PLOVDIV UNIVERSITY
"PAISII HILENDARSKI "

M.Eng. Ivaylo Detelinov Uzunov

SIMULATION MODEL AND FINAL SOLUTIONS OF SECURITY SYSTEMS

ABSTRACT

of a dissertation for the acquisition of the educational and scientific degree "DOCTOR"

Field of higher education:
5. Technical sciences

Professional field:
5.3. "Communication and computer technology"

Doctoral program:
"Automation of areas of the intangible sphere (medicine, education, science, administrative activities, etc.)"

Scientific supervisor:
Prof. Slavi Yasenov Lyubomirov, Phd

Plovdiv, 2025

The dissertation is 176 pages long. , including 61 figures, 3 tables, formatted in an introduction, 4 chapters, general conclusions, scientific-applied and applied contributions, a list of terms and abbreviations used, a list of the author's publications. The list of cited literature includes 143 titles.Appendix 1

The designations of formulas, figures and tables in the abstract coincide with those in the dissertation.

The dissertation work was discussed and directed for defense at a meeting of the department council of the department "ELECTRONICS, COMMUNICATIONS AND INFORMATION TECHNOLOGIES" at the "PAISII HILENDARSKI" UNIVERSITY OF PLOVDIV.and 13.02.2025

The dissertation defense will take place on May 14, 2025 at 1:00 PM. hours, floor 4, 21 Kostaki Peev St.

The materials for the doctoral defense are available to those interested in the office of the Faculty of Physics and Technology at the "PAISII HILENDARSKI" UNIVERSITY OF PLOVDIV,room 214.

Scientific jury: Prof. Nevena Stoyanova Mileva, Phd
Prof. Dimitar Mihaylov Tokmakov, Phd
Prof. Todor Stoyanov Jamiikov, Phd
Assoc. Prof.Vladimira Krasteva Ganchovska, Phd
Assoc. Prof.Nikolay Atanasov Shopov, Phd

Author: M.Eng. Ivaylo Detelinov Uzunov
Title: SIMULATION MODEL AND FINAL SOLUTIONS OF SECURITY SYSTEMS

Circulation: 30 pcs.

GENERAL CHARACTERISTICS OF THE DISSERTATION

Relevance of the problem

In the modern information society, free and safe access to the Internet, security and safety of information flows are of vital importance for individuals, organizations and society as a whole. Today, all major social activities (governance, economic, educational, information, trade, entertainment) are carried out in the information space and everyone tries to use them to achieve their own political goals, which leads to the so-called "Information War".

We are already living in the conditions of such a war - the facts presented in the Verizon 2020 Data Breach Investigation Report show that as many as 90% of cases of breaching someone's information base are carried out by external sources; 4% of cases involve insiders, and only 1% come from business partners; 79% of information security breaches are due to a system flaw; 85% of breaches are discovered only after 2 weeks.

Information is the most valuable asset that organizations have. Intellectual property, know-how, patents, customer and supplier lists – this information is vital for any organization and forms its competitive advantage. One of the most important challenges facing them is the protection of information in all its forms – electronic and physical. Information must be reliably protected both from external attacks – hackers or natural disasters, and from internal ones – current and former employees, partners and suppliers.

The rapid development of information technology and the expansion of internet connectivity have led to an increase in threats to the security of data and information systems. According to Forbes (John, 2024), in 2023 alone, 2,365 cyberattacks were reported with 343,338,964 victims, which is a 72% increase in data security breaches since 2021. In this context, protecting information and ensuring reliable and secure computer systems and networks are essential to prevent cyberattacks and minimize the risks associated with data leakage, unauthorized access and other malicious actions.

Creating practical guidelines for protecting network infrastructures and web applications based on the researched techniques and tools is of utmost importance.

Modern threats require an integrated approach that includes regular testing, simulation analysis, implementation of cryptographic models, and active monitoring of network systems. The results obtained can serve as a basis for developing new protection strategies and implementing innovative solutions in a dynamically changing cyber environment.

Purpose of the dissertation:

Based on the overview of the problems related to network security and protection of valuable information resources of a given organization, as well as ensuring the integrity of information in order to minimize the damage resulting from modification or destruction. Based on the analysis of the situation, the goal and objectives of the dissertation work are formed.

The aim of the dissertation is to investigate the possibilities of applying a simulation model and final solutions to security systems. On this basis, to justify approaches for conducting research on network information systems in terms of security.

Tasks to achieve the goal:

1. To conduct a study and analysis of the specifics of the main types of threats, the specific criteria and their impact factors.
2. To conduct research on the basic methods and approaches for encrypting information in order to prevent attacks. To conduct simulation analysis and research of cryptographic models in security systems.
3. To conduct research on network information systems in terms of security using various network scanning tools.
4. Choosing an approach to conduct research on different types of attacks in a Matlab environment. To investigate the different stages, efficiency and resilience against cryptographic attacks.
5. To conduct and present experimental research by applying simulation models and final solutions to security systems with the aim of a strategy for minimizing the risks associated with computer threats and analyzing the results.

Research methods and tools used:

The research methods used are from the scientific fields: theory of techniques and tools for computer security for assessing the structure and parameters of basic components of communication systems,computer security methods, modeling and simulation analysis.

Implementation and practical applicability

Data on the impact of computer attacks on system security has been implemented, researched and analyzed.

Models have been developed to study types of attacks, encryption algorithms, and countermeasures against various types of attacks.

Publications on the topic

The main results have been published in: 2 issues in the 17th International Technology, Education and Development Conference, INTED2023 Proceedings, 1 issue in the collections of reports of the International Conference of Young Scientists, SUB - Smolyan. 2 issues in the collection of reports "EDUCATION, SCIENCE, SOCIETY" Four of the publications are co-authored with the scientific supervisor and one is independent.

CONTENT OF THE DISSERTATION

Chapter 1. Literature review on the topic of the dissertation

This dissertation presents a simulation model and final solutions for security systems for the types of threats in computer systems. An analysis and evaluation was carried out in laboratory conditions provided by the Faculty of Physics and Technology (FTT) - Smolyan, for the purposes of the study and for creating the simulation model. The tasks set, as well as the scientific methods and tools used, outline the significance of the goal set in the dissertation:

Innovative approaches are proposed for interpreting the results of scientific research on the given issue;

A review and analysis of algorithms for determining the types of threats in computer networks is carried out;

A verified algorithm is proposed for discussion, taking into account the main types of threats, specific criteria and impact factors.

With the evolutionary development of technologies, requiring new approaches to communication and data storage, new operating systems, protocols or simply new versions thereof, new vulnerabilities appear, leading to new threats and, accordingly, attacks. For modern information security, it is of vital importance to periodically study, research, systematize and develop new protective procedures, techniques, mechanisms and solutions.

*Timeliness.*Cybersecurity breaches are now a part of everyday life, and the personal information of millions of users is increasingly compromised. Organizations are making significant efforts to reduce the damage from hacker attacks and change their cyber defense tactics. The main problem for business organizations remains – whether protection policies are implemented and whether they are ultimately reliable enough. The main challenges faced by all organizations are:

Sustainability – maintaining the basic functions of organizations in crisis situations;

Detection and recovery of security incidents and breaches;

Creating secure system and product architectures and designs;

Developing secure code;

Information security and reliability – encryption, authentication, protection, communication methods;

Integration of security models and improvement of business processes;

Results of the literature review on the topic of the dissertation

Based on the literature review, it is established that modern computer threats are multifaceted, with their diversity and complexity growing proportionally with the advancement of technology. The main types of computer threats can be categorized into the following groups:

1. Malware: Includes viruses, worms, Trojan horses, ransomware, and spyware. These threats aim to steal data, disrupt systems, or extort money.
2. Network security threats: These include attacks such as DDoS, MITM (Man-In-The-Middle) attacks, infiltration of networks through unsecured access points, and exploitation of vulnerabilities in network protocols.
3. Social engineering: This category of threats is based on user manipulation, such as phishing, scams, and fraud aimed at extracting sensitive information.
4. Threats related to unauthorized access: These include attacks based on weaknesses in authentication, such as using weak passwords, exploiting vulnerabilities in authorization systems, and misconfigured accounts.
5. Threats to cloud environments: The development of cloud technologies has led to new risks, including data breaches, lack of access control, and infrastructure vulnerabilities.

6. Industrial and IoT threats: Devices connected to the Internet of Things (IoT), as well as industrial process control systems, are subject to specific risks, such as hacker attacks that can lead to physical damage.

The literature review reveals that effective threat management requires a multidisciplinary approach, including technical, organizational and legal measures. Also, maintaining awareness of new forms of threats and their development is of key importance for the protection of information systems.

Prevention, combined with timely detection and response, remains a key strategy for minimizing the risks associated with computer threats.

Chapter 2. Simulation analysis and research of cryptographic models in security systems

This chapter examines the basic methods and approaches for encrypting information. It discusses the principles and tools of encryption that underlie modern data protection solutions. It analyzes the basic methods for ensuring information security, as well as the factors affecting the speed of encryption algorithms.

Particular attention is paid to the presentation of schemes for the operation of encryption algorithms, with the emphasis placed on the key problem of ensuring information protection. The different types of encryption, their characteristics in terms of speed and security, as well as the modern challenges associated with these aspects are considered. The main goal of this chapter is the presentation and analysis of methods and solutions for data protection, including the assessment of their effectiveness.

2.4. Basics of information encryption

The AES (Encryption Keys and Rounds) encryption algorithm is a block cipher consisting of a block of 128 bits in length that uses the same key to perform multiple rounds of encryption. It converts the entire text into a single block of bits. In AES, the block length can be 128, 192, and 256 bits.

The term "blockwise" refers to how the algorithm mixes block data by re-encrypting it from the initial 10 to 14 rounds depending on the choice of key length.

AES is based on a design principle known as a substitution-permutation network and is efficient in both software and hardware [1]. This cipher is a variant of Rijndael encryption (Fig. 2.1.) with a fixed block size of 128 bits and a key size of 128, 192, or 256 bits. Rijndael is defined with block and key sizes in multiples of 32 bits with a minimum of 128 and a maximum of 256 bits.

2.6. Results of the research conducted

In symmetric encryption, the sender and receiver must have a common shared secret key, which they exchange before initiating communication. The sender uses this key to encrypt the plaintext according to the values of its requirements, and the receiver uses it to decrypt it with the sender's shared key. One of the main advantages of using symmetric algorithms is that they operate at the maximum speed at which data can be encrypted and decrypted with low computational energy. One of the conditions in AES is the requirement for an efficient key management system.

Conclusions

The study of cryptographic models and simulation analysis in security systems demonstrate the key role of these technologies in protecting information in the modern digital world. As a result of the analyses conducted and the review of existing research, the following main conclusions can be drawn:

1. Efficiency of cryptographic algorithms: Simulation of various cryptographic algorithms has shown that their efficiency depends on factors such as key length, encryption method (symmetric or asymmetric), and the key management techniques applied.
2. Security against attacks: Simulations have revealed that cryptographic models with more complex and adaptive structures offer greater resilience against attacks such as cryptanalysis, brute force attacks, and man-in-the-middle (MITM) attacks.
3. Choosing appropriate algorithms: The analyses emphasize that the choice of algorithm depends on the specific application context – for example, symmetric algorithms (such as AES) are preferred for fast encryption of large volumes of data, while asymmetric algorithms (such as RSA and ECC) are better suited for secure key transmission and authentication.
4. The role of hash functions: Simulations have confirmed the importance of hash functions (such as SHA-256) for data integrity and security of authentication protocols. They play a key role in protecting against data tampering.
5. Opportunities and limitations of quantum-resistant algorithms: Research in this area has shown that quantum-resistant algorithms such as those in the Lattice-based and Hash-based cryptography classes offer potential protection against quantum attacks, but at the same time pose new challenges related to performance and their integration into real systems.
6. Importance of simulation analysis: Conducting simulations contributes to assessing the resilience of cryptographic systems in various scenarios, allowing for the identification of weaknesses and optimization of security before implementation in real applications.

Chapter 3. Research on network information systems in terms of security

In order to reduce attacks and improve security, methods for checking and eliminating gaps leading to potential unauthorized access by third parties have been researched and presented.

An algorithm of steps for protecting the computer system from potential threats is presented.

In this context, the focus is on one of the main problems, namely cybersecurity. The emphasis is on the types of vulnerabilities and vulnerable points in computer systems.

3.1.Network scan research

At this point in the dissertation, a study of network scanning using the Nmap product has been made. It was created to facilitate users who are not familiar with the command line by providing an intuitive interface for performing complex network analyses.

Nmap is widely used in areas such as ethical penetration testing, network administration, and vulnerability research and analysis.

3.1.1.1. Phishing attack investigation with SEToolkit

Preparing the attack:

The attacker runs SEToolkit on their system (usually a Linux-based distribution like Kali Linux);

From the tool menu, the relevant settings for a phishing attack are made, which allows cloning a website (Fig. 3.5).

3.7. Researching PHP Code Injection

Researching and analyzing PHP Code Injection plays an important role in computer security, as it is a serious vulnerability in web applications that allows attackers to insert and execute arbitrary PHP code on the server. Fig. 3.7 illustrates a PHP Code Injection attack, in which malicious code is injected through input fields or query parameters that are not adequately validated.

3.7.1. Researching protection against PHP Code Injection

Researching and analyzing PHP Code Injection plays an important role in computer security, as it is a serious vulnerability in web applications that allows attackers to insert and execute arbitrary PHP code on the server. Fig. 3.7 illustrates a PHP Code Injection attack, in which malicious code is injected through input fields or query parameters that are not adequately validated.

3.8. SQL Injection Research

Research on SQL Injection (SQLi) has shown that it is one of the most widespread and critical vulnerabilities in web applications, which puts data security and system functionality at risk. It allows malicious actors to inject and execute malicious SQL commands through improperly secured input fields. Fig. 3.8 shows a demonstration of a SQL Injection attack, in which an attacker exploits a vulnerability in a database query to bypass security checks or extract sensitive information.

Parameterize the query – you need to use prepared statements to separate the SQL command from the data:

- $stmt = $pdo->prepare("SELECT * FROM users WHERE username = ? AND password =?");
- $stmt->execute([$username, $password]);

sed in ORM - Eloquent or Doctrine tools will automate application processing, minimizing the risk of vulnerabilities.

Minimize privileges – Restrict database rights to application users in order to limit access to critical operations.

Conclusion

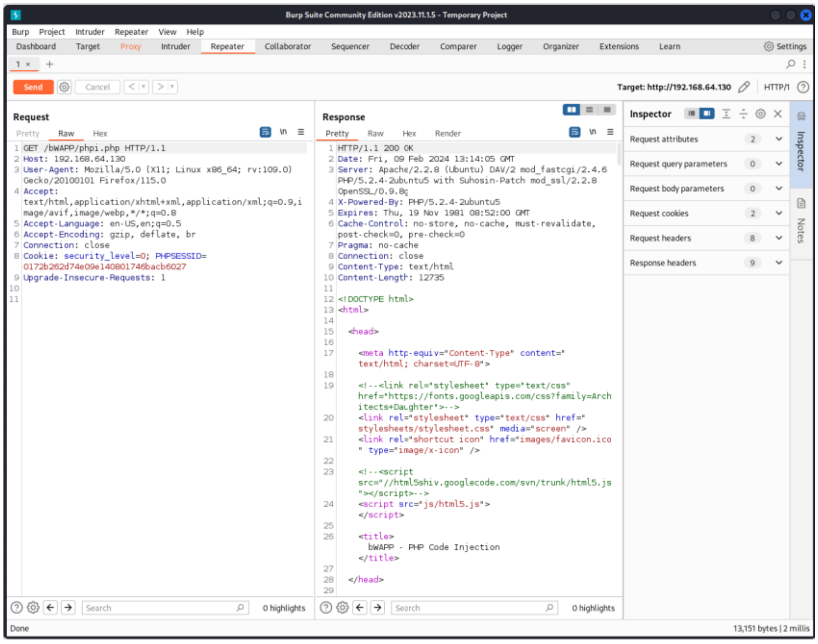


Fig. 3.8. *SQL Injection – How it works and Prevention*

3.8.1. Researching SQL Injection Types

Classic SQL Injection- Direct code injection into the SQL query.

Blind SQL Injection- The attacker obtains indirect information by analyzing the responses from the server

Union-based SQL Injection - The UNION operator is used to combine results from different tables.

Error-based SQL Injection- Abuse of errors generated by the database to extract information Fig. 3.9.

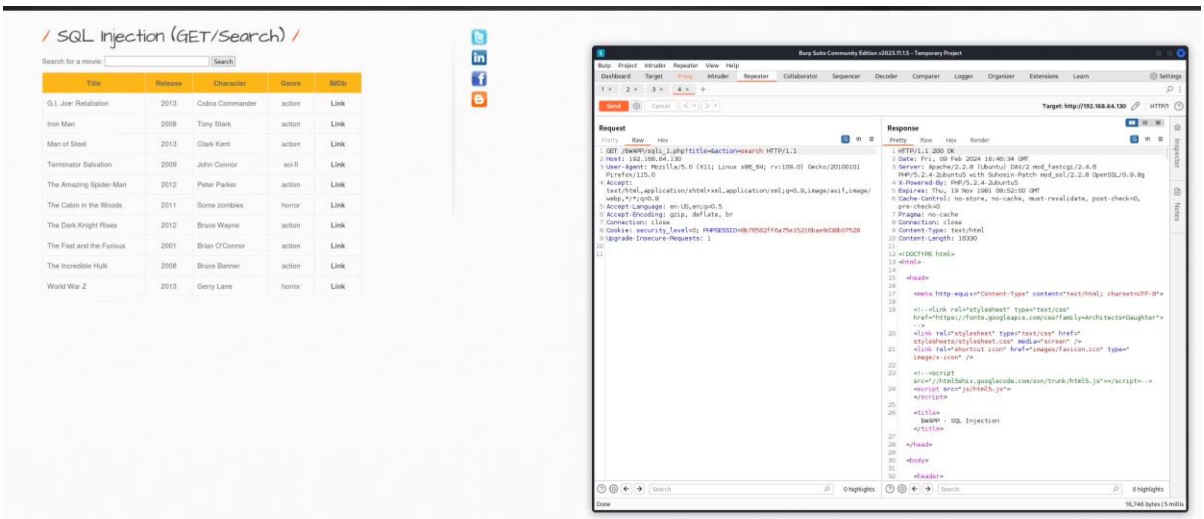


Fig.3.9. *Intercepting and Compromising the Request with Burp Suite*

3.9. Analysis of Action Search and its role in the system

The study uses Action Search, which provides functionality for performing direct database queries. Action Search is a robust information retrieval platform that eliminates the need for user intervention in the main search process.

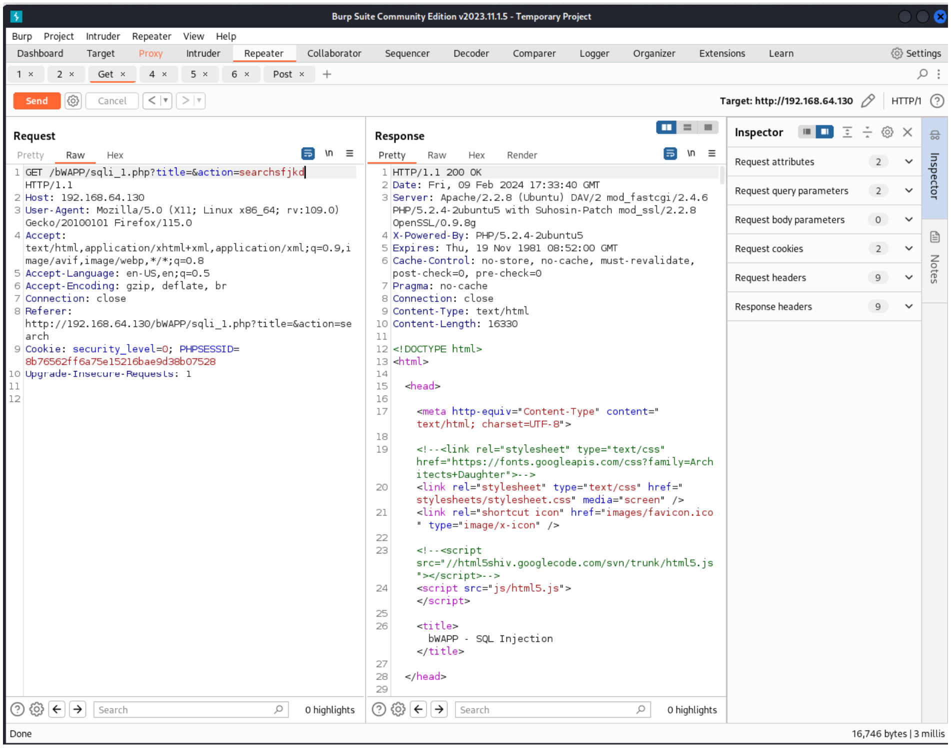


Fig.3.10. Action Search

3.16. Research Base64 encoding

In many cases, web application requests and responses are encoded in different formats. A common example is the use of Base64 to encode data such as usernames and passwords. Decoding data such as that captured with Burp Suite can reveal important vulnerabilities.

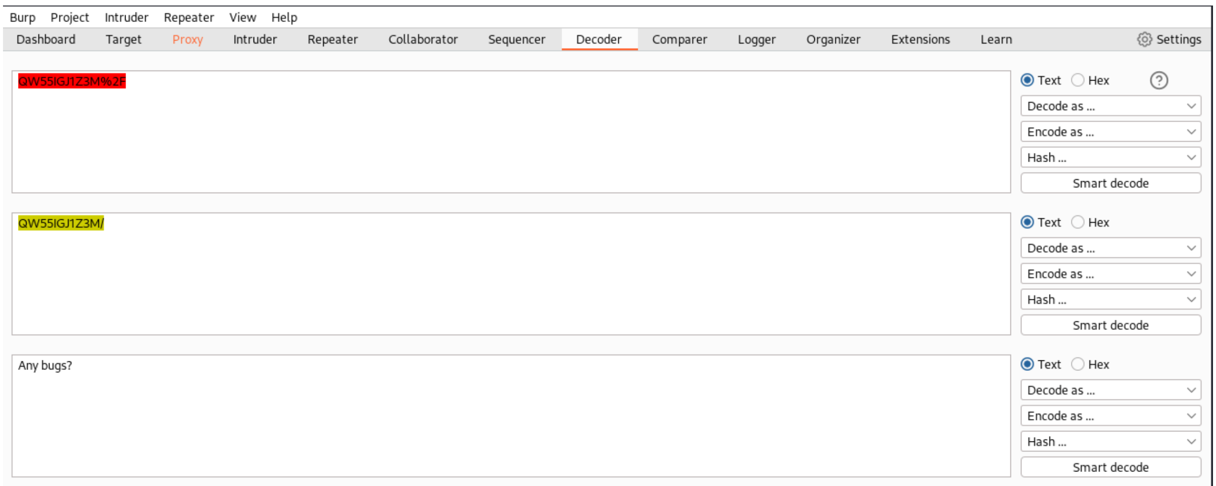


Fig 3.14. Password decoding

As can be seen from Figure 3.14, Base64 provides no security whatsoever, as anyone can easily decode the data. This is especially vulnerable if it is used for sensitive information such as usernames and passwords.

Recommendations:

Avoid using Base64 for sensitive data;

The use of cryptographic methods for data protection is of particular importance in protecting information;

Regularly check and analyze encrypted data for potential vulnerabilities.

3.17. Researching Cross Site Scripting

Stored Cross-Site Scripting (XSS) vulnerabilities pose a serious threat to the security of web applications, allowing malicious users to inject and store malicious JavaScript code on the server. During testing of a web application, a vulnerability was discovered in a blog section that allows the input and storage of invalid user data. This research presents an analysis of the vulnerability and offers recommendations for addressing it.

Conclusion

The discovery of a stored XSS vulnerability highlights the need for strict control over input and output data in web applications. Although no escalation to a successful attack was observed in this case, the vulnerability poses a serious risk that requires immediate addressing. Implementing the proposed measures will significantly reduce the likelihood of similar incidents in the future.

The experimental studies conducted in this chapter demonstrated practical approaches to identifying and analyzing vulnerabilities in network and information systems through the use of a variety of tools and methods for scanning and attacking. Based on the experiments conducted, the following conclusions can be drawn:

1. Scan tool performance:
   - The Discover tool provides a comprehensive analysis of network structures, including identification of open ports, active services, and configuration weaknesses;
2. Social engineering and automation:
   - SEToolkit has shown high effectiveness in simulating social engineering-based attacks, including phishing and malicious file creation, which highlights the importance of user awareness.
3. Code injection tests:
   - In PHP Code Injection and OS Command Injection, experiments have shown that incorrect input validation allows malicious code to be executed on servers;
   - SQL Injection demonstrates the possibility of extracting sensitive information from databases, highlighting the need for parameterized queries and other security mechanisms.
4. Vulnerability tests in CMS platforms:
   - Exploit tests targeting Drupal have confirmed that outdated versions of the software can be compromised through specific exploits, highlighting the importance of regular updates.
5. File structure manipulations:

- Directory Traversal experiments revealed that poorly configured file systems allow access to sensitive data outside of permitted directories.

6. Cryptographic Manipulations:
   - Data decoding and manipulation with Base64 highlighted the importance of proper data encryption to prevent unauthorized actions.
7. Cross-site attacks:
   - Cross-Site Scripting (XSS) experiments identified vulnerabilities that allowed attackers to insert and execute scripts in users' browsers, highlighting the importance of input filtering.
8. Search for actions and automated tests:
   - Tools like Action Search and Testwane have shown the potential for automated security testing and assessment, reducing the time to identify vulnerabilities.

Experimental research shows that vulnerabilities often arise from a combination of technical and organizational shortcomings. The tools and methods used in this chapter have proven their usefulness in identifying weaknesses, which is critical for increasing the level of information security. It has been found that effective protection requires an integrated approach that includes regular testing, software updates, strict input control, and staff training.

CHAPTER 4. EXPERIMENTAL RESEARCH

In the fourth chapter of the dissertation, methods for checking and eliminating gaps leading to potential unauthorized access by third parties are studied and presented, in order to reduce attacks and improve security. Simulation models in the Matlab environment are presented in the context of information security. Results from simulation of attacks on a server, a firewall for filtering attacking traffic, encryption and decryption of data to ensure secure exchange of information, etc. are presented.

4.1.Modeling AES encryption in MATLAB

The cryptographic algorithm (AES) is widely used, which provides reliable and effective data protection. In the MATLAB environment, the AES algorithm can be modeled to study its stages, efficiency and resistance against cryptographic attacks. In this part of the thesis, modeling of AES encryption in MATLAB is presented, with a focus on the simulation of basic operations and analysis of the results.

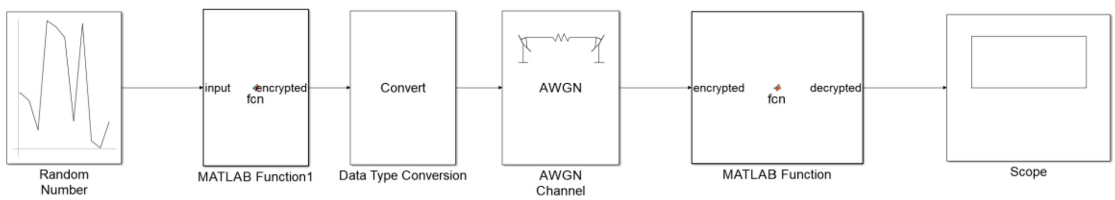
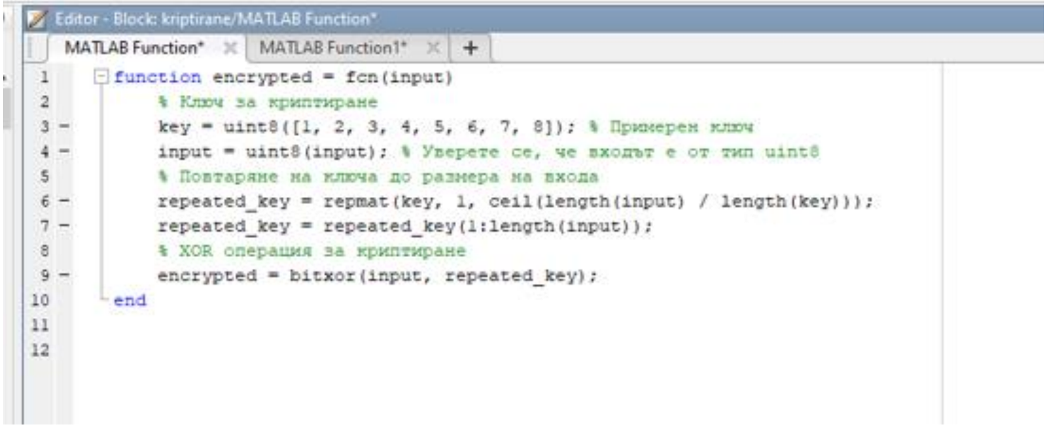


Fig. 4.1. *Simulation model of AES encryption*

Figure 4.1 presents a simulation model for implementing XOR encryption of an input signal and performing subsequent processing via a data stream. The simulation model consists of the following blocks:

- Random Number – used to generate a sequence of random data streams;
- Encrypting Matlab Function 1 - a block containing encryption code written in the Matlab development environment;
- Data Type Conversion - the block serves to unify the data types of the relevant signals used in the model. This way, the possibility of errors is avoided;
- AWGN Channel - the block is important in the simulation model designed in this way, because it provides the opportunity to implement a real communication channel environment by adding additive white Gaussian noise;
- Decryption block Matlab Function - which contains decryption code written in the Matlab development environment;
- Scope block in Matlab - for real-time signal visualization.




```matlab
function encrypted = fcn(input)
    % Ключ за криптиране
    key = uint8([1, 2, 3, 4, 5, 6, 7, 8]); % Примерен ключ
    input = uint8(input); % Уверете се, че входът е от тип uint8
    % Повтаряне на ключа до размера на входа
    repeated_key = repmat(key, 1, ceil(length(input) / length(key)));
    repeated_key = repeated_key(1:length(input));
    % XOR операция за криптиране
    encrypted = bitxor(input, repeated_key);
end
```

Fig.4.2. *Encryption code*

Figure 4.2 shows a MATLAB function that uses XOR encryption to process input data. The code takes an input vector, applies bitwise XOR encryption with a given key, and returns the encrypted result.

1. Function definition:
   - We define a function named fcn that accepts one input argument input (the text to encrypt) and returns the encrypted text encrypted.
2. Defining the encryption key:
   - Specifies a symmetric encryption key, which is a vector of uint8 numbers (8-bit integers);
   - The vector [1, 2, 3, 4, 5, 6, 7, 8] represents an example key.

3. Input conversion:

- Converts the input text to type uint8. This is necessary because the XOR operation works with numeric data, and text data is converted to numbers using the ASCII character codes.

4. Repeat key:
   - The repmat function repeats the key as many times as necessary to cover the length of the input text;
   - ceil(length(input)/length(key)) calculates how many times the key must be repeated to be at least as long as the input.
5. Key abbreviation:
   - repeated_key(1:length(input)) trims the extra characters from the repeated key so that its length exactly matches that of the input text.
6. Encryption via XOR:
   - It uses the XOR operation (bitxor) between each character of the input text and the corresponding character of the repeated key;
   - XOR encryption: If the same key is applied twice, the original text is recovered.

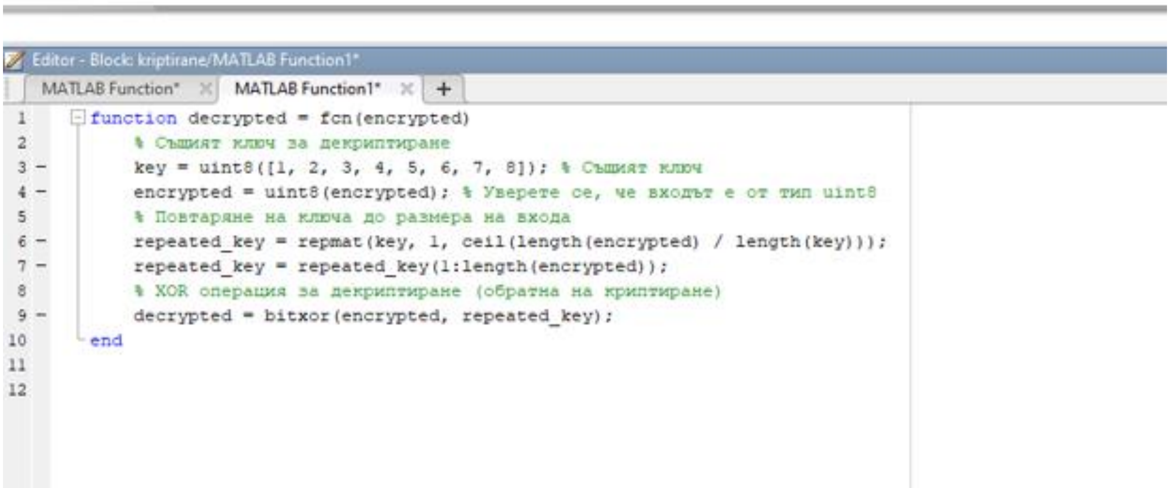


Fig. 4.3. *Decrypt AES_Decrypt*

Figure 4.3 shows a MATLAB function that uses an XOR operation to decrypt encrypted data. The code is identical to the encryption function, which is expected for XOR-based symmetric encryption.

In AES, decryption in MATLAB follows the reverse process of encryption to recover the original text from the ciphertext. The basic operations are performed in reverse order, with each operation having its own inverse version:

Reverse order of circles- Decryption starts with the final encryption round and proceeds to the initial one. This involves using the round keys in reverse order.

Decryption steps:

- *Inverse ShiftRows:*Reverse the rows in the matrix;
- *Inverse SubBytes:*Byte replacement using a reverse S-box;
- *Inverse MixColumns:*Linear transformation that restores the original state of the columns;

- *AddRoundKey: XOR*a ring key operation that restores the original data.
- *Padding*- After decryption, the added padding is removed to restore the original text. This approach ensures correct data recovery, guaranteeing the same security and efficiency as encryption.

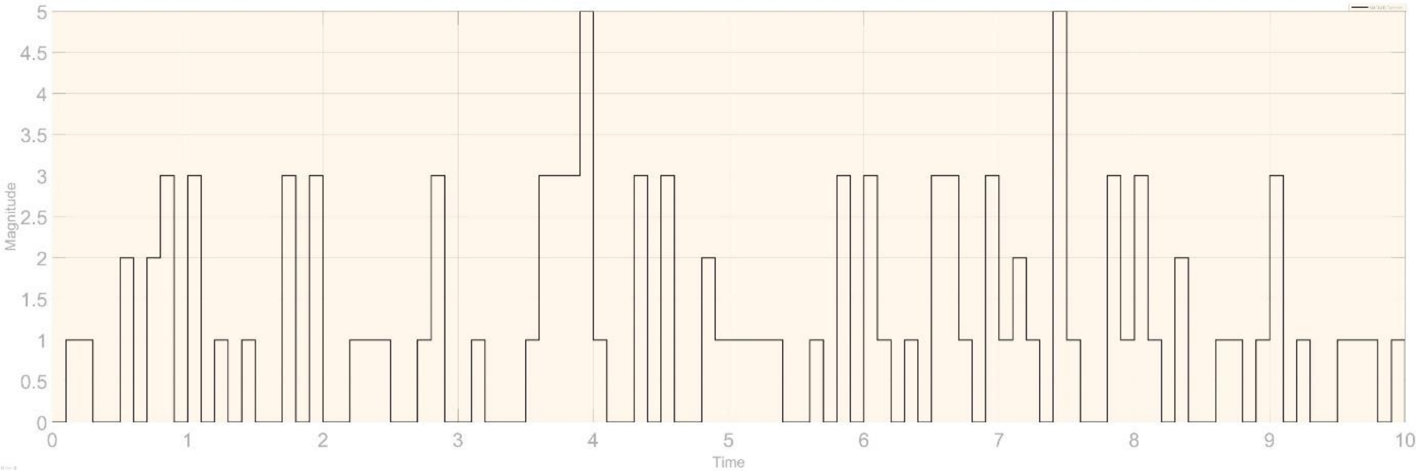


Fig. 4.4. *Data visualization after encryption and decryption*

This figure shows a MATLAB/Simulink Scope plot that visualizes a discrete signal. This signal is an encrypted binary stream obtained by XOR encryption. The plot visualizes the changes in the bits – transitions between 0 and 1, which create a step-like shape. If the same key is applied again to the encrypted signal, the decrypted (original) signal will be obtained.

4.2.Man-in-the-Middle (MITM) attack research

A Man-in-the-Middle (MITM) attack is a scenario in which a malicious actor intercepts, eavesdrops, or manipulates communication between two parties. In MATLAB, such a model can be implemented to simulate the operation of a MITM attack, as well as to explore methods for preventing it.

4.2.1. How MITM works in MATLAB

MITM simulation in MATLAB involves three main components:

Legitimate participants:

- Sender (Client) and recipient (Server) exchange data using symmetric encryption (e.g. AES);
- In this model, the client encrypts the data before sending it, and the server decrypts it upon receipt.

Attacker (MITM):

- The attacker positions himself between the client and the server, intercepting the data;
- It can intercept messages, modify them, or inject them back to the recipient.

Encryption and decryption mechanisms:

- In AES encryption is used to protect data. A MITM attack can be implemented by intercepting and simulating compromise of the encryption key.

4.2.3. Conclusion

Modeling a MITM attack in MATLAB allows understanding the principles of this type of attack and demonstrating the risks to communication security. Furthermore, through extensions such as digital signatures and secure key exchange, MATLAB can also be used to design mechanisms to protect against MITM. This simulation is useful for both educational and research purposes.

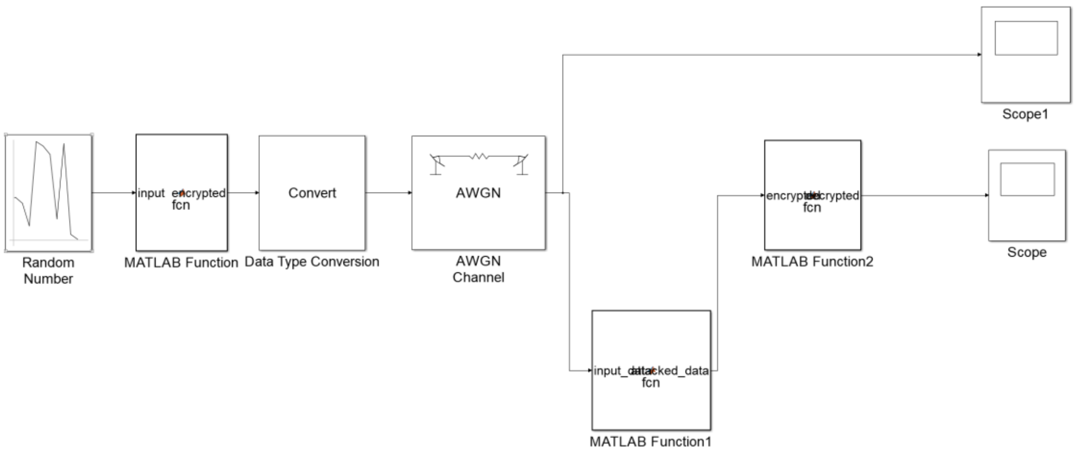


Fig. 4.5. *Simulation model MITM*

Figure 4.5 is an extended version of Figure 4.14, the difference being the addition of the Matlab Function 1 block. In the present context, this block is used to implement a Man-in-the-Middle (MITM) attack. For this purpose, specialized code has been developed in the Matlab programming environment.

4.2.4.Main components of MITM simulation

- The client encrypts a message with AES and sends it to the server.
- The MITM attacker intercepts the encrypted text, decrypts it (if he has the key), modifies the message, and sends it to the server.
- The server decrypts the received message and processes it.
  Working principle
- • Encryption (AES_Encrypt) - The input text is converted into bytes and encrypted using a symmetric key.
- • Decryption (AES_Decrypt) - The encrypted message is decrypted back to the original text or a modified version.
- • Key Expansion - Used to generate ring keys, which is an essential part of the AES algorithm Fig. 4.5.
- Role of MITM
- The MITM attacker:
- • Intercepts the encrypted text between the client and the server;

- • If he has access to the key, decrypts the message;
- • Modify the message and encrypt it again before sending it to the server.

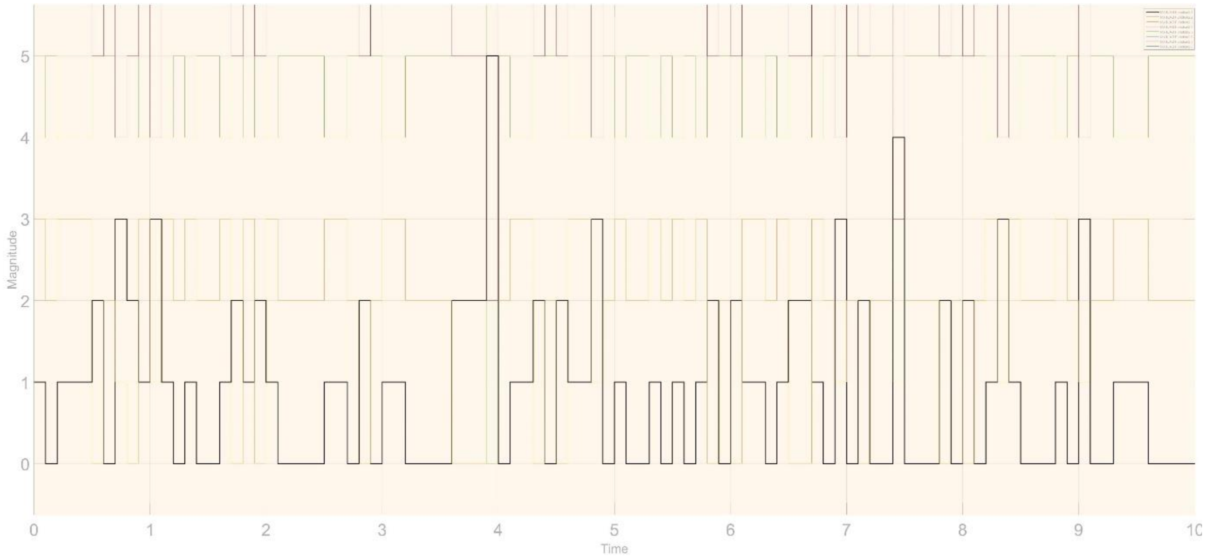


Fig.4.6. Data visualization with MIMT

Conclusion

The Man-in-the-Middle attack demonstrates the need for stronger defenses, such as:

1. *Two-factor authentication:*To ensure the identity of the parties.
2. *Digital signatures:*To verify the integrity and authenticity of the message.
3. *Secure protocols:*TLS/SSL for communication encryption.

This MATLAB study illustrates the basic mechanism of a MITM attack and how compromised keys or lack of protection can lead to serious security breaches.

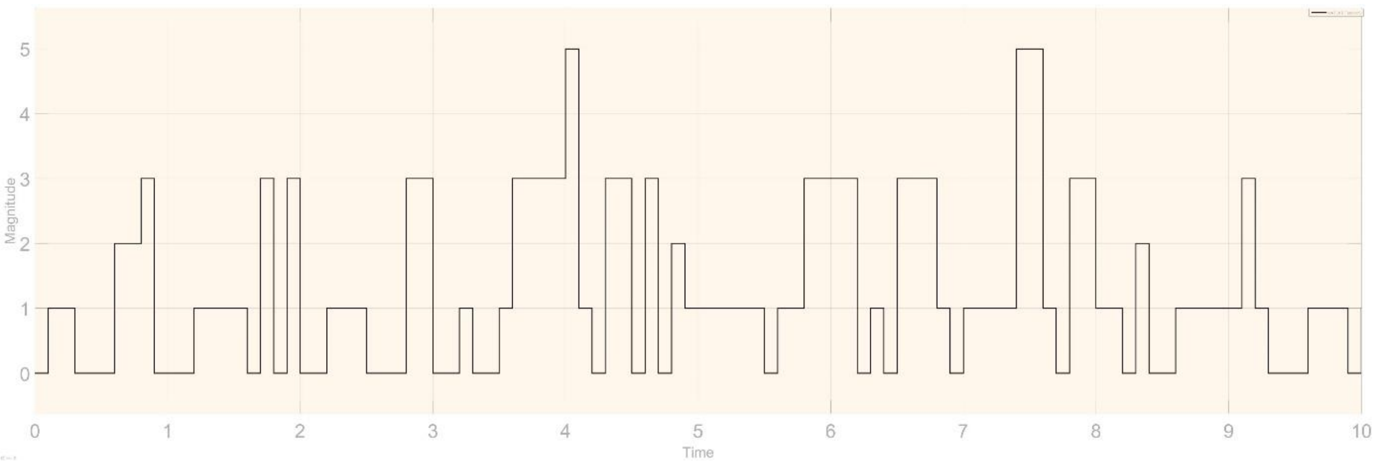


Fig. 4.10.*Compromised data latency and repetition*

The results shown in Fig. 4.10 from the Scope of Matlab Simulink represent a signal processed in the context of the simulation after a Replay and Delay attack. The incorrect values and periodic deviations in the signal are the result of the playback and delay of the uncompromised signal, which confirms the impact of the attack.

4.3. A model for simulating a DoS attack on an information system.

A model for simulating a Denial of Service (DoS) attack is presented. The goal is to make an information system, service, or network inaccessible to legitimate users by overloading it with unnecessary requests or blocking access to resources. MATLAB is used to model and simulate DoS attacks in order to analyze their impact on systems.

Figure 4.12 presents different types of attacks on a server, represented as traffic volume (packets/second) versus time (seconds). DoS attacks in the red line have the highest traffic volume, simulating server overload. Brute Force attack – green line has a constant stream of packets, representing attempts to guess passwords or other data. In the Mawlare attack blue line – has a higher traffic volume simulating the distribution of malware.

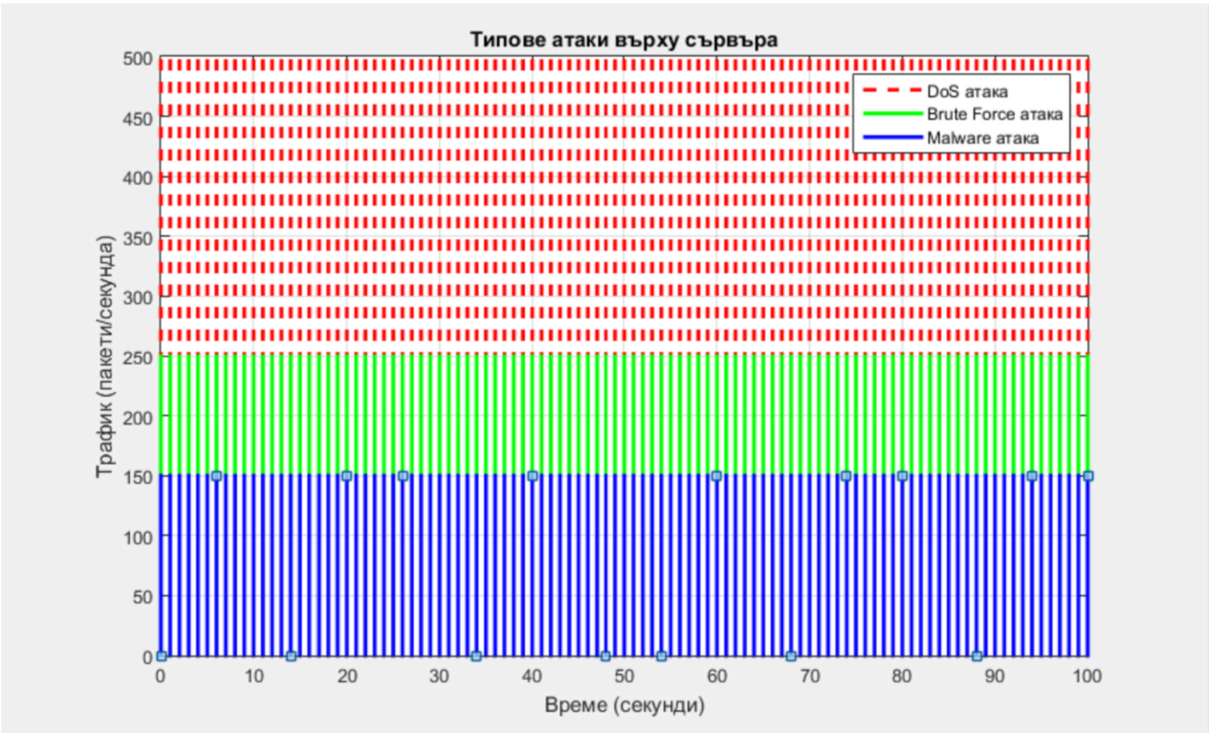


Fig. 4.12. *Exploring attack types in Matlab*

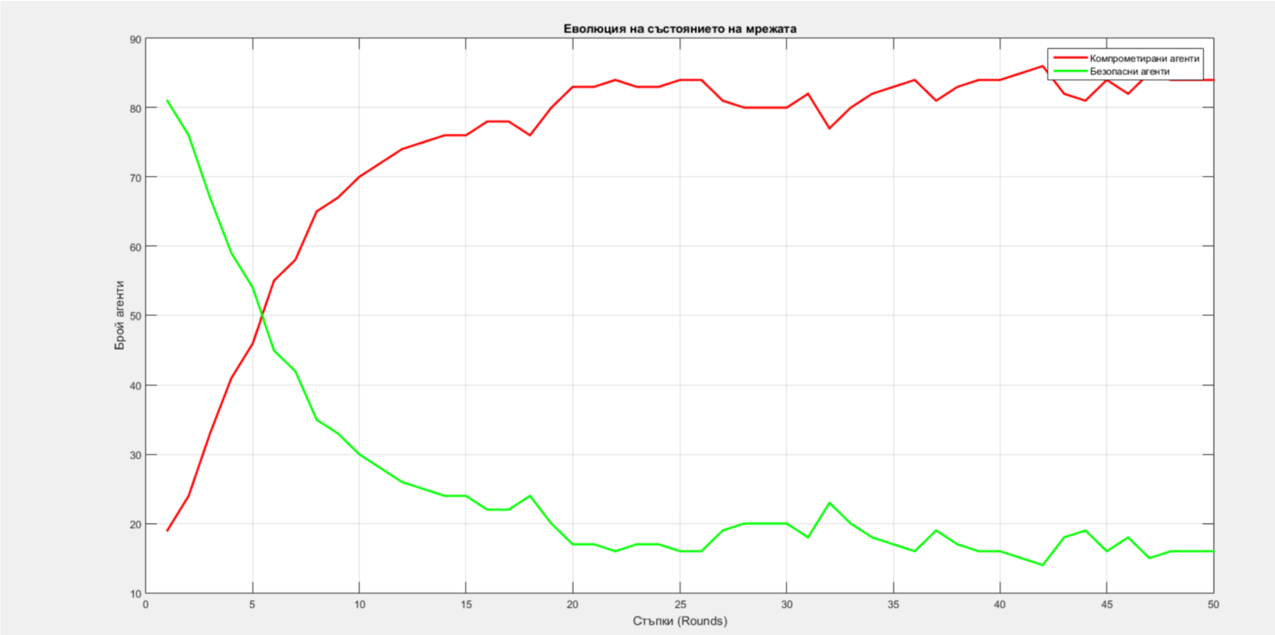


Fig.4.19. *Network evolution graph*

The graph in Fig. 4.19 illustrates the evolution of the network state over the course of 50 simulation steps. The red line shows the increase in compromised agents as the steps progress. At the beginning, the compromised agents are few, but over time their number increases significantly. The green line represents the decrease in safe agents, which mirrors the increase in compromised ones. The graph highlights the effectiveness of attackers in compromising the network, with defenders managing to maintain a certain balance only in the initial steps.

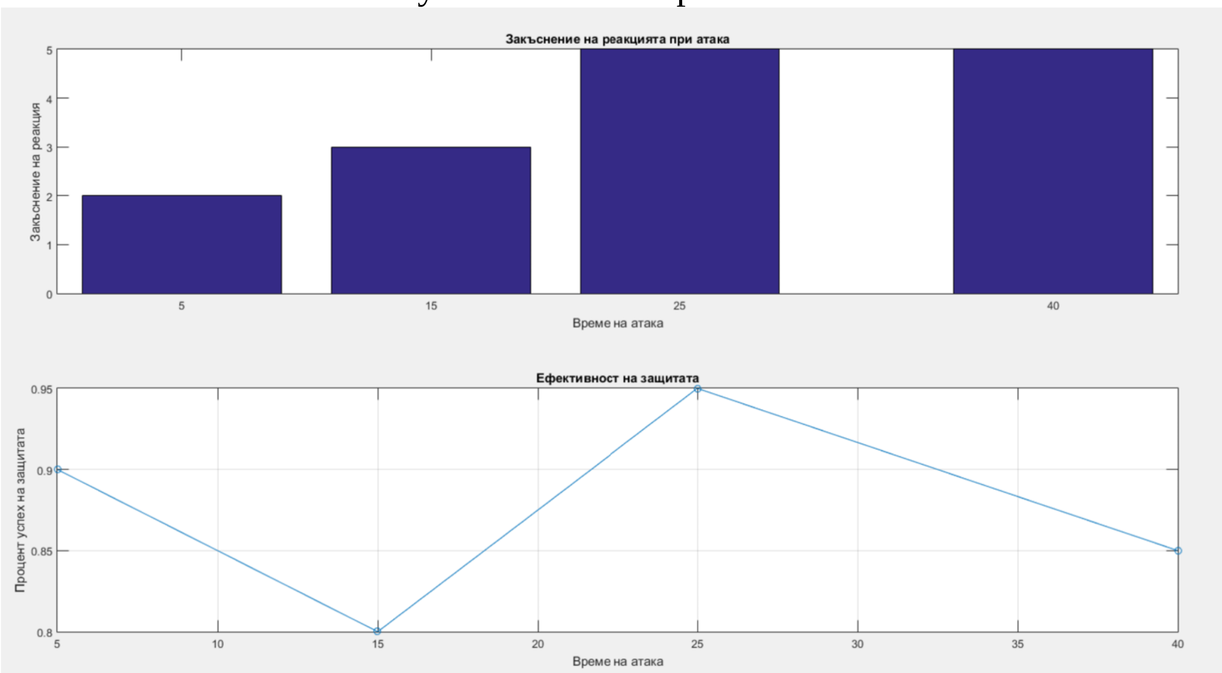


Fig.4.21. *Sustainability analysis*

Figure 4.21 illustrates two different dependencies related to attack protection:

- The attack response delay graph plots attack time on the x-axis against response delay on the y-axis. As time progresses, the response delay increases;
- The Defense Efficiency graph illustrates the defense percentage over time. There is a noticeable drop in efficiency at the beginning followed by an improvement in the 25th attack, after which the efficiency decreases again.

4.4.Researching Replay and Delay attacks in MATLAB

In the research of Replay and Delay attacks, it was found that these are types of network security threats in which valid messages between two participants are intercepted, repeated or delayed by a third malicious "participant". A simulation of these attacks is presented, which allows their study and testing of protective mechanisms Fig. 4.7.

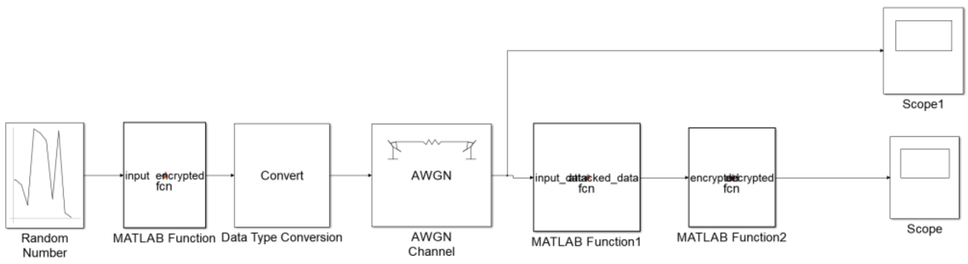


Fig. 4.7.*Block diagram of Replay and Delay attack*

The study presented in Fig. 4.7 is based on the blocks used in the previous two studies with the only difference that a programmable Matlab Function 1 block has been added. This block performs software simulation of the Replay and Delay attacks Fig. 4.8. The code implemented in it simulates repetition and delay of transmitted data in the time domain.

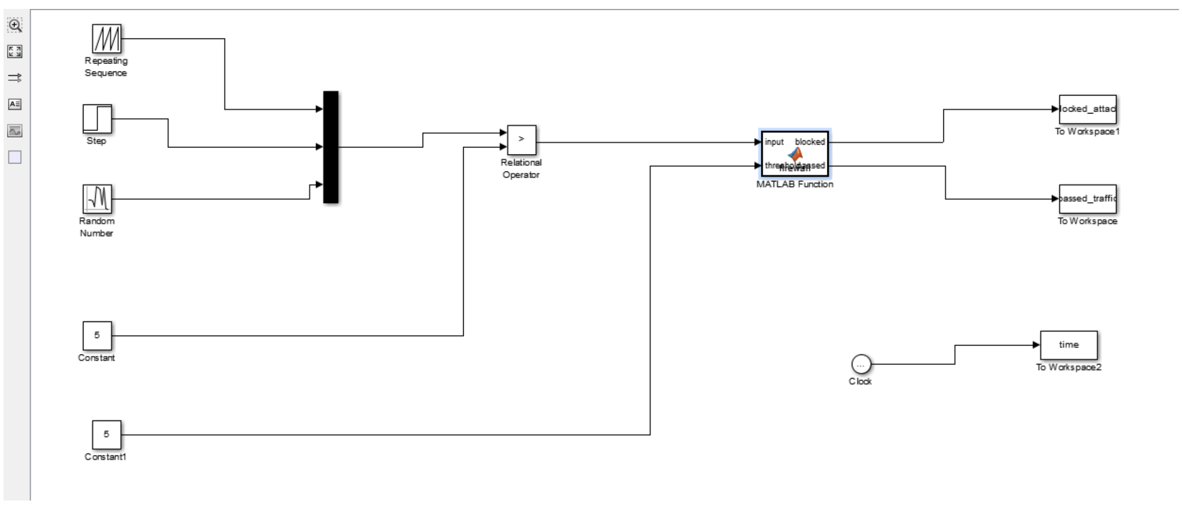


Fig. 4.22.*Simulation model and final decision-making process of a security system*

4.5.Main modules used in the simulation:

The graph represents the system behavior, showing the number of allowed and blocked packets over time;

The red line (Blocked Packets) - represents packets blocked due to violation of firewall policies;

The green line (Allowed Packets) - Represents the allowed packets that have passed the firewall;

In time ranges around 3-4 seconds, activity related to packet blocking is seen as a reaction to an attack.

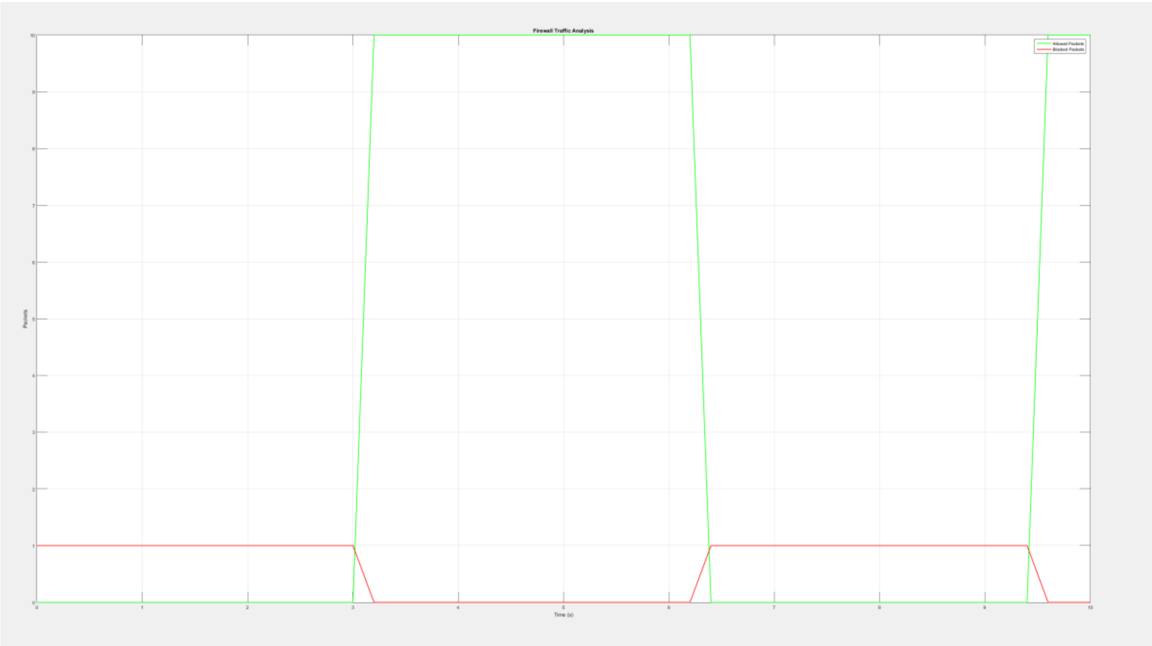


Fig. 4.25.*Graphical visualization of results*

The graph represents the system behavior, showing the number of allowed and blocked packets over time;

The red line (Blocked Packets) - represents packets blocked due to violation of firewall policies;

The green line (Allowed Packets) - Represents the allowed packets that have passed the firewall;

In time ranges around 3-4 seconds, activity related to packet blocking is seen as a reaction to an attack.

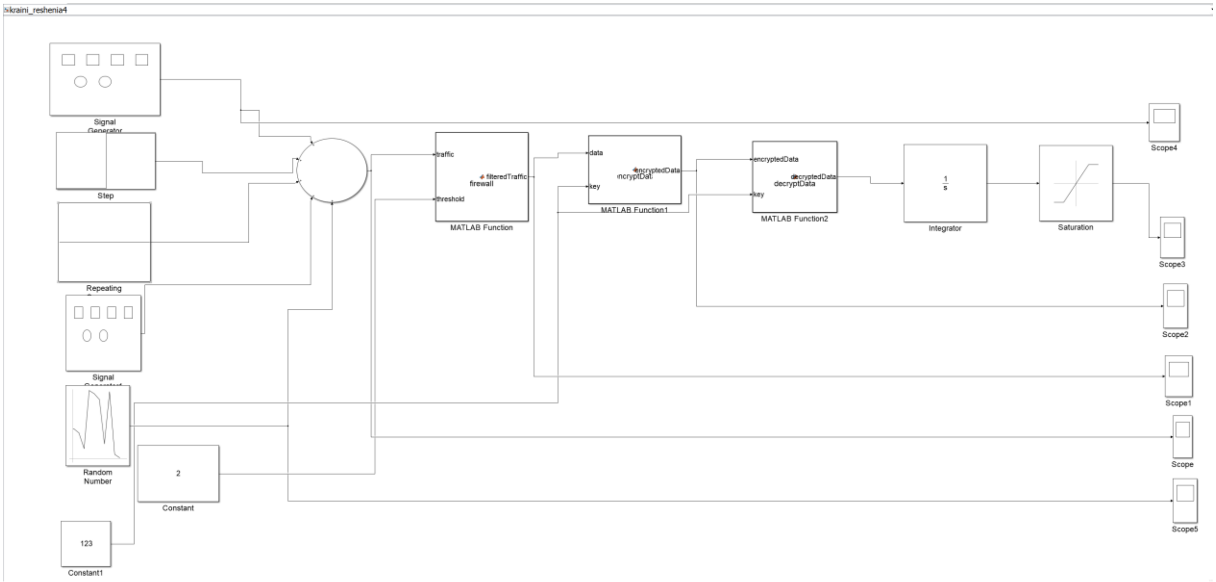


Fig. 4.26.*Server attack simulation model*

The model includes simulation of attacks on a server, a firewall to filter attacking traffic, and data encryption and decryption to ensure secure information exchange.

Components of the model are: traffic generation - normal and attack traffic.

Firewall - detects and blocks attacking traffic.

Encryption and decryption - simulates secure data exchange between client and server.

Server system - processes only normal (filtered) traffic.

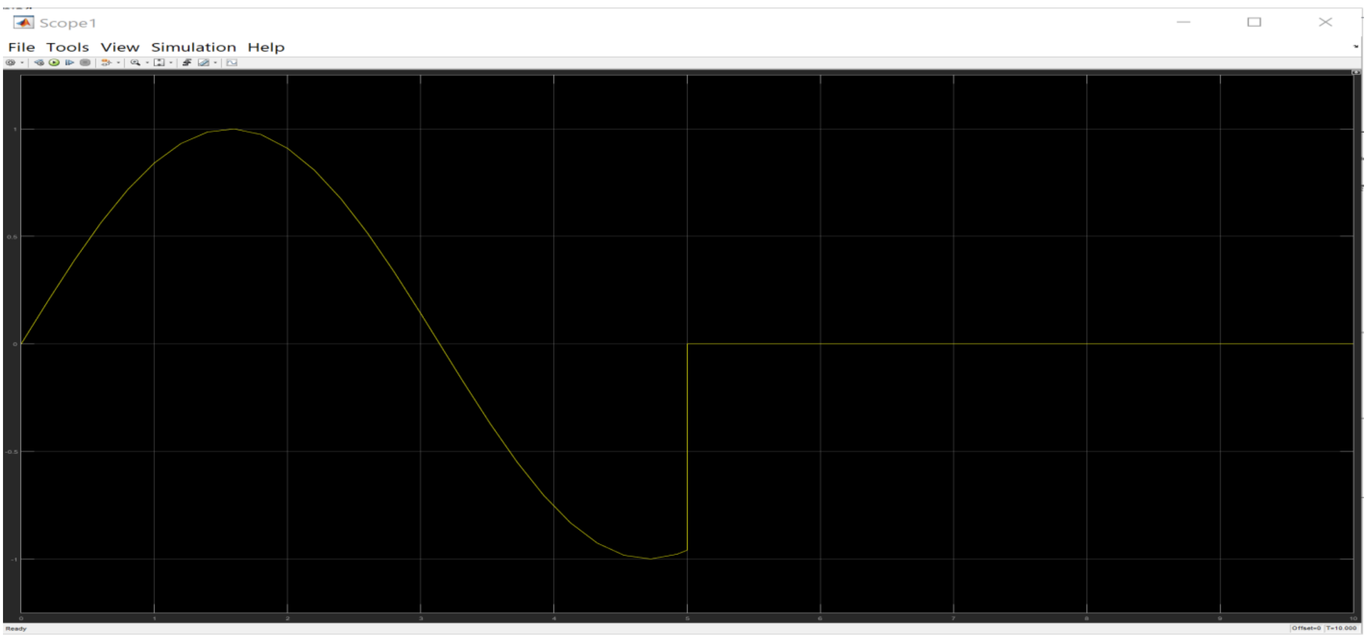


Fig. 4.27.*Incoming combined traffic (outgoing from Sum Block)*

From step 0 to step 5 the signal has a sinusoidal shape, which represents normal traffic to the server. It is visible that the signal decreases and reaches a negative value, which indicates an increase in the attacking traffic. When the threshold (set in the firewall) is reached, the signal abruptly changes to a constant value, as a result of the attack being blocked by the firewall.

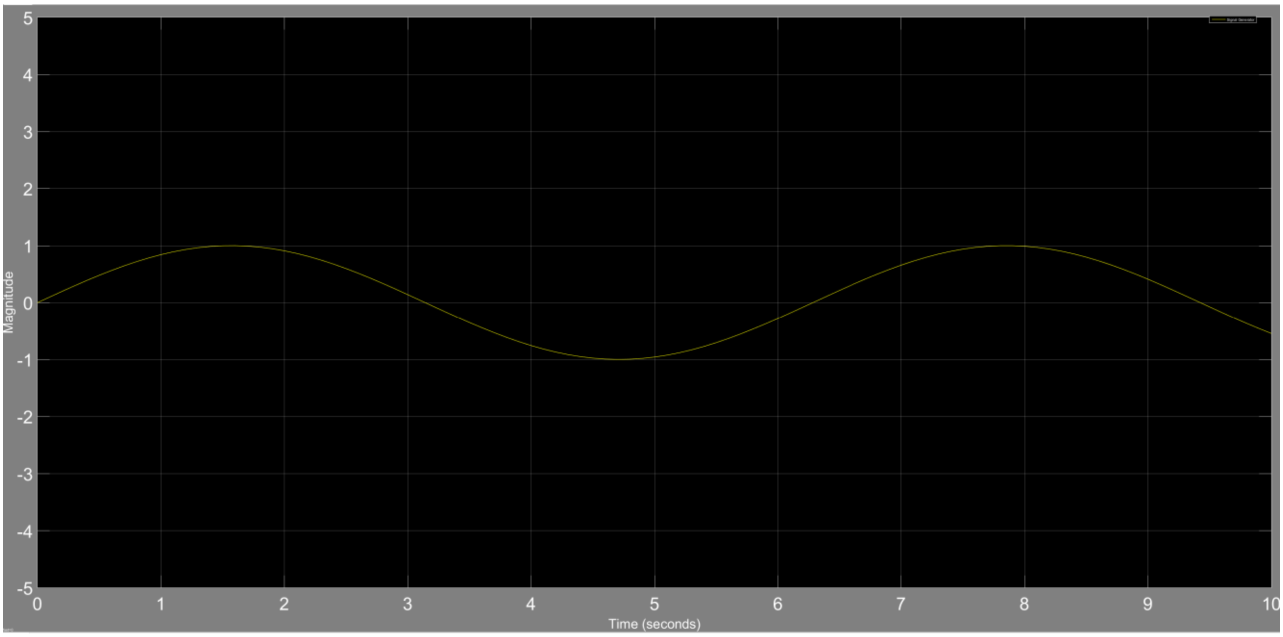


Fig. 4.28.*Network traffic*

Normal network traffic - This is a reference signal that shows standard communication with the server before the attack begins.

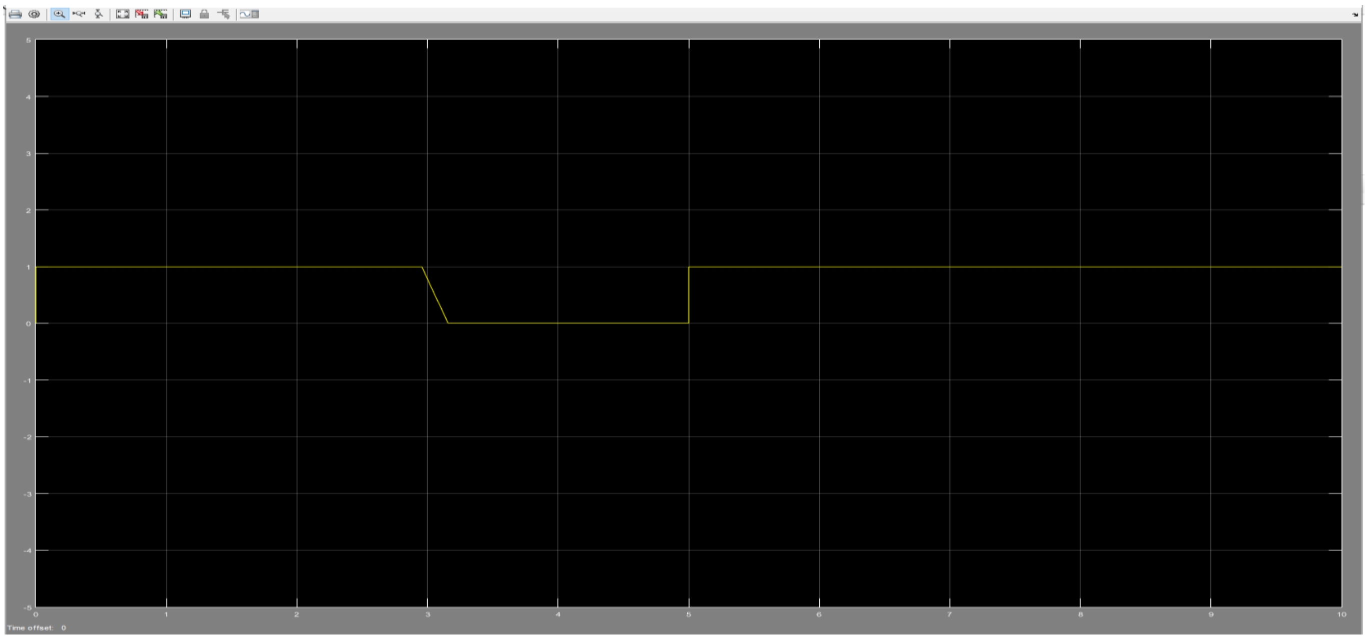


Fig. 4.29.*Firewall filtered and blocked traffic*

The graph shows that at the beginning the signal is stable at one level, which means normal network functioning. From the 3rd to the 5th period there is a sharp drop, which represents an attack detection. The firewall detects suspicious activity and takes action.

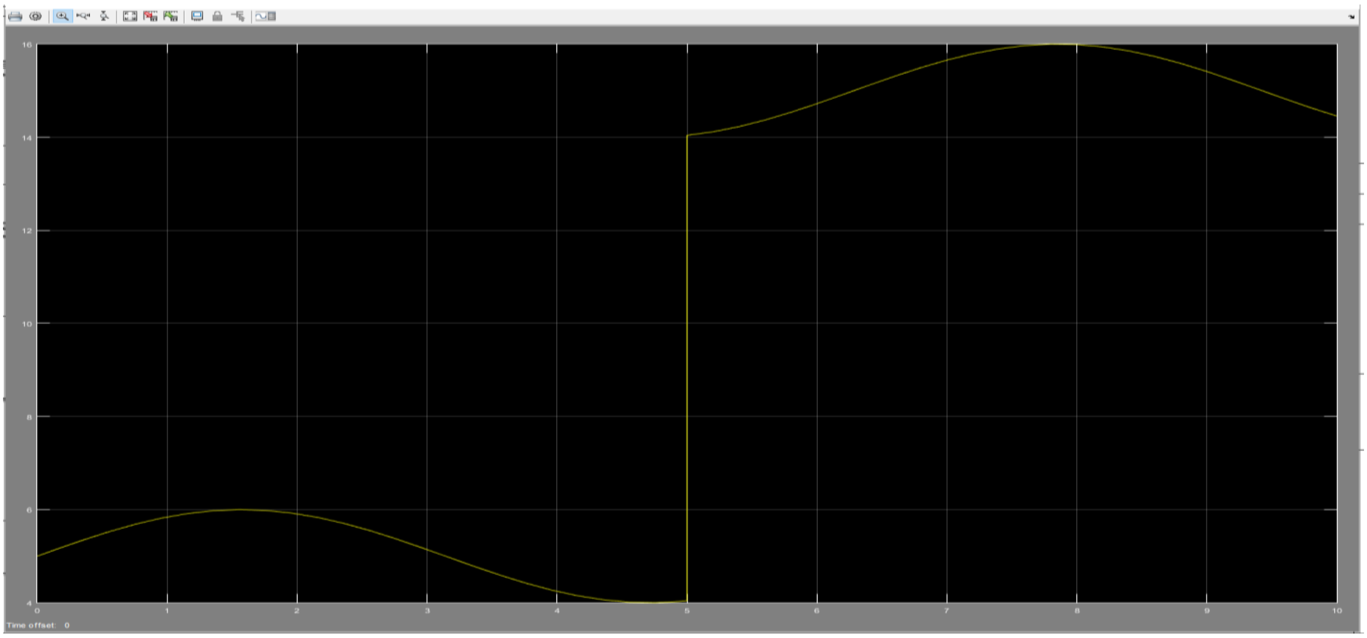


Fig. 4.30.*Server traffic analysis.*

From the graph in Fig. 4.30 it is seen that at the beginning the signal has a sinusoidal shape, which represents normal traffic to the server. At a certain point (around the 5th second) there is a sharp jump, after which the signal continues as a sinusoid, but with a higher amplitude. This behavior is caused by filtration and reaction – at the beginning there is a traffic limit, but after the firewall recognizes safe requests, the traffic increases.

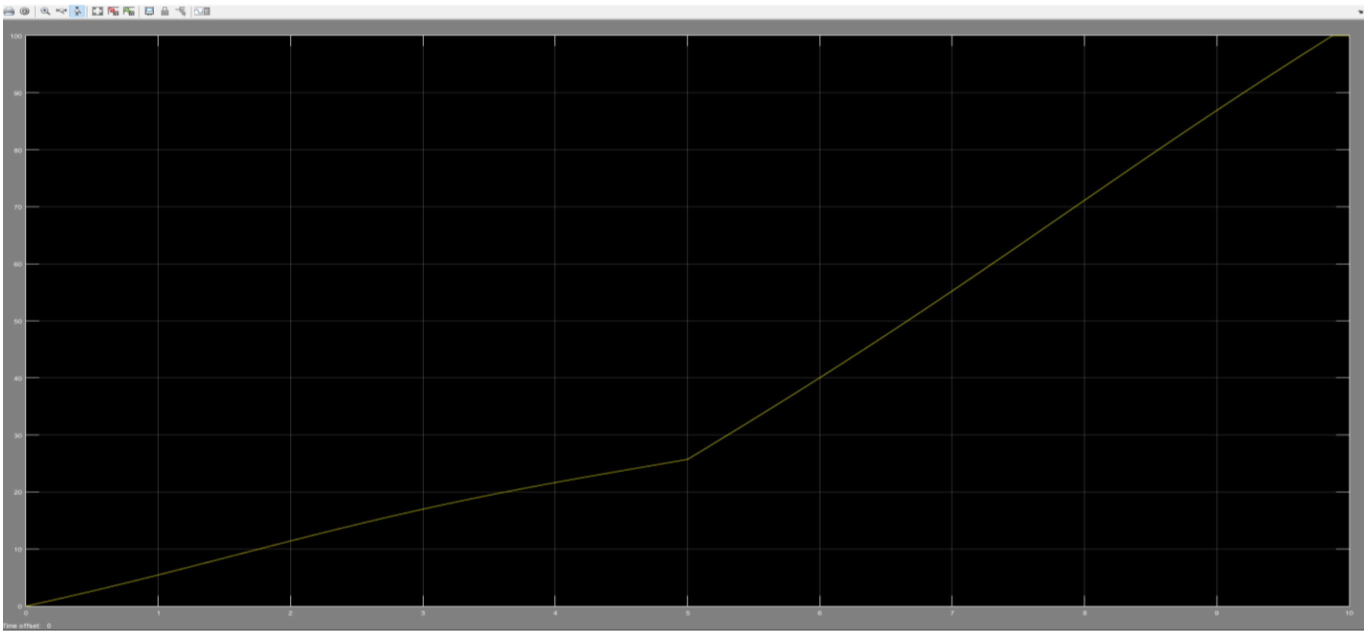


Fig. 4.30.*Server traffic analysis.*

Fig. 4.31. shows the graph, which has a linear growth due to resource accumulation, such as blocked packets - the firewall blocks traffic, due to the counter of rejected requests. A change in the slope around the 5th second is a result of blocked traffic by the firewall.

The simulation demonstrates that properly configured firewalls can provide effective protection against attacks. Such simulations can be used to develop adaptive security mechanisms that automatically adjust their parameters based on the characteristics of network traffic.

Conclusions

The study of network information systems in the context of their security has revealed a number of key aspects that determine the effectiveness of protection against modern threats. The main conclusions that can be drawn based on the research and analysis are the following:

1. Modeling AES encryption in MATLAB provides a deep understanding of the algorithm and its stages. This implementation can be used to perform security research, optimization, and analysis. MATLAB offers a powerful platform for designing and testing cryptographic algorithms, making it a valuable tool for training and research in the field of cybersecurity.
2. Vulnerability identification: Analysis has shown that a significant percentage of vulnerabilities in network systems stem from incorrect configuration, outdated software, or insufficient protection of devices connected to the network.
3. Research has shown that DoS attacks affect the availability of information systems. To reduce the effects of DoS attacks, it is necessary to implement:
   - Mechanisms for detecting DoS attacks.
   - Security systems (e.g. Firewall and Rate Limiting).
   - Load-balanced architectures.
4. The Monte Carlo method is extremely useful for modeling probabilities in the context of information security. Through simulations, we can understand how different factors (such as password length or character set) affect the probability of a successful attack. MATLAB offers a convenient way to implement these simulations, while also allowing us to visualize the results through graphs.
5. Methods for analyzing simulation results include a combination of statistical, graphical, and comparative approaches. They allow for:
   - Identification of weaknesses;
   - Optimization of strategies;
   - Better understanding of complex system behavior;
   - Appropriate analysis is crucial to extracting value from simulations and making informed decisions about system security.

6. The Agent-Based Model in the context of information security provides a useful understanding of the dynamics of attacks and defenses in network environments. Through the study in MATLAB and the presented graphs, we can observe how agents with different roles interact with each other and how these interactions affect the state of the network over time.

In summary, network information system security requires a holistic and systematic approach that integrates technology, procedures, and governance. The study highlights the need for continuous adaptation of security measures to evolving threats, as well as the importance of training and awareness for all participants in the network ecosystem.

CONCLUSION

This dissertation examines various aspects of information security through theoretical and practical research, with an emphasis on analyses, simulations, and experiments aimed at identifying and overcoming vulnerabilities.

The first chapter of the dissertation provides an overview of cyberattacks that directly correspond to the topic of the dissertation.

The literature review highlights the increasing complexity and diversity of computer threats, which include malware and vulnerabilities in traditional network and information systems. Effective protection requires an integrated approach combining technical, organizational and legal measures.

An information security model is presented. Information is classified with an emphasis on security management and the most common incidents. Attention is paid to the standards for information security management systems. Various security procedures are presented. The types of attacks are emphasized and examined with an emphasis on building a model for simulations and final solutions in security systems. Based on the literature review, it is established that modern computer threats are multifaceted, with their diversity and complexity growing proportionally with the progress of technologies.

Based on the literature review, the goal and objectives of the dissertation work have been formulated.

In the second chapter of the dissertation, the main methods and approaches for encrypting information are studied. Particular attention is paid to the presentation of schemes for the operation of encryption algorithms, with the emphasis placed on the key problem of ensuring information protection. The different types of encryption, their characteristics in terms of speed and security, as well as the modern challenges associated with these aspects are considered. The focus is on the encryption/decryption process, which is based on a mathematical method known as an encryption algorithm. In this context, it is emphasized that the source information is usually called plain text, regardless of whether it refers to text or non-text messages. Asymmetric cryptographic algorithms, their principle of operation and their application are presented. It is concluded that modern systems often combine symmetric and asymmetric cryptography to cope with the challenges of cybersecurity. The principle of operation of AES is studied, the main factors influencing their operation are given. The research found that in symmetric encryption, the sender and recipient must have a common shared secret key, which they exchange before starting the communication. Figure 2.9 examines and presents the results of the 256-bit encryption process using the SHA (Secure Hash Algorithm) hashing function. Figure 2.10 examines and presents the results of the integration of a string function in the data processing process. The addition of the string function aims to improve the processing of text values, providing additional capabilities for data manipulation and transformation. The integration, research and analysis of the results show that the addition of the string function allows for more efficient work with text data and improves the overall reliability of the system. Figure 2.11 examines and analyzes the results of the tests conducted using the AES symmetric encryption algorithm.

The research found that AES provides a high level of security and performance, with an increase in encryption/decryption time with increasing key length. This confirms the balance between security and efficiency of the algorithm, which makes it suitable for a wide range of applications.

Figure 2.12 presents the results of combining the cryptographic algorithm AES and the hash function SHA with additional processing of text data. This study aims to analyze the impact of adding text on the performance and security of the system.

From the research and analysis of the results, it becomes clear that adding text to the input data, before its hashing and encryption, shows a positive effect on security by increasing the complexity of attacks.

Figure 2.14 shows the process of hash cracking using a hash cracker. This process is used to convert a hash to the original password using techniques such as brute-force attacks.

In summary, the simulation analysis and the study of cryptographic models have proven that the combined approach between traditional and innovative methods is essential for building secure information systems. Theoretical developments and simulation results can serve as a basis for further improvement of cryptographic technologies and their application in the conditions of dynamically changing cyber environment.

Chapter 3 of the dissertation covers in detail the research on various vulnerabilities and tools used in the field of information security. The content is structured into several main sections that consider experimental research, analysis, and recommendations for preventing cyberattacks.

A study of a network information system using the TCP SYN option was conducted. It was found that the use of SYN scanning in networks with complex security mechanisms can provide valuable security information by identifying active services and potential vulnerabilities. It was concluded that scanning filtered ports highlights the complexity of network analysis in the presence of security mechanisms or unstable networks. A study of UDP scanning was conducted. For the purpose of the study, UDP scanning was used, which is a tool for identifying open ports and services using the UDP protocol.

The applications, features and capabilities of the Discover tool for identifying vulnerabilities are examined. Potential countermeasures when using it are also studied. An analysis of phishing attacks carried out using SEToolkit is presented, with an emphasis on the way the tool works and an assessment of its effectiveness. An analysis of vulnerabilities related to PHP Code Injection and the protective mechanisms that can prevent such attacks is made. Different types of SQL injections and their features are studied. Effective measures for protection against this type of attack are also described, which is supported by visualizations and analysis of the results. An analysis of the exploitation of specific vulnerabilities in the Drupal platform is presented. Visualizations of SQL injections and recommended measures for their prevention are discussed. Base64 encoding and its potential vulnerabilities when used are studied and analyzed. XSS vulnerabilities, their nature, attack mechanisms, potential consequences and effective countermeasures are studied.

Chapter 3 concludes with an analysis of the research results, highlighting the effectiveness of the methods examined and recommending practical measures to enhance security.

This overview demonstrates a comprehensive and systematic approach to researching vulnerabilities and protection in information systems.

In the fourth chapter of the dissertation, methods for checking and removing gaps leading to potential unauthorized access by third parties are researched and presented, with the aim of reducing attacks and improving security.

AES encryption has been modeled in the MATLAB environment. The AES model in MATLAB simulates the encryption and decryption of data, including all the main stages of the algorithm. The encryption code from the AES encryption study is presented. A Man-in-the-Middle attack has been studied, a scenario in which a malicious participant intercepts, eavesdrops or manipulates communication between two parties. A study of Replay and Delay attacks in MATLAB has been carried out. For the purpose of the study of Replay and Delay attacks, it was found that these are types of threats in network security, in which valid messages between two participants are intercepted, repeated or delayed by a third malicious participant. A model for simulating a DoS attack on an information system is presented. The DoS attack simulation model aims to make an information system, service or network inaccessible to legitimate users by overloading it with unnecessary requests or blocking access to resources. The source code of the model is given.

A study of different types of attacks has been carried out in the Matlab environment. The results are presented graphically and a part of the source code is given. A simulation of the probability of a successful attack on a system using the Monte Carlo method has been made and studied. The results are depicted graphically in order to analyze the behavior of the attacks and defenses.

Guidelines for the development of research in this area

1. It is necessary to implement new practices for monitoring network requests for the purpose of early detection of vulnerabilities.
2. It was found that vulnerabilities were identified in outdated versions of Drupal, including SQL Injection capabilities, leading to the development of update and security recommendations.
3. The shortcomings of Base64 as a cryptographic method and the need to develop guidelines for using more efficient algorithms are demonstrated.

4. Using MATLAB to visualize processes such as network attacks, encryption, and decryption will allow for an intuitive understanding of complex processes in the field of cybersecurity.

CONTRIBUTIONS OF THE DISSERTATION

1. Scientific Scientifically applied contributions

1.1. Researched, systematized and analyzed existing methods, techniques and tools for scanning network systems and their application in identifying vulnerabilities.
1.2. AES modeling was performed in MATLAB to test the algorithm as well as to understand its key operations, which demonstrate the algorithm's resilience against attacks.
1.3. Simulation models have been developed for the analysis of DoS, Replay, Delay and MITM attacks, which demonstrate the impact of these threats on information systems.
1.4. The Monte Carlo method in MATLAB was studied, applied to estimate the probability of successful attacks on passwords, providing a quantitative assessment of the risks.
1.5. Agent-based models for the dynamics between attacking and defending agents have been simulated and studied, allowing for the investigation of the effectiveness of different defense strategies.

2. Applied contributions:

2.1. MATLAB simulations have been developed and performed that can be used to train cybersecurity specialists, as well as to test new protection mechanisms.
2.2. Methods and simulations are presented that can be adapted for analysis and protection of network systems in corporate and institutional environments.
2.3. A structured reconnaissance process has been created that significantly speeds up the identification of vulnerabilities in complex systems.
2.4. Methods have been created to protect against SQL Injection, PHP Code Injection and OS Command Injection, based on validation analysis, parameterized queries and privilege minimization.
2.5. Practical data on the impact of DoS and other attacks on network performance has been studied, which helps optimize security solutions.

LIST OF RELATED PUBLICATIONS THE DISSERTATION THESIS

1. **Ivaylo Uzunov.**Problems and solutions related to the consequences of cyberattacks. Third National Scientific Conference “Man and the Universe”, Union of Scientists in Bulgaria – Smolyan, November 25–26, 2021, Scientific Papers, Volume III, Part 3, pp. 637 – 646, ISSN:1314-9490 (online).
2. **Ivaylo Uzunov**, Slavi Lyubomirov. (2022) Research on Network Information Systems in Terms of Security, Proceedings of the National Scientific Conference with International Participation on the topic "Education, Science, Society" November 3-4, 2022, ISBN 978-619-7663-43-3 (online), pp. 950-961.
3. **Ivaylo Uzunov,**Slavi Lyubomirov. (2022) Simulation analysis and research of cryptographic models in security systems, Proceedings of the national scientific conference with international participation on the topic "Education, Science, Society" November 3-4, 2022, ISBN 978-619-7663-43-3 (online), pp. 938-948.
4. **Uzunov, I.**and Lyubomirov, S. (2023) Networked information systems research on security in engineering education, 17th International Technology, Education and Development Conference, INTED2023 Proceedings, Valencia, Spain, ISBN: 978-84-09-49026-4, ISSN: 2340-1079, Pages:5589-5598, doi:10.21125/inted.2023.1462.
5. **Uzunov, I.**and Lyubomirov, S. (2023) Analysis and research of cryptographic models to ensure information security in engineering education, 17th International Technology, Education and Development Conference, INTED2023 Proceedings, Valencia, Spain, ISBN: 978-84-09-49026-4, ISSN: 2340-1079, Pages:5578-5583, doi: 10.21125/inted.2023.1459.