АНАЛИЗ И ОСОБЕНОСТИ НА СИГУРНОСТТА В ЕЛЕКТРОННИТЕ КОМУНИКАЦИИ

ANALYSIS OF SECURITY IN THE ELECTRONIC COMMUNICATIONS

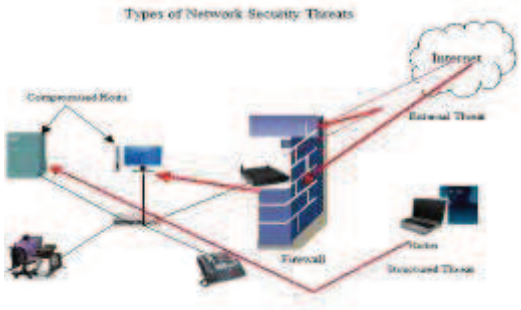
Борислав Нецов, Тодорка Георгиева

Abstract: Security is important part in constructing and building a communication network. There are many areas that are vulnerable in security and an improvement is needed. Types of malicious software are presented, compared and analyzed in the paper and suggestions of guarding the networks and user data are made.
Keywords: Mobile ad hoc networks, information security, routing.

I. ВЪВЕДЕНИЕ

Сигурността е важна част от проектирането и изграждането на всяка една компютърна мрежа. Хората, занимаващи се с кражба на онлайн информация са отлични програмисти, запознати в детайли с комуникационната техника и нейните недостатъци.. Това е предпоставка за създаване и използване на по - добра мрежова сигурност.

Лесен начин за защита на мрежа от външна атака е да се отдели напълно от външният свят. Затворените мрежи предоставят свързаност единствено на сигурни и безопасни лица и обекти, не допускат връзка с публични мрежи. Поради тази причина проектираните по този начин мрежи се считат за сигурни, но опасностите все още съществуват. С развитието на големите отворени мрежи опасностите за сигурността значително се повишават, а инструментите и приложенията за злонамерени атаки се увеличават. [1]



Фиг. 1. Типове мрежови опасности

Опасностите в социални мрежи като Facebook, Twitter и LinkedIn са голями. Те могат да се използват за професионално общуване и търсене на работа, като средство за повишаване приходите от продажби, като средство за усведомяване на общността, но също така и за връзка с роднини и приятели. Това създава предпоставки за нежелани опити за хакерски атаки към личните данни на потребителите. Тези заплахи се отнасят и за личните данни предоставени за медицински цели - преглед на резултати и снимки на пациенти и обмяна на лична информация. Злонамерен софтуер и пробив в сугурността на мрежата заплашват и интернет банкирането.

В настоящата работа е направен анализ на проблемите в сигурността в електронните комуникации, видовете заплахи, от които трябва да се страхуваме, както и препоръки и решения отнасящи се към по - безопасното използване на предоставените ни услуги.[1]

II. АНАЛИЗ

Типове злонамерен софтуер

Типовете атаки могат да включват пасивно наблюдение на комуникацията, активни мрежови атаки, близки атаки, неправомерно използване от вътрешни за мрежата лица, атаки чрез доставчика на предоставените услуги. Информационните системи и мрежи предоставят важна и атрактивна информация и трябва да бъдат устойчиви на атаки от всеки тип. Системата трябва да ограничи щетите и да бъде в състояние да се възтанови бързо в случай на атака.[1

2.1. Пасивна атака

Пасивната атака наблюдава некодиран трафик и следи за текстови пароли и важна информация, която може да се използва в други типове атаки. Тя включва трафичен анализ, наблюдение на незащитена пакетна информация, декриптиране на лошо криптиран трафик и прихващане на поверителна информация.

Фиг. 2. Пасивна атака

2.2. Активна атака

При този тип действие, атакуващият се опитва да заобиколи или да влезе в дадена защитена система. Това може да се случи чрез вируси, червеи, или троянски коне, като се прекъснат защитните функции и се въведе зловреден код и се открадне или промени информация. [2]

2.3. Разпределена атака

При този тип атака се изисква зловреден код за вграждане в даден компонент или софтуер, който по - късно ще бъде разпределен и интегриран в много други мрежи и устройства.

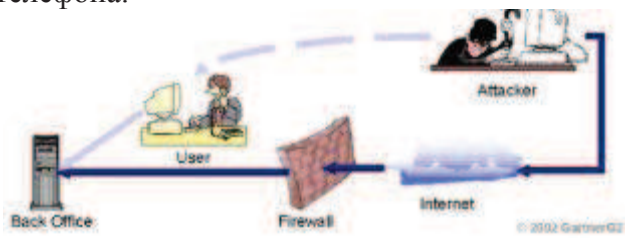
2.4. Атака отвътре

Една вътрешна атака включва някой, например недоволен служител, който атакува мрежата отвътре. Тези атаки могат да бъдат злонамерени или не злонамерени. Злонамерените умишлено подслушване, крадат, или повреждат информация; отказват достъп на потребители до мрежата. Незлонамерени атаки обикновено са резултат от небрежност, липса на знания, или умишлено заобикаляне на сигурността.[2]

2.5. Близка атака

Близка атака включва някой опитващ се да получи физически близък контакт до мрежовите компоненти, данни и системи, за да научи повече за мрежата с цел промяна, събиране, или отказ на достъп до информация.

Често срещана форма на близка атака е социалното инженерство. Нападателят компрометира мрежата или системата чрез социално взаимодействие с лице, чрез изпращане на електронно съобщение или по телефона.



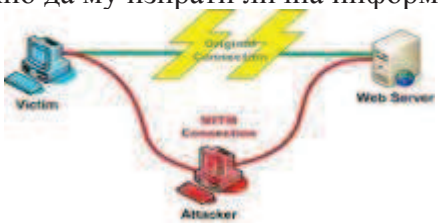
Фиг. 3. Близка атака

2.6. "Phishing" Атака

Тази атака създава фалшив уеб сайт, който изглежда точно като друг популярен сайт, например банка или PayPal. След това се изпраща съобщение по електронна поща в опит да се излъже потребителя чрез натискане върху линк, водещ до фалшивият сайт. Когато потребителят се опита да влезе вътре, данните на профила му се записват.[2]

2.7. Hijack атака (man in the middle)

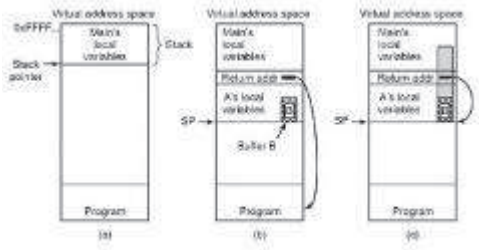
При тази атака, хакерът се включва в комуникация между двама души и изключва единият от съобщението. Другият все още вярва, че разговаря с оригиналната страна и е възможно да му изпрати лична информация.



Фиг. 4. "Man in the middle" атака

2.8. Buffer overflow (Препълване на буфера)

При тази атака атакуващият изпраща повече информация към дадено приложение, отколкото се очаква. Препълването на буфера обикновено води до придобиване на административни права до системата от страна на нападателя.



Фиг. 5. Препълване на буфер

a)работа на основна програма; b) работа на две програми; c) препълване показано в сиво

2.9. Атака чрез експлоатиране на слаби звена в системата

При тази атака, атакуващият знае за проблем в сигурността в дадена операционна система или част от софтуер и се възползва от тази уязвимост.

2.10. Атака чрез декриптиране на пароли

Нападателят се опитва да открие паролите съхранявани в мрежова база от данни или във файл защитен с парола. Съществуват три основни типа атаки: речникова, атака "груба сила", и хибридна атака. Речниковата атака използва списък файл от думи съдържащ списък на потенциалните пароли. При атаката "груба сила" нападателят опитва всяка възможна комбинация от символи.[2]

Препоръки и решения

1. Препоръки и решения към потребителите

- Използване на криптиращи методи

Потребителите трябва да използват пароли с минимална дължина от 8 символа, смяна на големи и малки букви, числа и поне един специален знак. Не трябва да използват думи от речкик и думи със сменен само един символ, рожденни дати имена от семейството, домашни любимци и имена които могат лесно да бъдат открити. Паролите трябва да бъдат променяни често.

- Инсталиране и подръжка на антивирусен софтуер

Важна препоръка е използване на антивирусен софтуер с прикрепени инструменти за почистване и прихващане на червеи, троянски коне, прихващане на фалшиви сайтове и др. На един компютър не трябва да бъдат използвани повече от един антивирус с цел избягване на нежелани действия един спрямо друг. Антивирусните програми трябва да са надежни и да бъдат обновявани редовно.

- **Използване на защитна стена**

Всички компютърни системи тябва да бъдат снабдени със защитна стена, спомагаща на антивирусният софтуер при все още незаразени системи. Защитната стена може да бъде софтуерен продукт или физическо устройство, като основното му свойство е да следи всички влизащи съобщения в системата (от интернет или от локалната мрежа) и по определен критерий да реши кои от тях са доброжелателни и кои не са.

- Контрол на физическият достъп и ограничаване на достъпа до мрежата

Трябва да бъде въведен контрол както върху физическите устройства за съхранение на информация така и върху мобилните устройсва с достъп до мрежата. Необходимо е ограничаване на устройствата в мрежата и самата мрежа до по големи мрежи с не оторизиран достъп или интернет.

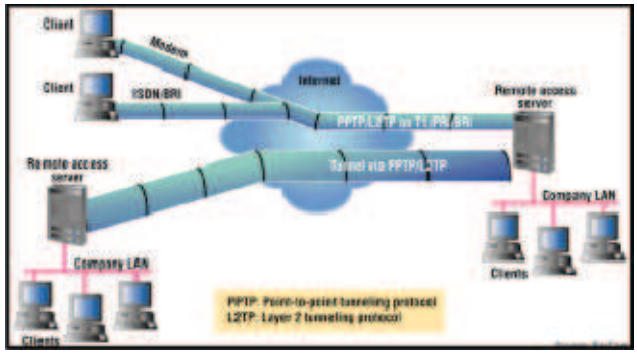
- Защита на мобилните устройства

Необходима е защита на мобилните устройства с ценна информация в тях и на мобилните устройства с достъп до мрежи с ценна информация. Тези съоръжения трябва да са защитени с пароли при достъп до тях от неоторизирани лица и обекти.[2]

2. Използване на VPN мрежи

Виртуална частна мрежа или **VPN** (от английски *Virtual Private Network*) е компютърна мрежа, логически изградена чрез криптиране, използваща физическата и програмна инфраструктура на по-голяма обществена мрежа, най-често Интернет.

Съществуват 3 основни приложения на виртуалните частни мрежи — прехвърляне на работата (аутсоурсинг) по отдалечен достъп, разширени интранет мрежи и разширени екстранет мрежи. Спестяванията, които се постигат със замяната на няколкостотин наети линии с VPN мрежи достигат до 75-80%. Виртуалните частни мрежи обикновено криптират трафика между отделните хостове в Интернет и така допринасят за информационната сигурност на използващите ги организации.[3]

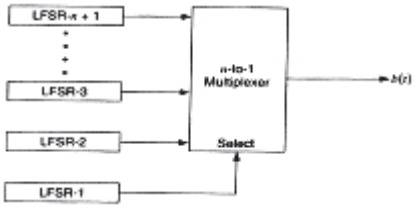


Фиг. 6. VPN мрежа

3. Използване на криптиращи механизми

Едни от най - често използваните методи за защита са линейните преместващи регистри с обратна връзка. LFSR регистрите заемат широко приложение като генератори на псевдослучайни последователности за шифриране на информацията чрез потокови шифри. Често използвани потокови шифри с тези регистри са:

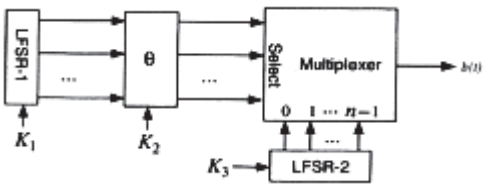
- Geffe Generator (Генератор на Гефи)



Фиг. 7. Генератор на Гефи

Генераторът използва три LFSR регистъра, комбинирани нелинейно. Два от регистрите са вход на мултиплексора, а третият контролира изхода му. Периода на генератора е най-малкото общо кратно (НОК) от периодите на трите регистъра. Въпреки че генератора изглежда добър на пръв поглед, той е слаб и се поддава на корелационни атаки.

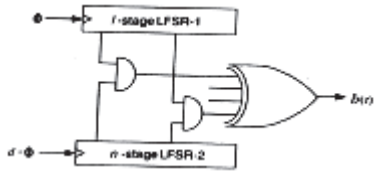
- Jennings Generator (Генератор на Дженингс)



Фиг. 8. Генератор на Дженингс

Схемата използва мултиплексор за да се комбинират два изместващи регистъра. Той е контролиран от LFSR-1 и избира един бит от LFSR-2 за всеки изходен бит. Има и функция, която насочва изхода на LFSR-2 към входа на мултиплексора.

- Бърз генератор с вътрешни произведения (Multispeed Inner-Product Generator)



Фиг. 9. Бърз генератор с вътрешни произведения

Предложен от Мейси и Руйпел (*Massey & Rueppel*), той използва два изместващи регистъра тактувани с две различни скорости. LFSR-2 се тактува ‘d’ пъти по-бързо от LFSR-1. На отделен бит от всеки от изместващите регистри се прилага логическо умножение (AND) а след това се прилага логическа схема „*изключващо или*” (XOR) на други два побитово умножени бита за да получи крайния изходен бит от генератора.

Този генератор има висока линейна сложност и притежава добри статистически характеристики. [4]

III. ИЗВОДИ

Въпреки използваните механизми за защита мрежите за електронни комуникации са уязвими по отношение на сигурността на информацията. Една от причините за това е небрежността на потребителите към личните си данни и несериозното отношение към тяхното опазване. Друга сериозна причина са остарелите методи на криптиране при комуникация. Това дава предпоставка за търсене на нови решения в областа на сигурноста и защитата на личните данни.

Използвана литература:

[1].S. V. Kartalopoulos, "Security of Information and Communication Networks", 2009.
[2]. L. Chen, G. Gong. Communication System Security, 2012.
[3].Dowd P.W., McHenry, J.T., "Network security: it's time to take it seriously", 2008
[4] S. V. Kartalopoulos, "Differentiating Data Security and Network Security", 2008

За контакти:
Борислав Нецов
Технически университет - ВАРНА,
кат. „КТТ”, 9010, Варна, ул."Студентска" № 1
e-mail: sharkiller@abv.bg
e-mail: tedi_ng@mail.bg