Week 1: Introduction

Main topics: concept of security, adversaries, security services

1. What are the types of security available?

Security through obscurity: is where internal working, sensitive components and details are hidden. This may work in some cases, however it may attract hackers

Security through legislation: Laws prescribe allowable user activities. However, efficiency may be limited as the offender may be in another jurisdiction.

2. Covert vs overt channels

Overt channels: they are openly publicized, documented channels for authorized transfer of data.

Covert channels: Data in these channels have a subliminal meaning. For instance, the existence or absence of data carries the information, but the actual value is irrelevant. This channel is not intended for transfer of information. The transfer of information is slow. Often created by misusing overt channels.

Examples include:

- Timing channel: process modulates its own use of system resources, i.e malware causing the hard drive LED to blink
- Storage channel: communicate by modifying a stored object i.e file lock (open/close) channel
- Data hiding in the OSI model. i.e in ICMP error packets

3. Threats to security

Interference with normal operation

- Malware: viruses (attached to host program)
  - worms: self-propagating
  - trojans: hides hidden info
  - spyware: collects data in an unauthorized manner
  - rootkit: hides the presence of malware
- Denial of service (DoS): blocking access to a service

4. Adversaries of a security system

Hackers: well educated users with above average computer skills. Their aim is to make a point, meet a challenge

- White hat hacker: computer expert specialized in security testing
- Black hat hacker (cracker): computer expert who uses his expertise for criminal activities
- Hacktivist: utilizes technology to announce a (usually ideological or political) message

Amateurs (lamers). They are regular, sometimes uneducated users trying to exploit some vulnerabilities (e.g script kids). Aim: thrill

Career criminals: they are criminals who may lack computer skills. They employ corrupt hackers. Their aim: financial gain, and industrial espionage

5. Difference between a security policy and a security mechanism

Policies describe the aims of protection. Example: resources should only be available to authorised users only.

Mechanisms implement the policies. Example: users need to log in in order to use the resources.

6. Basic aspects of security; a TLDR

Confidentiality: unauthorized users cannot read information

Only authorised entities (humans or computer programs) can acquire knowledge of some data content. Example: Medical records, student results should not be disclosed improperly

Integrity: unauthorized users cannot alter information

Implicit meaning: the data is correct and comes from a trustworthy source. Example: bank statements show correct details

Availability: unauthorized users cannot access information

Privacy: Restricts the use of legally obtained data

Meaning: only authorised entities (humans or computer programs) can disclose legally obtained data to secondary users.

Example: A company cannot sell your personal data without your approval

Authenticity: Verifiable source of origin

The quality of being genuine, trustworthy. Truthfulness of origin, attributes.
Meaning: the source of a document, identity of a person, is as claimed.

Computers check authenticity in a number of ways (most common: user authentication)

Week 2: Vulnerabilities, Threats & Attacks

1. Security terms/definitions

Vulnerability: A weakness in the application (design flaw, bug, ect) that allows an attacker to cause harm. Example: hole in fence

Exploit: technique that allows the attacker to take advantage of vulnerabilities. Example: go through hole

Attack: use of an exploit

Threat: the potential of a harmful event. Example: loss of stereo.

Threat agent: capabilities + intentions + past activities. Example: thief

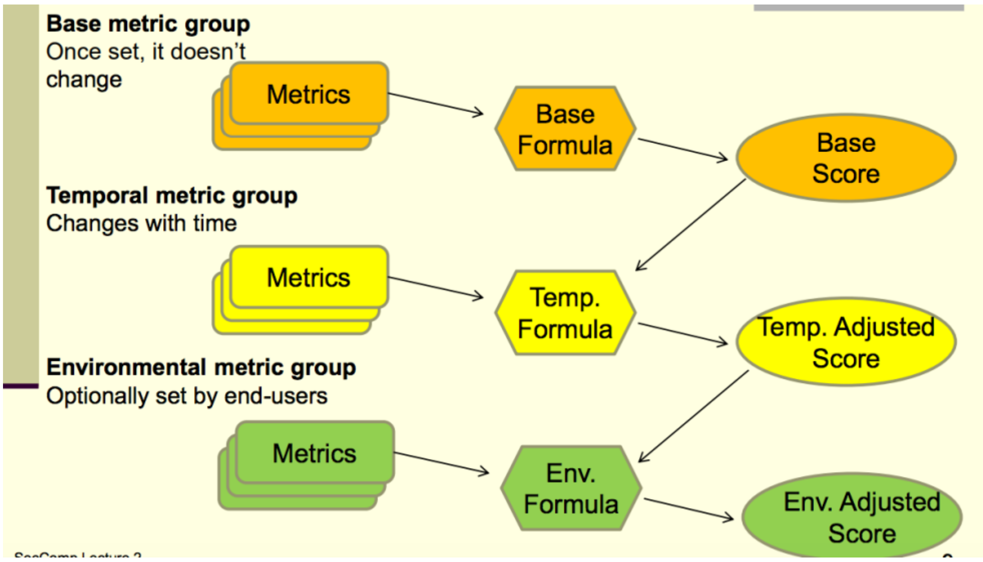
Vulnerability -> threat -> attack -> response

1. Common Vulnerability Scoring System (CVSS)

It is a standardized method to assess security vulnerabilities
Scoring is based on a number metrics in three main categories:

Base: immutable (unchangeable) features of a core vulnerability
Temporal: evolve during the lifetime of the vulnerability
Environmental: how the vulnerability affects a particular installation

2. The CVSS Calculation Process



Base metric group
Once set, it doesn't change

Temporal metric group
Changes with time

Environmental metric group
Optionally set by end-users

CVSS Base score

It indicates the general severity and represents the innate characteristics of the vulnerability, that is not expected to change. It has the strongest influence on the final score.

It's main metrics are:

- **Exploitability:** access vector (e.g local or remote) and access complexity (high-low)
- **Impact:** none, partial or complete loss of confidentiality, integrity, availability

CVSS Temporal Score

It represents changes over time and introduces mitigating factors that usually decrease the final score. It is expected to be re-evaluated periodically. It also indicates urgency.

It's main metrics are:

- **Exploitability:** Theoretical, proof of concept exists, functional (works for most situations), high (always works)
- **Remediation:** official/temporary fix, workaround, not available

CVSS environmental Score

It represents vulnerability in an installation and address deployment and configuration. It is defined by the consumer/end user and indicates overall priority.

It's main metrics are:

- **Collateral damage potential**
- **Target distribution:** number of systems vulnerable in a particular environment

3. Threat assessment

Aim: identify system vulnerabilities, assess the risk of threats, and define an effective mitigation plan.

4. What is an attack vector + attack surface?

Attack vector: a way/route/method of triggering or reaching a vulnerability

E.g. malicious email, attachments, worms, web pages, downloads, deception (aka social engineering). This is different from malicious payloads (e.g. viruses, trojans, malicious scripts)
Attack vector analysis is useful for: understanding the severity of a vulnerability & defence (e.g. allows the blocking of certain inputs)

Attack surface: a sum of different attack vectors threatening a software environment. Reducing the attack surface improves security

Zero-day attack: Attack (method) exploiting a vulnerability that has no defense/solution/fix yet

5. What are some common attack methods: passive vs active?

Passive attacks: obtain information in an unauthorized manner

- Privacy violation: Targeted attack E.g. gain information about a specific bank account OR Data harvesting E.g. collect credit card numbers/email addresses
- Publicity attacks: Attack for the sake of publicity, e.g. press

Active attacks: Interfere with the operation (e.g. manipulate objects)

6. What do the attacks target?

Theft of information: Private data (bank account number, password, …) Spyware: collects information without the user's knowledge (e.g. keyloggers)

Theft of resources: Computer hijacking Botnet: network of computers that can be remotely controlled without the lawful owner's knowledge; used e.g. for spamming, DoS attacks

Interfering with the operation: Denial of service (DoS) Overwhelming the target with bogus requests and making it inaccessible for legitimate users

7. **What are some common attack strategies?**

Attacker's aim: To "own" the target machine

- have privileged (root/administrator) access
- execute programs in privileged (kernel) mode

Infiltration method

- Social engineering
- Exploit root-level flaws
- Exploit lower-level flaws and escalate privileges via other exploits

Dissemination of malware

- Virus (needs a host to spread, e.g. via infected emails, data, …)
- Worm (spreads on its own)

8. **Types of Malware**

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

9. **Types of authentication (password) attacks**

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

10. **Definition of Spoofing vs Denial of Service**

Spoofing: Masquerading as someone else by falsifying data

- Spoofing Attacks i.e Phishing: Tricking the user into volunteering confidential information

Denial of service (DoS) attacks

- **Direct attacks:** overwhelming traffic from attacker to victim
- **Reflected attack:** sending a spoofed packet (the victim is shown as the source) to many hosts, the responses overwhelming the victim
- **Distributed DoS (DDoS) attacks:** Using a network of machines (botnets) for a DoS attack

11. **What are the DDoS attack types?**

Volume based attacks

- Method: bandwidth saturation

- E.g. UDP/ICMP floods (usually spoofed packets)

Protocol attacks

- Method: server resource attack
- E.g. SYN floods

Application layer attacks

- Method: crash the application
- E.g. GET/POST floods

12. What are botnets?

Botnets are a: Network of compromised computers that are controlled from a single command point

Features:

- Well organized hierarchy of computers
- Workers at the bottom layer
- Infected computers are zombies – activated by a central command
- Attack/malicious activity method by the same computer can vary
- Workers back off randomly, to disguise themselves

Use

- Honest use - rare E.g. Distributed computing
- Malicious use – most often i.e Spam mailer & DDoS attack tool

13. Definition of Injection attacks/rootkits/social engineering

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

Code injection: Inserting code that is interpreted by the application

- Command: Execute system commands by the application and have the application's privileges
- SQL injection: Inserting a database query via the input of the application
- Cross-site scripting- Malicious scripts inserted into benign and trusted web sites

Rootkits: Malware that hides its presence via modifying system data. They attempt to hide the presence of malware

Social engineering: Exploiting human gullibility to extract confidential information

Social engineering is the most effective method for getting around security obstacles. The hardest form of attack, it cannot be detected by hardware or software alone

14. Human vs computer based social engineering

Human based:

a) Phone call: to helpdesk by impersonating a legitimate (important) user, or referring to tech support by using names or impersonating tech support

b) In person
   - Shoulder surfing: watching what others are typing
   - Dumpster diving: going through the trash

Computer based i.e Phishing: asking the user to verify account details. Example: popup windows, spam, and websites offering something free or a chance to win something.

15. Talk about social engineering exploits

Contrived situation: Inventing several factors to improve plausibility (forgot a password, looming deadlines, …)

Personal persuasion

Request methods

- Direct request: Often challenged and refused, and hence rarely used
- Context-aware request: The perpetrator sets up a scenario (e.g. cuts a cable) then offers help

16. How does one respond to incidents? What are the main steps?

Steps:

1. Detection: Includes identification of the attack
2. Containment: Prevention from causing damage and from spreading (quarantine)
3. Eradication: Remove the agent
4. Recovery: Restore the normal operation

Response tools: Assist or automate some of the steps E.g. antivirus programs automate steps 1-3