Introduction and Basics

Foundations of Cybersecurity

Luca Caviglione

Institute for Applied Mathematics and Information Technologies

National Research Council of Italy

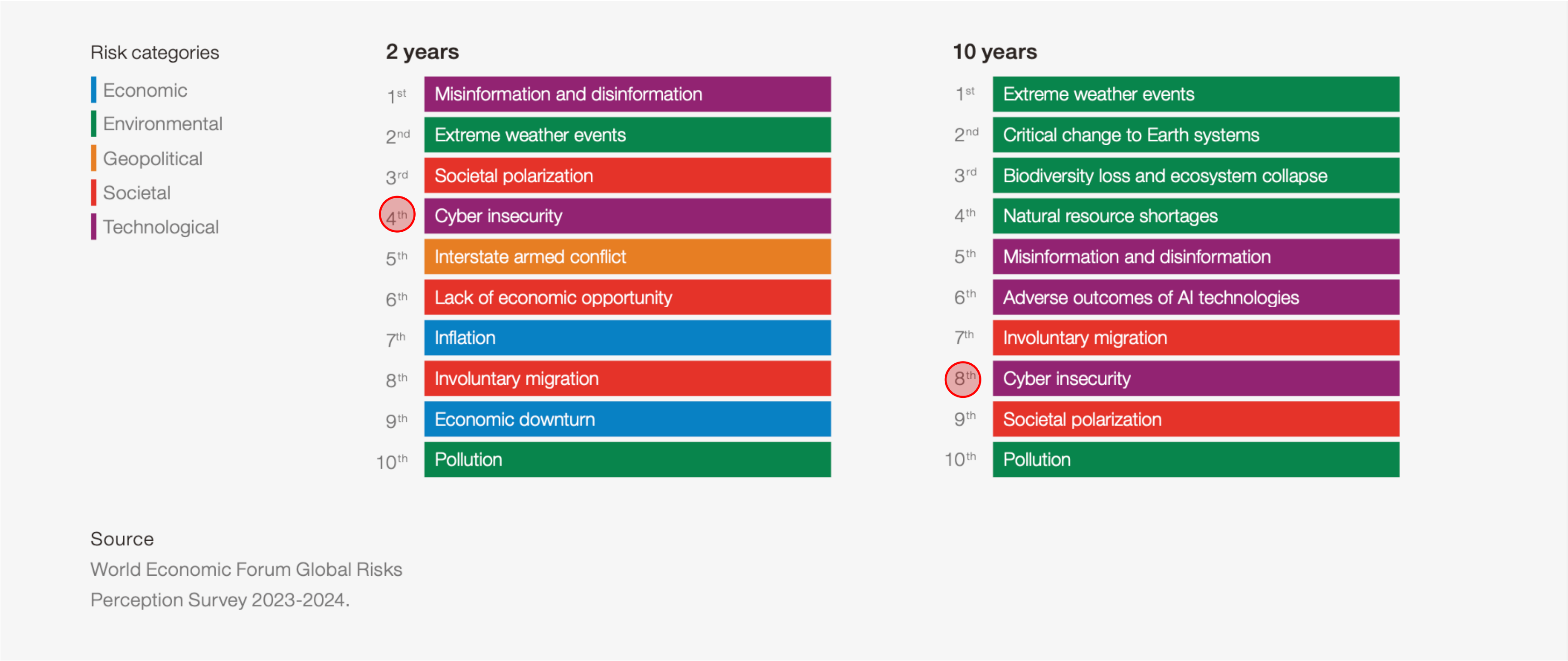
luca.caviglione@cnr.it

University of Pavia – Department of Electrical, Computer and Biomedical Engineering

Outline

- Why a cybersecurity course?
- The Cyber Kill Chain
- Attack Surface
- Attack Tree
- Attack Surface Reduction
- Possible Vulnerabilities
- The Human Element
- Wrap Up

Why a Cybersecurity Course?



Risk categories

- Economic
- Environmental
- Geopolitical
- Societal
- Technological

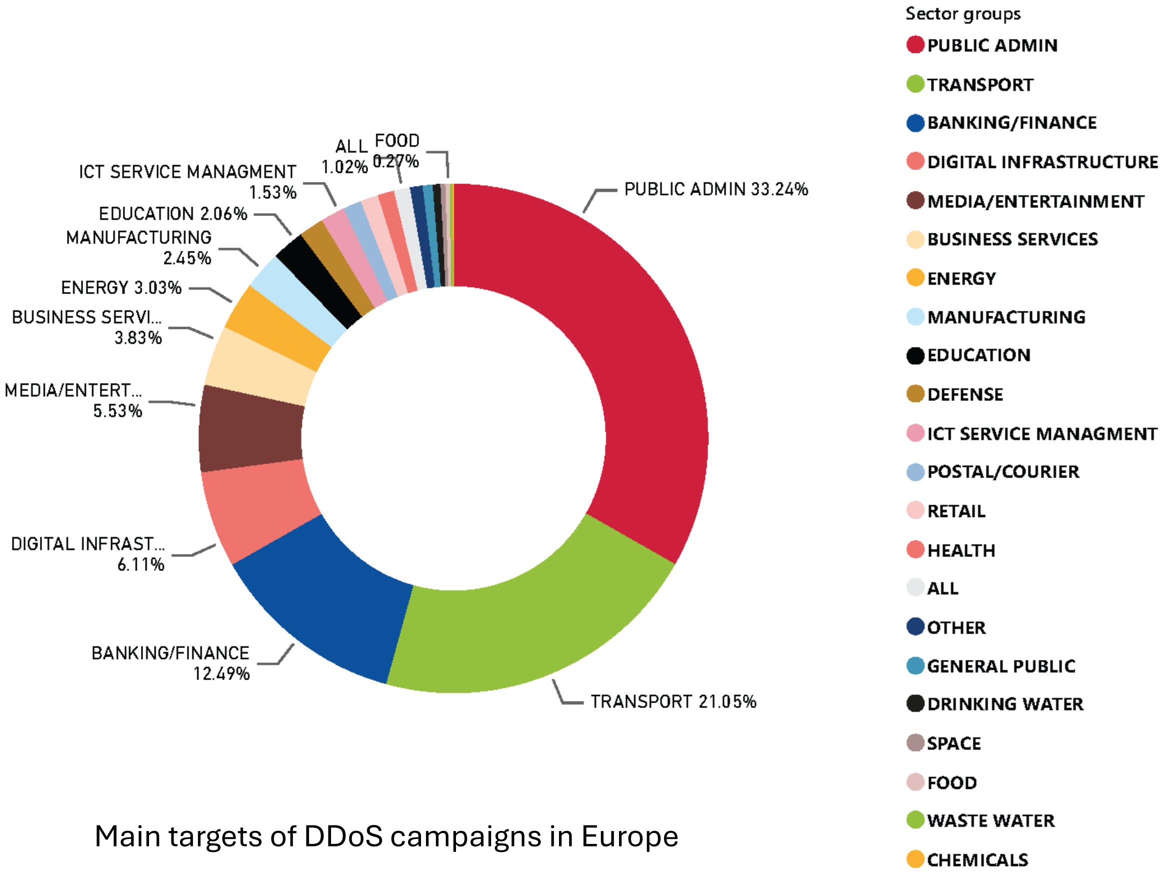
	2 years		10 years
1st	Misinformation and disinformation	1st	Extreme weather events
2nd	Extreme weather events	2nd	Critical change to Earth systems
3rd	Societal polarization	3rd	Biodiversity loss and ecosystem collapse
4th	Cyber insecurity	4th	Natural resource shortages
5th	Interstate armed conflict	5th	Misinformation and disinformation
6th	Lack of economic opportunity	6th	Adverse outcomes of AI technologies
7th	Inflation	7th	Involuntary migration
8th	Involuntary migration	8th	Cyber insecurity
9th	Economic downturn	9th	Societal polarization
10th	Pollution	10th	Pollution

Source

World Economic Forum Global Risks Perception Survey 2023-2024.

Source: World Economic Forum – Global Risks Report 2024 (data collected from over 11,000 business leaders in 113 economies).

Why a Cybersecurity Course?



Main targets of DDoS campaigns in Europe

Source: ENISA Threat Landscape 2024 (July 2023 – June 2024).

As an example, Distributed Denial of Services are increasing in frequency, size, and complexity.

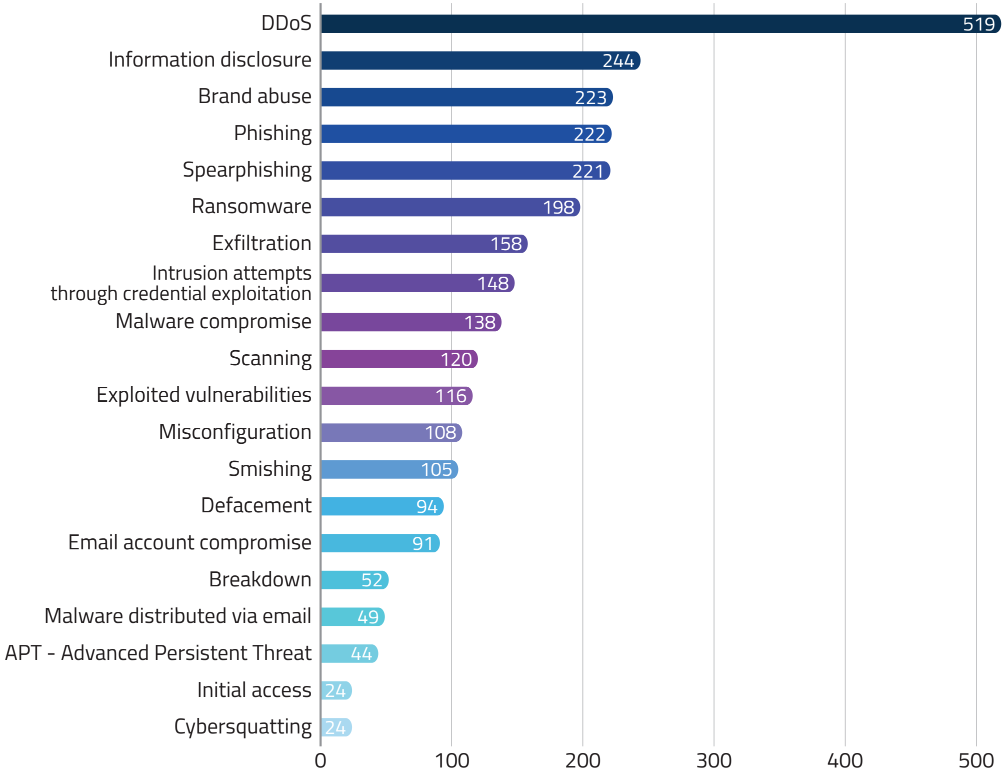
Some **major facts**:

Microsoft reported an average of 1,700 DDoS attacks per day, totaling 13 million attacks globally in 2023.

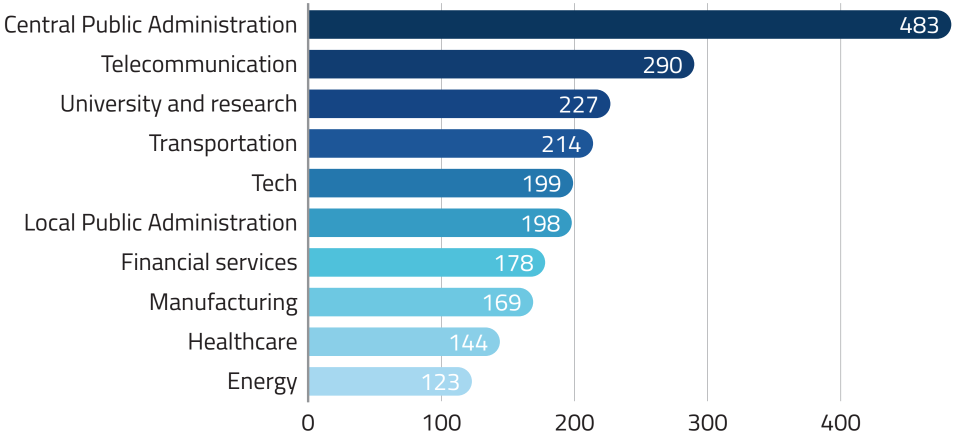
Gcore reported more than a 100% increase in peak attack volumes over the past three years, i.e., from 300 Gbps in 2021 to 1.6 Tbps in 2023.

Cloudflare reported thousands of massive HTTP DDoS attacks in Q3 2023, many exceeding 100M rps. The largest hitting was 200M rps, which is 8 times the 2022 record. The largest L3/L4 attack peaked at 2.6 Tbps and was a UDP flood launched by a Mirai-like botnet.

Why a Cybersecurity Course?



Top 20 handled cyber events



Top 10 economic sectors of victims

Source: ACN 2024 Year in Review.

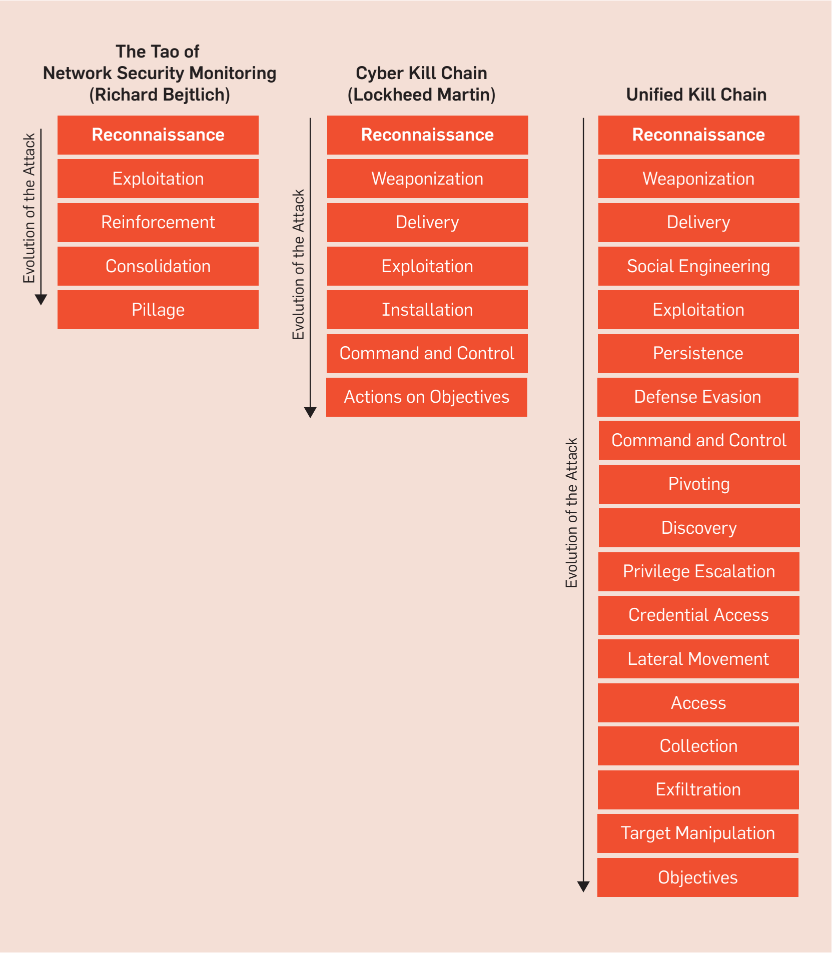
Why a Cybersecurity Course?

February **2023**	April **2023**	February **2024**	July **2024**	December **2024**	February **2025**
Hackers took down the Italian Agenzia delle Entrate website and sent **phishing emails** with a fake login page mimicking the official site.	Mandiant linked a 3CX Desktop App **supply chain attack** to North Korean hackers. It was the first case they found where a past supply chain vulnerability was reused in a new attack.	Starting in 2023, Russian hackers targeted embassies in Georgia, Poland, Ukraine, and Iran, using a **webmail bug** to install malware and gather political and military intelligence.	A **faulty** CrowdStrike **update** for Microsoft Windows caused a global IT outage, affecting 8.5 million machines and disrupting airlines and hospitals. Fortune 500 companies lost an estimated $5.4 billion.	Russian hackers launched over 85,000 cyberattacks on Romania’s election systems, **leaking credentials online**. The attacks occurred around the presidential vote and continued through election day.	North Korean hackers stole $1.5 billion in Ethereum from ByBit by exploiting **third-party wallet software**. They laundered $160 million within 48 hours, marking the largest crypto heist ever.

Source: Center for Strategic & International Studies – Significant Cyber Incidents since 2006.

The Cyber Kill Chain®

- An attack can be decomposed into some general and recurrent phases.
- Different models:
  - **Tao of Network Security Monitoring** subdivides the attacks into **five** stages
  - **Cyber Kill Chain** subdivides the attack into **seven** stages
  - **Unified Kill Chain** subdivides the attack into **eighteen** stages.
- The Cyber Kill Chain framework:
  - is the most used
  - subject to various critics
  - used as a reference and adapted.



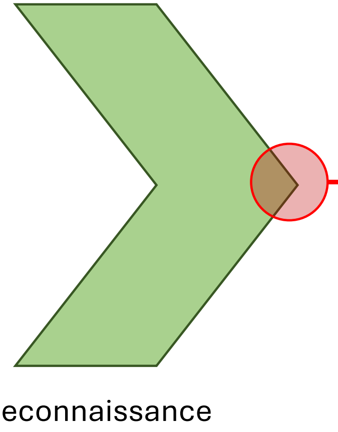
Source: W. Mazurczyk, L. Caviglione, "Cyber Reconnaissance Techniques", Communications of the ACM, Vol. 64, No. 3, pp. 86-95, March 2021.

The Cyber Kill Chain®

- Cyber Kill Chain:
  - describes the process used to carry out a cyber attack
  - adaptation of the military kill chain used to outline the structure of an attack
  - proposed by Lockheed-Martin.

The Cyber Kill Chain®

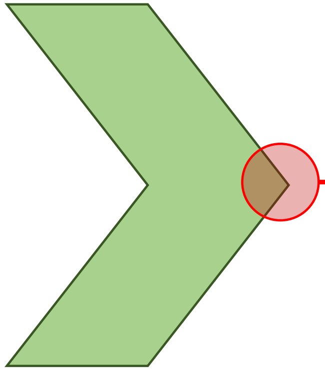
- Cyber Kill Chain:
  - describes the process used to carry out a cyber attack
  - adaptation of the military kill chain used to outline the structure of an attack
  - proposed by Lockheed-Martin.



This is the **initial phase** of the attack, which is used to select the target and search for vulnerabilities or possible entry points. Here, the attacker tries to prepare an effective **offensive plan**. The reconnaissance stage relies upon a composite set of techniques and processes and is **not limited** to **technical information**, but also includes details on the physical location of the victim, phone numbers, names of colleagues, etc. It may also heavily rely upon **social engineering**.

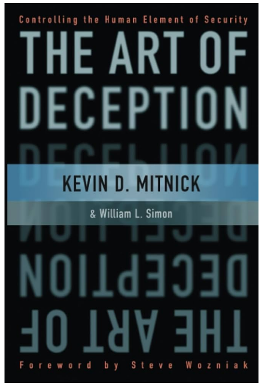
The Cyber Kill Chain®

- Cyber Kill Chain:
  - describes the process used to carry out a cyber attack
  - adaptation of the military kill chain used to outline the structure of an attack
  - proposed by Lockheed-Martin.



Reconnaissance

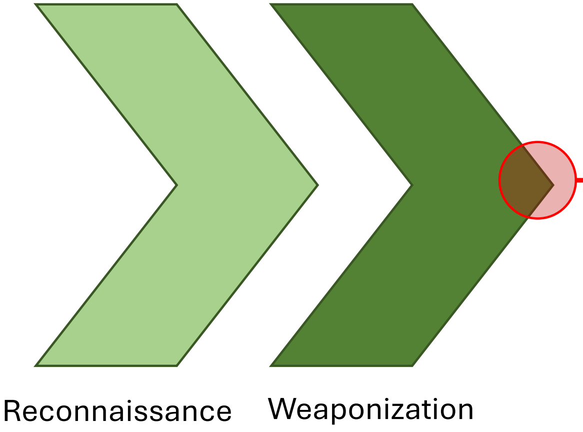
This is the **initial phase** of the attack, which is used to select the target and search for vulnerabilities or possible entry points. Here, the attacker tries to prepare an effective **offensive plan**. The reconnaissance stage relies upon a composite set of techniques and processes and is **not limited** to **technical information**, but also includes details on the physical location of the victim, phone numbers, names of colleagues, etc. It may also heavily rely upon **social engineering**.


Controlling the Human Element of Security
THE ART OF DECEPTION
KEVIN D. MITNICK
& William L. Simon
Foreword by Steve Wozniak

Suggested book and movie!

The Cyber Kill Chain®

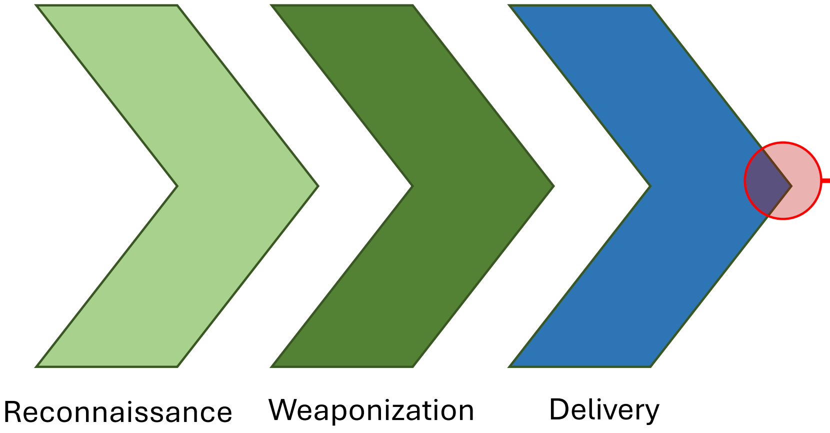
- Cyber Kill Chain:
  - describes the process used to carry out a cyber attack
  - adaptation of the military kill chain used to outline the structure of an attack
  - proposed by Lockheed-Martin.



Attacker creates a **malicious payload** that can be delivered (e.g., a malware or a worm) and tailored to one or more vulnerabilities. To this aim, an exploit or a backdoor are used.

The Cyber Kill Chain®

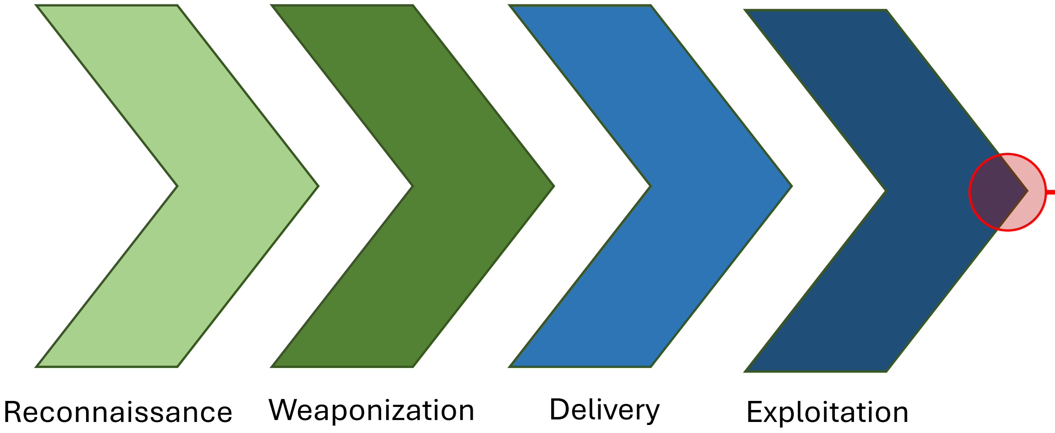
- Cyber Kill Chain:
  - describes the process used to carry out a cyber attack
  - adaptation of the military kill chain used to outline the structure of an attack
  - proposed by Lockheed-Martin.



The **malicious payload** is then **delivered** to the victim. Typical examples are emails, a crafted website, or an USB key.

The Cyber Kill Chain®

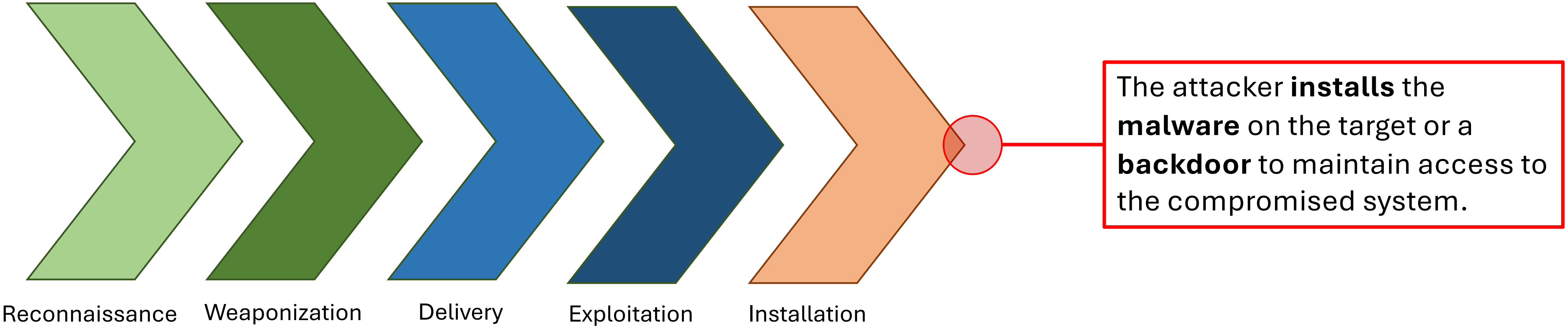
- Cyber Kill Chain:
  - describes the process used to carry out a cyber attack
  - adaptation of the military kill chain used to outline the structure of an attack
  - proposed by Lockheed-Martin.



Code is **executed** on the system of the victim to **exploit** a **vulnerability** and gain some form of **access** or **control**.

The Cyber Kill Chain®

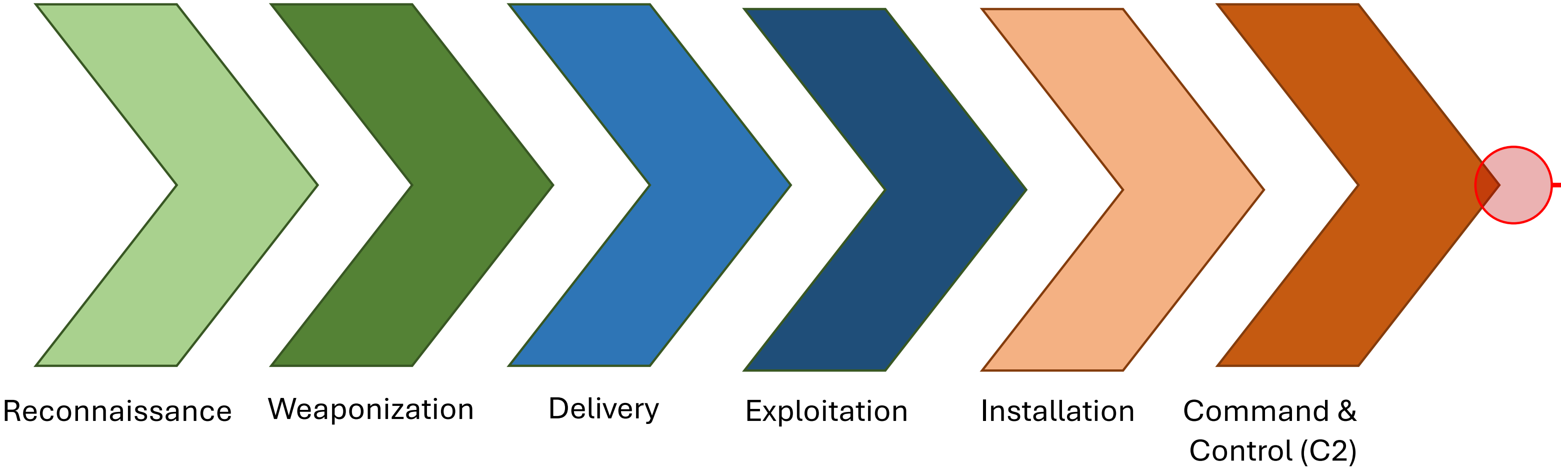
- Cyber Kill Chain:
  - describes the process used to carry out a cyber attack
  - adaptation of the military kill chain used to outline the structure of an attack
  - proposed by Lockheed-Martin.



The attacker **installs** the **malware** on the target or a **backdoor** to maintain access to the compromised system.

The Cyber Kill Chain®

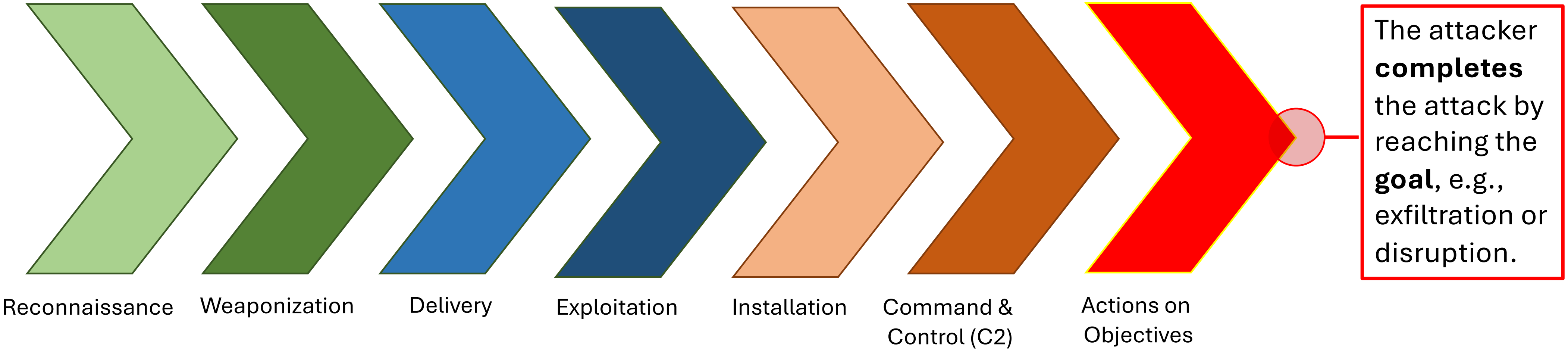
- Cyber Kill Chain:
  - describes the process used to carry out a cyber attack
  - adaptation of the military kill chain used to outline the structure of an attack
  - proposed by Lockheed-Martin.



The attacker creates a **communication channel** to send **commands** or for the **remote manipulation** of the victim.

The Cyber Kill Chain®

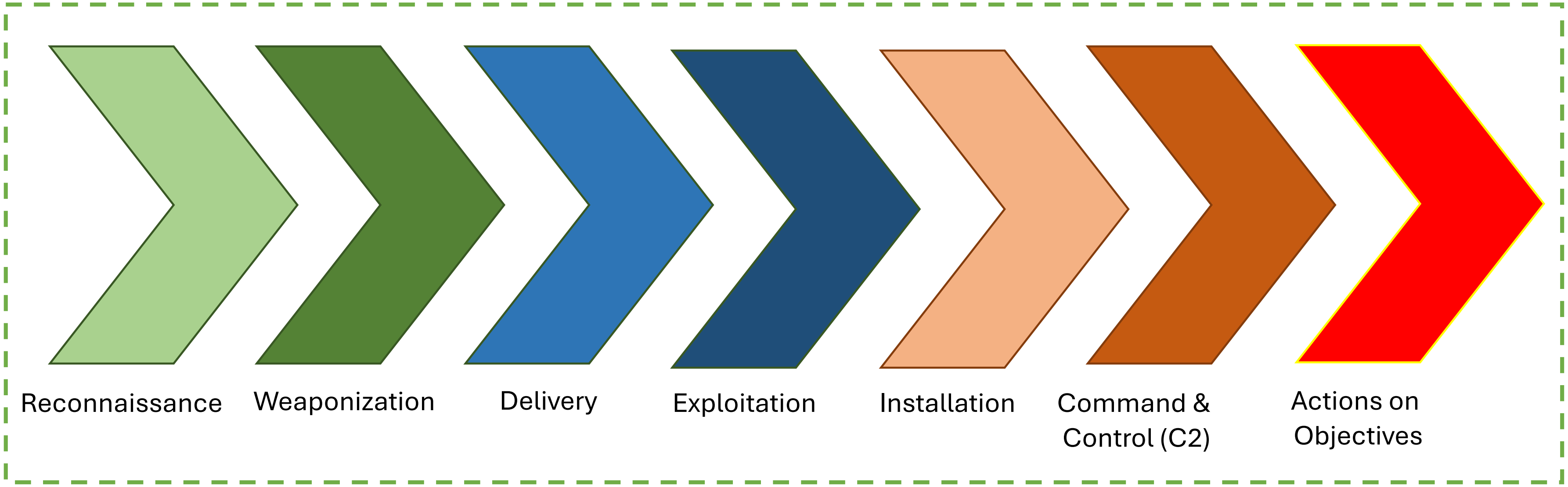
- Cyber Kill Chain:
  - describes the process used to carry out a cyber attack
  - adaptation of the military kill chain used to outline the structure of an attack
  - proposed by Lockheed-Martin.



The attacker **completes** the attack by reaching the **goal**, e.g., exfiltration or disruption.

The Cyber Kill Chain®

- Cyber Kill Chain:
  - describes the process used to carry out a cyber attack
  - adaptation of the military kill chain used to outline the structure of an attack
  - proposed by Lockheed-Martin.



The Cyber Kill Chain is especially suited for describing sophisticated attacks, such as **Advanced Persistent Threats** (APTs)

Attack Surface

- An **attack surface** is:
    - the **sum** of all **entry points** and **vulnerabilities** that an **adversary** can **exploit** to attack a system.
- There are different attack surfaces that may coexist:
    - **hardware**: devices and USB ports or drives
    - **cloud**: resource-as-commodity infrastructures used by an organization
    - **physical**: physical access points that can be exploited.

Attack Surface

- An **attack surface** is:
  - the **sum** of all **entry points** and **vulnerabilities** that an **adversary** can **exploit** to attack a system.
- There are different attack surfaces that may coexist:
  - **hardware**: devices and USB ports or drives
  - **cloud**: resource-as-commodity infrastructures used by an organization
  - **physical**: physical access points that can be exploited.

myself walking near Torriglia (GE)

Attack Surface

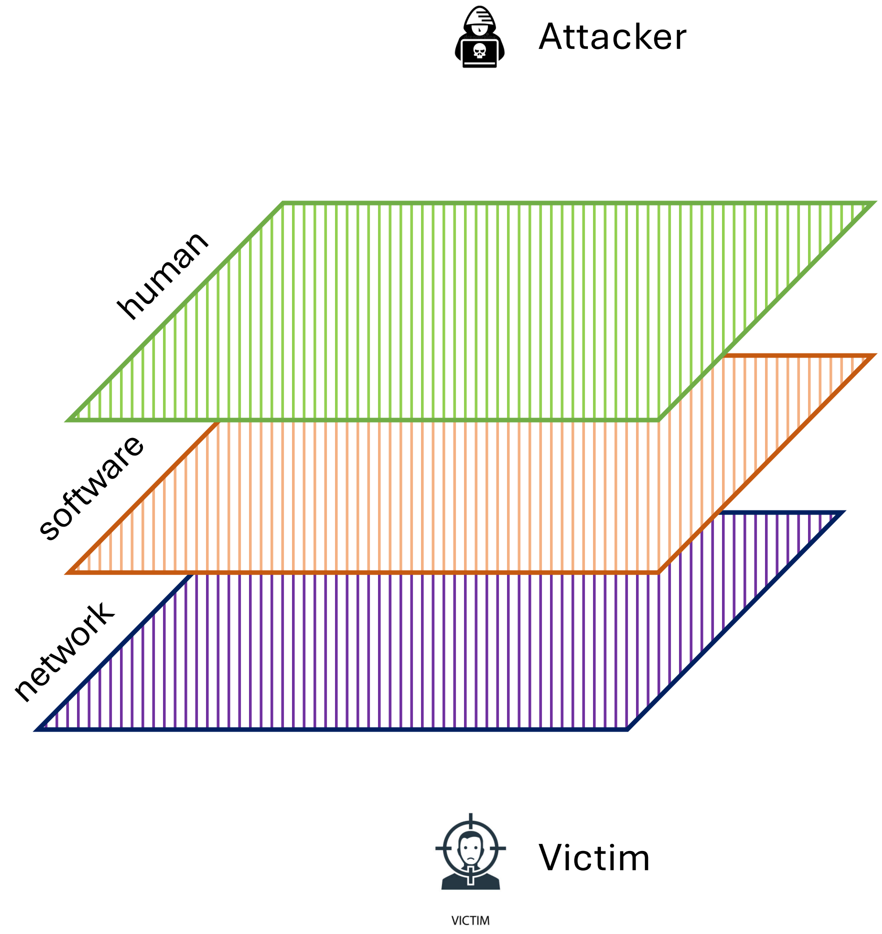
- In this course we are **interested** in:

By Product

  - **human attack surface**: outlined by vulnerabilities caused by people, e.g., via social engineering, human errors, and insiders

Main Focus

  - **software attack surface**: outlined by vulnerabilities plaguing applications, operating systems, firmware, and software ecosystems
  - **network attack surface**: outlined by vulnerabilities of wide-area networks or the Internet, e.g., firewall configurations.

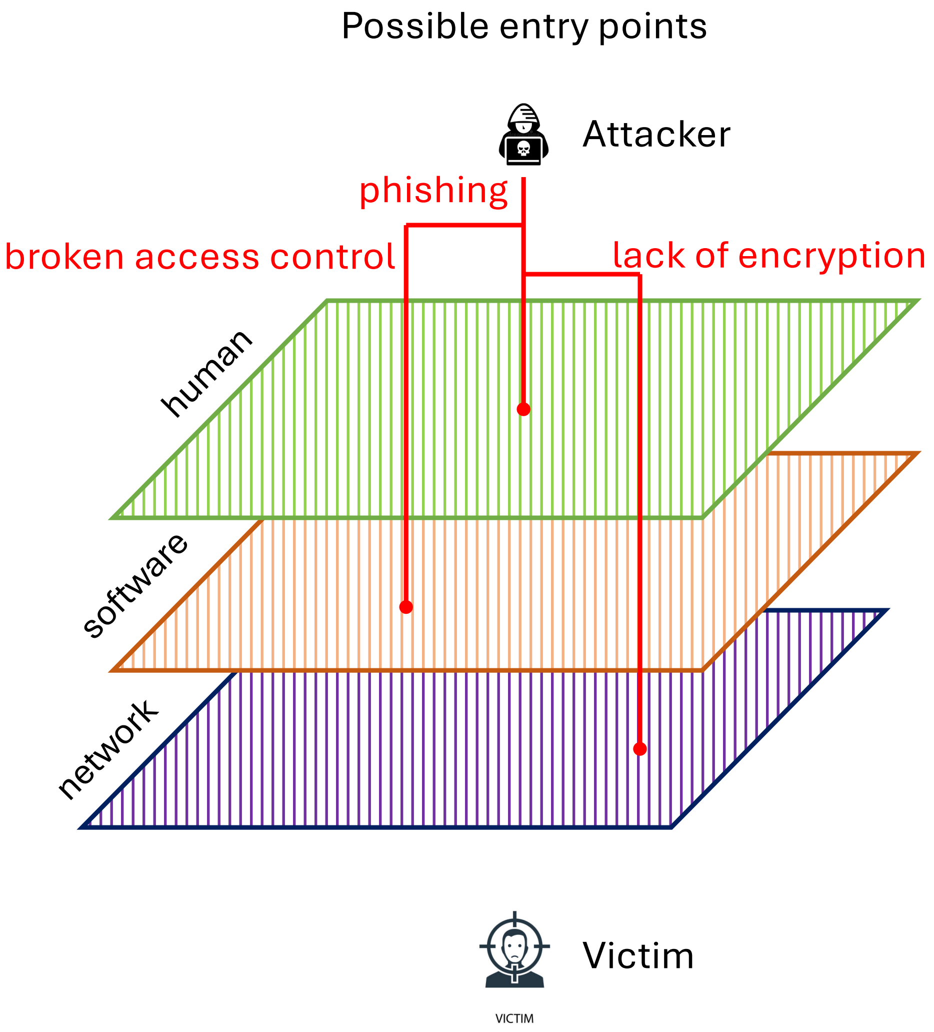


Attack Surface

- In this course we are **interested** in:
  - **human attack surface**: outlined by vulnerabilities caused by people, e.g., via social engineering, human errors, and insiders
  - **software attack surface**: outlined by vulnerabilities plaguing applications, operating systems, firmware, and software ecosystems
  - **network attack surface**: outlined by vulnerabilities of wide-area networks or the Internet, e.g., firewall configurations.

By Product

Main Focus



Attack Surface

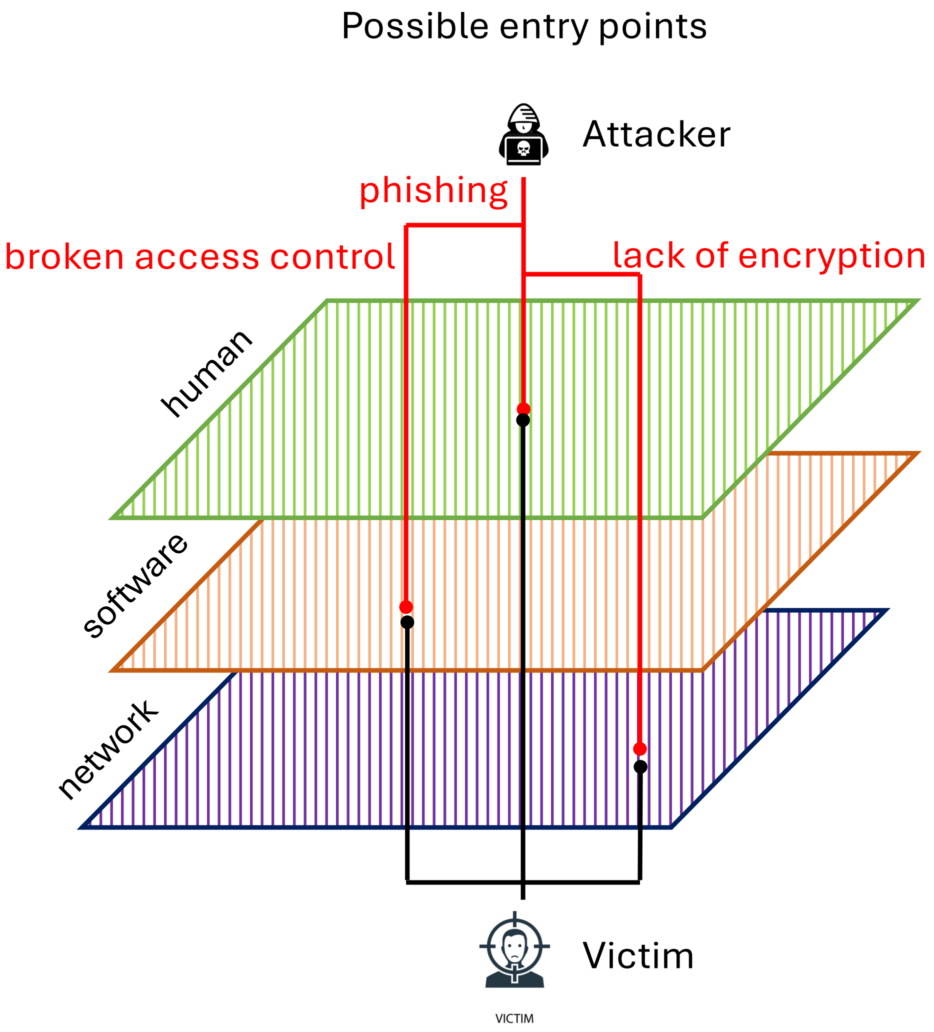
- In this course we are **interested** in:

By Product

  - **human attack surface**: outlined by vulnerabilities caused by people, e.g., via social engineering, human errors, and insiders

Main Focus

  - **software attack surface**: outlined by vulnerabilities plaguing applications, operating systems, firmware, and software ecosystems
  - **network attack surface**: outlined by vulnerabilities of wide-area networks or the Internet, e.g., firewall configurations.



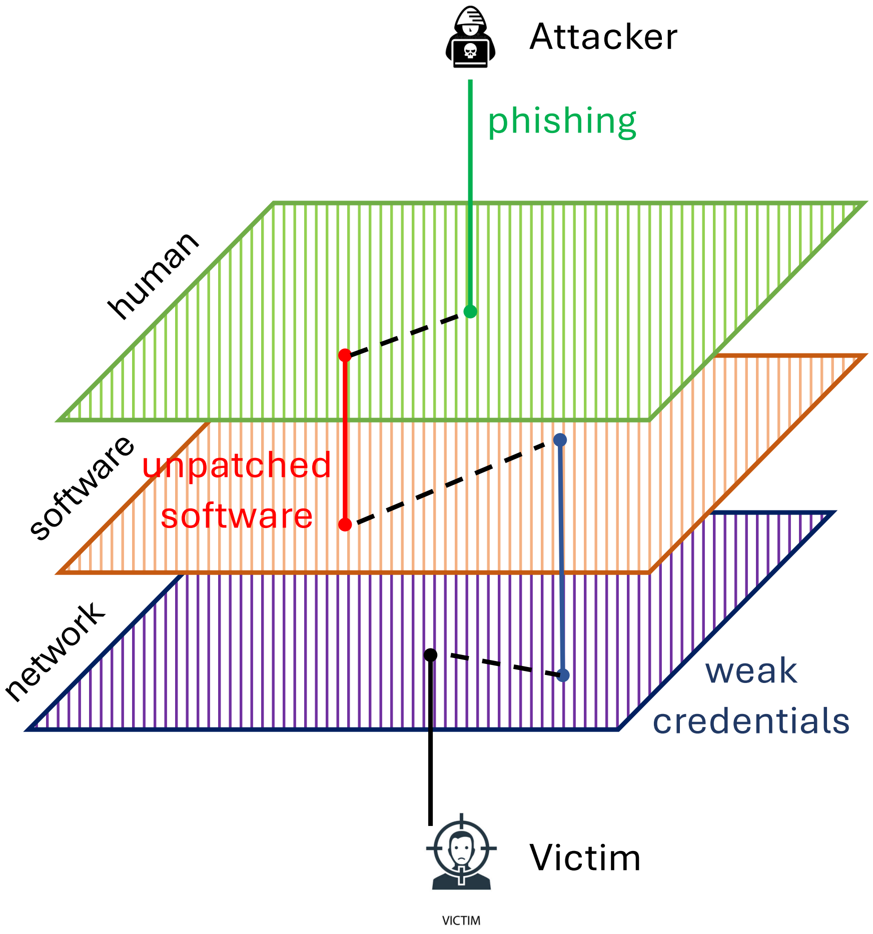
Attack Surface

- In this course we are **interested** in:
  - **human attack surface**: outlined by vulnerabilities caused by people, e.g., via social engineering, human errors, and insiders
  - **software attack surface**: outlined by vulnerabilities plaguing applications, operating systems, firmware, and software ecosystems
  - **network attack surface**: outlined by vulnerabilities of wide-area networks or the Internet, e.g., firewall configurations.

By Product

Main Focus

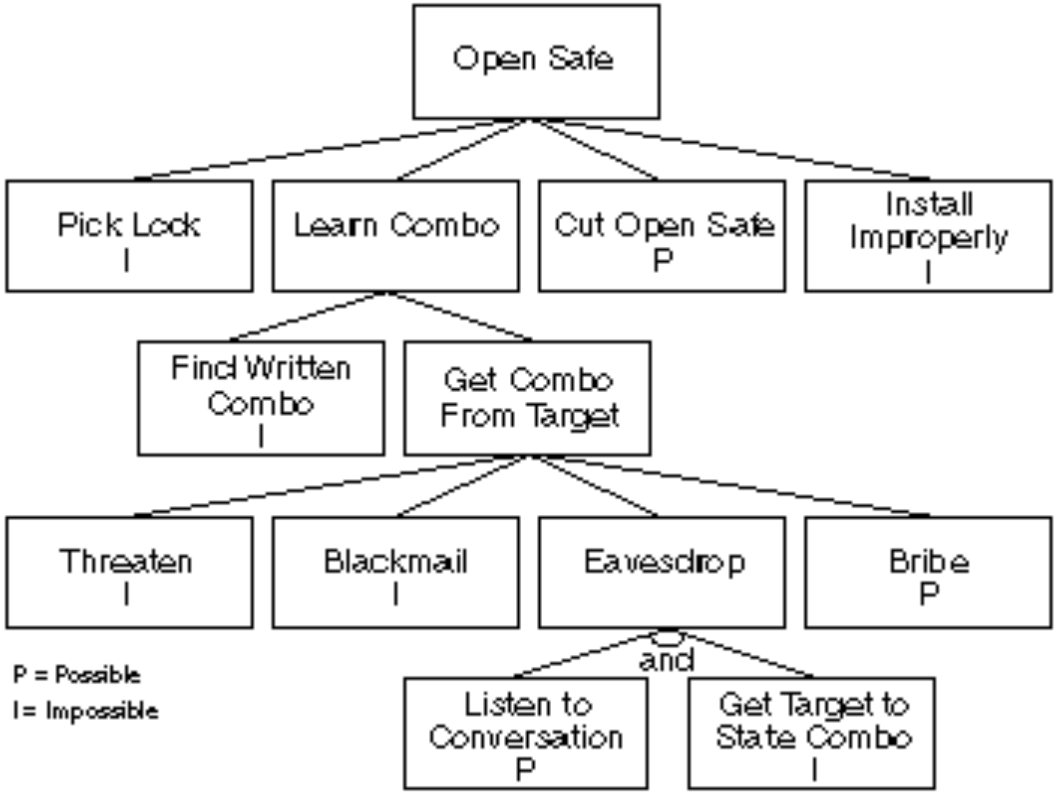
Attacker can “move” through surfaces



Attack Tree

- An **attack tree** is a conceptual diagram that shows how a target can be attacked.
- Basic concepts:
  - the **goal** of the attack is **the root node** of the tree
  - the **ways** that an attacker could reach that goal are **branches** and **subnodes**
  - each **subnode** defines a **subgoal** (each **subgoal** may have its own set of further **subgoals**)
  - the **leaves** of the tree are the **different ways** for **initiating** an attack.
- Other concepts:
  - **nodes** other than a leaf is either an **AND-node** or an **OR-node**
  - **branches** can be **labeled** with values representing difficulty, cost, or other attack attributes (attacks can be then compared).

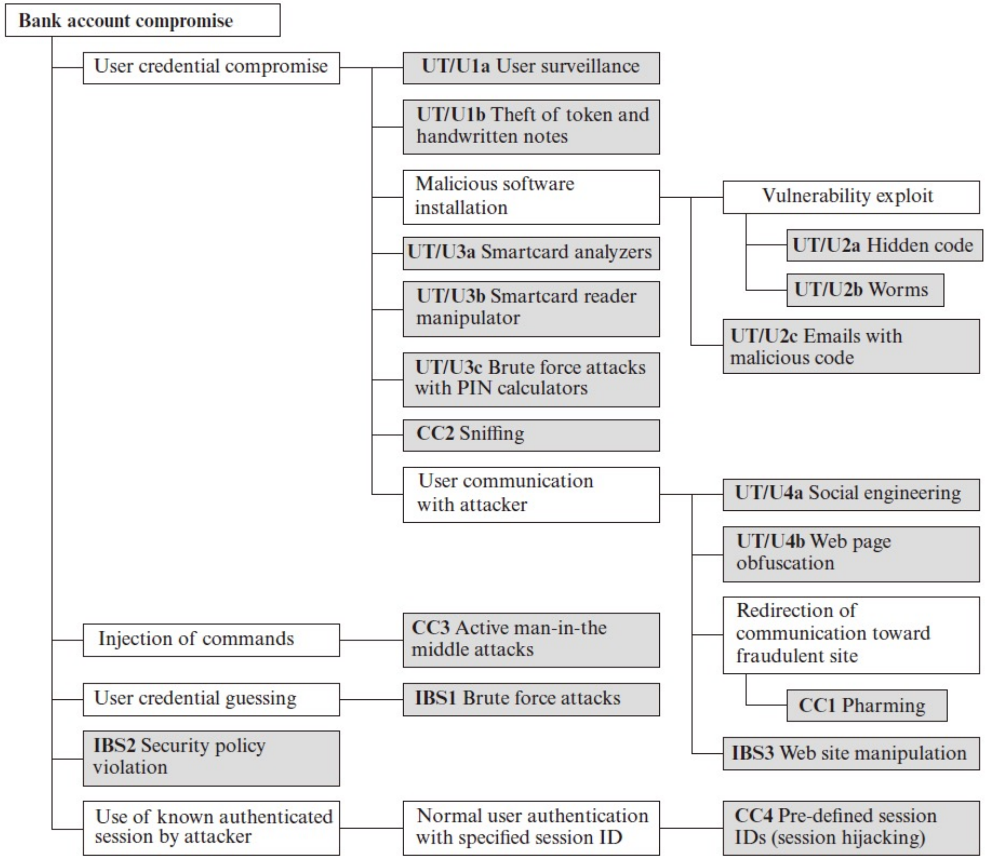
Attack Tree: A “Classic” Example



Bruce Schneier

Source: https://www.schneier.com/academic/archives/1999/12/attack_trees.html

Attack Tree: Internet Banking Authentication



- Bank account compromise
  - User credential compromise
    - **UT/U1a** User surveillance
    - **UT/U1b** Theft of token and handwritten notes
    - Malicious software installation
      - Vulnerability exploit
        - **UT/U2a** Hidden code
        - **UT/U2b** Worms
      - **UT/U2c** Emails with malicious code
    - **UT/U3a** Smartcard analyzers
    - **UT/U3b** Smartcard reader manipulator
    - **UT/U3c** Brute force attacks with PIN calculators
    - **CC2** Sniffing
    - User communication with attacker
      - **UT/U4a** Social engineering
      - **UT/U4b** Web page obfuscation
      - Redirection of communication toward fraudulent site
        - **CC1** Pharming
      - **IBS3** Web site manipulation
  - Injection of commands
    - **CC3** Active man-in-the middle attacks
  - User credential guessing
    - **IBS1** Brute force attacks
  - **IBS2** Security policy violation
  - Use of known authenticated session by attacker
    - Normal user authentication with specified session ID
      - **CC4** Pre-defined session IDs (session hijacking)

Legend:

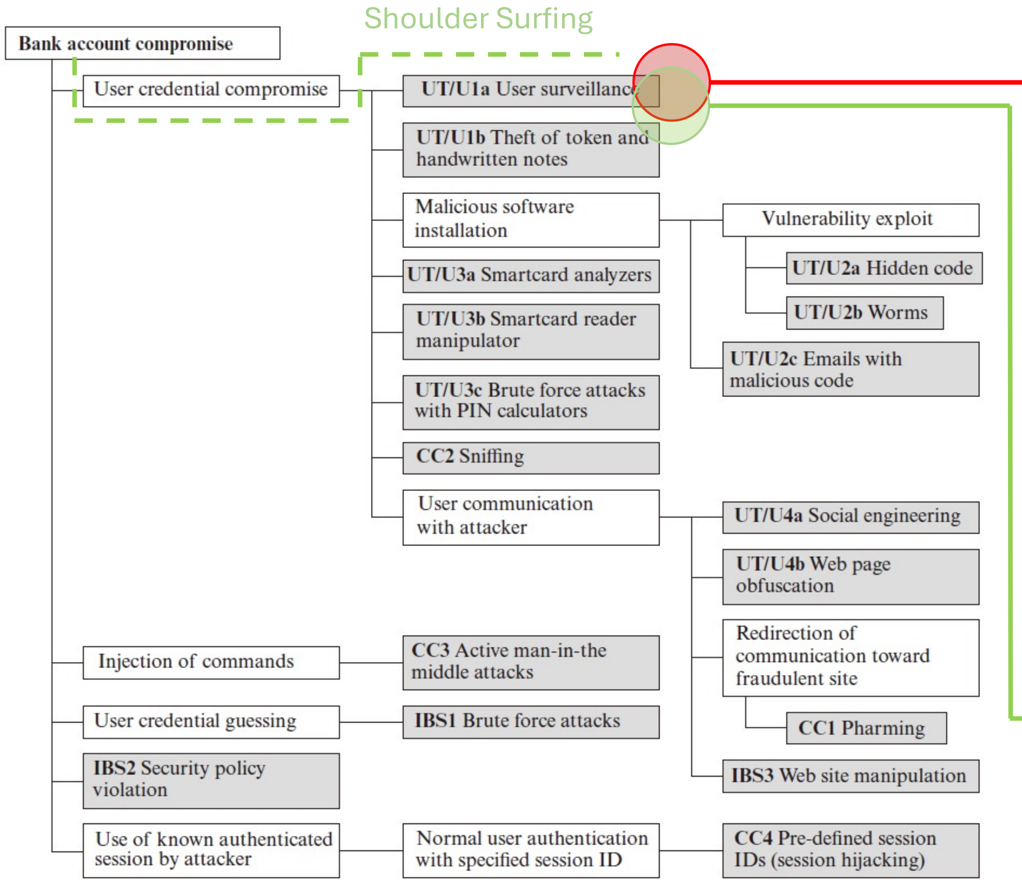
User **T**erminal and **U**ser (**UT/U**): attacks targeting the user equipment, including smartcards and password/token generators; they also include actions of the user.

Communications **C**hannel (**CC**): attacks focusing on communication links.

Internet **B**anking **S**erver (**IBS**): attacks targeting hosts/nodes running the banking application.

Source: W. Stallings, “Network Security Essentials - Applications and Standards”, Sixth Edition, Pearson.

Attack Tree: Internet Banking Authentication



Shoulder Surfing

- Bank account compromise
  - User credential compromise
    - UT/U1a User surveillance
    - UT/U1b Theft of token and handwritten notes
    - Malicious software installation
      - Vulnerability exploit
        - UT/U2a Hidden code
        - UT/U2b Worms
      - UT/U2c Emails with malicious code
    - UT/U3a Smartcard analyzers
    - UT/U3b Smartcard reader manipulator
    - UT/U3c Brute force attacks with PIN calculators
    - CC2 Sniffing
    - User communication with attacker
      - UT/U4a Social engineering
      - UT/U4b Web page obfuscation
      - Redirection of communication toward fraudulent site
        - CC1 Pharming
      - IBS3 Web site manipulation
  - Injection of commands
    - CC3 Active man-in-the middle attacks
  - User credential guessing
    - IBS1 Brute force attacks
  - IBS2 Security policy violation
  - Use of known authenticated session by attacker
    - Normal user authentication with specified session ID
      - CC4 Pre-defined session IDs (session hijacking)

The **attacker simplest path** principle: an attacker usually exploits the path of least resistance, which is the most straightforward, low-effort route for exploiting vulnerabilities and achieve his/her/their goal.

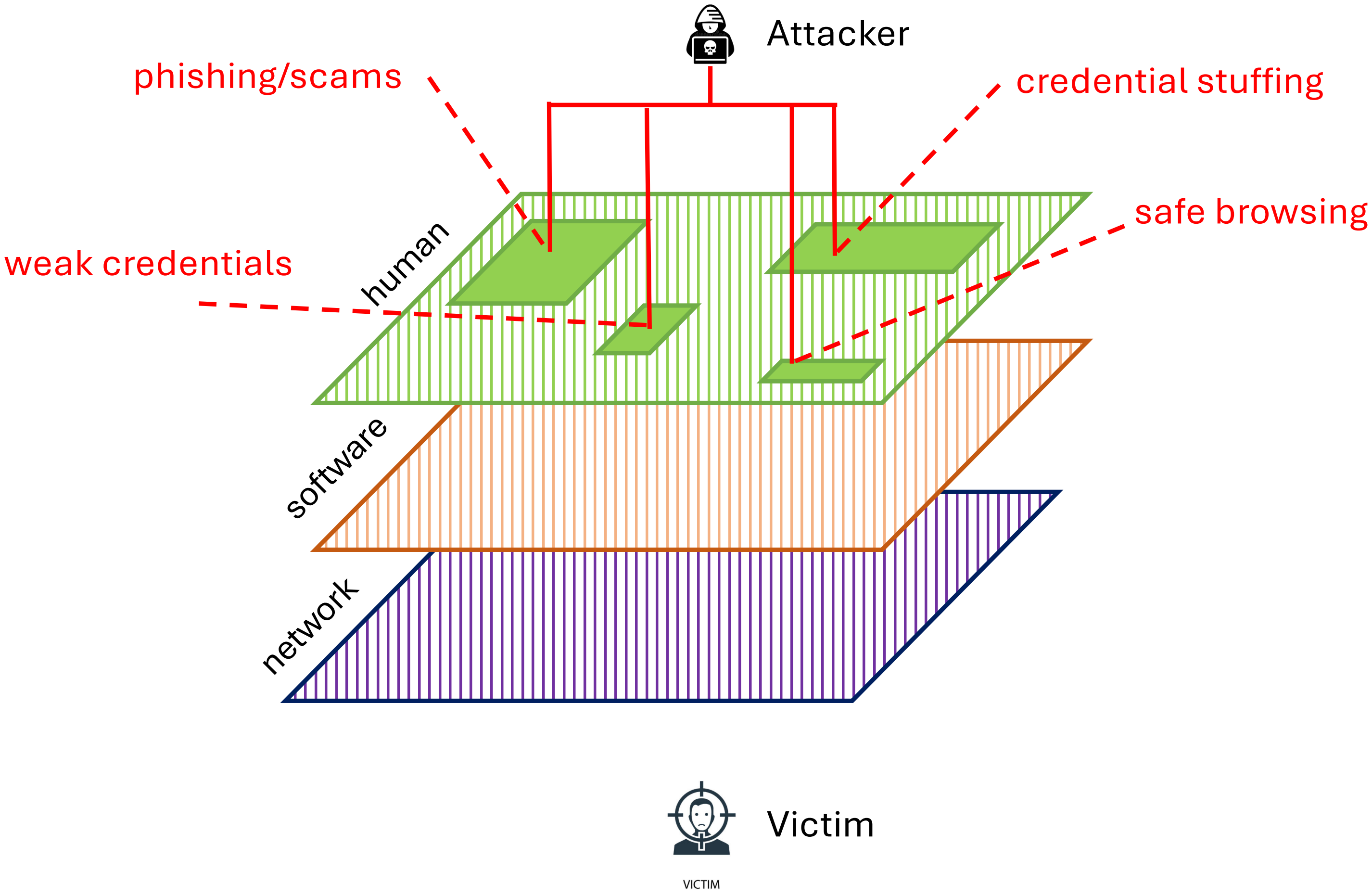
The “**simplest path**” is often found in overlooked, externally-exposed, or misconfigured systems and resources.

Source: W. Stallings, “Network Security Essentials - Applications and Standards”, Sixth Edition, Pearson.

Attack Surface Reduction

- The **attack surface reduction** is the process of minimizing:
  - potential entry points
  - vulnerabilities
  - chances of attacking a system/network.
- Possible strategies:
  - **Zero-trust policies**: enforce that only the **right people** have the **right level** of access
  - **Access control**: give to users and applications only the permissions they need to perform their tasks, i.e., **least privilege principle**
  - **Training/Education**: train users on cybersecurity best practices, e.g., recognize phishing and scams.

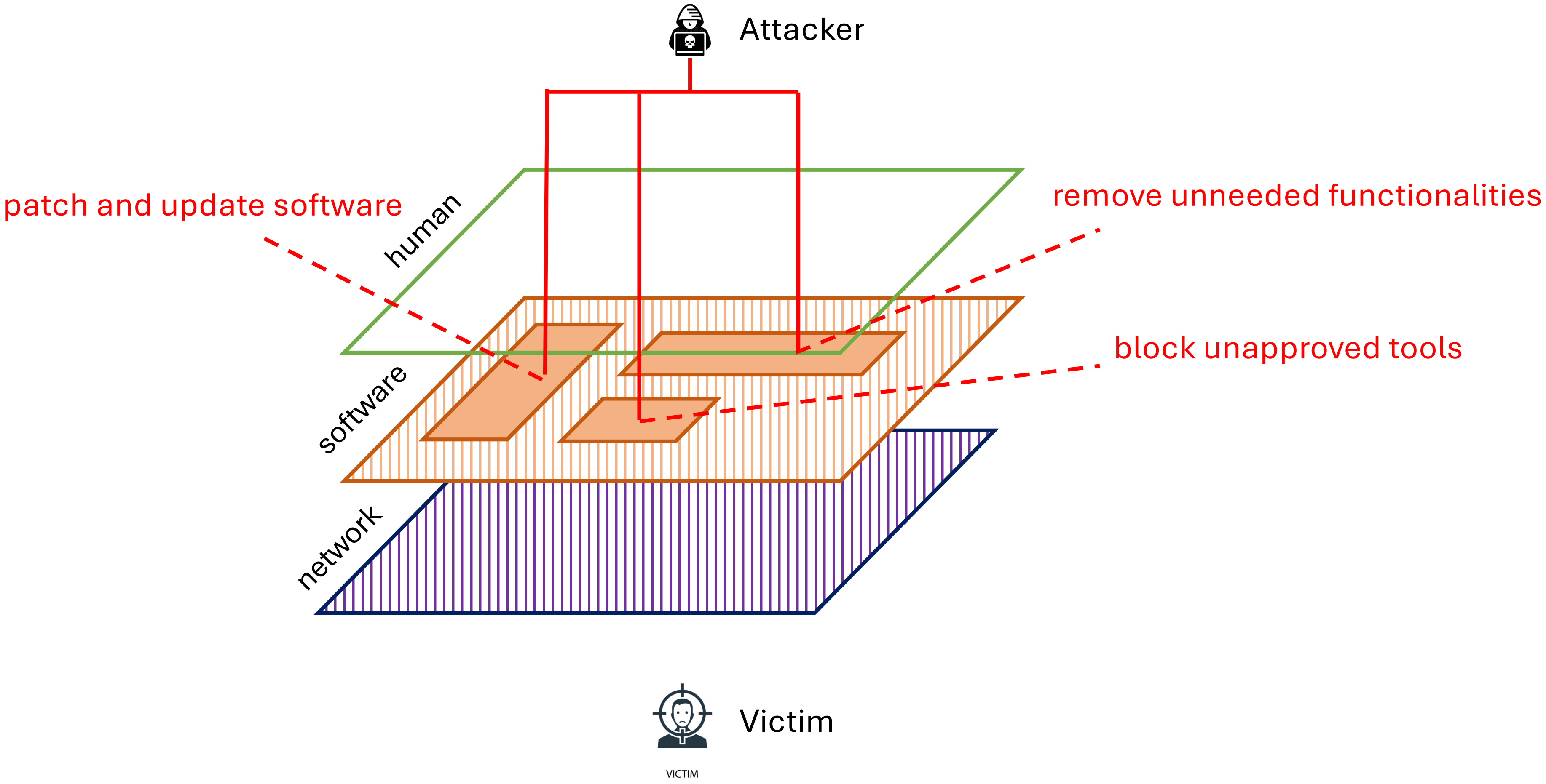
Attack Surface Reduction



Attack Surface Reduction

- The **attack surface reduction** is the process of minimizing:
  - potential entry points
  - vulnerabilities
  - chances of attacking a system/network.
- Possible strategies:
  - **Reduce complexity**: disable unnecessary or unused software and devices and reduce the number of endpoints being involved
  - **Patch and update**: regularly update all software, hardware and firmware to fix known vulnerabilities and prevent their exploitation
  - **Perform tests**: perform periodically vulnerability scans, penetration tests, and security audits to identify and fix potential weaknesses.

Attack Surface Reduction



Attacker

patch and update software

remove unneeded functionalities

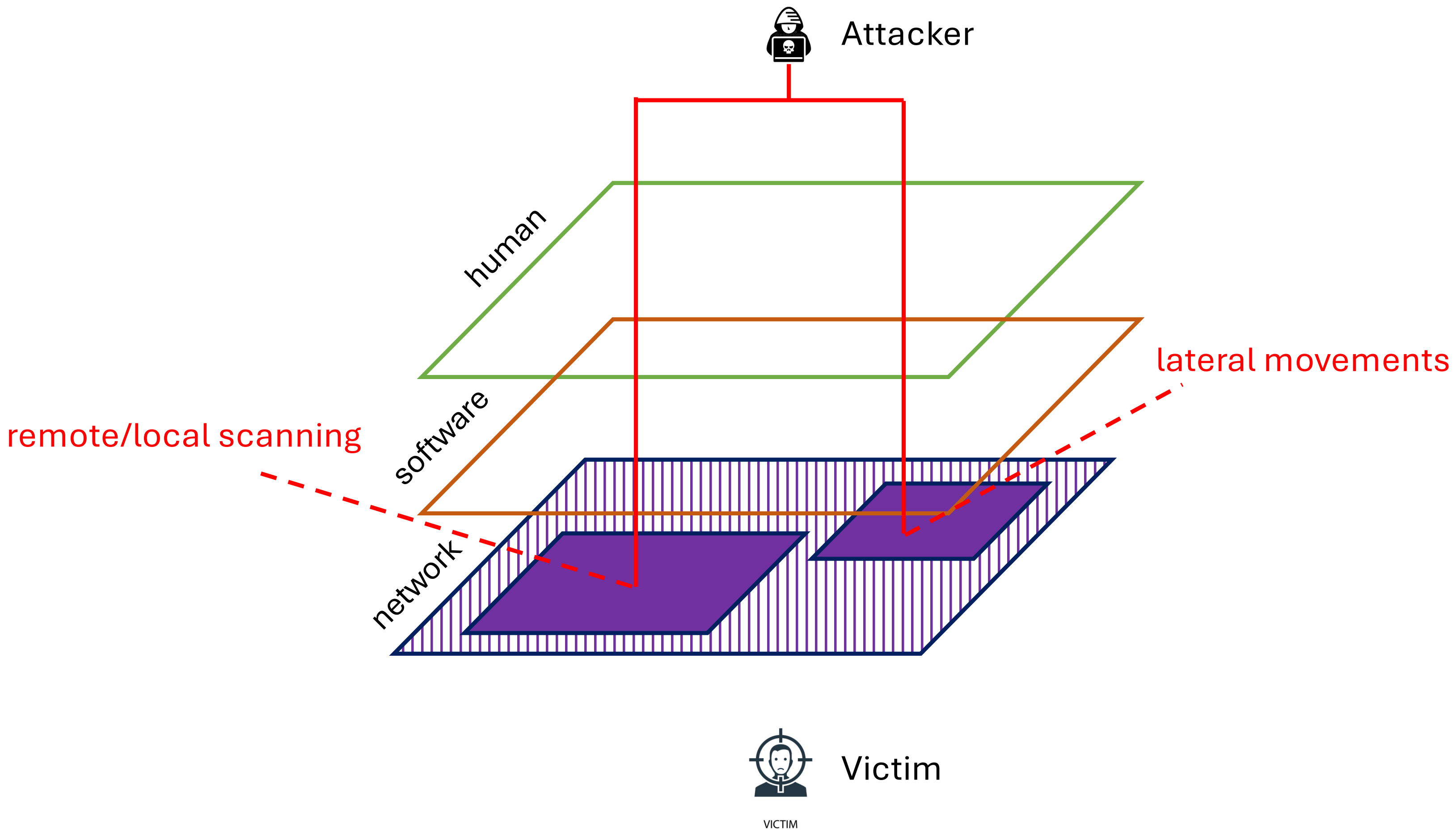
block unapproved tools

Victim

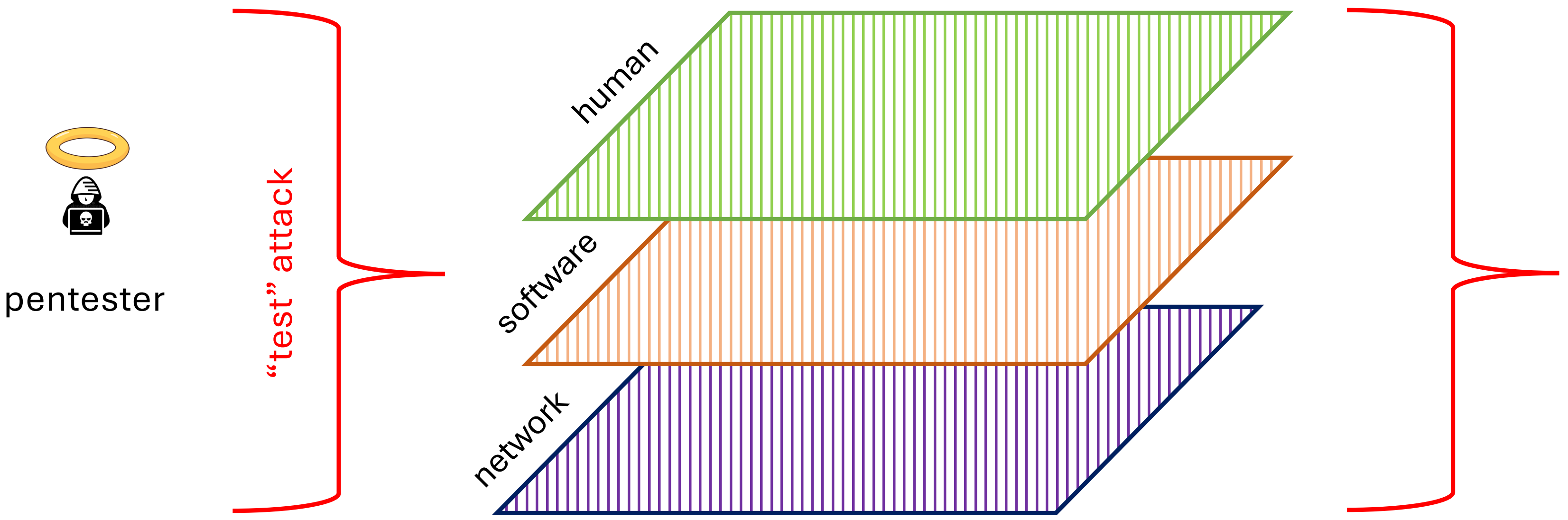
Attack Surface Reduction

- The **attack surface reduction** is the process of minimizing:
  - potential entry points
  - vulnerabilities
  - chances of attacking a system/network.
- Possible strategies:
  - **Segment network**: divide the network into smaller, isolated segments to contain impacts of potential attacks
  - **Patch and update**: regularly update all nodes or appliances to fix known vulnerabilities and prevent their exploitation
  - **Perform tests**: perform periodically vulnerability scans, penetration tests, and security audits to identify and fix potential weaknesses.

Attack Surface Reduction



Attack Surface Reduction



pentester

“test” attack

human

software

network

Report

I.T. CONGRATULATING ME FOR NOT FALLING FOR THE PHISHING TEST
ME WHO DOESN'T READ EMAILS

@InfosecMemes_

Possible Vulnerabilities

- Vulnerability:
  - a flaw or weakness in an information system or system security procedures that could be exploited for violating a security policy.
- Examples of **vulnerabilities** by “**nature**”:
  - **unintentional**: bugs
  - **intentional**: backdoors.
- Examples of **vulnerabilities** by **domain**:
  - **technology**: flawed designs or specifications and software/hardware implementations
  - **operation** and **management**: inadequacy of detection approaches or ineffective practices and tools
  - **human**: bad behaviors or permeability to psychological manipulation (e.g., social engineering).

Possible Vulnerabilities

- Vulnerability:
  - a flaw or weakness in an information system or system security procedures that could be exploited for violating a security policy.
- Examples of **network** and **protocol** **vulnerabilities**:
  - protocol specification flaws
  - protocol implementation flaws
  - misuses: abuse of dynamic configuration protocol or unsecure communications.
- Examples of **software** and **hardware** **vulnerabilities**:
  - implementation flaws
  - OS flaws
  - hardware flaws.

Question Time

How to quantify the “strength” of an encryption algorithm?

```
nWEOJ90QeSlg518Klh+9Y3YEw6Rj/psI/Si2i13SXu2hd/8ZRU
wjAlIcMbnSjFILj0GX86dNKud8OxYhtSb9CLZf3e5v4fg+DT+F
zoLKpNoeNetCLVbC+txAj5QFCYSV3kkcTSa63RWHNN1mzn
Z/qAVGGVNtPN3gpLEYQZWikfkDXIOlhEGUnGiN2X1kwPeC
UV+ZDySVLalN4GoqKFIetZYnrmmtXKh0xEjJUQxzq9RUbsaJ
cnw3quGRlPk0eXE2
```

(*)

(*) Leslie Edward Claypool, detto Les (Richmond, 29 settembre 1963), è un bassista, cantante e compositore statunitense, membro fondatore e leader del gruppo alternative metal Primus.

Question Time

How to quantify the “strength” of an encryption algorithm?

nWEOJ90QeSlg518Klh+9Y3YEw6Rj/psI/Si2i13SXu2hd/8ZRU
wjAlIcMbnSjFILj0GX86dNKud8OxYhtSb9CLZf3e5v4fg+DT+F
zoLKpNoeNetCLVbC+txAj5QFCYSV3kkcTSa63RWHNN1mzn
Z/qAVGGVNtPN3gpLEYQZWikfkDXIOlhEGUnGiN2X1kwPeC
UV+ZDySVLalN4GoqKFIetZYnrmmtXKh0xEjJUQxzq9RUbsaJ
cnw3quGRlPk0eXE2 (*)

Possible factors to consider: the length of the key, the availability of plaintext, the “complexity” of the used algorithm, and the required/available computational resources.

AES: CBC, PKCS5 Padding, no IV,
Secret Key: 2312896327181234

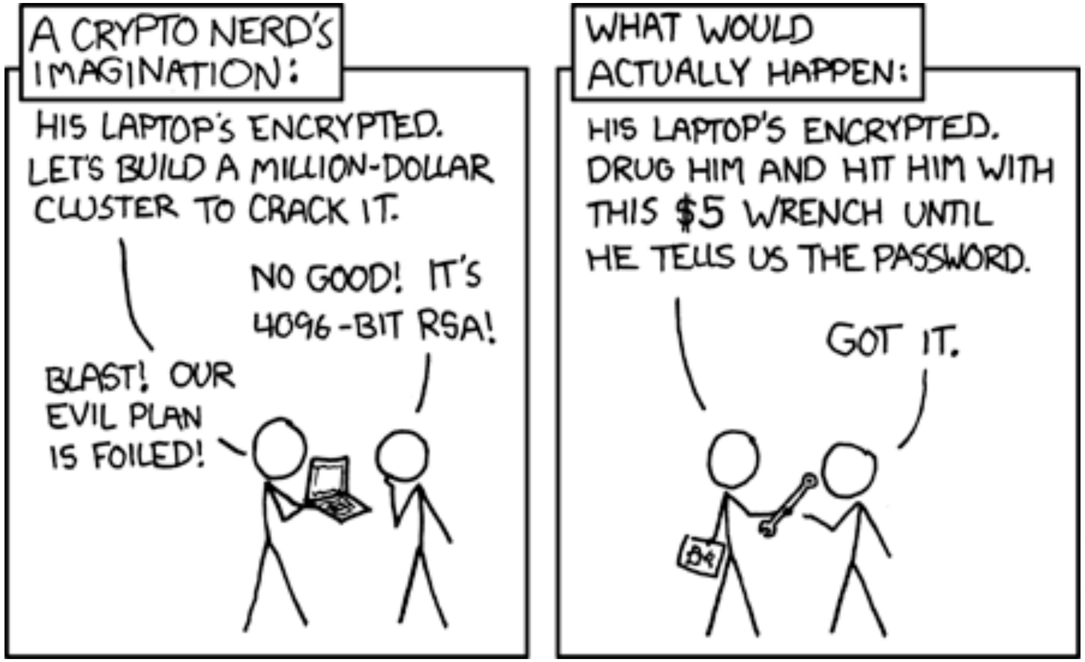
(*) Leslie Edward Claypool, detto Les (Richmond, 29 settembre 1963), è un bassista, cantante e compositore statunitense, membro fondatore e leader del gruppo alternative metal Primus.

The Human Element

- *Rubber-hose cryptanalysis,* Marcus J. Ranum, 1990.

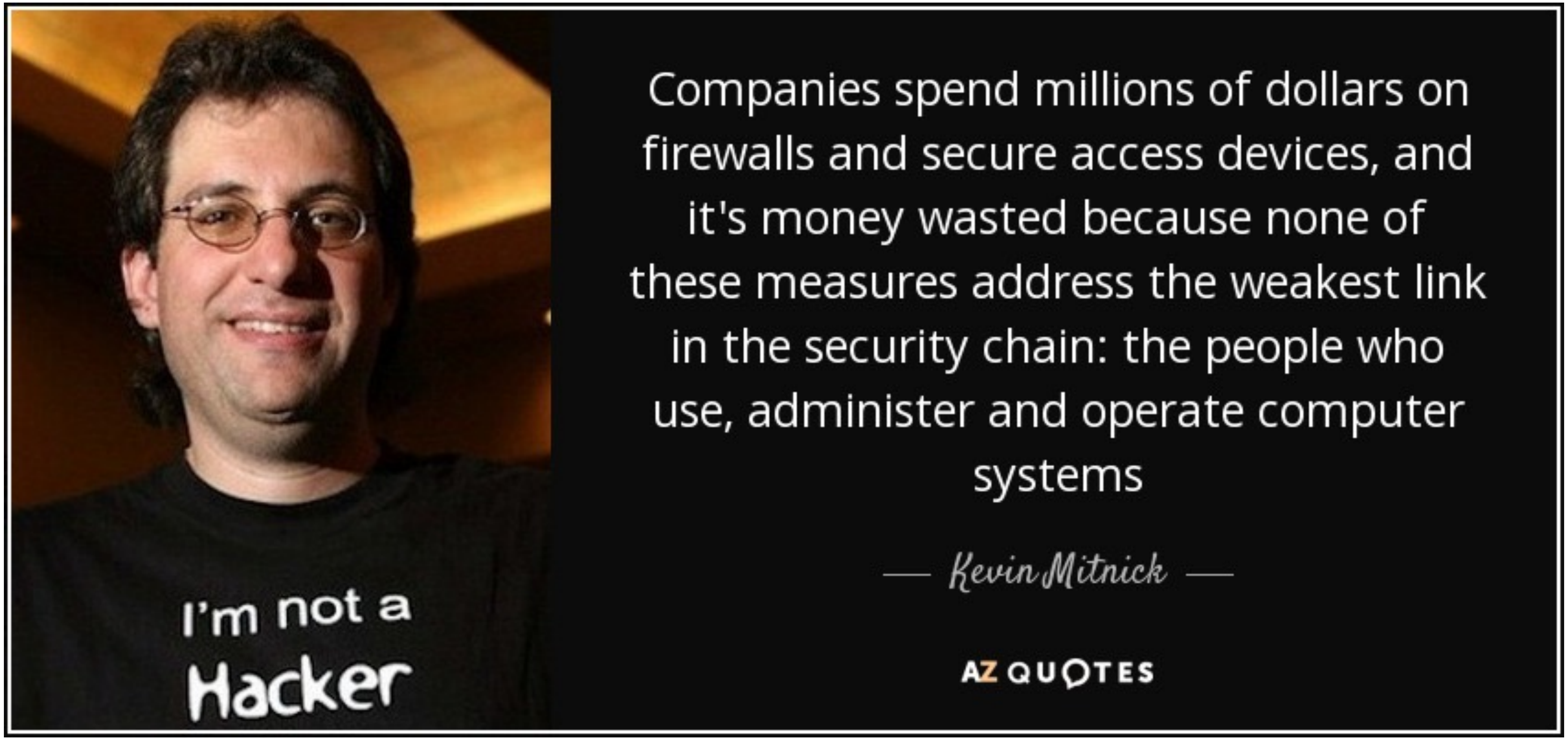
The Human Element

- *Rubber-hose cryptanalysis,* Marcus J. Ranum, 1990.


A CRYPTO NERD'S IMAGINATION:
HIS LAPTOP'S ENCRYPTED. LET'S BUILD A MILLION-DOLLAR CLUSTER TO CRACK IT.
NO GOOD! IT'S 4096-BIT RSA!
BLAST! OUR EVIL PLAN IS FOILED!
WHAT WOULD ACTUALLY HAPPEN:
HIS LAPTOP'S ENCRYPTED. DRUG HIM AND HIT HIM WITH THIS $5 WRENCH UNTIL HE TELLS US THE PASSWORD.
GOT IT.

Source: XKCD

The Human Element


I'm not a
Hacker

Companies spend millions of dollars on firewalls and secure access devices, and it's money wasted because none of these measures address the weakest link in the security chain: the people who use, administer and operate computer systems

— Kevin Mitnick —

AZ QUOTES

Source: AZ Quotes

Question Time

What is wrong?

Q	w	e	r	t	y	u	i	o

1	2	3	q	w	e

1	q	2	w	3	e	4	r

Question Time

- These passwords are:
  - predictable
  - easy to guess
  - easy to generate via software
  - **patterns**!

Q	w	e	r	t	y	u	i	o

1	2	3	q	w	e

1	q	2	w	3	e	4	r

The Human Element

- These passwords are:
  - predictable
  - easy to guess
  - easy to generate via software
  - **patterns**!

Q	w	e	r	t	y	u	i	o

1	2	3	q	w	e

1	q	2	w	3	e	4	r

Dig: Jonh The Ripper (*https://github.com/openwall/john*)

Dictionaries are quite easy to prepare and “wallow” in social engineering!

The Human Element

- These passwords are:
  - predictable
  - easy to guess
  - easy to generate via software
  - **patterns**!

Q	w	e	r	t	y	u	i	o
1	2	3	q	w	e			
1	q	2	w	3	e	4	r	

Dig: Jonh The Ripper (*https://github.com/openwall/john*)

https://github.com/ihebski/DefaultCreds-cheat-sheet

Very easy to **automate** the **search** for **default credentials** or the creation of **mutations**!

The Human Element

- These passwords are:
  - predictable
  - easy to guess
  - easy to generate via software
  - **patterns**!

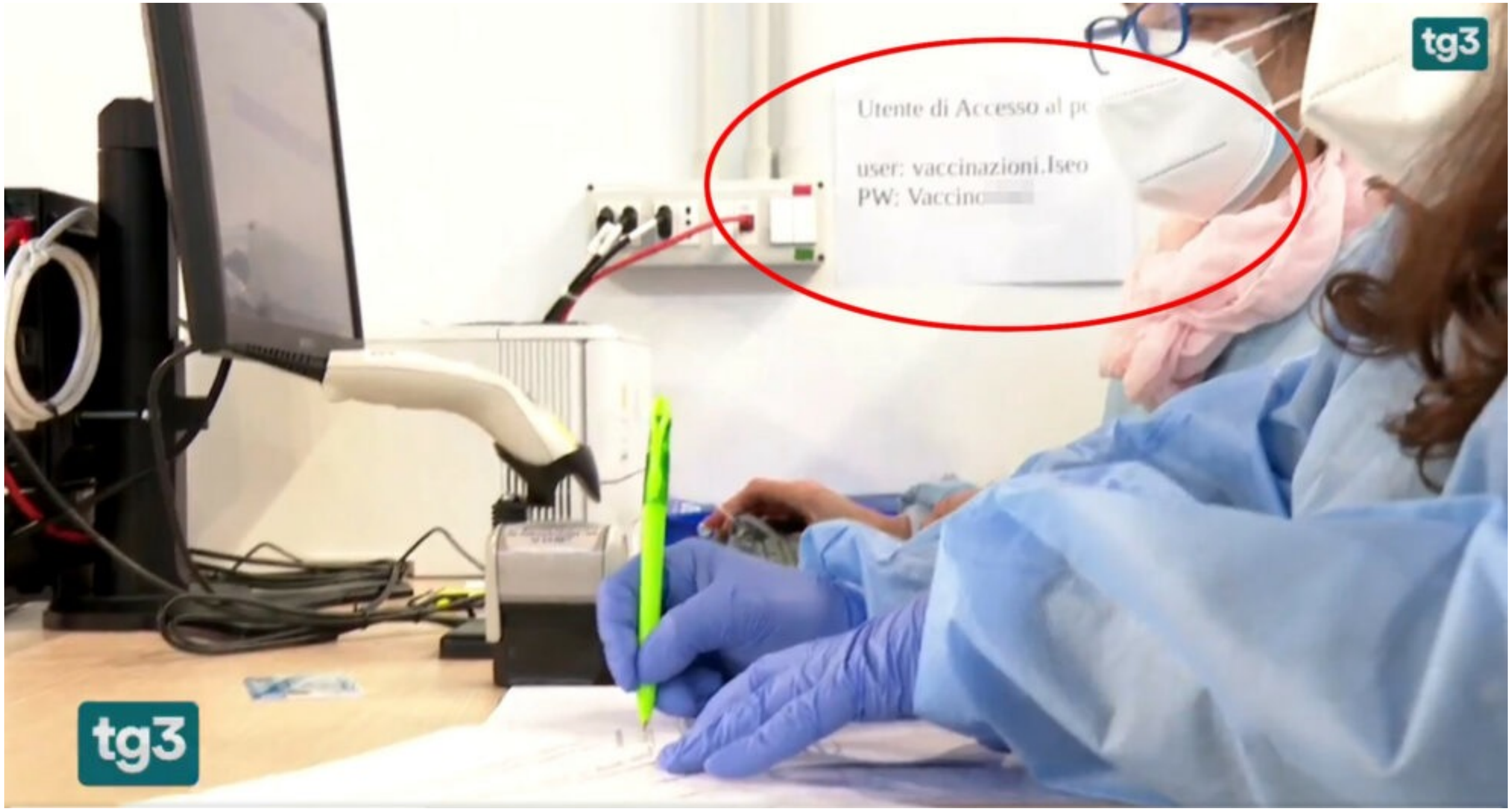
Q	w	e	r	t	y	u	i	o

1	2	3	q	w	e

1	q	2	w	3	e	4	r

It would be better to use something more complicated, being careful not to ruin the attempt.

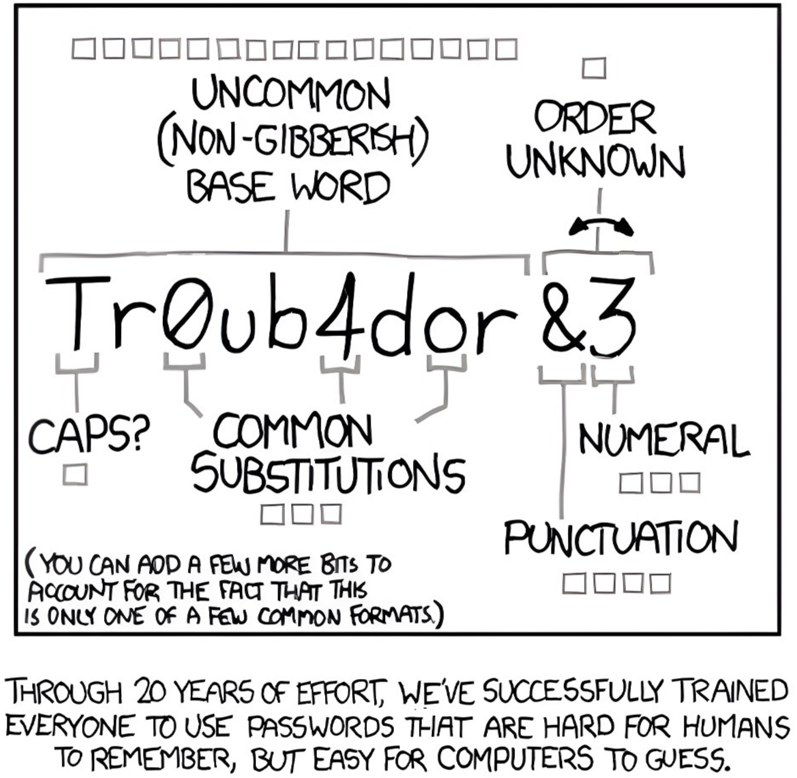
…a Dramatic Turn of Events



Vaccination Hub in Brescia, Italy

Source: TG3 of 6 March 2021.

The Final Recap on the "Human Element"


UNCOMMON (NON-GIBBERISH) BASE WORD
ORDER UNKNOWN
Tr0ub4dor&3
CAPS?
COMMON SUBSTITUTIONS
NUMERAL
PUNCTUATION
(YOU CAN ADD A FEW MORE BITS TO ACCOUNT FOR THE FACT THAT THIS IS ONLY ONE OF A FEW COMMON FORMATS.)
THROUGH 20 YEARS OF EFFORT, WE'VE SUCCESSFULLY TRAINED EVERYONE TO USE PASSWORDS THAT ARE HARD FOR HUMANS TO REMEMBER, BUT EASY FOR COMPUTERS TO GUESS.

Source: XKCD

It is **very hard** to **protect** or **reduce** an attack surface when "stupid" things are done by **humans**. And poor management of credentials and passwords are just the **tip of the iceberg**!

Wrap Up

- Cybersecurity has a huge **impact** on our **society**, also in terms of **economical losses** and **socio-political implications.**
- **Everyone** has a **responsibility** in the overall security posture!
- Prime **conceptual frameworks** to describe a cyber attacks are the **Cyber Kill Chain** and **attack trees**.
- It is vital being able to **outline** and **recognize attack surfaces**, which are different and composite.
- A relevant amount of the cybersecurity **routine** is to operate in an **attack surface reduction flavor**.
- **...but the human element will always play a major role**.