САЈБЕР КРИМИНАЛ И ЗАШТИТА НА ДИГИТАЛНИТЕ ПОДАТОЦИ ВО КОМПЈУТЕРСКИТЕ МРЕЖИ

Југослав Ачкоски, Методија Дојчиновски

Воена академија "Генерал Михаило Апостолски" – Скопје

Апстракт: *Појавата на новите облици на криминал, а предизвикани од развојот на информациско-комуникацискатa технологија, преставуваат предизвик на современото општевството, што значи дека во иднина се потребни големи напори со кои ќе се спречи остварување на целта на сајбер криминалот. Предводници во спречувањето на извршителите на овие дела, пред се треба да бидат институциите на системот кои ја разработуваат проблематиката за сајбер криминалот. Слободно може да се констатира дека сајбер криминалот, со своите каракеристики во иднина ќе претставува облик, кој ќе ја завзема водечката позиција во однос на останатите облици на криминал. Наведената констатација се темели на брзиот развој на инфомациско-комуникацискатa технологија, бидејќи на сите позитивните придобивки од технологијата еднакво кореспондираат и негативните. Во трудот се презентирани основите за сајбер криминалот и заштитата на дигиталните податоци во компјутерски мрежи, со цел да се даде придонес во справувањето со овој модерен облик на криминал.*

Клучни зборови: сајбер криминал, заштита на податоци, безбедност, криптографија, клучеви за шифрирање.

Abstract: *New types of crime caused by rapid development on Information Communication Technology became challenge for modern society which means that is needed to put big efforts in prevention of cyber crime in the future. Leaders in prevention should be institutions of the country which have closer points with this issue related to cyber crime. Also it is affordable to say that cyber crime with its characteristics in the future will take leader's position in comparisons with other traditional types of crime. That is based on rapid development of ICT, because all benefits from ICT for each society have also negative responds. In this paper are presented basics of cyber crime and encryption of digital data in computer networks, with aim of giving contribution in prevention of this modern type of crime.*

Key words: cyber crime, security, encryption, data protection, cryptography

Вовед

Појавата и се поголемата употреба на информациските технологии условува и појава на нови видови криминал. Компјутерите и компјутерската технологија може да се злоупотребуваат на разни начини, а криминалитетот што се извршува со помош на компјутер може да има облик како и останатите традиционални видови криминалитет, како што се кражба, прикривање, проневера, додека податоците кои неовластено се собираат со злоупотреба на информационите системи, може да се користат на разни начини за стекнување на противправна корист. Со појавата и употребата на современите технологии, извршувањето на криминални дела станува многу полесно и побрзо.

Постојат одредени проценки од НАТО алијансата, кои укажуваат на опасностите од компјутерскиот криминал, заради брзиот развој на информациско-комуникациската технологија (***engl.***ICT – Information Communication Technology) и дека истиот има транснационален карактер, при што се бришат границите помеѓу државите. Исто така, се проценува дека во иднина ситуацијата се повеќе ќе се менува во однос на моменталната, од причина што бројот на инфицирани програми, софтверски платформи и оперативни системи постојано се зголемува.[1]

Историјат на сајбер криминалот

Сајбер криминалот датира од раните седумдесетти на минатиот век, така да во текот на осумдесеттите и деведесеттите години, државите увиделе колкава е опасноста од новиот облик на криминал.

Грешката која се појавува во програмите, наречена „интернет црв“, во 1988 година има предизвикано паѓање на оперативните системи на 6.000 компјутери. Истата година бил уапсен Роберт Морис(САД) и е осуден на 400 часа доброволна работа и глоба од 10.000,00 долари. Во периодот од јуни до август 1994 година во осумнаесет напади Владимир Левин од Петроград, извлекол над 10 милиони долари од системот на Citibank, при што е уапсен е во Лондон, а за извршеното дело е осуден на 36 месеци затвор и глоба од 250.000 долари. Познатиот Кевин Митник е уапсен и осуден во 1995 година во САД заради фалсификување на 20.000 броеви на кредитни картички.[2]

Во сајбер просторот, сајбер криминалците, се почесто прават најразлични обиди не само за добивање на бенефити од државниот сектор, туку нивна цел е и приватниот сектор, при што се предизвикуваат голем број на негативни последици поради неможноста за навремено спречување на криминалните активности. Така на пример, финасискиот сајбер криминал во Австралија во 2003 година придизвикал загуби од 3,5 милиони долари, а „вирусите“, „црвите“ и „тројанците“ преку 2 милиони.[3] Следната година финансискиот

---

[1] Интернет страница http://www.maturskiradovi.net/forum/Thread-kompjuterski-kriminal

[2] Интернет страница http://www.maturskiradovi.net/forum/Thread-kompjuterski-kriminal

[3] Australian Institute of Criminology, www.aic.gov.au

сајбер криминал се намалил на 2 милиони долари, но последиците од „вирусите“ се зголемиле на преку 7 милиони. Исто така и Велика Британија во 2003 година се соочува со загуби од 120 милиони фунти, предизвикани од сајбер криминалот, а од „вирусите“ со 27,8 милиони фунти.[4] Приватниот сектор и останатите корисници почнуваат да преставуваат значаен фактор во создавањето на услови за заштита на приватните компјутерски мрежи и нивната поврзаност со глобалната интернет мрежа. Развојот на безбедна интернет инфраструктура не може да се замисли без заеднички активности на секој од овие актери, бидејќи сајбер криминалот постанува глобален проблем.[5]

Типови на сајбер криминал

Разни документи на различни начини ги класифицираат облиците на сајбер криминал. Во документите од работилницата на тема „Криминалот на мрежа“ на десетитот конгрес од ОН е констатирано дека постојат две подкатегории на сајбер криминалот[6]:

- **сајбер криминал во потесна смисла** – како секое противзаконито дејствување насочено на електронски операции за безбедност на компјутерските системи и податоците кои се обработуваат на истите;
- **сајбер криминал во поширока смисла** – како секое противзаконско дејствување поврзано за или во спрега со компјутерскиот систем или мрежа, вклучувајќи и криминал како што е незаконито поседување, нудење или дистрибуирање информации преку компјутерски системи и мрежи.

Во истите документи се наведени конкретните облици на сајбер криминалот во согласност со препораката од Советот на Европа и листата на OECD (***engl.*** Organization for Economic Cooperation and Development) од 1989 година. Тоа се:

1) неавторизиран пристап на компјутерските системи или мрежа со кршење на мерките на безбедност (hacking);
2) оштетување на компјутерските податоци или програми;
3) компјутерска саботажа;
4) неовластено пресретнување на комуникациите од и во компјутерските системи и мрежи;
5) компјутерска шпионажа.

Наведените облици на сајбер криминалот може да се преплетуваат еден со друг, при што не може да се воспостави јасна дистинкција помеѓу облиците. Така да хакингот, покрај неовластеното влегување во

---

[4] Hi-Teh crime: The Impect to UK Business, www.nhtcu.org

[5] Robinson J., Internet as the Scene of Crime, International Computer Crime Conference, Oslo,2000., www.ccips.org

[6] Tenth United Nations Congress on the Prevention of Crime and the treatment of Offenders,www.oun.org

компјутерските системи и мрежи, често опфаќа и уништување на податоци или компјутерска шпијунажа (како што е случај со упади на веб сајтови и уништување или измена на податоци на истите или хакинг и трговија со лозинки и кориснички имиња). Измената на компјутерските податоци и програми вклучува и пуштање на „компјутерски црви“ и „вируси“ што е најчесто пропратено со престанок на работа на оперативниот систем и уништувањето на податоците. Во компјутерските мрежи, црвите и вирусите во поголемиот број на случаи, се пуштаат со електронска пошта, а исто така и хакерите често го прават тоа со неовластено пристапување.

Во поширока смисла како дела извршени преку сајбер криминалот се појавуваат:

- компјутерски фалсификати;
- компјутерски кражби;
- техничка манипулација со уредите или електронските компоненти на уредите;
- злоупотреба на системот за плаќање како што се манипулација и кражба на електронските кредитни картички или користење лажни шифри во противзаконити финасиски активности.

На наведените дела во поново време се додаваат и дела поддржани од персоналните сметачи. Овие дела опфаќаат растурање на материјали или само нивно поседување, при што мрежата се користи за полесно извршување на криминалните дела или можност за избегнување на правдата. Во овие дела се вбројуваат разни противзаконски и штетни содржини, кршење на авторски права, продажба на забранета стока (оружје, крадена роба, лекови) или давање на недозволени услуги (коцкање, проституција). Најголемо внимание во оваа група на дела привлекува детската порнографија и дистрибуција на разни материјали на интернет.

Европската конвенција за сајбер криминалот (донесена на 23 Ноември 2001 година, во Будимпешта, Унгарија) предвидува 4 групи на дела[7]:

- **дела против доверливоста, интегритет и достапноста на компјутерските податоци и системи** - како што се противзаконски пристап, пресретнување, менување на податоци и влегување во системи, користење на уреди, програми и лозинки.
- **дела поврзани за компјутери** - каде фалсификувањето и кражбата се најтипични облици на напад;
- **дела поврзани за содржини –** каде детската порнографија е најчеста содржина која се појавува во оваа група опфаќајќи поседување, дистрибуција, трансмисија, чување или правење достапни на овие матријал, нивно производство заради дистрибуција и обработка во компјутерски системи или на носачи на податоци.

[7] Europena Committee on Crime Problems, European Committee of Experts on Crime in Cyber-Space, Draft Convention on Cyber-crime, April 2000., http://europa.eu.int

- **дела поврзани за кршење на авторските права –** опфаќаат репродукција и дистрибуција на неавторизираните примероци на дела во компјутерски системи.

Исто така, Конвенцијата под компјутерски систем подразбира и компјутерска мрежа.

Во Енциклопедијата за сајбер криминалот се наведува дека ФБИ (***engl.*** *Federal Bureau of Investigation*) и Националниот центар за криминал (***engl.*** *National White Collar Crime Center*) ги откриваат и пратат следните облици:

- упад во компјутерски мрежи;
- индустриска шпијунажа;
- софтверска пиратерија;
- детска порнографија;
- „бомбардирање“ со електрнска пошта;
- кражба на кредитни картички;
- крадење на лозинки;
- копирање на компјутери еден со друг, со цел да може да се пристапи на системот кој е заштитен.

Во зависност од типот на извршените дела, сајбер криминалот може да биде:

- ✓ **Политички:**
  - сајбер шпијунажа;
  - хакинг;
  - сајбер саботажа;
  - сајбер тероризам;
  - сајбер војување.
- ✓ **Економски:**
  - сајбер измами;
  - хакинг;
  - кражба на интернет услуги и време;
  - пиратски софтвери, микрочипови и бази на податоци;
  - сајбер индустриска шпијунажа;
  - измами на интернет аукции (неиспорака на производи, лажна презентација на производи, лажана проценка, зголемување на цена на производите, трговија со стока на црн пазар.)
- ✓ **Производство и дистрибуција на недозволени и штетни содржини:**
  - детска порнографија;
  - педофилија
  - верски секти;
  - ширење на расистички, нацистички и слични идеи и ставови;
  - злоупотреба на жени и деца;
  - манипулација со забранети производи, супстанци и роба;
  - дрога;
  - човечки органи;
  - оружје.

- ✓ **Повреда на сајбер приватност:**
  - надгледување на имејл пошта;
  - спам;
  - фичинг;
  - прислушкување, снимање;
  - пратење на е-конференција;
  - прикачување и анализа на "cookies"

Јасно е дека големиот број на различни класификации сам по себе ја покажува разновидноста на овие дела и комплексноста на нивните појавни облици, но и разликите во критериуми кои се користат. Во секој случај покрај нападите во компјутеските системи и мрежи, шпијунажа, саботажа, пиратерија, бомбардирање на електронска пошта со добивање на несакани пораки, обиди за откривање на лозинка, лажно преставување на компјутери на еден за друг, тука се вбројуваат и вирусите, односно нивно креирање и дистрибуција, а исто така свое место заземаат недозволени и штетни содржини почнувајќи од детска порнографија до растурање на верски, расистички и слични содржини. Посебно се бројни делата за десиминација на недозволена стока или пружање на недозволени услуги. Во ист контекст треба да се додадат и сајбер саботажата и тероризмот, како и кражабата на интернет време, услуги, идентитет, разни злоупотреби и кредитни картички.
Неоспорно е дека сајбер криминалот е повеќе врзан за активности на поединец. Криминалот врзан за компјутерските мрежи е повеќе дело на органинзирани групи од професионалци, специјализирани во нивната област (пр. групата *Phonemasters* станува позната заради честите напади на американските Национални информациони центри за криминал и како втора причина е вклучувањето во својот состав Канаѓани и Швајцарци, покрај Американци,). Овие групи од една страна се "традиционални" групи на организиран криминал, кои се усовршиле и софистицирале со примена на информациско комуникациска технологија и на тој начин се подготвувиле да ги извршуваат своите дела искористувајќи го сајбер просторот. Од друга страна, се појавуваат посебно организирани сајбер групи – сајбер мафија. Сајбер групите имаат свои правила, друг начин на однесување за разлика од конвенционалните криминогени групи, како што се спецификите на опкружувањето. Активностите на ваквите групи се многу олеснети заради спецификите на опкружувањето во кое делуваат и оружјето кое го користат. Опкружувањето е виртуелно, оружјето е информационо, а знаењето е специјализирано.

Интернационализам, транснационалност, мултидимензионалност се само некои од својствата на сајбер групите. Нивната организациона структура не е ни малку едноставна, од причина што не постои континуитет или одредена константа, односно се е променливо, што истото не е случај со

останатите облици на организиран криминал, што уште повеќе ја потврдува сликата за нивната посебност. [8]

Заштита на дигиталните податоци

Дигиталините податоци се заштитуваат од: неовластен пристап, недозволено копирање и понатамошно дистрибуирање и докажување на автентичноста на податоците. Механизмите за заштита може да се поделат во неколку групи:

- механизми кои се однесуваат на заштитата и обезбедувањето на идентитетот на корисниците, според кои се врши доделување на права на пристап за одредени ресурси на ниво на системот;
- механизми поврзани со правата и привилегии на сопствениците и администраторите на ниво на системот кои одредуваат дали корисниците имаат дозвола да пристапат на одредена содржина без повреда на тие права;
- механизми на енкрипција, кои ја менуваат дигитализираната граѓа да биде читлива само на оние корисници кои легално набавиле клуч за декрипција;
- механизми за трајно шифрирање (*engl. persistent encryption*), кои овозможуваат употреба на граѓа за корисници, каде системот ги декриптира само оние делови кои се моментно потребни, а останатите остануваат криптирани;
- механизмите на дигиталните потписи и дигиталните водени жигови кои вградуваат информација за корисникот или сопственоста на дигитализираната граѓа.

Криптографија

Целта на криптографијата е заштита на дигиталните податоци од неовластено користење, при што содржината на информациите се менува и станува нечитлива. На тој начин се врши нивното заштитување сè додека не се изврши обратна операција и да се добијат оригиналните податоци. Процесот на енкрипцијата се користи за:

- осигурување на приватноста и тајноста на податоците;
- осигурување на интегритетот на податоците;
- можност за утврдување на автентичноста или идентификација - утврдување на идентитетот на личноста, компјутерскиот терминал, кредитна картичка и т.н.;
- можност за утврдување на автентичноста на пораката - утврдување на веродостојноста на изворот за информации;
- можност за вградување на дигитален потпис во пораката;
- можност за авторизација - можност за пренос на овластувањето на друго физичко или правно лице;

---

[8] **CYBER KRIMINAL,** Mirjana Drakulić Ratimir Drakulić, *Fakultet organizacionih nauka u Beogradu*

- можност за издавање на дигитално уверение - потврда дека информацијата доаѓа од проверен извор;
- можност за сведочење - потврда на создавање или постоење на одредена информација;
- можност за издавање на сметка - потврда за примање на информацијата;
- можност за потврдување - потврда за давање на одредена услуга;
- можност за доделување на сопственички права - доделување на доделување права на некое физичко или правно лице за користење и/или понатамошна продажба на граѓата;
- осигурување на анонимноста;
- осигурување на неможноста за одбивање на некоја, претходно договорена обврска;
- осигурување на можноста за отповикување на авторизацијата и уверението[9]

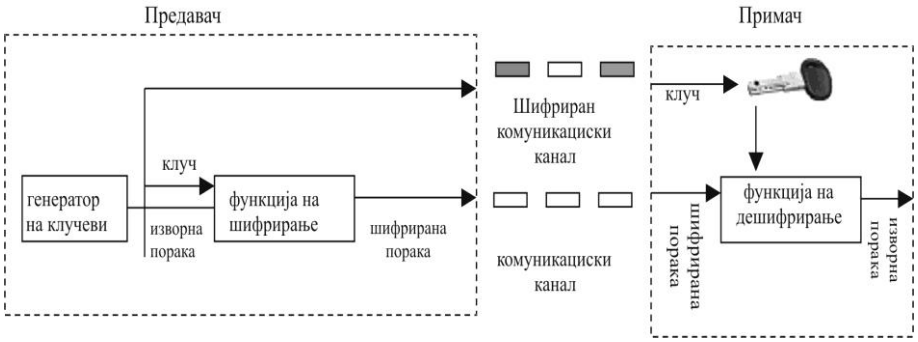
За да се изврши криптирање на податоците, потребно е тие да бидат во дигитализиран запис. За енкрипција на дигитализираниот запис се користи клуч за шифрирање, со кој се преобликува записот да не биде препознатлив, при што без познавање на клучот не може да се врати во својот изворен облик. Постојат два начини на шифрирање на дигиталините податоци: шифрирање со користење на симетричен клуч (*engl. symmetric - key encryption*) и шифрирање со користење на јавен клуч (*engl. public - key encryption*).

Шифрирање со симетричен клуч

Кај шифрирањето со симетричен клуч, истиот клуч се користи за шифрирање и дешифрирање на пораки, односно дигиталните податоци се праќаат по комуникациски канал. Таквиот систем се состои од три дела: генератор на клучеви, функции на шифрирање и функции на дешифрирање. Процесот се извршува на следниот начин. Прво предавачот го стартува генераторот на клучеви - програма која доделува единствен клуч за шифрирање на пораката. Секој клуч се користи за едно шифрирање. Потоа се стартуваат функциите за шифрирање, кои како влезни вредности ја имаат изворната порака и клучот за шифрирање. Таа функција ја преобразува пораката соодветно на клучот, а како резултат се добива шифрирана порака. Потоа, пораката преку комуникацискиот канал се испраќа до примачот. Примачот, кој треба да го познава клучот, во тој момент ги стартува функциите на дешифрирање, кои како влез ги имаат шифрираната порака и клучот за шифрирање. По внатрешното преобразување, функцијата резултира со изворна порака која за примачот е читлива.

[9] Stancic, 'Digitalizacija grage"

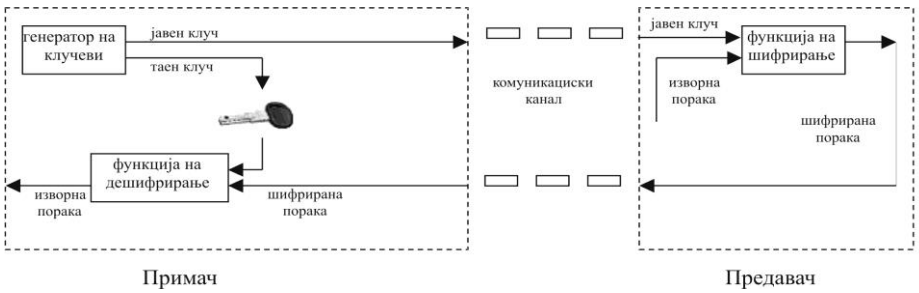
Тајноста на клучот е многу важна, бидејќи секој кој знае може да ја дешифрира пораката. Врз основа на тоа, главен проблем претставува како да се достави клуч до одреден корисник, без опасност да се дознае при преносот. Еден од начините за доставување на клучеви може да биде по пат на заштитен комуникациски канал. Целата порака не се пренесува преку заштитен комуникациски канал заради брзината на преносот. Заштитениот комуникациски канал е обично канал со помала пропусност. Од тие причини лесно може да се испрати клуч за шифрирање, заради малата големина и потоа целата порака по добивањето на клучот, може лесно да се препрати преку незаштитениот, јавен канал.



Слика 3.23: Постапка на шифрирање и дешифрирање со употреба на симетричен клуч

Шифрирање со јавен клуч

Оваа техника на шифрирање користи два вида на клучеви - јавен клуч и приватен клуч. Овие два клуча имаат единствено својство: пораката шифрирана со јавен клуч може да се дешифрира единствено со соодветен приватен клуч. Овој систем, исто така се состои од три дела: генератор на клучеви, функции на шифрирање и функции на дешифрирање. Процесот на шифрирање и дешифрирање се одвива на следниот начин. Прво примачот го стартува генераторот за клучеви - програма која доделува единствен пар на јавен и приватен клуч. Тогаш примачот јавно го објавува (на Интернет, во весници и сл.) или директно го доставува на предавачот својот јавен клуч, а приватниот клуч строго го чува. Предавачот ја стартува функцијата на шифрирање која како влезна вредност има изворна порака и јавен клуч на примачот. Шифрираната порака по пат на комуникациски канал се праќа на примачот. Така шифрираната порака може да ја дешифрира единствено сопственикот на приватниот клуч кој одговара на јавниот клуч со кој пораката е шифрирана. Примачот ја стартува функцијата за дешифрирање која како влезна вредност има шифрирана порака и приватен клуч, односно како резултат се добива изворна порака.



Слика 3.24: Постапка на шифрирање и дешифрирање со употреба на јавен клуч

Кога ќе се споредат методите за енкрипција со симетричен и јавен клуч може да се заклучи дека методата со јавен клуч е многу побезбедна, бидејќи клучот за дешифрирање не се пренесува, при што можноста за негово откривање е многу помала. Тајниот клуч на некој начин е одреден со јавниот клуч, но за негово откривање врз основа на познавањето на јавниот клуч треба да се примени метода со „груба сила“ (*engl. brute force*), т.е. начинот на кој се испробуваат сите можни комбинации додека не се погоди вистинската, меѓутоа со денешниот развој на компјутерите тоа би барало многу време.

Заради тоа може да се направи комбинација на овие два методи, каде што, може да се употреби шифрирање со симетричен клуч, а клучот кој се доставува на примачот се шифрира со техника на јавен клуч. Со оглед дека техниката на шифрирање со јавен клуч бара повеќе процесорско време споредено со шифрирањето со симетричен клуч, со ваквата комбинација се добива на брзината и истовремено се зголемува сигурноста.

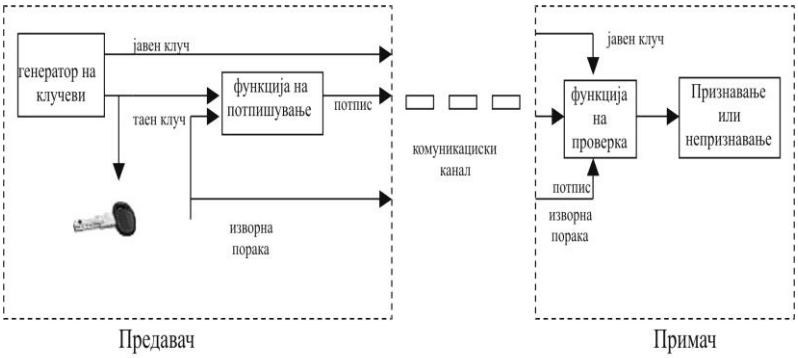
Дигитални потписи

Дигиталниот потпис го одредува идентитетот на учесникот во електронска размена на податоците и обезбедува интегритет на податоците. [10]Системот на дигиталните потписи се базира на технологијата на шифрирање со јавен клуч. Дигиталниот потпис е бинарна низа која се додава на документи за да се потврди неговата точност и исправност. Бинарната низа е изведена од тајниот клуч на потписникот на документот.

Дигиталните потписи функционираат на ист начин како и класичните потписи на хартиените документи. Така, во хартиен облик, одредената личност со својот потпис сведочи за точноста и исправноста на некој документ. Потписот е единствено обележје на секој човек и е зависен од личноста која потпишува. Наспроти тоа, дигиталните потписи може да се гледаат како функција на личноста која го потпишува и потпишаниот документ. Разликата се состои во тоа што кога една личност потпишува повеќе дигитализирани документи, сите потписи се разликуваат, додека за

[10] Strategija razvitka Republike Hrvatske, “Hrvatska u 21. stoljecu ”, Informaciska i komunikaciska tehnologija, Vlada R. Hrvatske, 2000, <http://www.hrvatska21.hr>, 2001

потпишувањето на хартиените документи не е тоа случај. Тоа мора да биде така зошто дигиталните потписи како бинарни низи, се праќаат со пораката, бидејќи ако истиот потпис би се користел за повеќе документи, секој кој добил од тие документи со дополнителна бинарна низа може да ја додаде на некој друг документ, т.е. да се потпише некој друг, и таквиот документ да се прати понатаму.



Слика 3.25: Постапка на дигитално потпишување

Системот за дигитално потпишување се состои од три дела: генератор на клучеви, функции на потпишување и функции на проверување. Процесот се одвива на следниот начин. Личноста која сака да потпише некој дигитален документ најнапред го стартува генераторот на клучеви со што добива единствен пар на јавен и приватен клуч. Потоа ја стартува функцијата на потпишување, која како влезна вредност има дигитален документ и таен клуч, при што како резултат се појавува дигитален потпис. Така потпишаниот документ, со почеток на јавниот клуч, предавачот по пат на комуникацискиот канал го доставува на примачот или јавно го објавува. Примачот на документите кој сака да ја провери автентичноста на документите мора да ја стартува функцијата за проверка која како влезна вредност има документ, дигитален потпис и јавен клуч. Функцијата за проверка резултира со признавање или непризнавање на изворниот дигитален потпис.

Дигитални сертификати

Со оглед на тоа, дека дигиталниот потпис го одредува идентитетот на учесникот во електронската размена на податоци потребно е издвојување на дигитални сертификати, т.е. дигитална потврда со која се докажува идентитетот (*engl. identity certificate*) за да примачот на податоците може да го провери идентитетот на предавачот. Сертификациониот авторитет (*engl. CA - certifying authorities*) е служба која издава дигитална потврда за идентитетот, таа поседува овластување со што дигиталните потврди имаа кредибилитет.

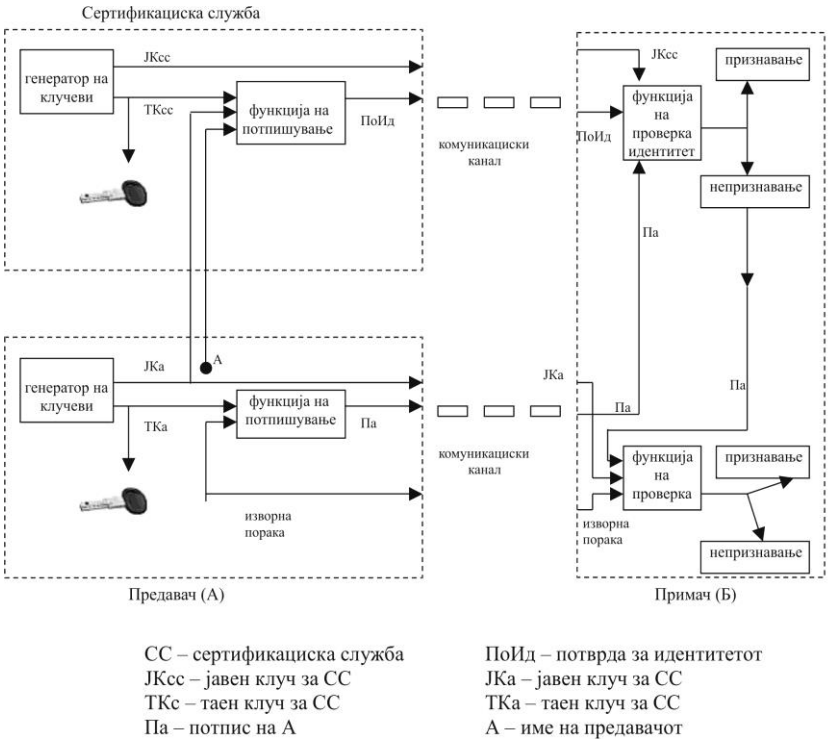
Проблемот на дигиталните сертификати и нивниот идентитет, се сведува на развој на инфраструктурата за управување на јавните клучеви. Сертификациониот авторитет издава потврда за идентитетот, при што ја потпишува со свој клуч за потпишување. Потврда за идентитетот на некоја личност, односно дигитално потпишан бинарен запис содржи јавен клуч и име на сопственикот, а може да содржи и некои податоци како "рок на употреба", т.е. информација во кој временски период јавниот клуч е валиден. Кога примачот го има јавниот клуч од сертификациониот авторитет, тогаш може врз основа на довербата во авторитетот да верува во исправноста на потврдата за идентитетот која таа го издала, а препознавајќи го јавниот клуч на личноста која е во потврдата, може да верува во фактите дека таа личност му ги пратила податоците кои ги примил.[11]

На пример, примачот Б примил документ кој го потпишала личноста А заедно со потврдата за идентитетот во која се наведува името на А и соодветниот јавен клуч. Примачот тогаш го користи јавниот клуч издаден од авторитетот за може да ја провери вистинитоста на дигиталниот потпис на потврдата за идентитетот. Ако вистинитоста е потврдена, тогаш примачот може со целосна доверба да го искористи јавниот клуч на личноста А, со што се утврдува дека личноста А го потпишала приемниот документ. Довербата на примачот во авторитетот значи негова доверба за вистинитоста на нејзиниот јавен клуч, доверба со која се докажува дека авторитетот навистина и доделила јавен клуч на личноста А.

Сегментот за верифицирано управување со јавните клучеви, т.е. издавање на потврда дека зад одреден јавен клуч и име, е личност за која се потврдува нејзиниот идентитет. Многу е важно за проверката на примачот, дали наведената институција го доставила одредениот документ, може ли да се верува дека документот е идентичен на оригиналниот, т.е. дали некој неовластен не го променил. Овој сегмент е исто така важен при потпишувањето на дигиталните договори кога двете договорените страни можат да се наоѓаат во два различни града или пак на две различни страни на светот, а мораат да имаат доверба дека другата потпишана страна е таа вистинската.

---

[11] National Academy of Sciences, "The Digital Dilemma. Intellectual Property in the information Age", USA, National Academy Press, 2000, http://books.nap.edu/html/digital _dilemma>, 2000



Слика 3.26: Постапка за употреба на дигитални сертификати

Дигитални водени жигови

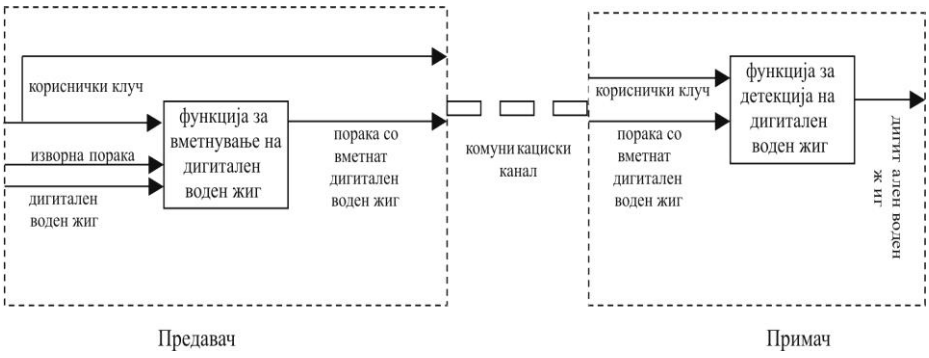
Дигиталниот воден жиг е сигнал кој е додаден на дигиталната граѓа со намера да се пренесе, одредена мала, количина на информација. Со детекција на присутност или неприсутност на воден жиг може да се докаже автентичноста или неавтентичноста на дигитализираната граѓа. Тие главно се користат за обележување на сликовната, звучната или видео граѓата. Постојат различни примени на дигиталните водени жигови кои најчесто се следните:

- докажување на сопственоста на некоја содржина;
- вметнување на податоци за примачот (*engl. fingerprinting*), за да може да се утврди од каде е потеклото на евентуалната нелегална копија;
- проверка на автентичноста и интегритетот;
- опишување на содржината (*engl. content labeling*);
- контрола на користење;
- заштита на содржината.[12]

[12] National Academy of Sciences, "The Digital Dilemma. Intellectual Property in the information Age", USA, National Academy Press, 2000, http://books.nap.edu/html/digital _dilemma>, 2000

Дигиталните водени жигови може да бидат видливи или невидливи за корисниците, а по обликот „меки“ (*engl. fragile*) или робусни (*engl. robust*). Видливите дигитални водени жигови се појавуваат во облик на логотип или порака на видливо или чујно подрачје од дигитализираната граѓа, кои на корисниците им служат како информација за сопственост или дозвола за користење. Некои институциите користат ваков вид на жигови за слободна дистрибуција на материјалот со низок квалитет за професионална употреба, а ја наплаќаат граѓата со висок квалитет. Невидливите жигови може да се користат како доказ за нелегално користење на дигиталните документи. Меките дигитални водени жигови не се постојани при обработка на дигитализираните документи, при што се користат за да се детектираат евентуалните измени на документите. Во моментот на преземање на дел од оригиналниот документ не е возможно да се докаже неговото потекло. Робусните водени жигови се провлекуваат низ целиот дигитален запис, при што неговите делови може да се детектираат и покрај тоа што се вградени и вклучени во некој документ.

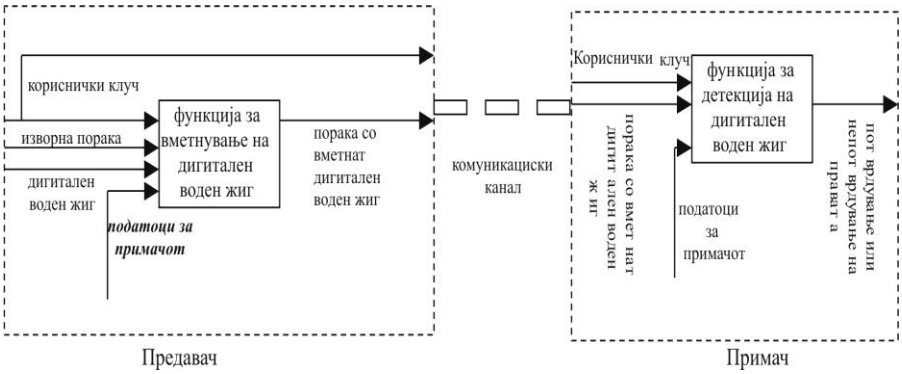
Системот на дигиталните водени жигови се состои од два дела: функции за вметнување на жигот и функции за детекција на жигот. Процесот се одвива на следниот начин. Предавачот на дигитализираниот документ ја стартува функцијата за вметнување на жигот која како влезна вредност го има изворниот дигитален документ, дигиталниот воден жиг и корисничкиот клуч, а како резултат се добива документ со вметнат дигитален воден жиг. Потоа, заедно со клучот се проследува таквиот документ на примачот, кој ако сака може да го детектира жигот. За да може да го детектира, примачот мора да ја стартува функцијата за детекција на жигот. Таа како влезна вредност има кориснички клуч и примен документ, а како резултат се добива дигитален воден жиг со што потврдува неговата автентичност или пак се негира.



Слика 3.27: Систем на дигитален воден жиг

За процесите, каде што се вметнуваат податоци за примачот на дигиталниот воден жиг, постои дополнителна влезна вредност, односно шифра на корисник, со која на единствен начин се одредува примачот, т.е. корисникот на кој е дозволена употреба на одреден дигитализиран документ.

Во тој случај како излезна вредност на функцијата за вметнување од жигот се добива дигитализиран документ со вметнат дигитален воден жиг и податоци за примачот. Функцијата за детекција на жигот тогаш како дополнителна вредност има шифра на корисник, а резултира со потврдување или негирање на правата на користење на одреден примач. Процесот за вметнување на податоците за примачот е својствен за робусните дигитални водени жигови.



Слика 3.28: Систем на дигитален воден жиг со вметнување на податоци за примачот

Шифрирани обвивки

Шифрираните обвивки (*engl. cryptographic envelopes*) се создадени како систем за засилена заштита на пренос и користење на дигитализираната граѓа. Овој систем користи шифрирана дигитална меморија која содржи изворна порака, изјава за правата на пристап и користење на пораката, а исто така може да содржи дигитален воден жиг како и дигитален воден жиг со вметнати податоци за примачот.

Користењето на пораката од страна примачот, мора да биде одобрено од софтвер кој го проверува правото на користење. Таквиот софтвер се користи на сервер . Исто така треба да изврши дешифрирање само на оној дел од пораката кој моментално се прегледува, со што се зголемува заштитата. Со системот на шифрирани обвивки се овозможува лесна достапност до дигиталните податоци, без загрозување на финансиските интереси на институцијата, како сопственик на граѓата, заради можна неовластена дистрибуција на копии.

Спротиставување на сајбер криминалот

Сајбер криминалот заради спецификите, општествената опасност што ја предизвикува и високата стапка на раст, во се поголема мера станува многу озбилен општествен проблем и тоа не само во национални туку и во меѓународни размери. Врз основа на наведените причини потребна е соодветна акција заради успешно спротиставување на новото општествено зло. Постојат три типа на механизми, кои може да помогнат во одговор на

предизвиците на сајбер криминалот: алатки за заштита, етика и закони. Овие механизми имаат превентивен и репресивен карактер, при што во нивната примена изразита предност мора да се даде на превентивните во однос на репресивните мерки.

Тенденција за зголемување на овој облик на криминал покажуваат и некои статистички податоци. Врз основа на податоците претставени од експертите на компанијата Sophos, во текот на 2007 година биле откриени 6.000 заразени веб страници, од кои 83% припаѓале на компании. Бројот на имејл заканите има тенденција на опаѓање, но обратнопропорционално се зголемува бројот на имејли кои содржат линкови кои водат до малициозни интернет страни.[13]

Голем проблем во сузбивањето на сајбер криминалот претставува фактот дека цел на извршителите е се што се поврзува на интернет, односно освен персоналните сметачи, тука се вбројуваат и мобилни телефони, iPhone, iPod Touch, терминали и други уреди кои се конектираат на интернет постојано или повремено. Според одредени сознанија, постојат и обвинувања, дека одредени држави се појавуваат како нарачатели на сајбер криминалот.[14] Врз основа на претходно изнесеното, може да се заклучи дека сајбер криминалот во иднина се повеќе ќе биде застапен, во однос на останатите видови на криминал.[15]

Земајќи го во предвид претходно наведеното, потребно би било превземање на следните мерки:

- заради општествената оправданост и целисходност, како и заради следење на општествените трендови и приклучување кон западноевропските држави, потребно е забрзување на активностите за донесување и усвојување единствени основи за заштита на автоматизираните информациони системи;
- од аспект на заштитата, една од најважните активности на која би требало да се посвети посебно внимание е изградба и развој на етички норми и принципи во доменот на информатиката;
- ревизија на кривичниот закон и негово прилагодување на новите појавни облици на општествено опасно однесување предизвикано од информацискатa технологија;
- нова систематизација и трансформација на телата или органите кои ја пратат состојбата во оваа област, извршуваат анализи на појавите, ги истражуваат причините, извршителите и методите и предлагаат соодветни мерки и акции за спречување, откривање, разјаснување и докажување на овие видови на кривични дела.[16]

---

[13]Интернет страница http://www.maturskiradovi.net/forum/Thread-kompjuterski-kriminal

[14]Интернет старница http://www.nezavisne.com/nauka-tehnologija/internet/Potrebni-ostriji-zakoni-za-sajber-kriminal-69298.html

[15]Интернет страница http://www.maturskiradovi.net/forum/Thread-kompjuterski-kriminal

[16]Sajber krize, Akademija za Bezbednost i Diplomatija, Beograd, 2009, http://www.scribd.com/doc/35038693/Cyber-Krize

ЗАКЛУЧОК

Бројните и разновидни потенцијални закани кои ги загрозуваат информационите системи во институциите, организациите и компаниите, а посебно оние кои имаат карактер на криминални дела, недвосмислено ја наметнуваат потребата за изградба на соодветни системи за заштита на дигиталните податоци во компјутерските мрежи. Во ниеден момент не смее дасе заборави на фактот дека не постои апсолутна заштита и дека секој информационен систем е изложен на ризици, но со навремено дејствување, големината на постоечкиот ризик, можно е да се доведе во прифатливи граници.

Особено значаен е аспектот на едукација и обичување на персоналот како и оспособување на носителите на КИС, во спротивставувањето на појавните облици како и идентификувањето феноменолошките и етиолошките карактеристики на компјутерскиот криминал.

ЛИТЕРАТУРА

[1] Cyberstalking, Anatomy of a Predator, www.cyberangels.org

[2] Robinson J., Internet as the Scene of Crime, International Computer Crime Conference, Oslo,2000., www.ccips.org

[3] Tenth United Nations Congress on the Prevention of Crime and the treatment of Offenders,www.oun.org

[4] Europena Committee on Crime Problems, European Committee of Experts on Crime in Cyber-Space, Draft Convention on Cyber-crime, April 2000., http://europa.eu.int

[5] United Nations office at Vienna, Global studies on organized crime, 1999., www.oun.org

[6] Communication from the Commission to the Council, The European Parliament, The Economic and Social Committee and Committee of the regions, Creating a Safer Information Society by Improving the Security of Information Infrastructures and Combating Computerrelated Crime, http://europa.eu.int

[7] Directive 2000/31/EC of the European Parliament and of the Council of 8 June 2000 on certain aspects of Information Society services, in particular electronic commerce, in the Internal Market, http://europa.eu.int

[8] The Prevention and control of organised crime: A European Union strategy for the beginning of the new Millennium (OJ 2000 C124, 3.5.2000).

[9] Legal Aspects of Computer-related Crime in the Information Society – COMCRIME, http://europa.eu.int/ISPO/legal/en/crime/crime.html.

[10] Australian Institute of Criminology, www.aic.gov.au

[12] Hi-Tech crime: The Impact to UK Business, www.nhtcu.org