6G7Z1009: Introduction to Computer Forensics and Security

Overview of Security

Contact detail

Prof. Liangxiu Han (Weeks 7 to 12)

Room: E138A, Email: l.han@mmu.ac.uk,

Phone: 0161 247 1225

Office hours: Monday 10:00 am - 11:00 pm

Wednesday 10:00 am - 12:00 pm

Course overview

- The first half term (6 weeks) mainly focuses on computer forensics:
  - Forensic Process (10%): Types of investigations, role of investigator, processes, and legal aspects.
  - File System Analysis (30%): Data acquisition, volume analysis, write blockers, signatures, file systems artefacts, locating and restoring deleted content.
  - Recent Developments and Advances in Digital Forensics (10%): topics such as mobile forensics, memory forensics and forensic data mining.

Course overview

- The second half term (6 weeks) mainly focuses on security:
  - Overview of security (10%): The need for security; types of security ; Threats; Security mechanisms and security services.
  - Introduction to Cryptography (20%) : Attacks on conventional and public key cryptography; Integrity (Hash functions and message authentication codes).
  - Access control (20%): Goals of protocols (Authentication and Authorisation; Key distribution and confirmation); Fiat-Shamir protocol; PKI; Digital certificates; Mediated authentication (Needham-Schroeder protocol); Access control lists and capabilities; Multilevel Security; Multilateral Security; Covert channels; Kerberos.

Grading

- Assignment 50% (25% for forensics and 25% for security)
- Final exam 50%

Acknowledgement and Reading List

- W. Stallings, Cryptography and Network Security: Principles and Practice (7th Edition), 2016, Pearson
- Nigel P. Smart, Cryptography Made Simple (Information Security and Cryptography), 2015, Springer
- M. Stamp, Information Security. Principles and Practice (2nd Edition), 2011, John Wiley.
- D. Gollmann, Computer Security, 3rd Edition, 2011, John Wiley
- Alexander Stanoyevitch, Introduction to Cryptography with Mathematical Foundations and Computer Implementations, 2010, CRC Press.
- J. Erickson, Hacking: The Art of Exploitation (2nd Edition), 2008
- Online resources:
  - The Critical Security Controls, www.sans.org/critical-security-controls/, [Online access 11 Sep. 2017].
  - Security controls, en.wikipedia.org/wiki/Security_controls, [Online 10 September 2017].

The purpose of this course

- This introductory course is in relation to information and network security
- It covers a diverse set of topics related to information and network security (e.g. cryptographic methods, security protocols)
- Recap and build a solid foundation for advanced security

Basic concepts

- Data
  - Recording of "something" measured
  - Raw material, just measured
- Information
  - The result of processing, manipulating and organising data in a way that adds to the knowledge of the receiver
  - Processed data

Basic concepts

- Knowledge
  - Processed by means of structuring, grouping, filtering, organising or pattern recognition
  - Highly structured information
- Information system
  - An integrated set of components for collecting, storing, processing, and communicating information.
  - Business firms, other organisations, and individuals in contemporary society rely on information systems to manage their operations, compete in the marketplace, supply services, and augment personal lives.

Information Security

- Information Security
  - The process of protecting information from unauthorised access, use, disclosure, destruction, modification, or disruption
  - The protection of computer systems and information from harm, theft, and unauthorised use.
  - Protecting the confidentiality, integrity and availability of information
  - Information security is an essential infrastructure technology to achieve successful information-based society
  - Highly information-based company without information security will lose competitiveness

Information Security

In a word,

- Information Security is defined as methods and technologies for deterrence (scaring away hackers), protection, detection, response, recovery and extended functionalities (e.g. while information in transmission over networks, storage, hardware, etc.)

- Information must be protected at various levels
  - The operating systems
  - The network
  - The data management system
  - Physical protection is also important

What Functions Should a Security Policy and System Provide?

- Deterrence: need to create and implement policies that allow the generation of a feasible and believable deterrence
- Detection: need to create and implement policies and procedures that allow the detection of how, when and where intrusion has taken place
- Protection: need to create and implement policies and procedures that allow the management of people and the IS in an effective manner so as to protect against unauthorised usage

What Functions Should a Security Policy and System Provide?

- Reaction
  - need to create and implement policies and procedures which define how to react to an intrusion
  - need to ensure that penetration does not happen again
  - need to ensure that vulnerabilities are eliminated

What Functions Should a Security Policy and System Provide?

- Recovery
  - need to create and implement policies and procedures to recover all data and programs after a breach in security

Aspects of security

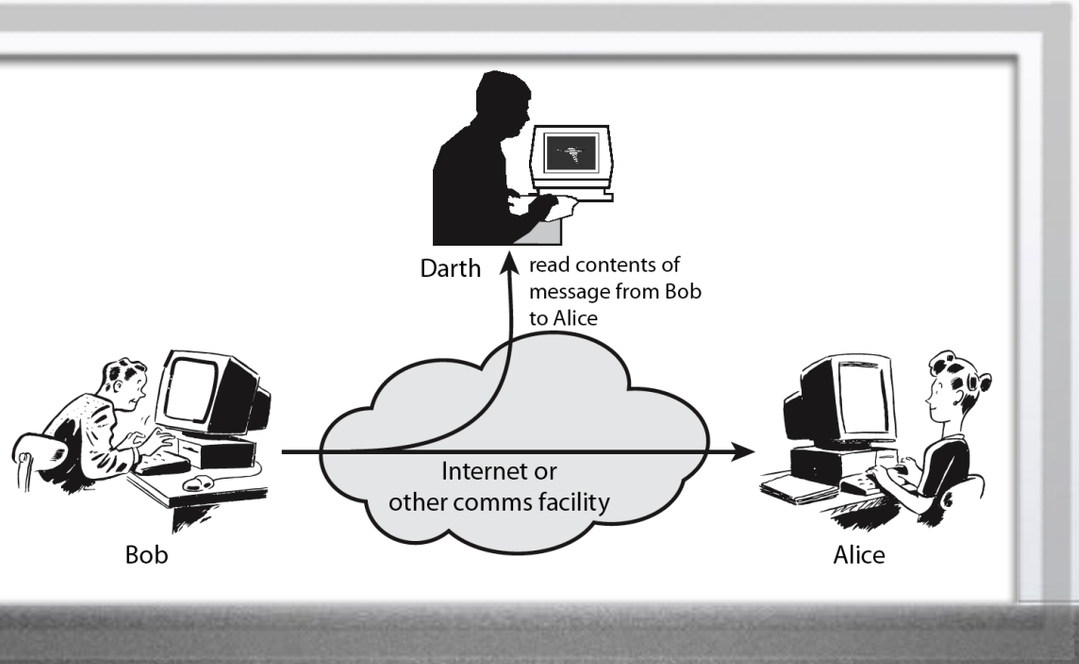
- Security attacks
- Security threats
- Security mechanism
- Security services

Security attacks

- Any action that compromises the security of information owned by an organisation
- Information security is about how to prevent attacks, or failing that, to detect attacks on information-based systems
- Often threat & attack used to mean same thing
- Have a wide range of attacks
- Two types of attacks
  - passive
  - active

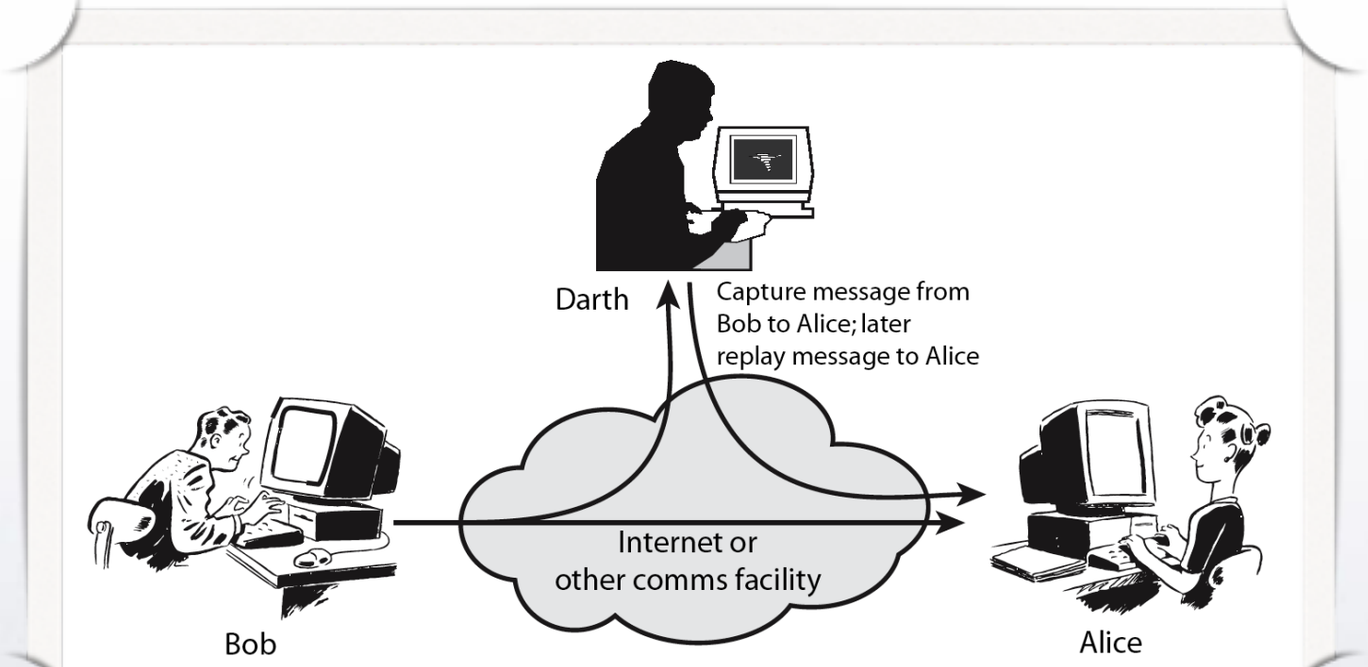
Security attacks

- Passive attack: a passive attack attempts to learn or make use of information from the system but does not affect system resources.
    - Release of message contents: we want to prevent an opponent from learning the contents of exchanged messages
    - Traffic Analysis: the opponent could determine the location and identity of communicating hosts and could observe the frequency and length of messages being exchanged.



Security attacks

- Active attack: An active attack attempts to alter system resources or affect their operation



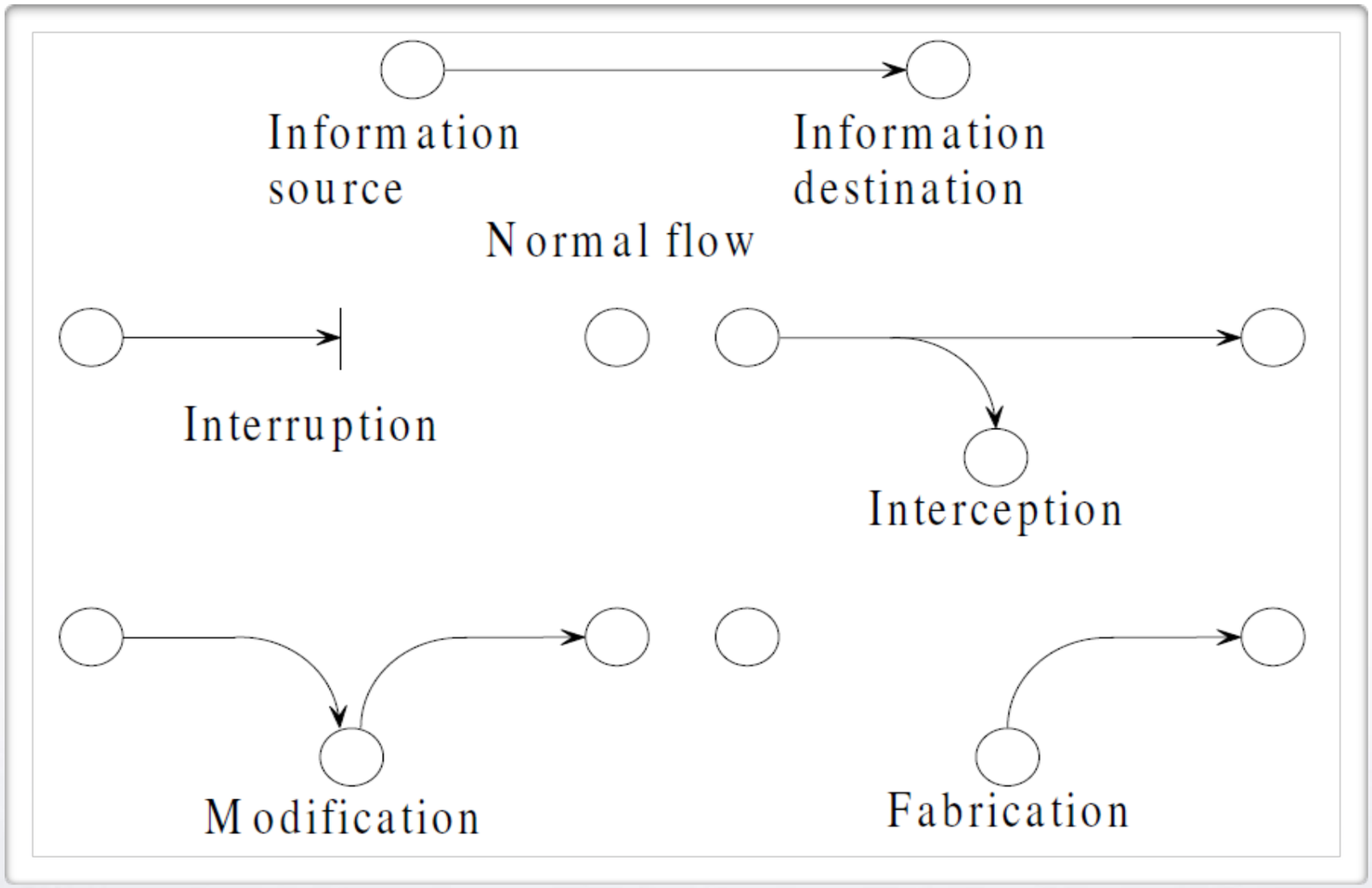
Security attacks

- Masquerade: takes place when one entity pretends to be a different entity.
- Replay: capture message from B to A; latter replay message to A
- Modification of message contents: some portion of the legitimate message is altered or the message is delayed or recorded to produce an unauthorised effect.
- Denial of Service: prevents or inhibits the normal use or management of communications facilities.

Security threats

- Interruption/Denial of service
- Interception: eavesdropping, wiretapping, theft …
- Modification
- Fabrication/Forgery
- Unauthorised access
- Denial of facts

Security threats



Security-mechanisms

A mechanism designed to detect, prevent, or recover from a security attack:

- Encryption
- Authentication
- Digital signature
- Key exchange
- Access control
- Monitoring & Responding

Security services

- Basic security services (CIA)
  - Confidentiality: prevention of unauthorised disclosure of information (To keep a message secret to those that are not authorised to read it).
    - Privacy: protection of personal data.
    - Secrecy: protection of data belonging to an organisation.
    - Potential implementation: A very key component of protecting information confidentiality would be encryption. Encryption ensures that only the right people (people who knows the key) can read the information. A very prominent example will be SSL/TLS, a security protocol for communications over the internet that has been used in conjunction with a large number of internet protocols to ensure security.

Security services

- Basic security services
    - Integrity: prevention of unauthorised modification of information (To make sure that a message has not been changed while on transfer, storage, etc.).
        - potential implementation: Commonly used methods to protect data integrity includes hashing the data you receive and comparing it with the hash of the original message. However, this means that the hash of the original data must be provided to you in a secure fashion. More convenient methods would be to use existing schemes such as GPG to digitally sign the data.
    - Availability: Prevention of unauthorised with-holding of information or resources (to make sure that the services

Security services

- Basic security services
    - Availability: Prevention of unauthorised with-holding of information or resources (to make sure that the services are available to users. some common attacks could cause lack of availability)
        - to ensure data availability, Backup is key. Regularly doing off-site backups can limit the damage caused by damage to hard drives or natural disasters. For information services that is highly critical, redundancy might be appropriate. Having a off-site location ready to restore services in case anything happens to your primary data centers will heavily reduce the downtime in case of anything happens.

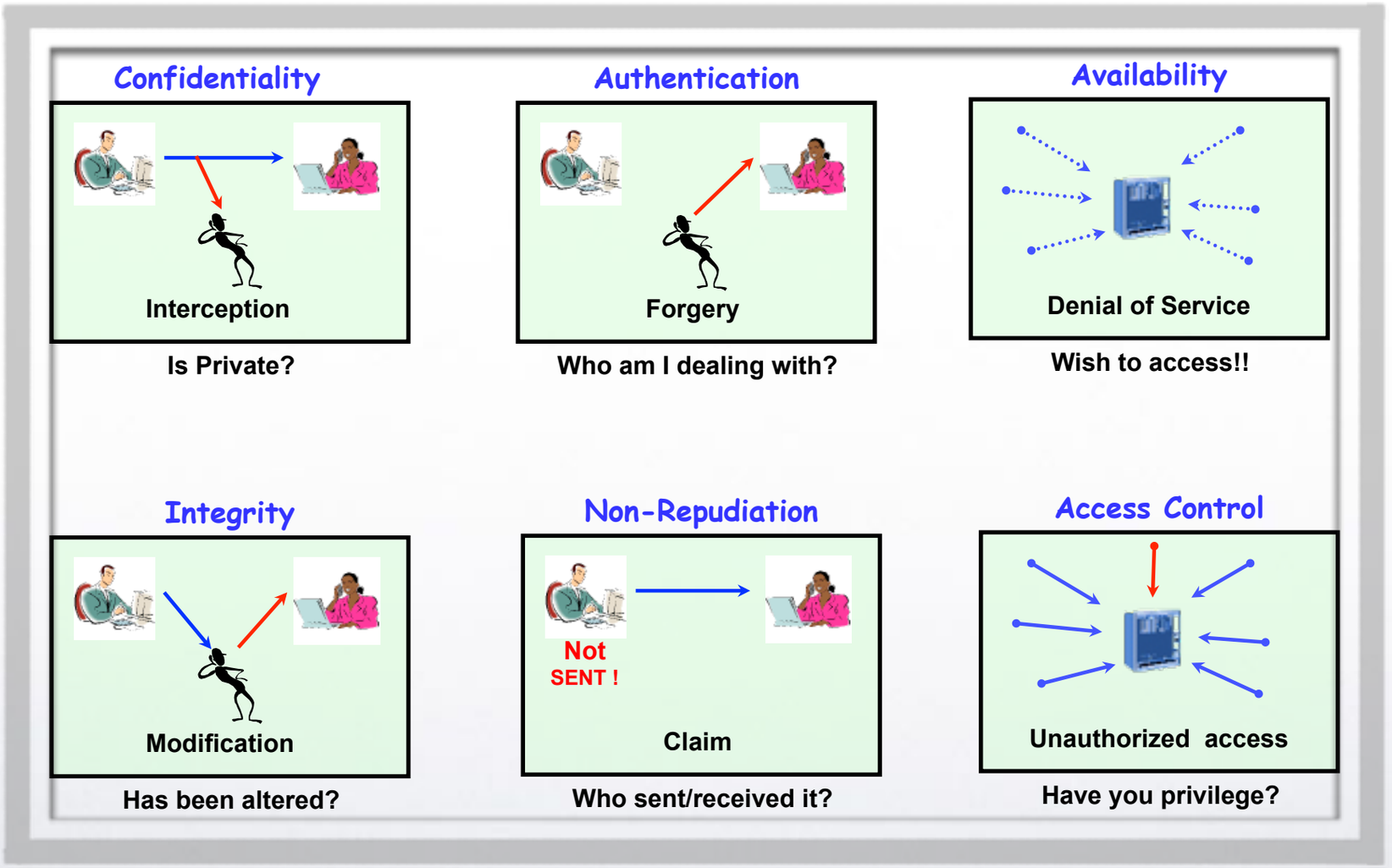
Security services

- Additional security services
  - Authentication: the process of verifying an identity claimed by or for a system entity (To verify the identity of the user / computer). Potential authentication protocol examples such as kerberos authentication protocol
  - Access control: protection of system resources against unauthorised access (To be able to tell who can do what with which resource). Examples of access control such as ACL

Security services

- Additional security services
  - Non-repudiation service: a security service that provides protection against false denial of involvement in a communication (To make sure that a user/server can't deny later having participated in a transaction)

Security needs



Source: http://www.slideserve.com/nhi/introduction-to-information-security-lecture-1-introduction-overview

Security controls

- Safeguards or countermeasures to avoid, counteract or minimise security risks relating to personal property, or computer software
- They can be classified in two different ways
  - according to the time that they act, relative to a security incident
  - according to their nature, for example:

Security controls

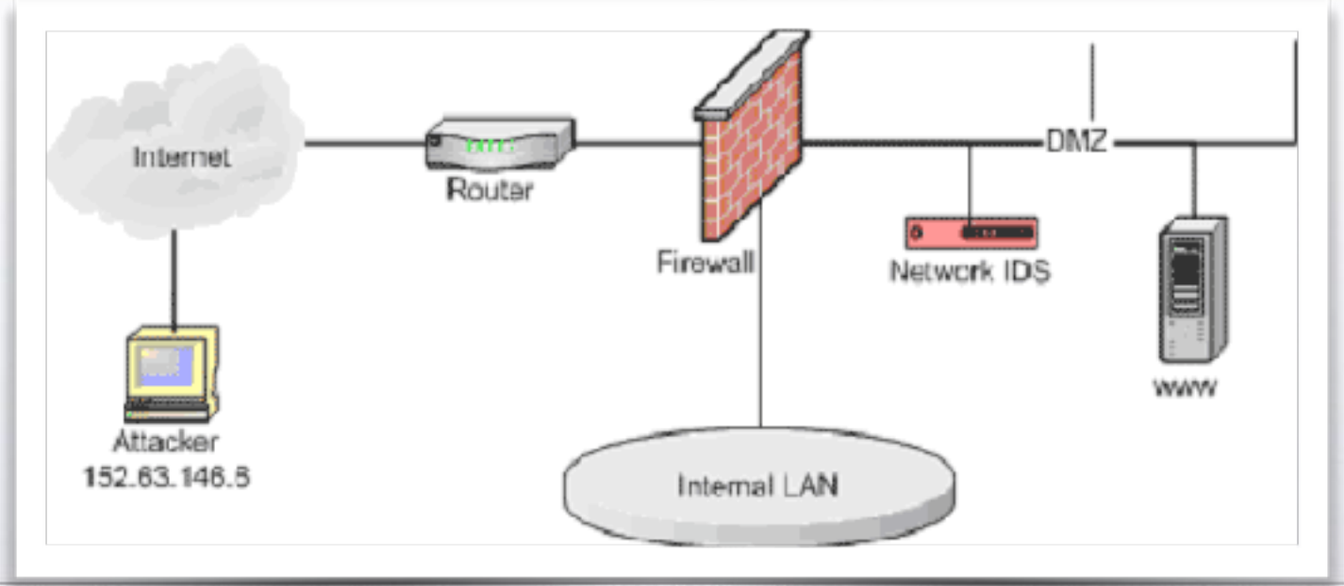
- Classification according to the time that they act, relative to a security incident
    - Before the event, preventive controls are intended to prevent an incident from occurring e.g. by locking out unauthorised intruders;
    - During the event, detective controls are intended to identify and characterise an incident in progress e.g. by sounding the intruder alarm and alerting the security guards or police;
    - After the event, corrective controls are intended to limit the extent of any damage caused by the incident e.g. by recovering the organisation to normal working status as efficiently as possible.

Security controls

- Classification according to the nature, for example
  - Physical controls e.g. fences, doors, locks and fire extinguishers;
  - Procedural controls e.g. incident response processes, management oversight, security awareness and training;
  - Technical controls e.g. user authentication (login) and logical access controls, antivirus software, firewalls;
  - Legal and regulatory or compliance controls e.g. privacy laws, policies and clauses.

Existing security systems/protocols

- Firewalls to prevent malicious packets from entering
- Software based: Runs as a local program to protect one computer (personal firewall) or as a program on a separate computer (network firewall) to protect the network
- Hardware based separate devices that protect the entire network (network firewalls)



Existing security systems/protocols

- Intrusion detection systems to detect intrusions and take action
- Host-based IDS Installed on a server or other computers (sometimes all). Monitors traffic to and from that particular computer
- Network-based IDS Located behind the firewall and monitors all network traffic

Existing security systems/protocols

- Network Address Translation (NAT) Systems to hide the IP address of network devices
- Located just behind the firewall. NAT device uses an alias IP address in place of the sending machine's real one "You cannot attack what you can't see"

Existing security systems/protocols

- Proxy Server: Operates similar to NAT, but also examines packets to look for malicious content. Replaces the protected computer's IP address with the proxy server's address
- Protected computers never have a direct connection outside the networkThe proxy server intercepts requests. Acts "on behalf of" the requesting client

Existing security systems/protocols

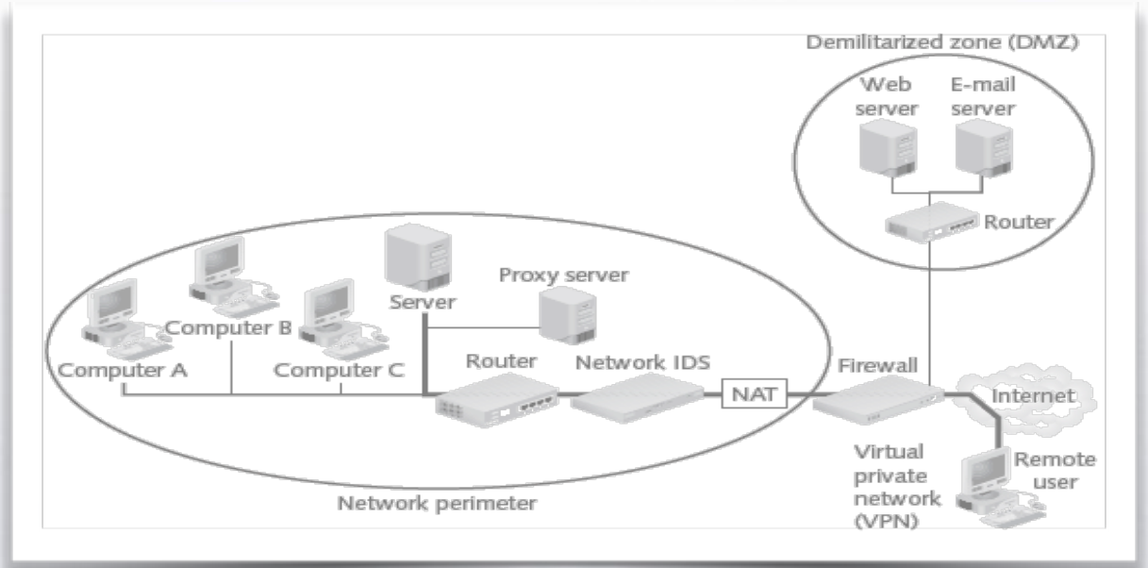
- Demilitarized Zones (DMZ): Another network that sits outside the secure network perimeter. Outside users can access the DMZ, but not the secure network
- Some DMZs use two firewalls. This prevents outside users from even accessing the internal firewall. Provides an additional layer of security

Existing security systems/protocols

- Virtual Private Networks (VPNs): A secure network connection over a public network.
- Sets up a unique connection called a tunnel

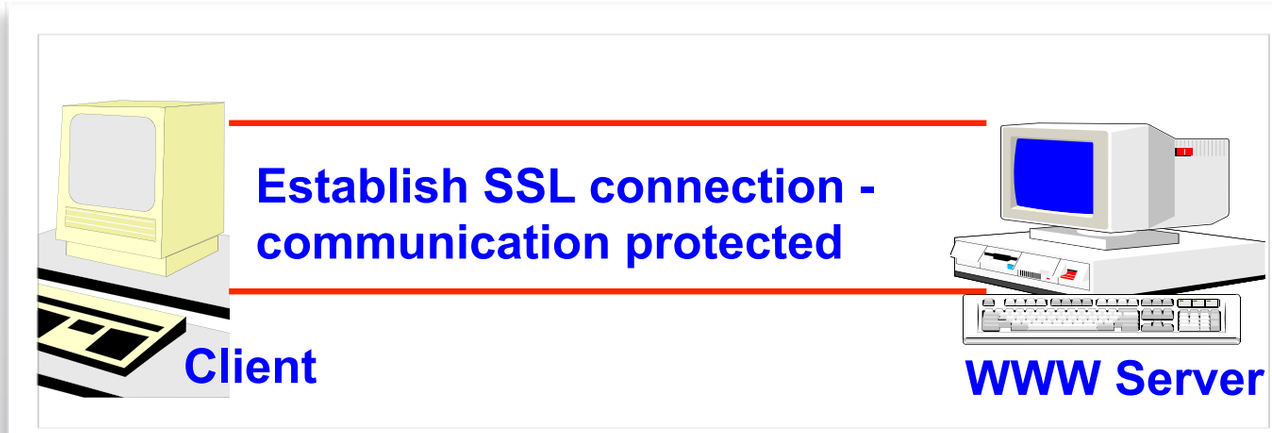
Existing security systems/protocols

- Honeypots: Computer located in a DMZ and loaded with files and software that appear to be authentic, but are actually imitations
- Intentionally configured with security holes
- Goals: Direct attacker's attention away from real targets; Examine the techniques used by hackers



Existing security systems/protocols

- SSL is used for securing communication between clients and servers. It provides mainly confidentiality, integrity and authentication



Summary

- Course information
- Overview of security:
  - Basic concepts
  - Aspects of security
  - Security controls, needs and existing systems/protocols