

MINISTRY OF EDUCATION AND SCIENCE OF THE REPUBLIC OF KAZAKHSTAN

AL-FARABI KAZAKH NATIONAL UNIVERSITY

Faculty of physical and technical
Department of solid state physics and nonlinear physics

Analysis of telecommunication network security mechanisms
based on security events.

Executor :Tursynbek Ye.N.

Scientific supervisor : Imanbayeva A.K.

Almaty , 2021

The aim of the graduation project:

- To research on local network security.
- To simulate the model of attacks to local network and analyse the how the local network will behave during an attack.

Relevance of the work:

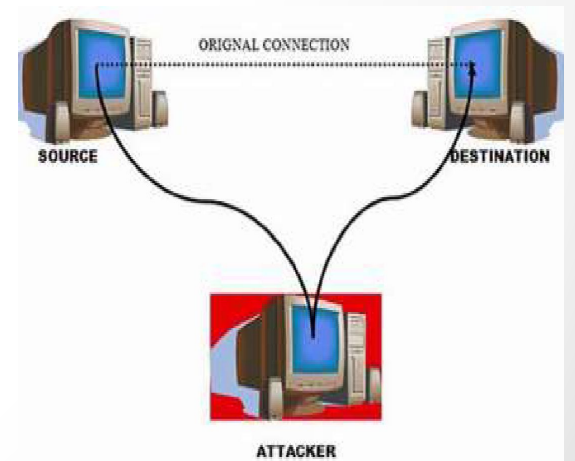
- Information in modern world is one of the most valuable things in life, requiring protection from unauthorized access of persons who do not have access to it.

The object of research of the graduation project: model of the local network in Arena simulation software.

Research methods: computer modelling and simulating.

What is a Cybersecurity Threat?

A cybersecurity threat is a malicious and deliberate attack by an individual or organization to gain unauthorized access to another individual's or organization's network to damage, disrupt, or steal IT assets, computer networks, intellectual property, or any other form of sensitive data.



Types of Cybersecurity Threats

While the types of cyber threats continue to grow, there are some of the most common and prevalent cyberthreats that present-day organizations need to know. They are as follows:



1) Malware

[Malware attacks](#) are the most common type of cyberattack. Malware is defined as malicious software, including spyware, ransomware, viruses, and worms, which gets installed into the system when the user clicks a dangerous link or email. Once inside the system, malware can block access to critical components of the network, damage the system, and gather confidential information, among others.

2) Phishing

Cybercriminals send malicious emails that seem to come from legitimate resources. The user is then tricked into clicking the malicious link in the email, leading to malware installation or disclosure of sensitive information like credit card details and login credentials.

3) Spear Phishing

Spear phishing is a more sophisticated form of a phishing attack in which cybercriminals target only privileged users such as system administrators and C-suite executives.

4) Man in the Middle Attack

Man in the Middle (MitM) attack occurs when cyber criminals place themselves between a two-party communication. Once the attacker intercepts the communication, they may filter and steal sensitive data and return different responses to the user.

5) Denial of Service Attack

Denial of Service attacks aims at flooding systems, networks, or servers with massive traffic, thereby making the system unable to fulfill legitimate requests. Attacks can also use several infected devices to launch an attack on the target system. This is known as a Distributed Denial of Service (DDoS) attack.



6) SQL Injection

A Structured Query Language (SQL) injection attack occurs when cybercriminals attempt to access the database by uploading malicious SQL scripts. Once successful, the malicious actor can view, change, or delete data stored in the SQL database.

7) Zero-day Exploit

A zero-day attack occurs when software or hardware vulnerability is announced, and the cybercriminals exploit the vulnerability before a patch or solution is implemented.

8) Advanced Persistent Threats (APT)

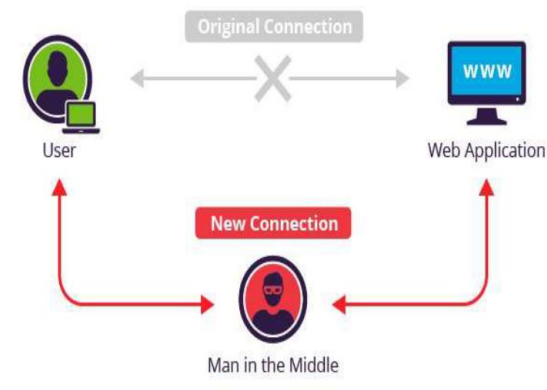
An advanced persistent threat occurs when a malicious actor gains unauthorized access to a system or network and remains undetected for an extended time.

9) Ransomware

Ransomware is a type of malware attack in which the attacker locks or encrypts the victim's data and threatens to publish or blocks access to data unless a ransom is paid.

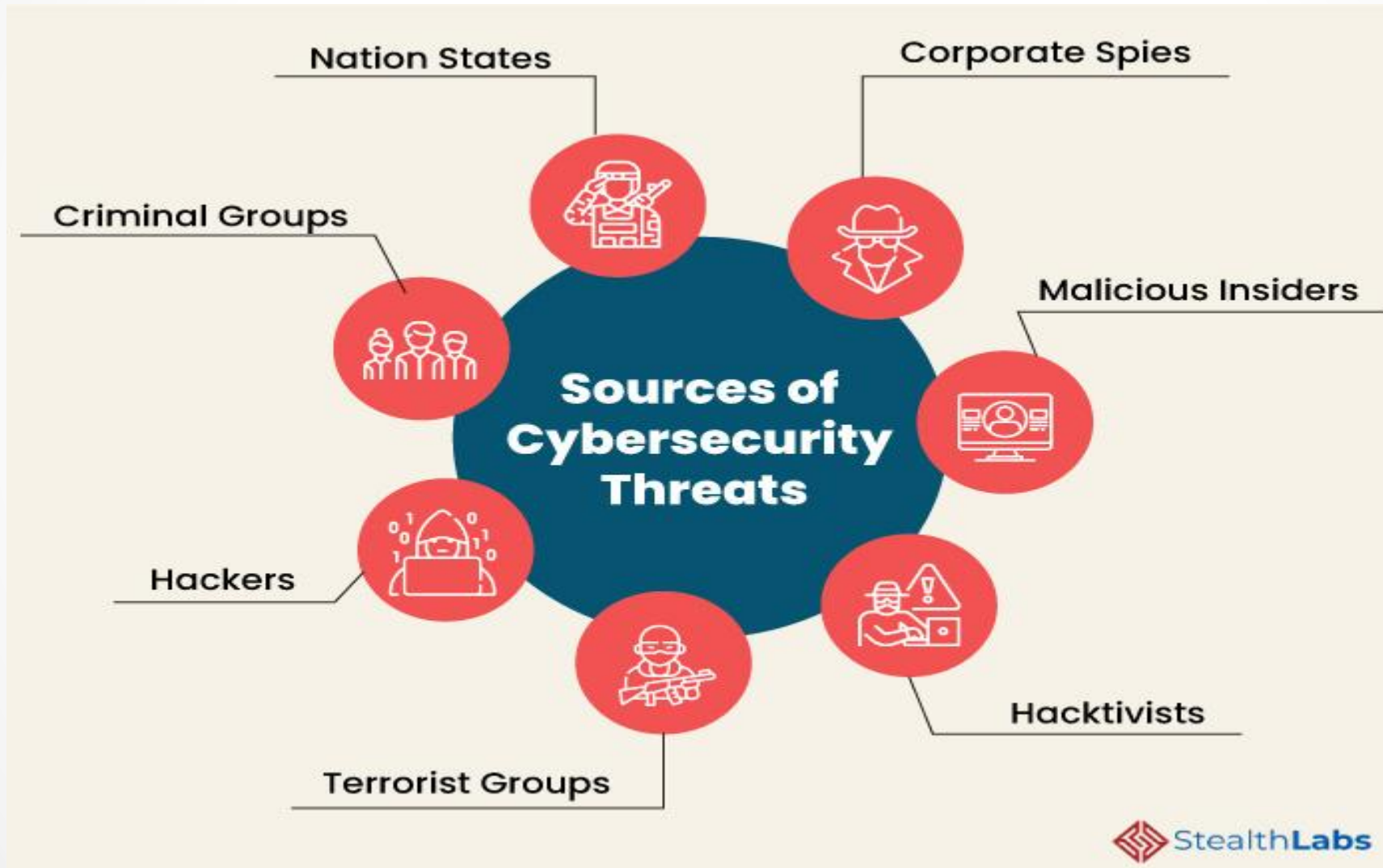
10) DNS Attack

A DNS attack is a cyberattack in which cybercriminals exploit vulnerabilities in the Domain Name System (DNS). The attackers leverage the DNS vulnerabilities to divert site visitors to malicious pages (DNS Hijacking) and exfiltrate data from compromised systems (DNS Tunneling).



Sources of Cybersecurity Threats

In order to respond effectively to a cyberattack, it's imperative to know the threat actors and understand their tactics, techniques, and procedures.



Here are some of the common sources of cyber threats:

1) Nation States

Cyber attacks by a nation can inflict detrimental impact by disrupting communications, military activities and everyday life.

2) Criminal Groups

Criminal groups aim to infiltrate systems or networks for financial gain. These groups use phishing, spam, spyware, and malware to conduct identity theft, online fraud, and system extortion.

3) Hackers

Hackers explore various cyber techniques to breach defenses and exploit vulnerabilities in a computer system or network. They are motivated by personal gain, revenge, stalking, financial gain, and political activism. Hackers develop new types of threats for the thrill of challenge or bragging rights in the hacker community.

4) Terrorist Groups

Terrorists conduct cyber attacks to destroy, infiltrate, or exploit critical infrastructure to threaten national security, compromise military equipment, disrupt the economy, and cause mass casualties.

5) Hacktivists

Hactivists carry out cyberattacks in support of political causes rather than financial gain. They target industries, organizations, or individuals who don't align with their political ideas and agenda.

6) Malicious Insiders

Insiders can include employees, third-party vendors, contractors, or other business associates who have legitimate access to enterprise assets but misuse that access to steal or destroy information for financial or personal gain.

7) Corporate Spies

Corporate spies conduct industrial or business espionage to either make a profit or disrupt a competitor's business by attacking critical infrastructure, stealing trade secrets, and gaining access.

What should we expect in 2021?

Here are some of the emerging cybersecurity threats that will dominate the cybersecurity landscape in 2021 and beyond:

1) Pandemic-related Attacks

The cybercriminals will continue to leverage the coronavirus pandemic and related topics as themes for their phishing and social engineering campaigns. Their attacks often coincide with significant events, such as a sudden surge in COVID-19 cases or the announcement of a new vaccine. The threat actors lure users into clicking a malicious link or attachment disguised as legitimate COVID-19 related topics.

2) Ransomware Attacks

According to Cybersecurity Ventures, businesses will fall victim to a [ransomware attack](#) every 11 seconds in 2021, down from every 14 seconds in 2019. The estimated cost of ransomware, including the cost to restore and mitigate following an attack, will cross USD 20 billion in 2021.

3) Cloud Breaches

As more companies migrate to the cloud to facilitate remote working and ensure business continuity, cybercriminals are following the same trend and targeting the cloud more frequently. Cloud-based security risks, including cloud misconfigurations, incomplete data deletion, and vulnerable cloud-apps, will be the common sources of cyberattacks.

4) Mobile Security Threats

In a bid to ensure business continuity amid the pandemic, almost all businesses initiated work from home facility. Employees working remotely use devices such as smartphones and tablets that are not properly secured, patched, and managed by the IT security department. Unfortunately, they bring some unique IT security threats and vulnerabilities, putting the organization at the risk of a cyberattack.

5) IoT Attacks

Global organizations are increasingly deploying IoT devices and applications to accelerate operations, capture more data, remotely manage infrastructure, improve customer service, and more.

What is Arena?

Arena is a simulation software product that provides an integrated framework for building simulation models in a wide variety of applications.

We will now look at the Arena simulation software, practical session 1.

Arena is a simulation software product that provides an integrated framework for building simulation models in a wide variety of applications. The functions needed for simulation include:

- Modelling
- Animation
- Model verification
- Analysis of inputs and outputs data
- Results of analysis

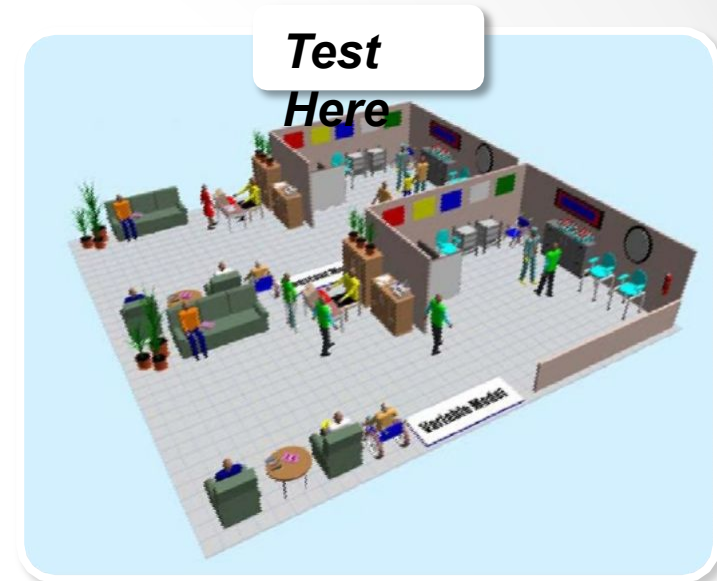


What is Discrete Event Simulation?

- **Discrete Event Simulation,**
 - *Modeling events that occur over **time**, with **variability** and **system interactions** to provide highly accurate predictions of system performance and capabilities under virtually any set of conditions.*

What Simulation does for your company?

- Understand how complex systems work
- Answer critical “What if..?” questions
- Visualize operations
- Insurance policy for major decisions
- Completely risk-free environment





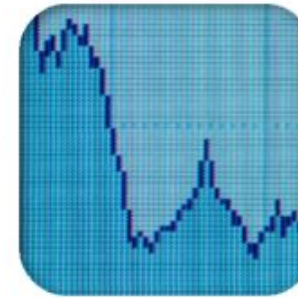
*Interface for data
and results*



*Crunched thru
model logic*



*Creates a Visual
Simulation*



*That outputs
statistical data*



That results in enlightenment





Thank you for attention!