Security (CS4028)

Lecture 1b. Introduction to Security

Chunyan Mu

chunyan.mu@abdn.ac.uk

The School of Natural and Computing Sciences

Schedule

	Week	Lecture 1	Lecture 2	Tutorial
⇒	1	Intro to course & security	Intro to Crypto	-
	2	Symmetric Crypto	Hash	Math for crypto
	3	Asymmetric Crypto-1	Asymmetric Crypto-2	Symmetric Crypto
	4	Signatures	Zero Knowledge Proof	Asymmetric Crypto
	5	Certificates	Authentication	Signature & certificates
	6	Access Control	AC models	Authentication
	7	Information flow control	Information flow control	Access control
	8	Security management	Protocols	Concepts & management
	9	Network security	Network security	Protocols and communications
	10	Advanced Topic	Advanced Topic	Network
	11	Revision		

Outline

Outline

Information security

Your interpretation of information security?

Information security

Your interpretation of information security?

- the process of preventing and detecting unauthorised use of your information
- the science of guarding information systems and assets against malicious behaviours of intelligent adversaries.
- Security vs. reliability (e.g. car safety)
  - Intentional vs. accidental fault/failure
  - Baddies in security are arbitrary smart

Information security

Malicious behaviours can include

- Fraud: deceiving sb to get money, goods or service
- Theft: stealing sth from a person or a place
- Terrorism: causing damage, disruption and intimidation
- Vandalism: damaging or destroying sth, deliberately and for no good reason
- Espionage: stealing info or (commercial) secrets by a spy
- Sabotage: causing damage/destruction to gain advantage

Crypto/security: application examples

Home and business

- mobile phones, tablets
- DVD player, pay-TV decoders,
- game consoles,
- prepayment electricity meters,
- Internet (SSL, S/MIME, PGP, SSH),
- software license numbers,
- door access cards, car door locks, burglar alarms, etc.

Crypto/security: application examples

Banking

- ATM (automatic teller machines)
  - the 1^{st} large scale commercial use of crypto
- card authentication codes,
- PIN verification protocols,
- funds transfers,
- online banking,
- electronic purses,
- digital cash, cryptocurrencies

Crypto/security: application examples

Military

- Identify friend/foe system,
- low probability of intercept and jamming resistant radios and radars,
- weapon-system unlock codes,
- permissive action links for nuclear warheads,
- navigation signals,
- GPS

Security violations

Types of violations

- In 1973, James Anderson identified three different types of security violation in computer systems:
  - unauthorised information release;
  - unauthorised information modification;
  - unauthorised denial of use.
- What we mean by "authorised" or "unauthorised"?
  - this is defined by the security policy.

Security violations

Types of violations

- In 1973, James Anderson identified three different types of security violation in computer systems:
  - unauthorised information release;
  - unauthorised information modification;
  - unauthorised denial of use.
- What we mean by "authorised" or "unauthorised"?
  - this is defined by the security policy.

Why it happens?

- inadequate physical controls;
- inadequate controls within the computer system.

Security violations

Example: unauthorised information release

- An unauthorised user reads and copies encrypted passwords from a password file.
- Then he/she may be able to decrypt passwords offline using brute force (thereby by passing methods to prevent on-line password cracking).

Security violations

Example: unauthorised information modification

An unauthorised user changes the password file:

- might then insert a new entry in the password file (a "backdoor") and subsequently be authenticated by the system;
- might simply change the root password.

Security goals

Goals for computer security: CIA

- Confidentiality - prevention of unauthorised information release (info is accessible only to authorised user);
- Integrity - prevention of unauthorised information modification;
- Availability - authorised users should not be prevented from accessing to info and associated assets when required;

Security goals

Confidentiality (privacy or secrecy)

- Confidentiality is about preventing unauthorised users reading information to which they are not entitled.
- Traditionally, the notions of security and confidentiality are often confused, e.g.
  - In a military environment, security was traditionally associated with keeping information secret, e.g. by using ciphers to protect communicated information.

Variants of confidentiality

- anonymity, copy protection, information flow control, unlinkability, unobservabability, ...

Security goals

Integrity: no unauthorised user can manipulate data

- In the context of computing: preventing unauthorised users writing information to which they are not entitled.
- In a general context: ensuring that the system state has not been modified by those not authorised to do so.
- In the context of data communication: detection of modifications to transmitted data.

Security goals

Availability

- Availability can be defined as ensuring that the services provided by a system are accessible on demand by an authorised entity.
- Availability covers areas beyond the normal scope of security, e.g., fault-tolerant computing.
- For the purposes of security we are primarily concerned with preventing denial of service attacks by unauthorised entities.
  - e.g., internet 'flooding' attacks, where the attacker(s) overwhelm a server by sending it large numbers of connection requests.

Security goals

Additional security goals

- Authentication
  - the process of verifying an identity claimed by or for a system entity
  - example potential authentication protocol: Kerberos protocol
- Access control (Authorisation)
  - protection of system resources against unauthorised access
  - example: ACL
- Non-repudiation
  - protection against false denial of involvement in a communication

Vulnerability

Vulnerability

- A vulnerability is a flaw in the design or implementation of a computer system that could lead to a security violation.
- Examples include:
  - program bugs;
  - configuration errors;
  - poor choice of passwords;
  - flawed management of passwords.
- A vulnerability represents a threat to the security of a system.

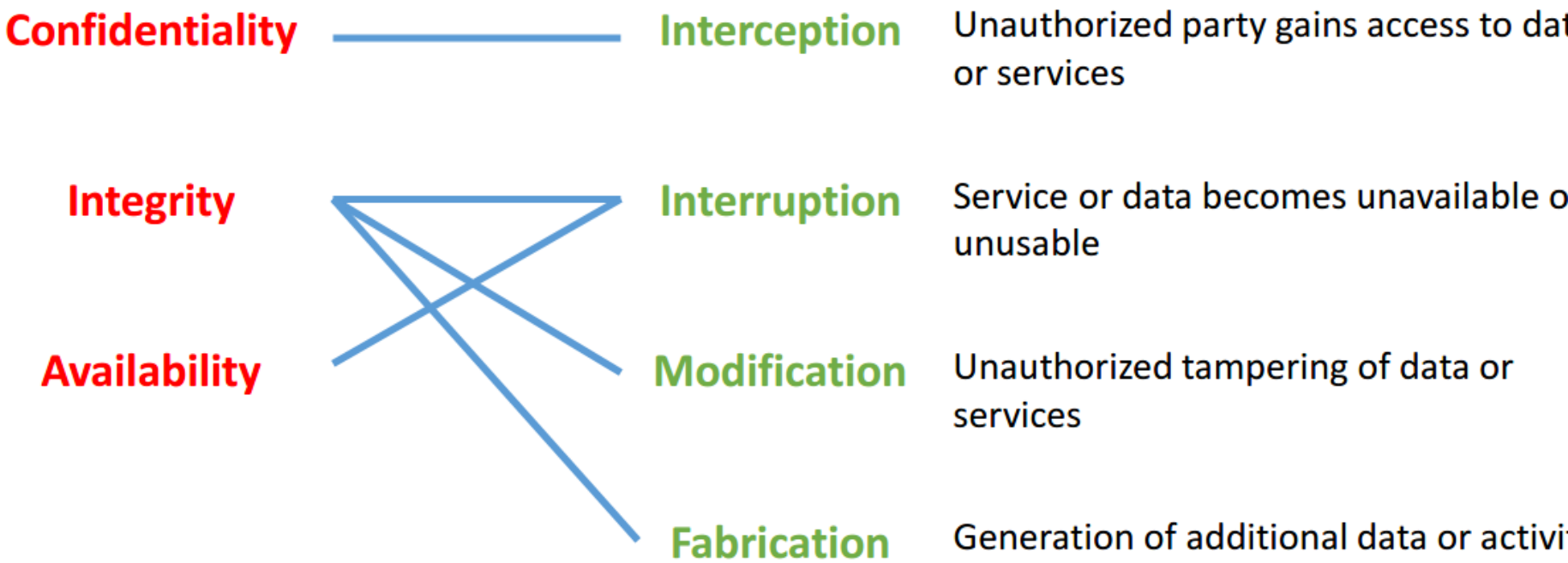
Information security analysis

Key elements

- Assets: what we want to protect
  - Hardware, Software, Data, Users
  - Some are easily replaceable, other not.
- Vulnerability: a weakness that could be exploited to cause harm.
- Threat: a set of circumstances that could cause harm.
- An attack is performed exploiting a vulnerability of the system.
- Countermeasure: action, device, procedure, or technique that remove or reduce a vulnerability.

Information security analysis

Security threats



Information security analysis

Example: Confidentiality

- Asset: E-mail message
- Vulnerability: E-mail is not a letter but rather a post card
- Threat: Everyone can read it along the way! (interception)
- Countermeasures:
  - protect the communication (network security)
  - protect the message content (encryption)

Information security analysis

Example: Integrity

- Asset: financial records (bank transfer)
- Vulnerability:
  - a defective software component allows unauthorized insider users to read and write records from the database
- Threat:
  - the payment amount can be changed (**Modification)**
  - **an unauthorized payment can be generated (Fabrication)**
- Countermeasures:
  - protect the integrity of the records (digital signature)
  - protect the access to the system (access control)

Information security analysis

Example: Availability

- Asset: online store (Communication with a server)
- Vulnerability:
  - there is no limit to the number of parallel transactions a user can begin
- Threat:
  - denial of service (Interruption)
- Countermeasures:
  - Authenticate the user and do not allow beginning a new transaction unless the previous one is terminated or aborted (secure software engineering)
  - Limit the number of incoming connections from the same network address (network security)

Outline

How to do/practice security

Security: intuitive strategies

- Prevention: take measures that prevent your assets from being damaged
  - E-commerce as example: encrypt your orders, rely on the merchant to perform checks on the caller, don't use internet (? ¨‿)...
- Detection: take measures so that you can detect when, how and by whom an asset has been damaged.
  - an unauthorised transaction appears on your credit card statement!
- Reaction: take measures so that you can recover your assets or to recover from a damage to your assets.
  - complain, ask for a new card number, etc.

Risk and threat analysis

Risk assessment

The challenge for the IT and Operations managers in this type of environment is to:

- properly analyse the threats to and vulnerabilities of an information system,
- identify the potential impact that the loss of information or capabilities of a system would have on the business, and, based upon these analyses,
- identify appropriate and cost-effective counter-measures.

Risk and threat analysis

Risk assessment

There are a number of ways of judging the security features of a computer system:

- can the operating system and hardware implement memory protection?
- is it possible to identify authorised users?
- is it possible to define and enforce a discretionary security policy?
- is it possible to define and enforce a mandatory security policy?
- is it possible to store and protect audit information?
- can it be proved that the system meets the above requirements?

Information protection: 3 steps

A method for tackling an information protection problem

1. Drawing up a threat model via security requirement analysis
2. Formulating a suitable security policy modelling what ought to be protected
3. Implementing specific protection mechanisms to enforce the policy

Information protection: 3 steps

1. Drawing up a threat model via security requirement analysis
   - Identify assets to be protected and their value
   - Identify vulnerabilities, threats and risk priorities
   - Identify legal and contractual requirements

Information protection: 3 steps

2. Formulating a suitable security policy
   - which activities are or are not authorised, which states are or are not required, and which information flows are or are not prohibited
   - precise and even formal definition of such protection goals; can be procedural instructions for employees
   - should be well documented and followed

Information protection: 3 steps

3. Implementing specific protection mechanisms to enforce the policy

e.g.,

- Hardware protection mechanisms
- Secure operating systems
- Secure coding
- Capabilities and access control lists
- End user security training
- Response to breaches

Outline

Summary

This lecture: information security concepts

- Course information
- Security concepts
- Security attacks, goals, vulnerabilities, existing security systems
- Security strategy development: 3 steps

Next lecture

- Introduction to cryptography