

# **CSCI262 : System Security**

## **Introduction**

# Contact Detail

- Dr. Partha Sarathi Roy
- Email: partha@uow.edu.au
- Office: 3.216
- If you email me then please include the subject and topic in the subject line. For example: **CSCI262 : A1**
  - This way I can tell if an email is about almost due assessment or similar important matters.
- **Please use your university account for email.**

# About me

- 2015: PhD in Mathematics, University of Calcutta, India
- 2016-2017: Assistant Professor at Kyushu University, Japan
- 2017-2019: Research Engineer, KDDI Research, Inc. Japan
- 2019-2024: Lecturer, University of Wollongong, Australia
- 2025-Present: Senior Lecturer, University of Wollongong, Australia
- Research Interest: Quantum and Post-quantum Cryptography

# Note

- It is encouraged to attend lectures
  - The textbook doesn't cover all the content, nor will the lecture notes themselves necessarily make sense without listening to explanations.
- Workshop material supplements the lecture material
  - Attending workshops is necessary to completely understand that material. Some solutions may only be available during the workshop.
  - Some of the workshops may require advance preparation.
- The **final exam** will be based on contents from the **lectures** and **workshops**.

# Lecture notes and resources

- The delivery method for lectures will be power point slides.
- These will be released as PDF, prior to the lectures.
- Additional materials will sometimes be made available.
- Material will be on the subjects eLearning site (Moodle Site).

# References

- **Textbook:**

- [SB18] William **Stallings** and Lawrie **Brown**, Computer Security : Principles and Practice, 4th edition, Pearson, 2018

- **References:**

- [B18] Matt Bishop, Computer Security: Art and Science, Addison-Wesley, 2nd Edition, 2018.
- [G06] Dieter Gollmann, Computer Security, Wiley, 2006.
- [A20] Ross Anderson, Security Engineering: A Guide to Building Dependable Distributed Systems, 3rd edition, 2020.

# The elearning site

- Check the eLearning site for this subject regularly!
  - Any change to the subject will be announced on the eLearning site.
  - Any information posted to the eLearning site is deemed to have been notified to all students.
- Check SOLS mail too, since urgent updates are likely to be sent there.

# Assessment: Passing the subject

- There are three assignments, worth 14%, 12% and 14%
  - The assignments generally involve some programming and some other activities:
    - Generally Python, Java, C++ or C will be acceptable.
- The exam is worth 60%

# Technical fail (TF)

- This subject has one requirement to avoid getting a technical failure.
- 24/60 (40%) in the Final Examination.
- If you don't meet this requirement and receive a total subject mark of 50 or higher, you may be given a TF.

# Assignments

- For programming tasks, all your work will need to compile on **Capa** (capa.its.uow.edu.au).
- You need to make sure that your assignments produce the appropriate output on **Capa** in accordance with specified instructions.
  - You must provide a readme.txt file with compilation instructions on Capa.
  - You might get zero for your code if it doesn't compile according to the instructions!
- Assignment submission will be through Moodle.

# Extension

- If you require additional time to complete an assignment you must submit claims for extensions electronically via SOLS, ideally before the DUE date.
- You may be granted an extension if your circumstances warrant it.
- Of course, if you are in hospital for the last week or similar, and cannot get in contact I will understand.
- <http://www.uow.edu.au/students/sols>

# Plagiarism

- The university handbook states: (<https://www.uow.edu.au/student/support-services/learning-development/plagiarism/> )

**“Plagiarism means using the ideas of someone else without giving them proper credit.”**

- It is recommended that you read the website about what is considered plagiarism.
- There are two primary concerns for us:
  - Students copying directly from sources, or copying without appropriate referencing.
  - Students copying each other.
  - You can discuss ideas but need to use your own words!
  - With code and mathematical solutions you need to work fairly independently.

# What is this subject about?

- A subject in computer system security:
- Basic problems and solutions in computer system security.
  - Access control and authentication.
  - User awareness.
- Theory and practice.
- A range of systems/domains are looked at:
  - Database Security.
  - Operating systems.
  - Code security.
  - Network security.
  - Cloud & IoT security.

# What is this subject not about?

- Cryptography:
  - There are some elements of cryptography that will be discussed, but cryptography is mostly in CSCI361.
- Mathematics:
  - There is some mathematics and statistics, but they certainly aren't the primary focus.
- Code syntax:
  - There is a fair amount of content relating to programming but this subject is not about teaching you the syntax of specific languages.

# Basic concepts

- What do we mean by computer security?
- NIST (National Institute of Standards and Technology) – Report NISTIR 7298 (2013)

**Computer Security:** Measures and controls that ensure **confidentiality, integrity, and availability** of information system assets including hardware, software, firmware, and information being processed, stored, and communicated.

- Computer security rests on **confidentiality, integrity and availability**
- **Confidentiality**: Assets should be inaccessible to unauthorised parties.
- **Integrity**: Assets should be unmodifiable or unforgeable, without detection, by unauthorised parties.
- **Availability**: Assets should be available to authorised people.
- These three concepts form what is often referred to as the CIA triad
- In this subject (CSCI262) we mainly look at availability, and how we distinguish between unauthorised and authorised entities.



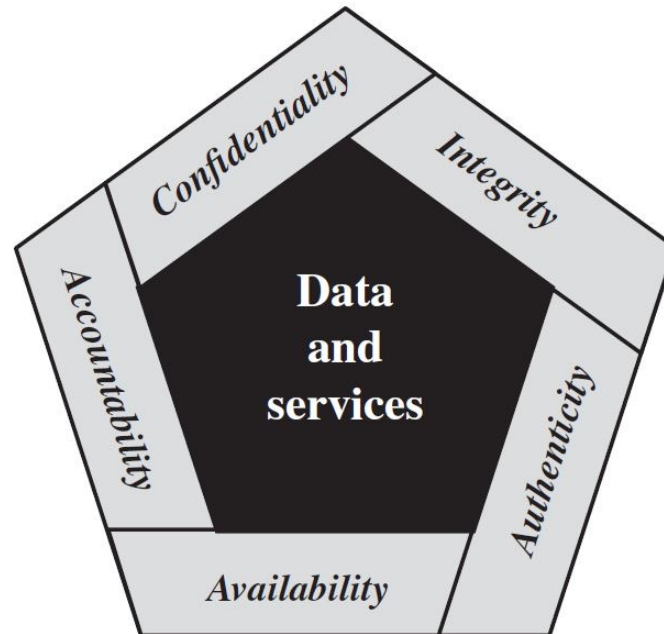
# Authorised versus Unauthorised

- Authorised persons are allowed to do something, unauthorised are not.
- How do we know someone (or something) is authorised?
- Two aspects:
  - Authentication is needed so we (the system) know who the “someone” is.
  - Access control is needed to determine what that identified someone is allowed to do.
- In most contexts we have authentication and access control. You should know a bit about those from CSIT115.

**We can summarise security as the control of access to resources.**

# Additional concepts

- **Authenticity:** verifying that users are who they say they are and that each input arriving at the system came from a trusted source.
- **Accountability:** The security goal that generates the requirement for actions of an entity to be traced uniquely to that entity.



**Figure 1.1** Essential Network and Computer Security Requirements

# Computer system assets

- **Hardware:** Including computer systems and other data processing, data storage, and data communications devices.
- **Software:** Including the operating system, system utilities, and applications.
- **Data:** Including files and databases, as well as security-related data, such as password files.
- **Communication facilities and networks:** Local and wide area network communication links, bridges, routers, and so on.

# Computer security terminology ([SB18])

- **Adversary** (threat agent): Individual, group, organization, or government that conducts or has the intent to conduct detrimental activities.
- **Attack** : Any kind of malicious activity that attempts to collect, disrupt, deny, degrade, or destroy information system resources or the information itself.
- **Countermeasure**: A device or techniques that has as its objective the impairment of the operational effectiveness of undesirable or adversarial activity, or the prevention of espionage, sabotage, theft, or unauthorized access to or use of sensitive information or information systems.
- **Risk**: A measure of the extent to which an entity is threatened by a potential circumstance or event, and typically a function of :
  - 1) the adverse impacts that would arise if the circumstance or event occurs; and 2) the likelihood of occurrence

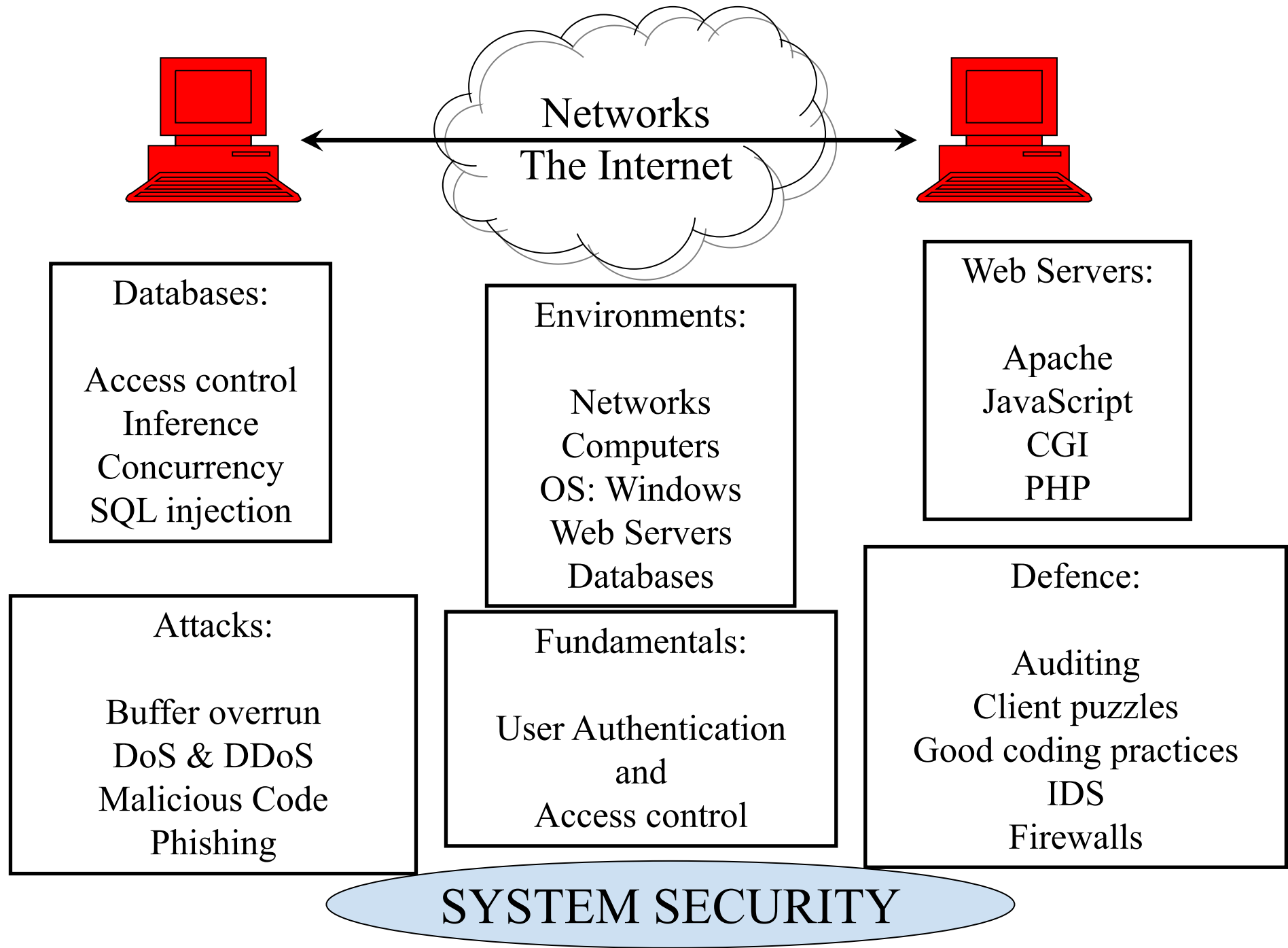
- **Security Policy:** A set of criteria for the provision of security services. It defines and constrains the activities of a data processing facility in order to maintain a condition of security for systems and data.
- **System Resource (Asset):** A major application, general support system, high impact program, physical plant, mission critical system, personnel, equipment, or a logically related group of systems.
- **Threat:** Any circumstance or event with the potential to adversely impact organizational operations (including mission, functions, image, or reputation), organizational assets, individuals, other organizations, or the Nation through an information system via unauthorized access, destruction, disclosure, modification of information, and/or denial of service.
- **Vulnerability:** Weakness in an information system, system security procedures, internal controls, or implementation that could be exploited or triggered by a threat source.

# Goal of security

- **Prevention:** prevent an attack from succeeding
- **Detection:** determine that an attack is under way, or has occurred, and report it.
- **Recovery:** two forms
  - Stop an attack and to assess and repair any damage caused by that attack
  - The system continues to function correctly while an attack is under way.

# Network exploitation

- One of the most expensive computer crimes is **denial of service**.
  - This attack usually involves distributed systems and remote access.
- **Viruses, worms and trojans** are the most common form of electronic attacks.
  - They are prevalent because of networking.
- Problems such as **spam** and **phishing** rely on the massive interconnectedness that exists.
- We will look at most of these in this subject.



# Tentative lecture schedule

- Introduction, basic concepts
- User authentication
- OS security
- Buffer Overflow
- Access control: basic concepts and security model
- Database security
- Malware
- Audit, IDS
- Firewall, IPS
- Side-Channel Attacks