

# Introduction to Computer Security Lecture Slides

© 2024 by [Mihai Chiroiu](#) & [Florin Stancu](#)

is licensed under [Attribution-NonCommercial-ShareAlike 4.0  
International](#)

# Introduction to cybersecurity

# Honor Code

*“My job is to talk to you, and your job is to listen. If you finish first, please let me know.”*

Harry Hershfield



# Selected topics

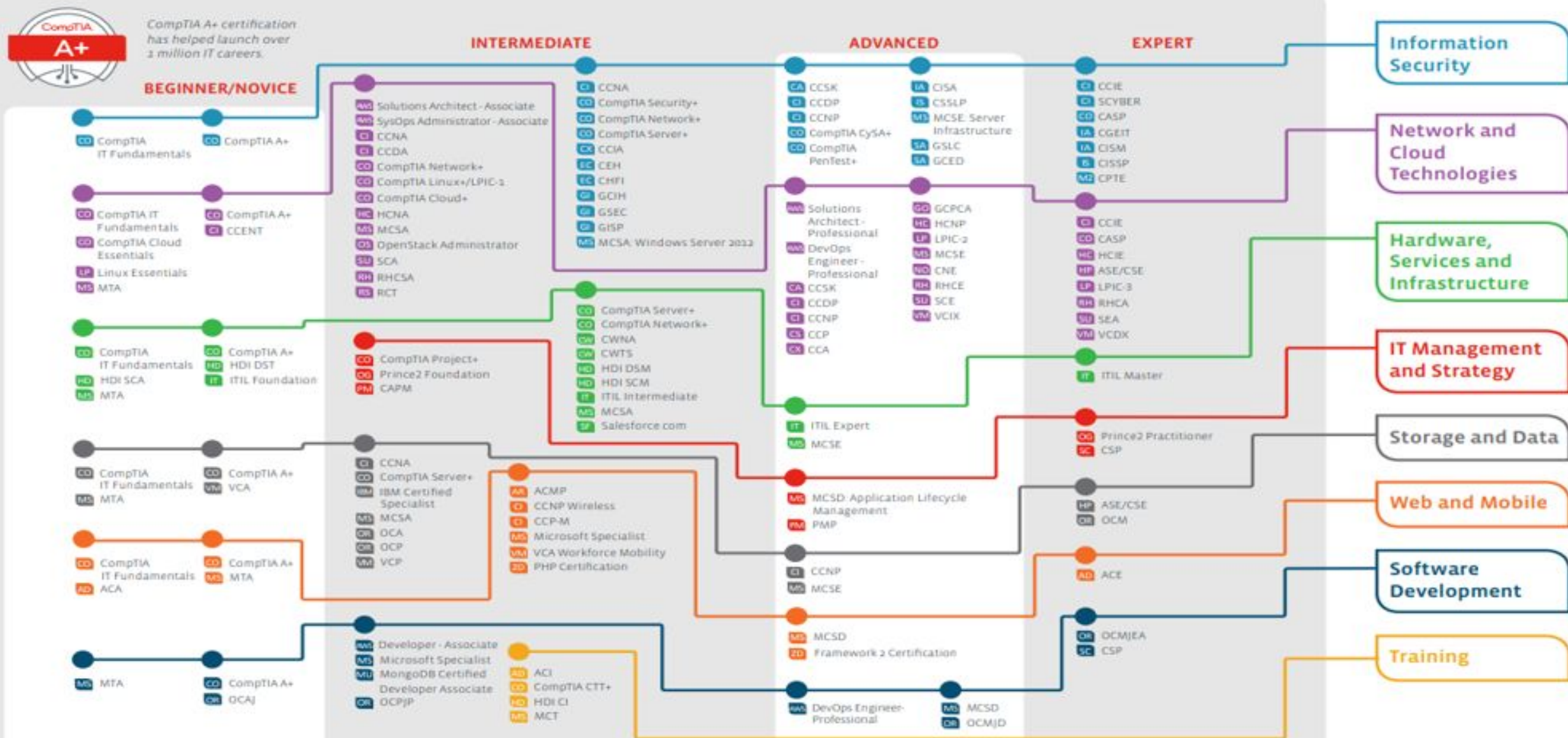
1. Introduction. Cybersecurity properties.
2. Cryptography fundamentals.
3. Authentication & Key Establishment.
4. Access Control & OS Security.
5. Application Security (Buffer overflow).
6. Malware and anti-malware techniques.
7. Web Applications Security (DB security, XSS).
8. Local Network Security.
9. Public Key Infrastructure.
10. Remote Network Security.
11. Privacy Preserving Technologies.
12. Hardware Security.
13. AI/ML security.

# IT Certification Roadmap

Explore the possibilities with the CompTIA Interactive IT Roadmap at:  
[CompTIA.org/CertsRoadmap](https://CompTIA.org/CertsRoadmap)

CompTIA

Certifications validate expertise in your chosen career.



Computer literacy certifications validating end user skills include IC3 and ECDL/ICDL

Updated 6/2018

# Logistics

# Materials

- <https://ocw.cs.pub.ro/courses/isc>

# Grading

- **1.5p** - Homework 1
- **1.5p** - Homework 2
- **2p** - 11 Labs (11 x 0.1818181818...)
- **3p** - Final practical exam (TBA)
- **2p** - Final written exam (TBD)
- **Total = 10p**
- **Min. 5p to pass the course. At least 50% at final exams!**



# Cybersecurity Properties

# What is security? (theory)

- Cybersecurity is, given an **attacker's model** and a specific **context**, the technique to control **who** may **use** or **modify** the **data**.

# What is security? (reality)

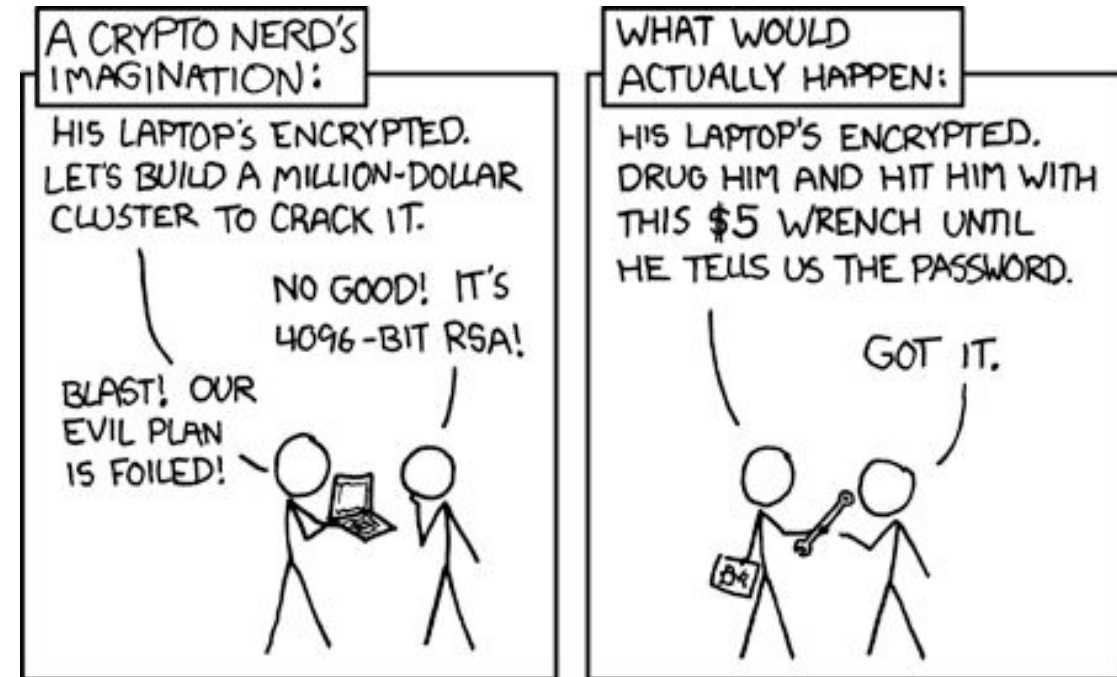
- “Measures designed to produce a feeling of security rather than the reality.” Bruce Schneier



<https://desciclopedia.org/wiki/Arquivo:Blogmouse.png>

# Theory vs. Reality

- Economics:
  - Don't protect \$1B with encryption that can be broken for \$1M.
  - Don't spend \$10M to protect \$1M.



# Romanian Legislation (not translated)

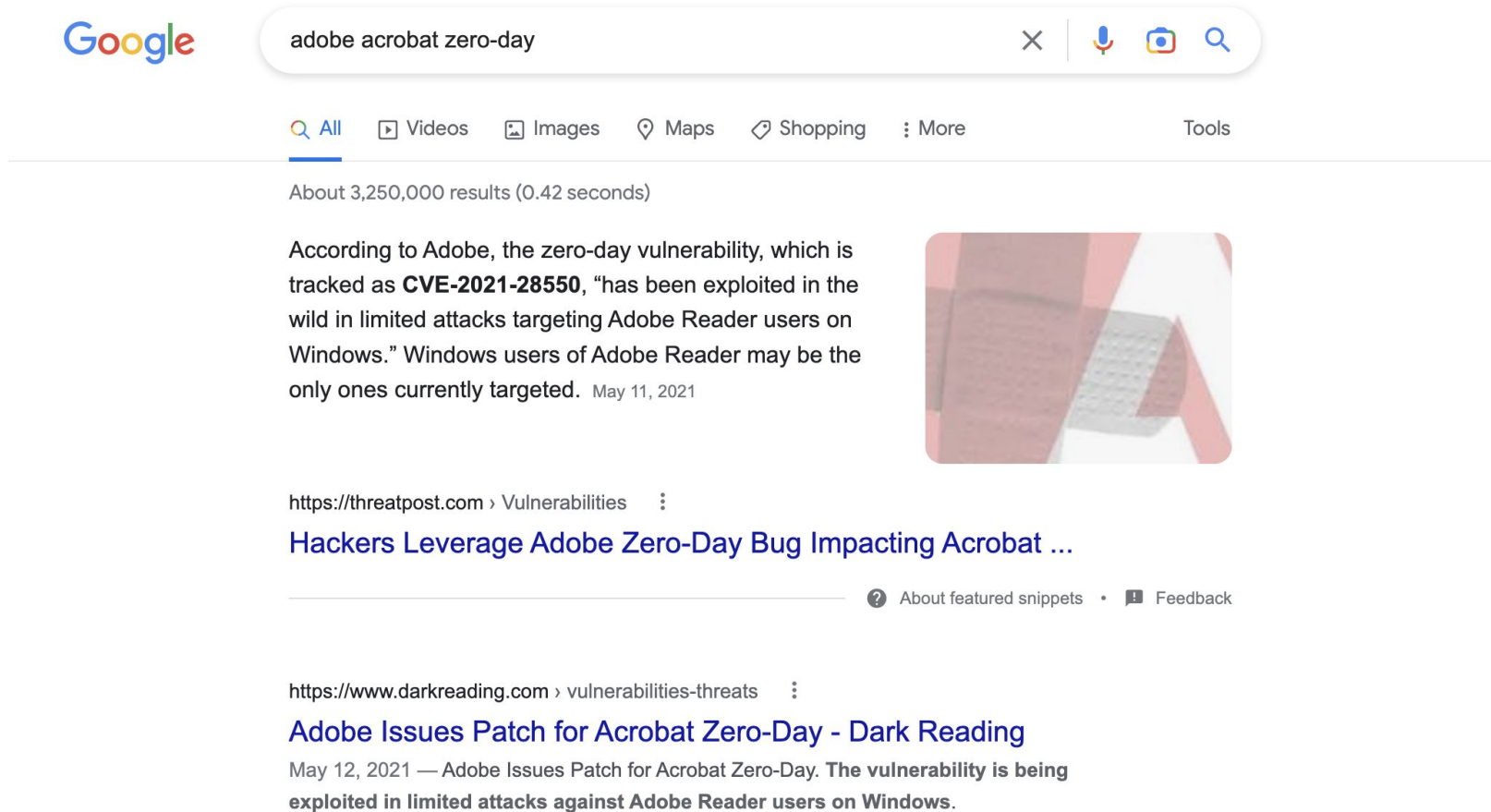
- Introducerea, modificarea sau ștergerea de date informatice, restricționarea accesului la aceste date ori împiedicarea în orice mod a funcționării unui sistem informatic [...] se pedepsește cu închisoarea de la 2 la 7 ani.
- Lege 286/2009 – Art. 360
  - (1) Accesul, fără drept, la un sistem informatic se pedepsește cu închisoare de la 3 luni la 3 ani sau cu amendă.
  - (2) Fapta prevăzută în alin. (1), săvârșită în scopul obținerii de date informatice, se pedepsește cu închisoarea de la 6 luni la 5 ani.
  - (3) Dacă fapta prevăzută în alin. (1) a fost săvârșită cu privire la un sistem informatic la care [...] accesul este restricționat sau interzis pentru anumite categorii de utilizatori, pedeapsa este închisoarea de la 2 la 7 ani.

# Security Theatre

# Assets

- What is interesting and why in the cyber world?
- Often not sufficiently accounted for, therefore hackable
  - E.g. because everyone wants fast business increases

# Exploitability of assets



The screenshot shows a Google search interface with the query "adobe acrobat zero-day". The search results indicate approximately 3,250,000 results found in 0.42 seconds. A featured snippet is displayed, stating that a zero-day vulnerability, tracked as **CVE-2021-28550**, has been exploited in limited attacks targeting Adobe Reader users on Windows. The snippet is dated May 11, 2021. Below the snippet, two search results are visible. The first result is from threatpost.com, titled "Hackers Leverage Adobe Zero-Day Bug Impacting Acrobat ...". The second result is from darkreading.com, titled "Adobe Issues Patch for Acrobat Zero-Day - Dark Reading", dated May 12, 2021, and states that the vulnerability is being exploited in limited attacks against Adobe Reader users on Windows.

Google

adobe acrobat zero-day

All Videos Images Maps Shopping More Tools

About 3,250,000 results (0.42 seconds)

According to Adobe, the zero-day vulnerability, which is tracked as **CVE-2021-28550**, "has been exploited in the wild in limited attacks targeting Adobe Reader users on Windows." Windows users of Adobe Reader may be the only ones currently targeted. May 11, 2021

<https://threatpost.com/Vulnerabilities>

**Hackers Leverage Adobe Zero-Day Bug Impacting Acrobat ...**

<https://www.darkreading.com/vulnerabilities-threats>

**Adobe Issues Patch for Acrobat Zero-Day - Dark Reading**

May 12, 2021 — Adobe Issues Patch for Acrobat Zero-Day. The vulnerability is being exploited in limited attacks against Adobe Reader users on Windows.



# Attack surface

- External
- Internal
  - Malicious
  - Mistake

# Attackers - headlines

- World's Biggest Data Breaches & Hacks
  - <http://www.informationisbeautiful.net/visualizations/worlds-biggest-data-breaches-hacks/>

# Attackers

- From pranksters to professionals:
  - Script Kiddies
  - Vulnerability Brokers vs Cybercriminals
    - Bug bounty programs
  - Hacktivists
  - National State Adversaries
  - Advanced persistent threat (APT)

# Hacker's tools

- Password crackers
  - John the Ripper, Ophcrack, L0phtCrack, THC Hydra, RainbowCrack, and Medusa.
- Wireless hacking tools
  - Aircrack-ng, Kismet, InSSIDer, KisMAC, Firesheep, and NetStumbler.
- Forensic tools
  - Sleuth Kit, Helix, Maltego, and Encase.

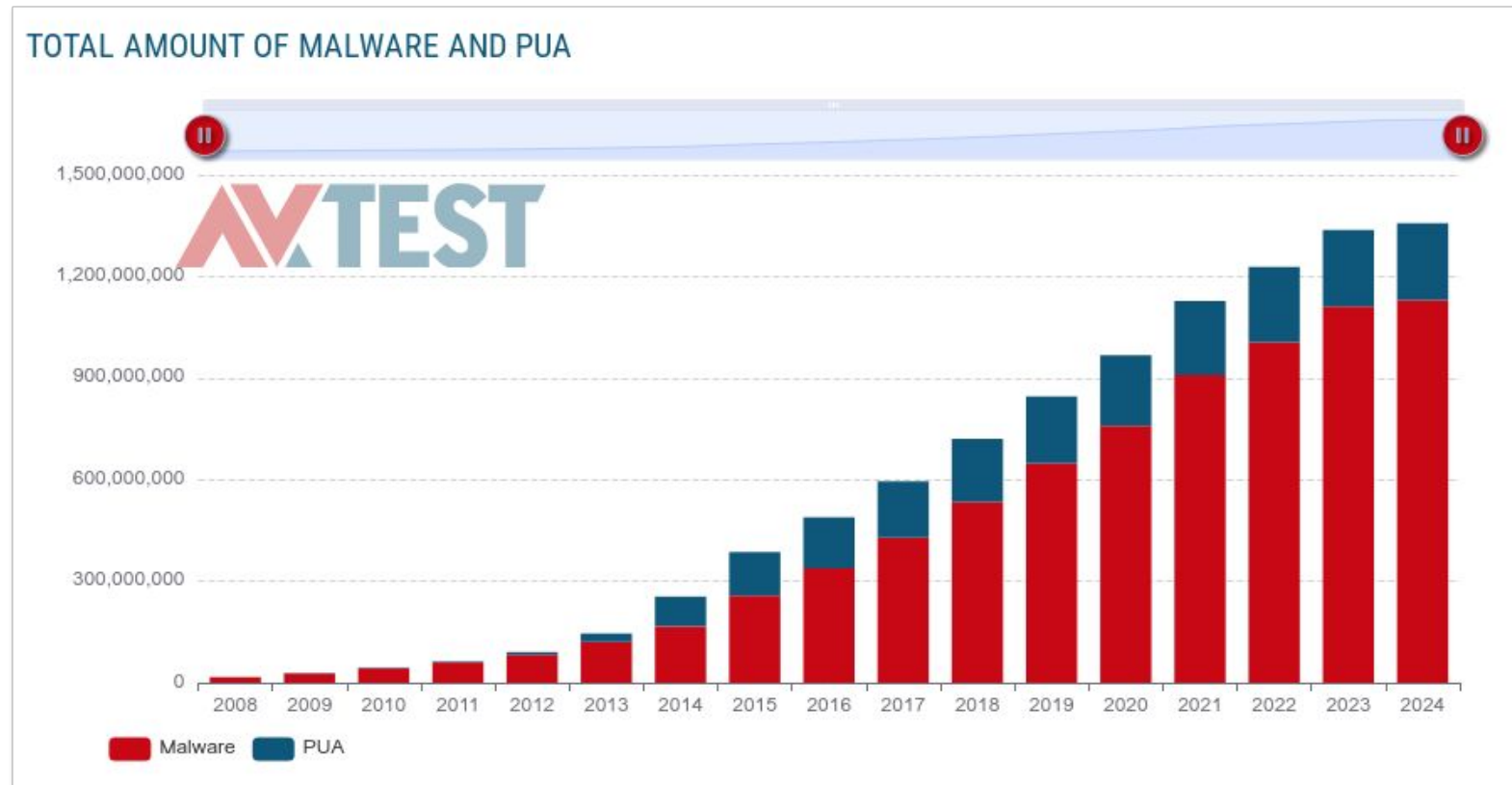
# Hacker's tools

- Network scanning and hacking tools
  - Nmap, SuperScan, Angry IP Scanner, and NetScanTools.
- Packet crafting tools
  - Hping, Scapy, Socat, Yersinia, Netcat, Nping, and Nemesis.
- Packet sniffers
  - Wireshark, Tcpdump, Ettercap, Dsniff, EtherApe, Paros, Fiddler, Ratproxy, and SSLstrip.
- Rootkit detectors
  - AIDE, Tripwire, RKHunter
- Fuzzers to search vulnerabilities
  - Skipfish, Wapiti, and W3af.

# Hacker's tools

- Debuggers
  - GDB, WinDbg, IDA Pro, and Immunity Debugger.
- Hacking operating systems
  - Kali Linux, SELinux, Knoppix, Parrot OS, and BackBox Linux.
- Encryption tools
  - VeraCrypt, CipherShed, Open SSH, OpenSSL, OpenVPN, and Stunnel.
- Vulnerability exploitation tools
  - Metasploit, Core Impact, Sqlmap, Social Engineer Tool Kit, and Netsparker.
- Vulnerability scanners
  - Nipper, Securia PSI, Core Impact, Nessus, SAINT, and Open VAS.

# New malware and potentially unwanted applications (PUA)



<https://www.av-test.org/en/statistics/malware/>

# Original war: Creeper & Reaper

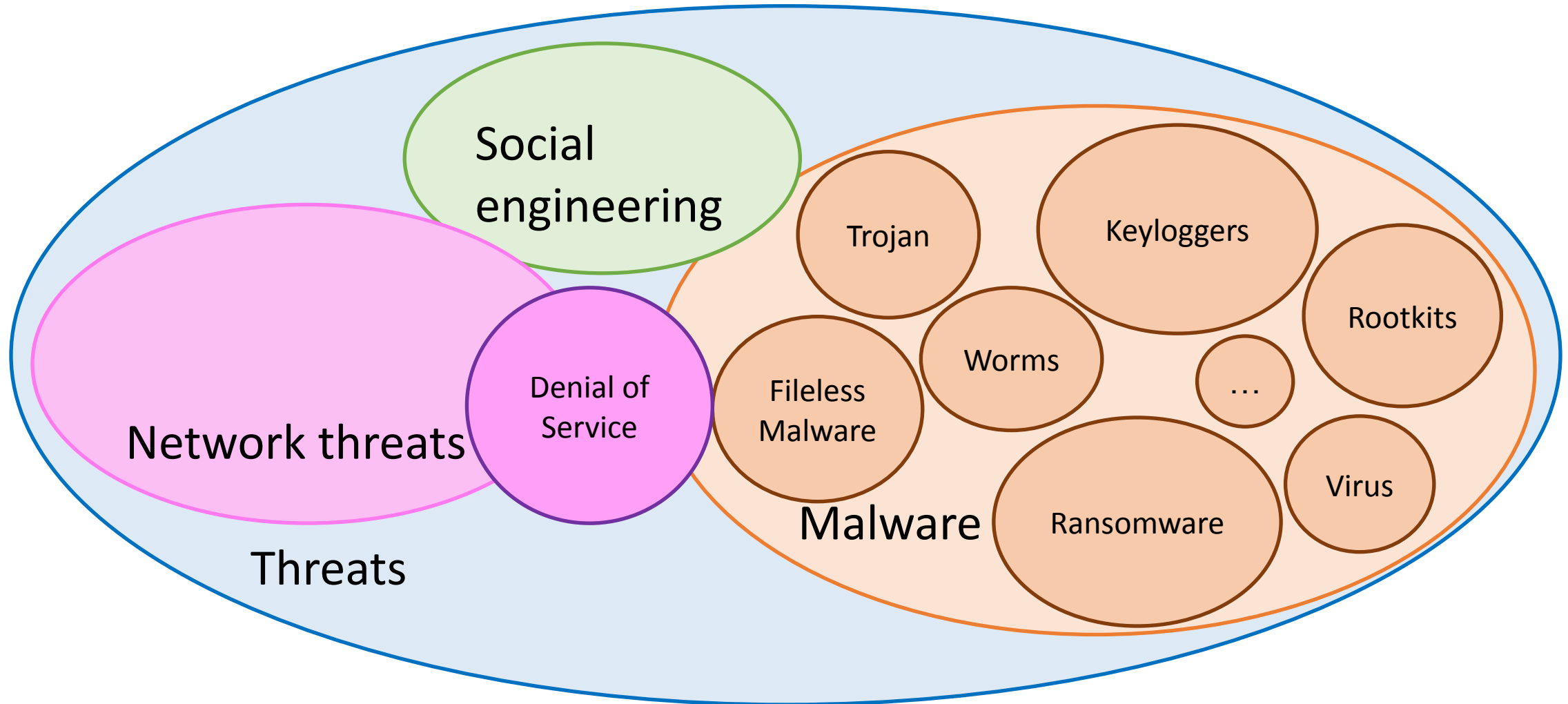
```
BBN-TENEX 1.25, BBN EXEC 1.30
@FULL
@LOGIN RT
JOB 3 ON TTY12 08-APR-72
YOU HAVE A MESSAGE
@SYSTAT
UP 85:33:19 3 JOBS
LOAD AV 3.87 2.95 2.14
JOB TTY USER SUBSYS
1 DET SYSTEM NETSER
2 DET SYSTEM TIPSER
3 12 RT EXEC
@
I'M THE CREEPER : CATCH ME IF YOU CAN
```

<https://corewar.co.uk/creeper.htm>

- Bob Thomas created “Creeper”, a software that moved between computers with a TENEX operating system in 1971.
- Ray Tomlinson (email creator) added self-copying, instead of moving.
- Ray Tomlinson created Reaper, to chase and delete “Creeper”.



# Types of threats



# Types of malware

- Virus – infects files, spreads when opening them
- Worm – automatically infects other systems!
  - Logic bomb
- Trojan horse – user must explicitly open crafted exe
  - Remote Access Trojan
- Ransomware – Money for your data!
- Spyware – NSA, Pegasus etc. ;)
- Adware – the entire WWW :(

# Attackers vs defenders

- Anti-viruses?
- In general, it's easier to destroy than to create
  - `"rm --rf --no-preserve-root /"`
- Evasion Method
  - Encryption and tunneling
  - Resource exhaustion
  - Traffic fragmentation
  - Protocol-level misinterpretation
  - Traffic substitution

# NIST framework



# Defenders

- Interesting maps
  - <https://cybermap.kaspersky.com/>
  - <https://www.talosintelligence.com/>
  - <https://threatmap.fortiguard.com/>
  - <https://threatmap.checkpoint.com/>

# Defender's tasks

- Use a trustworthy IT vendor
- Keep security software up-to-date
- Perform regular penetration tests
- Backups (online + offline + remote + recovery testing!)
- Periodically change passwords (e.g., WiFi)
- Keep security policy up-to-date
- Enforce use of strong passwords
- Use two factor authentication

# Defender's tools

- Penetration testing
  - Black box (unknown environment)
  - White box (known environment)
  - Gray box (partially known environment—to model insider threat agents, for instance)
- Tactics, Techniques, and Procedures (TTPs)
  - Generalized statement of adversary behavior
  - Campaign strategy and approach (tactics)
  - Generalized attack vectors (techniques)
  - Specific intrusion tools and methods (procedures)
- Indicator of compromise (IoC)
  - Specific evidence of intrusion
  - Individual data points
  - Correlation of system and threat data
  - AI-backed analysis
  - Indicator of attack (IoA)

# Threat hunting

- Use log and threat data to search for Indicators of Compromise (IoC)
- Plan threat hunting project in response to newly discovered threat
- Use Security Information and Event Management (SIEM)
- Consider possibility of alerting adversary to the search



# Security properties

# Rainbow Series (1985)

- Department of Defence Trusted Computer System Evaluation Criteria (TCSEC)
- Orange Book – computers, examples:
  - D = No security
  - C1 = Discretionary Access Control
  - B3 = Trusted Path & Tamperproof
  - A1 = Formal Methods & Supply chain security
- Red Book – networks
- Green Book - passwords



[https://en.wikipedia.org/wiki/Rainbow\\_Series#/media/File:Rainbow\\_series\\_documents.jpg](https://en.wikipedia.org/wiki/Rainbow_Series#/media/File:Rainbow_series_documents.jpg)

# Common Criteria for Information Technology Security Evaluation

- Cybersecurity meet bureaucracy ;)
- Two types kinds of evaluations:
  - A protection profile (PP) describes a family of products.
  - A security target (ST) addresses security issues relative to a specific product.
- EAL: Evaluation Assurance Level

# Common Criteria for Information Technology Security Evaluation

- <https://www.commoncriteriaportal.org/>
  - Canonical Ubuntu Server 18.04.4 : EAL2 (Evaluation assurance level 2), ALC\_FLR (Flaw remediation)
    - <https://ubuntu.com/security/certifications/docs/16-18/cc>
  - Microsoft Windows 11, Windows Server 2022: EAL4+
    - <https://learn.microsoft.com/en-us/windows/security/threat-protection/windows-platform-common-criteria>

# TCSEC vs CC

TCSEC	CC
D	-
-	EAL1
C1	EAL2
C2	EAL3
B1	EAL4
B2	EAL5
B3	EAL6
A1	EAL7

# Security properties - Basics

- Confidentiality
  - Prevent disclosure of sensitive information to unauthorized parties.
- Integrity
  - Protection/Detection of data from intentional or accidental modification.
- Availability
  - Assurance that systems and data are accessible by authorized users when needed.

# Security properties - Basics

- Non-repudiation – origin and/or reception of message cannot be denied in front of third party

# Security properties

- Data protection/personal data privacy
  - fair collection and use of personal data, in Europe a set of legal requirements
- Anonymity/untraceability
  - ability to use a resource without disclosing identity/location
- Pseudonymity
  - anonymity with accountability for actions.



# Security properties

- Unlinkability
  - ability to use a resource multiple times without others being able to link these uses together
  - Bad examples: HTTP “cookies” / most crypto-currencies
- Unobservability
  - ability to use a resource without revealing this activity to third parties

# Security properties

- Rollback
  - ability to return to a well-defined valid earlier state (backup, revision control, undo)
- Audit – monitoring and recording of user-initiated events to detect and deter security violations
- Copy protection, information flow control
  - ability to control the use and flow of information
  - Digital Rights Management

# What is there to secure?

- Data at rest
- Data in transit
- Data in use

# Security Administration

# Security Administration

- Policies
- Standards
- Guidelines
- Procedures
- Baselines

# Security Policy

- A **contract** that states how to protect information assets
  - It needs to be “s.m.a.r.t.” (specific measurable achievable timely)
  - Management instructions indicating a course of action, a guiding principle, or appropriate procedure
  - High-level statements that provide guidance to workers who must make present and future decisions
  - Must be communicated to others
- It defines what “security” means for an organization

# Security Policy - example

- Authentication policy
  - Specifies authorized persons that can have access to network resources and identity verification procedures.
- Password policies
  - Ensures passwords meet minimum requirements and are changed regularly.
- Acceptable Use Policy (AUP)
  - Identifies network applications and uses that are acceptable to the organization. It may also identify ramifications if this policy is violated.
- Remote access policy
  - Identifies how remote users can access a network and what is accessible via remote connectivity.
- Maintenance policy
  - Specifies operating systems and end user application update procedures.
- Incident handling procedures
  - Describes how security incidents are handled.

# Documents Supporting Policies

- Standards – dictate specific minimum requirements in our policies
- Guidelines – suggest the best way to accomplish certain tasks
- Procedures – provide a method by which a policy is accomplished (the instructions)



# Policy Example

- Your personal (protected) health information is stored in a personal electronic folder. (<https://ehr.des-cnas.ro/cnasportalext/index.html>)
- Design a security policy to protect them.
  - What is there to protect?
  - From whom?
  - How long should data be saved?
  - What about CIA?
- Enter **HIPAA Rules and Regulations.**

# Security vs complexity

- Downside: Complexity brings vulnerability
  - How secure is a 1000-computer network with >1000 users and 200 different applications?
  - How secure is a simple button?
- Still, we DO need complexity to accomplish our tasks

# Least privilege

- Complex systems are more difficult to secure.
- The more applications deployed, the more possible vulnerabilities.

# Weakest link

- An infrastructure is as strong as its weakest link.

# References

1. <http://www.phishing.org/history-of-phishing/> (on 31.10.2022)
2. [https://www.owasp.org/images/2/25/OWASP\\_angela\\_sasse\\_appsec\\_eu\\_aug2013.pdf](https://www.owasp.org/images/2/25/OWASP_angela_sasse_appsec_eu_aug2013.pdf) (on 31.10.2022)
3. <http://www.wired.com/2012/08/apple-amazon-mat-honan-hacking/> (on 31.10.2022)
6. <http://arstechnica.com/security/2013/03/spamhaus-ddos-grows-to-internet-threatening-size/> (on 31.10.2022)
7. <https://www.us-cert.gov/ncas/alerts/TA13-088A> (on 31.10.2022)
8. <https://csrc.nist.gov/csrc/media/publications/conference-paper/1998/10/08/proceedings-of-the-21st-nissc-1998/documents/early-cs-papers/dod85.pdf> (on 1.03.2023)

# References (2)

## Online book:

*Computer Security and the Internet: Tools and Jewels*, Paul C. van Oorschot. Springer, 2021.

<https://people.scs.carleton.ca/~paulv/toolsjewels.html>