University of Applied Sciences and Arts Northwestern Switzerland
School of Life Sciences



# S1 Personal Security
## D4 – Data and Ethics

# Naming Terminology

## Virus

- Virus is inserted into an application
- Can only reproduce if the app is executed

## Trojan Horse

- Similar to a virus
- Application pretends to be good, is designed to be malicious
- Does only reproduce if app is executed

## Worm

- Worm is an independent piece of software
- It reproduces itself without interaction
- See Conficker, Sassar, Stuxnet, WannaCry

## Rootkits

- Rootkit is a Tool that gets full administrative access on a computer
- Rootkits can be injected into applications, kernels, hypervisors, or firmware
- Hard to detect, often impossible from the same system (e.g. linux live antivirus helps)

## Backdoor

- Piece of software running on a machine
- Opening a port or a reverse connection
- Enable unauthorized user to access remote
- Installed by e.g. Worm
- Often seen in Botnets, Ransomware or Govware (Governmental Survaillance Software)

## Exploit

- Exploit is a chunk of code/data using a security weakness
- Zeroday-Exploit: publicly unknown exploit used by malware

## Payload

- Exploit is a chunk of code/data using a security weakness
- Zeroday-Exploit: publicly unknown exploit used by malware

**For the sake of terminology completeness**

## Data Breach

- An incident where sensitive or confidential data were stolen
- Can be an insider job
- Can be by unauthorized access
- Can be a combination of both

**For the sake of terminology completeness**

## Denial of Service (DoS) - Attack

- Bringing a system to a state where it cannot offer its service anymore
- Try to overload a system or a component of the system
- Other ways to crash the system
- DDoS: Distributed Denial of Service Attack
- Can be by a group of volunteers or a group of bots

**For the sake of terminology completeness**

# Threat and Security Modeling

## Threat and Security Model – Overview

**“Security is job zero”**

*Bill Murray, Director AWS Security, Amazon*

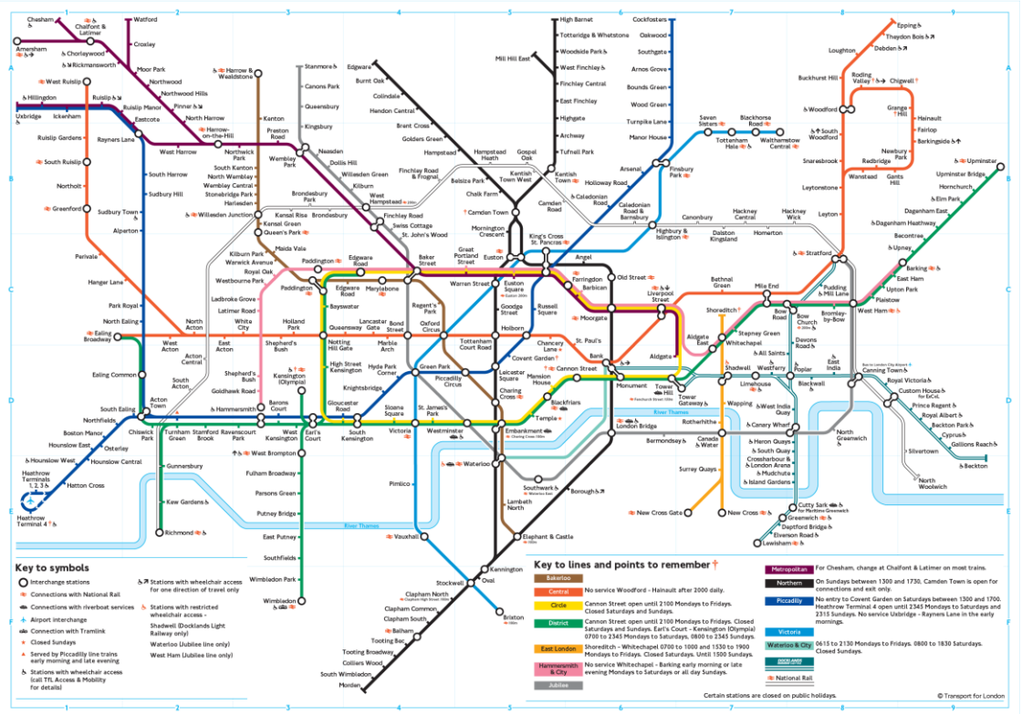
How to model security of a system:

- Policies the system should enforce

Threat Model: Assumptions about the bad guy and possible vectors of attack

- Security Model for each possible threat
- In practice people get policies wrong, people get the threat model wrong, people get the Security Model wrong.

# What is a Vector of Attack?




- A Vector of Attack is a class of ways how to get into a computer system
- Can involve multiple system components, so don't think about them individually
- Passive: gains access without affecting the system
- Active: Breaching into the system by "force"

# Attack Surface


- Attack Surface is the total number of attack vectors an attacker could use against a system
- In general: Small Attack Surface is good security practice
- Reduce your surface by closing unused ports, removing unnecessary components etc.

## Policies the System Should Enforce / Threat Model

Think about your system/software/company network.

- Which components exist in the system?
- Which input/output/access rights do each component have?
- Which behavior should each component have?

Possible attackers (e.g. Bad Guy, Insider, Nation State)?

Possible Vectors of Attack / Attack surface?

Is the system network connected?

What input does the system take?

What output does the system produce?

Who can use the system?

Which data/assets could an attacker be interested in?

**Information Security Policy – something in this direction (more user-friendly) will be introduced later in the D4 Module! Wont be too cybersec/techie – promise!**

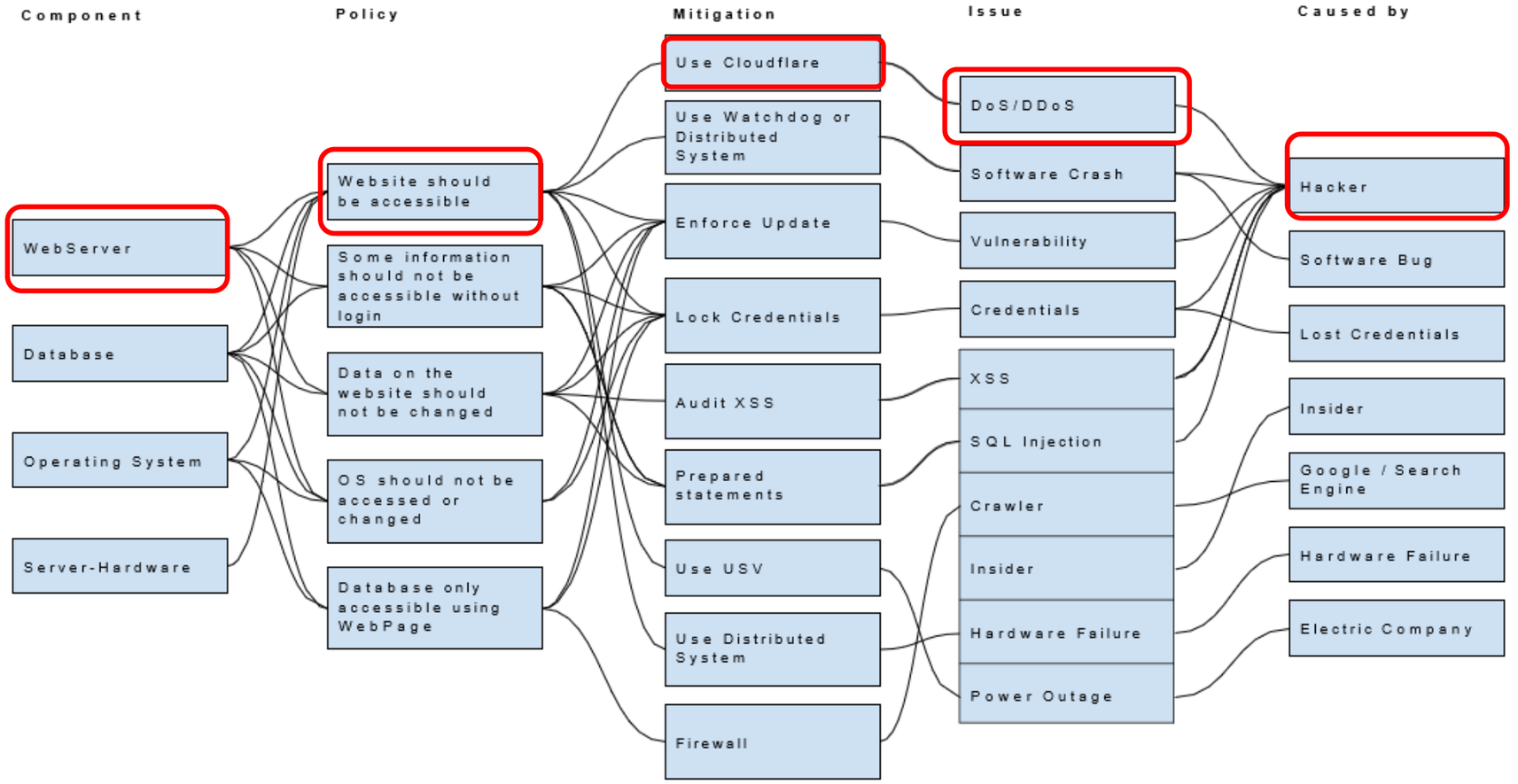
# Typical Vectors of Attack (a collection…)

- **Misconfiguration**
  - Unchanged default passwords
  - Cloud credentials not set correctly
  - Unwanted components running, which compromise security model
- **Phishing**
  - Form of social engineering.
  - Try to trick target to share credentials or execute code
- **Vulnerability**
  - Weakness in a Software
  - Makes the Software exploitable
- **Weak/Compromised credentials**
  - Username/Password can be broken easily
  - Username/Password are breached by phishing, malware, same PWs etc.
  - Most common attack vector
- **Malicious Insider**
  - Insider Jobs are often hard to defend.
  - Insider steals data he has access to
  - Insider convince people to give him more data
  - Insider deploys malware (lateral movement is easy than from outside)
- **Missing or poor encryption**
  - Sensible data are transferred without encryption
  - Password can be stolen, Data can be breached
- **SQL Injection**
  - Inject a customized SQL query into a database
  - Leads to information leak
  - Can be prevented by prepared statements
- **Trojans**
  - Software pretending to be useful but being malicious
- **Cross-site Scripting (XSS)**
  - Injecting malicious code into a website
  - Impact other users view on the website

**…. We stop here with examples, there are many more ☺ …..**

## Example: Modelling Security

Graphical Model (there are Tools for that):



# Macros – why is it still a thing?

## What is a MS-Office Macro?

- Word, Excel, Powerpoint-docs can be enhanced by scripting
- VBA (Visual Basic for Applications)

**Idea:**

- A company uses Excel for storing and organising data
- To add data to the Excel Sheet automatically from business process, sensor, api, net, etc
- Automatically process data in a way excel cannot do
- Automatize repetitive tasks
- Code shipped in the Excel sheet, so it is transportable

**Problems:**

- VBA can access system resources, start processes etc
- If macros are active, VBA is executed when the document is opened or by hotkeys
- Business Processes in some companies heavily relay on macros.

## What is a MS-Office Macro? (2)

- Since it is in use by companies, it cannot be easily switched off.
- Since data are exchanged between computers, macros travel and are a good carrier for malicious code
  - used to install spyware, goveware, ransomware
- Macros have a long history of being abused for malware
- Other programs offer scripting, too: Gimp, Photoshop, Ghidra, ...
- Important difference: Scripts are installed locally and **DO NOT TRAVEL** with the document

## What is a MS-Office Macro? (3)

- If a company uses Macros, Macros need to be part of the Threat Model
- It is one of the most common and most powerful vectors of attack
- You can run any code on a remote machine by tricking one person to open the document
- No exploit required.

## Questions?

- For a very long time people considered security as annoying
- Information Security is about being very precisely
- “I do not have to hide anything” — The question is from whom?