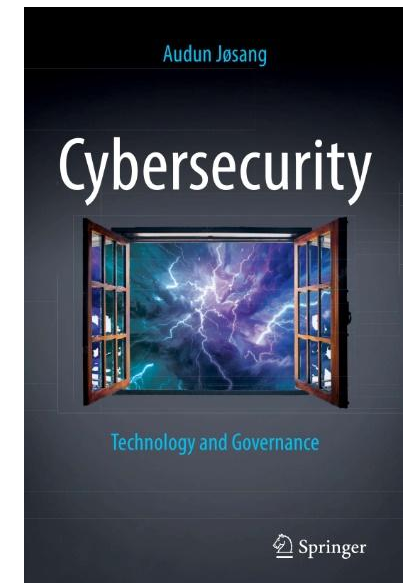


Chapter 2: Attack Vectors and Malware

Cybersecurity: Technology and Governance

Audun Jøsang,

1st Edition, Springer Nature, 2024.



Overview

- Threat actors
- Attack vectors
- Malware

Threat actors

	Threat actor	Motivation
1)	States and state-sponsored organizations	Geopolitical interests
2)	Cybercriminal organizations	Financial gain
3)	Hacktivists	Ideological interests
4)	Terrorist organizations	Violent ideological interests
5)	Thrill-seeking amateur hackers	Desire for excitement and recognition
6)	Insider attackers in organizations	Dissatisfaction, financial gain, or ideology

Attack vectors

Illegal tracking and wiretapping, e.g. of mobile phones, or illegal tracking of users through apps and websites.

Traffic overload against websites so that legitimate traffic is blocked.

10

Insider attacks.



12

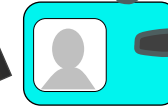


1

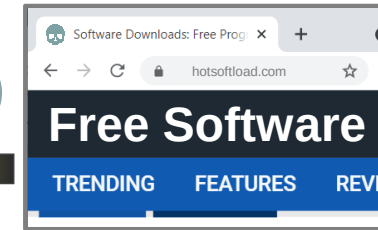
Phishing emails, SMS and messages with malware or links to malicious websites.

2

ID spoofing with cracked or stolen credentials.



3



Fake and malicious websites that send malware or steal credentials.

4



Physical theft, damage, tampering and breach of IT devices or sites.

6



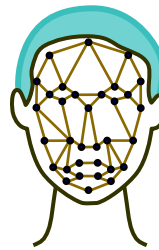
Supply chain attacks

7



Malicious peripherals.

9



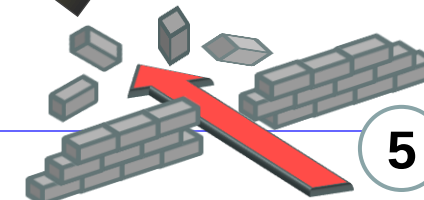
Deepfake audio and video to spoof identity in online meetings or in biometric authentication.

8



Hacking IoT devices.

5



Direct attacks against vulnerable systems and applications.



Phishing attack



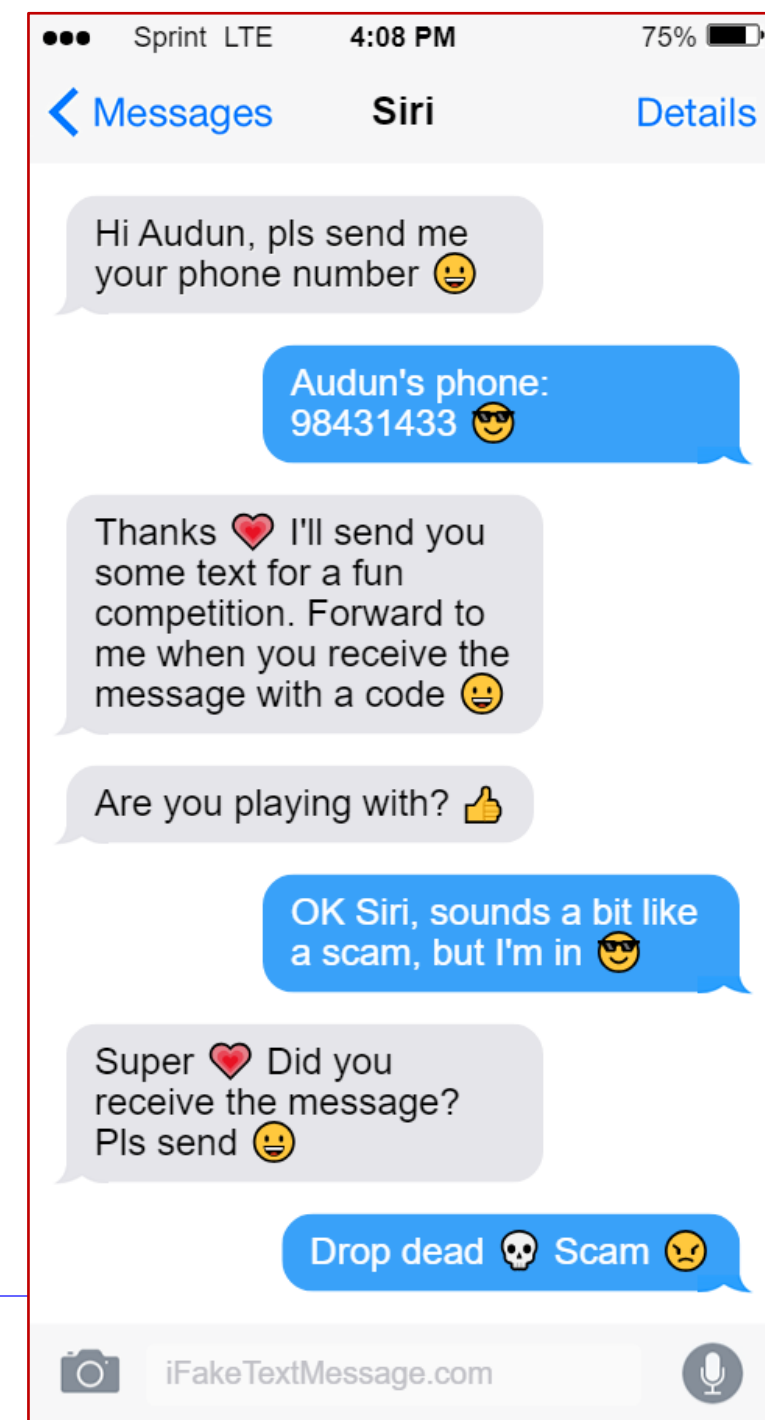
- Phishing is a type of social engineering.
- Can be sent as email, SMS or other messages.
- For example, a phishing email is designed to trick the recipient into providing sensitive information, visiting a fake website, or installing malware.
- From around 2015, phishing became the most common attack vector for cyber attacks and cybercrime on the Internet.
- Security culture, knowledge and awareness of phishing methods are important to prevent this type of attack.

Categories of Phishing Attacks

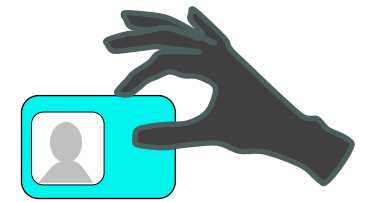
- Mass phishing
 - Large volume intended to reach as many people as possible
- Spear-phishing
 - Targeted at specific people or businesses
- Whaling
 - Spear-phishing targeting "big fish" (e.g., rich, high-profile, access to a lot of money,...)
- Clone phishing
 - Copy of legitimate message/email where links/attachments have been replaced by malicious versions

Other forms of social engineering

- Ask nicely
 - People are generally helpful and give away a lot of information
- Trick people into giving you access
 - «Hi, I'm calling from Microsoft»
 - Get hold of "secrets" to reset forgotten passwords
- Fake access cards
 - Gives a sense of connection
 - "you and I have something in common, and therefore I trust you"
- Use of stolen/fake accounts on social networks
 - You think you're getting a message from a friend, but actually it's an attacker who has stolen your friend's identity
 - If that happens, contact your friend through another "secure" channel, e.g. regular phone



ID spoofing through stolen credentials



- Stealing identities and credentials is perhaps the most attractive threat tactic.
- Spoofed identities provide a myriad of hard-to-detect attack opportunities.
- A goal high on the priority list of attackers is to steal data-bases with user IDs and credentials. Such databases are being offered for sale or are being published on the dark web.
- Passwords are typically not stored in cleartext, but in hashed form, as described in Ch.4. However, cleartext passwords can be recovered through password cracking described in Ch.8.
- Forging biometrics is described in Ch. 8. Forging face and fingerprints is relatively easy, or can be stolen from a sleeping or drugged victim.
- Mobile phone numbers represent a strong form of identity that can be stolen e.g. with SIM swapping attacks, as described in Sect. 7.4.6.

Unwitting installation of malware

- Tricking users into installing malicious programs through websites or other storage media can be used as part of attacks.
- The user may be tricked into installing malware in the belief that the software is legitimate.
- There are many different types of malware.
- Trojans (Trojan horses) are a type of malware that actually have a useful function, but at the same time has hidden malicious functions.
- To avoid malware, only download from reputable websites and check valid digital signatures.



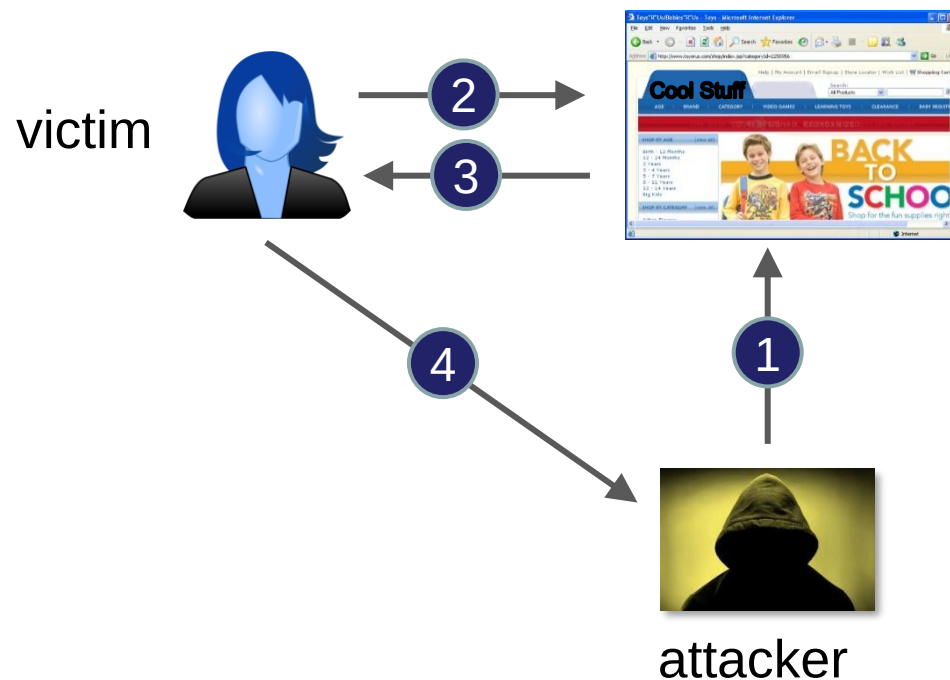
Drive-by Attacks



- Many different scenarios for drive-by attacks.
- In general, drive-by attacks happen without the user having to click on anything, explicitly download anything, or open any attachment for the client to get infected. The user only needs to visit the website to be attacked.
- Could be a regular website infected by a threat actor, or a fake website controlled by a threat actor.
- Possible scenarios are:
 - Direct download of malicious JavaScript
 - Redirecting to fake website

Drive-by attacks – example scenario

XSS (Cross Site Scripting) is an attack where a malicious script is injected into a website (which otherwise is benign).

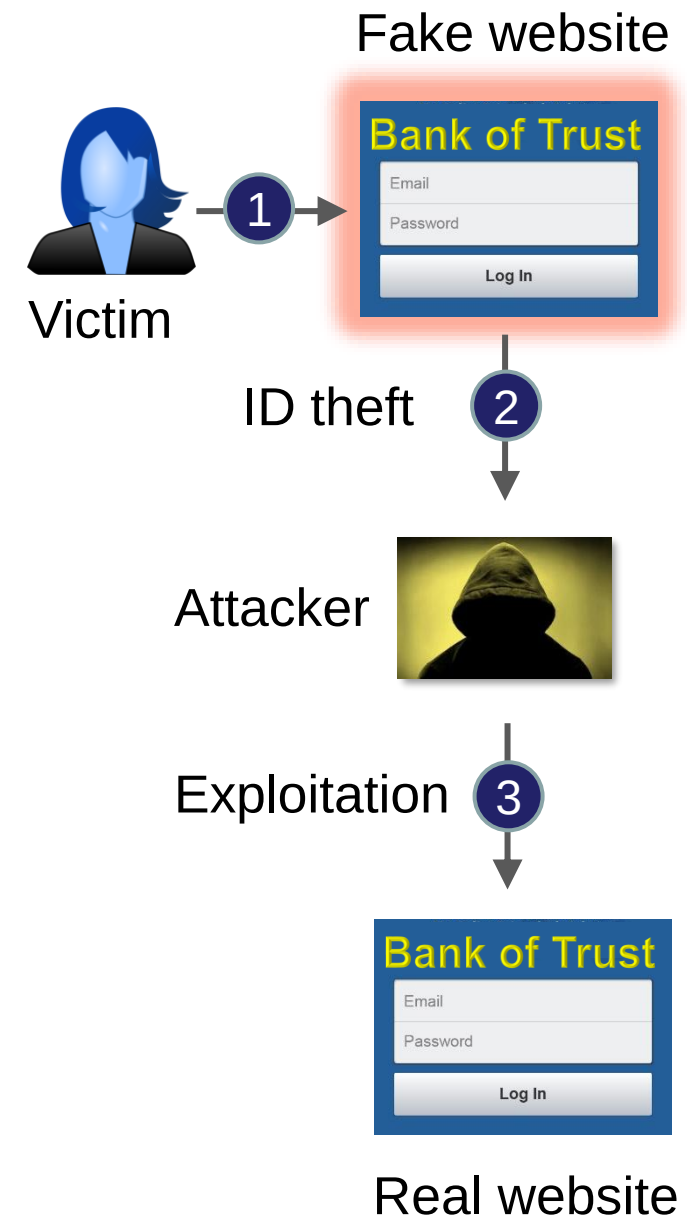


Scenario of direct download of malicious JavaScript, e.g. as a result of an XSS vulnerability on a web page.

1. Attacker injects malicious script
2. Victim visits the website
3. Malicious script sent to browser
4. Browser steals and sends sensitive data to attacker

Fake websites

- *Fake websites* can appear indistinguishable from real websites.
- Users may be misled into visiting a fake website, e.g. through phishing emails, through other fake or infected websites, or through malicious advertising.
- A user who has landed on a fake website may be tricked into providing their user ID and password or other sensitive information.
- The attacker can then use the stolen user ID to visit the real website and log in as the user.
- Ways to avoid fake websites are to not click on links in messages, or to carefully check the website's URL and certificate.



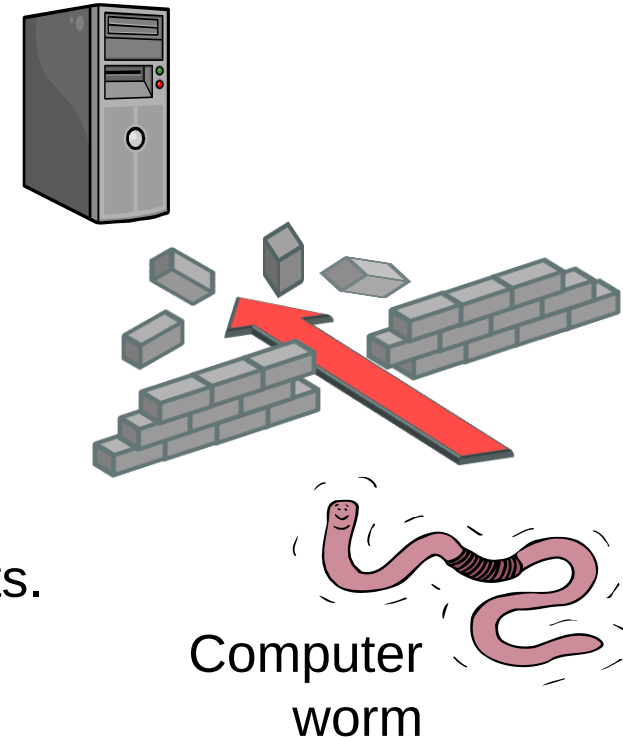
Physical attacks against IT infrastructures



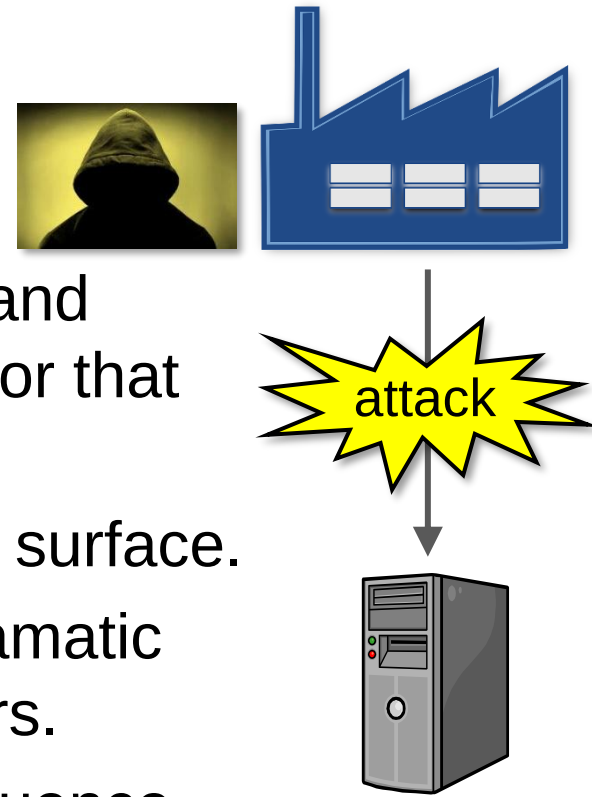
- Most technological security controls can be bypassed with physical.
- Essential to design physical barriers to prevent physical entry and tampering.
- Physical entry into buildings can e.g. performed by lockpicking, with brute force, or through social engineering.
- Breaking into devices and accessing data or executing functions can be done e.g. forging biometric credentials, or by opening up the casing where hardware components get exposed and can be tampered with.
- The last layer of physical protection is on the device itself, where robust authentication and tamper resistant/proof casing are possible techniques.

Direct network attacks

- Typical attacks against vulnerable web applications are e.g. SQL-injection and XSS (Cross-Site Scripting).
- Weak passwords can be cracked with password spraying, which means automatically trying typical passwords against many different user accounts.
- Spreading of malware can take place, for example, through a worm that automatically infects other computers through the internet.
- A computer worm exploits unknown or unpatched vulnerabilities to infect computers, and in turn uses them as spread further. This triggers a chain reaction that can quickly cause exponential infection rates.
- In addition to seizing significant bandwidth through spreading, worms can have serious intentional harmful effects.

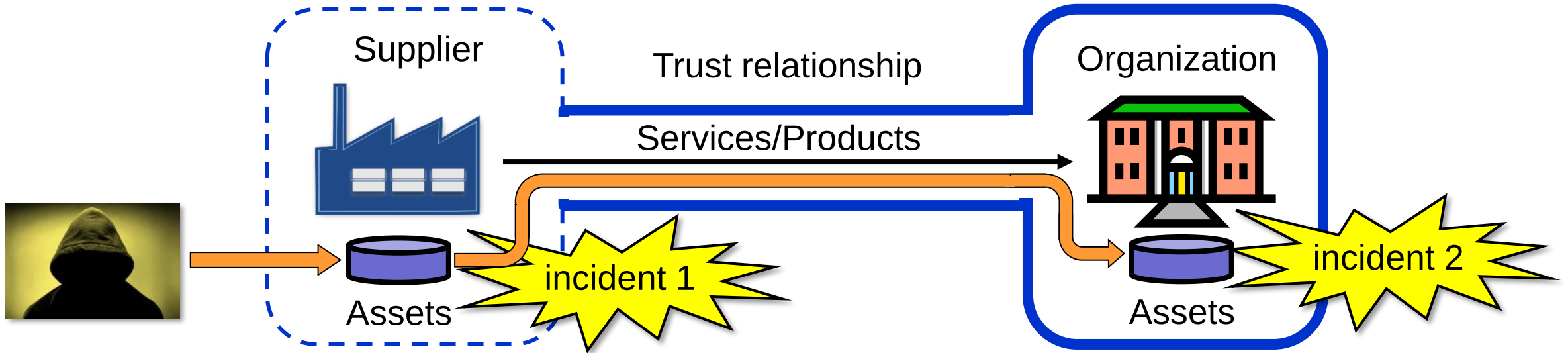


Supply chain attacks



- *Supply chain attacks* mean that attackers can infiltrate systems and networks through an external partner or vendor that has access or that supplies components within the organization's IT infrastructure.
- From a security perspective, supply chains are part of the attack surface.
- The reliance on long and complex supply chains has led to a dramatic enlargement of the attack surface of organizations in recent years.
- Any entity that contributes to a supply chain has the ability to influence security further up the supply chain.
- The longer and more complex the supply chain, the harder it is to get an overview of threats and vulnerabilities, and the harder it becomes to manage security incidents.

Supply chain attack illustration

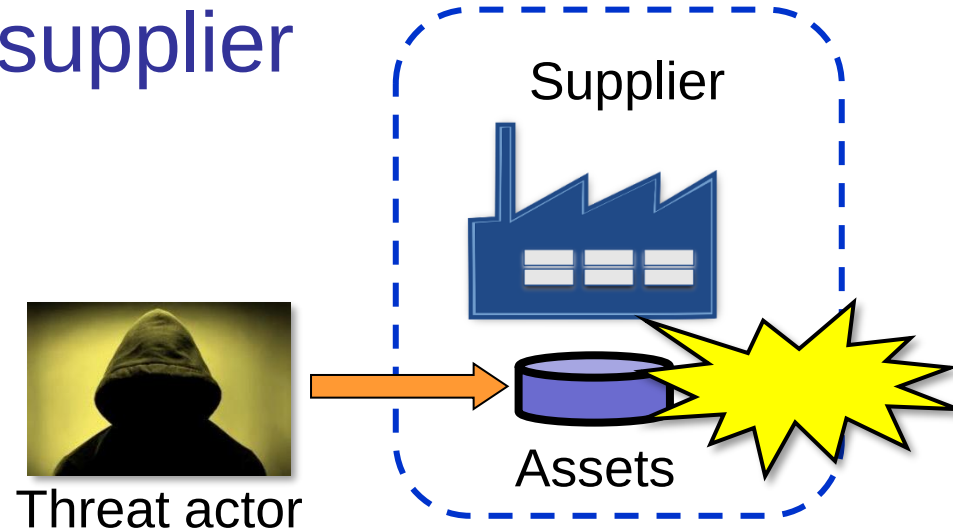


- Companies often have relatively good security, while suppliers can have relatively poor security
- Attacker chooses the weakest link in the chain
- Supply chain attacks happen in several stages
 1. The supplier is attacked, resulting in compromised products or services
 2. Companies that use compromised products/services from suppliers become vulnerable
 3. Vulnerable companies are being attacked

The threat actor's attack targets at the supplier

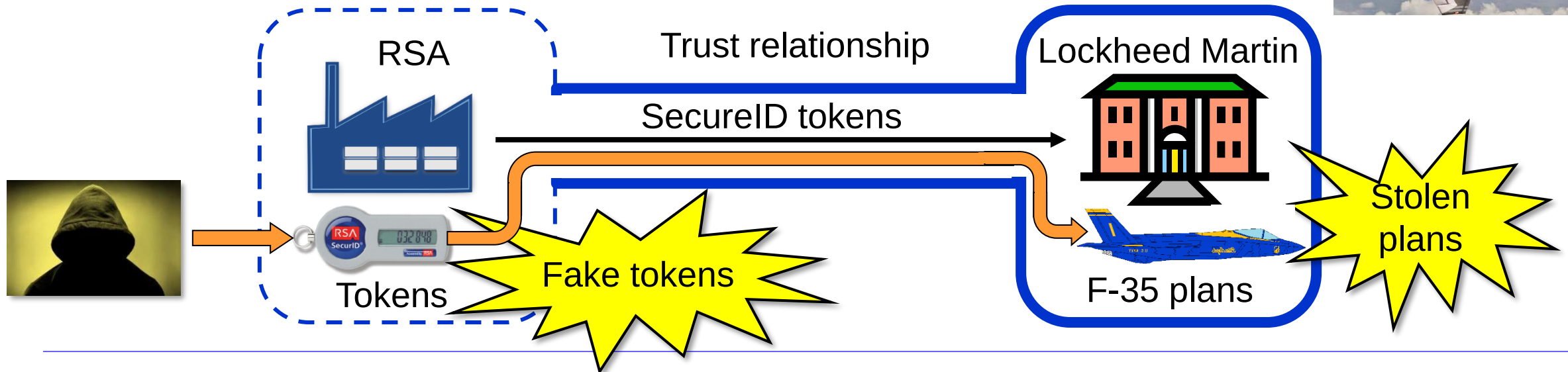
Threat actors will typically attack:

- Software developed by the vendor
- Configurations
 - e.g. passwords, API keys, firewall rules, URLs
- Data
 - e.g., confidential information, cryptographic keys, certificates, CRM data, personal data of vendor staff or customer employees
- Processes
 - e.g. update processes, backup processes, digital signature processes
- Hardware manufactured by the supplier
- ID theft of people with privileged access to data and infrastructure



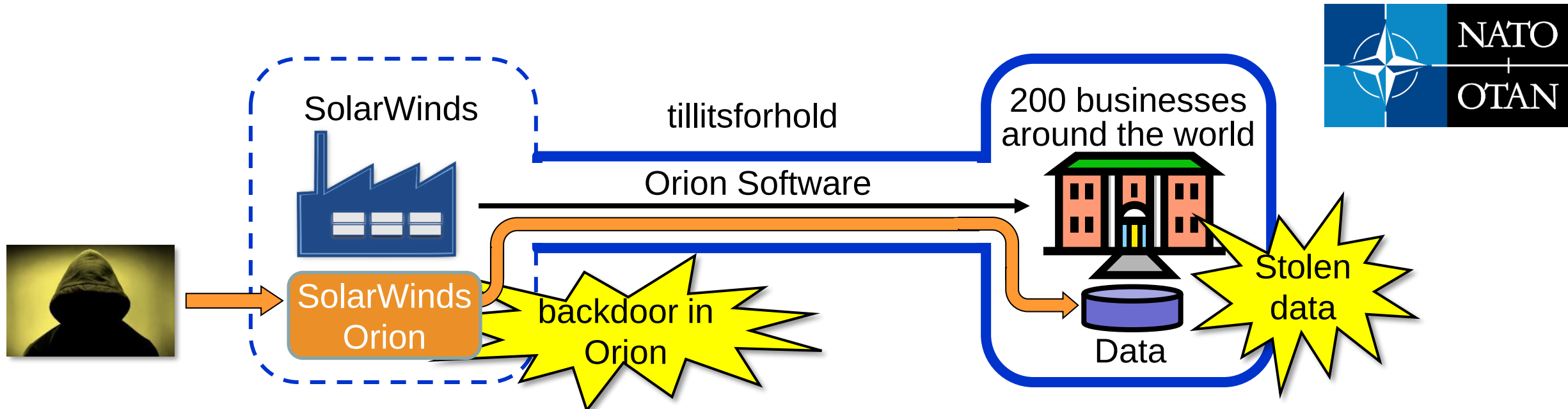
Fake SecureID chips for spoofed login

- RSA was hacked in 2007, lost sensitive data for SecureID chips
- Hackers created fake SecureID chips to spoof 2FA logins
- Companies that used 2FA with SecureID were vulnerable
- Lockheed Martin used SecureID for 2FA (2-Factor Authentication)
- Chinese attackers spoofed Lockheed Martin employees
- Stole plans for F-35 fighter jets



Manipulating SolarWinds Orion Software

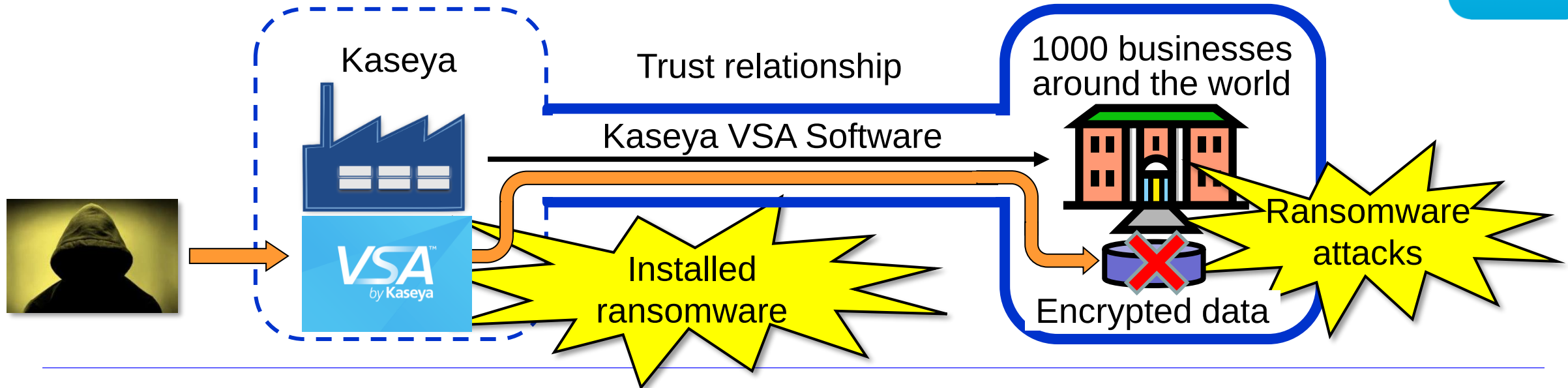
- SolarWinds was hacked in 2020
- Hackers installed backdoor in Orion network management software
- 18000 businesses worldwide using SolarWinds Orion software were vulnerable
- At least 200 businesses were attacked, including NATO
- The attack is believed to come from a Russian APT group



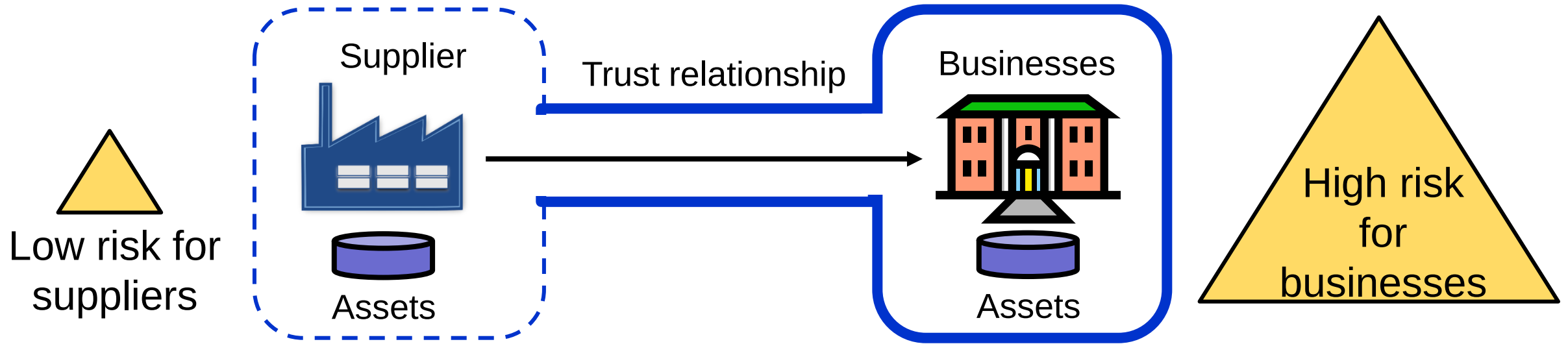
Manipulating the Kaseya VSA software



- Authentication vulnerability in Kaseya VSA (Virtual System Administrator) software
- Hackers installed ransomware in Kaseya VSA software
- Thousands of organisations around the world use Kaseya CSR
- At least 1000 companies worldwide fell victim to ransomware attacks, including Coop
- Coop Sweden had to close 800 stores for 1 week
- Attributed to the Russian REvil APT group



Market failure for supply chain risk management



- Suppliers may have low risk and thus little incentive to implement strong (and expensive) security controls
- Businesses may be at high risk, but few opportunities to implement effective security controls against vulnerabilities in the supply chain

Malicious peripherals

Malware



- For example, malicious peripherals can be plugged into the USB connector and used in attacks.
 - For example, a device may contain malware that the user installs out of curiosity.
 - A USB flash drive is configured as a Human Interface Device (HID), which tricks the computer into thinking it's a keyboard and sends a stream of keystrokes that constitute malicious commands.
 - USB charging connectors in public places may have been manipulated to send malicious commands.
 - A drop attack is when the attacker leaves harmful USB sticks, e.g. in cafes, and waits for someone to find them and plug them into a computer.

Stuxnet

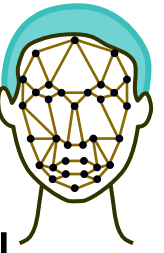
- Data worm/rootkit
Multiple zero-day vulnerabilities
- Attacked one of Iran's nuclear facilities in 2010
- Crossed the "air-gap" through transfer via USB
- The US and Israel (probably) behind the attack

Hacking vulnerable IoT devices



- While regular computers with full-fledged operating systems like Windows or Linux get regular security updates and patching to fix software bugs and security vulnerabilities, IoT devices are usually never updated after they have been manufactured and installed. The absence of full-fledged operating systems in IoT devices makes it technically difficult or impossible to perform online software updates on them.
- A smart home or an industrial facility with unpatchable and vulnerable IoT devices connected to the Internet can be an easy target for hackers.
- Many countries are aware of this problem. As the first country in the world to regulate IoT security, the UK introduced the Product Security and Telecommunications Infrastructure (PSTI) regime in April 2024.

Deepfake



- Tools based on ML allow an attacker to speak in a way that sounds like you, or act in a video meeting with a face and voice like you.
- Deepfake refers to the fact that fake sound and image are generated by technology based on deep neural networks (DNNs).
- For example, an attacker can spoof the identity of the company's director during an online meeting, and instruct an employee with high authorizations to transfer a large sum of money to an account controlled by the attacker.
- Alternatively, the attacker can spoof the identity of a company employee during a video meeting and send a chat message with a link to a malicious website. Because colleagues know and trust the employee, they will typically click on the link.
- Deepfake can also be used to spoof biometrics.

Insider attacks



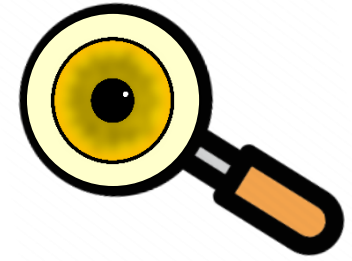
- Insider attacks are attacks that are committed by an employee or other person who is authorized to access the company's systems and data.
- An “insider” is the jargon typically used for such people.
- Insider attacks can be very damaging because the attacker has knowledge and access rights to systems and assets, so that typical security measures have limited benefit.
- In addition, insider attacks can be very difficult to detect because the attacker often knows how to hide traces.

DDoS - Denial-of-Service Attacks



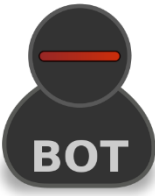
- A DDoS attack means that a website is bombarded with artificial traffic that overloads the web server which can no longer serve legitimate traffic.
- DDoS traffic is typically generated by botnets.
- Stopping DDoS traffic can be difficult and resource-intensive.
- Three main categories of DDoS attacks
 - Volumetric attacks are aimed at exhausting the capacity of the victim server's network by sending massive amounts of Internet traffic towards it
 - App layer attacks exhaust the victim server's CPU resources. The effectiveness of this attack comes from the asymmetry between the amount of CPU resources it takes to send a fake request relative to the amount of resources it takes to process it at the server end.
 - Protocol attacks exhaust the memory and CPU resources at the Transport or Internet layer of the victim server node. The attacker typically sends large amounts of malformed packets in a way that forces the server to use up all its memory, or to spend CPU time.

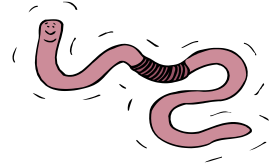
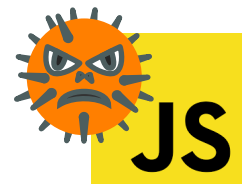
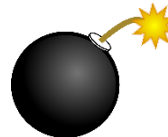
Illegal tracking and spying



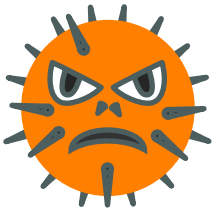
- There are many forms of tracking and spying
 - Mobile phones can be tracked with IMSI catchers (see chapter 7 on wireless security)
 - Websites and apps can be used to track and map users, which may be legal or illegal (e.g. under the GDPR), depending on how it is done and how users are informed (see chapter 10 on privacy).
 - TEMPEST is a collective term for all types of electronic surveillance, and measures against this. See chapter 3, specifically about side channels and covert channels. See also chapter about physical security. For example, the reflection of laser light against a window can be used to eavesdrop on conversations in the room behind the window. This is possible because the sound waves cause the glass to vibrate, which can be detected with the reflected laser light.

Malware

- 1) Computer virus 
- 2) Ransomware 
- 3) Spyware 
- 4) Bot program 
- 5) Exploit 
- 6) Makro virus 

- 7) Trojan 
- 8) Computer worm 
- 9) Rootkit 
- 10) Backdoor 
- 11) Malicious JavaScript 
- 12) Logic bomb 

Computer virus



- A computer virus infects a computer program by merging malicious code into the code of the program.
- The virus is executed only when the infected program is executed.
- The fact that a virus is intertwined with another program makes it particularly difficult to remove, and even the best antivirus programs struggle to do this correctly.
- Viruses were very widespread during the 1990s and 2000s.
- Pure computer viruses are less uncommon today, accounting for less than 10% of all malware.
- Note that the term "virus" is often used as a generic name for all types of malware, which can be confusing.

Ransomware



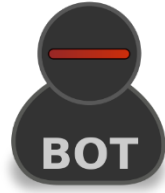
- Ransomware is a type of malware that, in the first stage, encrypts all, or a selection, of critical data on the victim's computer, making data and applications inaccessible.
- This is a form of denial-of-service attack that leads to breach of availability.
- The attacker follows up the first step by blackmailing and demanding a ransom to hand over the decryption key.
- Extortion can also be based on a threat to make the data public if a ransom is not paid. This can be a threat to privacy.
- Double Extortion is when the attacker both encrypts and threatens to publish
- Readiness against ransomware is to make regular backups of all important data, and have good recovery routines.
- However, backup does not protect against threats to publish stolen data.

Spyware



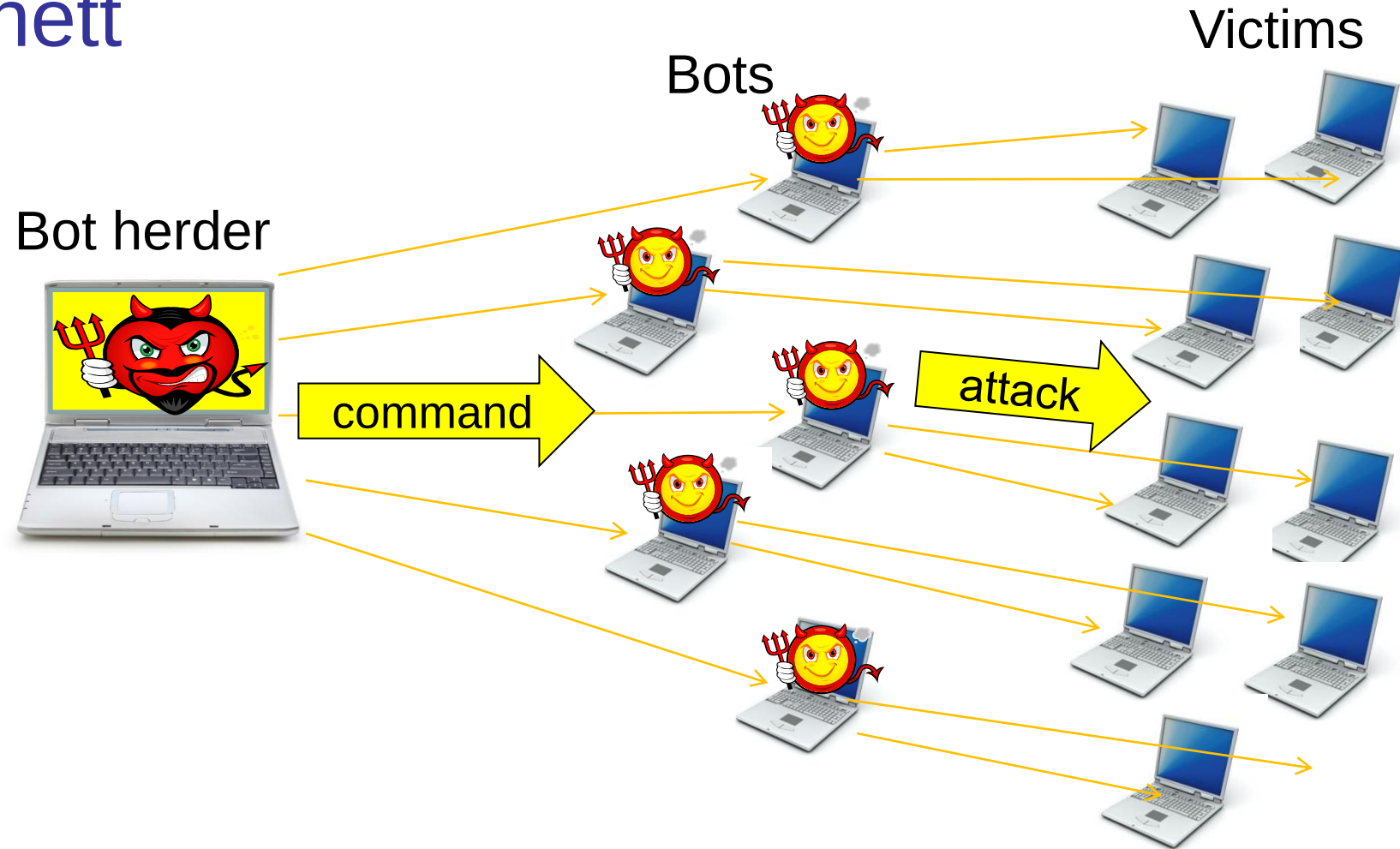
- Spyware and adware are programs that spy on the user or display advertising to the user.
- A keylogger is a type of spyware that logs keystrokes, allowing the attacker to steal passwords and other sensitive information.
- Such programs are often installed through some form of social engineering combined with one of the attack vectors, and they usually start every time the system starts.

Bot malware



- A computer infected with bot malware is called a bot, from "robot", i.e. something that runs automatically.
- Bot malware can be used for legitimate purposes
 - e.g. search engines to perform indexing.
 - Unfortunately, bot software is often used as malware by attackers.
- Bot malware is typically self-replicating, and is capable of receiving commands from a centralized or distributed bot herder. Attackers infect computers in large numbers to create a botnet that can carry out different types of attacks.
 - E.g., DDoS attacks or cryptocurrency mining with victims' electricity and computing resources.

Botnett



Mirai is (a computer worm that) is an example of botnet, with a focus on IoT devices and DDoS attacks.

Exploit



- An exploit is a small program, a string of data, a file, or a sequence of commands that exploits one or more bugs or vulnerabilities in a software, hardware, or other computer equipment to trigger corrupt or abnormal behavior.
- An exploit often triggers a buffer overflow (see the chapter 3 on system security)
- The attacker's purpose in triggering such behavior may be, for example, to gain control of a system, download backdoors, gain unauthorized access, or to carry out a denial-of-service attack.

Macro virus



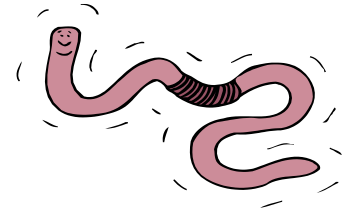
- Macros are used to automate functions in Office documents.
- However, attackers can hide malicious Office macros in Office files that are sent as attachments to phishing emails, for example.
- These files often have names that are meant to lure or scare people into opening them, and typically look like invoices, receipts, legal documents, etc.
- In the past, Office macros ran automatically, but not anymore. Now, the attacker needs to trick users into enabling macros in order for them to run.

Trojan



- Trojans masquerade as legitimate programs that actually (or apparently) have useful features, but at the same time have hidden malicious features.
- Trojans are popular among hackers and have mostly replaced computer viruses.
- Trojans are typically downloaded from criminal or infected websites, or come as an attachment to phishing emails.
- The user is tricked into believing that the program is useful and explicitly chooses to install it.
- It is ironic that fake antivirus programs are a widespread type of Trojan.

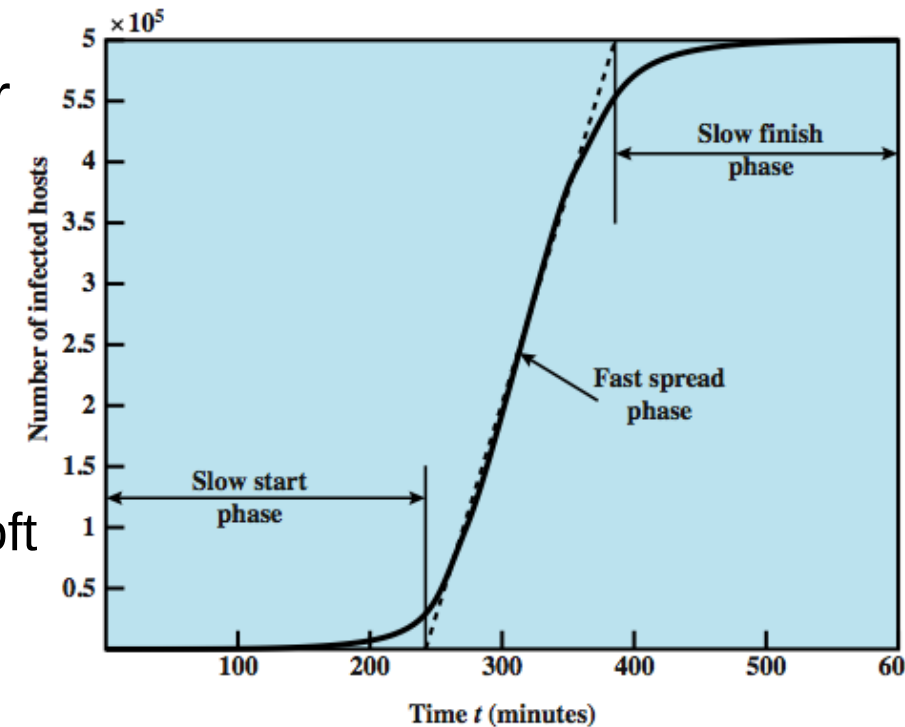
Computer worm



- Computer worms spread themselves to other computers within a computer network or across the internet in an automatic manner, usually without user interaction.
- Worms do this by connecting to other host nodes and exploiting vulnerabilities in programs that are exposed to the internet.
- Can be very destructive because they spread without user participation. Viruses and Trojans require at least a user to launch a program.

Examples of computer worms

- The Morris computer worm (1988) created by a student called Robert Morris was the first computer worms on the internet
- Stuxnet
- Wannacry & NotPetya
- SQL Slammer worm
 - In January 2003, the worm infected about 75,000 Microsoft SQL servers in only 10 minutes
 - shows its exponential infection rate.

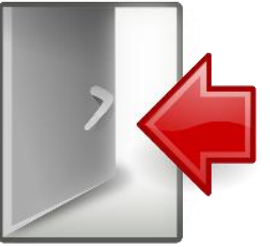


Rootkit



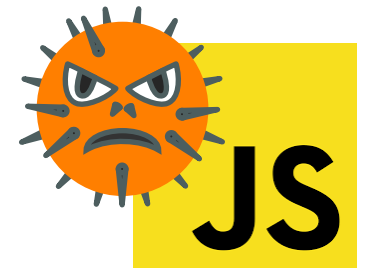
- Rootkit is a type of software that the attacker installs to hide the attacker's or malware's presence in the system
 - The name comes from the term "root", the most privileged user account in LINUX
- Typically, a rootkit will modify the process list to hide the malware
 - or it hides backdoors
 - or it hides fake users created by the attacker

Back door



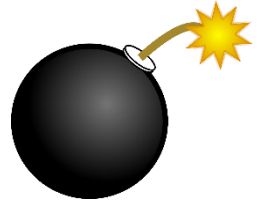
- A backdoor is a hidden method of bypassing normal authentication and access control in a system.
- Backdoors have legitimate uses, such as providing the manufacturer of systems and software with a way to perform maintenance and service.
- A backdoor can also be used by attackers to gain unauthorized access to systems.
- A backdoor can be a hidden part of a program, a separate program, code in the firmware of the hardware, or a part of the operating system.
- A malware backdoor can be installed by a Trojan or by an exploit, for example.

Malicious JavaScript



- Most websites contain JavaScript that is automatically downloaded and executed in the browser when a user visits the website.
- Typically, JavaScript is perfectly legitimate and is used for advanced functions on a web page, but it can also perform malicious functions, such as downloading an exploit from a website controlled by the attacker.
- JavaScript can also be abused to get the browser to mine cryptocurrency for the attacker or to steal sensitive information that is sent to the attacker.
- Malicious JavaScript can be injected into web pages through XSS attacks.
- Since JavaScript is executed automatically and completely without interaction when the user visits a website, JavaScript is typically used for drive-by attacks.

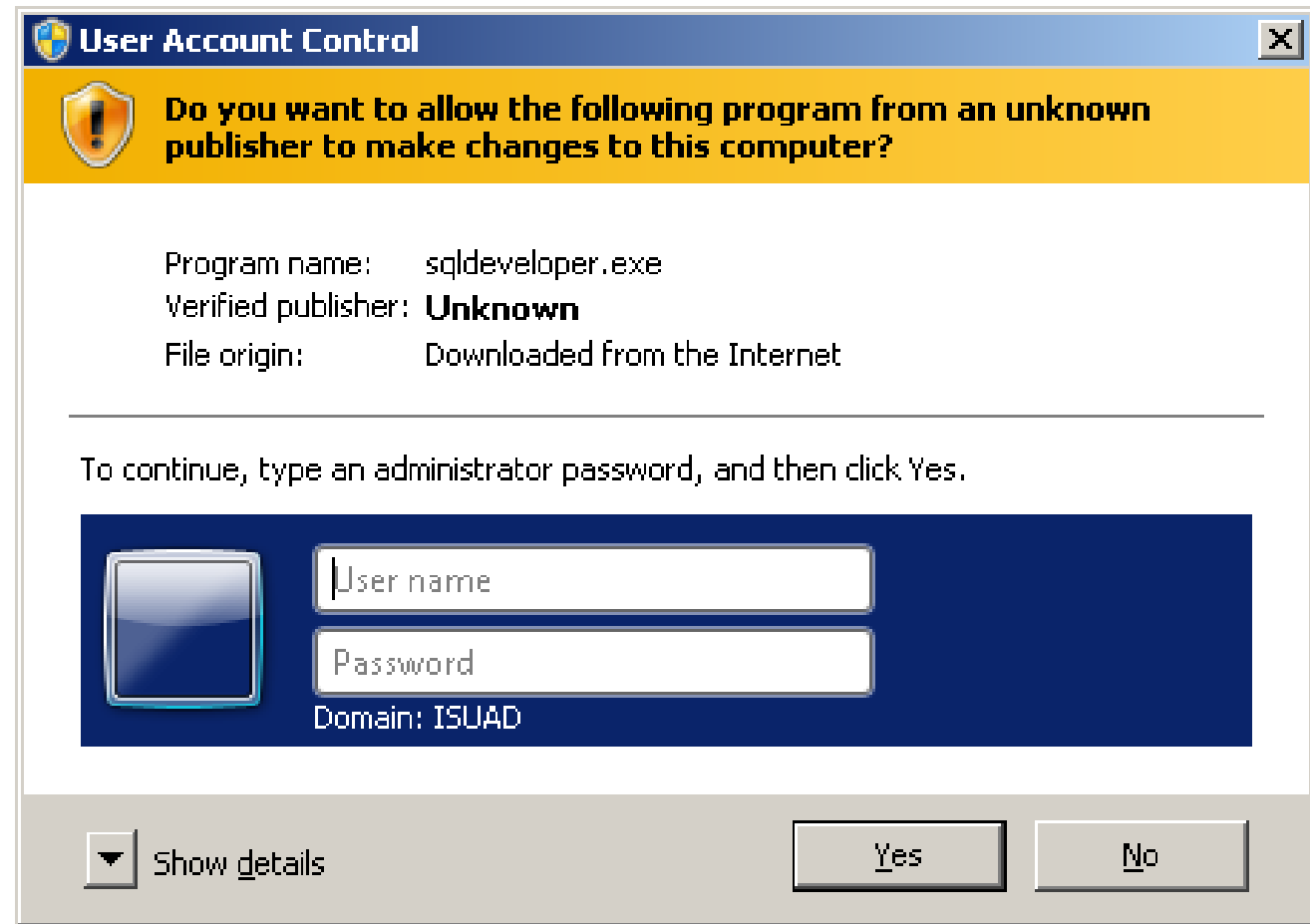
Logic bomb



- Logic bombs are one of the oldest types of malware
- Logic bombs are code embedded in a legitimate program, or a program that runs in the background.
- Malicious functionality is activated when certain conditions are met, e.g.
 - presence/absence of a file
 - specific date/time
 - Specific user
- Logic bombs deal damage when triggered:
 - change/delete files/disks, stop the machine, etc.
- Logic bombs are typically made by an insider

What access rights does the malware have?

- Exploits and other malware get the same access as the user/service being attacked
 - I.e.: if you run malware as a user, the malware gains user access.
 - If you run the malware as an administrator, the malware gets administrator access.
 - Therefore, security mechanisms such as UAC (User Account Control) are used.



End of presentation

