

CT437 COMPUTER SECURITY AND FORENSIC COMPUTING

DEFINITIONS, TERMINOLOGY, AND CASE STUDIES

Dr. Michael Schukat



What is Cybersecurity?

2

- Computer security, cybersecurity or information technology security (IT security) is the protection of computer systems and networks from the theft of or damage to their hardware, software, or electronic **data**, as well as from the **disruption or misdirection of the services they provide** (Wikipedia), i.e.:
- Protection from cybercrime of
 - ▣ data (from theft or manipulation)
 - ▣ services (from disruption or misuse)
- This protection can be on a personal, organisational or government level

States of Data

3

- Data at rest
 - ▣ Rest refers to data stored in memory or on a permanent storage device such as a hard drive, solid-state drive or USB drive
- Data in process
 - ▣ Processing refers to data that is being used to perform an operation such as updating a database record
- Data in transit
 - ▣ Transmission refers to data traveling between information systems, e.g. data transfer over a network via TCP/IP

How to provide Protection?

4

- **Awareness, training and education** are the measures put in place by an organisation to ensure that users are knowledgeable about potential security threats and the actions they can take to protect information systems
- **Technology** refers to the software and hardware-based solutions designed to protect information systems such as firewalls, which continuously monitor your network in search of possible malicious incidents
- **Policy and procedure** refers to the administrative controls that provide a foundation for how an organization implements information assurance, such as incident response plans and best practice guidelines

Defense in Depth

5

- Defense in Depth (DiD) is an approach to cybersecurity in which a series of defensive mechanisms are layered in order to protect assets
- If one mechanism fails, another one steps up immediately to thwart an attack



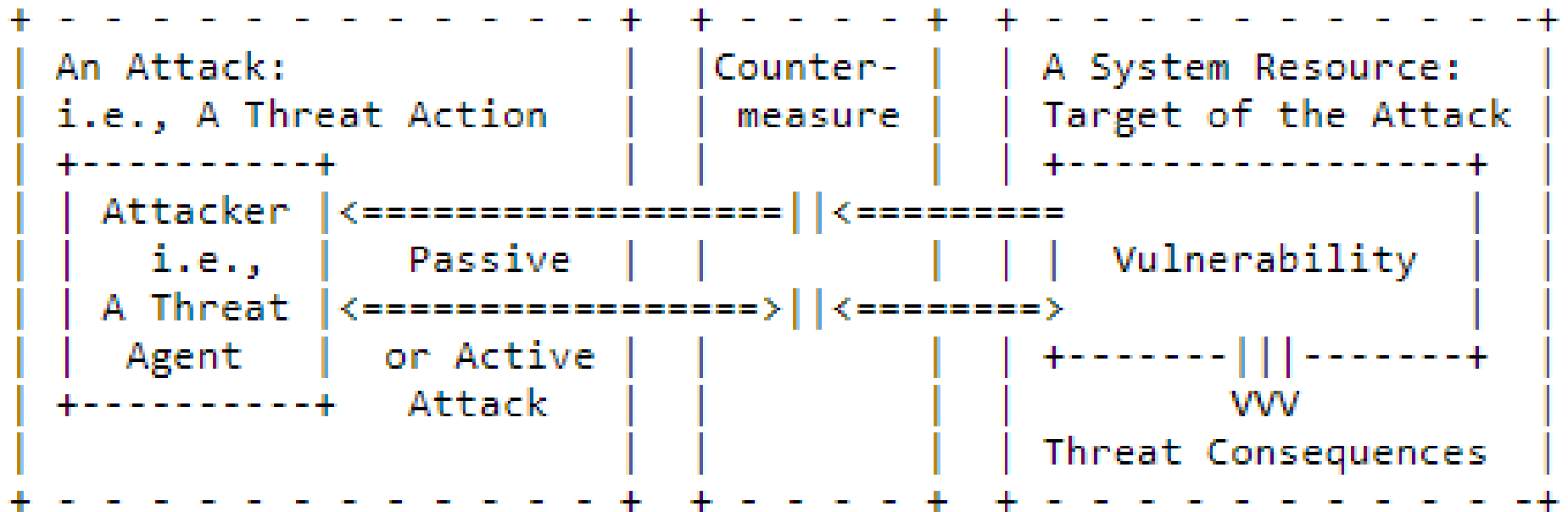
European Union Agency for Cybersecurity (ENISA)

6

- ENISA is the Union's agency dedicated to achieving a high common level of cybersecurity across Europe
- <https://www.enisa.europa.eu/>
- ENISA threat landscape report: <https://www.enisa.europa.eu/topics/cyber-threats/threat-landscape>
- ENISA has also issued a 2024 report *providing policy makers at EU level with an evidence-based overview of the state of play of the cybersecurity landscape and capabilities at the EU, national and societal levels, as well as with policy recommendations to address identified shortcomings and increase the level of cybersecurity across the Union current threat landscape (see also Canvas)*

The big Picture – RFC2828

- RFC2828, Internet Security Glossary
- <https://tools.ietf.org/html/rfc2828>



What is a Threat Agent/Actor?

8

- The term *threat agent* or *threat actor* is used to indicate an individual, thing or a group that can manifest a threat
 - ▣ In computer security, a threat is a potential negative action or event facilitated by a vulnerability that results in an unwanted impact to a computer system or application
- Threat actors include:
 - ▣ Non-target specific, e.g. computer viruses, worms, trojans and logic bombs.
 - ▣ Employees, e.g. disgruntled staff or contractors
 - ▣ Organized crime and criminals
 - ▣ Corporations, e.g. partners or competitors
 - ▣ Human, unintentional (including accidents and carelessness)
 - ▣ Human, intentional
 - ▣ Natural, e.g. flood, fire, lightning, meteor, earthquakes

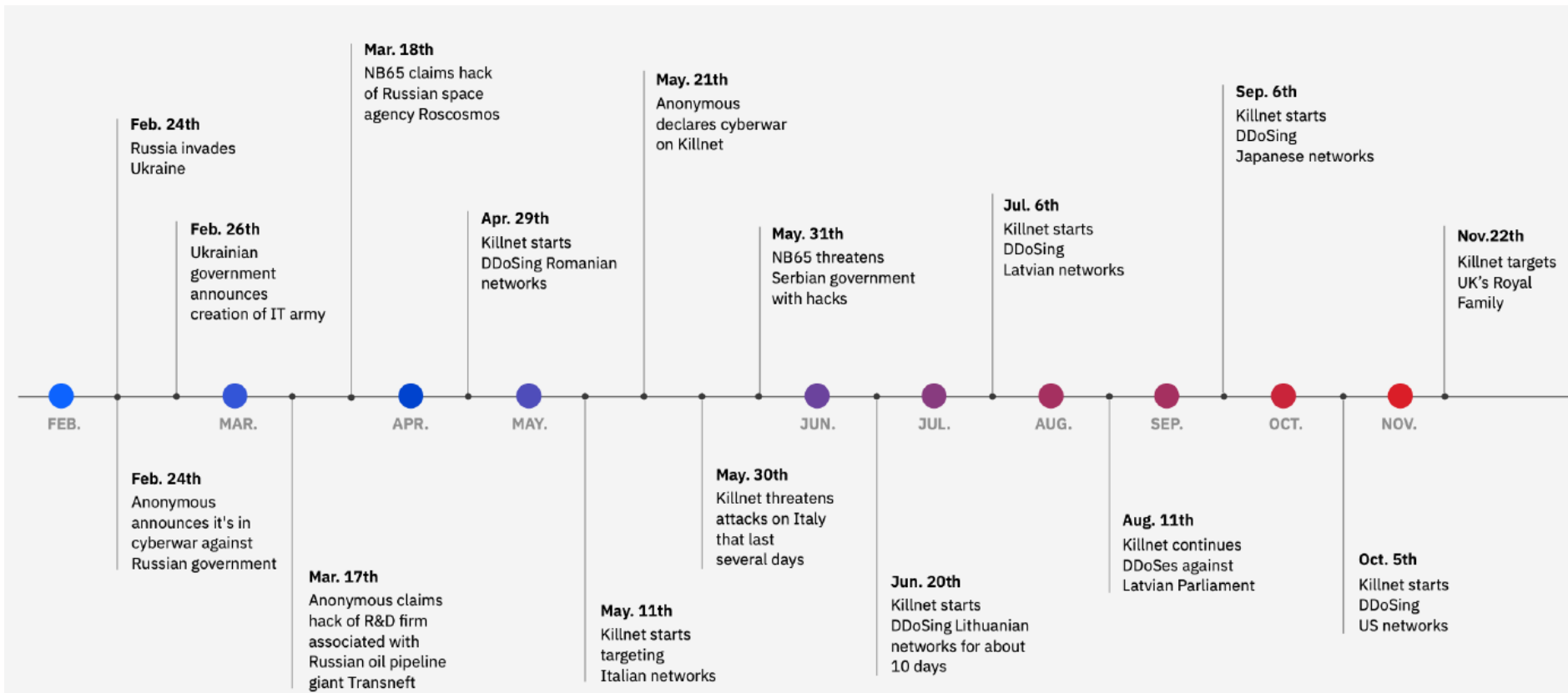
Hackers

- Threat actors that break into computer systems or networks to gain access:
 - **White hat hackers** break into networks or computer systems to identify any weaknesses so that the security of a system or network can be improved. These break-ins are done with prior permission and any results are reported back to the owner
 - **Black hat hackers** take advantage of any vulnerability for illegal personal, financial or political gain
 - **Gray hat hackers** may set out to find vulnerabilities in a system without prior permission of the owner. When they uncover weaknesses, they do not exploit them, rather they report them, but they may demand payment in return
- Unskilled hackers are called **script kiddies**; they use scripts or programs developed by others, primarily for malicious purposes

Hacktivists

- ❑ Hacktivists make political statements to create awareness about issues that are important to them
- ❑ In 2022, a significant increase in hacktivist activity has been observed, especially since the start of Russia-Ukraine conflict
- ❑ Target organisations through DDoS attacks, defacements and data leaks
- ❑ Some of the major Hacktivist groups include Anonymous, TeamOneFirst, GhostSec, Against the West, NB65, KILLNET, XakNet, and The Red Bandits

Timeline of selected Hactivist Events 2022



Timeline of select hactivist events 2022

Source: IBM Security X-Force Threat Intelligence Index 2023

Cyber Criminals

12

- Cyber criminals are usually highly sophisticated and organised
- Main interest in attacks that usually lead to ransomware deployment, coin mining, stealing cryptocurrency, or stealing credentials
- They may even provide cybercrime as a service to other criminals, aka hacker-for hire within the 'Access-as-a-Service' (AaaS) market

State Sponsored Threat Actors

13

- ❑ State-sponsored attackers gather intelligence or commit sabotage on behalf of their government
- ❑ They are usually highly trained and well-funded
- ❑ Their attacks are focused on specific goals that are beneficial to their government
- ❑ Mostly involved in destructive or disruptive operations
- ❑ Example: Since the start of the Russia-Ukraine conflict, widespread use of wiper malware attacks to destroy and disrupt networks of governmental agencies and critical infrastructure entities have been observed

Cyber Warfare

14

- Cyberwarfare is the use of technology to penetrate and attack another nation's computer systems and networks to cause damage or disrupt critical services
- The main reason for resorting to cyberwarfare is to gain advantage over adversaries
 - ▣ Industrial and military espionage e.g. steal defence secrets and gather information about technology
 - ▣ Impact infrastructure e.g. power grid
- Example Stuxnet

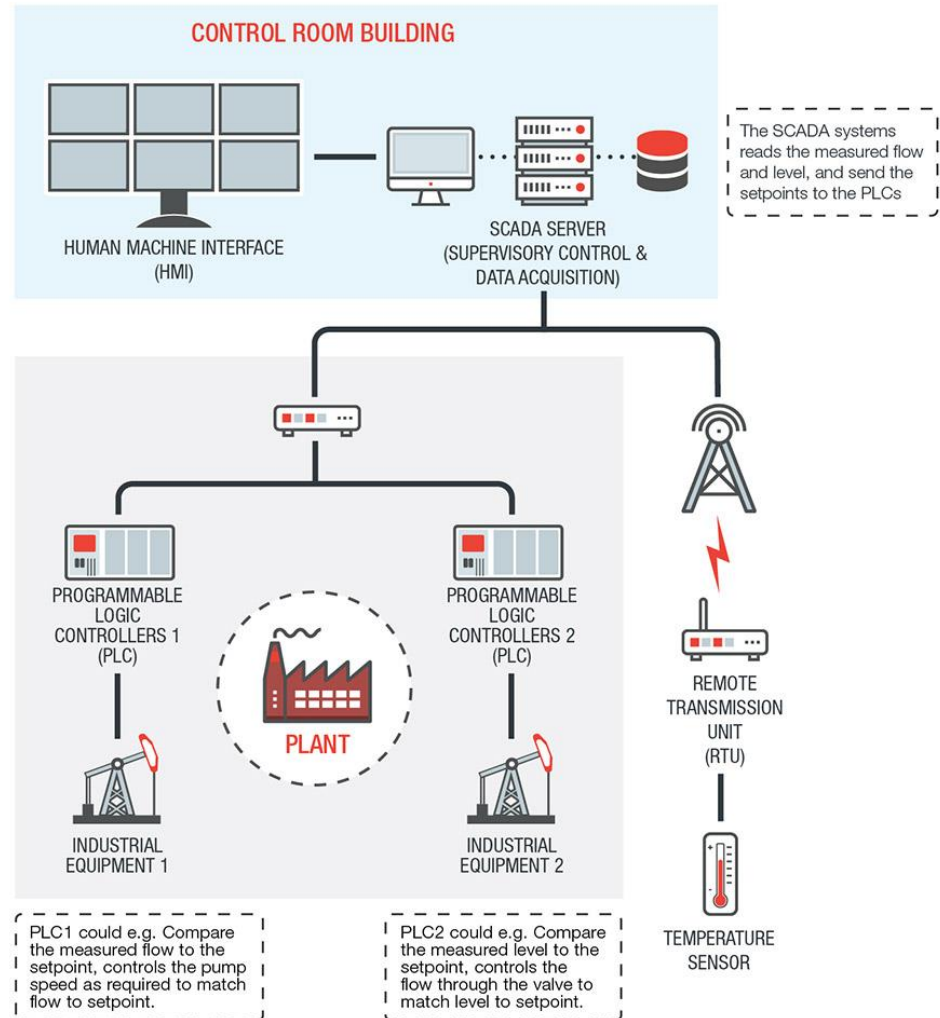
15

Some Case Studies

Background: Industrial Control Systems (ICS)

16

- An ICS is an electronic control system and associated instrumentation used for industrial process control
- Control systems can range in size from a few modular panel-mounted controllers to large interconnected and interactive distributed control systems (DCSs) with many thousands of field connections
- Control systems receive data from remote sensors measuring process variables (PVs), compare the collected data with desired setpoints (SPs), and derive command functions that are used to control a process through the final control elements (FCEs), such as control valves



Cyberattacks on ICS

17

- Traditionally relatively “niche”, but potentially high-impact attacks on critical infrastructure
 - ▣ Power generation
 - ▣ Chemical plants
 - ▣ Steel mills
 - ▣ Transport systems
 - ▣ Oil pipelines
- A summary of some recent high-profile attacks can be found here:
 - ▣ <https://www.makeuseof.com/cyberattacks-on-industry-hackers/>

Attacking Critical Infrastructure (Water Supply)

- https://edition.cnn.com/2021/02/08/us/oldsmar-florida-hack-water-poison/index.html?utm_source=twCNN&utm_term=link&utm_medium=social&utm_content=2021-02-09T02%3A55%3A27

Someone tried to poison a Florida city by hacking into the water treatment system, sheriff says

By Amir Vera, Jamiel Lynch and Christina Carrega, CNN

🕒 Updated 0407 GMT (1207 HKT) February 9, 2021



Pinellas County Sheriff Bob Gualtieri speaks at a press conference on Monday, February 8, about the attempted hacking of the city of Oldsmar's water treatment system.

(CNN) — A hacker gained access into the water treatment system of Oldsmar, Florida, on Friday and tried to increase the levels of sodium hydroxide -- commonly referred to as lye -- in the city's water, officials said, putting thousands at risk of being poisoned.

Cyberattacks on Industrial Infrastructure

19

German Steel Plant Suffers Significant Damage from Targeted Attack

12 janvier 2015

An unknown number of attackers knowledgeable in IT security and industrial control systems (ICS) processes have caused massive damage to a German steel plant in 2014. The incident has been confirmed by the Federal Office for Information Security (BSI) of the German government in an [IT security report](#).



The attack, which appeared to specifically target operators of industrial plants, caused components of the plant controls to fail, resulting in an unregulated furnace, which then caused physical damage to the steel plant.

The individual or group responsible for the attack was able to infiltrate the system using spear phishing and social engineering techniques. These two methods are proven ways by which threat actors lure their victims using emails or social media links that appear to come from a legitimate source but can actually introduce threats for attackers to get inside the network.

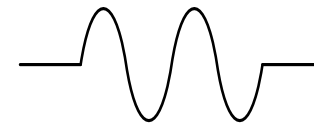
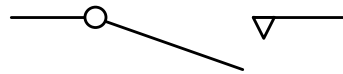
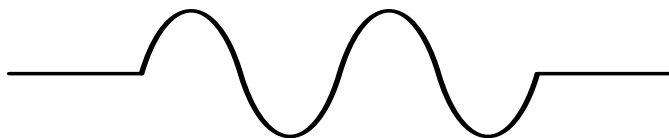
A number of news reports have dubbed this the second cyber attack to ever cause physical damage since the highly sophisticated [Stuxnet malware](#) wreaked havoc to the Natanz uranium enrichment plant in Iran. However, attacks affecting real-world operations of facilities have been

□ <https://www.trendmicro.com/vinfo/fr/security/news/cyber-attacks/german-steel-plant-suffers-significant-damage-from-targeted-attack>

Attacking Critical Infrastructure (Energy Systems) - Synchroscope

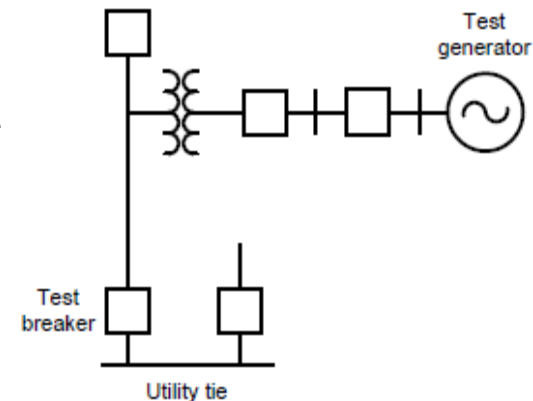
20

- In an electrical grid, power generators and distribution networks must be synced with regard to AC power frequency and phase
- Connecting two unsynchronized AC power systems together is likely to cause high currents to flow, which will severely damage any equipment



The AURORA Cyberattack

- ❑ Experiment conducted by U.S. Department of Energy's Idaho laboratory
- ❑ A hacker gained remote access to a Diesel generator's control system, see [Video](#),
 - ❑ rapidly open and close a diesel generator's circuit breakers, causing it to become out of sync with the transmission network
 - ❑ thereby subjecting the engine to abnormal torques and ultimately causing it to explode
 - high electrical torque translates to stress on the mechanical shaft of the rotating equipment



Example Stuxnet

22

- ❑ Stuxnet was a powerful computer worm designed by U.S. and Israeli intelligence around 2009 designed to disable a key part of the Iranian nuclear program
- ❑ It targeted the “air-gapped” nuclear facility at Natanz
- ❑ Stuxnet was designed to destroy the centrifuges Iran was using to enrich uranium as part of its nuclear program

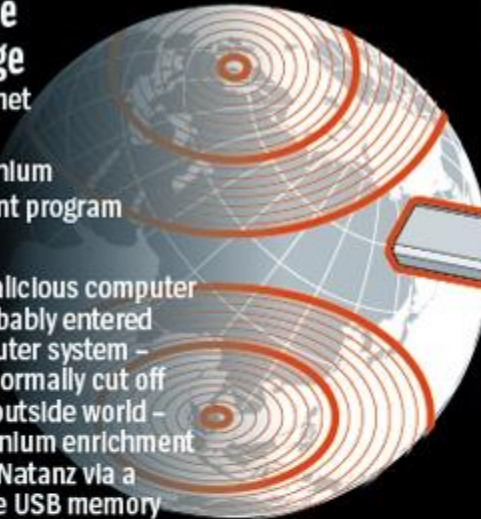


Stuxnet

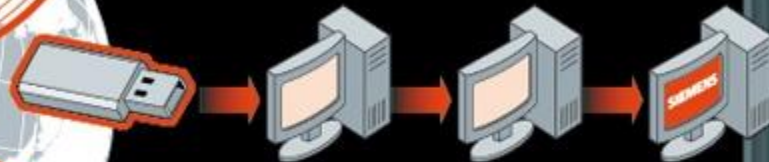
Software Sabotage

How Stuxnet disrupted Iran's uranium enrichment program

1 The malicious computer worm probably entered the computer system - which is normally cut off from the outside world - at the uranium enrichment facility in Natanz via a removable USB memory stick.

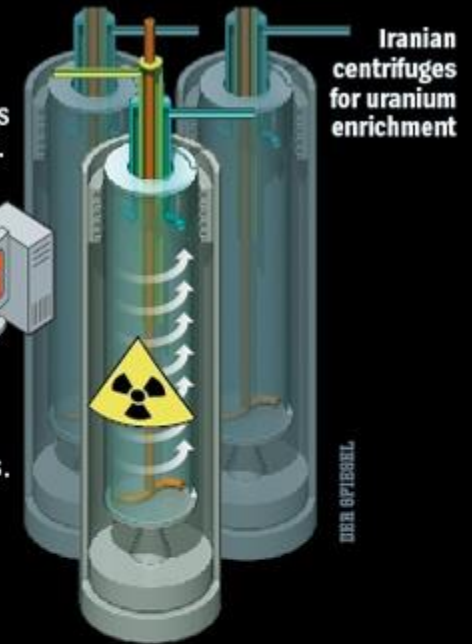


2 The virus is controlled from servers in Denmark and Malaysia with the help of two Internet addresses, both registered to false names. The virus infects some 100,000 computers around the world.

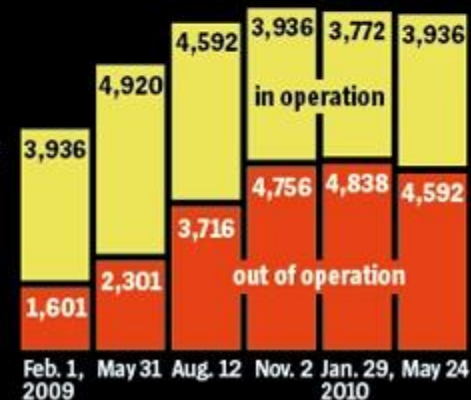


3 Stuxnet spreads through the system until it finds computers running the Siemens control software. Step 7, which is responsible for regulating the rotational speed of the centrifuges.

4 The computer worm varies the rotational speed of the centrifuges. This can destroy the centrifuges and impair uranium enrichment.



5 The Stuxnet attacks start in June 2009. From this point on, the number of inoperative centrifuges increases sharply.



Cyberattacks on Connected Cars

25

- <https://www.darkreading.com/attacks-breaches/cybercriminals-take-aim-at-connected-car-infrastructure>
- DEF CON 27: Car Hacking Deconstructed: <https://www.youtube.com/watch?v=gzav1K5KSI4>



Robert Lemos

Contributing Writer

October 29, 2021



Impact of attacks on automakers over the past decade.

Source: Upstream's "Global Automotive Cybersecurity Report 2021"

Cyberattacks on Medical Devices

- Many medical devices are connected to the Internet, or have a wireless interface
- This allows remote attacks, see for example
 - ▣ <https://www.youtube.com/watch?v=THpcAd2nWJ8>

Hacker Shows Off Lethal Attack By Controlling Wireless Medical Device

BY JORDAN ROBERTSON | FEB. 29, 2012 10:00 AM EDT | POSTED IN HACKERS, MEDICAL PRIVACY, POSTS, SECURITY, VIDEO | 15 COMMENTS



Photographer: David Paul Morris/Bloomberg

Barnaby Jack uses a mannequin equipped with an insulin pump to show the vulnerabilities of wireless medical devices.

What is a Vulnerability?

27

- A weakness which can be exploited by a threat actor/agent (an attacker) to cross privilege boundaries (i.e. perform unauthorised actions) within a computer system (Wikipedia)
- A flaw or weakness in a system's design, implementation, or operation and management that could be exploited to violate the system's security policy (RFC2828)
- A weakness in the computational logic (e.g., code) found in software and some hardware components (e.g., firmware) that, when exploited, results in a negative impact to confidentiality, integrity, OR availability (<https://cve.mitre.org/>)
- Vulnerabilities can be researched, reverse-engineered, hunted, or exploited using automated tools or customized scripts
- An exploitable vulnerability is one for which at least one working attack or exploit exists

Hardware Vulnerabilities

28

- ❑ Hardware vulnerabilities are usually the result of hardware design flaws
- ❑ Example DRAM:
 - ▣ DRAM memory requires one capacitor per bit (a capacitor is a component which can hold an electrical charge)
 - ▣ Modern DRAM chips have a very high memory capacity (4 – 32 gigabits) resulting in those capacitors being positioned installed very close to one another
 - ▣ However, it was discovered that due to their close proximity, changes applied to one of these capacitors could influence neighbouring capacitors
 - ▣ Based on this design flaw, an exploit called **Rowhammer** was created
 - ▣ By repeatedly accessing (hammering) a row of memory, the Rowhammer exploit triggers electrical interferences that eventually corrupt the data stored inside the RAM

Software Vulnerabilities

29

- Software vulnerabilities are usually introduced by errors in the operating system or application code
- Bug: An error that can be rooted to the source code, e.g.
 - ▣ Incorrect implementation of a security protocol
 - ▣ Buffer Overflow: When a program writes more data to a buffer than it can hold, potentially leading to arbitrary code execution
 - Example TLS Heartbleed (will be covered later and in an assignment)
- Flaw: An error at a much deeper level, particularly in the design, and likely in the code level, which may be very difficult and costly to correct; e.g.
 - ▣ Lack of security features, i.e. data encryption, to protect sensitive application data from unauthorised access

Example: Apple's 'goto fail;' Bug in TLS 1.0 and TLS 1.1 (2014)

30


- ❑ Affected iOS and Mac OS X operation systems
- ❑ This vulnerability allowed attacks on TLS connections

```
if ((err = ReadyHash(&SSLHashSHA1, &hashCtx)) != 0)
    goto fail;
if ((err = SSLHashSHA1.update(&hashCtx, &clientRandom)) != 0)
    goto fail;
if ((err = SSLHashSHA1.update(&hashCtx, &serverRandom)) != 0)
    goto fail;
if ((err = SSLHashSHA1.update(&hashCtx, &signedParams)) != 0)
    goto fail;
if ((err = SSLHashSHA1.update(&hashCtx, &signedParams)) != 0)
    goto fail;
if ((err = SSLHashSHA1.final(&hashCtx, &hashOut)) != 0)
    goto fail;

err = sslRawVerify(ctx,
                  ctx->peerPubKey,
                  dataToSign,
                  dataToSignLen,
                  signature,
                  signatureLen);
/* plaintext */
/* plaintext length */

if(err) {
    sslErrorLog("SSLDecodeSignedServerKeyExchange: sslRawVerify "
               "returned %d\n", (int)err);
    goto fail;
}

fail:
SSLFreeBuffer(&signedHashes);
SSLFreeBuffer(&hashCtx);
return err;
```



The Common Vulnerabilities and Exposures (CVE) Database

31

- CVE (<https://cve.mitre.org/>) is a central repository of all the reported security vulnerabilities associated with a specific software system
- Each CVE entry has a unique identifier which is commonly used by many commercial vulnerability management systems to refer to a specific software vulnerability, e.g.,
 - ▣ Heartbleed, CVE-2014-0160
 - ▣ “goto fail;”, CVE-2014-1266
- CVE ID Syntax: CVE prefix + Year + Arbitrary Digits

The Common Weakness Enumeration (CWE) Database

32

- ❑ CVE is complemented by CWE (<https://cwe.mitre.org/>)
- ❑ It provides a formal list of software weakness types that serve as a common language for describing software security weaknesses in architecture, design, or code, for example:
 - ❑ Unrestricted upload of files
 - ❑ Improper input validation
 - ❑ Out-of-bound writes (in arrays)
- ❑ CWE describes a generic vulnerability, while CVE has to do with the specific instance within a product or system not the underlying flaw

Exploit (Wikipedia)

33

- An exploit is a piece of software, data, or a sequence of commands that takes advantage of a vulnerability to cause unintended or unanticipated behaviour to occur on computer software or hardware
- Such behaviour frequently includes things like gaining control of a computer system, allowing privilege escalation, or a denial-of-service attack
- A **remote exploit** works over a network and exploits the security vulnerability without any prior access to the vulnerable system
- A **local exploit** requires prior access to the vulnerable system and usually increases the privileges of the person running the exploit past those granted by the system administrator
- A **zero-day exploit** takes advantage of a vulnerability in software, hardware, or firmware that is unknown to the vendor and for which no patch or fix is available

Heartbleed Exploit Extract (Python Code)

34

□ <https://gist.github.com/eelsivart/10174134>

Heartbleed (CVE-2014-0160) Test & Exploit Python Script

```
heartbleed.py Raw
1  #!/usr/bin/python
2
3  # Modified by Travis Lee
4  # Last Updated: 4/21/14
5  # Version 1.16
6  #
7  # -changed output to display text only instead of hexdump and made it easier to read
8  # -added option to specify number of times to connect to server (to get more data)
9  # -added option to send STARTTLS command for use with SMTP/POP/IMAP/FTP/etc...
10 # -added option to specify an input file of multiple hosts, line delimited, with or without a port specified (host:port)
11 # -added option to have verbose output
12 # -added capability to automatically check if STARTTLS/STLS/AUTH TLS is supported when smtp/pop/imap/ftp ports are entered and automatically
13 # -added option for hex output
14 # -added option to output raw data to a file
15 # -added option to output ascii data to a file
16 # -added option to not display returned data on screen (good if doing many iterations and outputting to a file)
17 # -added tls version auto-detection
18 # -added an extract rsa private key mode (orig code from epixoip. will exit script when found and enables -d (do not display returned data
19 # -requires following modules: gmpy, pyasn1
20
21 # Quick and dirty demonstration of CVE-2014-0160 by Jared Stafford (jspenguin@jspenguin.org)
22 # The author disclaims copyright to this source code.
23
24 import sys
25 import struct
26 import socket
27 import time
28 import select
29 import re
```

Attack Surface and Attack Vector

35

- An organisation's attack surface is the sum of all its attack vectors, i.e., vulnerabilities, pathways and methods, that hackers can use to gain unauthorised access to a network or sensitive data, or to carry out a cyberattack
- The smaller the attack surface, the easier it is to protect the system (obviously)
- We distinguish between the
 - ▣ digital attack surface,
 - ▣ physical attack surface (e.g. malicious insiders or device theft),
 - ▣ social engineering attack surface (e.g. phishing)

The Digital Attack Surface

36

- This includes:
 - Weak passwords, i.e., passwords that are easy to guess or easy to crack via brute-force attacks
 - Misconfiguration, e.g., improperly configured network ports or wireless access points
 - Software, operating system and firmware vulnerabilities
 - Outdated or obsolete devices, data, or applications

Social Engineering (Recall CT255)

37

- Social engineering is the manipulation of people into performing certain actions or revealing confidential information
- That information might be a password, credit card information, personally identifiable information, confidential data, or anything that can be used for fraudulent acts like identity theft
- There are different types of social engineering attacks:
 - ▣ Pretexting
 - ▣ Phishing
 - ▣ Smishing
 - ▣ Vishing
 - ▣ Tailgating

Pretexting

38

- This is when an attacker calls an individual and lies to them in an attempt to gain access to privileged data
- Example:



A fraudster **impersonates a trusted authority** and crafts a scenario to reach out to their victims.



The victim **believes the scenario** and shares any information the 'trusted' authority requests.



The fraudster **gains valuable information** from their victim and often uses it maliciously.

Phishing

39

- ❑ **Phishing** involves sending malicious emails from supposed trusted sources to as many people as possible, assuming a low response rate (shotgun method)
- ❑ In **spear phishing** the perpetrator is disguised as a trusted individual (boss, friend, spouse)
- ❑ **Whaling** uses deceptive email messages targeting high-level decision makers within an organisation, such as CEOs and other executives, who have access to highly valuable information

Subject: Shhh it's a surprise!

Clare,

We're planning a virtual baby shower for Amy in financial services and are in a time crunch. Could you buy the gift? Please **share your banking information** and we can transfer the money over.

Thanks,
Larry Scamington, HR director

Smishing

40

- Smishing is phishing by SMS or text messaging
- This can be a trusty avenue for pretexting attackers to connect with victims since texting is a more intimate form of communication

Text Message
Thu, 31 Aug, 12:57

AIB: Due to unusual activity, your card has been placed on hold. Please visit aibinfo8.com and follow the on-screen instructions to re-activate.

Text Message
Wed, 20 Sep, 10:18

AnPost: Your package has a €2.38 pending fee. To pay this visit: anpost-post-servicecharge.com If this is not paid the package will be returned to sender.

Text Message
Thu, 21 Sep, 12:05

AnPost: You've missed our delivery, for the redelivery of your parcel please visit: anpost-delivery-notice.com and confirm the settlement of €2.38

Text Message
Sat, 23 Sep, 19:31

MyGov: Pre-approved 2023 tax repayment available. Follow <https://incometaxcreditrevenue-mygov.com/ie> to verify information. Review may take up to 14 days.

Vishing

41

- It is the voice counterpart to phishing, e.g.
 - ▣ An email message asks the user to make a telephone call
 - ▣ Victims receive an unsolicited call
- Fraudsters might spoof, or fake caller IDs or use AI generated deepfakes to convince victims they are a trusted source and, ultimately, get victims to share valuable information over the phone
- Many different variations, see for example
 - ▣ <https://www.youtube.com/watch?v=PWVN3Rq4gzw>
 - ▣ <https://www.youtube.com/watch?v=lc7scxvKQOo>

Tailgating

42

- This is when
 - ▣ an attacker quickly follows an authorized person into a secure, physical location
 - ▣ fraudsters pose in real-life as someone else to gain access to restricted or confidential areas where they can get their hands on valuable information

An “internet service provider” shows up on your doorstep for a routine check. Once inside, they have free reins to snoop through your devices and valuable information.



TIP

If a service provider arrives without an appointment, don't just let them inside. Verify their legitimacy by asking questions about your plan.

Quid Pro Quo

43

- “Get something for doing something” (latin: quid pro quo)
- This is when an attacker requests personal information from a person in exchange for something, like a free gift

Congratulations, Steve!

You're eligible for a \$5,000 gift card.
To redeem, please **share your banking information** for wire transfer and also your **home address**.

Sincerely,
Notareal Co.

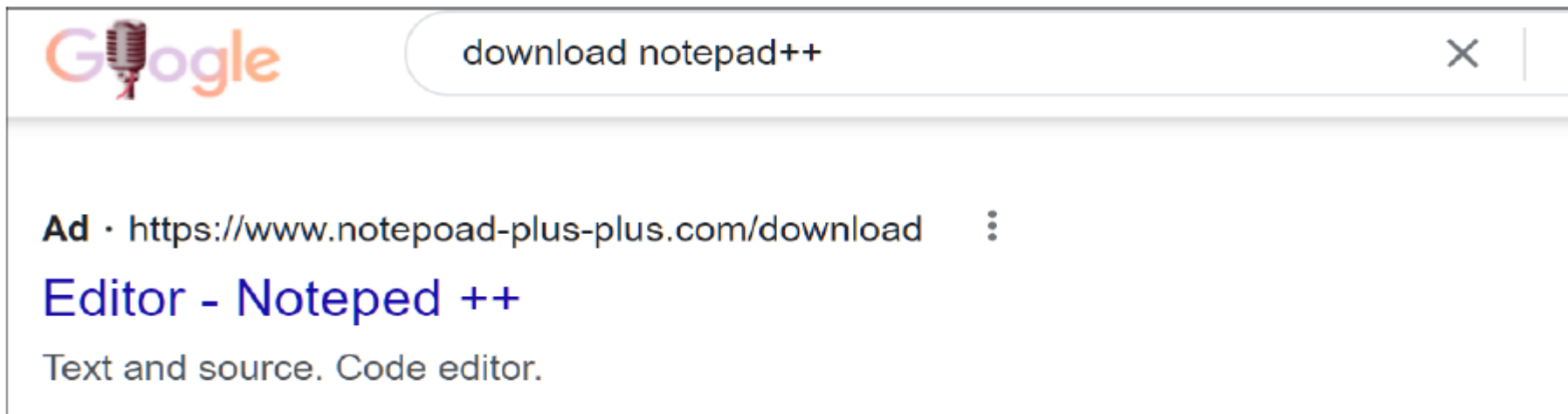
SEO Poisoning

- ❑ Search engine optimisation (SEO) is about improving an organisation's website visibility in search engine results
- ❑ Search engines such as Google present a list of web pages to users based on their search query. These web pages are ranked according to the relevancy of their content.
- ❑ SEO poisoning is a technique used by threat actors to increase the prominence of their malicious websites, making them look more authentic to consumers
- ❑ The most common goal of SEO poisoning is to increase traffic to malicious sites that may host malware or attempt social engineering

Typosquatting

45

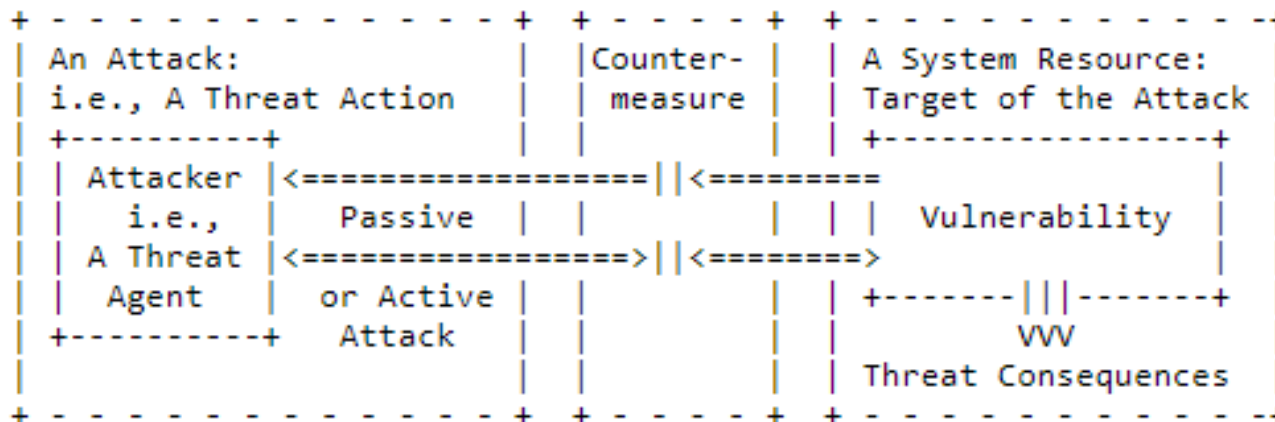
- ❑ Typosquatting targets users who might open their
- ❑ browser and input a website address that has an inadvertent typo or click on a link with a misspelled URL
- ❑ § To exploit these minor user errors, attackers register domain names similar to legitimate ones



Attack (RFC2828, Internet Security Glossary)

46

- An attack is an assault on system security that derives from an intelligent threat, i.e. a deliberate attempt
- An "active attack" attempts to alter system resources or affect their operation (e.g., a ransomware attack on a file server)
- A "passive attack" attempts to learn or make use of information from the system, but does not affect system resources (e.g., eavesdropping on an unprotected network connection)



Common Attack Types

47

- Malware
 - ▣ E.g., in a ransomware attack, an adversary encrypts a victim's data and offers to provide a decryption key in exchange for a payment
- Denial-of-Service (DoS)
 - ▣ A malicious, targeted attack that floods a network with false requests in order to disrupt business operations
- Phishing
 - ▣ A type of cyberattack that uses email, SMS, phone, social media, and social engineering techniques to entice a victim to share sensitive information
- Spoofing
 - ▣ A technique through which a cybercriminal disguises themselves as a known or trusted source
- Code injection attacks
 - ▣ An attacker injecting malicious code into a vulnerable computer or network to change its course of action (e.g. XSS and SQL injection)

Countermeasures (RFC2828, Internet Security Glossary)

48

- An action, device, procedure, or technique that
 - ▣ ... reduces a threat, a vulnerability, or an attack
 - ▣ ... by eliminating or preventing it,
 - ▣ ... by minimising the harm it can cause, or
 - ▣ ... by discovering and reporting it so that corrective action can be taken
- For example, a firewall filters unsolicited network traffic

Threat Consequences

49

- ❑ Threat consequences (as a result from an attack) include
 - ❑ disclosure of information
 - ❑ deception,
 - ❑ disruption of services
 - ❑ usurpation, e.g. unauthorized control of some part of a system

- ❑ Cybercrime: it's all around us
 - Posing a major threat to personal and organizational data and even national security



Personal level

Your identity, data, and computing devices



Organizational level

Reputation, data and customers



Government level

National security, economy and the safety of citizens

Vulnerability Testing

50

- ❑ Vulnerability testing is a process of evaluating and identifying security weaknesses in a computer system, network, or software application
- ❑ It involves systematically scanning, probing, and analyzing systems and applications to uncover potential vulnerabilities, such as coding errors, configuration flaws, or outdated software components
- ❑ The main goal of vulnerability testing is to discover and address these security gaps before they can be exploited by attackers

Vulnerability Testing

51

- ❑ **Network-based scanning:** Used to scan networks for open ports, misconfigurations, and other security weaknesses
- ❑ **Web application scanning:** Identify vulnerabilities in web applications, such as SQL injection, cross-site scripting (XSS), and broken authentication
- ❑ **Static application security testing (SAST):** Analyse source code or compiled code to identify potential security vulnerabilities without executing the application
- ❑ **Dynamic application security testing (DAST):** Interact with running applications to identify security weaknesses during runtime
- ❑ **Fuzz testing:** Generate and send malformed or unexpected inputs to applications to identify vulnerabilities related to input validation and error handling
- ❑ **Database vulnerability assessment:** Scan the database management systems for any potential security weaknesses, misconfigurations, or other vulnerabilities that could be exploited
- ❑ **Configuration management and compliance assessment:** Assess system and application configurations against established security best practices or compliance standards
- ❑ **Container and cloud security assessment:** Focus on identifying vulnerabilities and misconfigurations in cloud-based environments and containerized applications

Vulnerability Testing Steps

52

Asset discovery



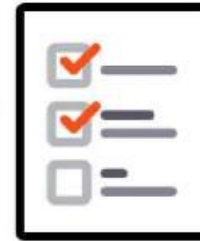
Detect and manage local and remote endpoints, roaming devices, and closed network (DMZ) devices

Vulnerability scanning



Spot all OS vulnerabilities, third-party vulnerabilities, and zero-day vulnerabilities.

Vulnerability assessment



Understand the impact of threats, and prioritize vulnerabilities based on severity, age, exploit code disclosure, patch availability, and various infographics for timely risk reduction.

Vulnerability remediation



Deploy automatically correlated patches to seal vulnerabilities, and leverage alternative mitigation measures if no patch is available.

Example Nessus: An automatic Network Vulnerability Scanner

53

Basic network Scan

Configure Audit Trail Report Export

Hosts 112 Vulnerabilities 272 Remediations 500 VPR Top Threats

Filter Search Hosts 112 Hosts

Host	Critical	High	Medium	Low	Info
192.168.1.46	147	278	59	0	189
192.168.1.83	60	333	86	0	184
192.168.1.10	42	320	81	0	186
192.168.1.53	28	48	0	0	508
192.168.1.44	39	293	78	0	169
192.168.1.66	22	228	52	0	174
192.168.1.55	113	172	29	0	130
192.168.1.40	65	154	89	0	56
192.168.1.56	48	166	41	0	66
192.168.1.11	15	87	0	0	178
192.168.1.12	15	87	0	0	177
data.tehgeek.local	0	12	0	0	266
sshsrvr.tehgeek.local	26	16	0	0	225

Notice: This scan has been updated with **Live Results**. [Launch](#) a new scan to confirm these findings or [remove](#) them.

Scan Details

Policy: Basic Network Scan
Status: Imported
Severity Base: CVSS v3.0
Modified: April 1 at 1:00 PM (Live Results)

Vulnerabilities

- Critical
- High
- Medium
- Low
- Info

Outlook Assignment 1

54

- ❑ In assignment 1 you will be doing a manual (non-automated) vulnerability analysis of a VM target, using Metasploit, focusing on a small number of exploits
- ❑ Metasploit is a
 - ▣ widely-used open-source framework for developing, testing, and executing exploits against target systems
 - ▣ powerful tool for penetration testing, enabling security professionals to identify and exploit vulnerabilities in networks, systems, and applications
- ❑ This assignment will reinforce your understanding of pentesting tools, vulnerabilities and exploits

Vulnerability Scanning versus Penetration Testing


55

- Both are essential components of a comprehensive cybersecurity strategy, but they serve different purposes and involve different methodologies
 - ▣ The primary goal of **vulnerability scanning** is to identify known vulnerabilities in systems, applications, and networks; it provides an automated way to check for security weaknesses
 - ▣ The primary goal of **penetration testing** is to simulate real-world attacks to assess the security posture of a system, application, or network, thereby determining the impact and the effectiveness of existing security measures
 - Pentesters use a combination of automated tools and manual techniques (e.g. social engineering) to find and exploit vulnerabilities by mimicking the actions of real attackers

Vulnerability Disclosure Options

56

- ❑ Tell no one (No disclosure)
- ❑ Report in full to public immediately (Full disclosure)
- ❑ Report to vendor only and potentially receive bug bounty!

 Amazon Vulnerability Research Program https://www.amazon.com Reports resolved: 746 Assets in scope: 35 Average bounty: -	SEVERITY	Amount (in USD)
	Critical	\$10,000 - \$20,000
	High	\$1,500 - \$5,000
	Medium	\$350 - \$500
	Low	\$150

- ❑ Report to vendor, wait for fix, report to public (Responsible disclosure)
- ❑ Sell vulnerability to middleman and don't report to vendor
- ❑ Develop fully weaponized malware and distribute on black market