CSCI361
Computer Security
(Cryptography and secure applications)

Subject introduction

Lecturer & Subject Coordinator

Professor Willy Susilo

School of Computing and Information Technology

Email: wsusilo@uow.edu.au

Tutor: Mr. Japit Sionggo

What is this subject about?

- We cover a wide range of topics in computer security.
  - We will put computer security into perspective later in this lecture.
- From understanding cryptographic algorithms …

  … through security programming (assignments) …

  … to applying cryptography to real-world applications.
- It is assumed that you can program:
  - In either Java or C/C++.
  - If you cannot, *you will need to learn!*
  - A significant proportion of the assignment assessment is for programming, either in C/C++/Java or using Number Theory Package.

The objectives of this subject.

- This is what we hope you will be able to do by the end of subject:
  - Understand fundamental cryptographic principles, including the types of cryptography and their properties.
  - Understand some basic building blocks of computer security (encryption, authentication, hashing …).
  - Understand and know some of the algorithms used to provide examples of those building blocks.
  - Identify security problems in computer systems.
  - Understand how to apply security algorithms to real-world applications.

Approximate Contents

- Introduction.
- Classical cryptology, Secret key cryptography.
- Modern secret key cryptography, block ciphers.
- Modern stream ciphers, AES.
- Message integrity, Public key cryptography (Knapsacks, RSA).
- Public key cryptography. Digital signatures.
- Digital signatures, hashing.
- Secret Sharing Schemes

Assessment

- 2 Assignments.
  - Programming may be required in all assignments, although the entire assignment need not be all programming.
- One written test.
- The final exam.

Resources

- References:
  - ***Cryptography Engineering.* Niels Ferguson, Bruce Scheiner and Tadayoshi Kohno, Wiley, 2010.**
  - *Cryptography and Network Security: Principles and Practices*. William Stallings. 4rd edition. Prentice Hall, 2005.
  - Cryptography: Theory and Practice. D. Stinson. 3nd edition. CRC Press, 2005.
  - *Fundamentals of Computer Security*. J. Pieprzyk, T. Hardjono and J Seberry, Springer-Verlag, 2003

CSCI361 – Introduction
Computer Security

What, why and who?

Outline

- We are basically going to address three questions.

- **What** do we mean by (computer) security?
  - Threats, attacks and vulnerabilities.
  - Distributed systems.
  - Design principles.
- **Why** does computer security matter?
- **Who** needs computer security?

Computer security: What is it?

- Briefly at this stage:
- Computer security is about protecting computer based *assets* against possible *threats*.
  - Primarily we are interested in protecting information from *attack*.

Why does computer security matter?

- Computer security matters because people do actually attack computer systems, for various reasons.
  - For money.
  - To obtain knowledge or intellectual property.
  - Industrial sabotage.
  - For fun.
  - Because they can …

Eugene Spafford:

> “*Using encryption on the Internet is the equivalent of arranging an armored car to deliver credit-card information from someone living in a cardboard box to someone living on a park bench.*”

Who needs computer security?

- Governments:
  - To safeguard military or diplomatic communications and to protect national interests.
- Private sector:
  - To protect sensitive information such as health and legal records, financial transactions, credit ratings.
  - To protect information ownership.
- Individuals:
  - To protect sensitive information, and to protect an individual's privacy in the electronic world.
  - Allow E-commerce, internet banking and so on.

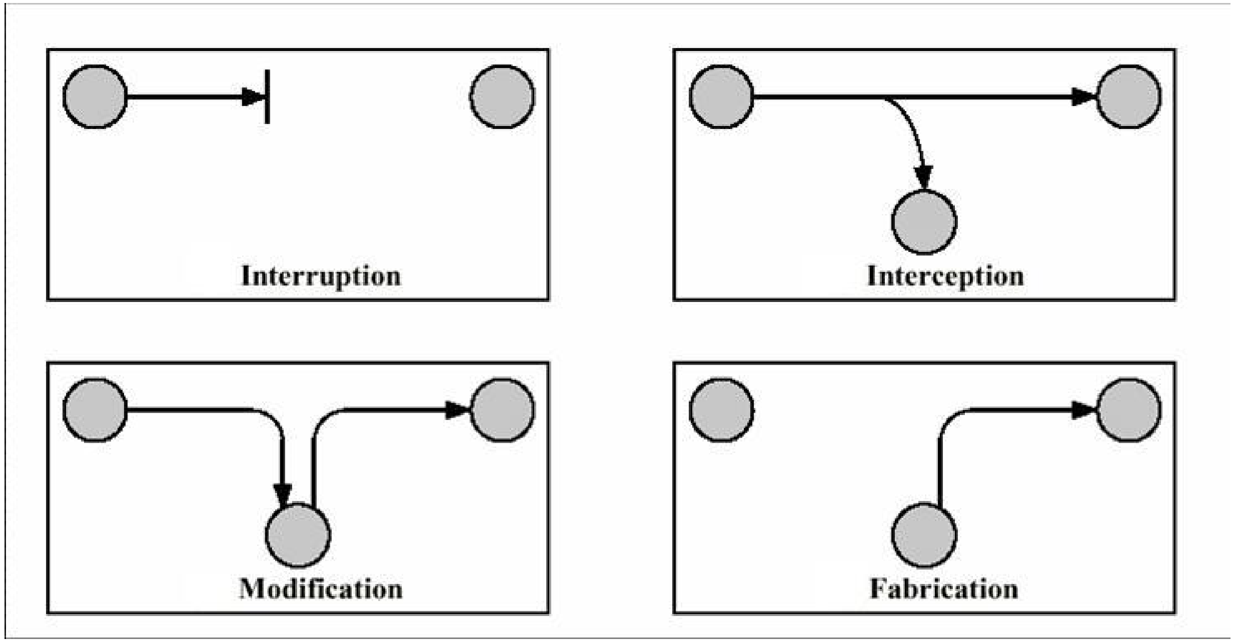
What do we mean by security?

- Security is about protecting *assets* against possible *threats*.
  - In particular we are concerned with computer security, but primarily in the sense of *information security*.
- **Assets** are anything we possess of value or use to us.
  - A computer system consists of **hardware**, **software** and **data**, each of which is an asset.
- A **threat** is something which potentially violates security. It exists when there is a circumstance, capability, action or event that could breach security and cause harm. In other words, a threat is a possible danger that might exploit a vulnerability.

- We need to be able to identify
  - Assets.
  - Threats.
  - Possible controls.

  … and estimate the cost and resulting benefits of implementing the controls.
- We would also like to be able to identify when **attacks** occur.
  - We use the term **attack** to mean a deliberate attempt to evade security services and violate the security policy of a system.
- Damage to assets can be intentional or accidental.
  - We will be mainly concerned with intentional damages, i.e. where people undertake attacks.

The four basic attack types



- Interruption: an attack on availability of an asset.
  - Hardware destruction, software erasure.
- Interception: an attack on confidentiality.
  - Wiretapping network, illegal copying of files.
- Modification: an attack on integrity.
  - Of database data or transmitted communications.
- Fabrication: an attack on authenticity.
  - Pretending to be someone else.

Asset vulnerabilities

- Hardware is vulnerable to such accidental damage as coffee, dust or power surges, although neither may be accidental.
- Hardware is vulnerable to deliberate damage such as theft or tampering.

- Software/Data may be damaged due to accidental media damage, for example, accidentally dropping a cup of coffee on a CD. Or someone accidentally deleting some files.
- It can also suffer from deliberate attacks which modify the purpose or content of the software/data.

- Damage can be:
  - **Easily detectable:** For example the software crashes when it is run or data is easily observed as being corrupted. Effectively this provides a denial of service.
  - **Not easily detectable:** For example, the replaced data looks realistic or software runs correctly but has an additional hidden purpose. Detection may only be possible through side effects, if at all.

Damage to software/data

- Deletion (interruption): Erasing a file, or copying it.
- Modification:
  - *Software modification* may cause a program to crash immediately, or at a certain time (logic bomb), or it can make program do what it is not supposed to do. For example. modifying access rights while copying.
  - *Data modification* can take many forms. Replaying used data, fabrications of messages etc.
- Software interception: Stealing software (including piracy).
- Data interception: Breaching confidentiality of data by wiretapping or monitoring electromagnetic radiation.

Distributed systems

- New distributed systems have added problems:
  - Laptops, handheld devices and mobile phones can be easily lost.
  - Hardware security cannot be relied on.
  - Communication between different parts of the system exposes the data. It also provides many more attack points for intruders to attack data and other resources.
- Sharing resources and access control is a much more complex problem that for single point systems.

Controls

- Hardware controls:
  - Devices for user identification,
  - Hardware implementation of encryption.
  - Chip sets with embedded security functionality,
  - Trusted systems (Microsoft Palladium/NGSCB).
- Software controls:
  - Standards for coding, testing and maintaining, to ensure software correctness.
  - Operating system controls on accessing data and programs.
  - Internal controls, for example, data base management systems access control.
- Cryptography is a powerful tool in providing security. It can add security to an “insecure” system.

Control policies

- The protection we can provide varies depending on the situation. Primarily we are interested in using **policy** or **protocol-based security** centred around cryptography.
- **Policies** are working procedures adopted by organisations to improve asset security.
  - Requiring frequent password changes.
- **Protocols** are agreed upon rules or standards enabling connection and interaction between parties.
  - They can specify data formats.
  - Rules of exchange, who does what when?
  - Specify termination or error rules or handling conditions.
- In this course we are only concerned with security of software and data, primarily data (information).
  - The first half of the course will be spent looking at cryptography.

Goals of security (CIA)

- ***C****onfidentiality*: Assets should be inaccessible to unauthorised parties.
- ***I****ntegrity*: Assets should be unmodifiable or unforgeable, without detection, by unauthorised parties.
- ***A****vailability (****A****uthenticity)*: Assets should be available to authorised people.

- There is a cost in achieving those goals, and one needs to balance this cost against what you can gain.

Security Principles: Construction and analysis

- Principle of **easiest penetration**:
  - Intruders will use any available means of penetration. This makes security assessment of security a very difficult problem because *all possible ways* of breaching security must be examined.
- Principle of **adequate protection**:
  - Also known as the *timeliness principle,* this means items should only be protected while they are valuable, and that the level of protection should be consistent with their value. This is a very practical principle which underlies a large proportion of modern computer security.
- Principle of **effectiveness**:
  - Controls must be used properly to be effective.
  - Controls should be efficient, easy to use and appropriate.
- Principle of the **weakest link**:
  - Security is only as strong as the weakest link in the system.

Other questions…

- We also want to think about **when** to use cryptography?
- … and **which** cryptography to use in a given situation?