ПЛОВДИВСКИ УНИВЕРСИТЕТ
„ПАИСИЙ ХИЛЕНДАРСКИ“

маг. инж. Ивайло Детелинов Узунов

МОДЕЛ ЗА СИМУЛАЦИЯ И КРАЙНИ РЕШЕНИЯ НА СИСТЕМИТЕ ЗА СИГУРНОСТ

АВТОРЕФЕРАТ

на дисертация за придобиване на образователна и научна степен
“**ДОКТОР**”

Област на висше образование:
5. Технически науки

Професионално направление:
5.3. „Комуникационна и компютърна техника“

Докторска програма:
„Автоматизация на области от нематериалната сфера
(медицина, просвета, наука, административна дейност и др.)“

Научен ръководител:
проф. д-р инж. Слави Ясенов Любомиров

Пловдив, 2025 г.

Дисертационният труд е с обем 176 страници , включително 61 фигури, 3 таблици, оформени в увод, 4 глави, общи изводи, научно-приложни и приложни приноси, списък с използваните термини и съкращения, списък с публикациите на автора. Списъкът на цитираната литература включва 143 заглавия. Приложение 1

Означенията на формулите, фигурите и таблиците в автореферата съвпадат с тези в дисертационния труд.

Дисертационният труд е обсъден и насочен за защита на заседание на катедрен съвет на катедра „ЕЛЕКТРОНИКА, КОМУНИКАЦИИ И ИНФОРМАЦИОННИ ТЕХНОЛОГИИ“ при ПЛОВДИВСКИ УНИВЕРСИТЕТ „ПАИСИЙ ХИЛЕНДАРСКИ“ на 13.02.2025 г.

Защитата на дисертационния труд ще се състои на 14.05.2025 г. от 13:00 часа, ет. 4, ул."Костаки Пеев"21.

Материалите по защитата на докторанта са на разположение на интересуващите се в канцеларията на Физико-технологичния факултет при ПЛОВДИВСКИ УНИВЕРСИТЕТ „ПАИСИЙ ХИЛЕНДАРСКИ“, стая 214.

Научно жури: проф. д-р Невена Стоянова Милева
проф. д-р Димитър Михайлов Токмаков
проф. д-р Тодор Стоянов Джамийков
доц. д-р Владимира Кръстева Ганчовска
доц. д-р Николай Атанасов Шопов

Автор: маг. инж. Ивайло Детелинов Узунов
Заглавие: **МОДЕЛ ЗА СИМУЛАЦИЯ И КРАЙНИ РЕШЕНИЯ НА СИСТЕМИТЕ ЗА СИГУРНОСТ**

Тираж: 30 бр.

ОБЩА ХАРАКТЕРИСТИКА НА ДИСЕРТАЦИОННИЯ ТРУД

Актуалност на проблема

В съвременното информационно общество свободният и безопасен достъп до интернет сигурността и безопасността на информационните потоци са от жизнено значение за отделните личности, организации и обществото като цяло. Днес всички основни социални дейности (управленски, икономически, образователни, информационни, търговия, забавления) се извършват в информационното пространство и всички се опитват да ги използват за постигане на собствените си политически цели, което води до така наречената „Информационна война“.

Ние вече живеем в условията на такава война – фактите представени във Verizon 2020 Data Breach Inverstigation Report показват, че цели 90% от случаите за пробив на нечия информационна база се осъществява от външни източници; в 4% от случаите са замесени вътрешни лица, а само 1% идват от бизнес партньори; 79% от пробивите на информационната сигурност са заради пропуск в системата; 85% от пробивите се откриват чак след 2 седмици.

Информацията е най-ценния актив, с които разполагат организациите. Интелектуалната собственост, ноу-хау, патенти, списъци с клиенти и доставчици – тази информация е жизненоважна за всяка организация и формират нейното конкурентно предимство. Едно от най-важните предизвикателства пред тях е защитата на информацията във всички и форми – електронна и физическа. Информацията трябва да бъде надеждно защитена както от външни атаки – хакери или природни бедствия, така и от вътрешни –настоящи и бивши служители, партньори и доставчици.

Бързото развитие на информационните технологии и разширяването на интернет свързаността доведоха до увеличаване на заплахите за сигурността на данните и информационните системи. Според Forbes (John, 2024) само през 2023 година са отчетени 2365 кибератаки с 343 338 964 жертви, което е увеличение от 72% на нарушенията на сигурността на данните от 2021 г. В този контекст, защитата на информацията и осигуряването на надеждни и сигурни компютърни системи и мрежи са от съществено значение за предотвратяване на кибератаки и минимизиране на рисковете, свързани с изтичане на данни, неоторизиран достъп и други зловредни действия.

Създаване на практически насоки за защита на мрежови инфраструктури и уеб приложения, базирани на изследваните техники и инструменти е от изключителна важност.

Съвременните заплахи изискват интегриран подход, който включва редовно тестване, симулационен анализ, внедряване на криптографски модели и активен мониторинг на мрежовите системи. Получените резултати могат да служат като основа за разработване на нови стратегии за защита и внедряване на иновативни решения в условията на динамично променяща се киберсреда.

Цел на дисертационния труд:

На базата на обзора на проблемите свързани с мрежовата сигурност и защита на ценни информационни ресурси на дадена организация, както и гарантиране целостта на информацията с цел минимизиране разрушенията, получени в следствие на модифициране или унищожение. На база анализ на състоянието се формират целта и задачите на дисертационния труд.

ЦЕЛ на дисертационния труд е да се изследват възможностите за прилагане на модел за симулация и крайни решения на системите за сигурност. На тази база да се обосноват подходи за извършване на изследвания на мрежови информационни системи по отношение на сигурността.

Задачи за постигане на целта:

1. Да се извърши проучване и анализ на спецификата на основните видове заплахи, конкретните критерии и факторите им на въздействие.
2. Да се направят изследвания за основните методи и подходи за шифриране на информация с цел предотвратяване на атаки. Да се осъществи симулационен анализ и изследване на криптографски модели в системите за сигурност.
3. Да се извърши изследване на мрежови информационни системи по отношение на сигурността чрез различни инструменти за сканиране на мрежата.
4. Избор на подход за провеждане на изследване на различни видове атаки в среда Matlab. Да се изследват различните етапи, ефективност и устойчивост срещу криптографски атаки.
5. Да се извършат и представят експериментални изследвания чрез прилагане на модели за симулация и крайни решения на системите за сигурност с цел стратегия за минимизиране на рисковете, свързани с компютърни заплахи и анализ на резултатите.

Използвани методи и средства на изследване:

Използваните методи за изследване са от научните области: теория на техники и средства за компютърна сигурност за оценка на структурата и параметрите на базови компоненти на комуникационните системи, методи за компютърна сигурност, моделиране и симулационен анализ.

Внедряване и практическа приложимост

Реализирани, изследвани и анализирани са данните, за влиянието на компютърните атаки върху сигурността на системата.

Разработени са модели за изследване на видове атаки, криптиращи алгоритми, противодействие на различни видове атаки

Публикации по темата

Основните резултати са публикувани в: 2 броя в 17th International Technology, Education and Development Conference, INTED2023 Proceedings, 1 брой в сборници доклади на Международна конференция на младите учени, СУБ

– Смолян. 2 броя в сборник с доклади „ОБРАЗОВАНИЕ, НАУКА, ОБЩЕСТВО” Четири от публикациите са в съавторство с научния ръководител и една е самостоятелна.

СЪДЪРЖАНИЕ НА ДИСЕРТАЦИОННИЯ ТРУД

Глава 1. Литературния обзор по темата на дисертационния труд

В настоящия дисертационен труд се представя модел за симулация и крайни решения на системите за сигурност на видовете заплахи в компютърните системи. Извършен е анализ и оценка в лабораторни условия, предоставени от Физико-технологичен факултет (ФТФ) - гр. Смолян, за целите на изследването и за създаване на модела за симулация. Поставените задачи, както и използваните научни методи и средства, очертават значимостта на заложената в дисертационния труд цел:

Извеждат се иновационни за тълкуване на резултатите от научните изследвания по така зададената проблематика;

Осъществява се преглед и анализ на алгоритмите за определяне на видовете заплахи в компютърните мрежи;

Предлагат се за обсъждане верифициран алгоритъм при отчитане на основните видове заплахи, конкретните критерии и факторите на въздействие.

При еволюционното развитие на технологиите, налагащи нови подходи за комуникация и съхраняване на данни, нови операционни системи, протоколи или просто техни нови версии, се появяват нови уязвимости, водещи до нови заплахи и съответно атаки. За съвременната информационна сигурност е от жизнено значение периодично проучване, изследване, систематизиране и разработване на нови защитни процедури, техники, механизми и решения.

Актуалност. Пробивите в киберсигурността вече са част от ежедневието, а личната информация на милиони потребители все по-често е компрометирана. Организациите полагат значителни усилия да намалят вредите от хакерските атаки и да променят своята тактика за киберзащита. Основния проблем за бизнес организациите остава – дали политиките за защита са изпълнени и дали те в крайна сметка са достатъчно надеждни. Основните предизвикателства пред които са изправени всички организации са:

Устойчивост – поддържане на основните функции на организациите в условията на кризисни ситуации;

Откриване и възстановяване на инциденти и пробиви в сигурността;

Създаване на сигурни системни и продуктови архитектури и дизайн;

Разработване на сигурен код;

Защита и надеждност на информацията – методи за криптиране, удостоверяване, защита, комуникация;

Интегриране на модели за сигурност и подобряване на бизнес процесите;

Резултати от литературното проучване по темата на дисертационния труд

На база литературния обзор се установява, че съвременните компютърни заплахи са многолики, като тяхното разнообразие и сложност растат

пропорционално с напредъка на технологиите. Основните видове компютърни заплахи могат да бъдат категоризирани в следните групи:

1. Малунерен софтуер (Malware): Включва вируси, червеи, троянски коне, рансъмуер и шпионски софтуер. Тези заплахи целят кражба на данни, нарушаване на работата на системите или изнудване.
2. Заплахи, свързани с мрежова сигурност: Те обхващат атаки като DDoS, MITM (Man-In-The-Middle) атаки, проникване в мрежи чрез незащитени точки за достъп и експлоатация на уязвимости в мрежови протоколи.
3. Социално инженерство: Тази категория заплахи се основава на манипулация на потребители, като например фишинг, скамове и измами, насочени към извличане на чувствителна информация.
4. Заплахи, свързани с несанкциониран достъп: Те включват атаки, базирани на слабости в автентикацията, като използване на слаби пароли, експлоатиране на уязвимости в системи за оторизация и неправилно конфигурирани акаунти.
5. Заплахи за облачни среди: Развитието на облачните технологии доведе до нови рискове, включително нарушения на данни, липса на контрол върху достъпа и уязвимости в инфраструктурата.
6. Индустриални и IoT заплахи: Устройства, свързани към Интернет на нещата (IoT), както и системи за управление на индустриални процеси, са подложени на специфични рискове, като хакерски атаки, които могат да доведат до физически щети.

Литературният обзор разкрива, че ефективното управление на заплахите изисква мултидисциплинарен подход, включващ технически, организационни и правни мерки. Също така, поддържането на информираност относно новите форми на заплахи и тяхното развитие е от ключово значение за защитата на информационните системи.

Превенцията, комбинирана със своевременно откриване и реакция, остава основна стратегия за минимизиране на рисковете, свързани с компютърни заплахи.

Глава 2. Симулационен анализ и изследване на криптографски модели в системите за сигурност

В настоящата глава са изследвани основните методи и подходи за шифриране на информация. Обсъждат се принципите и средствата за шифроване, които са в основата на съвременните решения за защита на данните. Анализирани са основните методи за осигуряване на информационна сигурност, както и факторите, влияещи върху бързодействието на алгоритмите за шифроване.

Особено внимание е отделено на представянето на схеми за действие на алгоритмите за шифроване, като акцентът е поставен върху ключовия проблем за осигуряване на защитата на информацията. Разгледани са различните видове шифроване, техните характеристики по отношение на бързодействие и сигурност, както и съвременните предизвикателства, свързани с тези аспекти.

Основната цел на тази глава е представянето и анализа на методите и решенията за защита на данните, включително оценката на тяхната ефективност.

2.4. Основни положения при криптирането на информация

Алгоритъмът за криптиране на AES (Encryption Keys and Rounds) е блоков шифър, състоящ се от блок с дължина от 128 бита, който използва един и същи ключ за извършване на няколко кръга на криптиране. Той преобразува целия текст в единичен блок от битове. В AES дължината на блока може да бъде 128, 192 и 256 бита.

Терминът „блоково“ се отнася за това как алгоритъма смесва блоковите данни, като ги криптира повторно от първоначалните 10 до 14 кръга в зависимост от избора на дължината на ключа.

AES се основава на принципа на проектирането, известен като мрежа за заместване-пермутация и е ефективен както в софтуера, така и в хардуера [1]. Този шифър е вариант на Rijndael криптиране (фиг.2.1.) с фиксиран размер на блока от 128 бита и размер на ключа 128, 192 или 256 бита. Rijndael е определен с размерите на блокове и ключове кратни на 32 бита с минимум 128 и максимум 256 бита.

2.6. Резултати от направеното изследване

При симетрично криптиране подателят и получателят трябва да имат общ споделен таен ключ, който разменят преди започване на комуникацията. Подателят използва този ключ за да шифрова обикновения текст според стойностите на своите изисквания, а получателят го използва за да го дешифрира със споделения ключ от подателя. Едно от основните предимства на използването на симетрични алгоритми е, че те работят с максимална скорост, с която данните могат да криптират и декриптират с ниска изчислителна енергия. Едно от условието в AES е изискването за ефективна система за управление на ключове.

Изводи

Изследването на криптографските модели и симулационният анализ в системите за сигурност демонстрират ключовата роля на тези технологии за защитата на информацията в съвременния дигитален свят. В резултат на проведените анализи и преглед на съществуващите изследвания могат да се направят следните основни заключения:

1. Ефективност на криптографските алгоритми: Симулирането на различни криптографски алгоритми показа, че тяхната ефективност зависи от фактори като ключовата дължина, метода на шифриране (симетрично или асиметрично), както и приложените техники за управление на ключовете.
2. Сигурност срещу атаки: Симулациите разкриха, че криптографските модели с по-сложни и адаптивни структури предлагат по-голяма устойчивост срещу атаки като криптоанализ, атаки със сила (brute force) и атаките тип "човек в средата" (MITM).
3. Избор на подходящи алгоритми: Анализите подчертават, че изборът на алгоритъм зависи от специфичния контекст на приложение – например,

симетричните алгоритми (като AES) са предпочитани за бързо криптиране на големи обеми данни, докато асиметричните алгоритми (като RSA и ECC) са по-подходящи за сигурно предаване на ключове и автентикация.

4. Ролята на хеш функциите: Симулациите потвърдиха важността на хеш функциите (като SHA-256) за интегритет на данните и сигурност на автентикационните протоколи. Те играят ключова роля в защита от подправяне на данни.
5. Възможности и ограничения на квантово-устойчивите алгоритми: Изследванията в тази област показаха, че квантово-устойчивите алгоритми като тези от класовете Lattice-based и Hash-based криптография предлагат потенциална защита срещу квантови атаки, но същевременно поставят нови предизвикателства, свързани с производителността и интеграцията им в реални системи.
6. Значение на симулационния анализ: Провеждането на симулации допринася за оценка на устойчивостта на криптографските системи в различни сценарии, като това позволява идентифициране на слабости и оптимизация на сигурността преди внедряването в реални приложения.

Глава 3. Изследване на мрежови информационни системи по отношение на сигурността

С цел намаляване на атаките и подобряване на сигурността са изследвани и представени методи за проверка и отстраняване на пропуски довеждащи до потенциален неоторизиран достъп от трети страни.

Представен е алгоритъм от стъпки за защита на компютърната система от потенциални заплахи.

В този контекст се акцентира върху един от основните проблеми а именно киберсигурността. Акцентирано е върху видовете уязвимости и уязвимите точки в компютърните системи.

3.1.Изследване на мрежово сканиране

В тази точка от дисертационния труд е направено изследване на мрежово сканиране чрез продукта Nmap. Той е създаден с цел да улесни потребителите, които не са запознати с командния ред, като предоставя интуитивен интерфейс за изпълнение на сложни мрежови анализи. Nmap е широко използван в области като етични тестове за проникване, мрежово администриране, изследване и анализиране на уязвимости.

3.1.1.1. Изследване на фишинг атака с SEToolkit

Подготовка на атаката:

Атакуващият стартира SEToolkit на своята система (обикновено Linux-базирана дистрибуция като Kali Linux);

От менюто на инструмента се извършват съответните настройки за фишинг атака, която позволява клониране на уебсайт фиг.3.5.

3.7. Изследване на PHP Code Injection

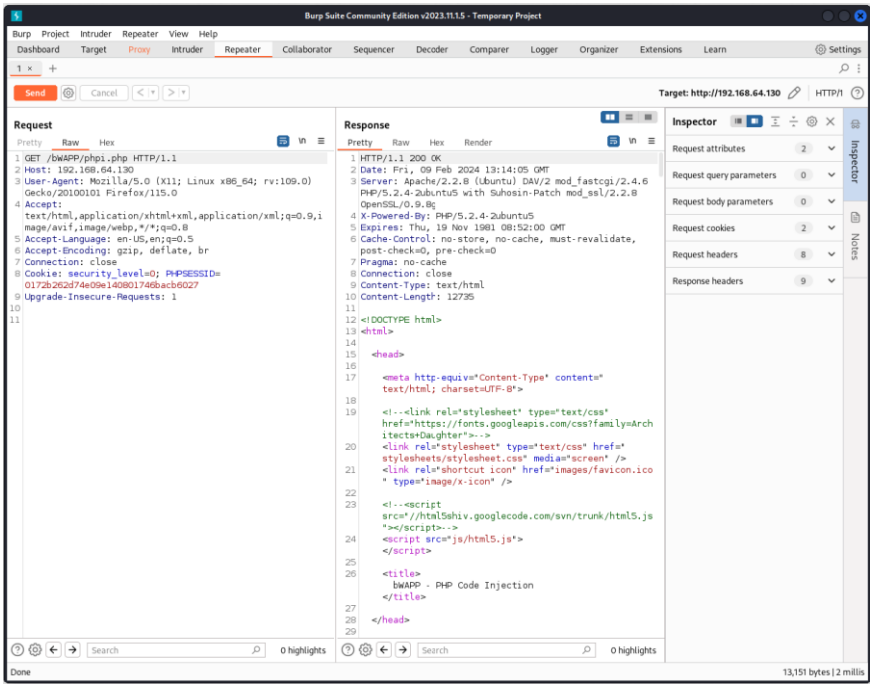
Изследването и анализирането на PHP Code Injection играе важна роля в компютърната сигурност, тъй като представлява сериозна уязвимост в уеб приложения, която позволява на нападателите да вмъкват и изпълняват произволен PHP код на сървъра. На Фиг. 3.7 е илюстрирана атака с PHP Code Injection, при която злонамерен код се инжектира чрез входни полета или параметри на заявката, които не са адекватно валидирани.

3.7.1. Изследване на защита срещу PHP Code Injection

Изследването и анализирането на PHP Code Injection играе важна роля в компютърната сигурност, тъй като представлява сериозна уязвимост в уеб приложения, която позволява на нападателите да вмъкват и изпълняват произволен PHP код на сървъра. На Фиг. 3.7 е илюстрирана атака с PHP Code Injection, при която злонамерен код се инжектира чрез входни полета или параметри на заявката, които не са адекватно валидирани.

3.8. Изследване на SQL Injection

Изследването на SQL Injection (SQLi) показва, че това е една от най-разпространените и критично опасни уязвимости в уеб приложенията, която излага на риск сигурността на данните и функционалността на системите. Тя позволява на злонамерени актьори да внедряват и изпълняват злонамерени SQL команди чрез неправилно защитени входни полета. На Фиг. 3.8 е представена демонстрация на SQL Injection атака, при която атакуващият използва уязвимост в заявката към база данни, за да заобиколи проверки за сигурност или да извлече чувствителна информация.



Фиг. 3.8. *SQL Injection – Принцип на работа и Превенция*

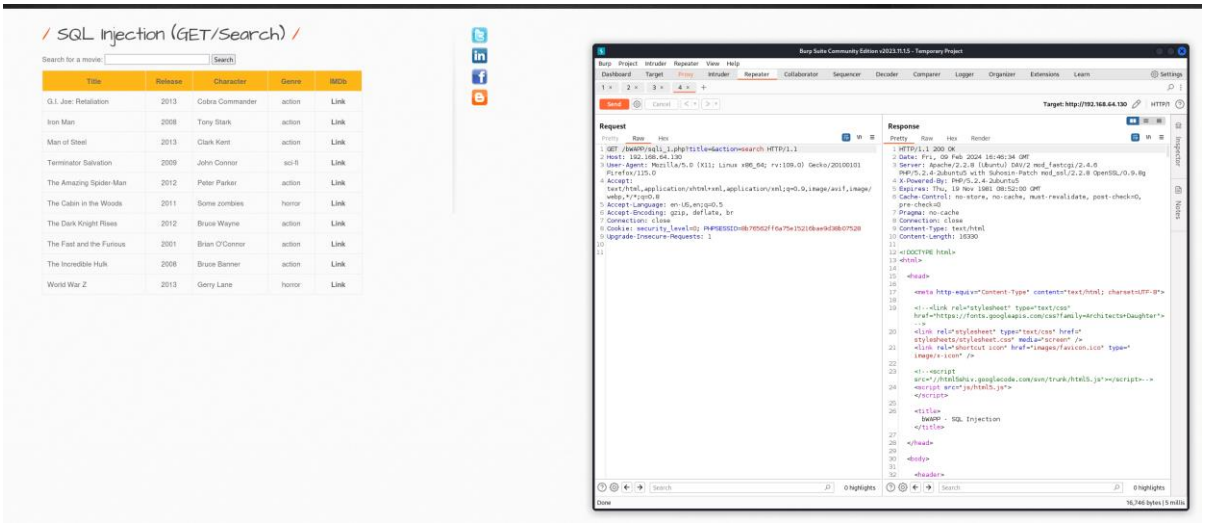
3.8.1. Изследване на типовете SQL Injection

Classic SQL Injection - Пряко инжектиране на код в SQL заявката.

Blind SQL Injection - Атакуващият получава индиректна информация чрез анализ на отговорите от сървъра

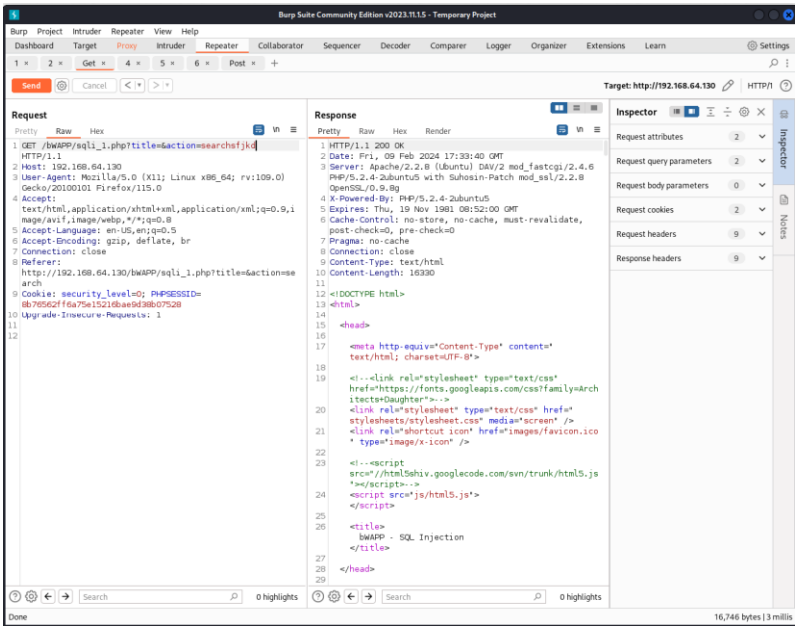
Union-based SQL Injection - Използва се операторът UNION за обединяване на резултати от различни таблици.

Error-based SQL Injection - Злоупотреба с грешки, генерирани от базата данни, за извличане на информация фиг.3.9.



Фиг.3.9. *Прихващане и компроментиране на заявката със Burp Suite*

3.9. Анализ на Action Search и неговата роля в системата

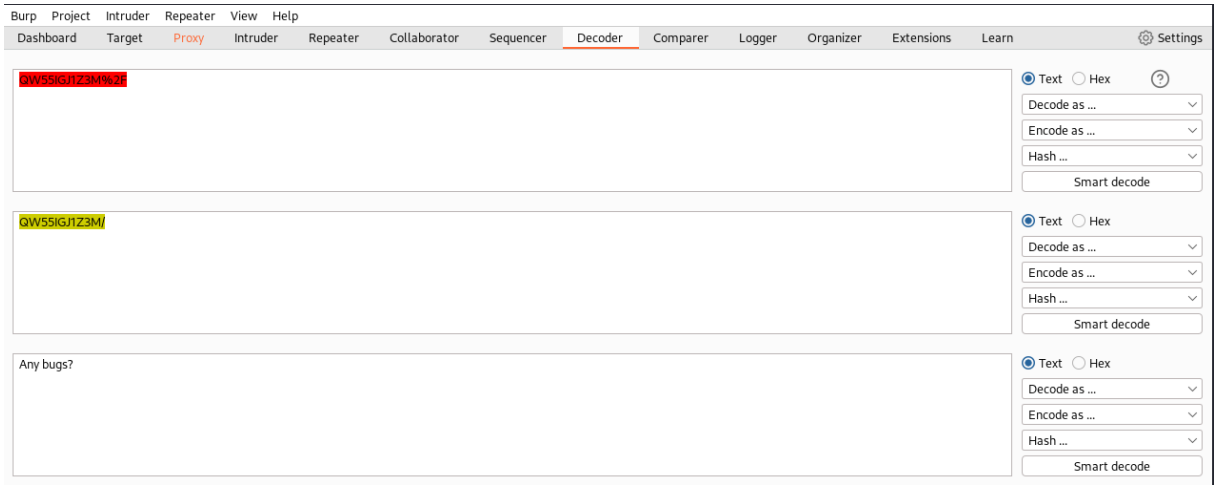


Фиг.3.10. *Action Search*

В изследването се използва Action Search, който предоставя функционалност, осъществяваща директни заявки към базата данни. Action Search е надеждна платформа за извличане на информация, като елиминира нуждата от намеса на потребителя в основния процес на търсене.

3.16. Изследване Base64 кодиране

В много случаи заявките и отговорите на уеб приложенията са кодирани в различни формати. Един често срещан пример е използването на Base64 за кодиране на данни като потребителски имена и пароли. При декодиране на данни, като тези, които са прихванати с Burp Suite, може да се разкрият важни уязвимости.



Фиг 3.14. *Декодиране на парола*

От фиг. 3.14 става ясно, че Base64 не осигурява никаква защита, тъй като всеки може лесно да декодира данните. Това е особено уязвимо, ако се използва за чувствителна информация като потребителски имена и пароли.

Препоръки:

Да се избягва използването на Base64 за чувствителни данни;

Използването на криптографски методи за защита на данните е от особено значение при защитата на информацията;

Редовна проверка и анализ на кодираните данни за потенциални уязвимости.

3.17. Изследване на Cross Site Scripting

Съхранените XSS уязвимости (Stored Cross-Site Scripting) представляват сериозна заплаха за сигурността на уеб приложенията, позволявайки на злонамерени потребители да инжектират и съхраняват злонамерен JavaScript код на сървъра. При тестове на уеб приложение беше открита уязвимост в блог секция, която позволява въвеждане и съхранение на невалидирани потребителски данни. Настоящото изследване представя анализ на уязвимостта и предлага препоръки за нейното адресиране.

Заключение

Откритата съхранена XSS уязвимост подчертава нуждата от строг контрол върху входните и изходните данни в уеб приложенията. Въпреки че не е наблюдавана ескалация до успешна атака в настоящия случай, уязвимостта

създава сериозен риск, който изисква незабавно адресиране. Прилагането на предложените мерки значително ще намали вероятността от подобни инциденти в бъдеще.

Експерименталните изследвания, проведени в рамките на тази глава, демонстрираха практически подходи към идентифициране и анализиране на уязвимости в мрежовите и информационните системи чрез използването на разнообразни инструменти и методи за сканиране и атаки. На база на проведените експерименти могат да бъдат направени следните изводи:

1. Ефективност на инструментите за сканиране:
   - Инструментът Discover осигурява цялостен анализ на мрежови структури, включително идентифициране на отворени портове, активни услуги и конфигурационни слабости;
2. Социално инженерство и автоматизация:
   - SEToolkit показа висока ефективност при симулиране на атаки, базирани на социално инженерство, включително фишинг и създаване на зловредни файлове, което подчертава значението на осведомеността на потребителите.
3. Тестове за инжектиране на код:
   - При PHP Code Injection и OS Command Injection експериментите показаха, че неправилното валидиране на входните данни позволява изпълнение на зловреден код на сървърите;
   - SQL Injection демонстрира възможността за извличане на чувствителна информация от бази данни, подчертавайки необходимостта от параметризирани заявки и други защитни механизми.
4. Тестове за уязвимости в CMS платформи:
   - Тестовете с експлойти, насочени към Drupal, потвърдиха, че остарели версии на софтуера могат да бъдат компрометирани чрез специфични експлойти, което подчертава значението на редовното обновяване.
5. Манипулации на файлови структури:
   - Directory Traversal експериментите разкриха, че лошо конфигурираните файлови системи позволяват достъп до чувствителни данни извън разрешените директории.
6. Криптографски манипулации:
   - Декодирането на данни и манипулирането с Base64 подчерта важността на правилното криптиране на данни, за да се предотвратят неоторизирани действия.
7. Междусайтови атаки:
   - При Cross-Site Scripting (XSS) експериментите бяха установени уязвимости, които позволяват на атакуващите да вмъкват и изпълняват скриптове в браузърите на потребителите, което подчертава значението на филтрирането на входни данни.
8. Търсене на действия и автоматизирани тестове:

- Инструментите като Action Search и Testwane показаха потенциала за автоматизирано тестване и оценка на сигурността, което намалява времето за идентифициране на уязвимости.

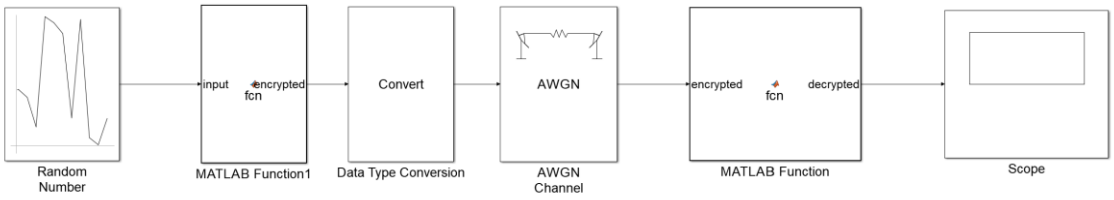
Експерименталните изследвания показват, че уязвимостите често произтичат от комбинация от технически и организационни пропуски. Инструментите и методите, използвани в тази глава, доказаха своята полезност за идентифициране на слабости, което е критично за повишаване на нивото на информационната сигурност. Установено е, че ефективната защита изисква интегриран подход, включващ редовни тестове, обновяване на софтуера, строг контрол на входните данни и обучения на персонала.

ГЛАВА 4. ЕКСПЕРИМЕНТАЛНИ ИЗСЛЕДВАНИЯ

В четвърта глава от дисертационния труд са изследвани и представени методи за проверка и отстраняване на пропуски довеждащи до потенциален неоторизиран достъп от трети страни, с цел намаляване на атаките и подобряване на сигурността. Представени са симулационни модели в среда Матлаб в контекста на информационната сигурност. Представени са резултати от симулация на атаки към сървър, защитна стена за филтриране на атакуващия трафик, криптиране и декриптиране на данните за осигуряване на защитен обмен на информация и др.

4.1. Моделиране на AES криптиране в MATLAB

Криптографският алгоритъм (AES) е широко използван, който предоставя надеждна и ефективна защита на данните. В средата MATLAB, алгоритъмът AES може да бъде моделиран, за да се изследват неговите етапи, ефективност и устойчивост срещу криптографски атаки. В тази част от дисертацията се представя моделиране на AES криптиране в MATLAB, с фокус върху симулацията на основни операции и анализ на резултатите.

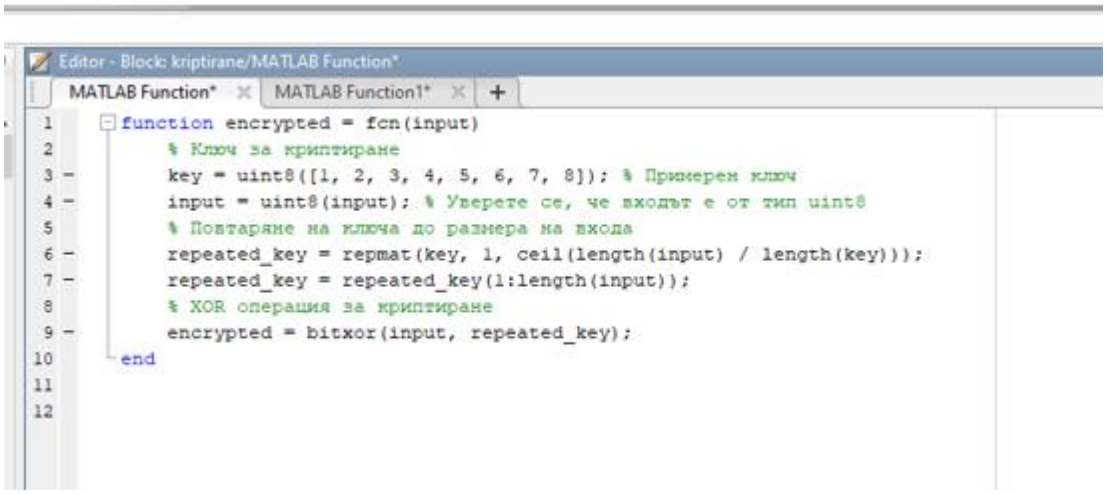


Фиг. 4.1. *Симулационен модел на AES криптиране*

На фигура 4.1 е представен симулационен модел за реализиране на XOR криптиране на входен сигнал и извършване на последваща обработка чрез поток от данни. Симулационният модел се състои от следните блокове:

- Random Number – използва се за генериране на последователност от произволни потоци от данни;
- Криптиращ Matlab Function 1 - блок, в който се съдържа криптиращ код написан в развойната среда на Matlab;

- Data Type Conversion - блокът служи за уеднаквяване на типовете данни на съответните сигнали, които се използват в модела. По този начин се избягват възможности да възникнат грешки;
- AWGN Channel - блокът има важно значение в така проектирания симулационен модел, защото чрез него се осигурява възможност да се реализира реална среда на комуникационен канал посредством добавяне на адитивен бял гаусов шум;
- Декриптиращ блок Matlab Function - в който се съдържа декриптиращ код написан в развойната среда на Matlab;
- Scope блока в Matlab - за визуализация на сигнала в реално време.



Фиг.4.2. *Криптиращ код*

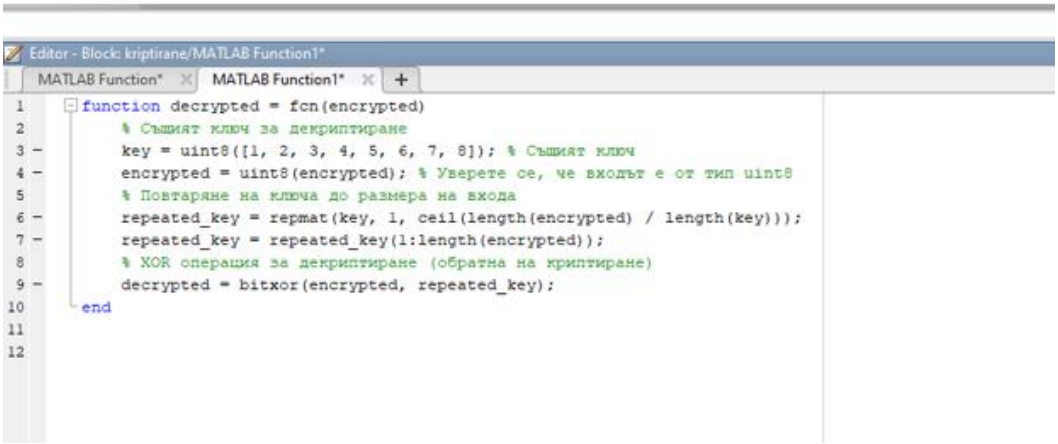
Фигура 4.2 показва MATLAB функция, която използва XOR криптиране за обработка на входни данни. Кодът приема входен вектор, прилага битово XOR криптиране със зададен ключ и връща криптирания резултат.

1. Дефиниране на функцията:
   - Дефинираме функция с име fcn, която приема един входен аргумент input (текста за криптиране) и връща криптирания текст encrypted.
2. Дефиниране на ключа за криптиране:
   - Задава симетричен ключ за криптиране, който е вектор от числа тип uint8 (8-битови цели числа);
   - Векторът [1, 2, 3, 4, 5, 6, 7, 8] представлява примерен ключ.

3. Преобразуване на входа:
   - Преобразува входния текст (input) в тип uint8. Това е необходимо, защото XOR операцията работи с числови данни, а текстовите данни се преобразуват в числа чрез ASCII кодовете на символите.
4. Повтаряне на ключа:

- Функцията repmat повтаря ключа толкова пъти, колкото е необходимо, за да покрие дължината на входния текст;
- ceil(length(input)/length(key)) изчислява колко пъти трябва да се повтори ключът, за да бъде поне толкова дълъг, колкото входа.

5. Съкращаване на ключа:
   - repeated_key(1:length(input)) изрязва излишните символи от повторения ключ, така че неговата дължина да съвпадне точно с тази на входния текст.
6. Криптиране чрез XOR:
   - Използва XOR операцията (bitxor) между всеки символ от входния текст и съответния символ от повторения ключ;
   - XOR криптиране: Ако един и същ ключ бъде приложен два пъти, оригиналният текст се възстановява.



Фиг. 4.3. *Декриптиране AES_Decrypt*

Фигура 4.3 представя MATLAB функция, която използва XOR операция за декриптиране на криптирани данни. Кодът е идентичен с функцията за криптиране, което е очаквано при XOR-базирано симетрично криптиране.

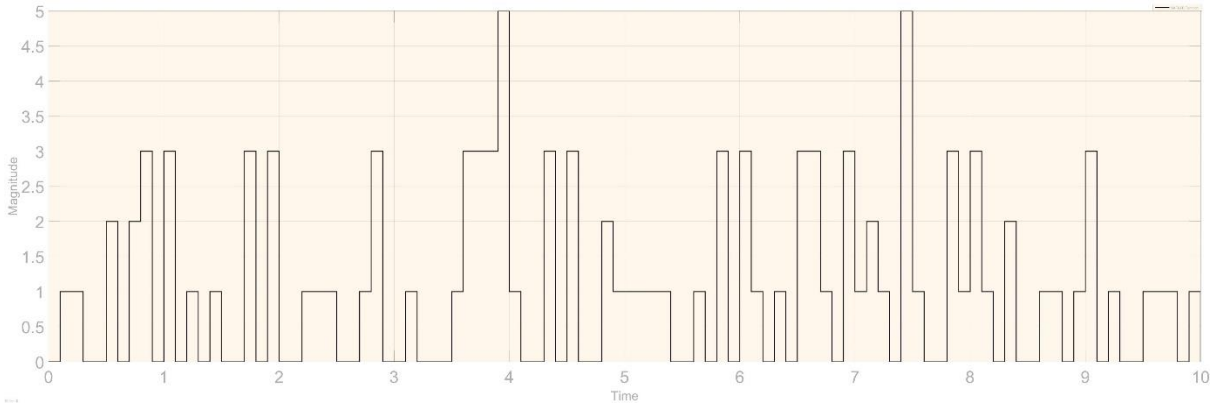
При AES декриптирането в MATLAB следва обратния процес на криптиране, за да възстанови оригиналния текст от криптирания. Основните операции се изпълняват в обратен ред, като всяка операция има своята обратна версия:

Обратен ред на кръговете - Декриптирането започва с финалния кръг на криптиране и преминава към началния. Това включва използване на кръговите ключове в обратен ред.

Етапи на декриптиране:

- *Inverse ShiftRows:* Обратно разместване на редовете в матрицата;
- *Inverse SubBytes:* Подмяна на байтовете с помощта на обратен S-box;
- *Inverse MixColumns:* Линейна трансформация, която възстановява оригиналното състояние на колоните;
- *AddRoundKey: XOR* операция с кръговия ключ, която възстановява оригиналните данни.

- *Padding* - След декриптиране се премахва добавеният padding, за да се възстанови оригиналният текст. Този подход осигурява коректно възстановяване на данните, като гарантира същата сигурност и ефективност, както при криптирането.



Фиг. 4.4. *Визуализация на данните след криптиране и декриптиране*

Тази фигура показва графика от MATLAB/Simulink Scope, която визуализира дискретен сигнал. Този сигнал представлява криптиран двоичен поток, получен чрез XOR криптиране. Графиката визуализира промените в битовете – преходи между 0 и 1, които създават стъпаловидна форма. Ако същият ключ се приложи отново върху криптирания сигнал, ще се получи декриптиран (оригинален) сигнал.

4.2. Изследване на Man-in-the-Middle (MITM) атака

Атаката Man-in-the-Middle (MITM) е сценарий, в който злонамерен участник прихваща, подслушва или манипулира комуникацията между две страни. В MATLAB подобен модел може да бъде реализиран, за да се симулира работата на MITM атаката, както и за да се изследват методи за нейното предотвратяване.

4.2.1. Принцип на работа на MITM в MATLAB

Симулацията на MITM в MATLAB включва три основни компонента:
Легитимни участници:

- Изпращач (Client) и получател (Server) обменят данни, като използват симетрично криптиране (например AES);
- В този модел клиентът криптира данните преди изпращане, а сървърът ги декриптира при получаване.

Атакуващ (MITM):

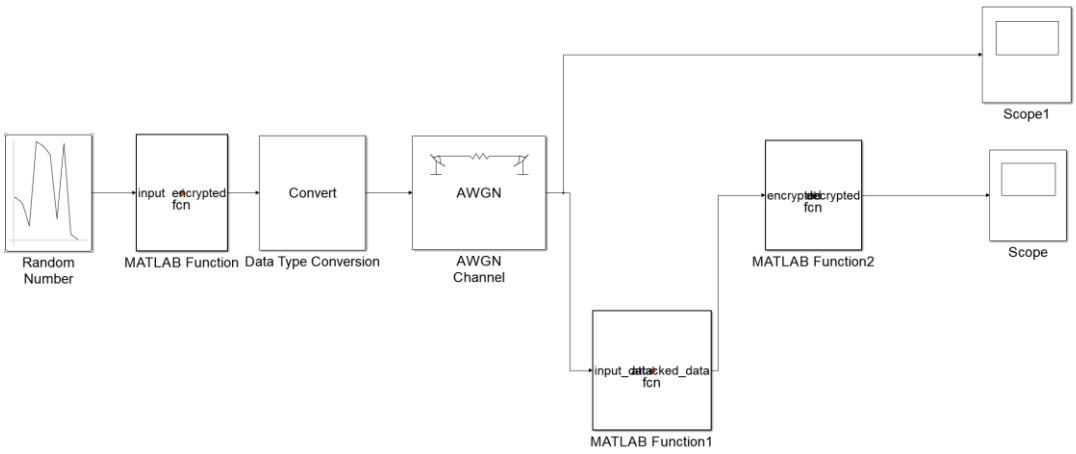
- Атакуващият се позиционира между клиента и сървъра, като прихваща данните;
- Той може да подслушва съобщенията, да ги модифицира или да ги инжектира обратно към получателя.

Механизми за криптиране и декриптиране:

- При AES криптиране се използва за защита на данните. MITM атаката може да бъде реализирана чрез прихващане и симулация на компрометиране на ключа за криптиране.

4.2.3. Заключение

Моделирането на MITM атака в MATLAB позволява разбиране на принципите на работа на този вид атака и демонстрация на рисковете за сигурността на комуникациите. Освен това, чрез разширения като цифрови подписи и сигурен обмен на ключове, MATLAB може да се използва и за проектиране на механизми за защита срещу MITM. Тази симулация е полезна както за обучителни, така и за изследователски цели.

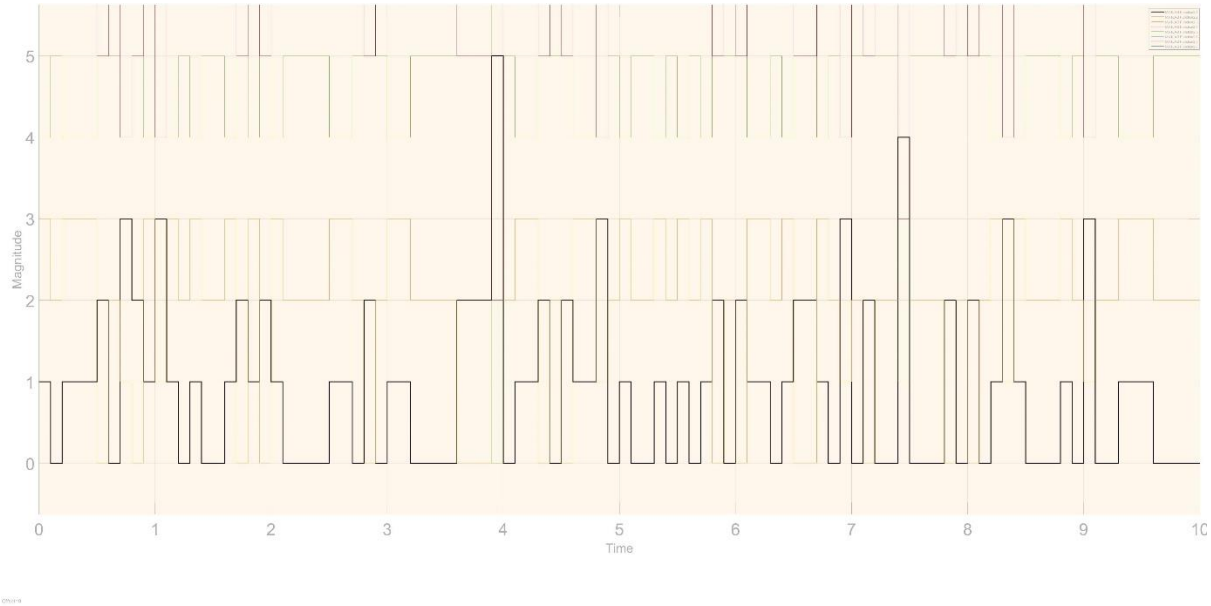


Фиг. 4.5. *Симулационен моделна MITM*

Фигура 4.5 представлява разширен вариант на Фигура 4.14, като разликата се изразява в допълнението на блока Matlab Function 1. В настоящия контекст този блок се използва за реализиране на атака Man-in-the-Middle (MITM). За тази цел е разработен специализиран код в програмната среда Matlab.

4.2.4.Основни компоненти на MITM симулацията

- Клиентът криптира съобщение с AES и го изпраща към сървъра.
- MITM атакуващият прихваща криптирания текст, декриптира го (ако разполага с ключа), модифицира съобщението и го изпраща към сървъра.
- Сървърът декриптира полученото съобщение и го обработва.



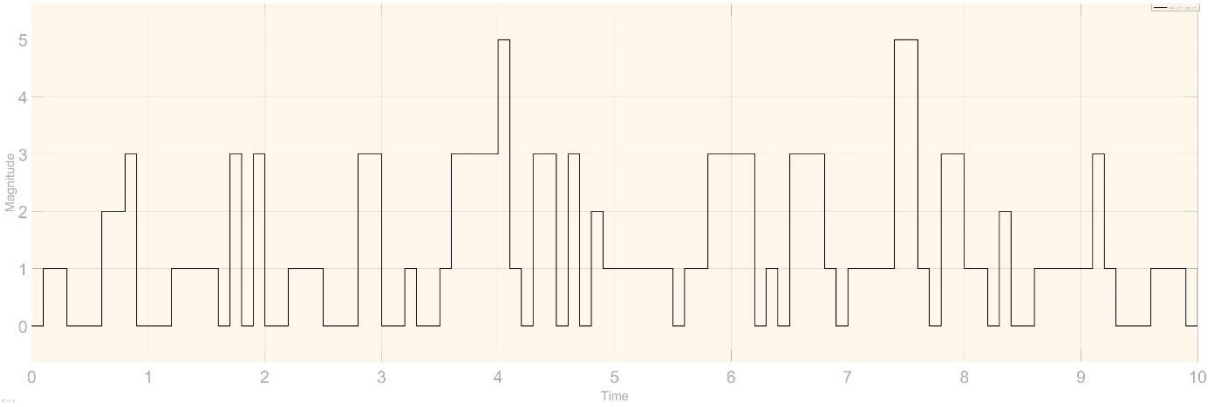
Фиг.4.6. *Визуализация на данните с MIMT*

Заключение

Man-in-the-Middle атаката демонстрира необходимостта от по-силни защити, като:

1. *Двуфакторна автентикация:* За гарантиране на самоличността на страните.
2. *Цифрови подписи:* За проверка на целостта и автентичността на съобщението.
3. *Сигурни протоколи:* TLS/SSL за криптиране на комуникацията.

Това изследване в MATLAB илюстрира основния механизъм на MITM атака и как компрометирането на ключове или липсата на защита може да доведе до сериозни нарушения на сигурността.

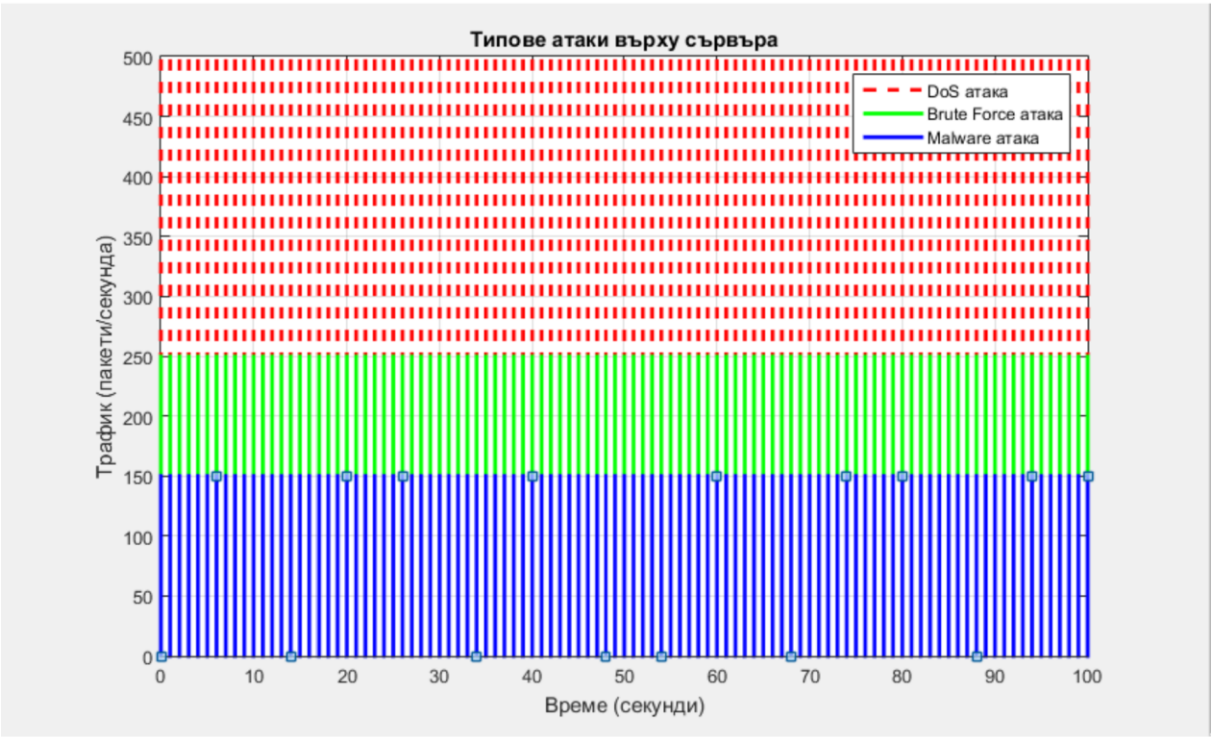


Фиг. 4.10. *Компрометирана забавяне и повторение на данните*

Резултатите изобразени на фиг.4.10 от Scope на Matlab Simulink представлява сигнал обработен в контекста на симулацията след атака Replay и Delay. Неправилните стойности и периодичните отклонения в сигнала са резултат от възпроизвеждане и закъснение на некомпрометирания сигнал, което потвърждава въздействието на атаката.

4.3. Модел за симулация на DoS атака върху информационна система.

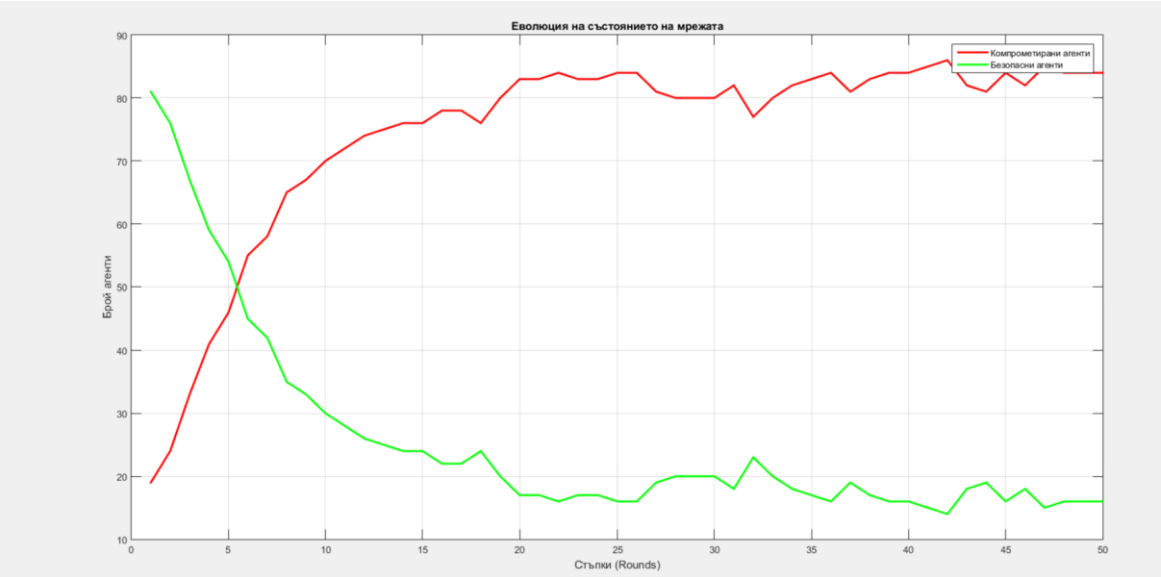
Представен е модел за симулация на атака тип Denial of Service (DoS). Целта е да се създаде информационна система, услуга или мрежа, недостъпна за легитимни потребители, като я претовари с излишни заявки или блокира достъпа до ресурси. Използван е MATLAB за моделиране и симулация на DoS атаки с цел анализ на тяхното въздействие върху системите.



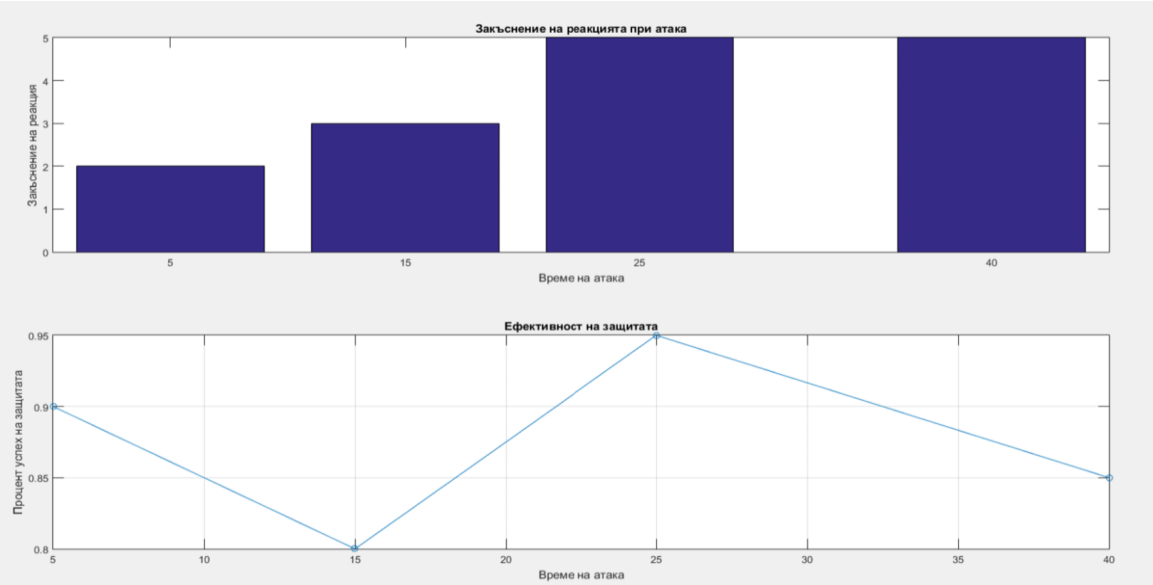
Фиг. 4.12. *Изследване на типовете атаки в Matlab*

Фигура 4.12 представя различни типове атаки върху сървър, представени като обем на трафика (пакети/секунда) спрямо времето в (секунди). DoS атаки в червена линия има най-голям обем трафик, симулиращ претоварване на сървъра. Brute Forse атака – зелена линия има постоянен поток от пакети, представляващ опити за отгатване на пароли или други данни. При Mawlare атака синя линия – има по-голям обем трафик симулиращ разпространение на зловреден софтуер.

Графиката от фиг.4.19 илюстрира еволюцията на състоянието на мрежата в хода на 50 симулационни стъпки. Червената линия показва увеличението на компрометираните агенти с напредване на стъпките. В началото компрометираните агенти са малко, но с времето броят им значително нараства. Зелената линия представя намаляването на безопасните агенти, което е огледално на увеличаването на компрометираните. Графиката подчертава ефективността на атакуващите в компрометирането на мрежата като защитниците успяват да задържат определен баланс само в началните стъпки.



Фиг. 4.19. *Графика на еволюцията на мрежата*



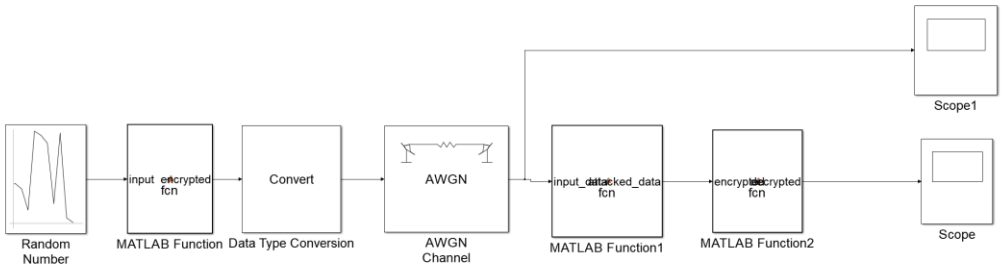
Фиг. 4.21. *Анализ на устойчивост*

Фигура 4.21 илюстрира две различни зависимости, свързани със защитата при атаки:

- Графика закъснение на реакцията при атака представя по оста x времето на атака спрямо закъснението на реакцията по оста y. С напредване на времето закъснението на реакцията се увеличава;
- Графика ефективност на защита илюстрира процента на защита с напредване на времето. Забелязва се спад на ефективността в началото последван от подобрение в 25 атака, след което ефективността отново намалява.

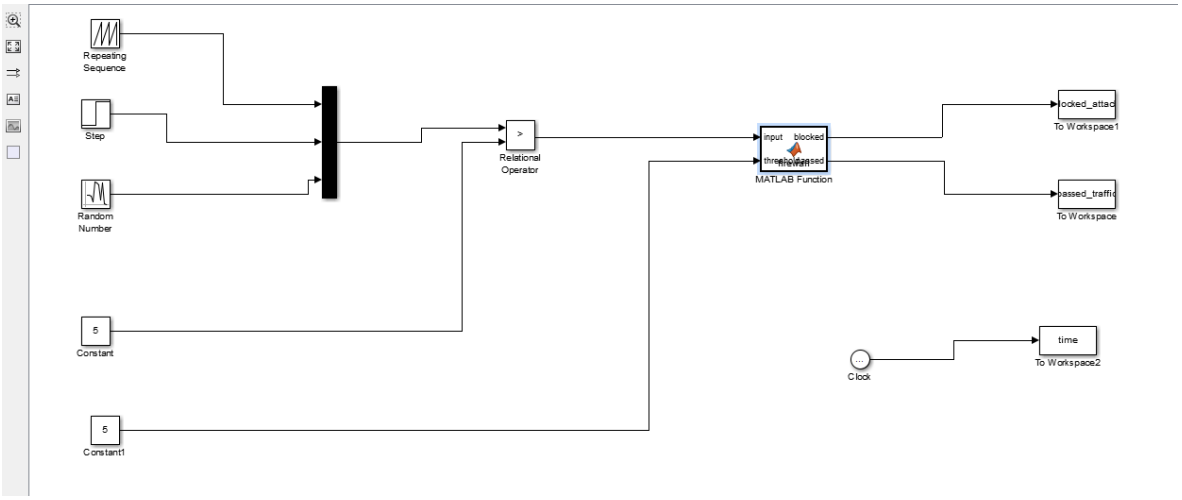
4.4.Изследване на атака тип Replay и Delay в MATLAB

При извършеното изследване на атаките от типа Replay и Delay, се установи, че това са видове заплахи в мрежовата сигурност, при които валидни съобщения между два участника се прихващат, повтарят или се забавят от трети злонамерен „участник“. Представена е симулация на тези атаки, което позволява тяхното изследване и тестване на защитни механизми фиг. 4.7.



Фиг. 4.7. *Блокова схема на атака Replay и Delay*

Изследването представено на фиг.4.7 се основава на блоковете, използвани в предходните две изследвания с единствената разлика, че е добавен програмируем блок Matlab Function 1. Този блок изпълнява софтуерна симулация на атаките Replay и Delay фиг.4.8. Кодът, имплементиран в него, симулира повторение и забавяне на предаваните данни във времевия домейн.



Фиг. 4.22. *Модел на симулация и процес на взема на крайни решения на система за сигурност*

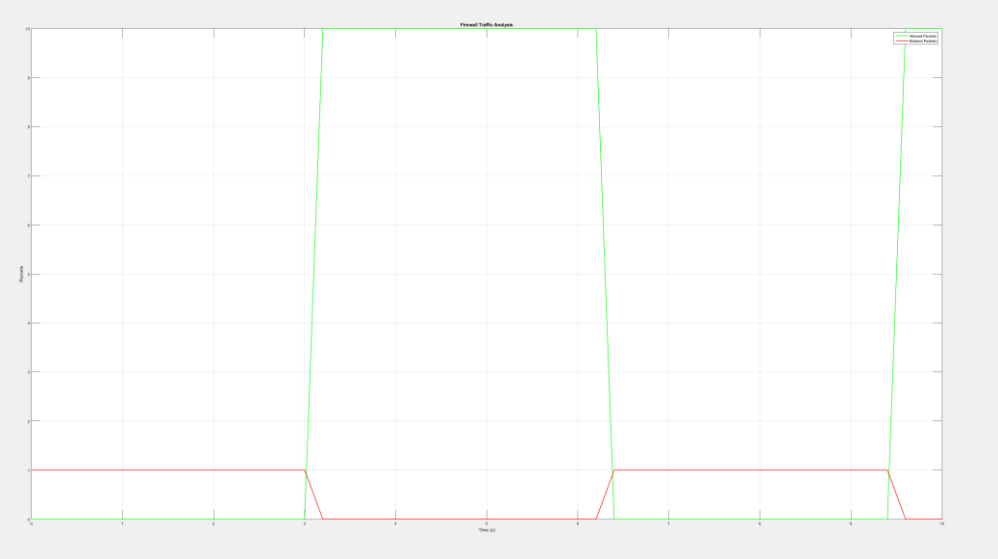
4.5.Основни модули, които са използвани при симулацията:

Графиката представя поведението на системата, показвайки броя на разрешените и блокираните пакети във времето;

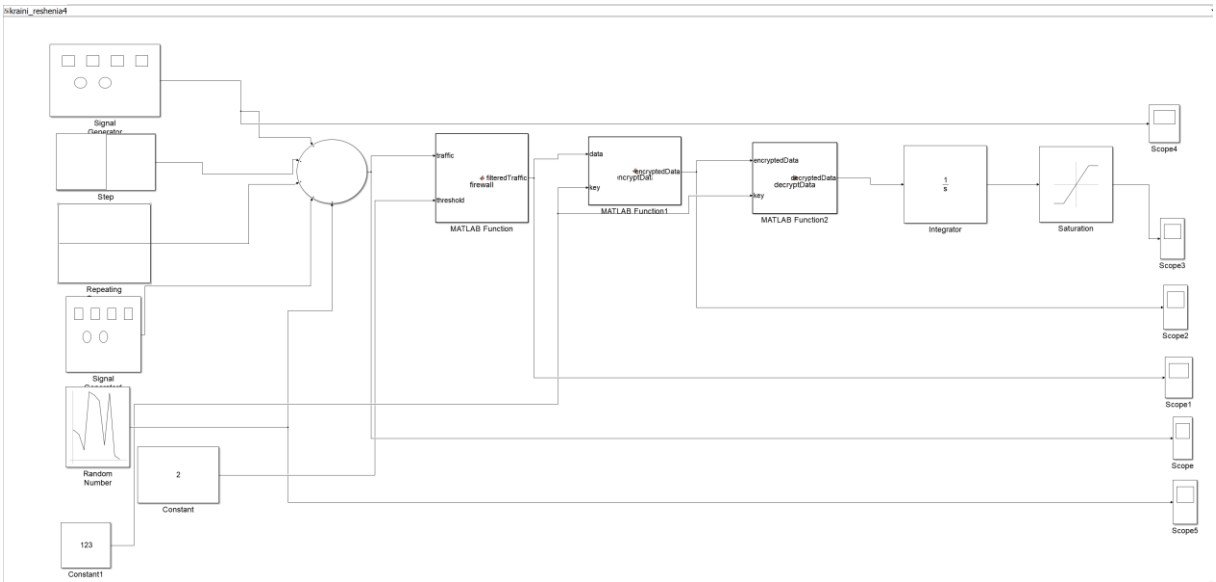
Червената линия (Blocked Packets) - представя блокираните пакети поради нарушаване на политиките на защитната стена;

Зелената линия (Allowed Packets) - Представя разрешените пакети, които са преминали защитната стена;

Във времеви диапазони около 3-4 секунди се вижда активност, свързана с блокиране на пакети, като реакция на атака.



Фиг. 4.25. *Графично визуализиране на резултатите*



Фиг. 4.26. *Модел за симулации на атаки към сървър*

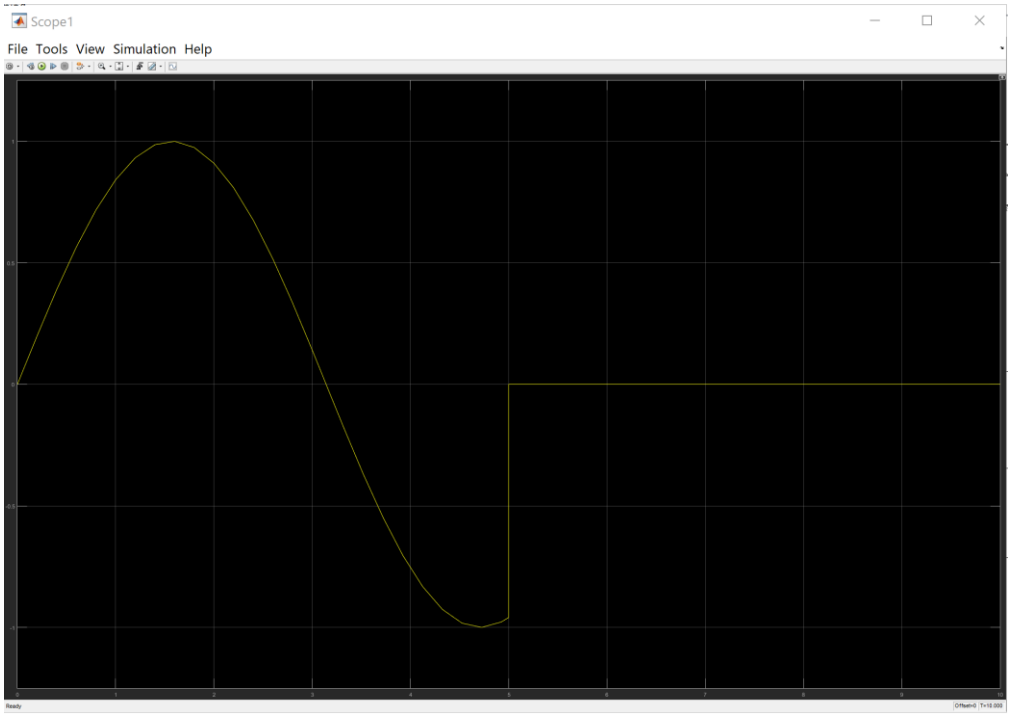
Моделът включва симулация на атаки към сървър, защитна стена за филтриране на атакуващия трафик, криптиране и декриптиране на данните за осигуряване на защитен обмен на информация.

Компоненти на модела са: генерация на трафик - нормален и атакуващ трафик.

Защитна стена - открива и блокира атакуващия трафик.

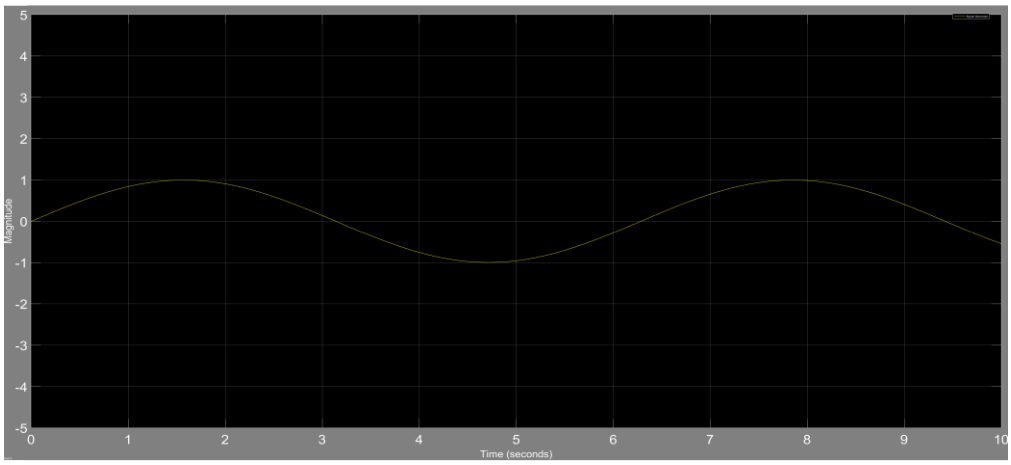
Криптиране и декриптиране - симулира защитен обмен на данни между клиент и сървър.

Сървърна система - обработва само нормалния (филтриран) трафик.



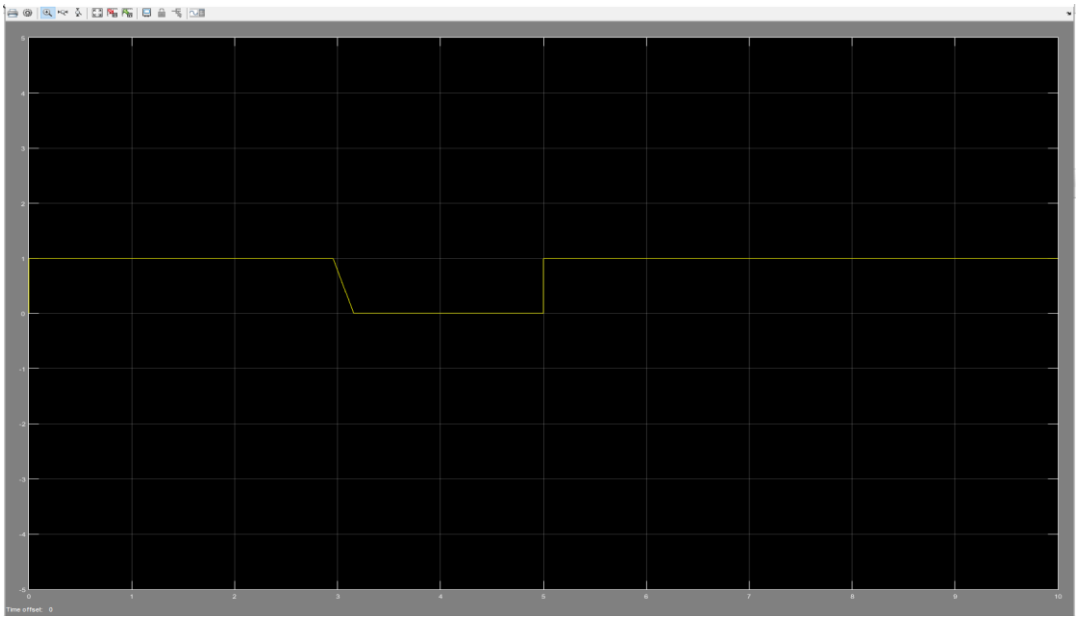
Фиг. 4.27. *Входящ комбиниран трафик (изход от Sum Block)*

От 0 до 5 стъпка сигналът има синусоидална форма, което представлява нормален трафик към сървъра. Видно е, че сигналът намалява и достига отрицателна стойност, което индикира увеличаване на атакуващия трафик. При достигане на прага (зададен в защитната стена), сигналът рязко се променя на константна стойност, вследствие от блокиране на атаката от защитната стена – firewall-ът.



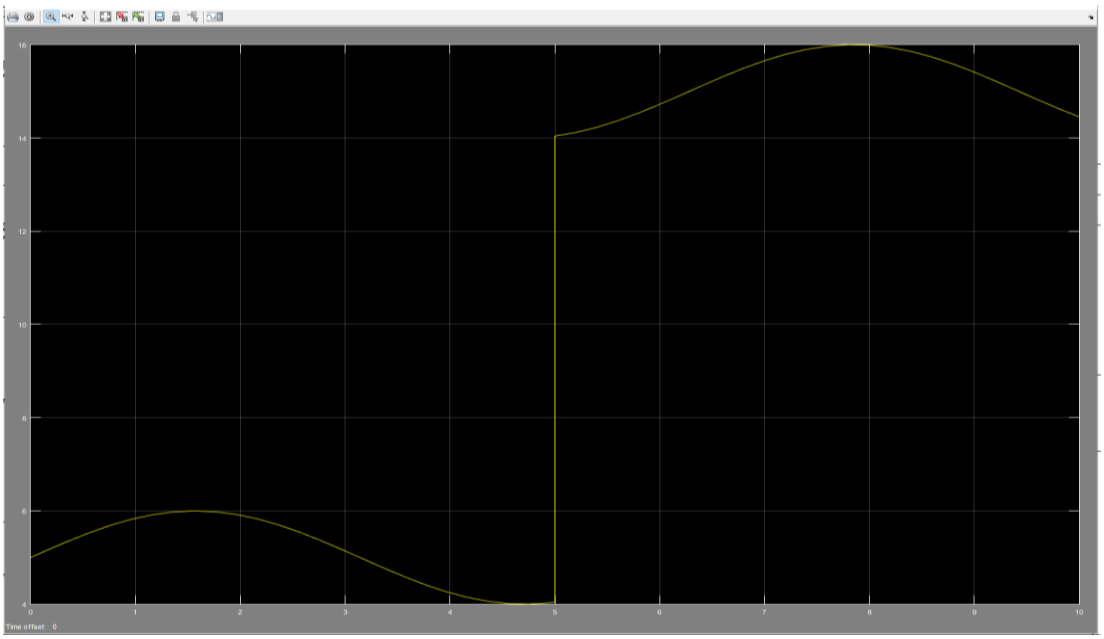
Фиг. 4.28. *Мрежов трафик*

Нормален мрежов трафик - Това е референтен сигнал, който показва стандартната комуникация със сървъра, преди атаката да започне.



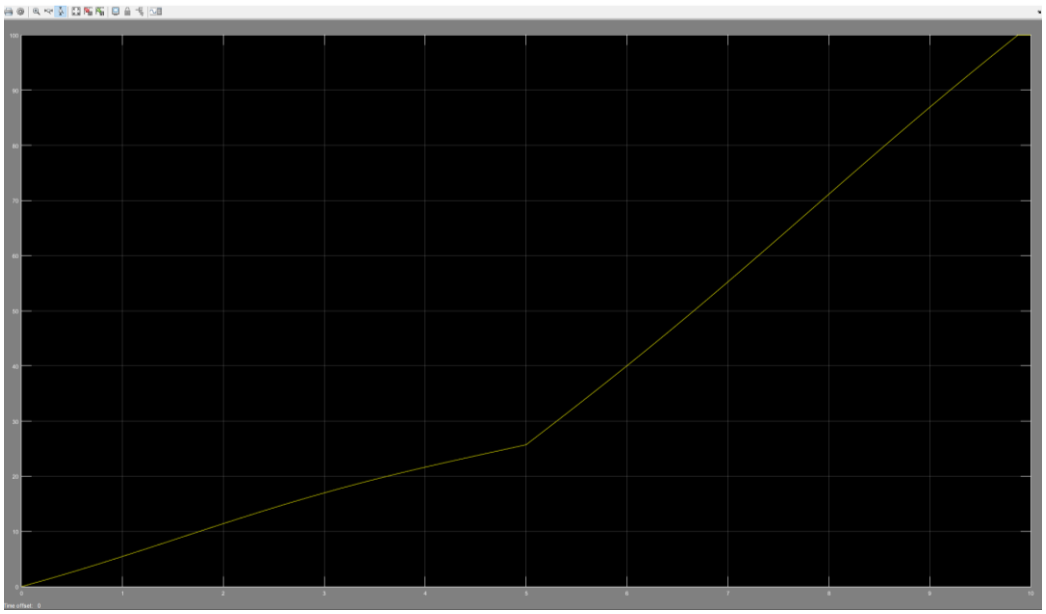
Фиг. 4.29. *Филтриран и блокиран трафик от защитна стена*

От графиката се вижда, че в началото сигналът е стабилен на едно ниво, което означава нормално функциониране на мрежата. От 3-ти до 5-ти период има рязък спад, което представлява, откриване на атака. Защитната стена засича подозрителна активност и предприема действие.



Фиг. 4.30. *Анализ на трафик към сървър.*

От графиката на фиг. 4.30 се вижда, че в началото сигналът има синусоидална форма, което представлява нормален трафик към сървъра. В даден момент (около 5-та секунда) има рязък скок, след което сигналът продължава като синусоида, но с по-висока амплитуда. Това поведение е причинено от филтрация и реакция – в началото има ограничение на трафика, но след като защитната стена разпознае безопасни заявки, трафикът се увеличава.



Фиг. 4.30. *Анализ на трафик към сървър.*

На фиг. 4.31. е представена графиката, която има линеен растеж в следствие от натрупване на ресурс, като блокирани пакети – защитната стена блокира трафик, следствие от брояча на отхвърлените заявки. Промяна в наклона около 5-та секунда е в резултат на блокиран трафик от защитната стена.

Симулацията демонстрира, че правилната настройка на защитната стена позволява ефективна защита срещу атаки. Подобни симулации могат да се използват за разработване на адаптивни защитни механизми, които автоматично коригират параметрите си в зависимост от характеристиките на мрежовия трафик.

Изводи

Изследването на мрежовите информационни системи в контекста на тяхната сигурност разкри редица ключови аспекти, които определят ефективността на защитата срещу съвременните заплахи. Основните заключения, които могат да се направят въз основа на направените изследвания и анализа, са следните:

1. Моделирането на AES криптиране в MATLAB осигурява задълбочено разбиране на алгоритъма и неговите етапи. Чрез тази реализация могат да се извършват изследвания, оптимизации и анализи на сигурността. MATLAB предлага мощна платформа за проектиране и тестване на криптографски алгоритми, което го прави ценен инструмент за обучение и изследвания в областта на киберсигурността.

2. Идентифициране на уязвимости: Анализът показа, че значителен процент от уязвимостите в мрежовите системи произтичат от неправилна конфигурация, остарял софтуер или недостатъчна защита на устройствата, включени в мрежата.

3. От направените изследвания се доказва, че DoS атаките влияят върху достъпността на информационните системи. За да се намалят ефектите на DoS атаките, е необходимо внедряване на:

- Механизми за откриване на DoS атаки.
- Системи за защита (например Firewall и Rate Limiting).
- Архитектури с баланс на натоварването.

4. Методът Монте Карло е изключително полезен за моделиране на вероятности в контекста на информационната сигурност. Чрез симулации можем да разберем как различни фактори (като дължината на паролата или наборът от символи) влияят на вероятността за успешна атака. MATLAB предлага удобен начин за реализиране на тези симулации, като същевременно ни позволява да визуализираме резултатите чрез графики.

5. Методите за анализ на симулационни резултати включват комбинация от статистически, графични и сравнителни подходи. Те позволяват:

- Идентификация на слабости;.
- Оптимизация на стратегии;
- По-добро разбиране на сложното поведение на системата;
- Подходящият анализ е от решаващо значение за извличане на стойност от симулациите и за вземане на информирани решения относно сигурността на системите.

6. Моделът Agent-Based в контекста на информационната сигурност дава полезно разбиране за динамиката на атаките и защитата в мрежови среди. Чрез изследването в MATLAB и представените графики можем да наблюдаваме как агенти с различни роли взаимодействат помежду си и как тези взаимодействия влияят на състоянието на мрежата с времето.

В обобщение, сигурността на мрежовите информационни системи изисква цялостен и систематичен подход, който обединява технологии, процедури и управление. Изследването подчертава необходимостта от непрекъсната адаптация на мерките за сигурност спрямо еволюцията на заплахите, както и важността на обучението и информираността на всички участници в мрежовата екосистема.

ЗАКЛЮЧЕНИЕ

Настоящата дисертация разглежда различни аспекти на информационната сигурност чрез теоретични и практически изследвания, като акцентът е поставен върху анализи, симулации и експерименти, насочени към идентифициране и преодоляване на уязвимости.

В първа глава от дисертационния труд е направен обзор на кибератаките, които пряко кореспондират с темата на дисертационния труд.

Литературният обзор подчертава нарастващата сложност и разнообразие на компютърните заплахи, които включват зловреден софтуер и уязвимости в традиционните мрежови и информационни системи. Ефективната защита изисква интегриран подход, обединяващ технически, организационни и правни мерки.

Представен е модел на информационна сигурност. Извършена е класификация на информацията с акцент върху управление на сигурността и най-честите инциденти. Обърнато е внимание на стандартите за системи за управление на сигурността на информацията. Представени са различните процедури за сигурност. Акцентирано и разгледани са видовете атаки с акцент върху изграждането на модел за симулации и крайни решения в системите за сигурност. На база литературния обзор се установява, че съвременните компютърни заплахи са многолики, като тяхното разнообразие и сложност растат пропорционално с напредъка на технологиите.

На база направения литературен обзор са формулирани целта и задачите на дисертационни труд.

Във втора глава от дисертационния труд са изследвани основните методи и подходи за шифриране на информацията. Особено внимание е отделено на представянето на схеми за действие на алгоритмите за шифроване, като акцентът е поставен върху ключовия проблем за осигуряване на защитата на информацията. Разгледани са различните видове шифроване, техните характеристики по отношение на бързодействие и сигурност, както и съвременните предизвикателства, свързани с тези аспекти. Оборното е внимание на процеса на криптиране/декриптиране, който се базира на математически метод, известен като алгоритъм за криптиране. В този контекст се акцентира, че изходната информация обикновено се нарича нешифрован текст (plain text), независимо дали се отнася за текстови или не-текстови съобщения. Представени са асиметрични криптографски алгоритми, принципа им на работа и тяхното им приложение. Стига се до заключението, че съвременните системи често комбинират симетрична и асиметрична криптография, за да се справят с предизвикателствата на киберсигурността. Извършено е изследване на принципа на работа на AES, дадени са основните фактори влияещи върху работата им. От направеното изследване се установява, че при симетрично криптиране подателят и получателят трябва да имат общ споделен таен ключ, който разменят преди започване на комуникацията. На фигура 2.9 са изследвани и представени резултатите от процеса на 256-битово криптиране с използване на SHA (Secure Hash Algorithm) функция за хеширане. На фигура 2.10 са изследвани и представени резултатите от интегрирането на string функция в процеса на

обработка на данните. Добавянето на string функцията има за цел да подобри обработката на текстови стойности, като предоставя допълнителни възможности за манипулация и трансформация на данните. Интегрирането изследването и анализирането на резултатите показват, че добавянето на string функцията позволява по-ефективна работа с текстови данни и подобрява цялостната надеждност на системата. На фигура 2.11 са изследвани и анализирани резултатите от проведените изпитвания с използване на алгоритъма за симетрично криптиране AES.

От направеното изследване се установява, че AES осигурява висока степен на сигурност и производителност, като се наблюдава увеличение на времето за криптиране/декриптиране с увеличаване на дължината на ключа. Това потвърждава баланса между сигурност и ефективност на алгоритъма, който го прави подходящ за широк спектър от приложения.

На фигура 2.12 са изследвани и представени резултатите от комбинирането на криптографски алгоритъм AES и хешираща функция SHA с допълнителна обработка на текстовите данни. Това изследване има за цел да анализира влиянието на добавянето на текст върху производителността и сигурността на системата.

От изследването и анализирането на резултатите става ясно, че добавянето на текст към входните данни, преди тяхното хеширане и криптиране, показва положителен ефект върху сигурността, като увеличава сложността на атаките.

На фигура 2.14 е представен процесът на разбиване на хеш чрез използване на инструмент за "кракване" на хешове (Hash Cracker). Този процес се използва за преобразуване на хеш към оригиналната парола чрез техники като brute-force атаки.

В обобщение, симулационният анализ и изследването на криптографските модели доказаха, че комбинираният подход между традиционни и иновативни методи е от съществено значение за изграждането на сигурни информационни системи. Теоретичните разработки и симулационните резултати могат да послужат като основа за по-нататъшно усъвършенстване на криптографските технологии и тяхното приложение в условията на динамично променяща се киберсреда.

Глава 3 от дисертационния труд обхваща детайлно изследванията на различни уязвимости и инструменти, използвани в сферата на информационната сигурност. Съдържанието е структурирано в няколко основни секции, които разглеждат експериментални изследвания, анализи и препоръки за предотвратяване на кибератаки.

Извършено е изследване на мрежова информационна система чрез опцията TCP SYN. Установи се, че използването на SYN сканиране в мрежи със сложни защитни механизми може да предостави ценна информация за сигурността, като идентифицира активни услуги и потенциални уязвимости. Стига се до заключението, че сканирането на филтрирани портове подчертава сложността на мрежовите анализи в присъствието на защитни механизми или нестабилни мрежи. Извършено е изследване на UDP сканиране. За целта на изследването е

използвано UDP сканиране, който е инструмент за идентифициране на отворени портове и услуги, използващи протокола UDP.

Разгледани са приложенията, характеристиките и възможностите на инструмента Discover за идентифициране на уязвимости. Изследват се и потенциални противодействия при използването му. Представен е анализ на фишинг атаки, извършени чрез SEToolkit, с акцент върху начина на работа на инструмента и оценка на ефективността му. Направен е анализ на уязвимостите, свързани с PHP Code Injection, и защитните механизми, които могат да предотвратят подобни атаки. Изследвани са различни видове SQL инжекции и техните особености. Описани са и ефективни мерки за защита срещу този тип атаки, което е подкрепено с визуализации и анализи на резултатите. Представен е анализ на експлоатирането на специфични уязвимости в платформата Drupal. Обсъдени са визуализациите на SQL инжекции и препоръчителните мерки за тяхното предотвратяване. Изследвано и анализирано кодиране от тип Base64 и неговите потенциални уязвимости при неговото използване. Изследвани са XSS уязвимостите, тяхната природа, механизми на атака, потенциални последици и ефективни контрамерки.

Глава 3 завършва с анализ на резултатите от изследванията, подчертавайки ефективността на разгледаните методи и препоръчвайки практически мерки за повишаване на сигурността.

Този обзор демонстрира цялостен и систематичен подход към изследване на уязвимости и защита в информационните системи.

В четвърта глава от дисертационния труд са изследвани и представени методи за проверка и отстраняване на пропуски довеждащи до потенциален неоторизиран достъп от трети страни, с цел намаляване на атаките и подобряване на сигурността.

Извършено е моделиране на AES криптиране в средата MATLAB. Моделът на AES в MATLAB симулира криптирането и декриптирането на данни, като включва всички основни етапи на алгоритъма. Представен е криптиращия код от изследването на AES криптиране. Направено е изследване на Man-in-the-Middle атака, сценарий в който злонамерен участник прихваща, подслушва или манипулира комуникацията между две страни. Осъществено е изследване на атака тип Replay и Delay в MATLAB. За целта на изследването от типа Replay и Delay атаките се установи, че това са видове заплахи в мрежовата сигурност, при които валидни съобщения между два участника се прихващат, повтарят или се забавят от трети злонамерен участник. Представен е модел за симулация на DoS атака върху информационна система. Модела за симулация на атака тип DoS цели да направи информационна система, услуга или мрежа недостъпна за легитимни потребители, като я претовари с излишни заявки или блокира достъпа до ресурси. Даден е сорс код на модела.

Извършено е изследване на различни видове атаки в среда Matlab. Резултатите са представени графично и е даден част от сорс кода. Направена и изследвана е симулация на вероятността за успешна атака върху система чрез метод Монте Карло. Резултатите са изобразени графично, с цел анализиране поведението на атаките и защитата.

Насоки за развитие на изследванията в тази област

1. Необходимо е внедряването на нови практики за мониторинг на мрежови заявки с цел ранно откриване на уязвимости.
2. Установено е, че са идентифицирани слабости в остарели версии на Drupal, включително възможности за SQL Injection, което води до разработването на препоръки за актуализация и защита.
3. Демонстрирани са недостатъците на Base64 като криптографски метод и необходимост от разработване на насоки за използване на по-ефективни алгоритми.
4. Използването на MATLAB за визуализация на процеси като мрежови атаки, криптиране и декриптиране, ще позволява интуитивно разбиране на сложни процеси в областта на киберсигурността.

ПРИНОСИ НА ДИСЕРТАЦИОННИЯ ТРУД

1. Научно Научно приложни приноси

1.1. Изследван Изследвани, систематизирани и анализирани са съществуващи методи, техники и средства за сканиране на мрежови системи и тяхното приложение в идентифициране на уязвимости.

1.2. Извършено е моделиране на AES в MATLAB за тестване на алгоритъма, както и за разбиране на неговите ключови операции, които демонстрират устойчивостта на алгоритъма срещу атаки.

1.3. Разработени са симулационни модели за анализ на DoS, Replay, Delay и MITM атаки, които демонстрират въздействието на тези заплахи върху информационните системи.

1.4. Изследван е методът Монте Карло в MATLAB, приложен за оценка на вероятността от успешни атаки върху пароли, предоставяйки количествена оценка на рисковете.

1.5. Симулирани и изследвани са агентно-базирани модели за динамиката между атакуващи и защитни агенти, което позволява изследване на ефективността на различни стратегии за защита.

2. Приложни приноси:

2.1. Разработени и извършени са MATLAB симулации, които могат да бъдат използвани за обучение на специалисти по киберсигурност, както и за тестване на нови защитни механизми.

2.2. Представени са методи и симулации, които могат да бъдат адаптирани за анализ и защита на мрежови системи в корпоративни и институционални среди.

2.3. Създаден е структуриран процес за предварителен анализ (reconnaissance), който значително ускорява идентифицирането на слабости в сложни системи.

2.4. Създадени са методи за защита срещу SQL Injection, PHP Code Injection и OS Command Injection, базирани на анализ на валидиране, параметризирани заявки и минимизиране на привилегиите.

2.5. Изследвани са практически приложими данни за влиянието на DoS и други атаки върху мрежовата производителност, което помага за оптимизиране на защитни решения.

СПИСЪК НА ПУБЛИКАЦИИТЕ, СВЪРЗАНИ С ДИСЕРТАЦИОННИЯ ТРУД

1. **Ивайло Узунов.** Проблеми и решения свързани с последствията от кибератаките. Трета национална научна конференция “Човекът и Вселената”, Съюз на учените в България – Смолян, 25–26 ноември 2021, Научни трудове, Том III, част 3, стр. 637 – 646, ISSN:1314-9490 (online).
2. **Ивайло Узунов**, Слави Любомиров. (2022) Изследване на мрежови информационни системи по отношение на сигурността, Сборник с доклади от национална научна конференция с международно участие на тема „Образование, наука, общество“ 3-4 ноември 2022 г., ISBN 978-619-7663-43-3 (онлайн), стр. 950-961.
3. **Ивайло Узунов,** Слави Любомиров. (2022) Симулационен анализ и изследване на криптографски модели в системите за сигурност, Сборник с доклади от национална научна конференция с международно участие на тема „Образование, наука, общество“ 3-4 ноември 2022 г., ISBN 978-619-7663-43-3 (онлайн), стр. 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.