Intro to Cybersecurity and Useful Tools

By Athina Bampzeli

9/2/26

Contents

1. Introduction
2. Hardware Cybersecurity
3. Software Cybersecurity
4. Case study
5. Cybersecurity Organizations
6. Acronyms and Terminology
7. References and Licenses
8. Take-home message

1)

Introduction

1.1 What is cybersecurity? [1]

- Cybersecurity refers to the protection of people, data, and digital systems from malicious online activities. It involves a combination of technologies, processes, and best practices designed to defend against cyberattacks.
- For organizations, cybersecurity plays a vital role in overall risk management, especially when addressing threats that can disrupt operations or compromise sensitive information. Common risks include ransomware, malware, phishing attempts, data breaches, and increasingly, attacks enhanced by artificial intelligence.
- As these threats become more advanced and frequent, companies are allocating larger budgets toward prevention and response strategies. According to the International Data Corporation (IDC), global spending on cybersecurity is expected to climb to around **$377 billion by 2028**.
- The growing importance of digital security is also driving demand for skilled professionals. The U.S. Bureau of Labor Statistics estimates that jobs for information security analysts will expand by about **32%** between 2022 and 2032, making it one of the fastest-growing career fields.

1.2 Are Cyberattacks crucial? [1]

- Cyberattacks and other forms of cybercrime have the power to disrupt businesses, harm communities, and impact people's lives. Security breaches can result in identity theft, financial extortion, and the exposure of sensitive data, consequences that can severely affect both organizations and the global economy. Experts estimate that by 2025, the total cost of cybercrime could reach **$10.5 trillion annually** worldwide.
- Modern cybercriminals are increasingly using emerging technologies to gain an advantage. As companies move more of their operations to the **cloud** for flexibility and innovation attackers see this shift as an opportunity, an expanded digital landscape with more potential points of entry.
- Criminal networks are also taking advantage of the **dark web**. The IBM X-Force Threat Intelligence Index 2025 reports that advanced threat groups, including some linked to nation-states, are using the dark web's anonymity to trade tools, data, and expertise.
- These actors are operating with unprecedented levels of coordination and automation, turning isolated data breaches into large-scale, highly disruptive cyber incidents.

1.3 Types of Hackers [2]

- Hackers are often grouped into different "hat" categories, each representing their intent and approach toward cybersecurity.
- Black hat hackers are malicious individuals who exploit weaknesses in computer systems or networks for personal gain or to cause harm. They often use malware and other attack methods to steal data or disrupt operations.
- White hat hackers, also known as ethical hackers, are professionals authorized to test systems and uncover vulnerabilities before criminals can exploit them. They work legally, often as part of a company's cybersecurity team or as independent consultants.
- Sitting somewhere between black and white hats, gray hats may uncover and exploit security flaws without permission, but usually not out of malice. While their actions can still be illegal, their goal is often to expose weaknesses or even profit from reporting them.
- Green hat hackers are beginners or enthusiasts who are new to hacking. Though they lack advanced skills, they are eager to learn and experiment as they develop their technical abilities.
- The term blue hat can have different meanings, but it commonly refers to individuals who hack for revenge. Like green hats, they're often amateurs, but their motivation is retaliation rather than learning or professional growth.
- Red hats are sometimes described as vigilantes. Like ethical hackers, they aim to stop black hats, but instead of reporting them, they fight back directly, often using aggressive methods to take down attackers' systems.
- Purple hat hackers test their own systems in controlled environments to improve their skills. The term can also refer to a blend of blue and red hats, those who legally focus on identifying threats and black hat activity, often as part of pre-release testing or system defense.

1.4 Hardware VS Software Cybersecurity

- While software security focuses on safeguarding **applications and systems** through coding practices and digital controls, hardware security builds protection directly into the **physical components** of a device. Both must work together to defend against today’s sophisticated cyber threats and to establish a strong, layered security framework. [3]
- Software-based defenses are often targeted by malware, exploits, or delayed updates. In contrast, hardware security provides features like trusted execution environments and built-in resistance to tampering. [3]
- Software solutions offer flexibility and can quickly adapt to emerging threats, whereas hardware delivers a stable, physical foundation that can protect against vulnerabilities beyond software’s reach. Together, they form a balanced approach to comprehensive cybersecurity. [4]

2)

Hardware Cybersecurity

2.1 Importance of Hardware Cybersecurity

- Cybersecurity hardware appliances and physical modules play a crucial role in protecting both digital operations and physical infrastructure from cyber threats. These devices integrate key security measures such as encryption enforcement, authentication, and intrusion detection. Their protection capabilities extend from network firewalls at the perimeter to secure elements embedded directly within computer chips.[3]
- Physical security devices are **purpose-built** to defend systems from potential vulnerabilities. Examples include secure boot processes, Trusted Platform Modules (TPMs), and Hardware Security Modules (HSMs). These technologies help prevent tampering, hardware Trojans, and side-channel attacks. [4]
- Because they operate at the **physical layer**, hardware-based protections can defend against both known and emerging threats that exploit the same type of access. They also support secure data transfer and long-term data storage, providing a strong foundation for overall system integrity. [4]

2.2 Hardware Attacks [3]

- Threat actors increasingly focus on hardware supply chains as entry points for cyberattacks, often by inserting malicious components or altering firmware.
  - **Physical Tampering**: Attackers may physically access and open devices to install rogue chips, extract cryptographic keys, or manipulate internal components.
  - **Supply Chain Attacks**: These occur when hardware or firmware is compromised during production, assembly, or shipment, allowing malicious code or components to be embedded before the device even reaches its destination.
  - **Side-Channel Attacks**: This technique exploits indirect information, such as power consumption patterns or electromagnetic emissions, to extract sensitive data without directly accessing the system.

2.3 Standards, Protocols and Compliance for Hardware Security [3]

- Security Standards and Certifications
  - **IPS 140-2/3**: A U.S. government standard that defines the security requirements for cryptographic modules used to protect sensitive information.
  - **Common Criteria (ISO/IEC 15408)**: An internationally recognized framework for evaluating and certifying the security of IT products and systems.
  - **PCI DSS & ISO/IEC 27001**: These standards set the foundation for secure handling of payment data and the implementation of comprehensive information security management systems.
- Protocols and Guidelines
  - **TLS & IPsec**: Protocols that enable secure, encrypted communication over networks, protecting data in transit.
  - **IEEE 802.1X**: A standard for controlling access to networks at the port level, often used to authenticate devices before they connect.
  - **NIST SP 800-147 and SP 800-193**: Publications from the U.S. National Institute of Standards and Technology that provide best practices for protecting hardware throughout its lifecycle, from manufacturing to deployment and maintenance.

2.4 Cyber Tools – Hardware [5]

Firewalls	Fortinet FortiGate, pfSense, Ubiquiti UniFi Dream Machine Pro
VPN Hardware Appliances	Cisco Meraki MX, Netgate VPN appliances, Zyxel ZyWALL VPN Firewalls
Secure Routers	Asus AiProtection routers, Netgear Nighthawk Pro with Armor, TP-Link SafeStream series
Network Switches with Security Features	Cisco Catalyst Series, Juniper EX Series, Ubiquiti UniFi Switches
HSM	Thales Luna HSM, AWS CloudHSM
MFA Devices	YubiKey 5 Series, Google Titan Security Key, RSA SecurID tokens
IDS/IPS Hardware	Snort-based appliances, Suricata on pfSense boxes, Cisco Firepower appliances
Servers with Built-In Security	Dell PowerEdge servers, HPE ProLiant with iLO security features
AI-Powered Security Appliances	Darktrace, Palo Alto, Fortinet with AI features
Cybersecurity Kits	Bitdefender BOX, Norton Core, Gryphon Guardian routers
Unidirectional Gateways	Waterfall, SecuriCDS Data Diode, SDoT Diode

2.4.1 Firewalls (UTM Devices & Next-Gen Firewalls)

- A firewall acts as a digital security barrier, monitoring and filtering data that moves between an internal network and the internet. Modern solutions such as **Next-Generation Firewalls** (NGFWs) and **Unified Threat Management** (UTM) systems go far beyond simple traffic blocking, they analyze behavior patterns, detect intrusions, and stop malware from spreading within the network. [5]
- Traditional firewalls mainly inspect traffic based on ports, protocols, and IP addresses. In contrast, NGFWs can examine the actual **content of network traffic**, allowing them to identify and control specific applications. This deeper level of inspection enables stronger protection against advanced cyber threats operating at higher layers of the network stack.
- Unified Threat Management (UTM) **integrates several security tools** into a single device. These typically include firewalls, antivirus and anti-malware protection, web and email filtering, anti-spam measures, intrusion detection and prevention systems (IDS/IPS), virtual private network (VPN) capabilities, and data loss prevention features. By consolidating these defenses, UTM simplifies management while offering comprehensive protection. [6]
- Popular examples of firewall and UTM solutions include Fortinet FortiGate, pfSense, and Ubiquiti UniFi Dream Machine Pro.

2.4.2 VPN Hardware Appliances

- A Virtual Private Network (VPN) in general creates a secure, encrypted connection between a device and the internet. By routing traffic through a remote server, a VPN hides the user's real IP address and encrypts data, protecting online activity from hackers, ISPs, and other potential eavesdroppers. [7]
- A hardware VPN is a dedicated device that **encrypts internet traffic** for all users on a network without requiring VPN software on each individual device. Unlike software VPNs, which can slow down connections, hardware appliances handle encryption at the device level, offering both speed and enhanced security. [5]
- Hardware VPNs typically **include several components**: a VPN gateway or router, network interface cards (NICs), an encryption/decryption engine, a network switch, redundancy and high availability features, a management interface, authentication mechanisms, additional security functions, and sometimes a load balancer. [8]
- Examples of hardware VPN solutions include Cisco Meraki MX, Netgate VPN appliances, and Zyxel ZyWALL VPN Firewalls.

2.4.3 Secure Routers

- A router **connects two or more packet-switched networks** or subnetworks. It manages data traffic by directing packets to their correct IP addresses and allows multiple devices to share a single internet connection efficiently. [9]
- A secure router is a networking device equipped with **advanced security features**, such as automatic firmware updates, intrusion detection, and malware filtering. Because outdated routers are a common target for hackers, using a secure router helps protect your network from attacks at the very point where traffic enters your system. [5]
- Examples of routers with built-in security features include Asus AiProtection routers, Netgear Nighthawk Pro with Armor, and TP-Link SafeStream series.

2.4.4 Network Switches with Security Features

- A network switch **directs data packets** between devices within the same network, enabling efficient communication. [9]
- Advanced network switches provide features like VLAN support, port security, and anomaly detection, helping to **prevent lateral movement**. This means that if one device is compromised, attackers cannot easily spread to other devices on the network. [5]
- A **Virtual Local Area Network** (VLAN) allows a single physical network to be divided into multiple logical segments. This lets administrators group devices by role rather than location, improving security, simplifying management, and enhancing network performance by reducing unnecessary broadcast traffic. [10]
- Examples of advanced switches include Cisco Catalyst Series, Juniper EX Series, and Ubiquiti UniFi Switches.

2.4.5 Hardware Security Modules (HSMs)

- A Hardware Security Module (HSM) is a dedicated device designed to securely generate, store, and manage **encryption keys**. Unlike keys stored in software, which can be stolen or compromised, keys within an HSM are protected against extraction, making them extremely difficult for attackers to access. [5]
- Tamper-proof modules provide additional security by preventing unauthorized **physical modifications**. In critical systems, such as power grids, these modules ensure the integrity of devices that manage power flows or grid operations. Because many power systems are managed remotely, HSMs and tamper-proof devices help guarantee that commands are transmitted and received securely, protecting against interception or malicious tampering. [4]
- Examples of HSM solutions include Thales Luna HSM and AWS CloudHSM.

2.4.6 Multi-Factor Authentication Devices (MFA Tokens & Keys)

- A hardware security token is a physical device that provides an additional layer of authentication beyond a password. Even if a password is compromised, an attacker cannot access the account without the hardware token, making it a highly effective form of two-factor authentication. [5]
- Examples of hardware tokens include YubiKey 5 Series, Google Titan Security Key, and RSA SecurID tokens.

2.4.7 Intrusion Detection & Prevention Systems (IDS/IPS Hardware)

- A hardware intrusion detection and prevention system (IDPS) is a dedicated device that monitors network traffic for suspicious activity and can automatically block potential threats. These systems detect attacks in real-time, helping prevent significant damage before it occurs. [5]
- Examples of hardware IDPS solutions include Snort-based appliances, Suricata running on pfSense devices, and Cisco Firepower appliances.

2.4.8 Servers with Built-in Security (TPM Chips, Secure Boot)

- Trusted Platform Modules (TPMs), Secure Boot, and Intel SGX are hardware-based security technologies designed to protect system integrity and ensure that only trusted software is executed. They prevent tampering with firmware and enhance overall platform security. [5]
- A server is a computer that provides resources, data, or services to other computers, known as clients, over a network.
- A **Trusted Platform Module** (TPM) is a secure cryptoprocessor that follows the ISO/IEC 11889 standard. It is commonly used to verify that a system boots from trusted hardware and software and to securely store encryption keys. [11]
- **Secure Boot** is a feature in UEFI firmware that blocks unauthorized operating systems or malicious software from running during startup. It ensures that each component, from firmware to the OS bootloader, is signed with a trusted digital certificate. [12]
- **Intel Software Guard Extensions** (SGX) is a CPU technology that creates secure enclaves (isolated memory regions) to protect sensitive data while in use. SGX shields data from other software, the operating system, and even hypervisors, providing hardware-based protection that is central to confidential computing. [13]
- Examples of servers with these security features include Dell PowerEdge and HPE ProLiant systems with iLO security capabilities.

2.4.9 AI-Powered Security Appliances

- AI- and ML-powered cybersecurity devices leverage artificial intelligence and machine learning to detect abnormal network activity, ransomware, and insider threats. By analyzing patterns in real time, these systems help security teams **respond faster and stay ahead** of increasingly sophisticated attackers. [5]
- Examples of AI-enabled security solutions include Darktrace, Palo Alto Networks, and Fortinet devices with AI capabilities.

2.4.10 Cyber Security Kits for Home & Small Business

- All-in-one security devices combine multiple functions, such as firewalls, VPNs, and network monitoring, into a single unit. These solutions simplify cybersecurity for users who may not have advanced technical knowledge, offering comprehensive protection with minimal configuration. [5]
- Examples of all-in-one security devices include Bitdefender BOX, Norton Core, and Gryphon Guardian routers.

2.4.11 Unidirectional Gateways

- Data diodes are essential components in modern operational technology (OT) environments. They allow **data to flow in only one direction**, blocking any inbound traffic and preventing cyber threats from reaching critical systems, such as those in power grids or industrial control networks. [4]
- An **OT environment** refers to industrial settings where specialized hardware and software are used to monitor, manage, and control physical processes and infrastructure.
- Examples of data diode solutions include Waterfall, SecuriCDS Data Diode, and SDoT Diode.

3)

Software Cybersecurity

3.1 Importance of Software Cybersecurity [4]

- Software-based cybersecurity involves programs and data designed to protect systems, networks, and information. This includes solutions such as antivirus software, firewalls, intrusion detection systems, and encryption tools.
- These tools defend against malware, phishing attacks, and unauthorized software intrusions. They can be updated regularly to address emerging threats, though they may still be vulnerable to unknown or zero-day exploits.

3.2 Cyber Tools - Categories [14]

- Free Open-Source Software (FOSS)
  - These are programs that are both open-source and free to use. They allow users to access and modify the source code while requiring no payment.
- Open-Source Software
  - Open-source software gives users access to the program's source code, enabling collaboration, peer review, and customization. While many open-source programs are free, some may still require a purchase or subscription.
- Paid / Closed-Source Software
  - Closed-source software is owned and controlled by its developer. Users cannot view or modify the source code, and the software typically requires payment to use.

3.2.1 Cyber Tools – Open Source (1/2)

- Using open-source software offers several advantages:
  - Frequently available at no cost
  - High transparency, since users can inspect the source code
  - Flexibility, allowing developers to modify and customize the software
  - Potentially greater security, as a larger developer community can identify and fix vulnerabilities [14]

- *As a cryptography and computer security expert, I have never understood the current fuss about the open-source software movement. In the cryptography world, we consider open source necessary for good security; we have for decades.* ***Public security is always more secure than proprietary security****. It's true for cryptographic algorithms, security protocols, and security source code. For us, open source isn't just a business model; it's smart engineering practice. [15]*

  Bruce Schneier

3.2.1 Cyber Tools – Open Source (2/2) [14,16]

Penetration Testing & VA	Metasploit, Nmap, Nikto, John the Ripper, ZAP, OpenVAS
Network Protocol Analysis	Wireshark, httpry, NGREP, TCPFLOW, Arkime
Host-Based IDS/HIPS	OSSEC, Tripwire, Wazuh, Samhain, Security Onion
Network-Based IDS/NIPS	Snort, Suricata, Security Onion
Threat Detection Security	Abuse.ch, AlienVault OTX, InfraGard, DHS AIS, BlockList.de, MISP
Incident Response & Forensics	OSForensics, MISP, Security Onion
SIEM	ELK Stack, AlienVault OSSIM, SIEMonster
IAM	FreeIPA, OpenIAM, Keycloak
Endpoint Protection	ClamAV, OSSEC, Wazuh
Encryption & Cryptography	GnuPG, OpenSSL, VeraCrypt
Password Management	KeePass

3.2.1.1 Penetration Testing

- Penetration testing tools are used to identify vulnerabilities and simulate real-world attacks on systems and networks. Key tools include:
- **Metasploit**: Simplifies vulnerability scanning and automates exploit testing. Supports post-exploitation techniques, IDS evasion, patch testing, regression testing, auditing, and network port scanning. [14]
- **Nmap**: Maps networks and identifies open ports, host types, and operating systems. Can use scripts to detect security issues before or during audits. [16]
- **Nikto**: Scans web servers for vulnerabilities, such as outdated software, server misconfigurations, and version-specific security issues. [16]
- **John the Ripper**: Password-cracking tool using dictionary attacks, brute force, and rainbow tables. [14]
- **ZAP**: Web application security testing tool that detects SQL injection, XSS, and other vulnerabilities. Includes passive scanning, web crawling, brute force testing, directory search, and fuzzing capabilities. [14]

3.2.1.2 Vulnerability Management [17]

- Vulnerability management is the continuous process of identifying weaknesses in IT infrastructure, evaluating their risk, and recommending specific remediation steps. By addressing vulnerabilities proactively, organizations can reduce the likelihood of successful cyberattacks. The process involves detection, assessment, mitigation, and ongoing monitoring.
- **OpenVAS** is a comprehensive vulnerability scanner that supports both authenticated and unauthenticated testing. It covers a wide range of internet and industrial protocols, offers performance optimization for large-scale scans, and includes a powerful scripting language to implement custom vulnerability tests.

3.2.1.3 Network Protocol Analysis [16]

- Network traffic monitoring tools capture and analyze data as it moves across communication channels, helping identify issues and potential threats. Key tools include:
- **Wireshark**: Provides detailed visibility into network traffic, allowing packet inspection, format analysis, and troubleshooting.
- **httpry**: Logs network data to monitor user requests, evaluate server configurations, analyze usage patterns, and detect malicious files.
- **NGREP**: A text-based protocol analyzer that identifies connection anomalies, flags specific transactions, and supports platforms like Solaris IPnet.
- **TCPFLOW**: Records TCP connection packets for later analysis and debugging.
- **Arkime**: Stores and indexes network packet data in PCAP format for comprehensive traffic analysis.

3.2.1.4 Host-Based Intrusion Detection and Prevention Systems [16]

- Host-based intrusion detection systems (HIDS) monitor computers or networks for suspicious activity, logging events and alerting administrators. Key tools include:
- **OSSEC**: Performs log analysis, file integrity checking, policy monitoring, rootkit detection, and active responses using both signature-based and anomaly detection methods.
- **Tripwire**: Detects changes to system files and alerts administrators to corruption or tampering.
- **Wazuh**: Combines anomaly and signature detection to identify rootkits, monitor logs, check file integrity, and track Windows registry changes. It integrates with ELK and can monitor files in Docker containers.
- **Samhain**: Provides centralized, encrypted monitoring over TCP/IP, with stealth features to avoid detection. Supports logging for SQL databases, consoles, email, syslog, and Prelude IDS.
- **Security Onion**: Offers full packet capture and intrusion detection, correlating host-based and network-based events. Includes tools like Snort, Suricata, Bro, and Sguil.

3.2.1.5 Network-Based Intrusion Detection and Prevention Systems

- Network-based intrusion detection systems (NIDS) monitor network traffic to detect malicious activity in real time. Key tools include:
- **Snort**: Employs anomaly, protocol, and signature-based inspection to identify suspicious activity. Can log events, capture packets, and function as an IDS or IPS. [14]
- **Suricata**: Monitors network traffic by logging HTTP requests, storing TLS certificates, and extracting files from network flows for analysis. [18]
- **Security Onion**: Provides full packet capture and intrusion detection, correlating host-based and network-based events. Integrates tools such as Snort, Suricata, Bro, and Sguil for comprehensive monitoring. [16]

3.2.1.6 Threat Detection Security [16]

- Threat intelligence platforms and collaborative defense mechanisms provide sources for threat indicators, enable information sharing, and support organizational cybersecurity practices, including policy implementation, employee training, and tool integration. Key platforms include:
- **Abuse.ch**: Assists ISPs and network operators in protecting infrastructure from malware by sharing threat data.
- **AlienVault OTX**: Facilitates collaboration among private companies, security researchers, and government agencies to share information about emerging threats and malicious actors, strengthening community-wide security.
- **InfraGard**: Offers education, information sharing, networking opportunities, and workshops on emerging technologies and cyber threats.
- **DHS AIS**: Enables real-time exchange of machine-readable threat indicators and defensive measures, helping participants reduce the prevalence of cyberattacks.
- **BlockList.de**: Reports attacks to the appropriate abuse departments and helps notify customers about infected systems, ensuring faster mitigation.
- **MISP**: Provides a standardized format to collect and share indicators of compromise for improved threat intelligence and response. [14]

3.2.1.7 Incident Response and Forensics [14]

- Digital forensics and incident response tools help cybersecurity professionals investigate security breaches, reconstruct attacks, and gather evidence for post-incident analysis. Key tools include:
- **OSForensics**: Provides a comprehensive view of system activity by analyzing recently accessed websites, USB interactions, downloads, and login events. It can generate detailed reports and disk images for later examination.
- **MISP**: Standardizes the collection and sharing of indicators of compromise, supporting threat intelligence and forensic investigations.
- **Security Onion**: Offers full packet capture and integrates intrusion detection systems to correlate network and host-based events. Includes tools such as Snort, Bro, Sguil, and Suricata for thorough forensic analysis. [16]

3.2.1.8 Security Information and Event Management [14]

- Log aggregation and event analysis tools help organizations collect, correlate, and interpret data from multiple sources to identify security incidents and improve response times. Notable platforms include:
- **ELK Stack**: Combines Elasticsearch for indexing and searching security data, Logstash for server-side data processing, and Kibana for interactive visualization and dashboards. Supports snapshots of entire clusters or individual nodes for detailed analysis.
- **AlienVault OSSIM**: Provides automated asset discovery to identify network devices, generates events based on anomalous activity, performs vulnerability assessments, and can function as an IDS or HIDS.
- **SIEMonster**: Leverages machine learning, virtualization, and human behavior correlation to detect sophisticated threats across complex environments.

3.2.1.9 Identity and Access Management [14]

- Identity and access management (IAM) tools help organizations manage user authentication, authorization, and identity federation, ensuring secure and streamlined access to resources. Key solutions include:
- **FreeIPA**: Provides centralized authentication, authorization, and account management, with both GUI and command-line interfaces for administrative control.
- **OpenIAM**: A comprehensive IAM platform that supports single sign-on (SSO), multi-factor and adaptive authentication, social login, and self-service portals. It also automates identity-related business processes.
- **Keycloak**: Enables SSO and social network authentication, supports user federation with LDAP and Active Directory, offers intuitive admin and account management consoles, and provides role-based and fine-grained authorization capabilities.

3.2.1.10 Endpoint Protection

- Endpoint security focuses on protecting individual devices such as desktops, laptops, and servers from malware and unauthorized access. Key tools include:
- **ClamAV**: A free, cross-platform antivirus engine that detects viruses, trojans, and other malware. It primarily relies on signature-based detection and offers a command-line interface for scanning file systems and filtering emails. [14]
- **OSSEC**: Provides log analysis, file integrity monitoring, policy enforcement, rootkit detection, and active response capabilities, using both signature-based and anomaly detection methods. [16]
- **Wazuh**: Combines anomaly and signature detection to identify rootkits and other threats. It also performs log analysis, file integrity monitoring, and Windows registry checks. Wazuh integrates with ELK and can monitor containerized environments like Docker. [16]

3.2.1.11 Encryption and Cryptography

- Ensuring the confidentiality, integrity, and authenticity of data is critical for preventing unauthorized access and maintaining trust. Key tools include:
- **GnuPG**: Provides encryption and digital signing of data. It features a flexible key management system and supports integration with various public key directories. [14]
- **OpenSSL**: A command-line tool for generating private keys, creating certificate signing requests (CSRs), installing SSL/TLS certificates, and inspecting certificate details. [14]
- **VeraCrypt**: Allows the creation of virtual encrypted disks within files or the encryption of entire partitions or storage devices, including USB drives and hard disks. It also offers plausible deniability, protecting users if they are forced to reveal passwords. [19]

3.2.1.12 Password Manager [16]

- Encrypted digital vaults, known as password managers, securely store login credentials for apps, websites, and other services. Beyond protecting identities and sensitive information, top password managers include features such as strong password generation and prevention of password reuse across accounts.
- **KeePass**: Stores passwords in a secure database protected by a single master key. It uses robust encryption algorithms like AES-256, ChaCha20, and Twofish to encrypt all database contents, including usernames, notes, and password fields.

3.2.2 Cyber Tools – Paid

- Incident Response and Forensics:
  - **EnCase**: A comprehensive digital forensics tool that guides investigators through the entire process using built-in workflows and templates. It supports both data acquisition and analysis, allowing investigators to create bit-by-bit copies of hard drives and examine slack space to recover deleted files. The software automatically generates a clear timeline of key events, simplifying case review and reporting. [14]
- Password manager:
  - **NordPass**: Employs XChaCha20 encryption combined with Argon2 for secure key derivation. Includes an integrated password generator to help create strong, unique credentials. [16]
  - **Dashlane**: Uses AES 256-bit encryption to protect data. Supports two-factor authentication and can be linked to a single device for added security. [16]
  - **RoboForm**: Secures all passwords with AES-256 encryption. Passwords are stored on a protected server, and only the master password can unlock the vault. Two-factor authentication is available for extra protection. [16]
  - **LastPass**: Implements robust, industry-standard encryption, encrypting data locally before uploading it to servers. Supports multiple two-factor authentication methods, including authenticator apps and PIN verification. Features a customizable password generator, with options for length and character types, and allows passwords to be quickly saved to the vault. [16]

4)

Case Study

4. Use of Tools in a Company

- Case 1: Big company
  - Emphasis on protecting intellectual property, firmware, supply chain security.
  - Strong perimeter, segmentation, zero-trust, and defense in depth.
  - Use of HSM and secure code signing to protect device software integrity.
  - Full orchestration of logs, threat intel
  - Regular adversarial testing (pen tests, red-team) and forensics readiness
  - Governance, audit, and training to ensure sustainability
- Case 2: Startup
  - Focuses on free/open-source tools
  - Self-hosted SIEM, VPN, and IAM keep costs low
  - Covers major risks: access control, malware, phishing, endpoint compromise
  - Practical without sacrificing core security
  - Training

4.1 Use of Tools in a Company – Case 1

Foundational Security and Identity Control	IAM	Keycloak	Centralize authentication, single sign-on, role-based access control for all internal systems (R&D, manufacturing, admin)
	HSM	Thales Luna	Store cryptographic keys (firmware signing, code signing, certificate authorities) in hardware so they can’t be exfiltrated easily
Network and Infrastructure Protection	Firewall	Fortinet FortiGate	Deep packet inspection, intrusion prevention, application-level filtering for the perimeter and internal segments
	VPN	Cisco Meraki MX	Secure remote access for employees, partners and suppliers; especially for remote maintenance of security systems or firmware updates
	Endpoint Protection	OSSEC	Monitor and respond to threats on desktops, laptops, engineers’ workstations, and servers
	HIDS	OSSEC	Detect unauthorized changes to firmware, build artifacts, servers.
	IDS/IPS	Suricata	Real-time detection and blocking of suspicious traffic at the network layer
Monitoring	SIEM	SIEMonster	Centralize logs from endpoints, firewalls, devices, manufacturing systems to detect anomalies and trigger alerts
	Threat Detection	MISP	Feed the SIEM and firewall rules with indicators of compromise, threat signatures, firmware attack patterns
Pen testing and Incident Response	Pen Testing	Metasploit	Regular internal and external penetration tests to probe weak points in web portals, device management, firmware update servers
	Forensics	OSForensics	Investigate breaches, trace intrusion paths, recover forensic artifacts

4.2 Use of Tools in a Company – Case 2

Foundational Security	IAM	Keycloak	SSO and access control
	Password Manager	KeePass	Secure, shared credentials
	MFA	Google Titan Security Key	Hardware for extra login step beyond password
	Encryption	OpenSSL	CLI tool for securing files, emails
	VPN	WireGuard	Easy, affordable VPN setup
Detection and Endpoint Defense	Firewall	Ubiquiti UDM	Low-cost perimeter defense
	Endpoint Protection	Wazuh	Basic malware and host monitoring
	SIEM	ELK Stack	Log collection and alerting
	IDS/IPS	Suricata	Lightweight intrusion monitoring
Pen testing and Incident Response	Pen Testing	Metasploit	On-demand internal audits
	Forensics	OSForensics	Basic incident handling

5)

Cybersecurity Organizations

5. Cybersecurity related Organizations

- NIST = National Institute of Standards and Technology
- ISO = International Organization for Standardization
- ISACA = Information Systems Audit and Control Association
- ISC2 = International Information System Security Certification Consortium
- SANS = SysAdmin, Audit, Network and Security
- ENISA = European Union Agency for Cybersecurity
- FIRST = Forum of Incident Response and Security Teams
- Εθνική αρχή κυβερνοασφάλειας = National Cyber Security Authority

5.1 NIST/ISO/ISACA

- NIST = National Institute of Standards and Technology
  - NIST Cybersecurity Framework (CSF) is a voluntary set of guidelines that helps organizations manage and reduce cybersecurity risks by providing a structured approach to best practices in five core functions: Identify, Protect, Detect, Respond, and Recover. NIST also provides resources on various cybersecurity topics, including passwords, incident response, and cryptography. [20]
- ISO = International Organization for Standardization
  - ISO is known for setting global standards to help organizations safeguard information. The most recognized standard is ISO/IEC 27001, which defines the requirements for an Information Security Management System (ISMS), ensuring organizations can protect their information assets effectively. Another important standard, ISO/IEC 27002, offers guidance on implementing the security controls recommended within the ISMS framework. [21]
- ISACA = Information Systems Audit and Control Association
  - ISACA provides widely respected credentials that validate the skills of IT and information security professionals across areas such as audit, security, risk, privacy, governance, and emerging technologies. These certifications help professionals build credibility, demonstrate expertise, and advance their careers. [22]

5.2 ISC2/SANS/ENISA

- ISC2 = International Information System Security Certification Consortium
  - ISC2 is a non-profit organization dedicated to advancing the field of cybersecurity through professional training and certification. It is widely recognized as the world’s largest association for IT security professionals, providing globally respected credentials that validate expertise in various areas of information security. [23]
- SANS = SysAdmin, Audit, Network and Security
  - The SANS Institute is a leading global provider of cybersecurity education and certification. It offers a wide range of training programs, the GIAC (Global Information Assurance Certification) credentials, and even a Master’s degree through the SANS Technology Institute. The organization’s mission is to equip cybersecurity professionals with the practical skills and knowledge needed to defend against evolving cyber threats. [24]
- ENISA = European Union Agency for Cybersecurity
  - ENISA serves as the European Union’s center of expertise in cybersecurity. Its primary goal is to enhance cybersecurity resilience across Europe by developing policy guidance, supporting the protection of critical infrastructure, and strengthening cooperation among EU Member States, businesses, and citizens. The agency promotes trust in digital systems through initiatives such as awareness programs, knowledge sharing, and the development of EU-wide cybersecurity certification schemes. [25]

5.3 FIRST/ Εθνική αρχή κυβερνοασφάλειας

- FIRST = Forum of Incident Response and Security Teams
  - FIRST is a global, non-profit organization that unites Computer Security Incident Response Teams (CSIRTs) from government, academic, and commercial sectors. Its mission is to enhance global cybersecurity by encouraging collaboration in incident prevention, facilitating quick and coordinated responses to security incidents, and promoting information sharing among its members. [26]
- Εθνική αρχή κυβερνοασφάλειας = National Cyber Security Authority
  - The National Cybersecurity Authority is responsible for shaping and maintaining the country's overall cybersecurity posture. It drafts, develops, and updates the National Cybersecurity Strategy, which defines the strategic goals, priorities, and policies for safeguarding national digital infrastructure. It also prepares the National Incident Response Plan for managing large-scale cyber incidents and crises. As the designated supervisory and regulatory body, it oversees compliance, monitors the national cybersecurity landscape, and ensures the effective implementation of security measures. It also serves as the national Computer Security Incident Response Team and coordinates the activities of other CSIRTs operating within its jurisdiction. In addition, it organizes a national certification program to ensure professional competence in the cybersecurity field, and promotes education, awareness, and training to strengthen cyber resilience across public and private sectors. [27]

6)

Acronyms and Terminology

6.1 Acronyms

- VA = Vulnerability Assessment
- SIEM = Security Information and Event Management
- IDS = Intrusion Detection System
- IPS = Intrusion Prevention System
- TCP = Transmission Control Protocol
- IP = Internet Protocol
- PCAP = Packet Capture
- CISA = Cybersecurity and Infrastructure Security Agency
- ISP = Internet Service Providers
- SOC = Security Operations Center
- IAM = Identity and Access Management

6.2 Terminology

- Forensics
- Audit
- On-Premise Software
- Infrastructure as a Service
- Platform as a Service
- Software as a Service
- Router
- Modem
- Security Operations Centre

6.2.1 Forensics/Audit

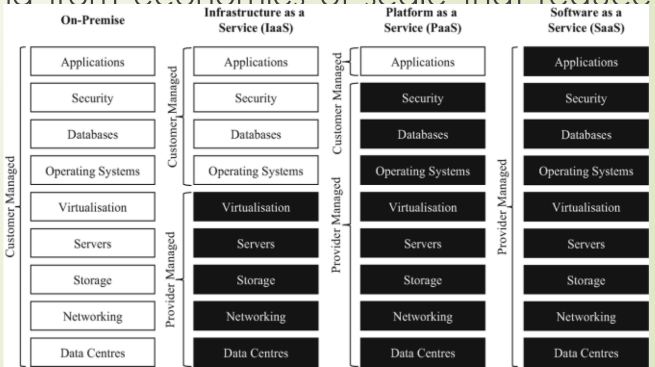
- Forensic cybersecurity involves uncovering, analyzing, and preserving digital evidence after a cyberattack. Its purpose is to help organizations limit damage, determine how an incident occurred, and prevent similar events in the future. Often referred to as digital forensics or computer forensics, it focuses on investigating cyberattacks and other unlawful activities in the digital space. The process includes identifying, collecting, preserving, and examining digital evidence to understand the nature and scope of an attack. It is essential that evidence is handled properly to maintain its integrity and ensure it remains admissible in court. [28]

- Beyond investigating past incidents, forensic cybersecurity also plays a proactive role in improving an organization's overall security resilience. It helps identify system vulnerabilities, assess potential attack vectors, and recommend measures to strengthen defenses. The ultimate goal is not only to respond effectively when incidents occur, but also to prevent them. Building an incident-ready culture (supported by clear policies, regular training, and strong forensic readiness) enables organizations to remain resilient and minimize the impact of future threats. [28]

- A cybersecurity audit is a thorough evaluation of an organization's security infrastructure, policies, and procedures. It aims to identify weaknesses, vulnerabilities, and potential risks across both technical systems (such as networks and firewalls) and human factors (like employee security practices). The audit measures how well an organization aligns with industry standards and regulatory requirements. Its findings provide actionable recommendations to strengthen overall security posture, enhance risk management, and ensure ongoing compliance. [29]

6.2.2 On-Premise/IaaS/PaaS/SaaS [30]

- On-premises software is installed and operated directly within an organization's internal IT infrastructure. This means that both the software and the necessary hardware are maintained and managed locally by the organization's own technical team. This setup gives full control over security, data management, and system configurations, but also requires greater investment in equipment, maintenance, and expertise.
- Infrastructure as a Service (IaaS) is the foundational layer of cloud computing. In an IaaS model, organizations rent computing resources such as servers, storage, and networking from a cloud provider instead of owning physical hardware. This allows infrastructure capacity to be scaled up or down quickly without waiting for new hardware to be purchased and configured. However, users are still responsible for managing the operating systems, middleware, and applications that run on the infrastructure.
- Platform as a Service (PaaS) builds on top of IaaS by including operating systems, middleware, and development tools, but not the end-user applications themselves. It provides a ready-to-use environment for developers to build, test, and deploy applications without managing the underlying infrastructure.
- Software as a Service (SaaS) represents the final layer of cloud computing and is the one most familiar to end users. SaaS applications are hosted and maintained by the provider and accessed online (typically through a web browser or mobile app) on a subscription basis. Users don't need to install or update the software themselves, as maintenance and scalability are handled by the provider. Examples include email platforms, customer relationship management (CRM) systems, and streaming services. SaaS solutions are often built upon PaaS or IaaS frameworks for scalability and performance.
- Cloud-based software is delivered over the internet and can be accessed anytime, from anywhere. Users typically only need a web browser or an app to use its services. In contrast, on-premises solutions require local installation and maintenance, offering more control but less flexibility. Cloud-based options provide greater accessibility, automatic updates, and scalability while benefiting from economies of scale that reduce costs.



6.2.3 Router/modem [9]

- A router is responsible for creating networks and managing the flow of data between the devices within those networks, while a modem connects the network to the wider Internet. The modem establishes this connection by converting the signals from an Internet Service Provider (ISP) into digital data that can be understood by connected devices. A single device can connect directly to the Internet through a modem. However, by pairing a router with a modem, the Internet connection can be shared among multiple devices within a local network, allowing them all to go online simultaneously. The router typically connects to the modem using an Ethernet cable.
- To illustrate:

  Bob has a router but no modem. He can create a Local Area Network (LAN) and share files between devices, but he can't access the Internet.

  Alice has a modem but no router. She can connect one device (e.g. her laptop) to the Internet, but she can't share that connection with other devices.

  Carol has both a router and a modem. She can form a LAN connecting her computer, tablet, and smartphone, and all of them can access the Internet at once.
- Together, the router and modem form the essential foundation for both local networking and Internet connectivity.

6.2.4 Security Operations Centre [31]

- A Security Operations Centre (SOC) is a centralized unit responsible for managing and responding to security threats across an organization. Its core functions include monitoring, detecting, analyzing, and responding to cybersecurity incidents using advanced technology, well-defined processes, and skilled personnel. Operating around the clock, a SOC provides continuous surveillance and rapid incident response to minimize the impact of potential cyberattacks.
- Beyond reactive defense, a SOC also plays a proactive role in threat management. It uses sophisticated monitoring tools and threat intelligence to identify and prevent risks before they can cause damage. By consolidating all security operations in one place, a SOC offers unified visibility, better coordination, and stronger control over the organization's entire security environment.
- A well-functioning SOC provides access to experienced cybersecurity professionals who receive ongoing training to stay ahead of evolving threats. This expertise is crucial for effective incident response and swift recovery, whether managed internally or outsourced to a trusted provider.
- In addition, a SOC supports compliance and regulatory requirements, helping organizations align with industry standards and streamline audit and reporting processes. While establishing or managing a SOC requires investment, it is often cost-effective in the long term, as it prevents costly breaches and optimizes the use of security resources.

7)

References and Licenses

7. References (1/4)

[1] Jonker, A., Lindemulder, G., & Kosinski, M. *What Is Cybersecurity?* IBM. Retrieved November 7, 2025, from https://www.ibm.com/think/topics/cybersecurity © IBM Corporation. All rights reserved.

[2] Shea, S. (2024, August 28). *Types of hackers: Black hat, white hat, red hat and more.* TechTarget. https://www.techtarget.com/searchsecurity/answer/What-is-red-and-white-hat-hacking © Informa TechTarget. All rights reserved.

[3] OPSWAT. (2025, July 3). *Cybersecurity Hardware: Protecting Physical Devices and Systems.* OPSWAT. https://www.opswat.com/blog/cybersecurity-hardware © 2025 OPSWAT Inc. All rights reserved.

[4] BlackBear. *An In-depth Look at Hardware-based Cybersecurity*. BlackBear. Retrieved November 7, 2025, from https://blackbear-ics.com/cybersecurity-hardware/ © 2021-2023 BlackBear (Taiwan) Industrial Networking Security Ltd. All rights reserved.

[5] TechnologyHQ. (2025, September 19). *Best Hardware for Cyber Security in 2025: Top Devices to Keep Hackers Out.* TechnologyHQ. https://www.technologyhq.org/best-hardware-for-cyber-security-in-2025/ © TechnologyHQ. All rights reserved.

[6] Fortinet. *What Is Unified Threat Management (UTM)?* Fortinet. Retrieved November 7, 2025, from https://www.fortinet.com/resources/cyberglossary/unified-threat-management © 2025 Fortinet, Inc. All rights reserved.

[7] Fortinet. *What Is a VPN? Virtual Private Networks Explained.* Fortinet. Retrieved November 7, 2025, fromhttps://www.fortinet.com/resources/cyberglossary/what-is-a-vpn © 2025 Fortinet, Inc. All rights reserved.

7. References (2/4)

[8] Nakutavičiūtė, J. (2023, June 21). *VPN hardware vs. VPN software*. NordVPN. https://nordvpn.com/blog/vpn-hardware/?srsltid=AfmBOoryFyMwdJfxw8l96GRVJSwzlVmfdnu7c84cM_r-JYliXtnOXDa0 © 2025 Nord Security. All rights reserved.

[9] Cloudflare. *What is a router?* Cloudflare. Retrieved November 7, 2025, from https://www.cloudflare.com/learning/network-layer/what-is-a-router/ © 2025 Cloudflare, Inc. All rights reserved.

[10] Omnitron. *What is a VLAN (Virtual LAN), and how does it work?* Omnitron. Retrieved November 7, 2025, from https://www.omnitron-systems.com/blog/what-is-a-vlan-virtual-lan-and-how-does-it-work © 2025 Omnitron Systems Technology, Inc. All rights reserved.

[11] Wikipedia. *Trusted Platform Modules*. Wikipedia. Retrieved November 7, 2025, from https://en.wikipedia.org/wiki/Trusted_Platform_Module Licensed under CC BY-SA 4.0.

[12] Microsoft Learn. (2023, August 2). *Secure boot*. Microsoft Learn. https://learn.microsoft.com/en-us/windows-hardware/design/device-experiences/oem-secure-boot © Microsoft 2025. All rights reserved.

[13] Intel. *Reduce the Attack Surface Around Your Data to Unlock New Opportunities*. Intel. Retrieved November 7, 2025, from https://www.intel.com/content/www/us/en/products/docs/accelerator-engines/software-guard-extensions.html © Intel Corporation. All rights reserved.

[14] Abel, S. (2025, May 29). *20 Essential Open Source Cyber Security Tools for 2025*. STATIONX. https://www.stationx.net/open-source-cyber-security-tools/ © 2025 STATIONX LTD. All rights reserved.

7. References (3/4)

[15] Schneier, B. (1999, September 15). *Open Source and Security*. Schneier. https://www.schneier.com/crypto-gram/archives/1999/0915.html#OpenSourceandSecurity © 1999 Bruce Schneier

[16] Tudor, D. (2025, October 5). *25 Free & Open Source Cybersecurity Tools for Businesses*. Heimdal. https://heimdalsecurity.com/blog/25-free-open-source-cybersecurity-tools-for-businesses/ © 2025 Heimdal. All rights reserved.

[17] OPENVAS. *OPENVAS by Greenbone*. OPENVAS. Retrieved November 7, 2025, from https://www.openvas.org/ © 2020-2025 Greenbone AG

[18] Suricata. *Features*. Suricata. Retrieved November 7, 2025, from https://suricata.io/features/ © 2025 OISF

[19] VeraCrypt. *What does VeraCrypt bring to you?* VeraCrypt. Retrieved November 7, 2025, from https://veracrypt.jp/en/Home.html

[20] National Institute of Standards and Technology (NIST). *Cybersecurity Framework*. NIST. Retrieved November 7, 2025, from https://www.nist.gov/cyberframework

[21] International Organization for Standardization (ISO). *ISO/IEC 27001:2022*. ISO. Retrieved November 7, 2025, from https://www.iso.org/standard/27001 © ISO. All rights reserved.

[22] ISACA. Retrieved November 7, 2025, from https://www.isaca.org/ ©2025 ISACA. All rights reserved.

[23] Wikipedia. *ISC2*. Wikipedia. Retrieved November 7, 2025, from https://en.wikipedia.org/wiki/ISC2 Licensed under CC BY-SA 4.0.

7. References (4/4)

[24] SANS. *World-Class, Expert-Led Cybersecurity Training*. SANS. Retrieved November 7, 2025, from https://www.sans.org/emea © 2025 The Escal Institute of Advanced Technologies, Inc.

[25] ENISA. *What we do*. ENISA. Retrieved November 7, 2025, from https://www.enisa.europa.eu/about-enisa/what-we-do © 2025 European Union Agency for Cybersecurity

[26] FIRST. *FIRST is the global Forum of Incident Response and Security Teams*. FIRST. Retrieved November 7, 2025, from https://www.first.org/ © 2015-2025 by Forum of Incident Response and Security Teams, Inc. All rights reserved.

[27] National Cybersecurity Authority. *Η ΕΘΝΙΚΗ ΑΡΧΗ ΚΥΒΕΡΝΟΑΣΦΑΛΕΙΑΣ*. Cyber Gov. Retrieved November 7, 2025, from https://cyber.gov.gr/ © 2025 Εθνική Αρχή Κυβερνοασφάλειας

[28] SentinelOne. (2025, August 17). *Cybersecurity Forensics: Types and Best Practices*. SentinelOne. https://www.sentinelone.com/cybersecurity-101/cybersecurity/cybersecurity-forensics/ © 2025 SentinelOne. All rights reserved.

[29] Vicente, V. (2023, April 19). *Security Audits: A Comprehensive Overview*. AuditBoard. https://auditboard.com/blog/what-is-security-audit ©2025 AuditBoard. All rights reserved.

[30] Wikipedia. *Cloud computing*. Wikipedia. Retrieved November 7, 2025, from https://en.wikipedia.org/wiki/Cloud_computing Licensed under CC BY-SA 4.0.

[31] Obrela. (2024, March 12). *What is a SOC in cyber security? Definition & Meaning*. Obrela. https://www.obrela.com/blog/what-is-a-soc-in-cyber-security-definition-meaning/ © 2025 Obrela

Licences

Take-home message

No matter how informative or well-structured a presentation may be, it can’t replace personal initiative and independent research. Take charge of your learning: look up a new word you heard today, ask someone about it, or follow a trusted source for insightful content. Small, consistent steps lead to deeper learning and lasting self-growth.

Take this quiz to test your understanding:

It's quiz time!