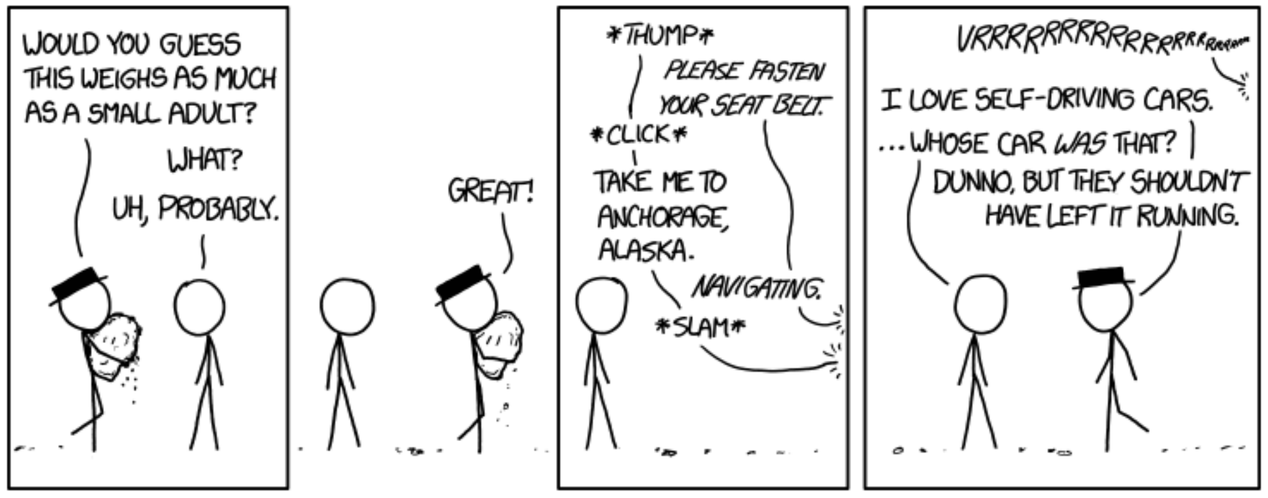
FIT 1047

Introduction to computer systems, networks and security

MONASH University

There are many ways to attack systems



(xkcd.org)

Nicely shows that not all security issues are technical...

Security: overview

Encryption and digital signatures

- Symmetric key encryption
- Public key cryptography
- Message Authentication Code (MAC)
- Hash functions

Security: overview

Access control

- ACLs, mandatory access control, role-based
- Multi-factor authentication

Security: overview

Firewalls

- Port-based firewalls
- Parameters for filtering
- Intrusion detection, Intrusion prevention

Security Properties

Authenticity

Something has definitely happened in the way we assume.

Security Properties

Integrity

Some data has not been changed since some authentic event.

Security Properties

Confidentiality

Some information is only known to some principals.

Security Properties

Privacy

Protection of personal information (also includes protection of personal space).

Security Properties

Availability

Some service or resource can be used within a particular time with particular quality.

Security Properties

- Authenticity
- Integrity
- Confidentiality
- Privacy
- Availability

plus other properties, e.g. safety

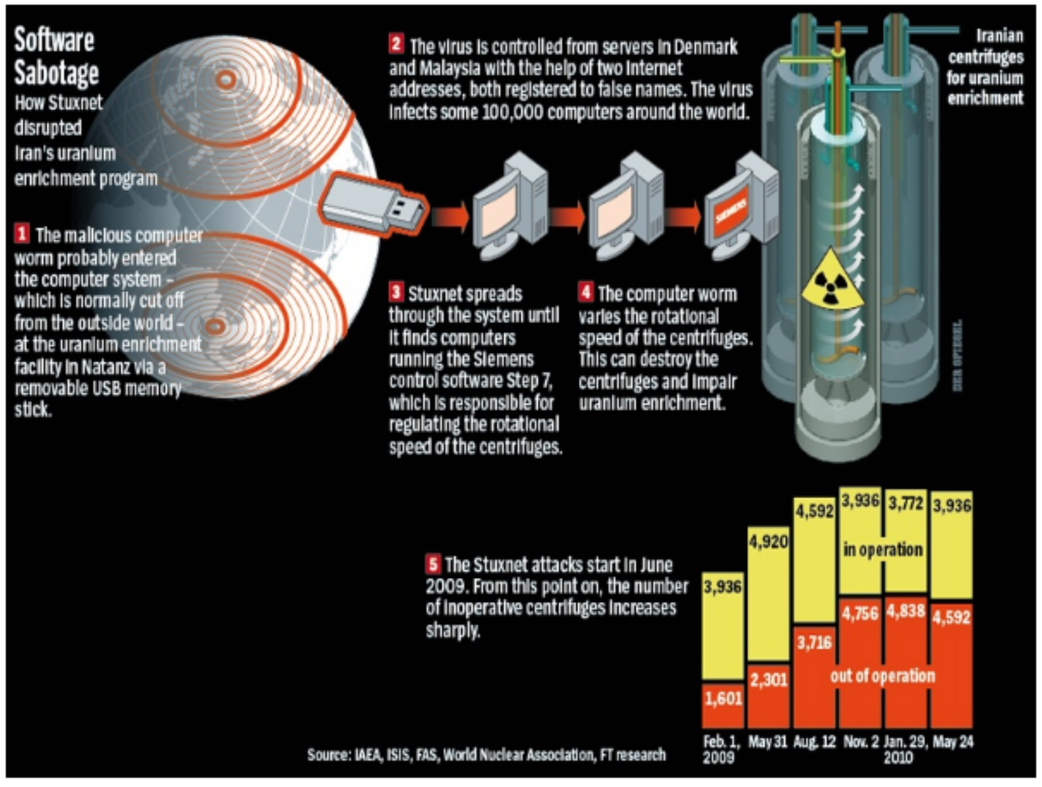
Attacks on industrial control systems

- Can cause physical damage and injuries
- Potentially affects critical infrastructures
- Control systems are more and more connected

Stuxnet - Attack on nuclear facilities in Iran

- A worm spreading between Windows PCs
- Target is Siemens programmable logic controllers PLC
- Amazingly sophisticated malware
- Bridges *air gap* to PLC during configuration of PLC from Windows computer
- Changed motor speed on centrifuges used to enrich uranium
- Apparently destroyed 900-1000 Iranian centrifuges in 2009/2010

Stuxnet



(Source: Der Spiegel)

Computer Worm

A computer worm is a standalone malware computer program that replicates itself in order to spread to other computers. It can use computer networks and other links (e.g. USB memory) to actively spread itself. Unlike a computer virus, it does not need to attach itself to an existing program, but it usually relies on weaknesses on the target computer.

An earlier example from 2008

In August 2008 a pipeline exploded in Turkey. None of the sensors and cameras monitoring each meter of the pipeline triggered any signal. Control rooms only learned about the blast 40 min after it happened.

(Photographer: Anatolian-Muhammet Ispirli/Corbis)

Main weapon was a keyboard

- Security camera system was hacked and used as entry point into the systems.
- Single infrared camera showed 2 men with laptops walking along the pipeline.
- Computers at small valve stations hacked and pressure in the pipeline increased.
- Units for sending alerts were tampered with.
- Super-high pressure destroyed the pipeline in a massive explosion. No evidence of explosives was found.

Attacking a bank on a large scale

- February 2016: The SWIFT network for international transfer of money between banks is instructed to transfer 951 Million US Dollar from Bangladesh Bank to various bank accounts.
- Five transaction were successful (101 Million US Dollar). Remaining transaction were blocked.
- Money was transferred to Sri Lanka (20 Million, later recovered) and the Philippines (81 Million).

How to find targets to attack?

Thi is (unfortunately) not very difficult.

Thousands of devices can just be found on the Internet.

Search engine Shodan:

Shodan **https://www.shodan.io/**

Lets look at Shodan

There is quite a number of spectacular attacks.
But: Many attacker dont go for large-scale breaches.
Most of them go for "low-hanging fruit".

Attacking the normal user

- Phishing
- Ransomware
- Botnets

Phishing

- Create a fake website with a login prompt
- Motivate a person to access this website (e.g. by fake mail)
- Person types in username and password that is now phished by the attacker
- For all types of services: Bank, Paypal, Enterprise access

Ransomware

- Install malicious software that e.g. encrypts all data
- Ask for money (BitCoin) to get data back
- Very professional

Ransomware - What to do?

- Don't panic! Try first to get more information.
- Some infections are easy to clean, or it is only scareware.
- A lot of useful information can be found.
- **https://www.nomoreransom.org/**
- You might need to re-install your system and restore from backup.

Bot

- Is derived from "robot"
- Automated process interacting with network services
- Malicious bots connect many devices to a command and control centre
- Gather information (camera, keystrokes, access information)
- Remote control, run distributed Denial of Service attacks
- Botnet

Denial of service attacks, Distributed DoS

- Attack that prevents a service from working
- From inside a computer through a virus/trojan horse
- From outside by massive requests/traffic (e.g. using a Botnet, i.e. a network of bots)

Viruses, Worms, Trojans

Different types of malware with different ways how to spread and different tasks.

Virus

- Inserts itself into another program/document
- Gets distributed with the program/document
- Runs and spreads, when the host program is executed
- Might try to load additional malware/rootkits etc.

Worm

- Similar to a virus, but is a standalone program
- Uses weaknesses in the system or tricks the user into executing the worm
- Once it is running it can spread via networking, file transfer, etc.

Trojan

- Malware hidden in a seemingly legitimate piece of software
- Many different variants, creating backdoors to give attackers access, manipulate banking, activate additional malware,etc.

A malicious program on your computer automatically starts whenever you boot. Then, if you plug in a USB drive, it copies itself to the drive in order to spread to other devices. What type of malware is this?

A. Botnet
B. Virus
C. USB Poisoner
D. Worm
E. Spider

Feed:

A malicious program on your computer automatically starts whenever you boot. Then, if you plug in a USB drive, it copies itself to the drive in order to spread to other devices. What type of malware is this?

A. Botnet
B. Virus
C. USB Poisoner
D. Worm
E. Spider

Feed:

Do only careless people get malware?

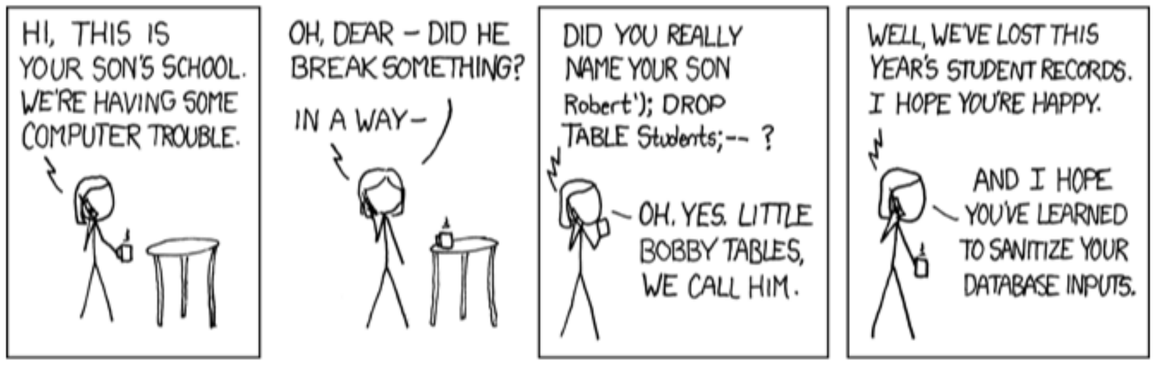
- Careless people probably get malware more often.
- But: Malware can spread without user interaction!
- E.g. via active content (flash) in advertisement on normal news websites (e.g. using Angler exploit kit in ads at BBC, New York Times, AOL, NFL in March 2016).
- But: Anti-malware programs, up-to-date with security updates, backups, etc. do help.

Virus Scanner - Anti-Virus Software

Virus Scanner - Anti-Virus Software

- Anti-Virus Software can efficiently prevent infections with known malware.
- Is the first thing to be manipulated by malware.
- Unable to detect new malware.

There are many ways to attack systems



(xkcd.org)

For explanations look here:
https://www.explainxkcd.com/wiki/index.php/327:_Exploits_of_a_Mom