Изазови информационе безбедности – прошлост, садашњост, будућност

Велимир Радловачки

Наставник рачунарске групе предмета

Школски центар „Никола Тесла“, Вршац

velimir.radlovacki@gmail.com

# 1. Увод

Информатичка јавност је углавном упозната са историјатом развоја дигиталних електронских рачунара. Из војних кругова, након другог светског рата, рачунари су брзо нашли своје место и примену на универзитетима, у банкама, поштама и сл. Други светски рат јесте био завршен, међутим хладни рат и трка у наоружању светских сила и даље је трајала. Највећа бојазан у САД-у била је од ваздушних напада и стога је приоритет био развијање централизованог радарског система помоћу којег би се видела јединствена слика комплетног ваздушног простора. Такав војни систем назван SAGE (Semi-Automatic Ground Environment) је на крају и реализован у сарадњи са компанијом IBM, што се сматра почетком развоја савремених рачунарских мрежа.

Као и рачунарски системи, рачунарске мреже убрзо су доживеле комерцијализацију. Из војних кругова један од првих примера комерцијализације рачунарских мрежа био је систем за резервацију авионских карата SABRE (Semi-Automatic Business Research Environment) који је заживео 1960. године у компанији American Airlines. И овај систем заснован на IBM 7090 mainframe развила је компанија IBM и наплатила 40 милиона долара.

Уследио је талас техничких решења за умрежавање од стране разних компанија и коначно 29.10.1969. успостављена је прва ARPANET веза између универзитета у Лос Анђелесу и инстраживачког института Станфорд. У року од месец дана мрежа је проширена са још два чвора, универзитетом у Санта Барбари и универзитетом у Јути. До 1981. године број чворова порастао је на 213, а нови чворови придруживани су скоро на сваких 20 дана. 01.01.1983. NCP протокол на ARPANET-у замењен је TPC/IP скупом протокола, чиме започиње ера модерног интернета. 1989 на институту CERN у Швајцарској рођен је данас најпопуларнији сервис интернета – World Wide Web. Временом су се ове технологије из војних и академских институција преселие у наше домове и постале доступне широкој популацији.

# 2. Кратак историјат информационе (не)безбедности

Појава нових технологија увек са собом носи и питање сигурности. Данас би већина људи одговорила да сигурност рачунарских система и мрежа угрожавају хакери – неовлашћено приступају рачунарским системима, не поштују софтверске лиценсе и „иновативно“ модификују хардвер. Речи hack и hacker су први пут почеле да се користе ван изворног значења на МИТ-у 1946. у студентском моделарском клубу. Студенти су израђивали макете возова и технички их осавремењивали и унапређивали. Хакерима су називани студенти, чланови клуба, који хакују макете возова – праве их бољим него што јесу. Пре 30-40 година хакери су били синоним за добре програмере који уживају у интелектуалним изазовима решавања проблема и превазилажења или заобилажења ограничења, или особе које суштински разумеју како функционишу системи, а посебно рачунари и рачунарске мреже. Шта је утицало да термин хакер добије тако контроверзна значења?

Први злоупотребљен сигурносни пропуст био је документован 1965. на МИТ-у, а тицао се коришћења системског текст едитора и замене привремених фајлова са фајловима у којима се чувају лозинке. 1971. започела је ера рачунарског малвера када је Боб Томас из компаније BBN Technologies направио је први рачунарски вирус Creeper како би тестирао Вон Нојманову теорију само-репродуктивних аутомата. 1974. настао је вирус Rabbit, 1975. вирус Animal итд. 1971. године у часопису Esquire изашао је чланак Secrets of the Little Blue Box који описује алат за неовлашћено коришћење јавне телефонске мреже. Експериментисање, експлоатација и неовлашћено манипулисање телекомуникационим системима, а најчешће јавним телефонским мрежама, названо је phreaking, а особа која се тиме бавила phreaker (phone-freak).

1983. године изашао је филм WarGames – први играни филм који упознаје ширу јавност са феноменом хакера. Необавештеност, незнање, хладни рат и параноја у јавности погрешно су описали хакере као тинејџере са рачунарима и модемима, који могу да лансирају нуклеарне пројектиле притиском тастера из своје собе. Истовремено, амерички конгрес је почео са саслушањима на тему нарушавања сигурности ICT система, FBI и тајна служба почели су да истражују рачунарски криминал и основан је први Computer Emergency Response Team (CERT) од стране агенције DARPA. Професори рачунарства у својим предавањима почели су да користе термин хакер у негативном контексту. Осамдесетих су основане и прве хакерске групе Chaos Computer Club, Legion of Doom, Masters of Deception, Cult of the Dead Cow и др. Основани су и хакерски часописи 2600 и Phrack и одржан је први хакерски конгрес Chaos Communication у Немачкој.

# 3. Ко данас угрожава информациону безбедност

White Hat или етички хакери су ICT професионалци који користе алате и методологију специфичну малициозним хакерима са циљем испитивања могућности пробоја система клијента. Пре почетка испитивања обавезно потписују уговор са клијентом у коме је прецизиран план испитивања. Испитивање подразумева активно тестирање система у циљу откривања рањивости које могу бити последица неодговарајуће конфигурације, грешака или оперативних слабости. У извештају клијенту, представља се процена ризика, откривени пропусти, решења за отклањање пропуста и/или предлози за смањење ризика. Данас се од ICT професионалаца све чешће захтевају и додатни сертификати из области сигурности рачунарских система и мрежа, поред формалног образовања и обука. Сертификати обично долазе од The International Information Systems Security Certification Consortium, EC-Council и др. Специјализовани сајтови и курсеви о сигурности ICT система почели су да се појављују и у Србији, мада тек неколико компанија нуди услуге испитивања пробојности система.

Gray Hat хакери користе алате и методологију испитивања могућности пробоја система специфичну малициозним хакерима, али без дозволе. Од Black Hat хакера разликују се јер откривене сигурносне пропусте обично пријављују вендорима, како би их отклонили. Black Hat хакери угрожавају сигурност система са циљем неовлашћеног приступа, наношења штете, крађе информација, прибављања материјалне користи итд. Крше правила рачунарске етике и законе који се тичу рачунарског криминала. Script Kiddies (Skiddies) угрожавају сигурност система користећи туђе алате, без разумевања процеса који се дешава у позадини. Надимак Script Kiddie користи се као увреда за почетнике тј. за особе које нису вичне програмирању и немају довољно знања о рачунарским системима и мрежама.

Хактивисти спроводе борбу за социјална, идеолошка, религијска и политичка питања нападима на рачунарске системе и мреже. То су најчешће напади одбијања услуга (Denial of Service - DoS). Неовлашћено мењају садржаје wеб сајтова (defacement) или их обарају. Често објављују тајне/поверљиве/персоналне информације до којих су дошли током напада. Организоване криминалне групе врше криминалне активности угрожавајући сигурност рачунарских система и мрежа са циљем остваривања материјалне користи. Најчешће су то: банкарске преваре, крађа корисничких информација, крађа идентитета, изнуде, илегална трговина, индустријска шпијунажа итд. Глобални губици од cyber криминала процењени су на ≈ 500 милијарди долара у 2014. години. Скуп софистицираних процеса који угрожавају сигурност рачунарских система и мрежа усмерених ка некој већој организацији или држави називају се напредне трајне претње (Advanced Persistent Threat, APT). APT изводе веће организације или државе које имају мотив и средства. Радње које се могу уврстити у APT су шпијунажа, надзор, напади, неовлашћени приступи, инфицирање малвером, саботаже итд.

# 4. Како се данас угрожава информациона безбедност

Пет фаза специфичних за скоро сваки напад на рачунарске системе и мреже су:

1. Извиђање (reconnaissance)

2. Скенирање (scanning)

3. Добијање приступа (gaining access)

4. Одржавање приступа (maintaining access)

5. Прикривање трагова (covering tracks)

Извиђање је најдужа фаза у којој нападач користи разне извори да прикупи податке о мети (веб претраживаче, социјалне мреже, онлајн именике, регистре предузећа, регистре домена итд). У овој фази често се користи и социјални инжењеринг –психолошка манипулације у циљу откривања информација. Одбрана је немогућа у овој фази јер информације о мети (запосленима, клијентима, компанији, пословању) увек доспеју на Интернет. Могуће је применити мере предострожности: едукацијом запослених; избегавањем непотребне публикације имена, позиција, персоналних података, емаил адреса, података о компанији, пословању компаније и клијентима; сакривањем података о регистрантима домена веб сајта компаније итд.

Следећа фаза напада је периферно и интерно скенирање свих ИКТ ресурса мете. Нападач тражи „живе системе“ на мрежи; тражи отворене портове на тим системима; идентификује сервисе који раде на тим портовима; идентификује оперативни систем и софтвер који користе те сервисе; тражи сигурносне пропусте који постоје у откривеним сервисима, оперативном систему или софтверу. Скенирање је могуће детектовати помоћу система за откривање упада (Intrusion Detection System - IDS), односно система за превенцију упада (Intrusion prevention system - IPS). Ради предострожности треба: искључити све непотребне портове и сервисе; редовно ажурирати оперативни систем и апликације сигурносним закрпама; користити анти-малwаре и фиреwалл решења; редовно ажурирати фирмвер (нарочито у мрежних уређајима); и користити енкрипцију на комуникационим везама.

Добијање приступа ИКТ ресурсима мете је најважнија и најкомпликованија фаза. Врши се у циљу крађе, измене информација, уништавања информација, коришћења ресурса за друге нападе или ради коришћења самих ресурса у неке друге сврхе. Могуће активности нападача у овој фази су: разбијање лозинки, експлоатисање сигурносних пропуста система или сигурносних пропуста на вебу, напади на бежичне мреже и клијенте итд. Одбрана у овој фази подразумева прецизно дефинисање корисничких група и њихових привилегија и енкрипцију саобраћаја и важних информација.

Следећи корак је одржавање приступа, довољно дуго да може да се реализује циљ напада. Одржавање приступа реализује се имплементацијом бацкдоор-а на системима жртве, који омогућавају нападачу удаљени приступ заобилазећи процес аутентификације и детекције. Одбрана у овој фази подразумева детекцију и превенцију: сесија за даљински приступ, непознатих мрежних сесија, мрежних сесија са великим протоком, конекција на неуобичајеним TCP/UDP портовима, чудних догађаја на серверу, мрежи и мрежним уређајима итд.

Након реализације циља напада, нападач прикрива трагове напада како би сакрио свој идентитет и локацију од систем администратора, ИТ форензичара или органа закона – уништава све логове и историју на систему. Лог фајлови приказују сваку неуспешну или успешну пријаву на систем као и друге догађаје везан за сигурност система. History фајлови приказују историјат извшавања команди или кретања кроз систем. У Microsoft Windows оперативним системима, Event Viewer приказује логове догађаја у вези грешака у раду система, апликација, сервиса и безбедности. Брисање логова могуће је из командне линије са администраторским привилегијама помоћу команде wevtutil. Linux чува логове у текстуалним фајловима у директоријуму /var/log. Логови се могу едитовати или обрисати. Историја извршених команди налази се у bash\_history и може се уништити командом shred. Савети за одбрану у овој фази су: водити рачуна о конфигурацији корисничких налога и дозвола; релоцирати битне логове са подразумеваних локација; битне логове аутоматски прослеђивати електронском поштом и/или их аутоматски копирати на независну локацију; користити IDS/IPS решења и аутоматски алармирати администратора на критичне догађаје (SMS порука, електронска пошта…).

# 5. Будућност и информациона безбедност

Један од „најлакших“ изазова који нас чека је UNIX Epoch Bug – слично као Y2K Bug време у UNIX, Linux, Andoid и сличним системима чува се и рачуна у формату signed 32-bit integer, односно од 00:00:00 UTC 01.01.1970. до 03:14:07 UTC 19.01.2038. (231-1 = 2,147,483,647 секунди после 01.01.1970.). Пробијање овог интервала доводи до integer overflow проблема.

Не тако давно, сматрали смо да ће врхунац вештачке интелигенције бити када рачунар победи човека у шаху. У мају 1997. рачунар је победио човека у шаху. Тај рачунар имао процесорску моћ од 11 гигафлопса. Телефон у вашем џепу данас сигурно има процесорску моћ већу од 500 гигафлопса. У међувремену променили смо мишљење о томе шта је вештачка интелигенција и померили циљеве унапред. Као врхунац процесорске моћи биће сигурно потпуно функционални квантни рачунари. Ми можда нећемо доживети њихово постојање, међутим и довољно функционалан квантни рачунар моћи ће у реалном времену да разбије било какву енкрипцију на интернету по данашњим стандардима (SSL/TLS).

Пре десет година компанија Аpple представила је први паметни телефон и променила свет. Интернет се преселио из десктоп рачунара и сервера у наше џепове. Технологија која покреће паметне телефоне као и развој мобилне телефоније створили су још једну грану индустрије – интернет ствари (Internet of Things - IoT). Већ данас рачунаре који су способни да комуницирају у TCP/IP мрежи проналазимо свуда – у камерама за надзор, аларним системима, кућним уређајима, индустријским машинама итд. Ово је отворило потпуно нове просторе за малициозне нападаче чије последице нећемо сагледавати у губитку података или новца, већ у физичкој безбедности људи!

Уграђене рачунаре способне да комуницирају у TCP/IP налазимо и у критичној инфраструктури сваке државе и на жалост, већ смо видели да нису безбедни. Још у прошлој деценији рачунарски црв Stuxnet који напада Siemens PLC системе онеспособио је иранско постројење за обогаћивање уранијума, а пре само годину дана привремено је онеспособљено постројење компаније која се бави електродистрибуцијом у Украјини Prykarpattyaoblenergo, услед сајбер напада. Свакако, не смемо заборавити на развој и примену роботике и савремених информационо-комуникационих технологија у модерном ратовању. Не смемо ни помислити какве би несагледиве последице изазвале злоупотребе и безбедносни пропусти у овом пољу људске делатности.

# 6. Закључак

У свету информационо-комуникационих технологија не постоји потпуно сигуран систем. Илузија о потпуној сигурности има контра-ефекат. Технички аспект сигурности рачунарских система и мрежа јесте битан, али је једнако битан и људски фактор. Едукација ради повећања свести о сигурности је неопходно улагање. Тестирање сигурности методама и алатима специфичним малициозним нападачима и отклањање откривених пропуста знатно смањују сигурносне ризике. Процесу тестирања сигурности рачунарских система и мрежа поменутим методама и алатима треба приступати крајње одговорно и опрезно!