If this slot does not suit you, try to arrange for a separate slot through email, preferably one day before.

Mondays/Wednesdays are less suitable due to a busy schedule.

Administrative Information

- Course Website (Google Classroom):
  - BDS-7A → https://classroom.google.com/c/NzA5NDIzMjIxNTY0
  - Code: 2pxbc6i
  - BDS-7B → https://classroom.google.com/c/NzA0ODg2MjIzNDMx
  - Code: zhbekn3
  - BSE-7A → https://classroom.google.com/c/NzA3MjM5MTcyMDUx
  - Code: yuc5ldq

- Class Schedule:
  - BDS-7A – Mon/Wed (08:30 - 10:00, Venue: NB-308)
  - BDS-7B – Mon/Wed (11:30 - 13:00, Venue: NB-308)
  - BSE-7A – Tue/Thu (08:30 - 10:00, Venue: CS-3)

My Research/Academic Background

- BS, MS and PhD in Computer Science from LUMS
  - 1998-2002, 2004-2005, 2012-2018
- Taught at Air University, LUMS, GIFT University, UMT
- Software Industry Experience: Alachisoft, Prosol Technologies
- PhD Thesis: *Resilient Network Load Balancing for Datacenters*
  - *Advisor – Dr. Ihsan Ayyub Qazi*
- Google Scholar Page:
  - https://scholar.google.com/citations?hl=en&user=wHazKsgAAAAJ
- Main Interests:
  - Datacenter Networking: network layer and transport layer protocols
  - Network Traffic Engineering, Congestion Control, Queue Management

Classroom Etiquette

- Please come on time
- Minimize cross-talk
- Please do not attend phone calls/messages during class
- Do not copy other people’s work
- Try to write notes, this will improve your retention

Course Objectives

This course serves as a comprehensive overview to the field of information security at senior undergraduate level.

At the end of the course, hopefully you will be able to:

1. Explain key concepts of information security such as *design principles, cryptography, risk management, and ethics*
2. Discuss *legal, ethical, and professional issues* in information security
3. Apply various *security and risk management tools* for achieving information security and privacy
4. *Identify appropriate techniques* to tackle and solve problems in the discipline of information security

Course Outline (some changes may happen)

- Course Introduction
- Security Design Principles
- Cryptography (~7 lectures)
- Software Security (~3 lectures)
- Database Security (~2 lectures)
- Web Security (~2 lectures)
- User Authentication
- Access Control

Course Outline (some changes may happen)

- Network Security (~4 lectures)
- Theoretical Models of Access Control
- Cybercrime Laws and Ethics
- Project Evaluations and Revision (~3 lectures)
- Final Exam

Textbook

- Computer Security: Principles and Practice, William Stallings, Lawrie Brown
- Principles of Information Security, Michael E. Whitman, Herbert J. Mattord
- Cryptography and Network Security: Principles and Practice, William Stallings

- Reference:
    - Computer Security Fundamentals (second edition): William Chuck Easttom
    - Hands-on Labs for Security Education, by SEED labs

Grading Policy – Tentative

- Quizzes → 10%
    - Unannounced, can be held at the start or end of class
    - If we have 7 or more quizzes, we will drop the worst two quizzes
- Assignments → 10%
    - All assignments will count to your grade
- Project → 10%
- Midterm I & II → 25% ~ 30%
- Final Exam → 40% ~ 45%
    - Comprehensive exam (all course contents included)

What is Security?

- “*The quality or state of being secure—to be free from danger*”
- A well secured organization should have multiple layers of security in place:
  - Physical Security
  - Personal Security
  - Operations Security
  - Communications Security
  - Network Security

Information Security

- *“The protection of information and its critical elements, including systems and hardware that use, store, and transmit that information”*

- Necessary tools: *policy, awareness, training, education, technology*

- C.I.A. triangle was standard based on confidentiality, integrity, and availability

- C.I.A. triangle now expanded into list of critical characteristics of information

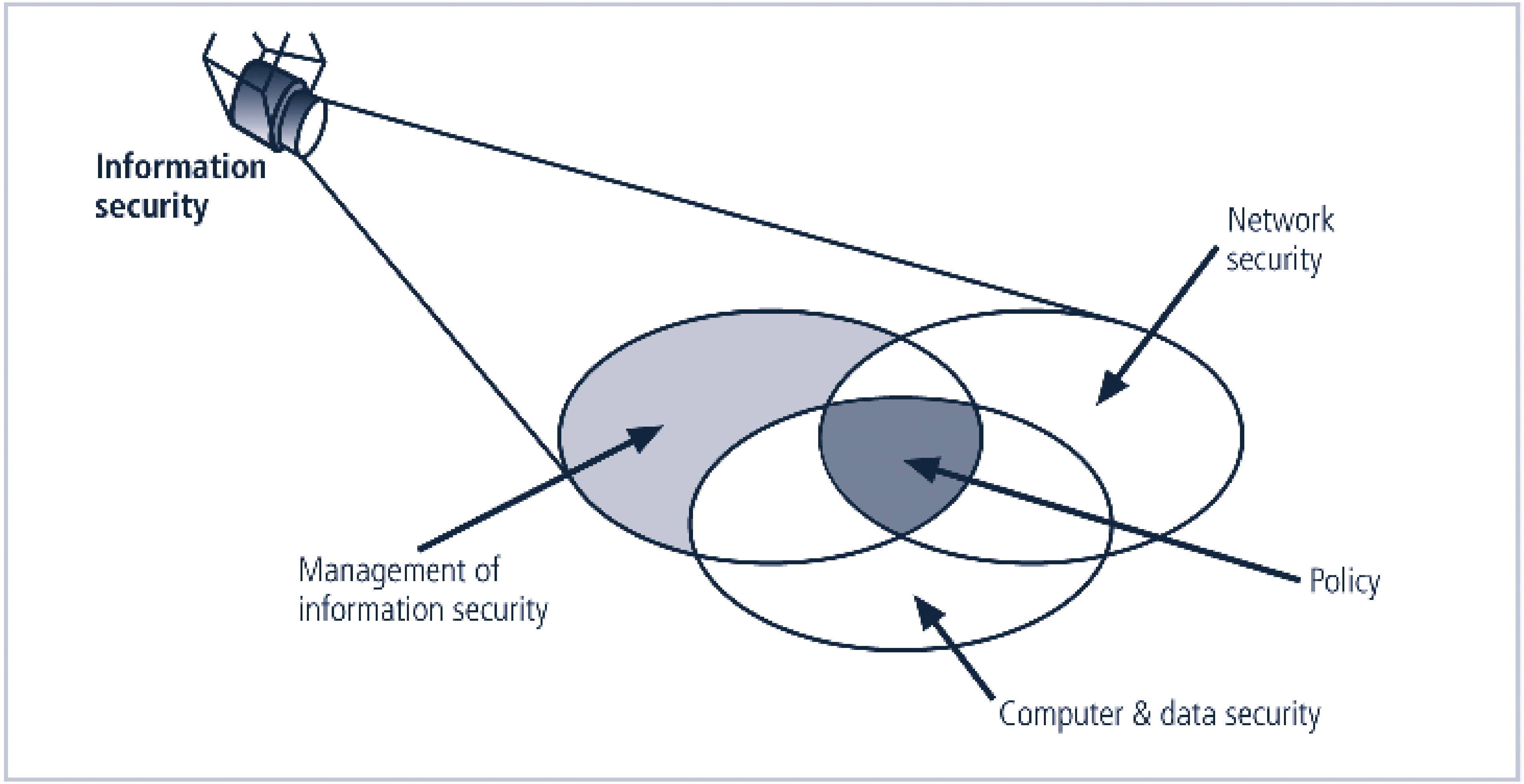


FIGURE 1-3 Components of Information Security

Book: Principles of Information Security

Critical Characteristics of Information

- The value of information comes from the characteristics it possesses:
  - *Timeliness*
    - No value if it is too late
  - *Availability*
    - No interference or obstruction
    - Required format
  - *Accuracy*
    - Free from mistakes
  - *Authenticity*
    - Quality or state of being genuine, i.e., sender of an email

Critical Characteristics of Information

- *Confidentiality*
  - Disclosure or exposure to unauthorized individuals or system is prevented
- *Integrity*
  - Whole, completed, uncorrupted
  - Cornerstone
  - Size of the file, hash values, error-correcting codes, retransmission
- *Possession*
  - Ownership
  - Breach of confidentiality results in the breach of possession

Components of an Information System

- An Information System (IS) is the *entire set of software, hardware, data, people, procedures, and networks* necessary to use information as a resource in the organization
- *Software*
    - Perhaps most difficult to secure
    - Easy target
    - Exploitation substantial portion of attacks on information
- *Hardware*
    - Physical security policies
    - Securing physical location important
    - Laptops
    - Flash memory

Components of an Information System

- *Data*
  - Often most valuable asset
  - Main target of intentional attacks
- *People*
  - Weakest link
  - Social engineering
  - Must be well trained and informed
- *Procedures*
  - Threat to integrity of data
- *Networks*
  - Locks and keys won’t work

Securing Components

- A computer can be the *subject* of an attack and/or the *object* of an attack
  - When it is the *subject* of an attack, the computer is used as an active tool to conduct the attack
  - When it is the *object* of an attack, the computer is the entity being attacked
- Types of attack
  - *Direct*
    - Hacker uses their computer to break into a system
  - *Indirect*
    - System is compromised and used to attack other systems

Risk estimation

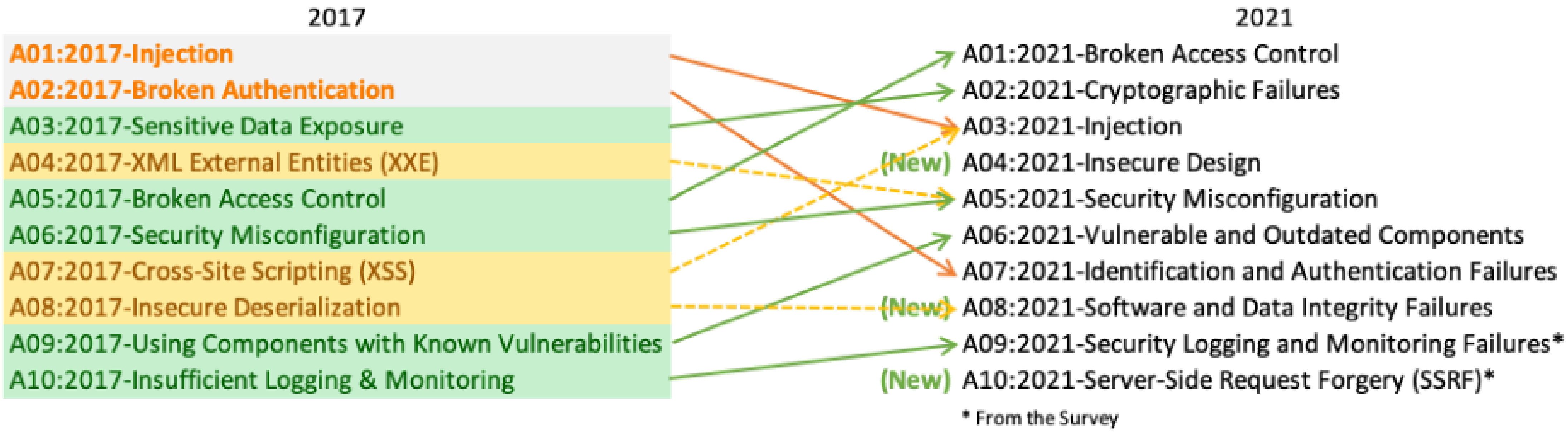
- Assets: Objects, data, people
- Vulnerability: Weakness of an asset
- Threat: loss of security due to vulnerability
- Attack: threat occurrence

- Risk estimation is the process of identifying vulnerabilities and threats and their impact and probability of an attack occurring.

OWASP top 10 Vulnerabilities

Category	IoT Security Consideration	Recommendations
I1: Insecure Web Interface	•Ensure that any web interface coding is written to prevent the use of weak passwords …	When building a web interface consider implementing lessons learned from web application security. Employ a framework that utilizes security …
I2: Insufficient Authentication/Authorization	•Ensure that applications are written to require strong passwords where authentication is needed …	Refer to the OWASP Authentication Cheat Sheet
I3: Insecure Network Services	•Ensure applications that use network services don't respond poorly to buffer overflow, fuzzing …	Try to utilize tested, proven, networking stacks and interfaces that handle exceptions gracefully...
I4: Lack of Transport Encryption	•Ensure all applications are written to make use of encrypted communication between devices…	Utilize encrypted protocols wherever possible to protect all data in transit…
I5: Privacy Concerns	•Ensure only the minimal amount of personal information is collected from consumers …	Data can present unintended privacy concerns when aggregated…
I6: Insecure Cloud Interface	•Ensure all cloud interfaces are reviewed for security vulnerabilities (e.g. API interfaces and cloud-based web interfaces) …	Cloud security presents unique security considerations, as well as countermeasures. Be sure to consult your cloud provider about options for security mechanisms…
I7: Insecure Mobile Interface	•Ensure that any mobile application coding is written to disallows weak passwords …	Mobile interfaces to IoT ecosystems require targeted security. Consult the OWASP Mobile …
I8: Insufficient Security Configurability	•Ensure applications are written to include password security options (e.g. Enabling 20 character passwords or enabling two-factor authentication)…	Security can be a value proposition. Design should take into consideration a sliding scale of security requirements…
I9: Insecure Software/Firmware	•Ensure all applications are written to include update capability and can be updated quickly …	Many IoT deployments are either brownfield and/or have an extremely long deployment cycle...
I10: Poor Physical Security	•Ensure applications are written to utilize a minimal number of physical external ports (e.g. USB ports) on the device…	Plan on having IoT edge devices fall into malicious hands...

OWASP (Current) – Top Ten



2017		2021
A01:2017-Injection		A01:2021-Broken Access Control
A02:2017-Broken Authentication		A02:2021-Cryptographic Failures
A03:2017-Sensitive Data Exposure		A03:2021-Injection
A04:2017-XML External Entities (XXE)	(New)	A04:2021-Insecure Design
A05:2017-Broken Access Control		A05:2021-Security Misconfiguration
A06:2017-Security Misconfiguration		A06:2021-Vulnerable and Outdated Components
A07:2017-Cross-Site Scripting (XSS)		A07:2021-Identification and Authentication Failures
A08:2017-Insecure Deserialization	(New)	A08:2021-Software and Data Integrity Failures
A09:2017-Using Components with Known Vulnerabilities		A09:2021-Security Logging and Monitoring Failures*
A10:2017-Insufficient Logging & Monitoring	(New)	A10:2021-Server-Side Request Forgery (SSRF)*

* From the Survey