**Week1**

**Explain the following terms in one sentence each: confidentiality, privacy, integrity, availability and authenticity of information.**

Confidentiality

Restricts read access/only authorized individuals can view

Privacy:

Only authorized entities can disclose legally obtained data to secondary users

Integrity

Only authorized entities (humans or computer programs) can modify some data content

Availability

Authorized users can access information

Authenticity

The source of a document, identity of a person, is as claimed.

**What is security by obscurity and what is security via legislation?**

Obscurity

Hide internal working, sensitive components

Legislation

Law prescribe allowable user activities

**What is a covert channel? Explain it on a simple example.**

I) Channel not intended for transfer of information

II) May be very slow.

III) Often created by misusing over channels

E.G.

Timing channel

Storage channel

Data Hiding in OSI model

**What is the difference between a security policy and a security mechanism?**

Security policy

Describe the aim

Security mechanism

Implement the policies

**Week 2**

**Explain the following security terms: vulnerability, exploit, attack, threat, threat agent**

Vulnerability

A weakness in the application

Exploit

Technique that allows the attacker to take advantage of vulnerabilities

**Attack**

Use of an exploit

**Threat**

The potential of a harmful event

**Threat agent**

Capabilities + Intentions + Past Activities

**What is CVSS? What are the metric groups used in CVSS? What are the metrics in each group?**

Base metric group

Exploitability

Access vector (e.g. local or remote) and access complexity

Impact

None, partial or complete loss of

Temporal metric group

Exploitability

Theoretical, proof of concept exists, functional (works for most situations), high (always works)

Remediation (补救)

Official/temporary fix, workaround, not available

Environmental metric group

Collateral damage potential (附带损伤可能)

Target distribution

Number of systems vulnerable in a particular environment

**Explain the following malware types: virus, worm, Trojan horse, logic bomb, Easter egg**

Virus

needs a host to spread (e.g. via infected emails, data,…)

Worm

Spreads on its own

Trojan horse

Code doing what it is supposed to do, plus something else

Trapdoor

Access to services by non-standard methods

Logic bomb

Dormant malicious code, waiting for a triggering event

Easter egg

"Cute" but harmless behavior triggered by special input

**Explain the following attack types: dictionary attack, replay attack, password sniffing, spoofing, denial of service.**

**Dictionary**

Dictionary attack

Testing correct words (e.g. From a dictionary)

Replay attack

Using data from an earlier, recorded, valid session

Password guessing

Relies on intuition

Password sniffing

Having access to and monitoring a valid session

Spoofing

Masquerading as someone else by falsifying data

denial of service

Overwhelming the target with bogus requests and making it inaccessible for legitimate users

**Explain the following terms: injection attack, rootkit, social engineering.**

Injection attacks

Exploiting the input vulnerability of data not being checked or sanitized properly

Rootkits

Malware that hides its presence via modifying system data

Social engineering

Exploiting human gullibility to extract confidential information

**What are the main steps when responding to an incident?**

Detection

Includes identification of the attack

Containment

Prevention from causing damage and from spreading (quaranteen)

Eradication

Remove the agent

Recovery

Restore the normal operation What is the aim of DOS attacks? Explain the main DDOS attacks types.

**What is the aim of DOS attacks? Explain the main DDOS attacks types.**

To let website down

Volume based attacks

Method: bandwidth saturation

Protocol attacks

Method: server resource attack

Application layer attacks

Method: crash the application

**Week 3**

**What is a security mechanism? What are its main tasks? What types of mechanisms are used in computing? Give an example of each.**

Implement security services

Deal with:

prevention of incidents

detection of incidents

recovery from incidents

Pervasive mechanisms

Protect against a number of threats

network firewalls

Protect individual computers or whole networks

virus checking programs (email filters)

Specific mechanisms

Protect against a specific threat

E.g. data integrity protection

Protect an individual data or a piece of hardware

E.g. controlling access to individual data items

**What is the difference between pervasive and specific security mechanisms? Give an example for each.**

Pervasive:

More economical, less accurate

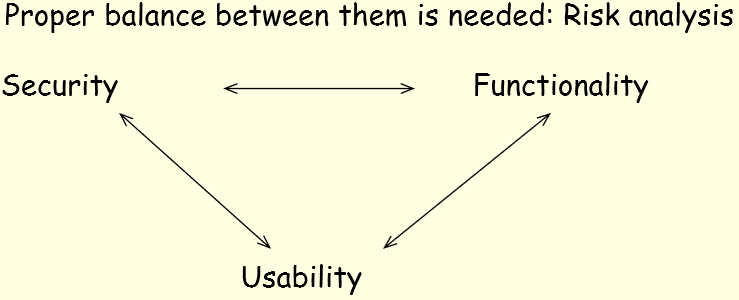
Specific

More accurate, less economical

**What are the security trade-offs?**

Security features may restrict functionality

Security mechanisms may complicate user interaction



**How can you measure risk?**

Risk = asset value \* accident probability

Value of assets

Replacement value (equipment, software)

Potential damage (loss of data, privacy)

Probability of an accident

Identify potential accidents

Assess their frequency

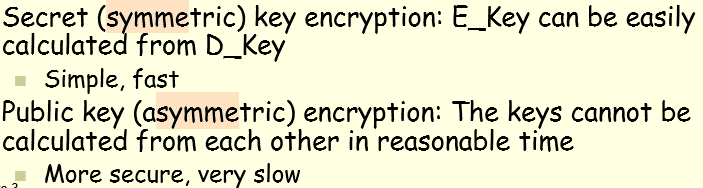
**What is encryption? What is the role of an encryption key?**

processing a message so that its meaning becomes obscured

Encryption key

Parameter that enables to translate the same plaintext with the same algorithm to different ciphertexts

**What is the basic difference between symmetric key encryption and asymmetric key encryption?**



**Compare symmetric and asymmetric key encryption (keys, security, complexity, speed)**

**What is a stream cipher and what is a block cipher?**

Stream cipher:

The transformation depends only on the actual symbol, does not consider the previous or next symbol(s)

Block ciphers

Transforms a group of data (a block) at a time

**Explain each of the following methods: describe their characteristics and most important features. AES, RSA, Diffie-Hellman.**

**Advanced Encryption Standard (AES)**

A version of the Rijndael block cipher

RSA

encryption and digital signatures

Diffie-Hellman

Protocol for establishing a shared secret via an insecure communication channel

**Explain cipher block chaining and electronic code book (ECB) encryption.**

**CBC**

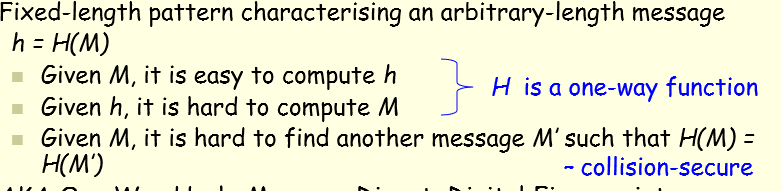
**Electronic code book (ECB)**

A plaintext always encrypts to the same ciphertext A “code book” can be built for each key (and any plaintext-ciphertext combination can be entered into this book)

**CBC**

The plaintext is XOR-ed with the previous ciphertext block and then encrypted

**What is a hash (or secure digest) function and what are its main features?**



Digital signatures, protecting messages from alteration

**What is a digital signature used for? How is it produced?**

A recipient of a document can verify that the claimed originator is the real originator, and the message has not subsequently been altered.

**Week 4**

**What is the difference between identification and authentication?**

Identification:

Establish the identity of

A user

A communicating peer

A process

Authentication:

Verifying that the user is who they claim to be

**What are the three main authentication factor types? Give a real-life example of multifactor authentication.**

Proof by knowledge: password

Proof by possession: SIM card

Proof by property: Finger prints

**What is single sign-on?**

User is authenticated once; subsequent authentications are re-using the result without user interaction

**Explain the challenge-response authentication method. How is it used with passwords?**

Challenge response authentication method:

Server presents a challenge to the user, user answers the challenge. If the answer is correct, the user is authenticated

**Explain the difference between http Basic and http Digest authentication**

Http Basic:

Password is forwarded in plain form (not encrypted)

The browser needs to 'forget' the information

Http Digest

Only the digest(hash) is forward

Support by most browsers

**Explain the following three password protection methods: exponential backoff, blacklisting, reverse Turing test**

Exponential Backoff

Increasing waiting time after every failed attempt

Backlist

Locking the account after a certain number of consecutive incorrect guesses

Reverse Turing test

Asking the user to perform a task only a human can do

**What is a one-time password? Explain one method of generating it**

Definition:

Generate

Each password is generated from the previous one by calculating the hash (MD5 etc.) of the previous one

**What is biometric authentication? What is the difference between physiological and behavioural methods?**

Definition:

Measure physical characteristics and evaluate them against a stored pattern (verification or identification)

**What is iris recognition used for in computing, and how?**

How:

Acquisition

Segmentation

Normalization

Feature extraction

Matching

**What are the main problems in fingerprint authentication?**

Low-quality images

Distortions (non-linear) (失真)

Connotations

**What are the major issues in face recognition?**

Disguises

Illumination

Facial expression

Natural aging

**What is an X.509 certificate for? What does it contain and how is it secured? What is a Certificate Revocation List?**

The most widely used certificate type. To provide an identity or right to access certain resources, digital sign, protect content, identify the issuer/subject

Certificate Revocation List

List of invalid certificates, Can be subject to DoS attacks

**Explain the role of a Certificate Authority in Public Key Infrastructure.**

**For what purpose is the Kerberos protocol used? Who are the participants in the protocol?**

works on the basis of tickets to allow nodes communicating over a non-secure network to prove their identity to one another in a secure manner.

Participants:

Client.

Service.

Key Distribution Center (KDC)

Account database

Kerberos policy

**Week 5**

**What is the difference between authentication, access control and authorization? What is the connection between them?**

Authentication

Authentication is a process by which you verify that someone is who they claim they are.

Access control

Access Control is the process of enforcing the required security for a particular resource.

Authorization

Authorisation is the process of establishing if the user (who is already authenticated), is permitted to have access to a resource. Authorisation determines what a user is and is not allowed to do.

Identity 
Client 
Attributes 
O ration 
Policies 
Server 
Resource 
Authorisation 

**Explain the terms ‘subject’ and ‘object’ in relation to access control.**

Subjects:

Active entities that perform operations

Objects:

Passive entities on which operation are performed

**What is the access control matrix? What are the columns and rows representing?**

Definition:

Protection state represented by a matrix

Column subjects:

Row Objects:

**What is an access control list and what is an access control capability? Which one is easier to maintain and why? Which method is used in (i) Windows and in (ii) Unix?**

ACL: A list of access rights attached to an object

Capability:

a token allowing a subject (user, process) to access/use a resource

No one is easier to maintain:

Delegation of rights:

ACL need interaction with administrator

Capabilities:Can be passed from subject to subject

Revocation:

ACL:Remove subject from the list

Capabilities: Need interaction with capability holder

ACL (Windows & Unix)

Capability (Unix)

**Mention at least two methods used by the Apache web server for access control.**

By host

By environment variable

By binary criteria

**What are the two types of access control in a network? Explain them briefly.**

**Compare mandatory and discretionary access control. What is the basic difference, and what other features differ?**

Mandatory access control

The operating system prescribes and enforces users' access rights to resources (files, communication ports)

* Central administration and control
* Hierarchical structure

Discretionary access control

Certain users can pass on certain rights to other users

* More flexible
* Difficult to enforce global rules

**How are privileges assigned to a user in role-based access control?**

1) Users

Collection of people, processes etc. who use the system

Have possibly different sets of access rights

2) Roles:

Typical functions performed by users

Medication between users and access rights

3) Permissions (Access rights)

Approval of a mode of access to a resource

4) Role assignment

Set of roles the user may take on

5) Role activation

Role the user is current acting in

**What is a private role in RBAC?**

Non-inheritable permissions can be assigned to private roles

**Explain the following terms with relation to RBAC: separation of duty, cardinality and prerequisite roles.**

Separation of duty

A user can assume a role only if it is not in conflict with other roles of the user

Cardinality

Restriction on the number of users in a role

Prerequisite roles

A user can be assigned to a role if the user is already assigned to another role

E.g. Programmer must be a Project Member

**What is SELinux? State its most important features in one sentence.**

a Linux kernel security module that provides a mechanism for supporting access control security policies

Define security policy interfaces

**Week 6**

**Explain the following security principles: least privilege, economy of mechanism, open design, complete mediation, permission basis, separation of privilege, least common mechanism, ease of use**

Least privilege

Assign the least amount of privileges need to complete the task

Economy of mechanism

Small and simple mechanisms reduce opportunities for attacks

Open design

Security should not depend on obscurity (不明的) of the mechanism

Complete mediation

Every access has to be checked

Permission basis

Fail-safe defaults (default is denial of access)

Separation of privilege

Program divided into parts, each part runs with least privileges

Least common mechanism

Programs cannot corrupt each other's state

Ease of use

User's security expectations should match the mechanisms available

**What is the difference between user-oriented access control and data-oriented access control?**

User-oriented Access Control

User profile assigned after authentication

e.g.system

Data-oriented Access Control

Access control considers both data accessed and user identity

e.g. Database

**What is security by separation? Explain it in the context of physical, temporal, logical and cryptographic separation.**

Physical:

Different processes use different resources

Temporal:

Different processes run at different times

Logical:

Processes do not see anything related to other processes (sandboxing)

Cryptographic:

Processes conceal their internal working in a way that makes them incomprehensible for others

**Explain the memory layout of a user program. What segments are there, and what do those segments contain? How does segmentation help security?**

Machine generated alternative text:
Low 
address 
Operating 
system 
User program 
High 
address 
SecComp Lecture 6 
Program code 
Static data 
Dynamically allocated 
memory - Heap 
Room for growth 
Subroutines /Methods 
area - Stack 
(Return addresses, 
parameters and 
internal variables) 
Data 
area 
13 

**What is virtual memory and what is the major limitation in protecting it?**

Memory is protected only while in use (allocated)

Disk will contain virtual memory pages even after the computer is turned off

**File access control is based on two major factors. What are they?**

Subject:

Who want to access the file?

Operation intended

What type of access it is

**What is file permission inheritance? How can it be overridden?**

Permissions can be

Assigned directly

Inherited from a parent directory, process etc

Inherited permissions can be overridden by directly assigned permissions in most systems

**Explain temporarily acquired file permissions. What can they be based on? Give an example for each method.**

**What type of storage system failures affect file system reliability? List them and explain each.**

Hard disks have bad blocks:

Interconnections:

Network mounted file systems

Performance failure:

The hard ware cannot deliver the data in time

**Explain the key concepts of redundant array of independent disks (RAID).**

Definition:

Method to divide and replicate (重复) data among multiple disks

Key concepts

Replication (mirroring)

Writing identical data to more than one disk

Striping

Dividing data among several disks

Error correction:

Additional, redundant data is stored to help recovery of damaged data

**Explain the Unix file protection model (what type of access control it uses, how permissions are set and how access authorizations are granted).**

Method: Combination of access control lists (ACLs) and capabilities

a Objects have ACLs represented by protection bits

Capabilities established at authorisation time

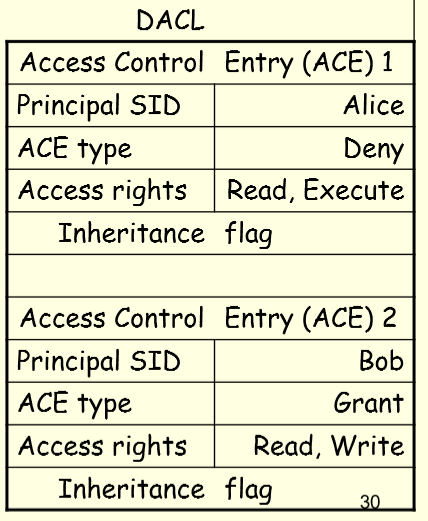
Discretionary access control

Each object has a protection state

Authorisation is granted or denied in the file open operation

**Explain the Windows file protection model (what type of access control it uses, how permissions are set and how access authorizations are granted).**

Discretionary ACL



**Access token**

**Authorization process**

**Mediation**

**Week 7**

**On what levels has database integrity to be provided?**

Physical (hardware) integrity

Logical (schema) integrity

Element (data) integrity

**Explain a method used to ensure that updating data in a database is done in a reliable manner.**

Two-phase updating methods

**Explain a usual method used to prevent data loss in a database.**

Error detection code

Shadow Copy

Monitors

**What is two-phase updating and why is it used?**

Intent:

Collect information for changes

Commit

Make permanent changes

**What does a database monitor do?**

Assure the availability and correct operation of the database, and enforce

**What access constraints can be imposed on sensitive data?**

Data availability

Scenarios when data cannot be accessed

Acceptability of access

Access to certain fields or to a combination of certain fields may not be allowed

Time of access

data is accessible during working hours only

Location of access

data can be accessed from within the organization only

History of user queries

Current query, combined with precious ones, can reveal sensitive information

**Explain why the following types of disclosures can violate confidentiality: bounds of data values, existence, probable value, negative query result.**

Bounds of data values:

Can lead to informed guess about data values, e.g. by iteratively reducing range

Existence

E.g. being on a patient list provides medical information

Probable value

Sometimes almost as good as an accurate value

Negative query result

E.g. a person does not have a particular disease

**What is the difference between data suppression and data concealing?**

Data Suppression:

Data access explicitly denied

Combine multiple answers (to hide actual data)

Data concealing

Data returned is not exact, but still close enough

 rounding

 range of result given

 obfuscation (data masking): data is replaced with realistic, but not real data

**What are the major security threats in database queries and database updates?**

Queries:

Information leak

Update:

Integrity compromise

**What is a statistical inference attack on a database? Explain it on an example.**

Inferring sensitive data from non-sensitive data

e.g.

Q1: Is element X of type A? – A: - (No answer)

Q2: Is element X of type B? – A: No

Q3: Is element X of type C? – A: No

Q4: Is element X of type D? – A: - (No answer)

Conclusion: Element X is of type A

**What is a direct inference attack on a database? Explain it on an example.**

Direct access to certain individual records is not allowed

List NAME where (sex=m and drugs = y) or (sex≠m and sex≠f) or (home=nowhere)

**What is an indirect inference attack on a database? Explain it on an example.**

Inferring sensitive data from non-sensitive data

Select SUM(salary)Select SUM(salary) where lastname != 'Smith';

**Why is data aggregation a threat to privacy?**

Combining different data

Can easily lead to the identification of a single item/person

**What is an SQL injection attack? Explain it on an example.**

Entering user input that can be interpreted as an SQL command

SELECT \* FROM items WHERE owner = 'john' AND itemname = 'name' OR 'a'='a';

**Compare the hot-swap and off-line backup methods. How are they done and what are the advantages of each?**

Off-line

CD, DVD, flash drive (e.g. USB memory)

Hot-swap

External hard disk, flash drive

**Compare the incremental and mirroring backup methods. How are they done and what are the advantages of each?**

Incremental

Saves changes since the last backup

Adv:

Faster to do a backup

Dis:

Takes longer to restore

Mirroring

Saves all data or the whole system

Adv:

Restore is easy and straightforward

Dis:

Longer time

Frequency:

Should be regular/periodic

Should mix incremental and mirroring

**Why is backup separation important? What types of separation are the most prevalent?**

In case of natural disaster, data will still be safe

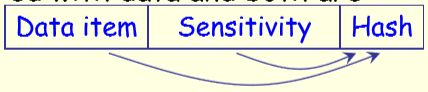
Different methods should be used together If the backup hardware/software (tape, DVD …) fails, you still have another method to rely on (on-line backup, offsite …)

**Compare the multilevel database integrity lock and the multilevel database sensitivity lock. What do they have in common, and how do they differ?**

**What are the major issues with distributed databases?**

Integrity lock

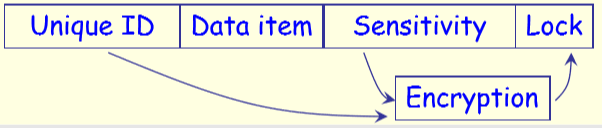
Sensitivity level is stored with data and both are protected by a hash



Sensitivity lock

Combination of a unique ID and the sensitivity level in encrypted form

The lock’s content is not accessible in ordinary view



**Week 8**

**Wired media can be easily tapped for eavesdropping. Is this statement true for every wired media? Explain the case for coaxial cable, twisted pair and optical fiber.**

Depends on types.

Coaxial cable:

Very easy to tap unnoticed

Twisted pair:

Fairly easy to tap

Optical fiber

Can be tapped unnoticed after removing other protection

**What are the major security issues with wireless communication?**

Eavesdropping (窃听)

Anyone in the vicinity can receive the signal

Easy to interfere with data integrity problem

Anyone in the vicinity can transmit

**Compare wired and wireless media security. Explain the advantages and disadvantages of both.**

Wired:

Signal confined to the cable

Cable costs

Wireless:

Adv:

No cabling costs

Dis

Reduced range

**What is the main function of a firewall?**

protect computers and networks

**How many network nodes can a firewall protect?**

Single host protection:

Installed in workstations

Network segment or a whole network protection:

Installed at

Network entry/exit points

Computer connections

**What are the basic differences between a dedicated firewall device and firewall software running on the protected device?**

Dedicated

Fast

Should not run any other application software

Advanced management features

Software

Less secure

Cheap

**What is a packet filter and what is a proxy? What is common in them, and how do they differ?**

Packet filter:

Look at the message and take action

Fast

Pass or discarding

Proxies

Interpret the message

Generate a new message with the same content

Processing is slower

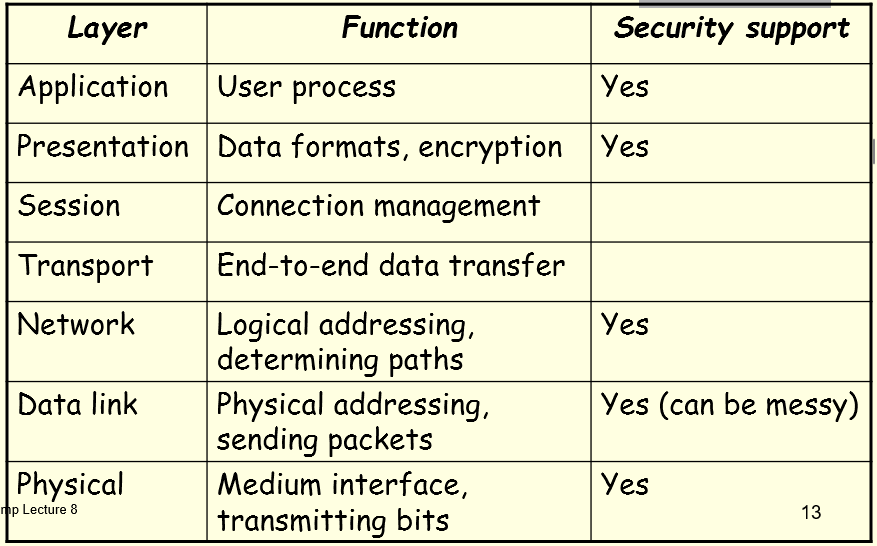
**Name at least two Internet-related security protocols and indicate in which OSI layer they are used.**

IPsec

communication.

TLS(SSL)

The transport layers



**What are the main aims of a host compromise?**

Collect sensitive data from target

Use compromised computer to launch further attacks

**How can direct flooding be used in a denial of service attack? Can indirect flooding be used?**

Direct flooding:

Traffic via established connections

Legitimate connection requests

Malformed/unfinished connection requests

Indirect flooding

Directing responses to maliciously formed queries to the victim (e.g. DNS amplification attack)

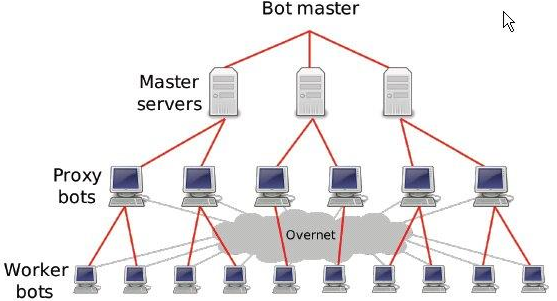
**What is a botnet? Describe how it is organized, how it works and name one famous one. (Look at lectures 2, 8 and 12 as well)**

Definition:

Network of compromised computers

Controlled from a single command point

Organized:



Example:

Zeus Bot

**How does a person-in-the-middle attack work? How does it differ from traffic diversion?**

Person-in-the-middle

Active eavesdropping (“unauthorised proxy”)

Traffic diversion:

Redirecting messages to the attacker so that the intended recipient may not even receive it

**Explain three ways of session hijacking.**

Session fixation

Attacker tricks the victim into connecting to a server with a session ID set by the attacker

Session sidejacking (sniffing)

Attacker acquires an existing, valid session ID, and takes over the connection

Cross-site scripting (XSS)

Attacker tricks the user’s computer to run malicious code (and e.g. steal a session token)

**What are the most frequent targets when network administration is attacked?**

Attack on the authentication database

E.g. password file attack

Attack on network security devices

E.g. firewall attack

Attack on web servers

E.g. defacing

**What are the main differences between audit trails and logs?**

Logs

Traces of operation

Generated by system and application programs

Kept in a file

Easy to access, easy to review

Audit trails

A protected collection of information about system activities

Contains detailed information

Better chances to detect anomalies

More data to store & analyse

**What are the advantages and disadvantages of network-based, host-based, application-based and target-based intrusion detection?**

Intrusion Detection Systems

protect computers and networks

Second line of defense

Reactive tool

Operation:

Monitors the operations

Looks for evidence of unauthorized activity

Raises alarm

Network based

Adv:

few devices can protect a large network

Dis:

Cannot cope with current, high network speeds

Cannot analyses encrypted packets

Host based:

Adv:

Can analyse encrypted traffic

Dis

performance penalty borne by the host

Application based:

Adv:

Can observe user interaction

Dis:

Tied to particular application

Target based:

Target monitor their own data

**What are the basic differences between misuse and anomaly based intrusion detection?**

Misuse detection:

Looking for known attack patterns

Based on pattern matching

Anomaly detection:

Looking for deviation from normal system behavior

Based on behavior analysis

**Incident Handling steps:**

Detection

Containment

Eradication

Recovery

**Explain the steps in kill chain analysis.**

1. Reconnaissance: Intruder selects target, researches it, and attempts to identify vulnerabilities in the target network.
2. Weaponization: Intruder creates remote access malware weapon, such as a virus or worm, tailored to one or more vulnerabilities.
3. Delivery: Intruder transmits weapon to target (e.g., via e-mail attachments, websites or USB drives)
4. Exploitation: Malware weapon's program code triggers, which takes action on target network to exploit vulnerability.
5. Installation: Malware weapon installs access point (e.g., "backdoor") usable by intruder.
6. Command and Control: Malware enables intruder to have "hands on the keyboard" persistent access to target network.
7. Actions on Objective: Intruder takes action to achieve their goals, such as data exfiltration, data destruction, or encryption for ransom.

**What are the roles of red and blue teams in penetration testing?**

Red: as enemy

Blue: Defender

**Week 9**

**What are the major security threats of embedded content in web pages?**

Attack sites

Malware escaping browser protection mechanisms

**What are the main security issues related to communication produced by web scripting?**

Can be used for unattended installation of software

**Explain the sandbox web security policy.**

The browser and any application running in it have limited access to most local resources

**Explain the same origin web security policy.**

Documents and scripts originating from the same site can access each other’s methods and properties (e.g. HTTP PUT)

**What are the possible dangers when using a URL to find a web page? Is typing it in, cutting and pasting or clicking on a link more secure? Why?**

None is secure.

**What is cross-site scripting? How does it work? Explain at least two types of XSS attacks.**

Definition:

Attacker uses the web site to send malicious code to a different web-page user

Stored attack

The malicious code is permanently stored on the web server

Victim retrieves the malicious code when accessing the infected information

Reflected attack

The user is tricked into clicking on a malicious link or submit a specially crafted form to the vulnerable web server that will send it back to the user’s browser

**What are the possible consequences of a cross-site script attack? Name at least four.**

Cookie theft

Disclosure of end user files

Installation of Trojan horses

Redirection to other sites

Modification of presentation or content (e.g. stock price)

**How can the possibility of cross-site scripting attacks be reduced by the web site maintainer and by the browser/user?**

Maintainer:

Validate (check and sanitise) input

Ensure characters are treated as data, not relevant to the interpreter’s parser

Protect your cookies from client-side scripts (use the HTTPOnly flag)

Browser

Be careful with spam and forums

**What is cross-site request forgery? Why is it extremely dangerous?**

Steps:

The victim is tricked into accessing a malicious web page that contains the attack script

The attack script executes with the victim’s identity and privileges to perform an undesired function

If the victim has been authenticated to a server (has a valid, non-expired cookie), the attack script can access the victim’s account on the server (e.g. bank account)

Consequences:

Almost no limit on impact of CSRF

**What are the most frequent variants of CSRF? How can the browser/user mitigate the danger, and how can the web site maintainer reduce the risk?**

Cross posting

An HTTP POST request is sent to the web page (Data writing)

Cross authentication

The attacker can perform actions at a site in the victim’s name (by using the victim’s cookies)

**What is clickjacking? How does it work?**

Clickjacking

Multiple transparent and opaque layers of a web page result in a click on a concealed and unintended link

Work principle

HTML <iframe> tag defines an inline frame that includes another document

**How can the browser/user mitigate the danger of clickjacking, and how can the web site maintainer reduce the risk?**

Maintainer

not allowing pages appear in a frame

Browser

NoScript - scripts disabled in general, explicit permission can be granted by the user for individual sites

**What is cross-site framing? Explain the method.**

Site A (attacker) includes site B in the page

Victim believes to be operating on site B

Site A can use the victim’s credentials on site B

**What is cross-site double clicking? Explain the method.**

Two pages pop-up together, first is hidden below the second

The second click will be passed on to the first pop-up, without the victim noticing it

**Explain what a web crawler does and for what purpose.**

Definition:

Automated program that methodically browses the Web

Purpose:

Make index of data

**Explain the three main policies a web crawler should observe.**

Selection:

which pages to download (e.g. which hyperlinks to follow)

Politeness:

how many pages of a website to download simultaneously to avoid web server overload

Parallelisation

improve performance

**Explain at least four blackhat methods that are used by unscrupulous web site maintainers to improve the search ranking of a web page.**

Cloaking:

presenting different content to URL users and search engines

Keyword stuffing

inserting irrelevant keywords

JavaScript redirects

crawlers may not execute scripts

Doorway pages

large sets of pages, each optimised for a different keyword, all pages redirect to one page

Link farming

group of web pages having links to other web pages in the group

**What is the purpose of search engine optimisation poisoning?**

**How are blackhat methods used in search engine optimisation poisoning?**

* A fake site is set up to serve
  + - * legitimate content to crawlers and
      * malicious content to users.
* The hacker creates a link farm to the fake site to be picked up by a crawler.
* A search spider crawls the link farm.
* The fake site appears in the search results. The fake site is built around themes of the day to increase the number of searching users.
* A user clicks on the search result link leading to the hacked site and is redirected to the malicious page.

**Week 10**

**Consider physical security and software security of (i) mobile computers and (ii) fixed hosts. Explain which one is more important in case (i) and in case (ii) and why it is so.**

Physical security

Easy to steal or lose (mobile)

Software security

Computers

Additional malware, mostly related to location privacy

Phone:

Smart phones are mostly affected

**What is the main security issue when a mobile computer is attached to a (i) wired network and when to a (ii) wireless network.**

Wired networks

(Precondition) Away from home network

(Precondition) Have access to wired networks (e.g. in hotel)

Connection to home network goes via public routes

**Explain the major security issue in WiFi hotspots.**

Communication channel is wide open

**Explain at least three major security issues in WiFi home networks.**

Channel pollution

WiFi networks too close to each other may interfere with each other’s operation

WarXing

Searching for WiFi networks without using its services Problems: Ethical and legal questions, privacy concerns

Piggybacking

Connecting to a network and using it without explicit authorisation

Easy attack launch by intruders

E.g. DNS (URL to IP address) spoofing

**Explain at least four reasons why WEP has been superseded by better protection methods.**

Authentication is one way only (mobile device to access point)

The same secret key is used for authentication and encryption

Device can be impersonated

No re-play protection

Message integrity check is ineffective

**What are the main security advantages of WPA/WPA2 over WEP?**

Improved data encryption

Temporal key integrity protocol (TKIP): default for WPA, supported by WPA2 for backward compatibility

AES: default for WPA2

Improved authentication via the extensible authentication protocol (EAP)

**What security services are available in Bluetooth?**

Authentication

Authorization

Confidentiality (encryption)

**What are the Bluetooth security levels for services and for devices?**

Services

Authentication and authorisation required

Authentication only

Open access

Devices

Trusted

Untrusted

**Explain at least three Bluetooth vulnerabilities.**

Encryption Keys

are negotiated and can be short, device keys can be shared, cipher algorithm is weak …

Authentication

Attempts have no limits, no user authentication, …

Bluejacking:

sending unsolicited messages

Bluesnarfing:

unathorized access of information via Bluetooth

Bluebugging:

attacker takes over the device by exploiting some flaws in firmware of older devices

Denial of service

Fuzzing attacks: sending malformed messages/data to discover device firmware vulnerabilities

**Explain two major protection methods used by the manufacturer to protect iPhones.**

Applications run in a sandbox

Applications are signed by Apple or by the developer using an Apple certificate

**What is ‘jailbreaking an iPhone’?**

enabling the iPhone to run applications not approved by Apple

**Name at least three methods used to propagate mobile phone malware.**

Drive-by-downloads

Emails

Bluetooth file transfers

Multimedia messages (MMS), ringtones

Infected memory cards

SMS download links

**Explain how (mobile) malware evolves.**

Target:

Trojans subscribe people to unnecessary services

Fake mobile bank steal money

Evolution:

Criminals release skeleton with simple functions

Malicious functionality is added

Massive attack campaign begins

**What is phishing and how does it work?**

Definition:

Aims to extract private information (banking details, via spoofed sites)

**What is spear phishing and what is vishing? (Look at lecture 12 too)**

Spear phishing

Targeted phishing, eg to senior executives

Vishing

Phone (eg VoIP) phishing (eg fake call centre)

**What is pharming? (Look at lecture 12 too)**

Attacker redirects website traffic to another fraudulent site (eg DNS redirects)

**Mention at least four different types of information that can be obtained by spying on mobile phones.**

Capture screenshots

Capture photos using the front and back cameras

Passwords for WiFi networks and online accounts

Record using the microphone

Collect contacts and decode messages from IM accounts

Collect SMS, MMS, and Gmail messages

Record location

Capture real-time voice calls in any network or app by hooking into the “mediaserver” system service

**Describe some mobile spyware/malware detection and defense methods.**

Users

Any extra charges on my bill?

Has my phone opened unexpected connections?

When rebooting, are there screens/dialogs that flash and disappear instantaneously?

Experts:

Check network connections

Check every process running on the phone

File system analysis

Defense:

Apply updates

Use only signed application

Have a lock code, personalize the phone

Tools:

Anti-virus products

Encrypted communication:

VoIP

Protects the conversation only

**Week 11**

**What are the major security and privacy concerns in cloud computing, and how can they be addressed?**

Potential problems:

Shared environment

In theory:

Users control access

In practice:

Users have to trust technology not revealed to them by the cloud service provider (CSP)

Service provider problems

Possibility of CSP internal attacks

Lack of immediate client control

Users may not have any say in how/where the data is stored

Availability

Users may experience unforeseen system shutdowns

Solution:

Data auditing

Regular checking of data accuracy & consistency

Encryption

**What is the business model of social network sites? How does that affect privacy?**

Targeted advertising based on personal interests is more effective

Affect privacy

Leaking user data

User activity monitoring

**What is the purpose of a privacy policy e.g. in a social network? How effective are those policies in practice?**

Theory

Tells users about the site’s practices and obligations

Users then can decide what features are acceptable, they can opt in or opt out

The presence of such a policy increases user trust

Practice

Policies are

hard to find

take a long time to read

can change without notice

**Explain why trust modelling in social networks can be considered simplistic.**

A connection may not mean friendship in everyday sense

Membership and trust are binary

**Why does personal data need more protection than financial data?**

Finical data can be cancelled but personal data cannot

**What is the major concern with single sign-on between social sites?**

Data aggregation

**What limitations need to be considered on personal information directly published on the web?**

Scope in time

Scope in space

Searchable attributes

**Explain two ways of indirect publishing of personal data by social network friends.**

Photos showing you

Others can infer attributes via friends or friends’ attributes

**Explain the indirect publishing of personal data by social network applications.**

When a user installs an application, the application acquires the privileges of the profile owner

Many of these applications are “marketing businesses built on top of the idea that third parties can get access to data on Facebook."

**Why do employers monitor social network sites? Explain at least two reasons.**

learn employee’s off-duty behaviour (private life)

prevent leaking of company information

screen job applicants

**Explain at least four ways of criminal use of social network sites.**

Blackmail

Impostors

Scam

Identity theft

Users’ irresponsible actions

**What information can be collected from social network sites by law enforcement agencies?**

reveal personal communication

establish personal relations

reveal motives

provide location information

prove and disprove alibis

**Describe three types of services that use location as the main input parameter.**

Location-based information

E.g. “find a restaurant near me”

Location-based billing

E.g. roaming

Emergency services

Tracking

E.g. vehicle movements for fleet operators

**Explain the main components of location-based services.**

**Positioning**

Most frequently used method: Global positioning system (GPS)

Other methods (triangulation, phone cell information, etc) can also be used

**Geographic information systems (GIS)**

Processes map data (e.g. streets) and points of interest (e.g. restaurants)

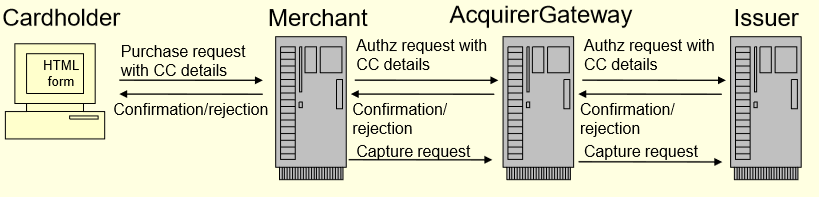
**Location management function**

Processes positioning and GIS data for LBS applications

**Explain the primary functions of the Office of the Australian Information Commissioner briefly.**

**Week 12**

**Explain the steps in processing a credit card payment via the Internet.**



**What technology is available to prevent phishing?**

Web application security

Restrict Track / Trace HTTP methods

Output Encoding

Web application firewalls

XSS detection

Content referrer restrictions

**Explain the reason for authenticating emails and describe two email authentication methods.**

Easily to be spoofed

Publishing the identity of servers

Digitally signing emails

**Describe three methods of mobile banking.**

Mobile Phones

Thick clients / mini-browsers for iPhone

SMS authentication

Peer to peer payments

EftPOS

Debit-card transaction processing

ATMs

Mag-stripe or chip-and-pin bank cards

**Explain a popular digital currency. How does it work and how can be it attacked?**

Cryptocurrencies:

use crytpographic solutions to secure transactions and control the creation of units

Attack

Bitcoin mining

Websites can use their visitors for calculations in background scripts

Botnets used for mining

Attacking Bitcoin exchange

**What are the six major requirements of the Payment Card Industry Data Security Standards?**

Build and Maintain a secure network

Regularly Monitor and Test Networks

Protect Cardholder data

Maintain a Vulnerability Management Program

Maintain an Information Security Policy

Implement Strong Access Control Measures

**Explain what the Darknet is. What is the Darknet market?**

Darknet:

Overlay network

Accessible with special software only

Main types

Friend-to-friend

Anonymity networks

Darknet market

for illicit (and legal) goods

**What is Blackhole and what are the most important features of it?**

Malware kits

Tools for criminals to create and distribute malware

Systems to manage networks of infected machines

**Features:**

Targets a variety of vulnerabilities

Provides management services

**What are the advanced technological features of botnets?**

WebInjects and Jabber IM