**Cybersecurity & cyber defence, blockchain**

By Mehmet Ali Erturk

*Istanbul University (Turkey)*

Hello and welcome. Today we will take a quick look at two technologies that are part of digitalization: cyber security and blockchain.

Today we live in a digital world—computers, information technologies, and electronic devices are involved in every aspect of our lives. For example, we use our personal computers when teaching online courses or smartwatches while we record and monitor our health data. We use ATMs to transfer money or we use our computers for e-commerce sites with our credit cards. In addition to that, we keep all our personal or corporate information in cloud systems. All these processes take place on computer systems.

So what is a computer or what is a computing device? Computers are electronic devices designed to execute logical and arithmetic operations automatically. Input, process, output, and storage are the primary functions of computers. For instance, if you want to add two numbers, the two integers are the input, adding to these numbers is the process, and the result is displayed as output. If you want to keep the result in our disks, we use storage functions.

Computer systems can be as small as our smartwatch or very large like supercomputers. Mainly, we have two main components in our computers: one is hardware, and the other one is software. Hardware is the physical component that makes up all the computer; it is the parts that we can touch. Software is the collection of programs running on computer systems. Programs contain instructions that tell computers what to do. For example, we might have useful software such as our browsers we use all day for surfing the internet. However, some software or some programs may not be as good in our browsers. Malicious software, for example, may aim to harm us or our computer systems.

As we said, computers are programmable devices that work on data. We can define data as an effect that computer systems can use, such as letters, numbers, pictures, videos, etc. Information is a form of data that is processed to become meaningful. Actually, we don't need computers to process information; however, computing devices make our lives easier and enable us to reach accurate results with less effort. Also we use our computers and mobile devices to send data over the internet and share our information with others.

So, if we look at the internet, it is the communication infrastructure in today's digital world. It is a network of networks. The history of the internet dates back to the early 1960s. It was first used for military and scientific purposes. Over time, with the increase in public interest and widespread use, the internet has become part of our lives. Now it is possible to access 5G, fifth-generation networks, in many countries. Thanks to the high speed and low latency communication links, what was a dream in the past is now possible today. For example, when using 5G, doctors in different parts of the world can participate and collaborate in a robotic surgery operation. Also, with the expansion of the 5G infrastructure, many objects can now easily have an internet connection, and these objects can be managed remotely.

These ubiquitous connections raise a question: how to keep and maintain our privacy in this digital world? Although access to information is effortless with digitalization, committing crimes in the digital field has become very easy. Hackers with different motivations can break into computers, hijack internet accounts, leak corporate data, alter corporate records, or even shut down power grids. Cyber security, or information security, is the study of protecting systems, networks, and data from unauthorized attacks. The aim of cyber security is to keep our data consistent and prevent unauthorized access.

Today, there are different types of cyber threats available; however, we are going to look at the most well-known methods, such as malware. Malware is malicious software designed to gain access to computer systems. Devices impacted with this software may perform operations against the user's intention. It can cause damage or steal information. Also, the host computer can become a vector for hackers and criminals, so criminals can hide their identities and commit crimes using these computers. There are a lot of malware types available today, however the most popular one these days is ransomware. Ransomware encrypts the victim's file system for ransom and blocks access. It usually results from clicking a malicious link in an email or an instant messaging app, and sometimes it is not easy to recover encrypted data.

Phishing is another type of attack where victims are targeted with fake emails. The motivation of the hackers is to steal money or sensitive data from the victims. They send fake links by emails or other platforms to redirect victims to a webpage where they can steal their credentials easily.

Denial of Service (DoS) Attacks are a different type of attack than malware. In the DoS attacks a network or internet service is targeted to make it temporarily or permanently inaccessible to targeted users. For example, a DoS attack targeted against an e-infrastructure, such as e-government, can block citizens from accessing its services. There are many kinds of DoS attacks that use various techniques such as distributed denial of service (DDoS) attacks.

Another type of attack is Advanced Persistent Threats (APT) attacks. APT attacks attackers need to be high-profile secured persons. Usually these kinds of attacks require advanced knowledge and resources to carry out. These types of attacks are usually funded by organizations or governments. APT attacks are quite sophisticated and aim to gain access to a system undetected for a long time, allowing criminals to inspect these systems deeply.

So what makes computer systems insecure against these threats? There are a few methods or a few factors that make these systems insecure, and we are going to discuss only three of them. The first one we have is design issues, hardware and software design is a key point. Engineers should consider security features when designing a system. Designs without security in mind result in flawed systems that are open to exploits that will allow attackers to gain access.

The second reason is misconfiguration. A system can be designed with security in mind; however, faults in security configuration can lead to potential leaks. A system designed to be very secure must be updated with configurations for zero-day and new threats.

Our third subject is humans. As long as humans are involved, there is always a security risk. For example, any wrong action by an employee can cause an internal system to be infected by viruses or Trojans. Also, an unmotivated employee could steal their company's data or allow criminals to access these systems. No system can be guaranteed to be 100% secure; however, we have tools with which we can take actions.

The first and most important thing is cyber security awareness. It is the education process that introduces cyber threats and how to take necessary precautions. These trainings should be given regularly to users at different levels and should be regularly repeated to increase awareness of security threats.

In addition to that, we have hardware and software security solutions that prevent unauthorized access to our systems. For example, we have firewalls that monitor network traffic and analyze outgoing and incoming data to enforce predefined security rules. They can block or allow access requests from servers to users. Firewalls can operate at any level in the stack, such as physical, network, or application. There are specific versions of firewalls dedicated to web applications, called Web Application Firewalls (WAFs), which contain web-specific security rules.

We have another tool which is called Intrusion Detection Systems (IDS), which uses advanced analytical methods to generate alerts about suspicious activity on the network or within a company. To give a concrete example, we can configure our firewalls so that only the set of services we allow are accessible from outside the organization, thus unauthorized persons cannot connect to servers behind firewalls. Another example is we can use our WAFs to block SQL injection attacks in our web servers. Any request with suspicious activity will be blocked by our Web Application Firewalls. Also, we can use IDS systems to identify and generate alerts when employees act outside their usual patterns. For example, if an employee tries to access office files from an unusual location, the IDS system can generate a warning, and this situation can be reported to the security manager.

We can discuss many more examples, but let's move to another security prevention mechanism, authentication. Authentication is a mechanism that verifies whether users are what they claim to be. We have various methods have been developed for authentication, but the essential one is the username and password that we use daily in online services.

Today, malware, viruses, ransomware, and Trojans are spreading rapidly. Antivirus software are security tools developed to prevent these malicious software from impacting our computers and servers.

Another method we can use to stay secure in the online world is encryption. It is a method in which information is changed in such a way that observers cannot read it while it is transmitted over the internet. We call unreadable text as a cipher. Advanced mathematical algorithms are available to create strong encryption so that it cannot be decoded using external intervention. Today, we have symmetric and asymmetric cryptographic algorithms to secure, restore our data, or transmit over a communication channel.

We can develop secure, persistent, and modifiable systems against cyber attacks with encryption and cryptographic algorithms. One of the use cases are the blockchain technologies. Blockchain is a digital ledger that works in a distributed manner. The idea was first introduced in 1991; however, the technology became popular with the digital cryptocurrency Bitcoin. When the decentralized trust-based Bitcoin network introduced it, it caught the world's attention, and the digital ledger idea started appearing in various applications.

A distributed system doesn't need central management, and the network takes the necessary actions. For example, today's banking system is centralized and requires an authority to regulate all its operations. The bank handles all the necessary steps if someone needs to send money to another entity. In contrast, distributed systems such as blockchain and blockchain-based cryptocurrencies work peer-to-peer. One can send money directly to another entity without needing a bank.

Both centralized and distributed systems have their advantages and disadvantages. The main drawback of a distributed system is execution time. Centralized architectures enable faster transactions since everything is centralized. Operations on distributed systems can take a lot of work and time; however, it offers freedom of choice.

Blockchain relies on secure cryptographic algorithms and consensus methods that enable information to be persistent, valid, and unmodifiable across the network. Simply, a record is a representation of a single transaction, called a block, and these blocks are linked together to construct the blockchain. Blockchain is simply a distributed database system that doesn't require central authority. Each node in the network can work without central intervention. Whenever a transaction is initiated, this operation is distributed to all nodes over the network, and it is necessary to validate if the transaction is correct. If the operation is correct, it is approved to be persistent in the ledger.

The consensus mechanism is necessary to check if the current action is valid or not. This method is called proof of work. Blockchain networks work in a distributed manner, and the network's peer operations must be validated. The technical term for this validation is the consensus mechanism. Several algorithms are developed to provide consensus; however, proof of work is the most popular due to cryptocurrencies, such as in the case of Bitcoin. Whenever an entity sends Bitcoins to another entity, nodes in the network perform complex cryptographic algorithms to generate hashes and verify if the transaction is valid. This distributed consensus method is called proof of work; however, proof of work requires more computational power and execution time. We have alternative methods like proof of stake and proof of identity exist.

Consensus algorithms enable all nodes in the network to have the same consistent state. This means whenever a transaction request pops up on the network, it is validated and distributed to all nodes, thus nodes in the network have all the same information.

In blockchain networks, we have smart contracts that can be defined as programs that perform automatic tasks based on predefined conditions. Smart contracts execute necessary actions based on the terms and conditions agreed upon among the parties themselves. The terms and conditions are implemented as software applications and executed on nodes, if something happens a specific action is taken.

We are able to use smart contracts to build blockchain applications. Blockchain applications and networks can be distributed as public or private. In private networks, there is a joining procedure called authorization.

There are many applications for blockchain, not only limited to finance. It can be used in healthcare, such as for storing our health records on blockchain, it can be used in education, logistics, and the Internet of Things (IoT). Another application could be e-government. For example, an e-voting system can be implemented in a blockchain infrastructure so attackers or criminals are not able to access or modify the data in the network.

Today, we have discussed two important topics, which were cyber security and blockchain. Hope to see you all in the next lecture. Thank you.

* -

*This material was recorded at the University of Tartu (Estonia) in March 2023. Its transcript was edited for clarity purposes.*

Mehmet Ali Erturk (2023) *Cybersecurity & cyber defence, blockchain.* Material developed within theErasmus+ project 2021-1-TR01-KA220-HED-000027609 “Digital Diplomacy: Building the Common Future with Technology (DD-Tech)”. Tartu: University of Tartu.