ОДБРАНА

СПЕЦИЈАЛНИ ПРИЛОГ 70

Криминал у сајбер простору

КРИМИНАЛ У САЈБЕР ПРОСТОРУ

Пише
Милорад МАРКАГИЋ

Злоупот напретк

Технолошки развој коме се не могу сагледати последице омогућио је, заједно с другим узрочницима, стварање „data heaven-a“ – раја за крађу података и „criminal heavena“ – криминалног раја, нарочито у мање развијеним друштвима, с непостојећом или непотпуном правном регулативом у области рачунарског криминала. Процене Интерпола говоре да је штета настала компјутерским криминалом одмах иза штета насталих трговином дрогом и оружјем.

Сви људски афинитети, интелигенција, образовање и различитост међу појединцима добијају на значају тек у комуникацији са другим људима и окружењем у коме живимо. Све до средине 15. века комуникација се сводила на основне елементе, говор и писмо, а после тога развијају се и други видови комуникације, коришћењем разних и све савршенијих техничких средстава. Светска информацијска и информациона револуција у комуникацији међу људима доживеле су неслућени технолошки бум тек проналаском и развојем модерних информатичких и комуникацијских уређаја, уређаја и мрежа којима се уносе, обрађују и чувају подаци и преносе слика, говор, звук и сигнали у дигиталном облику. За разлику од информацијске, информатичка револуција обухвата сва она технолошка решења која се остварују коришћењем техничких помагала и технолошких решења.

Информатичка револуција

Технолошка, а самим тим и информациона револуција почиње 1440. године, проналаском и првом употребом Гутенбергове машине за штампање, па је тако 1455. први пут штампана „Библија”, што се сматра почетком масовног ширења писмености у свету. После периода затишја, од око два века, долази до појаве и увођења у масовну употребу нових техничко-технолошких достигнућа: телеграф 1840. (Морзе), телефон 1875. (Бел), 1891. прва филмска представа, 1909. радио и иконоскоп 1926. који отвара пут савременој телевизији.

Истовремено се стварају предуслови за информатичку револуцију (1833. када се развија аналитички уређај и постављају теоријске основе за рад савремених рачунара, 1944. када је конструисан рачунар МАРК-1 и, од педесетих година 20. века, када почиње производња компјутера за комерцијалну обраду података).

Развој рачунарске технологије пратио је развојна достигнућа на пољу електротехнике, електронике и теоријских сазнања на пољу ки-

бернетике. Историјски развој рачунара може се посматрати у неколико етапа, у зависности од тога како су се уводиле новине у развоју телекомуникационих и информатичких средстава и система. Прва фаза траје од 1951. до 1958, када се у обради и преносу података користе електронске цеви и кабловске везе. Друга наступа 1959, када у масовну употребу улазе транзистори и магнетна језгра. Трећа фаза, у којој се развија технологија интегрисаних кола и почиње коришћење виших програмских језика, траје од 1964. до 1970, да би у следећој, од 1971. до 1987, дошло и до интеграције полупроводничких елемената. Пета фаза односи се на период од 1989. до 1992, када долази до развоја паралелне архитектуре и арсенид чипова и, на крају, у шестој фази, од 1993. године, усавршавају се неурокомпјутери на бази неуронске мреже и долази до развоја и експерименталне примене вештачке интелигенције.

У односу на претходна раздобља људско знање се нагло удвостручава у све краћим периодима. На пример од 1900. до 1950. знање је двоструко повећано, да би до наредног удвостручења дошло већ до 1960. године. То је и основни показатељ уласка човека у раздобље научнотехнолошке револуције. Разумљиво је да централно место и улогу у том процесу има чип. Такође, почиње употреба микропроцесора – једног или неколико повезаних чипова који делују као самостални рачунар.

Велике наде полажу се у скори проналазак и развој савршеног биочипа, који делује слично као људски мозак, што представља подлогу за развој вештачке интелигенције, увођење масовне роботизације и дигиталне универзалне комуникације.

Глобалне мреже

Ниво развоја који је данас достигнут у области рачунарске технике омогућава повезивање компјутера у мреже и њихово глобално повезивање у јединствену комуникацијско-информацијску мрежу – интернет. На тај начин створено је и плодно тло за злоупотребу, односно развој и ширење компјутерског криминала, мада су неки појавни облици злоупотребе постојали и пре стварања и развоја глобалне мреже.

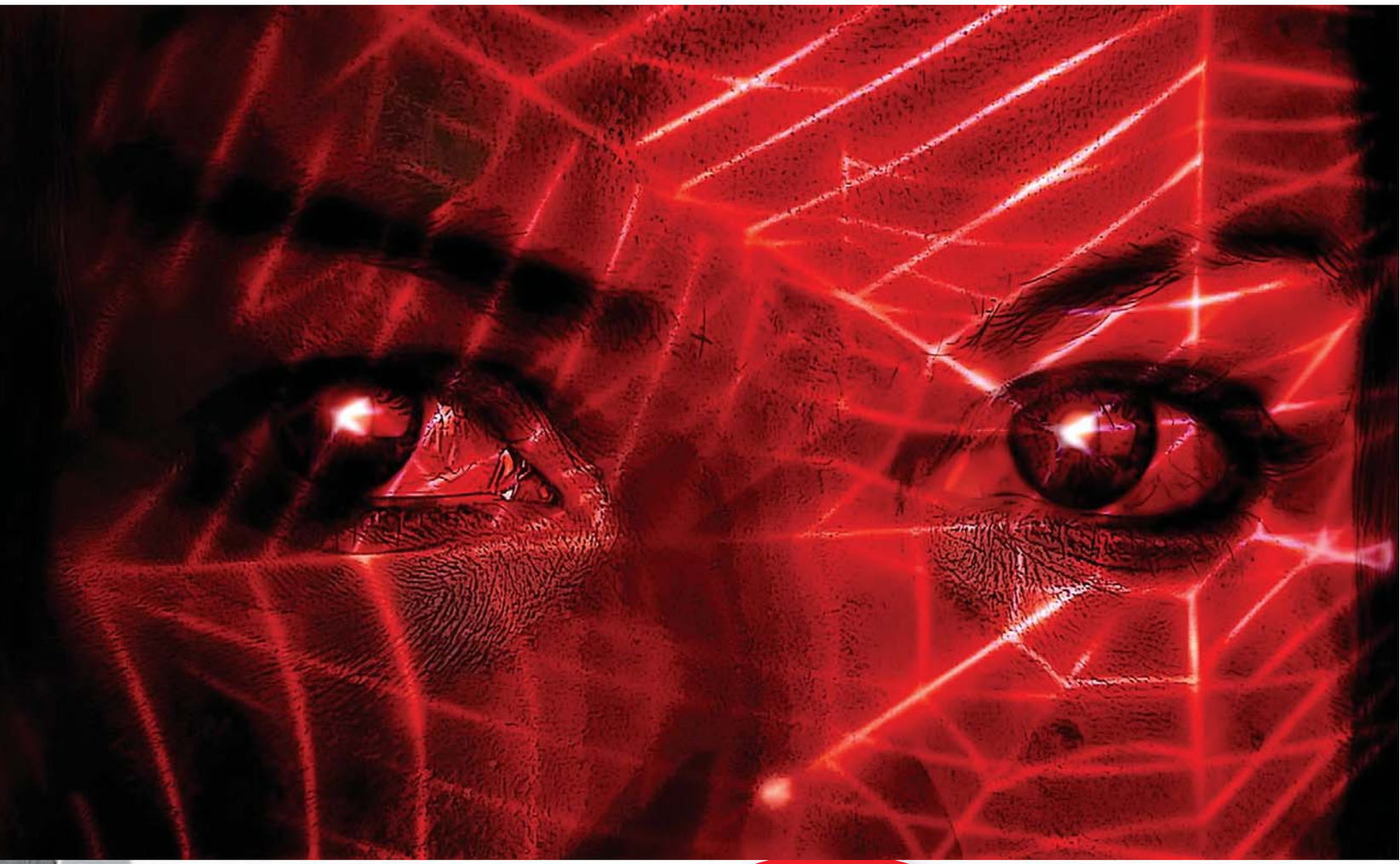
Технолошки развој коме се не могу сагледати последице омогућио је заједно са другим узрочницима стварање „data heaven-a“ (рај за крађу података) и „criminal heavena“ (криминални рај), нарочито у мање развијеним друштвима, с непостојећом или непотпуном правном регулативом на подручју рачунарског криминала.

По неписаном правилу, проблемима се приступа и они се решавају тек када наступе знатне штете и видљиве последице по појединца, организацију или систем у целини. Такође, указала се потреба да се променама управља како би се задаци те фазе развоја што брже и са што мање жртава остварили и превазишли, за шта је потребно ујединити више наука и научних области, те створити солидну законодавну основу која регулише употребу и санкције злоупотребе киберпростора.

Централно и основно питање није ко користи и управља данашњицом, већ првенствено ко усмерава, креира и уобличава будућност.

УКЛАЊАЊЕ ДОКАЗА

Починиоци рачунарских напада не остављају доказе о неовлашћеном приступу. Анонимност је један од темеља компјутерског криминала и основни разлог зашто га је тако тешко открити, спречити и сузбијати. Нападачи из логичких датотека настоје да уклоне податке о свом приступу и коришћењу јер се свака активност у њима бележи (дневник рада који бележи сам компјутер, односно његов оперативни систем). Некада настоје и да осигурају слободан поновни приступ тако што остављају задња врата и замке.



Деловање алгоритма

Приликом дефинисања информацијских мрежа честа су и оправдано постављана питања – који је циљ, које су им функције и од чега се састоје.

Основни циљ постојања сваке информацијске мреже јесте да достави информацију на право место, у право време и уз минималне утрошке и улагања временских и финансијских ресурса.

Свака мрежа састоји се од улаза, излаза, процеса и повратне везе. Постоје три стања у којима се може наћи информацијска мрежа: када има само улаз – информисана мрежа; када има само излаз – информишућа мрежа; и када има и улаз и излаз – потпуна информацијска мрежа (у пракси углавном и постоје само такве мреже).

Управљање је најважнија функција и особина сваке информацијске мреже, па од тог процеса зависи функционисање читаве мреже. Било која мањкавост и непотпуност у формирању и деловању мреже, или недостатак информација о томе има за последицу недовољну организованост, где се и ствара погодно тло за компјутерски криминал, а у екстремним условима доводи се у питање и опстанак мреже.

Управљачки процес мрежом је најважнији, стога и најугроженији у насртају компјутерског криминала, и често се назива интегрисаном информацијском мрежом са четири основне активности: прикупљање података и информација, обраду података и информација, меморисање (складиштење) података и информација и дистрибуција информација према крајњим корисницима.

Информацијску мрежу сачињавају – рачунари, комуникацијски уређаји, комуникацијске и рачунарске

ШТА ЈЕ ИНТЕРНЕТ?

Интернет је глобална информацијско-комуникацијска мрежа која повезује и спаја појединачне рачунаре, мреже појединих земаља и организација и тако омогућава власницима рачунара у целом свету да путем својих локалних мрежа и телефонских веза комуницирају, размењују информације и користе друге услуге.

Иако је хијерархијски организован, интернет је у суштини децентрализован. За решавање глобалних питања заједничких за целу мрежу надлежан је WWW конзорцијум или W3C. Он одређује стандарде комерцијалног дела интернета којих се морају придржавати сви произвођачи хардвера и софтвера, ако своје производе желе користити и продавати на интернету.

мреже, подаци и информације које се могу складиштити, обрадити и користити, програмска документација и поступци везани уз рад, коришћење или одржавање, а у ширем смислу чине је људи, средства, подаци, поступци и методе које се користе ради добијања валидних информација на основу којих ће крајњи корисници правовремено доносити одлуке.

Састав, делатност и циљ информатичке мреже одређују три основна начела – економичности, ефикасности и сигурности.

Рачунарски програм јесте систем дигиталних инструкција забележених на неком материјалном носиоцу, које омогућавају његово функционисање и решавање одређених задатака. Срце сваког програма је алгоритам – апстрактно математичко правило за решавање одређеног мисаоно-логичког проблема.

Напади на интернету

Развој интернета почиње 1969. године. Настао је као пројекат ARPANET с основним циљем да се створи поуздана мрежа која ће моћи да функционише и када неки њен део не ради, било због напада или техничке неисправности. Развој мрежног протокола омогућио је да се комуникација путем мреже аутоматски преусмерава, мимоилазећи место где је проблем настао, а тиме и спречи немогућност добијања информација без обзира на настале проблеме.

Почетком 1970. године у употребу улази први централни компјутер на UCLA и успоставља се NCP (Network Control Protocol) – као службени протокол за мрежну комуникацију. Мрежа је у почетку била намењена војним и научним потребама.

Средином седамдесетих развија се нови мрежни протокол TCP/IP, али се почиње користити тек 1982. године. Заменио је NCP, а служио је за комуникацију различитих врста рачунарских мрежа. Ускоро се из мреже због сигурности издваја MILNET (Military Network), који добија назив интернет (тако да 1989. ARPANET и званично постаје интернет). У потпуности се отворио јавности, после чега вртоглавом брзином расте и број корисника који је у наредних петнаестак година превазишао 200 милиона.

Ширењу доприноси развој WWW. Користећи нови протокол HTTP и формат HTML, WWW представља могућност доступа информацијама на нови начин и то комбинацијом текста, звука и слике – речју мултимедија.

Интернет је данас учинио размену и доступност информација лакшом него икада. Издвојило се неколико његових функција – прикупљање, чување и приступ информацијама, једноставнија и бржа размена података и програма, велики простор за оглашавање, и-мејл (електронска пошта која скоро у потпуности истискује класичну), интерактивна и непосредна комуникација између корисника, телеконференција и интернет телефонија, електронско банкарство и електронско пословање.

На почетку, намена мреже није била комерцијална нити усмерена на оно што данас представља, па се тиме и безбедности није поклањала довољна пажња и протоколи су били усмерени углавном развоју ефикасности, флексибилности и отворености мрежа. Коришћењем ARPANETA у почетним фазама развоја, догађале су се мање безазлене повреде безбедности у ужем кругу корисника који су се међусобно познавали и то у облику интерних шала и смицалица.

Први озбиљнији напад на мрежу ARPANETA догодио се 1986. године када је хакер успео да се повеже и копира податке из разних установа корисника интернета. Треба нагласити да том приликом није било злоупотребе прибављених информација.

Други озбиљнији напад уследио је 1988. године, а представљао је први аутоматизовани мрежни безбедносни напад. Морис Ворм је написао програм помоћу кога се могао спојити на други компјутер, искористити

слабост како би се сам пребацио на други компјутер и тако проширио мрежом. Тако се програм унедоглед умножавао на мрежу и искоришћавао за то њене ресурсе док није настало више од 5.000 копија црва који су „појели“ меморију мрежа и које су у том тренутку и срушене. Велики број мрежа је на тај начин трајно изашао из употребе. Ворм је прва особа осуђена на основу „Закона о компјутерској превари и злоупотреби“.

Већ 1989. напади на мреже се настављају у облику црва – WANK/OILZ. После се јављају Packet Sniffers, који су намењени копирању података из пакета у којима путују мрежом, а садрже корисничка имена и лозинке за приступ мрежама. Током 1995. године развијају се програмски алати за откривање „веза поверења“ и њихову симулацију с удаљеног рачунара како би се осигурао несметан приступ мрежи.

Електронско пословање

Електронско пословање је новији појам који обухвата све облике пословних трансакција или размене информација помоћу информацијске и комуникацијске технологије међу организацијама, између организација и купаца или организације и државне администрације.

Омогућава понуду, потражњу, продају, размену информација, подношење платних налога, електронски пренос средстава без непосредног контакта и посредништва између заинтересованих страна. На тај начин смањују се трошкови, време, непотребне залихе, а пословање се прилагођава интересу странака.

Такав облик рада има корене у електронском преносу новца с краја 19. века, када су коришћени уређаји попут мрежа Roter.

За разлику од електронске размене података, електронско пословање је шири појам који осим размене података обухвата и низ активности усмерених ка јавном и према приватном сектору, али и према сваком грађанину који има приступ мрежи. Од раста интернета највише користи имају они чија је делатност повезана са радом и коришћењем интернета – произвођачи софтвера и хардвера, интернет провајдери и они који пословање први прилагоде новим условима – компаније које ширење пословања виде у новом тржишту.

Основне препреке даљем расту електронског пословања јесу несигурност организација које послују на тај начин, неповерење корисника у безбедност, правни проблеми, тешкоће у погледу криптографских производа и приликом постизања међународног консензуса опорезивања електронског тржишта.

Умножавање штете

Раст интернета прати раст броја и учесталости напада. Тачан, па ни приближан број стварних напада не може се и никада неће утврдити. Када је реч о великим информацијским мрежама честа је тенденција да се напади прећуте због тајности података или због страха од губитка корисника. Зато је тешко утврдити стварне последице, али процене Интерпола говоре да је штета настала компјутерским криминалом одмах иза оних насталих трговином дрогом и оружјем.

Највећи број инцидената се не објави или чак никада и не открије. Пример је случај NASA-е 1998. годи-

ШИРЕЊЕ ХАКЕРСТВА

Ширењу хакерства доприноси:

- развој мрежа и њихово повезивање, phreaking – phone breaking,
- појава персоналних рачунара (1981. године, IBM PC),
- развој телекомуникационих уређаја намењених раду с удаљеним компјутерима,
- појава хакерских BBS-ова (Bulletin Board System) – омогућује им да тајно комуницирају и размењују искуства и програме намењене провалама,
- појава и раст интернета и улога медија у популаризацији хакера.

не, која је претрпела низ организованих напада на сервере засноване на Windows-у. Дошло је до рушења мрежа и понуда услуга холандских хакера Садаму Хусеину за време америчких припрема за Пустињску олују, што је он одбио.

Развојем интернета расте и број потенцијалних нападача. Све веће техничко знање и напреднија опрема омогућавају стварање напредних софтверских алата намењених лакшем и бржем нападу, па је и починиоцима с мањим знањем омогућено да једноставно и лако изведу напад.

Основни разлог јесте и доступност изворних кодова програма, које омогућава увид починиоцима у структуру програма и коришћење његових слабости. Честа мета су агенције за заштиту интелектуалне својине. Хакери веома брзо откривају безбедносне багове. Хардверске или софтверске грешке до које долази кривицом произвођача често се откривају тек после изласка производа на тржиште.

Постоји могућност да се и тројанским коњем мења програм, посебно делови за идентификацију и приступ мрежи како би јој се могло неовлашћено приступити, а да се тај поступак региструје као легалан. До напада најчешће долази у тренуцима неовлашћеног приступа, неовлашћеног мењања података и програма, неовлашћеног брисања података и програма, преснимавањем малициозних програма (вируса и црва), коришћењем туђег рачунара за приступ другој мрежи, стварањем услова за настанак штете на мрежи и крађе, оштећења, уништења хардверске основице и медија.

Нападачи настоје да осигурају приступ компјутерској мрежи, прошире приступ како би могли даље деловати и предузимати друге радње у зависности од мотива и намера (прибавити, уништити или изменити програме и податке). Такође, настоје да уклоне доказе о присуству и предузетим радњама.

У односу на вољу нападача, напади се могу, условно, разврстати у оне које се учине намерно, односно свесно или случајно, када је то учинила особа која није знала шта ради. Према учинку напади могу бити активни и пасивни, у зависности од тога да ли се објекат с подацима мења или не.

С обзиром на место одакле напад долази може бити унутрашњи и спољашњи, а с обзиром на информацијске ресурсе може бити напад на податке, на основу програма (брисање и делимична или потпуна промена софтвера), и груби напад, односно напад на хард-диск.

Последице напада су неовлашћено прибављање информација, њихово мењање, маскирање и лажно представљање, неовлашћено коришћење ресурса и ускраћивање услуга.

Методе приступа

Да би приступили мрежама починиоци користе различите методе:

- друштвени инжењеринг – обухвата многобројне начине прибављања лозинки за неовлашћен при-

ступ мрежи који су резултат непажње, а најпознатији су Shoulder surfing – откривање лозинке физичким увидом приликом уписивања лозинке и Scavenging и Dumpster diving (стрвинарење) – „копање“ по туђем смећу, баченим папирима или белешкама како би се пронашла лозинка;

■ Masquerading – лажно представљање (као друга особа или компјутерска мрежа), поготово у случају такозване злоупотребе поверења (симулирање мрежа с којим постоји успостављена „веза поверења“);

■ Spoofing – више метода помоћу које нападачи долазе до жељених података користећи слабости интернет протокола али и непажњу корисника; може бити: Login spoofing – маска и лажно представљање, када овлашћени мрежни корисник не зна да није приступио жељеној мрежи и да су његови подаци у рукама нападача, Web spoofing – маска WWW странице, E-mail spoofing – слабости SMTP протокола, променом информација одакле је послата пошта (представљање као овлашћени корисник те и-мејл адресе), затим, DNS spoofing – тражење бројчане адресе компјутера, пресретање и слање лажних информација мрежи коју намерава напасти након чега се комуникација преусмерава на његов компјутер, те IP spoofing – пресретање и модификација IP адресе, шаље се лажна слика мрежи која верификује приступ па она мисли да је нападач, у ствари, овлашћен за приступ;

■ Guessing – насумични вишеструки покушаји погађања лозинки за приступ, по методи покушај-промашај;

■ Scanning – приступ мрежи уз помоћ посебних алата и програма, а користе је почетници (War Dialing);

■ прислушкивање – на телефонским линијама, уграђивање прислушних уређаја у саме компјутерске центре или персоналне рачунаре;

■ оптичко шпијунирање – праћењем, осматрањем и снимањем зграде или просторије у близини, увид у лозинке са екрана рачунара, пресретање ЕМ зрачења са терминалног видео-уређаја – екрана;

■ Socializing – дружење са запосленима у одређеној организацији, при чему долази до отицања података приликом разговора и размене искустава;

■ компромитација – разни видови уцена, подмићивање, искоришћавање људских слабости и порока;

■ програмске манипулације – различита програмска решења попут Pocket/Password Sniffer, „тројанског коња“...

Проширење утицаја

Када су нелегално приступили мрежи, нападачи настоје да прошире приступ јер имају мала права и њихово је деловање ограничено само на оно подручје, односно на извршење оних радњи на које је корисник, од кога је украдена лозинка, овлашћен. Повећање приступа реализује се на следеће начине:

■ Browsing – прегледање доступних садржаја (потрага за датотекама са лозинкама);

■ Back/Trap door – циљ је омогућити ономе ко их је направио неовлашћени приступ компјутерској мрежи заобилажењем редовног поступка идентификације и ауторизације код приступа; његови облици су – Back door (задња врата) пречице које су оставили после приступа неовлашћени корисници, манипулацијама на мрежи и Trap door (замке) – пречице које су оставили аутори мрежа ради бржег системског приступа мрежама ради поправки, надоградњи (update-а);

■ програми за анализу и надзор рада – првобитна намена им је да упозоре на грешке у мрежи и мањкавости, али их хакери злоупотребљавају; примери за то су SATAN, ISS, SPI;

■ Superzapping – назив од помоћног програма Superzap (IBM mainframe), који омогућава систем администратору да заобиђе сигурност мреже ради што бржих поправки стављају изван функције мрежне заштите;

■ грешке у програму – несвесне грешке које се у развоју нису приметиле; примери су многобројни упади у мреже због слабости софтвера, NASA, NATO, грешке на Explorer-у, Netscape-у, Microsoft OS, те случај cookie-ја.

Акције нападача

Могуће је да се претходно наведеним поступцима напад завршио, али је могуће и да су се тек тада створили услови за наставак напада. Нападачи, често, предузимају следеће акције:

■ манипулације програмима – коришћењем појединих програма за обраду база података или измена постојећих програма, с већег броја рачуна скидају мање износе новца и пребацује на своје рачуне или пребацују износе после друге децимале, такозвано француско заокруживање; такође, премештају или преправљају податке;

■ Denial of service – онемогућавају овлашћеног корисника да користи мрежу слањем велике количине података који оптерете и „загуше“ сервере, те им ометају рад (Spamming, Worm);

■ употреба малициозних програма: Trojan Horse – рачунарски програм који осим видљиве има и скривену, кориснику непознату намену, која може бити безазлена али и опасна јер аутору обезбеђује безгранична овлашћења над мрежом – back door. За разлику од осталих програма, „тројански коњ“ се не размножава и не преноси. Подврсте су му – софтверске бомбе (активирају се покретањем програма), логичке бомбе (активирају се испуњењем услова) и временске бомбе (у одређено време или након истека неког времена се активирају). Међу поменутим програмима су и Worm – рачунарски програм који када се покрене сам се и умножава на компјутеру или рачунарској мрежи, а користи ресурсе мреже тако да она не може нормално да функционише све док се садржај мултиплицираног програма не уклони. Делује потпуно независно и за разлику од вируса не угрожава податке. Такви програми су Bacteria, Rabbits, Crabs, Creepers (гмизавци).

Вирус је такође рачунарски програм или део програма који се после активације сам размножава и шири. Најчешће је написан у асемблеру, ретко неком вишем језику, преноси се помоћу CD-а, USB-а, флеш меморија или мрежом. Активира се покретањем програма, у одређени дан или сат, доводећи до различитих безазлених али и опасних последица. Након активирања могу остати резидентни или не. Активност престаје завршетком рада зараженим програмом. Забрињавајући је број и брзина настанка вируса.

ЦИЉЕВИ НАПАДА

Циљеви већине напада на интернету су:

■ корисничке лозинке – нападачу омогућују несметан приступ мрежи,

■ подаци који се налазе у меморији, на хард-диску или су у слободном транзиту каналима,

■ базе с бројевима кредитних картица ради остваривања новчане добити,

■ компјутерски програми – омогућавају неовлашћено коришћење, брисање, мењање, копирање или препродају,

■ веб-странице и News групе – неовлашћена промена садржаја страница, онемогућавање коришћења мрежа па овлашћени корисник не може да користи мрежу,

■ материјални ресурси мрежа – физички приступ с намером да се трајно оштете, отуђе или униште делови или мрежа у целини.

Месечно се појави више од 100 нових вируса, а од тог броја само 60 њих застари.

Према начину деловања вируси могу бити boot sector – активирају се покретањем DOS-a; паразитски – активирају се покретањем програма кога су заразили; вируси multi-partite који су комбинација претходне две врсте; макро вируси – активирају се покретањем макроа (саставни делови програма Word, Excel). Вируси се могу активирати у одређено време (Yankee Doodle), одређеног дана (Pathogen), датума (Michelangelo) или после копирања одређени број пута (Disk Washer).

Изразито су опасни полиморфни вируси (Queeq) који мењају облик да би заварали антивирусне програме. Користе се и енкрипцијом (шифровањем) како би прикрили постојање и отежали проналажење. Опасни су и Stealth вируси који се тешко откривају јер се у тренутку покретања антивирусног програма одвајају од зараженог програма да би му се након тога поновно припојили. Вируси се преносе и електронском поштом.

Развој хакерства

Настанку хакера претходиле су злоупотребе јавних телефонских мрежа. Починиоци таквих дела називали су се Phreakers. Јавили су се шездесетих, углавном као људи запослени у телекомуникационим установама. Познавали су слабости мрежа и користили знања ради постизања бесплатног коришћења телекомуникационих услуга. Њихово знање касније су користили хакери.

Хакерство настаје седамдесетих. Први хакери били су запослени на терминалима који су покушавали да продру до централног рачунара, користећи се терминалима на послу (јер су рачунари за приватну употребу били тек у повоју и веома скупи). Осамдесетих се хакерство нагло проширило (развојем интернета омогућено је глобално повезивање, дошло је до веће отворености мрежа, смањене су сигурности мрежа, тако да, на разне начине, лични, али и тајни војни, владини и службени подаци постају доступни нападачима).

На различите начине хакери покушавају да дођу до шифри. Познати су софистицирани методи, као што је cracking, односно копирање фајлова у којима се налазе лозинке, па и криптоанализе, којом се пробија енкрипција. Да би то постигли, хакери користе алате и програме којим насумице настоје да открију кључ испитујући и 50.000 до 200.000 упоређења у секунди. Таква веза углавном се остварује даљински, с туђе телефонске линије, како би се отежало праћење трагова. Све је то учинило хакерство једним од највећих глобалних проблема на почетку 21. века.

Стварна слика хакера различита је од оне коју су о њима створили медији. Хакери о себи мисле да су чланови елите, борци за слободу информација и демократију. На основу података јединица за рачунарски криминал, хакери су обично мушкарци, између 15 и 35 година старости, арогантни, непристојни, неуредни, неорганизовани, љубитељи SF-a. Нападе чине зарад стицања имовинске користи, али и жеље за публицитетом. Најбоље их описује термин „информацијски брокери“ – врста мешетара информацијама..

Разлози због којих нападају мреже крећу се од племенитих и безазлених (знатижеља) до најнижих и најопаснијих (користољубље). Свом деловању настоје да дају и политичку димензију јер верују да се боре за слободу информација и да су борци за људска права и слободе. При томе, заборављају да управо они крше права и слободе човека, пре свега право на приватност.

Хакерским радњама се не сматрају оне до којих је дошло случајно, које су усмерене на физичко онеспособљавање рачунарске мреже или средстава телекомуникација, затим, радње запослених којима компјутерски системи користе за личне потребе.

Информацијски брокери

На основу мотива напада и степена опасности приликом акција, хакери могу бити:

- Hackers – особе које из незнања, радозналости или због доказивања, упадају, понекад и несвесно, у туђе мреже, без намере да нанесу штету, копирају, мењају или на неки други начин утичу на функционисање мрежа;
- Crackers – опасне особе, вишег нивоа знања, које поседују квалитетна техничка средства која им омогућују да продру и у велике и јаче чуване мреже, најчешће из користољубља.

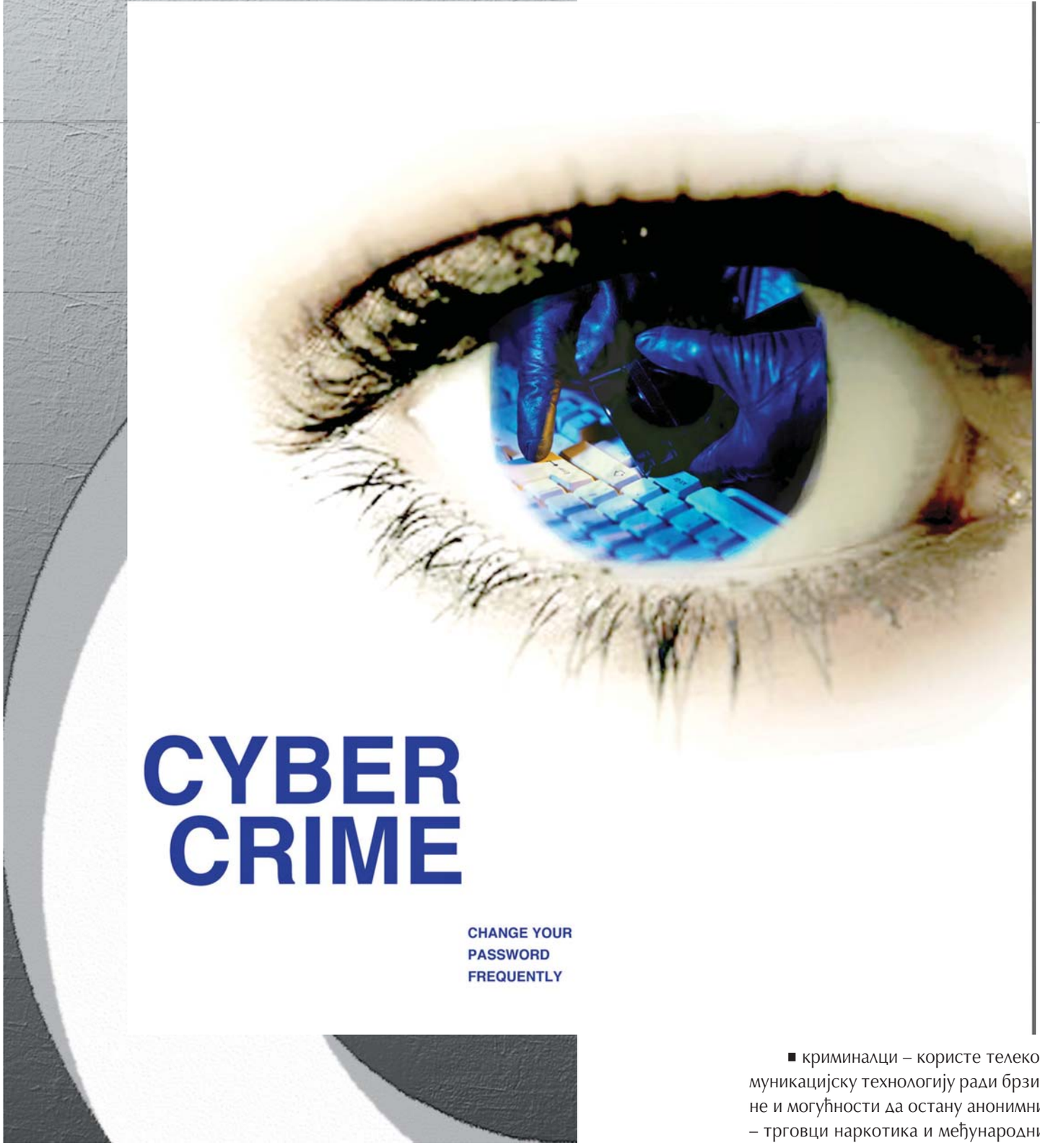
С обзиром на циљ напада и стручно знање које користе разврставају се у следеће групе:

- Hackers – занимају их само компјутерске мреже, поседују високо стручно знање, а циљеви напада су им, углавном, више мреже;
- Phreakers – изучавају телефонске и телекомуникацијске мреже, располажу знањем из тих области што им омогућава да помоћу средстава и метода неограничено и бесплатно користе услуге.

Према месту одакле делују разликују се хакери који су унутрашњи – запослени у организацији на чијем компјутеру желе починити саботажу, и спољашњи, које делују ван органи-

ЕНТРОПИЈА МРЕЖЕ

Ентропија мреже представља меру њене неорганизованости. Погрешна или недовољна организованост и слаба информисаност морају се смањити бољом организацијом мреже, сређеношћу елемената, благовременим и тачним информацијама о свим процесима. Што је организованост и сређеност већа, мања је могућност угрожавања, а већа могућност извршења очекиваног.



зације, фирме или институције, чије рачунарске системе угрожавају.

Сходно методама, средствима и циљевима, хакери могу бити:

■ почетници – млади починиоци који то раде из радозналости и досаде,

■ студенти – раде из интелектуалне знатижеље за сигурност мрежа,

■ туристи – проваљују у мреже и настављају активност ако нешто интересантно запазе,

■ разбијачи – уживају у томе да изазову пад мрежа,

■ лопови – најозбиљнији починиоци, образовани, нападачки расположени – „криминални кракери".

Према мотивима напада и последицама које проузрокују познати су следећи хакери:

■ Pure Hackers – настоје бити што уочљивији како би привукли пажњу и задовољили своје егоистичке потребе; не улазе у зоне високог ризика;

■ унутрашњи хакери – мотивисани користољубљем, запослени радници овлашћени за приступ мрежи; њих је најтеже открити;

■ криминалци – користе телекомуникацијску технологију ради брзине и могућности да остану анонимни – трговци наркотика и међународни криминалци;

■ индустријски шпијуни – краду информације које након тога нуде на тржишту информација;

■ хакери у функцији страних обавештајних служби – с велике удаљености пробијају најзаштићеније мреже и баријере како би дошли до информација од интереса за стране обавештајне службе.

Уколико се анализира криминално понашање, хакери могу бити:

■ кракери – чије је незаконито понашање подстакнуто интелектуалним изазовом,

■ рачунарски криминалци – незаконито понашање је ради остваривања финансијских или политичких циљева,

■ вандали – њихово понашање подстакнуто је незадовољством или љутњом према некој организацији.

Ако се говори о појавним облицима рачунарског криминала, хакери се могу разврстати као:

■ копи-пејст – они умножавају, затим продају или деле информације;

■ рачунарски лопови – преправљају податке и програме да би се на брзину обогатили;

■ кријумчари – сарадници тајних служби и индустрије; тргују оним што доноси брзу зараду, најчешће оружјем, наркотицима, програмима;

■ хакери – који неовлашћено упадају у туђе рачунарске системе;

■ саботери – имају слободан приступ уређајима или им тајно прилазе како би их оштетили или уништили;

■ осветници – бивши запослени који се од саботера разликују на основу мотива;

■ шпијуни – проваљују по наредби да би дошли до различитих тајних података.

Средства заштите

Методе и средства заштите морају да осигурају несметан и сигуран рад информацијске мреже, с једне стране, а сигурност података и комуникација, и унутар мрежа и према околини, с друге стране. Уз то, треба да осигурају физичку, људску, комуникацијску и оперативну сигурност мрежа.

Примењују се многе методе заштите:

■ Физичка заштита – скуп метода и средстава ради заштите хардвера од непосредног физичког приступа мрежи и коришћења њених ресурса, али и заштите од непредвидивих спољашњих фактора, попут струјних удара. Користе се аларми и видео-надзор,

■ Провера приступа – најчешћи начин заштите мреже од неовлашћеног мрежног, односно даљинског приступа преко комуникацијских канала. Састоји се од два поступка – идентификације корисника и ауторизације (утврђују се овлаштења и права после приступа). Корисник приликом приступа овлашћеној мрежи уписује име и шифру. Новије мреже примењују уређаје којима се идентитет корисника проверава помоћу магнетских картица, анализом отиска прста или длана, провером зенице ока, анализом гласа, потписа,

■ Криптографија – користи се од најстаријих времена као средство тајне комуникације. Потиче од грчке речи crypto – скривен, и graphein – писање, а значи мрежно размештање или замењивање знакова с циљем да се сачува тајност текста од сваког коме није намењен. Криптологија је наука о сигурној комуникацији, обухвата криптографију (енкрипцију) и криптоанализу (дешифрирање – декрипцију). Данас се криптографија користи за кодирање података помоћу алгоритама за енкрипцију, с намером да се тајно и сигурно пренесу комуникацијским каналом до примаоца. Алгоритми користе кључеве у облику бинарних бројева дужине до 1.024 бита. Делотворност таквог поступка зависи од алгоритма и дужине кључа који се користи. Кодирање је могуће спровести софтверски (коришћењем програма) и хардверски (коришћењем наменских уређаја).

Криптографскє мрєжє

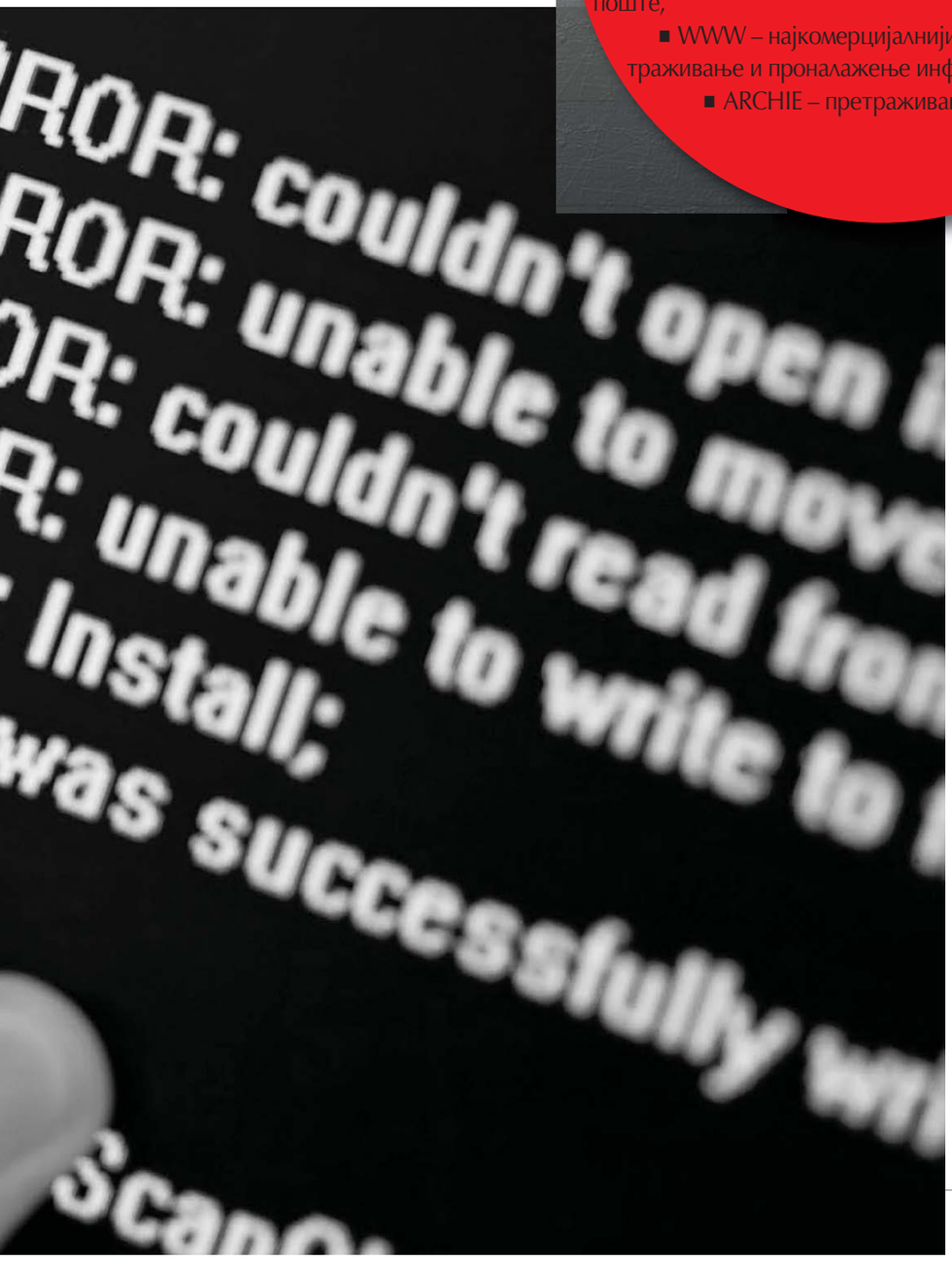
Криптографске мреже могуће је класификовати према:

- математичким операцијама којима се изворна порука скрива, коришћењем енкрипцијског кључа, приликом које се премештају знакови унутар поруке или замењују другим знаковима или симболима;
- кључу који користе пошиљалац и прималац – може бити исти или различит; симетрична криптомрежа користи тајни кључ који поседују и прималац и пошиљалац (DES – Data Encryption Standard кључ од 56 бита и већи); она је најбржа, али је пренос кључа несигуран; асиметрична криптомрежа позната је као метода „јавног кључа“; користи пар различитих кључева, тајни и јавни – такав је PCA алгоритам (Rivest-Shamir-Adelman); тајни кључ има само прималац, а јавни кључ за шифрирање доступан је свима, па је интернетом до њега једноставно доћи; иако спорија, метода је далеко сигурнија од претходне;

МРЕЖНИ СЕРВИСИ

Познати мрежни сервиси за комуникацију с другим корисницима или приступ ресурсима других компјутера на мрежи су:

- GOPHER – мрежа за проналажење и претраживање мрежних ресурса и база података,
- FTP – мрежа за пренос података,
- USENET – мрежа за комуницирање с другим корисницима путем тематских конференција,
- E-MAIL – мрежа за слање и примање електронске поште,
- WWW – најкомерцијалнији део, мрежа за претраживање и проналажење информација,
- ARCHIE – претраживање FTP-а.

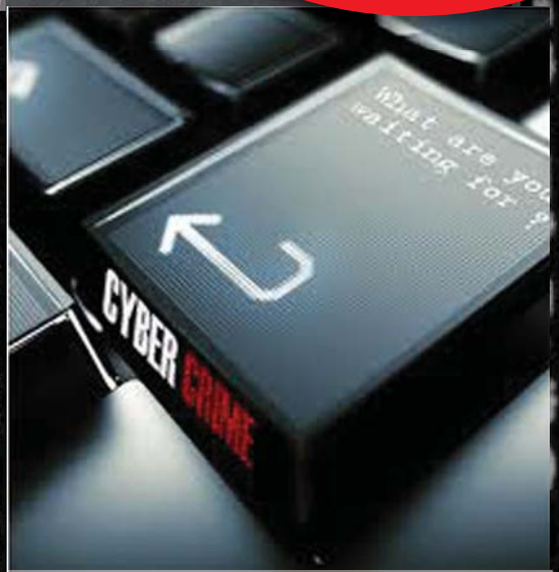


- стеганографија – умеће скривеног писања, користи се за уметање инфо у неискориштене делове информацијског пакета који се преноси комуникацијским каналом; тако се подаци крију у безазленим порукама (слици, тексту, звуку); важно је само да не дође до грешке у преносу;
- дигитални сертификат – представља исправу у дигиталном облику која потврђује идентитет правног лица или особе; издају их овлашћене организације; сигурност података из исправе омогућава се употребом асиметричне криптографије; издате исправе садрже тајни кључ за дешифрирање, а оверавају се јавним кључем који издаје надлежна агенција;
- дигитални потпис – јесте технологија провере веродостојности примљених порука у комуникацији између два удаљена рачунара; потпис у дигиталном облику је саставни део поруке која се шаље, а садржи израчунати скуп поруке; немогуће је изменити поруку, а да се тај број не промени; често се користи у комбинацији с дигиталним сертификатом јер дигитални потпис потврђује веродостојност текста који се шаље, односно прима, али не и идентитет особе која га шаље;
- дигитални временски запис – користи се за проверу када је дигитални документ креиран, односно последњи пут промењен, ради утврђивања веродостојности документа послатих интернетом;
- керберос – мрежни протокол за идентификацију, осигурава висок степен провере идентитета учесника мрежне комуникације коришћењем криптографске методе тајног кључа; приликом приступа серверу користи висок степен криптографске заштите;

УПАДИ У РАЧУНАРЕ

Поједине делатности хакера могу бити и корисне, јер упозоравају на слабости мрежа и пропусте у заштити. Ипак, чињеница је да су штете настале таквим упадима далеко веће од користи. Забрињавајућа је повезаност хакера с разним облицима организованог криминала – случај Левина и упада у банкарску мрежу Citybank-e, те неовлашћени трансфер новца на различите приватне рачуне у другим банкама.

Хакерским услугама све се више користе и обавештајне службе. Познат је догађај из 1989. када је у Немачкој откривена и ухапшена група хакера која је за потребе КГБ-а, уз велику новчану награду, покушала да уђе у око 450 рачунарских мрежа широм САД и западне Европе, или случај „Вјесника“ 1998. године када су српски хакери заменили садржај насловне странице непримереним садржајима, након чега је уследио одговор хрватских хакера на странице Народне библиотеке Србије. Догодило се и неколико напада албанских хакера на сајтове наших министарстава и на сајт Српске православне цркве.



Софтверска пиратерија

Убрзани технолошки развој, који прате велике зараде, не прати на одговарајући начин и брига о безбедности и заштити мрежа. Томе највише доприносе произвођачи софтвера и хардвера, који у немилосрдној борби за тржиште често у промет пуштају иновације пре конкуренције, које нису до краја испитане и имају многобројне недостатке. Сем тога, произвођачи скоро и да не одговарају за мањкавост производа, па се том проблему и не посвећује довољно пажње.

Повећањем броја физичких и правних корисника интернета свет постаје глобално информацијско се-

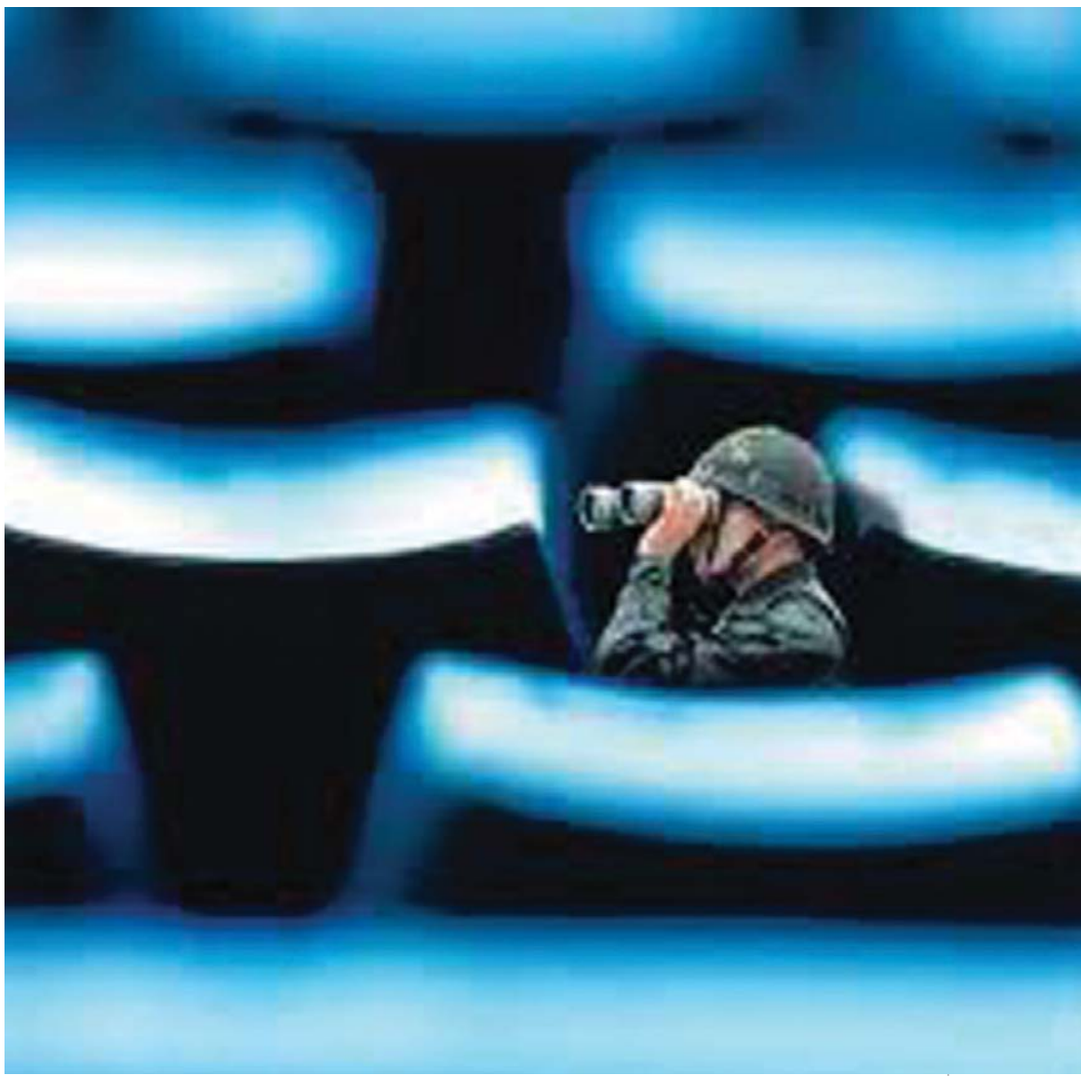
■ Firewall – начин заштите у мрежама који треба да спречи неовлашћени приступ подацима и програмима, а да, истовремено, корисницима омогући приступ интернету без опасности за податке на локалној мрежи с које се приступа; могуће их је користити као заштиту и интерно, унутар локалне мреже; слабости су управо у томе што су ограничења приликом приступа интернету заиста велика;

■ издвајање података или мрежа из мреже; ако то није могуће, онда се примењује једно од решења такозване мреже реплицирања садржаја, при чему се подаци с једног компјутера копирају на други; након што су пренесени, веза се прекида тако да рачунар коме приступају корисници нема везе са централним рачунаром;

■ Backup – редовно меморисање података и програма и њихово чување на заштићеном месту; ако и дође до напада, штета ће бити већа ако не постоје сигурносне копије података и ако су они, на пример, неповратно избрисани деловањем уметнутог малициозног програма;

■ антивирусна заштита – најефикаснија заштита јесте коришћење квалитетног антивирусног програма; пожељно је да је програм стално резидентан у меморији и да приликом копирања података препозна вирус, те одмах нуди кориснику могућност деловања;

■ надзор и анализа рада мреже – обухвата мере и средстава којима се проверава приступ, коришћење мрежа, анализира рад, те испитују њене слабости. Посебно се користи у комбинацији с другим методама (firewall-a). Ипак, упркос све већој аутоматизацији тог поступка, кључну улогу и даље има стручни кадар.



ло, укидају се регионална, просторна, етничка и слична ограничења, те се формира такозвана информацијска заједница. Интернет је тако постао технолошки, социјални, економски, медијски, политички, али и правни феномен. Имајући у виду да на садашњем нивоу развоја није могуће постићи апсолутну сигурност информацијске мреже, јавља се потреба за пружањем апсолутне и ефикасне правне заштиту када до злоупотребе дође. Ипак, то је могуће постићи само координираном акцијом и уз сугласност међународних фактора.

Такође, у великом броју земаља законски оквир за борбу против криминала у киберпростору сведен је на деловање полицијских структура које се баве борбом против високотехнолошког криминала, док заштита појединца или мреже често изостаје из правних оквира.

Најчешће грешке у заштити рачунарских мрежа последица су ниског степена информатичког образовања корисника услуга IS-а, погрешног избора лозинки, грешака у властитом или туђем софтверу и протоколима, погрешне имплементације софтвера и протокола, погрешне конфигурације рачунарског мрежа или мреже, коришћења мањкавих и застарелих метода физичке заштите, недостатака коришћеног начина надзора мрежа, или застарелог софтвера и хардвера, односно њихове некомпатибилности, непостојања сигурносне политике и недовољног улагања у заштиту и сигурност.

Од почетка осамдесетих, проблем заштите интелектуалног власништва односи се, пре свега, на заштиту програма и типологије чипова како би се спречила софтверска пиратерија, јер и држава и аутори софтвера губе приходе које би легалном продајом остварили.

Постојећа правна решења не приказују пиратерију као крађу – програми су нематеријални и не могу се уврстити под појам ствари. Правну заштиту могуће је постићи само применом права интелектуалног власништва, попут ауторског права или права индустријског власништва. Најпогоднија је ауторскоправна заштита која има међународни карактер. Патентно-правна заштита је скупа, а уговорна заштита и заштита пословне тајне немају апсолутни карактер јер не делују према трећим особама. ■

Аутор је члан удружења судских вештака за информационе технологије