"Funded by the European Union. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union. Neither the European Union nor the granting authority can be held responsible for them."

Co-funded by the European Union

Internet and Computer Security

dr Bojana Milosavljević

AASKM

Co-funded by the European Union

Internet, basic terms - evolution

- The history of the Internet began in 1961 with the theory of packet switching (packed switching), MIT (Massachusetts Institute of Technology)
- In 1965, two computers were connected for the first time, Massachusetts/California, using a slow telephone line.
- Work on the creation of the ARPANET network (Advanced Research Projects Agency Network) began in 1966. DARPA (Defense Advanced Research Projects Administration)
- The first node - a computer at the University of California Los Angeles (UCLA), the second node - a computer at the Stratford Research Institute (Stanford Research Institute/SRI).

Co-funded by the European Union

Internet, basic terms - evolution

- The original ARPANET eventually grew into the Internet.
- The Internet is based on the new idea of multiple independent networks, each arbitrarily designed, while the ARPANET envisioned a single network.
- A key idea on which the Internet is based is an open networking architecture,
- In Europe, the construction of the EARN network (European Academic and Research Network) began in 1984, which followed the concept of connecting networks.
- Yugoslavia joined the EARN network practically in 1989. The first computer connected to the network was the computer of the Republic Institute of Statistics.

Co-funded by the European Union

Internet, basic terms

- Computer network - a set of multiple computers, peripheral units and other devices that are interconnected with the aim of sharing information and sharing network resources.
- Communication between nodes in the network is based on a protocol.
- There are several classifications of networks:
- by range: LAN (Local Area Network), WAN (Wide Area Network), MAN (Metropole Area Network), CAN, PAN,
- according to the relationship between nodes: peer-to-peer and server network; I
- classification according to topology: bus, ring and star.

Internet, basic terms

- Protocols
- A protocol refers to a set of rules that determine how two programs can communicate. Computers communicate by exchanging a specific set of messages, and a protocol determines the formats of those messages.
- TCP/IP (Transmission Control Protocol/Internet Protocol) protocol, which enables communication between two or more computers.
- Protocols for each of the Internet services, for example:
- HTTP (Hyper-Text Transfer Protocol) for the World Wide Web,
- FTP (File Transfer Protocol) is a service for distributing files on the Internet,
- SMTP (Small Mail Transfer Protocol) for the transmission of e-mail messages,
- NNT (Network News Transfer Protocol) for the transmission of news messages, i
- Telnet - for working on remote servers / computers

Co-funded by the European Union

Internet, basic terms

- Ports
- Each internet protocol (www, ftp, smtp...) has its corresponding port (number).
- Internet addresses
- In order for computers to recognize each other, each individual computer must have its own unique address. Using the Internet successfully involves understanding several different types of addresses.
- IP addresses are simple numerical addresses of computers connected to the Internet.
- Symbolic addresses - domains. In order to make it easier to remember addresses, servers are assigned symbolic www type addresses. kpa.edu.. The division is done as follows : service name + server name + domain name + root domain name,
- URL (Uniform Resource Locator) is the web address of a specific resource on the Internet. A resource pointed to by a URL can be an HTML document (web page), an image, or any file located on a particular web server.

Co-funded by
the European Union

Internet, basic terms

Internet

Co-funded by the European Union

Basics of Internet and computer security

- The Internet and computer technology can be abused in various ways, and the abuse itself, which is realized using computers, can take the form of any of the traditional types of criminality.
- Emergent forms of computer crime are: illegal use of services and unauthorized obtaining of information, computer theft, fraud, sabotage, and computer terrorism and crime related to computer networks.

Co-funded by the European Union

Basics of Internet and computer security

- Crime related to computer networks is a form of criminal behavior in which cyberspace - the environment in which computer networks are located - appears in a triple role:
- Computer networks as a target of attacks - services, functions and contents located on the network are attacked. Services and data are stolen, parts or the entire network and computer systems are damaged or destroyed, or their functions are disrupted.
- Computer networks as a means or a tool - Today, modern criminals are increasingly using computer networks as a tool to realize their intentions.
- Computer networks as an environment in which attacks are carried out, most often computer networks are used to conceal criminal acts. There are other roles, such as e.g. using the net as a symbol of intimidation.

Basics of Internet and computer security

- *Tenth UN Congress (April 2000), document Crime related to computer networks, Convention on Cybercrime:*
- *"This crime means "crime that refers to any form of crime that can be committed with computer systems and networks, in computer systems and networks, or against computer systems and networks." It is, in essence, a crime that takes place in an electronic environment. If a computer system means "any device or group of interconnected devices that perform automatic data processing (or any other functions)" as defined.*

Co-funded by the European Union

Basics of Internet and computer security

- Cyberspace is the term for non-physical space created by computer systems. Cyber space is an artificial creation that requires high technical equipment, a good information infrastructure and which is nobody's and everyone's property, in which virtual and real co-exist in parallel and where communication is collective. In such an environment, it is extremely difficult to talk about the national scale of crime and social danger, at least not in the conventional sense of the word.

Co-funded by the European Union

Basics of Internet and computer security

- Depending on the type of committed acts, cybercrime can be:
- political: cyber espionage; hacking; cyber sabotage; cyber terrorism; cyber warfare.
- economic: cyber fraud; hacking; theft of Internet services and time; piracy of software, microchips and databases; cyber industrial espionage; fake Internet auctions
- production and distribution of illegal and harmful content: religious sects; spread of racist, Nazi and similar ideas and attitudes; abuse of women and children; manipulation of prohibited products, goods and substances, drugs, human organs and weapons.
- violations of cyber privacy: e-mail monitoring, spam, phishing, eavesdropping, recording of "chat rooms", monitoring of e-conferences, cookies...

Co-funded by the European Union

Basics of Internet and computer security

- **Computer security (cybersecurity)** refers to the protection of computer systems, networks and data from unauthorized access, attack, damage, or theft.
- Goal: preservation of confidentiality, integrity and availability of data and resources in information systems.
- The three principles of the CIA triad represent the basis of all information systems protection strategies and the basic guidelines in the development of security policies and systems.

Co-funded by the European Union

Basics of Internet and computer security

- CIA Triad:

- **Confidentiality** refers to ensuring that information is available only to those who have appropriate authorized access. This includes protecting data from unauthorized access, leakage or disclosure. Procedures that enable confidentiality are e.g. data encryption and access control

- **Integrity** refers to preserving the accuracy and consistency of data. This means that the data must not be changed or damaged without proper authorization. Verification of data integrity can be achieved using techniques such as hashing or digital signatures, which ensure that data has not been tampered with.

- **Availability** means the system's ability to be available to users and resources when they need them. This implies that infrastructure, networks and data must always be available and operational. One of the threats are DDoS attacks (Distributed Denial of Service) which aim to disable access to data.

Co-funded by the European Union

Basics of Internet and computer security

CIA Triad

Cyber threats and vulnerabilities

- Cyber threats and vulnerabilities are two key issues in the field of computer security, they refer to the various ways in which computer networks and systems can be compromised.

- **Cyber threats** represent potential dangers that can negatively affect computer systems and networks. These are attempts or actions that involve unauthorized access, manipulation, destruction of data or disruption of system operation.

- Examples of cyber threats: **hacking, malware** (malicious software), **phishing** attacks (fraud through fake e-mails or websites) or **ransomware** (data hijacking), as well as so-called unintentional errors (human error, configuration error)

- **Cyber vulnerabilities are weaknesses** in computer networks or systems that allow attackers to perform malicious activities.

- Examples of vulnerabilities: programming errors in the code, poor password protection, insecure communication protocols or inadequate protection against malware.

Cyber threats and vulnerabilities

- **Malware** is any type of software code designed to harm computers, networks, or users with various goals.
- Examples of malicious software: viruses and trojans, ransomware, spyware...
- **A virus** is software that attaches itself to files or programs and spreads by copying itself to other files, causing the computer to become "infected". Viruses usually have the ability to destroy data and system files.
- **A Trojan Horse** is a malicious program that masquerades as useful or harmless software, but actually allows an attacker to access and control your computer. Unlike viruses, Trojans do not replicate.
- **Ransomware**, this software hijacks data on a computer or device by encrypting it and demands a ransom from the victim in exchange for decrypting the data. Ransomware can have serious consequences as it can completely destroy a user's data.

Cyber threats and vulnerabilities

- **Spyware** is software that collects information about users without their knowledge. This may include passwords, bank details or other personal information. Spyware usually tracks a user's activities on the Internet.

- **Adware** - This software automatically displays or downloads advertisements on your computer. Although it is not necessarily destructive like some other malware, it can be very annoying and slow down your computer.

- **A rootkit** is software designed to hide the presence of other malicious programs on a computer. A rootkit gives an attacker "root" or administrative access to a computer, allowing control over it without detection.

- **Worms** are self-contained malicious programs that replicate and spread over networks, most often via e-mail or software vulnerabilities. They can cause network and computer problems.

Co-funded by
the European Union

Cryptography and data protection

- **Cryptography** is a science that in practice ensures the protection of information using mathematical algorithms, the aim of which is to ensure privacy, integrity and authentication of data.

- We conclude that data security and cryptography are closely related, it can even be said that information protection could not be realized without cryptography.

- The four basic functions of Cryptography are:
- confidentiality,
- data integrity (data integrity),
- authentication i
- non-repudiation.

Co-funded by the European Union

Cryptography and data protection

- **Confidentiality**, ensuring that the content of the information is not available to anyone other than the person for whom the information is intended. This is the oldest purpose of cryptography. Sometimes the terms privacy or secrecy are used for this purpose.

- **Data integrity** is ensuring the immutability of data, i.e. detection of any data change. Data changes mean actions such as addition, removal or replacement.

- **Identity verification** is related to the exchange of information. Its purpose is the identification of subjects when exchanging information and the information itself. Elements of information authenticity are its origin, time of creation and time of sending. Sometimes authentication is divided into two classes: entity identity authentication and data origin authentication.

- **Non-repudiation** makes it impossible for any participant to deny previously committed acts. From the aspect of information exchange, this means that neither party in that exchange can deny their participation in the exchange and the content of the exchanged information.

Cryptography and data protection

- **Symmetric cryptography**, the same key is used to **encrypt and decrypt** data. This key must be known and confidential between the sender and receiver of the data. This is why symmetric cryptography is also called "**shared key encryption**".
- Symmetric cryptography requires fewer computer resources, which makes it faster and more efficient, especially when large amounts of data need to be encrypted. The drawback is primarily the challenge of how to securely transfer the secret key between sender and receiver.
- Algorithms of symmetric cryptography:
- **AES (Advanced Encryption Standard):** one of the most popular and most secure symmetric algorithms. It uses keys of different lengths (128, 192, 256 bits). It is used in industry, banking, etc.
- **DES (Data Encryption Standard):** an older algorithm now considered insecure due to its relatively short key (56 bits).
- **3DES (Triple DES):** Increases the security of DES by encrypting data three times, using three different keys.
- **RC4 (Rivest Cipher 4**): Stream cipher used to encrypt data in streams, such as the HTTPS protocol.

Cryptography and data protection

- **Asymmetric cryptography (public key cryptography)** is a type of cryptography in which two different keys are used: one for encryption **(public key)** and one for decryption **(private key).** This principle enables secure communication, as it does not require the two parties to share secret keys in advance.

- Public key, freely shared for data encryption and digital signature verification.
- Private key, secret and used only when decrypting data.

- The recipient can use his private key to digitally sign the message, while the sender can use the public key to verify the authenticity of the signed message.

Co-funded by the European Union

Cryptography and data protection

- Asymmetric cryptography algorithms:

- **RSA** (Rivest-Shamir-Adleman): used for data encryption and digital signatures. RSA is based on the mathematical problem of factoring large numbers, typically using keys of 2048 bits or longer. RSA is widely used in protocols such as HTTPS and PGP.

- **ECC** (Elliptic Curve Cryptography): uses elliptic curves to generate keys and enables a higher level of security with shorter keys, used in mobile devices and in new security protocols.

- **DSA** (Digital Signature Algorithm): used for digital signatures, although today it is mostly used in combination with SHA (Secure Hash Algorithm) to create secure signatures. DSA is part of the wider Digital Signature Standard (DSS) system.

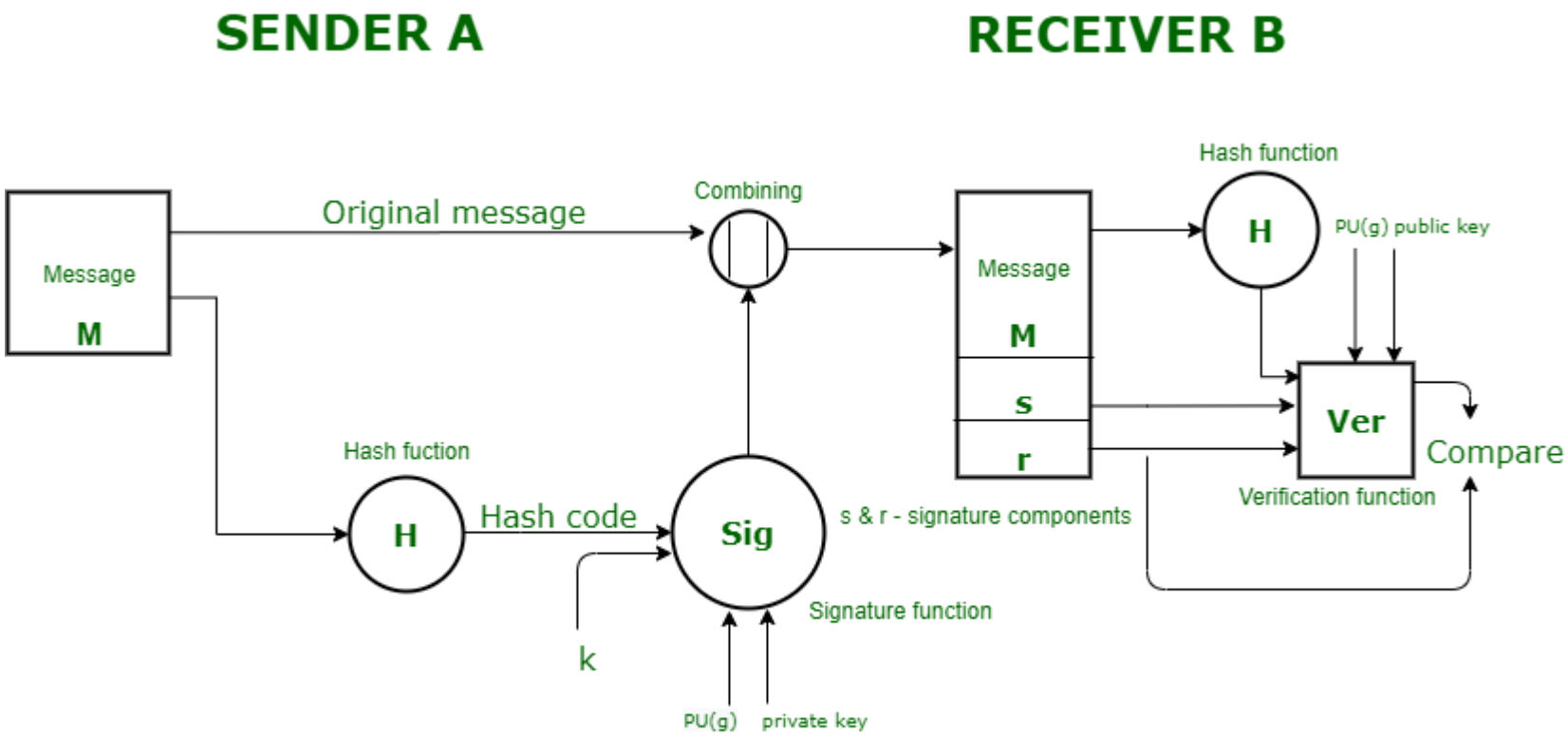
Cryptography and data protection

- Digital signature (Digital Signature Standard-DSS)
- **A digital signature** is mathematically based on asymmetric cryptography and allows users to confirm the authenticity of messages or documents. It is used as a software signature (it guarantees that the software has not been modified) and in e-mail communication.

- The sender uses their private key to sign the data (message, document, file, etc.), using a hash function (which generates a unique identifier for the data), and then that hash is signed with the private key.

- The recipient calculates the hash value of the received message, then uses the public key to decrypt the signature and obtain the original hash value. If the hash values match, it means that the data has not been modified and is signed by the sender.

Cryptography and data protection



DSS

Cryptography and data protection

- **A digital certificate** is an electronic document that serves to verify the sender's identity and enables the use of a public key in cryptographic operations.

- The certificate contains information about the owner, as well as his public key, and everything is signed by a trusted third party, called a certification authority (CA - Certification Authority). (CA) issues a certificate to the owner of the public key after verifying the user's identity.

- **Content of the certificate**:
- The user's public key
- User data: name, organization, e-mail address.
- Certification information: information about the certification authority, date of issuance and expiration of the certificate.
- CA Digital Signature: The certificate is signed by a CA to guarantee that the information in it is verified and correct.

Co-funded by
the European Union

Authentication and Authorization

- **Authentication and authorization** are components in the field of security of computer systems and networks. Although they are often used together, they represent different stages in the process of securing access to resources.

- **Authentication** refers to the process of confirming the identity of a user or system.
- Authentication mechanisms: user passwords, biometrics and two-factor authentication

- **Authorization** refers to the process of deciding what a user or system can do, i.e. what are its possibilities for content manipulation.

Authentication and Authorization

- A user's password is a secret string of characters that allows users to access files, programs or computers. At the same time, it prevents access by unauthorized persons, i.e. the password is used to authenticate and prove the identity of users who want to access certain data or network resources.
- Advantage - simple implementation
- Disadvantage - they can be weak or detected by phishing attacks, repeating passwords increases the risk

- Use of single-use passwords This method reduces the possibility of unauthorized access (usernames, passwords, credit card numbers, etc.), information and/or files. The same password can be used once, and a new password must be created for each subsequent login. An example of use are one-time passwords received via SMS, which are used to access certain web services.

- This method for user identification is mainly used in Internet banking. It is very similar to one-time passwords, except that users are given special devices that they use to prove their identity.

Co-funded by
the European Union

Authentication and Authorization

- Biometric methods
- Biometrics is an identity verification technique that uses the unique physiological characteristics of each person (fingerprint, corneal scan, DNA, etc.).
-
- Biometric data is collected using sensors and sent for analysis, and with it, a biometric sample is created, which is compared with the previously obtained sample.

- It is a method that is more secure than passwords because it is based on the specifics of each individual.
- Disadvantages: the price (which depends on the type of biometric verification) and the fact that user data cannot be transmitted if it is compromised.

Co-funded by
the European Union

Authentication and Authorization

- Two-factor authentication (2FA)

- The term two-factor authentication (T-FA or 2FA) is a term used to describe a mechanism for identification using two parameters.
-
- Two basic factors that are taken into account are:
- - something known to the user, it can be e.g. PIN number i
- - something that the user owns, e.g. mobile device with a code or token

- Examples of such devices are a token and/or a smart card.
- Advantages: Increases security compared to a simple password, as attackers must possess both factors.

Authentication and Authorization

- **Authentication protocols** enable the secure exchange of identity data between clients and servers.
- **Kerberos** is a protocol based on the principle of symmetric cryptography that enables authentication between clients and servers in distributed networks. Kerberos uses a Ticket Granting Ticket (TGT) to grant access to network resources.
- **OAuth (Open Authorization**) an authorization protocol that allows users to share certain resources with third parties, without having to share their user passwords. In OAuth, a user grants an application access to their resource via a "token".
- **OAuth 2.0** is a version that is very popular for authentication on websites and mobile applications.

Co-funded by
the European Union

Web Application Security

- Because of their availability over the Internet, Web applications are often the target of attacks.

- Considering the increasing use of web applications in business and everyday life, their security is becoming an essential part of Internet and computer security.

- Web applications are often exposed to various types of attacks. Some of the most common and dangerous attacks are:
- SQL Injection (SQLi)
- XSS (Cross-Site Scripting)
- CSRF (Cross-Site Request Forgery)

Co-funded by the European Union

Web Application Security

- SQL Injection (SQLi)
- In standard software practice, an SQL query is a request sent to a database for some type of activity or function such as querying data or executing SQL code.

- Typically, this type of web form is designed to only accept very specific types of data such as name and/or password. When that information is entered, it is checked against the database, and if it matches, the user is allowed to enter it.

- Hackers can exploit this weakness and use input boxes on a form to send their own requests to the database. Due to the prevalence of websites and servers that use databases, the SQL injection attack method is one of the oldest and most widespread types of attacks.

- Protection: parameterized queries: (separate data from SQL code, to prevent malicious code injection), Use of ORM (Object-Relational Mapping) tools…

Co-funded by
the European Union

Web Application Security

- XSS (Cross-Site Scripting) is an attack in which the attacker enters malicious JavaScript code into the user's web page, i.e. the attacker inserts the JavaScript code into the form or URL parameter, which allows him, that when the user opens the page, their browser executes the attack.

- CSRF (Cross-Site Request Forgery) An attacker can send a link that, when the user clicks on it, automatically performs an unauthorized action in the application, such as changing passwords or performing money transfers.

Co-funded by the European Union

Web Application Security

- General principles of protection:
- **Principle of Least Privilege**: Users and processes should have the minimum privileges they need to perform their tasks.
- **Regular code testing**: Using static code analysis tools to detect vulnerabilities.
- **Update**: Regular update of libraries, frameworks and all software components to the latest security versions
- **Data encryption**: Using strong encryption algorithms to protect data during transmission (eg SSL/TLS)
- **Secure password storage**: Passwords should be stored in an encrypted format using a secure technique such as bcrypt or Argon2

Co-funded by the European Union

Security incidents

- Consequences of the incident:
- System compromise, taking control of servers and devices
- Interruption of services: DDoS attacks cause denial of services, resulting in financial losses
- Damage to reputation: Attacks damage user trust and business reputation

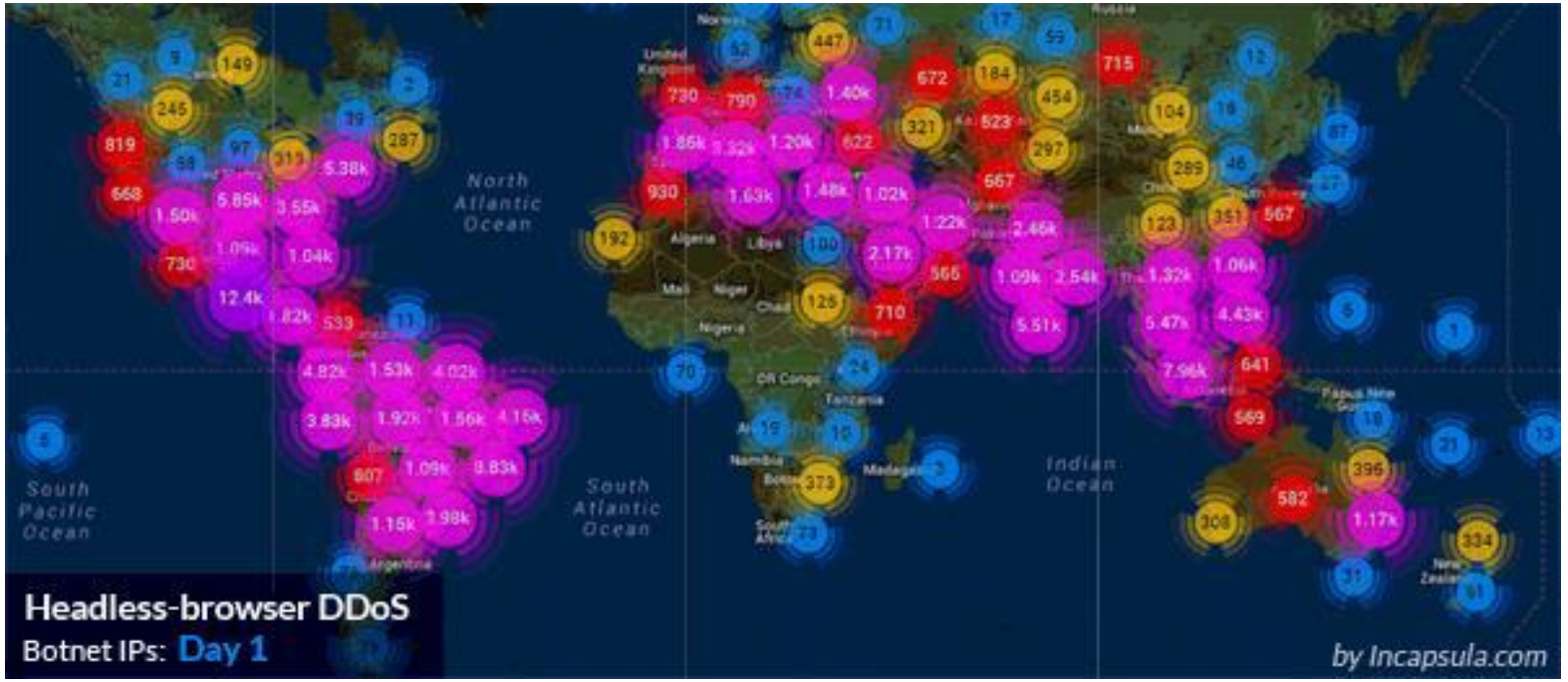
- Response to security incidents:
- Detecting incidents as soon as possible, through monitoring tools and log analysis
- Isolating affected systems to prevent further spread of the attack. For example, shutting down a server or restricting network access
- Analyzing the incident using forensic techniques to understand exactly what happened. This may include analysis of logs, network traffic, system resources and other data.
- Restoring system and data from safe copies. Also, check that all systems are working and secure before allowing users access again.
- Documenting all steps in incident response, including causes, consequences and strategies to prevent repeat attacks, reporting to relevant authorities if required by legislation (e.g. GDPR).

Security incidents

- Incidents:
- A distributed denial of service (DDoS) attack seeks to exhaust system resources. A DDoS attack is initiated by a large number of malware-infected host machines controlled by the attacker.

- DDoS attacks come in three forms:
- 1. Volume-based attacks: Includes UDP floods, ICMP floods and other spoofed packet floods. The aim of the attack is to saturate the bandwidth of the attacked site, and the size is measured in bits per second (Bps).
- 2. Protocol Attacks: Includes SYN Floods, Fragmented Packet Attacks, Ping of Death, Smurf DDoS and more. This type of attack consumes real server resources or those of intermediate communication equipment, and is measured in packets per second (Pps).
- 3. Application Layer Attacks: Includes low and slow attacks, GET/POST floods, attacks targeting Apache, Windows vulnerabilities, and more. Consisting of seemingly legitimate and innocent requests, the goal of these attacks is to crash a web server, and the size is measured in requests per second (Rps).

Security incidents



DDoS attack

Security incidents

- Incidents:
- MITM Attacks (Man in the Middle)
- MITM attacks refer to cyber security breaches where an attacker is allowed to eavesdrop on data sent back and forth between two people, networks or computers. The attacker positions himself in the "middle" or between the two communicating parties, ie the attacker spies the interaction between the two parties. An attacker illegally modifies or accesses a message before it reaches its destination.

- Phishing attack
- A phishing or identity theft attack occurs when a malicious actor sends emails that appear to come from verified, legitimate sources in an attempt to extract sensitive information from the victim. Phishing attacks combine social engineering and technology, and are so-called because the attacker actually "hunts" access to a restricted area using a "bait" from a seemingly trustworthy sender.
- In addition to e-mail, phishers also use other services on the Internet such as Windows Messenger, Skype, Google Talk, social networks (Facebook, Twitter, Pinterest) and others.

Security incidents

- Incidents:
- Brute force attack
- Brute Force Attack is named after the "brutal" or simple methodology used by the attacker. The method consists of the following steps:
- 1. An attacker simply tries to guess the login credentials of someone who has access to the target system. While this may seem time-consuming and difficult, attackers often use bots to crack credentials
- 2. The attacker gives the bot a list of credentials that they think can give them access to the secure area. The bot then tries each one until it hits.

- Botnet attack
- The term "botnet" is derived from the words "robot" and "network". Assembling a botnet is usually the infiltration phase of a multi-layered scheme. Bots serve as a tool to automate mass attacks, such as data theft, server crashes, and malware distribution. Bots use your devices and accelerate hackers' ability to carry out larger attacks.

Protection of networks

- Networks are often the target of attacks because they enable communication and data transfer between devices, if they are not properly protected, serious security incidents can occur. Network protection encompasses a variety of technologies and strategies to prevent, detect and respond to attacks.

- Types of network topologies:
- **Star topology**: All devices are connected to a central device (switch or router). Although it is effective in terms of control, it is also vulnerable if the central device is compromised.
- **Bus topology:** All devices are connected to one cable (bus). This topology is more prone to attacks like sniffing.
- **Ring topology**: Devices are connected in a circular chain. In this topology, attacks can affect the entire network if a single device is compromised or compromised.
- **Mesh topology**: All devices are connected to all other devices. This topology is the most resistant to attacks, but also the most complex.

Protection of networks

- Protection tools:

- **A firewall** is a basic security tool that protects the network from unauthorized access by filtering incoming and outgoing traffic according to defined security rules.
- **Packet-filtering firewall:** analyzes every packet of data entering or leaving the network and decides whether to let it pass or block it based on predefined rules
- **Stateful inspection firewall**: monitors the state of all open connections and allows/inspects packets only if they are part of a legitimate session
- **Proxy firewall**: replaces the real network address with its own, thereby hiding the network infrastructure and preventing direct interaction with the outside world.

- Purpose of Firewall:
- Restricting access to certain services or ports
- Blocking unauthorized traffic

Protection of networks

- Protection tools:

- IDS/IPS (Intrusion Detection/Prevention)
- An Intrusion Detection System (IDS) is a tool that detects suspicious activity in a network and alerts administrators to a potential threat. An IDS does not block an attack, but provides notification of the incident.
- Intrusion Prevention System (IPS), is a preventive tool that not only detects the attack, but also blocks or prevents the attack in real time.

- Purpose of IDS/IPS tools:
- Malicious traffic detection
- Warnings about unauthorized access to the network
- Scans for potential vulnerabilities

Protection of networks

- Protection tools:

- Virtual Private Networks (VPNs)
- A VPN (Virtual Private Network) enables secure and encrypted communication between devices on a public network, such as the Internet.

- VPN provides:
- IP masking: ensures anonymity on the Internet.
- Traffic encryption: uses encrypted tunnel protocols (eg IPSec, SSL, OpenVPN) to protect data traveling from user to destination
- Access to remote networks: allows users to access an organization's internal network as if they were physically present on that network, which is useful for working remotely or accessing sensitive data.

Trends in computer security

- **Security of IoT (Internet of Things)** devices:

- IoT devices have become increasingly prevalent in households and business environments
- The security of IoT devices is a challenge due to the number of devices connected to the Internet and the specific vulnerabilities of the devices themselves. IoT devices are present in various fields including homes, industry, healthcare, transportation...
- IoT devices offer great advantages in terms of automation, efficiency and connectivity, but also a significant security risk.

- Weaknesses of IoT:
- Weak passwords are used or lack authentication
- Most often they do not use encryption
- Irregular update
- Excessive access rights
- Physical vulnerability of the devices themselves
- Lack of safety standards

Trends in computer security

- The security of IoT (Internet of Things) devices can be improved by:
- Encryption of communication: Protocols such as TLS (Transport Layer Security) or SSL (Secure Sockets Layer) can be used to secure communication.
- OAuth and OpenID Connect and Two-factor authentication
- Network segmentation: IoT devices should be connected to separate networks from other critical systems. VLANs (Virtual Local Area Networks) and segmentation with firewalls can help achieve this protection.
- Physical protection
- Use of security protocols such as DTLS (Datagram Transport Layer Security) and MQTT (Message Queuing Telemetry Transport)

Co-funded by the European Union

Trends in computer security

- Using artificial intelligence (AI) in security
- AI and machine learning (ML) can significantly improve security, enabling faster attack recognition, automated incident responses, threat prediction and real-time analysis of large volumes of data.

- Application of AI in Security:
- Automatic threat detection
- Predictive analytics: AI analyzes past attacks and builds a model that predicts the types of attacks in the future.
- Automated responses to threats (SOAR - Security Orchestration, Automation, and Response): isolation of compromised systems, blocking of IP addresses of attackers, or automatic notification of administrators.
- Recognition of social engineering (phishing, vishing): AI analyzes e-mails, SMS messages, calls, can analyze texts, recognize suspicious phrases, links, impersonation. Natural Language Processing (NLP) techniques enable the analysis of language and writing styles
- Using AI to analyze security logs

Co-funded by the European Union

Trends in computer security

- Blockchain technology
- Blockchain is a distributed database technology. This principle enables secure and transparent recording of data in "blocks", which are connected in a linear, immutable and decentralized structure.
- Each block in the blockchain contains data (transactions, information, or other types of records), a timestamp, and a unique hash of the previous block. Through this structure, blockchain enables transparent and secure storage of data, without the need for a centralized intermediary or authority.
- Use of blockchain:
- Cryptocurrencies: the application of blockchain technology is in cryptocurrencies (eg Bitcoin), decentralized transactions without the need for traditional banks or intermediaries.
- Smart Contracts enable the automation and execution of contractual obligations without the need for intermediaries, when the conditions are met, the smart contract is automatically executed.
- Supply Chain Management
- Digital identity: reduces the risk of identity theft.
- Healthcare: security and efficiency in sharing medical data, enabling secure access and control of data by patients and doctors

Regulations in the field of cyber security

- The Council of Europe (CoE) gathers 47 member countries. Its Convention on Cybercrime (known as the 'Budapest Convention') is considered, for now, the most relevant international legal instrument that provides a legal framework for the fight against cybercrime.

- The Budapest Convention provides states with a list of attacks that are considered misdemeanors and are committed via computers, and procedural legal tools for conducting cybercrime investigations, as well as effective storage of electronic evidence of committed misdemeanors, and enables international police and judicial cooperation on cybercrimes and the exchange of e-evidence.

- The CoE has drawn up the Convention on the Protection of Individuals and Automatic Processing of Personal Data (convention number CETS 108), which aims to 'protect every individual, regardless of their nationality or place of residence, as well as the processing of their personal data
- data and thereby contribute to the respect of their human rights and fundamental freedoms, especially the right to privacy'.

Regulations in the field of cyber security

- The Organization for Security and Cooperation in Europe (OSCE) deals with cyber/ICT security issues, especially in the light of the fight against terrorism and cybercrime. In 2013, the OSCE adopted confidence-building measures (CBMs) for cyber proctors through Permanent Council Decision No. 1106, December 3, 2013. These measures aim to reduce conflicts that occur as a consequence of the use of information and communication technologies.
- The Organization of American States (OAS) established the Working Group for Cybercrime as early as 1999 as a basic forum for "strengthening international cooperation on the topic of prevention, investigation and prosecution of cybercrime, as well as enabling the exchange of information and experiences between its members and providing the necessary recommendations for improving and ensuring activities aimed at combating this type of crime."
- The Shanghai Cooperation Organization (SCO), an international organization that brings together six member states (China, Kazakhstan, Kyrgyzstan, Russia, Tajikistan and Uzbekistan), adopted the Agreement between the governments of the SCO member states on cooperation in the field of ensuring international information security in 2009.

Regulations in the field of cyber security

- In 2013, the EU published its first comprehensive document, its Cyber Security Strategy, which addresses a wide range of cyber threats. In 2016, the EU adopted the Directive on the security of networks and information systems (NIS Directive).

- The first cyber defense policy of the North Atlantic Treaty Organization (NATO) was published in 2008. At the Lisbon Summit in 2010, cyber defense was included in NATO's Strategic Concept, and the declaration adopted at the summit predicted the necessity of updating the Cyber Security Policy from 2011 and drafting the accompanying Action Plan from 2012.

Regulations in the field of cyber security

- Countries around the world are developing and adopting strategies to respond to these growing security threats, which include adopting new or amending existing national security policies. National security policies that deal with threats in cyberspace are called National Cyber Security Strategies (NCSS).

- The International Telecommunication Union (ITU) defines the National Cyber Security Strategy (NCSS) as:
- an expression of the vision of the most important goals, principles and priorities by which a country is guided in the fight against cyber threats;
- an overview of the stakeholders tasked with improving the country's cyber security and their respective roles and responsibilities;
- a description of the steps, programs, and initiatives the country will take to protect its national cyber infrastructure, thereby increasing security and resilience.

Regulations in the field of cyber security

- Official statistics indicate an increasing trend in the number of cyberattacks and cybercrime cases in Serbia. During 2020, there were about 26 million cyber attacks on information and communication technology (ICT) systems - the most common of which were attempts to break into ICT systems and unauthorized data collection.
- The field of information security in Serbia is regulated by the Law on Information Security from 2016, which defines the rights, duties and responsibilities of all legal entities and state authorities that manage and use ICT systems.
- This law describes in detail the protection measures against challenges, risks and threats related to ICT systems. The bodies responsible for the protection of these systems, the forms of coordination between these actors and the implementation of prescribed measures are also listed
- Three years after its adoption, this law was amended in order to improve its implementation and to solve problems identified in practice.
- .

Regulations in the field of cyber security

- Participant in the information security sector:
- The main state institutions in the field of information security are the MTTT, the Regulatory Agency for Electronic Communications and Postal Services (RATEL) and its computer emergency team (CERT), as well as the Information Security Coordination Body.
- The right to privacy is regulated by the systemic Personal Data Protection Act of 2018, which is harmonized with the EU General Data Protection Regulation (GDPR).
- GDPR (General Data Protection Regulation) is a European Union (EU) regulation that was adopted in 2016 and became mandatory in 2018. The goal of the GDPR is to protect the privacy and personal data of EU citizens and to provide them with greater control over that data.
- PCI-DSS (Payment Card Industry Data Security Standard) is a set of security standards developed by the Payment Card Industry Security Standards Council (PCI SSC) and refers to the protection of credit card data. PCI-DSS aims to improve transaction security and protect users from identity theft and fraud.

Regulations in the field of cyber security

The most common types of cybercrime in Serbia, source: Republic Public Prosecutor's Office

WBnet

Co-funded by the European Union

Questions & Answers

"Funded by the European Union. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union. Neither the European Union nor the granting authority can be held responsible for them."

Network of centers for regional short study programs in the countries of the Western Balkans

Call: ERASMUS-EDU-2023-CBHE

Project number: 101128813

ATYCC

UNIVERSITY OF L]UBL]ANA
Faculty of Electrical Engineering

POLITÉCNICA

University of Pristina
Kosovska Mitrovica