Bezbednost informacionih Sistema
- drugi deo-

Tanja Kaurin

5. Злоупотреба ИТ

ИТ је укључена у све аспекте друштвеног живота, укључујући државне органе,

- **науку,**
- **просвету,**
- **медицину,**
- **комуникације,**
- **трговину,**
- **банкарство и друго.**

Појединци и групе, независно од физичког растојања нападача и локације циља, времена, државних граница, царинских баријера и слично, извршавају веома озбиљне криминалне радње по целој планети, а да се нису ни померили из своје радне собе. Прошлост овако нешто није познавала.

Чињеница да се ова врста криминала извршава у амбијенту у којем ИТ има доминантну улогу, подразумева присутност одређених специфичности у односу на класичну ситуацију.
Те специфичности се огледају у чињеници да се овај криминал извршава

- **лакше,**
- **брже,**
- **обимније,**
- **анонимније и**
- **безбедније,**
- **али уз много више знања и специфичне стручности.**

Потенцијалне последице су у лепези од баналних до катастрофалних.
Зато питање заштите по својој сложености, озбиљности и значају мора бити високо на листи приоритета.

5.1. Врсте злоупотребе

Рачунарски криминал је у суштини класични криминал извршен у информационом амбијенту. Неки од облика су:

- Крађе;
- Проневере;
- Преваре;
- Фалсификовање;
- Изнуде и уцене;
- Нарушавање приватности;
- Саботаже;
- Одавање тајни;
- Шпијунажа;
- Порнографија;
- Пропаганда;

Постоје облици криминала који су специфични за рачунарски криминал. Неки од ових облика криминала су:

- Хакинг;
- Стварање и дистрибуција вируса;
- Пиратерија софтвера;
- Ускраћивање сервисних услуга;
- Електронско узнемиравање;
- Крађа рачунарских услуга;

5.1.1. Крађе

Основни типови крађе као облика рачунарског криминала, који подразумева електронски упад у информациони систем и преузимање објеката који се присвајају, су :

- **Крађа података и софтвера;**
- **Крађа лозинки, кодова и идентификационих бројева;**
- **Крађа идентитета;**

Крађа података и софтвера и њихово бесправно коришћење и/или трговина њима представља растући проблем.

Крађа лозинки, кодова и идентификационих бројева је **еквивалентна крађи кључева** у класичној ситуацији, јер су лозинке, кодови и идентификациони бројеви логички кључеви који омогућавају улазак у „заштићене зоне“ у којима се жели извршити нека илегална активност.

Крађа идентитета се јавља кад неко без знања и сагласности друге особе **присвоји њен електронски идентитет** ради извршавања криминалне радње, првенствено крађе или преваре.
Када криминалац преузме нечији електронски идентитет, обично се лажно представља ради:

- подизања новца,
- електронске куповине,
- узнемиравање других корисника и злоупотребу права правог власника.

Другим речима, врши кривична дела у име жртве.

Žrtva krađe identiteta

Krađa identiteta postaje unosan posao u Srbiji, pošto je sve veći broj žrtava na čije adrese stižu računi za dugovanja kao i prijave za utaju poreza. U Agenciji za privredne registre ističu da nisu dužni da naknadno proveravaju verodostojnost dokumenata.

Radio-televizija Srbije

Beograđanin Branko Mijajlović žrtva je krađe identiteta još od 2009. godine od kada mu na kućnu adresu stižu računi i prijave za utaju poreza. Sva dugovanja upućuju na firmu "Komiks global" čiji je direktor navodno Branko Mijajlović. Tužilaštvo je upoznato sa slučajem, ali je problem i dalje nerešen.

mu platim račun za suve šljive u
jasni da je reč o grešci. Posle mesec
ogradu da platim oko 50 hiljada dinara
e Mijajilović.

ao i da je sa celim slučajem upoznato

i tužilaštvo, ali da računi i prijave i dalje stižu.

"U martu 2010. godine zvali su me iz Poreske uprave da objasnim utaju poreza od oko pet miliona dinara za cement. Tu je i poziv iz "Ce marketa" o zakupu poslovnog prostora o kome ja ne znam ni gde se nalazi", kaže Mijajilović.

Sva dugovanja upućuju na firmu "Komiks global" čiji je direktor navodno Branko Mijajlović. Neko je očigledno zloupotrebio Brankove lične podatke i na falsifikovanoj ličnoj karti nalepio drugu sliku, a zatim registrovao preduzeće.

Policija identifikovala počinioca

Inspektor Policijske uprave Beograd tvrdi da je policija za sada identifikovala V.T. (46) iz Beograda, koja je, služeći se lažnom dokumentacijom, od oštećenih preduzeća iz Beograda naručivala robu i potom je prodavala za gotov novac.

Preduzeće "Komiks global" i dalje je aktivno i nalazi se na spisku u Agenciji za privredne registre. Da bi se registrovalo preduzeće potrebno je agenciji podneti odluku o osnivanju, račun iz banke, fotokopiju lične karte i, takozvani, OP obrazac.

Ako sud ili opština overi i izda dokument, u Agenciji za privredne registre ističu da, u tom slučaju, nisu dužni da naknadno proveravaju verodostojnost dokumenata, a da se eventualne greške moraju prijaviti.

Gabrijela Petković-Jovanović iz Agencija za privredne registre kaže da ukoliko se tako overen dokument preda Agencija za privredne registre, onda je ona dužna da u roku od pet dana registruje to privredno društvo.

Krađa identiteta

Pošto su kreditne kartice najrasprostranjenije sredstvo plaćanja, one predstavljaju raj za prevarante, pogotovo u zemljama u kojima se kartice tek uvode ili postaju osnovno sredstvo plaćanja. Osim novca sa Vašeg računa, kradu se i Vaši lični podaci.

Ovo je jedna od najopasnijih stvari koja može da Vam se desi i da Vas , što je najcrnje , košta mnogo novaca, vremena i živaca.

Jedan od najlakših načina da Vam ukradu identitet su Web stranice koje nude određene finasijske usluge ili nude kreditne kartice. Kad aplicirate preko intereneta za neku takvu karticu Vi prevarantima dajete sve podatke koji su im potrebni a oni samo promene adresu i ako ona stiže na adresu prevaranata a kasnije od Vas da traži da platite račune.

Sa sajta prevara.info

Drugi način su lažni promoteri. U ovom slučaju ponude Vam se aplikacije za kreditne kartice koje izgledaju kao prave i Vi iz radoznalosti ispunite jedan od tih formulara. Ti formulari se kasnije prepravljaju, odnosno promene se neki podaci i ako je kartica odobrena ona će otići u ruke prevaranata (Promeni se Vaše ime i adresa na koju će stizati informacije vezane za Vašu karticu)

Treći način je telefonski poziv. Kod telefonskih poziva se radi na "frku", tj , kažu Vam da ste potrošili ogroman novac sa kartice, da ste dužni određeni iznos koj je nenormalno visok i slično. Prevaranti će učiniti sve da Vas iznerviraju ili prepadnu i tako se najlakše dolazi do određenih podataka koji se kasnije korist za prevare. Isti će se predastavljati kao službenici banaka, velikih firmi ili čak i kao policajci.

Ovaj način je i najrasprostranjeniji. Prevaranti Vas pozovu, najčešće znajući unapred sa kojom bankom poslujete, i "obaveste" Vas da je sa Vašeg računa potrošena enormna količina novca i da morate da platite u roku od 24 sata. Vi se prepadnete ili počnete da vrištite, ali ma koja da je reakcija, ona odgovara prevarantima. Kad izazovu željenu reakciju kod Vas, ljubazno Vam kažu da se smirite i da sve može da se sredi i da je po sredi greška. Ipak, da bi saznali tačno o kakvoj grešci se radi, tražiće Vam podatke kao što su: Ime i Prezime, broj kartice i pin kod. Naravno tražiće i adresu i još neke podatke koji nisu uopšte bitni nego su samo tu da Vas "uvuku" u priču. Kad im date ove podatke dolazi do krađe identiteta.

5.1.2. Проневере

Основно обележје је прибављање противправне имовинске користи противзаконитим изменама или фалсификовањем докумената од стране онога коме је поверено вођење тих докумената.
Овај облик, широко распрострањен у категорији криминала беле крагне, увођењем ИТ у сферу материјално-финансијског пословања, знатно добија у квалитету и квантитету.

Типични облици проневера су :

- **Фалсификовање књиговодствене документације;**
- **Креирање фиктивних фактура, путних рачуна, платних спискова и друго;**
- **Фалсификовање кредитних извештаја; и**
- **Креирање лажних финансијских података;**

Novi Sad: Bankar uhapšen zbog pronevere

Novosadski bankar uhapšen je zbog sumnje da je kao direktor filijale Erste banke proneverio više miliona dinara.

Zoran R. (52) iz **Novog Sada** uhapšen je zbog sumnje da je kao direktor filijale **Erste banke** u Beočinu **proneverio** više miliona dinara, saopštila je novosadska policija.

Osumnjičeni je, kako se navodi, neovlašćeno podigao više miliona dinara sa štednog računa jednog 88-godišnjeg klijenta i taj novac potom ubacio u bankomat.

Dodaje se da je osumnjičeni tako pokušao da prikrije manjak koji je stvorio neovlašćenim uzimanjem novca iz bankomata.

- Novi Sad:Opljačkana Erste banka!
- Novi Sad: Traganje za misterioznim pilotom!
- Novi Sad: Razvoda koliko i brakova

(Beta)

Pronevere fondova EU

Dok evropske vlade ulažu ogromne napore da stabilizuju zajedničku valutu, milijarde evra nekontrolisano otiču iz budžeta Evropske unije.

Do ovakvog zaključka su došli autori istraživanja koja je za BBC sproveo glavni reporter *Biroa za istražiavčko novinartsvo* pri Siti koledžu u Londonu "Angus Stikler".

Istraživanje je pokazalo da su razmere pronevera i korupcije u trošenju evropskih fondova za regionalni razvoj zastaršujuće.

Fond za "strukturni regionalni" razvoj

Iako se stanovnici Evrope privikavaju na novu stvarnost, čija je glavna karakteristika drakonska štednja, Evropska unije i dalje nemilice troši.

Njen strukturalni fond raspolaže sa kolosalnih 350 milijardi evra, iz kojih se finansiraju programi za regionalni razvoj u zemljama članicama.

Radi se o 650 hiljada projekata čiji je glavni cilj da se podstakne razvoj najsiromašnijih delova Unije.

Ekipa BBCija je u saradnji sa *Biroom za istraživačko novinarstvo* od marta do novembra 2010. pregledala nekoliko stotina hiljada dokumenata koji ukazuju na pronevere ogromnih razmera i na to da se novac poreskih obveznika sliva u džepove italijanske mafije.

Novac za vetrenjače u džepu mafije

Diskretni zvuk turbina na vetar stiže sa gotovo svakog brda u unutrašnjosti Sicilije - a bezbrojni redovi ogromnih gvozdenih vetrenjača su vizuelni trag milijardi evra koje je Evropska unija uložila u ovo siromašno italijansko ostrvo.

Pre dva meseca, italijanske vlasti zaplenile su od mafije imovinu vrednu milijardu i po evra - ispostavilo se da su evropska sredstva za izgradnju vetrenjača na Siciliji završavala u džepovima mafije.

Šema pranja novca bila je vrlo složena, kaže najpoznatiji italijanski tužilac za organizovani kriminal Roberto Skarpenoto.

"*Naša istraga na Siciliji pokazala je da se nekoliko stotina kompanija bavi proizvodnjom alternativne energije - vetrenjača i solarnih panela. Sve su one u vlasništvu tri ili četiri čoveka, koji su povezani sa mafijom*", rekao je tužilac Skarpenoto BBC-ju.

Koza nostra je uložila dosta vremena i napora u složenu operaciju obezbedjenja sredstava iz fondova EU, ali joj se trud itekako isplatio.

"*Ti ljudi su, uz pomoć političara i opštinskih službenika dobijali dozvole koje su drugim kompanijama bile nedostupne, kupovali su zemlju zastrašivanjem vlasnika. Njihove ponude nisu se mogle odbiti.*" objašnjava Skarpenoto.

Mamac: nepovratna sredstva EU

5.1.3. Преваре

Превара је довођење неког у заблуду, лажним приказивањем чињеница или прећуткивањем чињеница, да би се тиме прибавила противправна имовинска корист.
Потенцијалне жртве су практично сви корисници ИТ, место извршења је практично цела планета, модалитети су у распону од једноставних и краткотрајних до сложених и дуготрајних.

Преваре су најчешће оријентисане на :

- **Државну управу;**
- **Услуге;**
- **Осигурања;**
- **Инвестиције;**
- **Финансијске институције;**
- **Физичка лица и др.**

http://gojko-prevareniodvinaera.blogspot.com/

KAKO SE ZAŠTITITI OD PREVARE OSIGURAVAJUĆE KUĆE

Prevareni od Viner Štetiše WIENER STÄDTISCHE

4,107

среда, 19. октобар 2011.

MALA BARA A KROKODILI SE MNOŽE ?!

Ko još normalan poverava kokoške na čuvanje liscu ili kupusište volu?

Niko naravno samo onaj koji ne prepoznaje maskiranog lisca i vola....

O čemu ja to govorim? O životnom osiguranju ...

Šta je to životno osiguranje?

Vaša iskustva sa životnim osiguranjem?

- Krajnje pozitivna
- Pozitivna
- Krajnje negativna
- Negativna
- Nemam ih

Vote Прикажите резултате

Досадашњи број гласова: 42
Преостали број дана за гласање: 6

Osiguranje života - veliki rizik?

5.1.4. Фалсификовање

Појава високо квалитетних скенера и ласерских штампача у боји, као и великог броја врло снажних пакета за графичку обраду, ствара изузетне услове и могућности за реализовање веома успешних фалсификата. Типични облици фалсификовања односе се на фалсификовање:

- **Новца;**
- **Докумената (сведочанстава, диплома, уверења, исправа);**
- **Хартија од вредности (меница, чекова, кредитних писама и слично);**
- **Улазница;**
- **Потписа;**
- **Печата, штамбиља и жигова;**
- **Знакова за обележавање робе;**
- **Знакова за вредности (поштанске и таксене марке);**
- **фалсификовање електронске поште**

Kosovski polic

Komentara 4

Share 2 Like

Veća grupa pripadnika kos
posedovanja falsifikovane
osnovnom školom nalazili
direktoratu Policije Kosova

Policajci sa lažnim diplomam
unutrašnju kontrolu policije.
dokumentima. Oni su udalje
falsifikovane diplome srednj
policiju.

Prasići "krili" falsifikatore novca

Komentara 0

Share 1 Like Tweet 0 +1 0

Bugarska policija otkrila je ilegalnu štampariju za izradu lažnih evra i dolara i uhapsila tri osobe u mestu Kazanlak, u južnom delu zemlje. Zanimljivo je da niko nije mogao da čuje prese dok rade, pošto su prasići u obližnjenjem svinjcu glasno groktale.

Bugarski ministar unutrašnjih poslova Cvetan Cvetanov izjavio je danas da je akcija pod nazivom "Sikret servis" realizovana tokom transfera 50.000 evra u gradu Šipka.

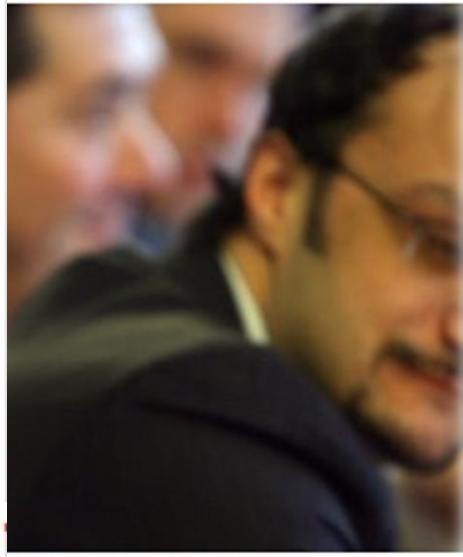
Groktanje prasićima "pomoglo" falsifikatorima

"Mašine su zaplenjena u selu Donje Sahrane kod Kazanlaka. Tamo su bile dve kuće, u jednoj je bila hala, gde je bila instalirana štamparija. Pored hale su čuvani prasići, koji su jako groktali, kada štamparija radi i tako maskirali njen šum",

ovao svoj naučni rad

7 +1 0

ra Martinovića, koji je 5 godina
rad, šokirao kolege pravne stručnjake,



m naslovima: Aleksandar Martinović

" moralno nedopustiva, kolege smatraju
krene disciplinski postupak i preispita

ultetu u Novom Sadu u naučnom
javljivao naučni rad iste sadržine samo
09. godine) i za to dobijao autorski

že da je Martinović izvršio klasičnu

5.1.5. Изнуде и уцене

Поред класичних претњи, код којих ИТ служи само за преношење претњи и захтева, постоје и претње оштећења или уништења рачунарских компоненти, софтвера и података, као и претње одавања података и информација до којих је извршилац нелегално дошао из информационог система корисника ИТ.

Објекти напада могу бити правна и физичка лица. Правним лицима се прети наношењем материјалне штете и нарушавањем угледа, а физичким лицима се прети нарушавањем угледа и части.

На пример у случајевима када је објект напада банка, најчешћа је претња да ће бити јавно објављени рачуни и износи финансијских средстава клијената, а у случају физичких лица најчешћа је претња да ће објавити податке о здравственом стању, инкриминисаној прошлости, сексуалној или другој настраности и слично.

Čovek izvršio samoubistvo zbog pretnje policijskog malvera

Sajber hronika, 14.03.2014, 09:02 AM

Prema pisanju lokalnih novina Braila24, tridesetšestogodišnji Marcel Datcu iz rumunskog sela Movila Miresii izvršio je samoubistvo zato što je poverovao da je upozorenje koje je video na računaru, kojim mu je zbog navodnog kršenja zakona naloženo da plati kaznu od 70000 leja (15519 evra) u zamenu za zatvorsku kaznu u trajanju od 11 godina, pravo i da zaista dolazi od policije.

Policijski malveri su pretnja sa kojom se korisnici računara širom sveta relativno često susreću. Ovaj biznis model pokazao se do sad unosnim za sajber kriminalce, jer ne mali broj žrtava poveruje u istinitost upozorenja koje prikazuje malver na zaraženom računaru. Oni koji nasednu na ovaj poznati trik kriminalaca plate kaznu koja uglavnom ne prelazi iznos od nekoliko stotina evra.

Ono što se dogodilo Marcelu Datcu je najgori scenario koji je do sada viđen. On je pronađen u dnevnoj sobi, obešen, sa četvorogodišnjim sinom u naručju oko čijeg vrata je takođe bio konopac. Jedno od njegove dece pronašlo je njihova tela.

Komšije kažu da je porodica Datcu bila normalna, srećna porodica. Datcu i njegova supruga imaju još troje dece iz prethodnih brakova.

Izvori bliski istrazi kažu da je nesrećni čovek ostavio oproštajno pismo svojoj ženi u kome je rekao da ne misli da je to što je uradio normalno i da se svima izvinjava. On je u pismu objasnio da je dobio upozorenje da mora da plati 70000 leja ili da odsluži 11-ogodišnju zatvorsku kaznu koju ne bi mogao da podnese, kao i da ne želi da njegov sin (koga je ubio) pati zbog njega.

Upozorenje koje je video Datcu nije bilo pravo. Posle poseta nekim porno sajtovima zarazio je računar policijskim ransomware-om. Zato je mislio da upozorenje zaista šalje policija i u očaju se odlučio na ovaj ekstremni korak.

Navodna kazna od 70000 leja koliko je Datcu trebalo da isplati kriminalcima nije uobičajena, posebno u Rumuniji u kojoj policijski malveri obično traže male sume, najviše oko 300 leja (66 evra).

Bez obzira na visinu "kazne", stručnjaci već godinama uporno ponavljaju savet korisnicima da ne izlaze u susret zahtevima sajber kriminalaca i ne plaćaju, posebno zbog toga što se u većini slučajeva ove pretnje lako mogu ukloniti sa

Prijavite se na našu mailing listu i primajte najnovije vesti (jednom dnevno) putem emaila svakog radnog dana besplatno:
vaš@e-mail Prijava

Izdvojeno

Čovek izvršio samoubistvo zbog pretnje policijskog malvera

Prema pisanju lokalnih novina Braila24, tridesetšestogodišnji Marcel Datcu iz rumunskog sela Movila Miresii izvršio je samoubistvo zato što je pov... Dalje »

Uhapšeno pet osoba koje se povezuju sa Tor online marketom Utopia

Holandsko tužilaštvo saopštilo je u sredu da je uhapšeno pet osoba zbog trgovine drogom i oružjem na skrivenim online marketima. Trojica uhapšen... Dalje »

Podignuta optužnica protiv Rosa Ulbrihta, vlasnika sajta Silk Road

Tužilaštvo u Njujorku podnelo je dopunjenu

5.1.6. Нарушавање приватности

Нарушавање приватности је кршење једног од основних људских права. Евидентирање, чување, ажурирање и коришћење података о физичким лицима је потребно за обављање многих послова, остваривање права и заштите. Корисник или власник података је дужан да, при обављању свих послова у вези података о физичком лицу, то ради у складу са законом и да онемугући злоупотребу тих података. Изнето важи како за класичне евиденције тако и за информационе ситеме који користе ИТ.

Главни сегмент заштите информационих система и података је управо заштита података о лицима, јер је то кључни основ правне сигурности за примену ИТ. У многим модалитетима кривичних дела је нарушавање приватности први корак, а често основ и повод за извршавање кривичних дела.

5.2. Технике реализације злоупотребе IT

У функционисању сваког информационог система постоји пет основних фаза које представљају критичне тачке са становишта заштите, и то:

- **Улаз;**
- **Излаз;**
- **Програмирање;**
- **Употреба, и**
- **Пренос/комуникације.**

5.2.1. Улаз

Ова манипулација, која носи назив „мућкање подацима“ (Data Diddling), представља свакако најједноставнији, најсигурнији и најопштији метод коришћен у рачунарском криминалу, а укључује измену података пре или у току њиховог уноса у рачунар.

Измене може извршити свако ко је повезан са или има приступ до процеса креирања, записивања, преноса, шифрирања, прегледа, контроле, конвертовања или трансформисања података који се коначно уносе у рачунар. Те манипулације се могу реализовати на више начина:

- **Додавање података;**
- **Изостављање података;**
- **Измена постојећих података;**
- **Замена постојећих података;**
- **Брисање постојећих података.**

Најчешћи циљеви наведених активности су прибављање одређене користи себи или другима, проневера, крађа и прикривање крађе кроз:

- **Модификацију платних спискова;**
- **Генерисање фиктивних запослених, спољних сарадника и снабдевача;**
- **Повећање прековремених часова;**
- **Фалсификовање износа зајма, кредита или кредитне рате;**
- **Исплаћивање снабдевача два пута;**
- **Фиктивно унапређење запослених;**
- **Увећање наплата одређених финансијских потраживања;**
- **Креирање фиктивних финансијских трансакција;**
- **Држање запослених на платном списку и након престанка радног односа;**
- **Трансфер новца на лажне рачуне;**
- **Фалсификовање стања у магацину друго.**

5.2.2. Излаз

Најчешћи видови криминалне активности на овом нивоу су усмерене на крађу података, као што су: листа купаца, кадровска листа, платни спискови, пословне тајне, планови и резултати истраживања и друге вредне и поверљиве информације, али и крађу вредних софтверских производа и програма.

Ови деликти често укључују сарадњу радника из фирме са једним или више особа изван фирме, који су најчешће пословни конкуренти, професионални криминалци или страни агенти.

Коришћене технике за ову врсту криминала су најчешће копирање или слање електронским путем датотека, база података, софтвера или програма.

5.2.3. Програмирање

Програмирање је један од најбитнијих сегмената у развоју и функционисању информационог система.
Могуће злоупотребе информационе технологије у фази програмирања најчешће се јављају у следећим облицима:

- **Замена програма;**
- **Брисање значајних програмских инструкција;**
- **Модификација програма;**
- **Саботажа програма;**
- **Неовлашћена измена/брисање података;**
- **Смањење перформанси рачунара .**

Манипулације на улазу или излазу се могу реализовати и без посебног информатичког знања,

Манипулације на нивоу програмирања су у смислу начина извршења много специфичније (потребно је познавање програмирања, приступ изворним кодовима програма, познавање организације функционисања информационог система и слично).

Откривање ових злоупотреба је доста тешко.

Постоје бројне и веома суптилне методе и технике, од којих су најпознатије:

- **Техника „сецкане саламе“;**
- **Ловац, Хватач;**
- **Писмо-бомба;**
- **Надмудривање**
- **Тројански коњ;**
- **Прикривен улаз;**
- **Логичка (временска) бомба;**
- **Прикупљање „отпадака“;**
- **Вируси и црви.**

Техника „сецкане саламе“ (Salami swindle): је заснована на програмираној процедури која је смештена (прикривена) у неком од програма којим се обрађују подаци са циљем да се, из великог броја стања **издвајају интересантни (значајни) подаци.**

Ловац, Хватач („Sniffer“ programi): Ови програми се инсталирају у чворовима мрежа и у стању су да електронски **контролишу пренос** који се кроз мрежу одвија, **хватајући идентификационе параметре и лозинке**, бројеве кредитних картица и поруке које садрже **кључне речи**.

Писмо-бомба (Letter bomb; E-mail bomb): E-mail бомба је једноставан и врло ефикасан разорни алат.
Као што и име показује, реч је о програму који иницијално активира хиљаде порука у „поштанском сандучету“ примаоца, стварајући хаос у његовом систему, па чак и блокирајући рад тог система.

„Надмудривање“ (Spoofing): Ова техника има два појавна облика: локали и мрежни.

Локални облик подразумева коришћење специјално урађеног програма који симулира поступак укључивања у систем (log-on процедура).

1. **Такав програм се активира на одабраном терминалу,**
2. **Легитимни корисник седа и уноси лозинку.**
3. **Добија одговор да лозинка није исправна.**
4. **Мислећи да је код уноса погрешио, понавља процедуру**
5. **Идентификациони подаци су већ евидентирани у датотеци преваранта и на тај начин „проваљени“.**

Мрежна техника подразумева хватање, измену и ретрансмисију комуникационог тока на начин који обмањује примаоца. Ову технику хакери користе да би мењали изворне адресе или друге податке у заглављу TCP/IP пакета (IP spoofing) ради симулирања поверљивог рачунара и на тај начин добијања приступа до циљног рачунара. Да би користили ову технику, хакери морају претходно различитим техникама доћи до IP адресе поверљивог рачунара.

- **Тројански коњ (Trojan horsse) је једна од најопштијих метода за преваре и саботаже базиране на рачунарским програмима.**

- **Састоји се од скупа илегалних инструкција (рутина) које су убачене у легални програм ради извршавања конкретних илегалних радњи.**

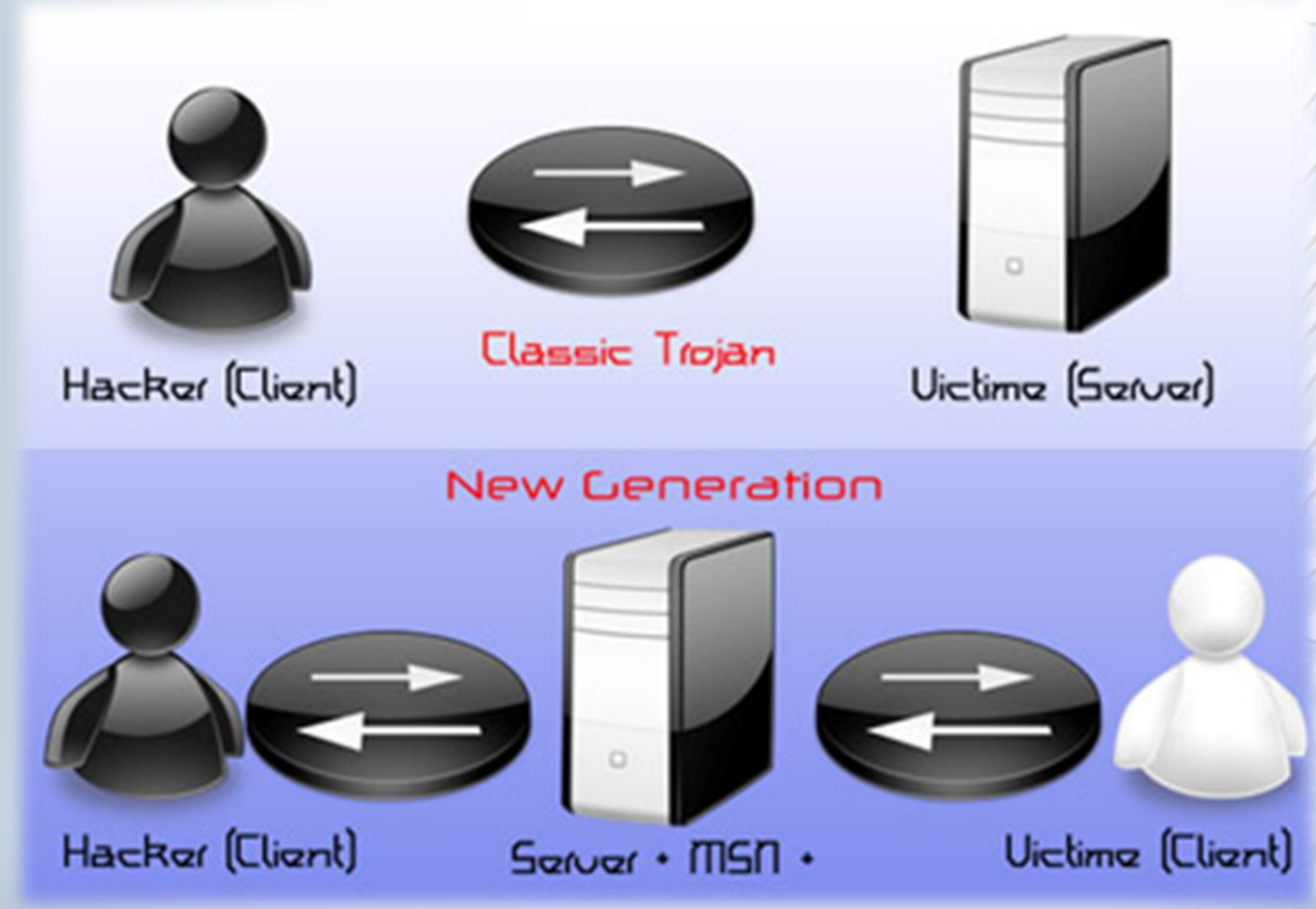
- **Ове рутине ће извршавати неовлашћене функције, али ће обично дозвољавати и програму, у који су убачене, да извршава оно чему је намењен.**

- **Тешко их је открити**
- **Инсталира се најчешће инсталацијом неког жељеног програма**
- **Нападач види апсолутно све што радите на рачунару и може да искључи и програме за заштиту**

- **Није вирус, не копира се и не умножава**

Тројанци нове генерације

- **Пример MSN тројанац**



Milijunima korisnika Facebooka upućen trojanac

Facebook je sa svojih 400 milijuna korisnika draga meta mnogim hakerima i spamerima. A kako izvještava tvrtka McAfee, koja izdaje sigurnosni softver, ovih su dana pojačali svoju zlonamjernu djelatnost.

18. ožujka 2010 15:48 Tihomir Mršić, Hi Tech

članak komentari (1) Sve iz: Office


From: Your Facebook
To:
Cc:
Subject: Facebook Password Reset Confirmation! Customer Support.
Message | Facebook_password_357.zip (699 B)

Dear user of facebook,

Because of the measures taken to provide safety to our clients, your password has been changed.
You can find your new password in attached document.

Thanks,
Your Facebook.

Mnogim je korisnicima Facebooka, upozorava McAfee, upućena poruka koja bi mogla zaraziti njihova računala softverom dizajniranim za krađu lozinke i drugih podataka.

"U posljednja dva dana poslani su milijuni poruka", ističe Dave Marcus, McAfeejev direktor sigurnosnih istraživanja.

"Čini se da poruke dolaze od Facebooka, s povratnom adresom koja izgleda legitimno, ali lažna je, poput 'help@facebook.com', pa ne nasjedajte", rekao je Marcus.

U poruci piše da će Facebook resetirati lozinku, a korisnik bi trebao preuzeti privitak koji sadržava novu. U potpisu stoji: "Hvala, vaš Facebook." Ispod teksta

Privitak je zapravo zloćudni program, trojanski konj koji može zaraziti računalo bez ikakvih vidljivih znakova.

"Ne postoji internetski servis koji će vam automatski resetirati lozinku i poslati novu, bilo u poruci, bilo u privitku, i već je to dovoljan znak za uzbunu", zaključuje Marcus.

No kako je internetske početnike lako prevariti, upozorenja nikad dosta...

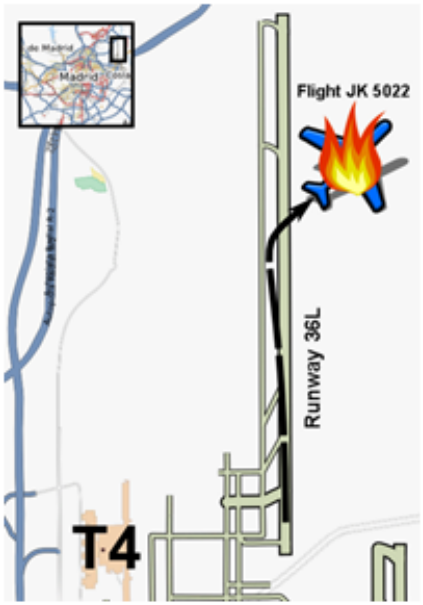
VEZANE VIJESTI

- Kupujmo hrvatsko na Facebooku i Twitteru
- Cameron Diaz "najopasnija" zvijezda
- Osniva se fond za financiranje novih Facebookova
- Akvizicije vesele Wall Street
- Fincher će masno zaraditi na filmu o Facebooku

Trojanac doprineo avionskoj nesreći 2008 u Španiji

26.08.2010

Rezultati istrage pada aviona 2008 godine u kome je poginulo 154 putnika i članova posade, **ukazuju na otkrivanje Trojanca u centralnom kompjuterskom sistemu koji je nadgledao tehničko stanje letelice**. Tragična nesreća se desila na letu *Spanair 5022* po poletanju sa Madridskog-Barajas internacionalnog aerodroma, na rutinskom letu ka Gran Kanariju. Svega 18 ljudi je preživelo ovu nesreću, i u Španiji se ovo smatra za najgoru avionsku nesreću u poslednjih 25 godina.



Prema novinama El Pais, interni izveštaj avionske kompanije je otrkio da je kompjuter lociran u glavnom štabu kompanije u Palmi, Majorka, trebao da identifikuje tri tehnička problema aviona, ali s obzirom da je bio zaražen sa malverom, ti problemi nisu otkriveni. Važna napomena je da malver nije prouzrokovao pad aviona, nego je samo sprečio otkrivanje tehničkih problema aviona.

Američki Nacionalni Odbor za sigurnost u transportu, na primer, je u svojoj preliminarnoj istrazi napisao, da je avion uzleteo sa ograničenim krilcima i poprečnim gredicama, i da audio alarm se nije čuo kao upozorenje jer je sistem koji dostavlja energiju do *take-off warning* sistema (TOWS) omanuo.

Ukoliko se pokaže da je priča EL Pais-a tačna, malver je doprineo tome da se ovi propusti ne otkriju, u suprotnom, avion sigurno ne bi ni poleteo. Zbog toka istrage, ime malvera još uvek nije objavljeno. Finanlni izveštaj o istrazi ove nesreće će biti prezentovan u Decembru mesecu.

Priredio **Redakcija** · Pripada kategorijama Bezbednost

POVEZANI ČLANCI

- Trojanac na mobilnim telefonima...
- Pentax Optio E90...
- Uhapšeni “hakeri” koji su emitovali “trojanca
- Kompanije moraju uvesti standarde bezbednosti...
- Trojanac za Mac-ove...

Прикривен улаз (Trap Door)

омогућава заобилажење механизама заштите
омогућава неовлашћеном лицу да извршава привилеговане инструкције.

У развоју оперативних система, сложених и великих апликација, уобичајена је пракса да програмери укључују у програме и помоћна софтверска средства за тестирање и отклањање уочених недостатака.
Ове могућности се означавају као „прикривени улаз“ или „задња врата“.
Они се по правилу елиминишу у финалној верзији програма, али се по некад оставе или намерно да омогуће каснији приступ и модификацију или ненамерно, као резултат грешке или логичког превида.

Логичка (временска) бомба (Logic(time)bomb)

- Програмирани, са одложеним дејством, изазивач нежељених догађаја у рачунару, као што су блокирање/успоравање рада рачунарског система или уништавање/модификовање података и/или програма.
- Логичка бомба је обично део неког већег програма.
- Она је практично невидљива у систему и постаје оперативна само под одређеним условима, као што су датум и време или одсуство/присуство неког податка, као што је на пример нечије име и слично.
- На наведени начине се оне могу контролисано активирати или у одређеном тренутку или периодично.

Прикупљање „отпадака“ (Scavenging)

Класично прикупљање података:

- **остављених у или око рачунара,**
- **претраживања одбачених штампаних извештаја и сл.,**

Префињеније методе:

- **Подаци прикривени, остављени (не намерно) у неком делу рачунара након извршења трансакције.**

Дешава се да ОС не обрише садржај бафера (служи за привремено смештање У-И података.
Неки ОС не бришу привремено коришћени хард дисковима.
Нови подаци се уписују преко старих, а то се може искористити да се прво прикупе (ишчитају) стари, пре него што се преко њих упишу нови подаци.

Класичан пример је кад корисник одбаци постојећи диск зато што је недовољног капацитета/брзине или делимично оштећен, а до њега дође злонамерано лице (дискове пре одбацивања треба физички онеспособити).

Вируси и црви (Viruses and Worms)

Вирус се дефин. као програм који се шири сопственим реплицирањем, инфицирајући друге програме модификујући их својом сопственом копијом.

Он се укључује у ОС и у стању је да „зарази“, брзо и комплетно, све његове програме, изазивајући потпун застој целог рачунарског система „харањем“ његовим садржајем. Ако се „заражен“ програм транспортује посредно (УСБ) или директно (преко рачунарске мреже) „инфекција“ се преноси.

Механизам „инфекције“ сам по себи није опасан, али вируси садрже и програмске инструкције које извршавају и неке додатне функције. Ове секундарне функције могу бити:

- **Промена бројева у датотекама,**
- **Извршавање непотребних рачунања што успорава рад,**
- **Брисање садржаја на диску и слично.**

Вирус се покреће када је инфицирани програм активан, али се може активирати и временским механизмом или неким догађајем.

Рачунарски црв

Рачунарски црв је програм или серија програма који се активирају независно и не атакују на друге програме, већ директно нападају рачунарски систем заузимањем његових ресурса преузимањем процесора и покушавањем извршавања илегалних активности у систему

Супротно вирусима, црви се не реплицирају додавањем својих копија другим програмима и обично се састоје од вишемодулног скупа инструкција, сувише великог да би се могао прикрити у датотекама оперативног система.

Тешко их је прикрити

5.2.4. Употреба

- **Неовлашћено коришћење рачунарског система слично је неовлашћеном коришћењу телефона, копир апарата, службеног аутомобила и слично, али како је рачунарско време знатно скупље, његово неовлашћено коришћење може изазвати озбиљне проблеме.**
- **Постоје бројни случајеви у којима су запослени користили рачунар за обављање приватних послова, а многи професионални информатичари и корисници, нажалост, често третирају рачунар и као играчку.**

5.2.5. Пренос/комуникације

Ово је један од најосетљивијих и најрањивијих нивоа информационог система, а основни разлог је што је, с једне стране, врло тешко обезбедити физичку заштиту комуникационих линија због великог географског простора који треба покрити, а с друге стране, већ постоји читав низ префињених метода и техника које се на овом нивоу могу користити у извршавању илегалних радњи.

Од познатих класичних метода и техника које се користе у мрежном амбијенту свакако треба поменути следеће:

- Лажно представљање (маскирање);
- Прикривање канала;
- Прислушкивање/пасивна инфилтрација;
- Активна инфилтрација;
- Електронско прислушкивање;
- Широко-скално скенирање мреже;
- Ометање сервиса.

Лажно представљање (маскирање):

Ова метода се заснива на **преузимању идентитета легалног корисника** или у неким случајевима кодираног терминала, ради извршавања неовлашћених трансакција.

Нападач се може претварати да је легалан корисник и да као такав покуша да приступи ситему и његовом садржају.

За овакву реализацију потребно је да претходно, на један од бројних начина, дође до идентификационих и аутентификационих информација о легалном кориснику, а да се затим укључи као корисник којег систем прихвата.

Прикривање канала

- Основу ове методе чини обезбеђивање комуникационог канала који је ван контроле и који омогућава пренос информација у и из рачунара без увида легалних субјеката.

- Легалне функције даљинског модификовања софтвера и одржавања рачунара и база података се могу злоупотребити на овај начин. Ове легалне функције се обично поверавају произвођачу и испоручиоцу опреме или специјализованим фирмама.

Прислушкивање/пасивна инфилтрација

Прислушкивање, у класичном смислу, може се дефинисати као тајно пресретање телефонских разговора у тачки која је удаљена од саговорника. У истом значењу термин се примењује и на рачунарске комуникације, с тим што су саговорници рачунари.

Подразумева укључивање специјалног уређаја на комуникациону линију и надгледање саобраћаја који се том линијом одвија између рачунара и легалних корисника.
Пасивна, или индиректна инфилтрација добила је назив, јер нападач само остварује увид, али се не меша у комуникацију.

Активна инфилтрација

Подразумева специјални уређај повезан на комуникациону линију, преко којег се прати пренос информација између легалног корисника и рачунарског система.

У овом случају реализатор инфилтрације (нападач) може

- **зауставити корисников улаз и модификовати га, или га комплетно заменити, пре него што га проследи до рачунарског система.**
- **Послати кориснику лажну поруку да систем није расположив или да је „пао“.**
- **Кад корисник пошаље систему поруку да се искључује, нападач ту поруку може зауставити, а кориснику шаље, за њега очекивану али лажну поруку да је рачунар прихватио прекид рада. Након тога нападач наставља да ради уместо легалног корисника.**

Метода је добила име активна, или директна инфилтрација, јер нападач активно учествује у преносу порука.

Електронско прислушкивање

Добро је познато да сваки електронски уређај производи електро-магнетно поље које може изазвати интерференцију (сметњу) на радио и ТВ пријемницима. Овај феномен се изучава већ неколико деценија, што је резултирало међународно прихваћеним методама за мерење интерференције коју изазива електронска опрема. Ово су искористиле многе земље за доношење закона о дозвољеном нивоу зрачења коју електронска опрема може генерисати.

Ово зрачење, нарочито код уређаја који раде у дигиталном режиму, може бити ухваћено, анализирано и декодирано, тј. електронски прислушкивано, чиме се могу репродуковати све информације и подаци садржани у том зрачењу.
Ово је нарочито опасно за системе у којима се захтева висок ниво тајности података.

Широко-скално скенирање мреже

Нападачи развијају и користе алате за скенирање великог броја рачунара (хостова) ради откривања њихових слабости и недостатака.

Десетине хиљада до милиона хостова може бити скенирано у кратком временском периоду, идентификујући који хостови су осетљиви а који нису.

Алати за скенирање могу лако утврдити који оперативни систем неки рачунар користи, како би се према њему активирао специфичан атак.

- **Нападачи користе нове технике скенирања, од којих неке могу продрети и кроз заштитне баријере (firewalls). Најчешће се скенирање обавља по мрежним адресама, именима домена DNS-у.**

- **Чињеница је да се нападачи све више усмеравају ка кућним системима и то из следећих разлога:**
- **кућни системи су генерално слабије заштићени и самим тим погодни за компромитацију;**
- **мања је вероватноћа да власници кућних рачунара постану свесни да су њихови системи компромитовани и**
- **кућни системи , након уградње „тајних врата“, врло су погодни да се користе за лансирање атака на друге системе.**

Ометање сервиса

Ометање сервиса се реализује намерним преоптерећивањем интернет сервера скоро непрекидним захтевима за Web страницама, чиме се спречавају легитимни корисници да приступе жељеним страницама или се чак обара сервер.

Сама техника ометања сервиса се спроводи на следећи начин:

1. **Криминалци најпре на већем броју рачунара који имају широк опсег приступа Интернету, подметну програме за даљинску контролу. Ови програми ће на команду криминалца издати скоро непрекидну серију ping-ова ка Web сајту жртве;**
2. **Када је криминалац спреман за напад, он активира програм да почне да пингује специфичне циљне адресе. Рачунар који садржи програме за даљинску контролу понаша се као „зомби“;**

3. **Жртвин рачунар одговара на сваки пинг, али зато што „зомби“ рачунари дају погрешне изворне адресе за пингове, жртвин рачунар није у стању да успостави конекцију са „зомби“ рачунарима. Зато што жртвин рачунар очекује одговор на његов повратни пинг и зато што има много више „зомби“ рачунара, жртвин рачунар постаје неуспешан и не ради ништа осим што одговара на лажне пингове и/или крахира;**
4. **Типично, после неког времена криминалац командује програмима да престану да пингују жртву. Ово кратко трајање пингова није зато што је криминалац постао фин, већ зато што би дуже трајање напада пинговима олакшало инжињерима жртве да уђу у траг извору напада.**

Програми за даљинску контролу и инструкције за њихову примену су расположиви на про-хакерским сајтовима од јуна 1999. године.

Постоји и други тип оваквих напада који користе такозвани „пинг смрти“ („ping of death“) да генерише грешке у софтверу (bug-ове) на Web серверу.

Kratak sadržaj:

- Kriptografija.
- Kerkohof princip.
- Klasične kriptografske metode.
- Dva fundamentalna principa kriptografije.

10. Zaštita podataka
10.1. Kriptografija

Reč kriptografija vodi poreklo od grčkih reči:
kriptos - skriveno, i
grafos - pisati.
U doslovnom prevodu značilo bi „skriveno pisanje”.

Istorija kriptografije doseže hiljadama godina unazad.

U stručnoj literaturi se pravi razlika između šifrovanja (*eng. cipher*) i kodiranja (*eng. code).*
Šifrovanje omogućava zamenu **znak za znak** (bit za bit) bez obzira na jezičku strukturu poruke.
Nasuprot tome **kodiranje** zamenjuje **jednu reč drugom** rečju ili simbolom.

- Kodovi se više ne koriste iako su imali slavnu istoriju.
- Najuspešnijim kodom smatra se onaj koji su koristile američke vojne snage na Pacifiku tokom Drugog svetskog rata.

Na krajevima veza postavili su Navaho Indijance koji su međusobno razgovarali na svom jeziku. Vojne izraze su opsivali rečima iz Navaho jezika.

Protivtenkovsko oružje su zvali *čaj-da-gahi-nail-caidi* (bukvalan prevod: ubica kornjača). Japanci naravno nisu poznavali taj jezik i nije postojao nikakav pisani trag o njemu.

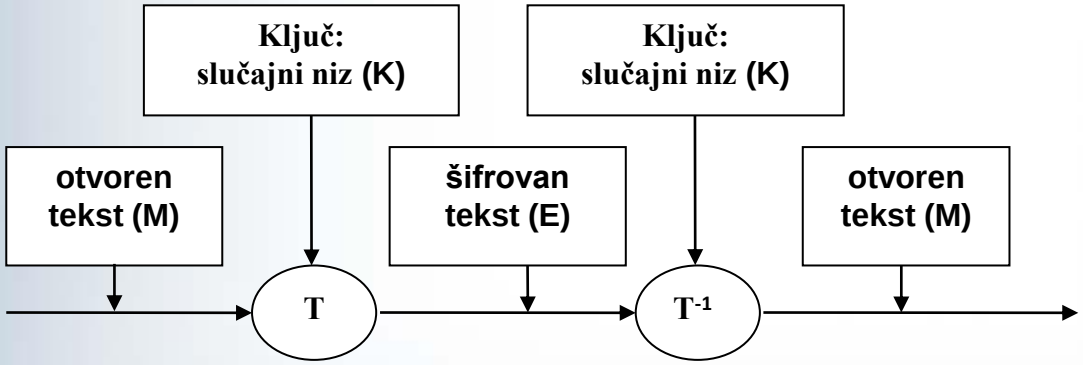
- 1945 novine San Diego Union su pisale:

„Japanci su hvatali čudne grlene poruke nalik zapevanju tibentaskog kaluđera i grgotanja iz naglo otvorene boce tople vode“.

Navaho „koderi“ su dobijali vojna priznanja za izuzetno zalaganje i hrabrost.

Činjenica da su Amerikanci uspeli da provale Japanski kod a Japanci nisu uspeli da provale Navaho kod bila je odlučujuća za Američku pobedu na Pacifiku.

- Suština kriptografije zasniva se na konceptu tajnog komuniciranja (tajne korespondencije) koji podrazumeva da se:
- **čitljiv** (otvoren) tekst (M), koji treba štititi,
- transformiše u **nečitljiv** (šifriran) tekst (E),
- kriptografskom transformacijom izabranom iz skupa transformacija (šifara) (T) na osnovu parametra – ključa kripto-sistema (K),
- a kasnije – primena inverzne transformacije (T-1) nad šifriranim tekstom (E) daje opet otvoren (izvorni) tekst (M).



- **Osnovni pojmovi koji se javljaju u kriptografiji su:**
  - **Otvoren tekst – svaki napisan logički tekst razumljiv čitaocu;**
  - **Poruka ili informacija – otvoren tekst koji predstavlja celinu i napisan u formi da bude dostavljen korisniku; i**
  - **Tajna poruka ili tajna informacija – poruka sa čijim sadržajem može biti upoznat samo onaj kome je namenjena.**

- **Svaki kripto-sistem se sastoji iz dve osnovne komponente (dela):**
  - **Algoritma (kriptografska metodologija), koji je uglavnom javni i koji predstavlja skup pravila (matematičku formulu) na osnovu kojih se vrši transformacija originalnog (čitljivog) teksta u kriptovanu (nerazumljivu) poruku i**
  - **Ključa, koji je tajni i koji personalizuje korišćenje algoritma za obavljanje transformacije.**

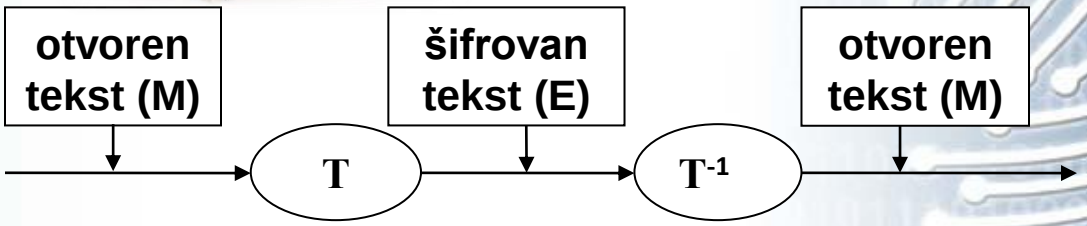
Zašto učimo o kriptografiji

Pojavom računarskih mreža kriptografija naglo dobija na značaju. Naročito je bitno obezbediti zaštitu važnih podataka (na primer finansijskih) koji se prenose mrežom.

Naime, podaci se razmenjuju računarskom mrežom u formi paketa podataka i oni dospevaju do većeg broja računara na putu od polaznog do odredišnog računara. Na svakom usputnom računaru moguće je te pakete podataka "uhvatiti" i pročitati njihov sadržaj, korišćenjem analizatora protokola ili nekog programa (*sniffera*).

Pasivan uljez
(samo prisluškuje)

Aktivan uljez
(može da menja poruke)



Presretač može prisluškivati ali i modifikovati poruke

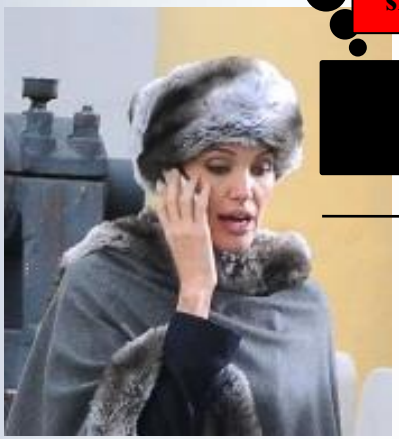
VOLIM TE

NE

VOLIM TE

Privatna poruka se prenosi javnim-nezaštićenim komunikacionim kanalima

BLA BLA TRUĆ
(za presretača nerazumljiv tekst)



Ključ: slučajni niz (Ke)

Ključ: slučajni niz (Kd)

šifrovan tekst (E)

T

T^{-1}

Ke – ključ za enkripciju
Kd – ključ za dekripciju

Ke = Kd privatna / simetrična
Ke ≠ Kd javna / asimetrična

- Algoritmi za kriptovanje se mogu podeliti u dve grupe:
  - **Tajni algoritmi**: bezbednost se zasniva na tajnosti algoritma
  - **Algoritmi zasnovani na ključu**: bezbednost se zasniva na ključevima, a ne na detaljima algoritma koji se može publikovati i analizirati.

Ovde je algoritam javno poznat, a ključ se čuva u tajnosti, da nije tako korisnici bi morali da razumeju i ključ i algoritam.

Ključ je niz podataka koji se koristi za kriptovanje drugih podataka i koji, prema tome, mora da se koristi i za dekriptovanje podataka.

- Osnovna pretpostavka kriptografije je da kriptoanalitičar zna metode uz pomoć kojih se obavlja šifrovanje i dešifrovanje.
- Količina truda koji treba uložiti u smišljanje, proveravanje i instaliranje **novog algoritma** kada je stari otkriven (ili postoji bojazan da je otkriven) oduvek je oneomogućavala da algoritam ostane tajan.
- Kada mislite da je nešto tajno što zapravo nije onda imate više štete nego koristi.
- Na ovom mestu uskače **ključ.**
- **Ključ** je za razliku od **algoritma** lako promeniti.

- Princip da kriptoanalitičari poznaju algoritme i da tajnost zapravo leži u ključevima naziva se **Kerkofov princip** po flamanskom vojnom kriptografu Augustu Kerckhoffu koji ga je prvi formulisao 1883. godine.

Kerkofov princip: Svi algoritmi moraju biti javni, samo su ključevi tajni.

Pokušaj da se algoritam zadrži u tajnosti nikada ne uspeva.

Pozitivna strana javnog objavljivanja je što veći broj stručnjaka daje svoje komentare i ako je duže vreme neprobijen opravdano se smatra prilično čvrstim algoritmom.

Očuvanje tajnosti se bazira na ključu pa je važna njegova dužina.

Količina truda koji kriptoanalitičar treba da uloži za isprobavanje svih mogućih kombinacija raste eksponencijalno sa dužinom ključa.

Danas se najviše koriste algoritmi za kriptovanje zasnovani na ključu, a mogu se klasifikovati u dve velike grupe:

- **Simetrični**, kod kojih se koristi jedan ključ,
- **Asimetrični**, kod kojih postoje dva ključa.

U cilju postizanja što bolje zaštite podataka algoritam za kriptovanje mora zadovoljiti sledeće zahteve:

- **Cena** "probijanja" algoritma mora da bude veća od cene šifrovanih podataka;
- **Vreme** potrebno za "probijanje" algoritma mora da bude duže od vremena u kome podaci moraju da ostanu tajni;
- **Broj podataka** kriptovanih pomoću jednog ključa mora da bude manji od broja potrebnih podataka da se dati algoritam "probije"

- Veoma je važno i da proces kriptovanja/dekriptovanja ima što je moguće kraće vreme izvršavanja.
- Postizanje što boljih performansi se ostvaruje ukoliko se ovi procesi realizuju hardverski.
- Kako bi algoritmi za kriptovanje bili što jednostavniji za hardversku realizaciju potrebno je da se izračunavanja u okviru njih baziraju na skupu jednostavnih operacija, kao što su aritmetičko sabiranje, XOR, operacije rotiranja i druge

10.1.1. Klasične kriptografske metode

- U transformaciji otvorenog u šifrirani tekst nasleđene su dve osnovne metode:
  - Kodiranje;
  - Šifriranje.
- Kodiranje
- Kodiranje podrazumeva korišćenje kodne knjige ili rečnika koji povezuju elemente otvorenog teksta (karaktere, slogove od dva ili više karaktera, reči, fraze, rečenice) sa elementima šifrata, koji se nazivaju kodne grupe. Pri tome, elementi otvorenog teksta su varijabilne dužine (slogovi, reči, fraze, rečenice). Za svaki element otvorenog teksta se u kodnoj knjizi traži njegova kodna grupa, odgovarajući element šifrata.

- Kodiranje neke poruke vrši se na taj način što se njene reči ili grupe reči (rečenice) pronalaze u kodnoj knjizi koja sadrži kodne ekvivalente koji mogu biti alfabetski ili numerički.
- Kodna knjiga je aranžirana u sekvencijalnom redosledu reči ili grupe reči. Zamenom komponentnih delova poruke sa njihovim kodnim ekvivalentima konstituiše se ceo proces kodiranja.
- Za efikasno dekodiranje kodirane poruke potrebna je druga odgovarajuća kodna knjiga, ovog puta indeksirana prema kodnim elementima.

- Tajni kodovi zauzimali su značajno mesto u kriptografskim tehnikama opšte namene.
- Oni mogu biti napravljeni efikasnije za ove potrebe obezbeđujući da u kodnoj knjizi postoje višestruki ekvivalenti, tako da kodni element korišćen za reč ili grupu reči nije uvek isti, već je izabran slučajno među raspoloživim alternativama.
- Na taj način značajna reč koja se u poruci često pojavljuje ne ponavlja istu učestanost i u kodiranom tekstu.

- Za zaštitu računarskih podataka kodovi su daleko od idealnog, zato što bi ekvivalent kodne knjige zahtevao glomazno skladište i ceo proces pregledanja bi konzumirao značajno vreme.
- Generisanje adekvatne kodne knjige predstavlja izuzetno složen i težak zadatak, a zaštitu uskladištenih kodnih tabela, vitalnih za ukupnu zaštitu, takođe bi bilo teško ostvariti.
- Zaštita i rapidni transport složenih kodnih tabela do lokacija na kojima su one potrebne je potencijalno težak problem, posebno ako se, zbog održavanja zaštite, zahteva česta izmena koda.

Šifriranje

- Za razliku od kriptografskih kodova šifre nisu povezane sa celim rečima ili grupama reči.
- U prošlosti su se one, generalno govoreći, primenjivale na nivou slova.
- Međutim, moderne kriptografske tehnike, primenjene u računarskom kontekstu, ponekad operišu sa većim jedinicama od mnogo karaktera, ponekad na nivou karaktera ili slova, a ponekad na nivou pojedinačnih binarnih cifara.

- Dve osnovne komponente klasičnih šifarskih tehnika su:
- supstitucija i
- transpozicija.

U supstituciji slova se zamenjuju drugim slovima, dok se u transpoziciji slova aranžiraju u drugačijem redosledu.

Mada se reč „transpozicija“ uobičajeno koristi za ovu vrstu operacija, reč „permutacija“ bi možda bolje odgovarala.

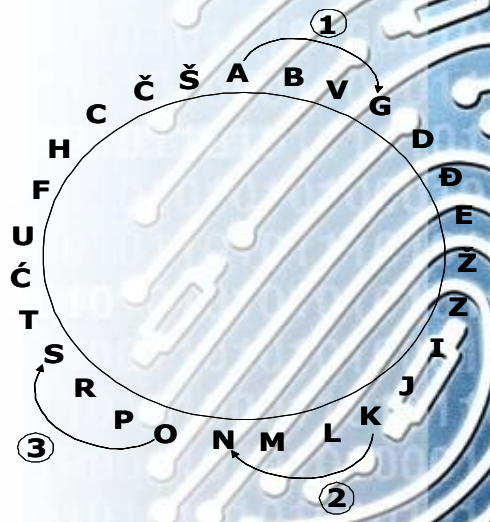
Šifriranje supstitucijom

- Postoji više tehnika šifriranja supstitucijom, među kojima značajno mesto zauzimaju sledeće:
  - Cezareva šifra;
  - Monoalfabetska supstitucija;
  - Polialfabetska supstitucija;
  - Vižnerova šifra;
  - Vernamova šifra.

- Da bi smo shvatili i razumeli osnovne principe šifriranja supstitucijom razmotrićemo samo Cezarevu šifru, Monoalfabetsku i Polialfabetsku supstituciju, kao jednostavne šifre i relativno lake za razumevanje.

Cezareva šifra

Ako se želi zamena slova jedne poruke sa drugim slovima na sistematičan način, pogodno je izraziti alfabet u kružnoj formi i onda za svako slovo iz otvorenog teksta birati zamenu pomeranjem za specificirani broj mesta u odabranom smeru. U primeru prikazanom na šemi je izabrano pomeranje za 3 mesta u smeru kazaljke na satu.



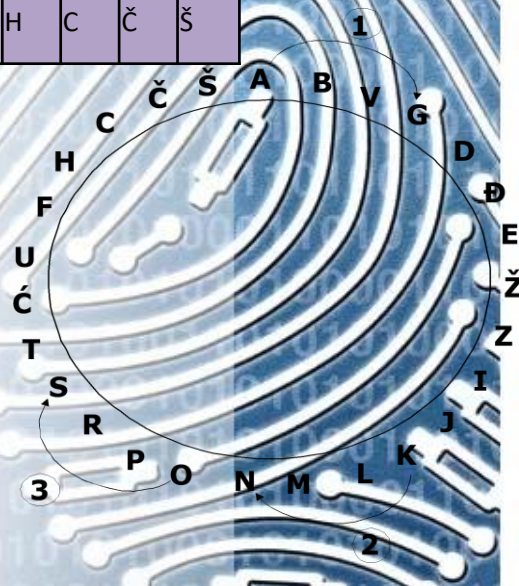
Otvoren tekst:	F	A	K	U	L	T	E	T	Z	A	P	R	A	V	N	E	I	P	O	S	L	O	V	N	E	S	.
Šifrovan tekst:	Č	G	N	C	O	F	I	F	K	G	T	Ć	G	Đ	R	I	L	T	S	U	O	S	Đ	R	I	U	.

Azbuka:	A	B	V	G	D	Đ	E	Ž	Z	I	J	K	L	M	N	O	P	R	S	T	Ć	U	F	H	C	Č	Š
Šifra:																											

Azbuka:	A	B	V	G	D	Đ	E	Ž	Z	I	J	K	L	M	N	O	P	R	S	T	Ć	U	F	H	C	Č	Š

G	D	Đ	E	Ž	Z	I	J	K	L	M	N	O	P	R	S	T	Ć	U	F	H	C	Č	Š

Azbuka:	A	B	V	G	D	Đ	E	Ž	Z	I	J	K	L	M	N	O	P	R	S	T	Ć	U	F	H	C	Č	Š
Šifra:	G	D	Đ	E	Ž	Z	I	J	K	L	M	N	O	P	R	S	T	Ć	U	F	H	C	Č	Š	A	B	V



Monoalfabetska supstitucija

- Nešto bolja zaštita može se ostvariti primenom monoalfabetske supstitucije, koja se sastoji u zameni slova poruke „izmešanom“ azbukom. U ovom slučaju **svako slovo otvorenog teksta se zamenjuje odgovarajućim slovom iz šifre**, pa se tako slovo A zamenjuje slovom Ć, B slovom M, V slovom I i td.

Azbuka:	A	B	V	G	D	Đ	E	Ž	Z	I	J	K	L	M	N	O	P	R	S	T	Ć	U	F	H	C	Č	Š
Šifra:	Ć	M	I	D	N	O	Ž	C	R	B	P	H	U	G	Č	Đ	J	V	A	L	Z	Š	E	F	S	K	T

Otvoren tekst:	F	A	K	U	L	T	E	T	Z	A	P	R	A	V	N	E	I	P	O	S	L	O	V	N	E	S	. . .
Šifrovan tekst:	E	Ć	H	Š	U	L	Ž	L	R	Ć	J	V	Ć	I	Č	Ž	B	J	Đ	A	U	Đ	I	Č	Ž	A	. . .

- Iako koristi samo jedan alfabet jasno je da postoji veliki broj mogućih substitucija, pa se može steći utisak da je reč o vrlo snažnom šifarskom mehanizmu.
- Međutim, ovo je ipak samo varka, jer postoje razlozi za slabost ovog mehanizma. Zato što postoji jedan prema jedan korespondencija između karaktera otvorenog i šifriranog teksta i zato što je većina govornih jezika visoko redundantna, kripto-analiza ovako šifriranog teksta relativno je laka i za kripto-analitičare amatere.
- Metod koji se koristi za probijanje ovakve šifre zasniva se na analizi frekvencija pojedinačnih karaktera, parova (bigrama) i trojki (trigrama) karaktera.
- Prema nekim procenama jedan ekspert za kripto-analizu može da kompromituje monoalfabetski sistem sa izvornim tekstom dužine 40 do 60 karaktera.

Šifriranje transpozicijom

- Transpozicione šifre se koriste za zaštitu sadržaja poruke rearanžiranjem redosleda karaktera ili bitova po unapred utvrđenim pravilima.
- Ovaj šifarski mehanizam su koristili još stari Grci, a njegova osnovna karakteristika je da se isti karakteri pojavljuju i u izvornom i u šifriranom tekstu, ali na različitim pozicijama.
- Prema tome, broj karaktera u izvornom i šifriranom tekstu je isti. Zbog ovakve čvrste korelacije između izvornog i šifriranog teksta transpozicija se ne može smatrati efikasnim mehanizmom za zaštitu tajnosti podataka.
- U nastavku će se razmotriti:
  - Prosta transpozicija;
  - Transpozicija korišćenjem tablice;
  - Premeštanje ključnom reči.

Prosta transpozicija

- Prosta transpozicija predstavlja najjednostavnije oblike premeštanja otvorenog teksta po unapred dogovorenom načinu. Slabe su kriptografske vrednosti i u praksi se ne primenjuju, jer ne mogu da obezbede potrebnu kriptografsku zaštitu.

- Jedan od takvih postupaka sastoji se u tome da se **permutuju parovi** slova.

Otvoren tekst:	F	A	K	U	L	T	E	T	Z	A	P	R	A	V	N	E	I	P	O	S	L	O	V	N	...
Šifrovan tekst:	A	F	U	K	T	L	T	E	A	Z	R	P	V	A	E	N	P	I	S	O	O	L	N	V	...

Dva fundamentalna principa kriptografije

Svi kriptografski sistemi se zasnivaju na dva osnovna principa koje je važno poštovati:

1. Redundantnost podataka

Šifrovane poruke moraju imati višak podataka odnosno podatke koji nisu neophodni za razumevanje sadržaja.

Na taj način primalac kada dešifruje ima način da proveri da li je poruka ispravna.

2. Svežina podataka

Moraju se preduzeti mere koje omogućavaju proveru da li je primljena poruka zaista sveža.

Na taj način se sprečava aktivni uljez koji reprodukuje stare poruke

Moderne kriptografske tehnike

- Zbog karakteristika koje poseduje, kriptografija je našla svoje mesto i u savremenom ambijentu i postala nezamenljiv vid zaštite u mnogim oblastima, posebno što su u današnjem svetu digitalnih brojeva i ostvarenoj brzini obrade i prenosa podataka i informacija nastali uslovi za stvaranje i primenu nove klase kriptoloških algoritama.
- Zahvaljujući, pre svega, informacionoj tehnologiji brzina i postupci kriptoštićenja su dostigli takav nivo da su mnoge klasične metode praktično diskvalifikovane.

- Došlo je i do drastične promene u do tada važećim kriterijumima za ocenu efikasnosti kripto-sistema:
  - Ključ više ne mora da bude jednostavan, jer računar nema problema sa pamćenjem;
  - Transformacije mogu biti veoma složene, jer ih računar obavlja brzo i bez greške;
  - Mogućnost propagacije (prenošenja) greške, koja nastaje u procesu transformacije, po sistemu je eliminisana

- Moderne šifarske šeme su mnogo razvijenije i složenije od klasičnih.
- Pri tome je značajna činjenica da širenje informacione tehnologije i računarskih mreža, s jedne strane, značajno zaoštrava zahteve za zaštitom komunikacija, a s druge strane osetno olakšava korišćenje kripto-zaštite omogućavajući i ne baš previše stručnim korisnicima da implementiraju i koriste najsofisticiranije šifarske pakete, što sve dovodi do drastičnog uvećavanja i broja i raznovrsnosti korisnika.
- Vojne i vladine agencije masovno koriste sofisticirane sisteme da zaštite senzitivne informacije, dok finansijska industrija i mnogi drugi koriste šifarske tehnike da zaštite komunikaciju svojih podataka i računarske sisteme, a servisi elektronske pošte potrebe i mogućnosti kripto-zaštite spustili su i na nivo pojedinaca, sve sa ciljem da se obezbedi sigurna komunikacija nesigurnim komunikacionim kanalima.

- Savremene kriptološke algoritme možemo klasifikovati po dva osnovna kriterijuma:
  - Po **načinu procesiranja** izvornog teksta i
  - Po **broju i vrsti ključeva**.

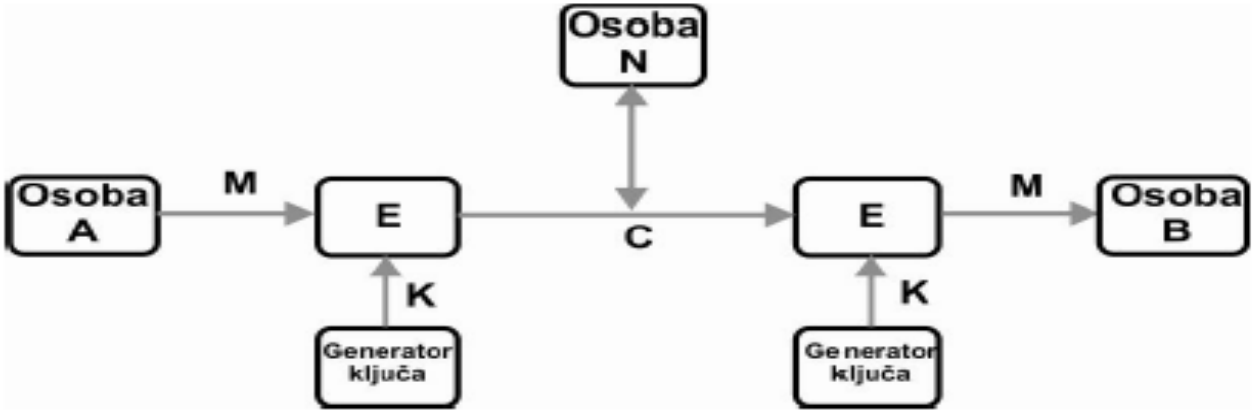
  Po načinu procesiranja izvornog teksta dele se na:
  - Šifriranje na nivou **Sukcesivnog niza znakova** („niz-šifra“);
  - **Bloka** („blok-šifra“).

  Po broju i vrsti ključeva:
  - **Simetrične** (konvencionalne);
  - **Asimetrične.**
- Simetrični algoritmi su sa istim (jednim) ključem i za šifriranje i za dešifriranje, a asimetrični algoritmi su sa različitim ključevima (dva), jedan za šifriranje i drugi za dešifriranje.

Simetrični algoritmi

- Kod simetričnih algoritama ili algoritama sa tajnim ključem, ključ korišćen za šifriranje mora biti identičan ključu korišćenom za dešifriranje.
- Većina šifri koje su danas u upotrebi koriste tajni ključ koji je poznat i pošiljaocu i primaocu informacije. Ovo su simetrične šifre zato što poznavanje tajnog ključa i od A i od B omogućava tajno komuniciranje bilo od A do B ili od B do A. U ovom kripto-sistemu se ne pravi razlika između A i B i prema tome on obezbeđuje zaštićen kanal u oba smera.
- Iz ovog proizilazi da ukoliko postoji više tačaka u mreži koje međusobno komuniciraju sve one moraju posedovati isti ključ i celina je poznata kao „kripto-mreža“.
- Dobar kripto-sistem je sistem u kojem je celokupna zaštita vezana za poznavanje ključa, a ne za poznavanje algoritma. Upravo zbog toga je upravljanje ključevima tako značajno u kriptografiji.

- Osoba *A* ima za cilj slanje poruke *M* osobi *B* preko nezaštićenog komunikacionog kanala.
- Osoba *A* najpre generiše poruku *M* (izvorni tekst) koja se upućuje u blok za šifrovanje *E*.
- U ovom bloku se vrši kriptovanje poruke *M* uz korišćenje ključa *K* dobijenog uz pomoć generatora ključa. Na taj način se kreira kriptovana poruka *C*.
- Potom se tako dobijena poruka komunikacionim kanalom šalje do osobe *B*



Prednosti simetričnih algoritama:

- Kod simetrične enkripcije isti ključ se koristi i za šifrovanje i za dešifrovanje. Baš zbog toga je velika raznovrsnost, a samim tim i sigurnost algoritama ovakve enkripcije.
- **Brzina** je najznačajnija prednost- simetrična enkripcija je veoma brza.
- Zbog velike brzine, kratkog vremena kriptovanja poruka smatraju se **visoko efikasnim**.Iz tih razloga se ova vrsta algoritama koristi za kriptovanje/dekriptovanje poruka velike dužine.

Nedostaci simetričnih algoritama:

- **Kako preneti tajni ključ**?

  Problem je u tome, što ako se tajni ključ presretne, poruka se može pročitati.

  Zato se ovaj tip enkripcije najčešće koristi prilikom zaštite podataka koje ne delimo sa drugima (šifru znate samo vi i nju nije potrebno slati drugome).

- **Ključevi moraju biti distribuirani tajno**.

  Oni su vredni onoliko koliko su vredne sve poruke koje se njima šifriraju, pošto poznavanje ključa omogućava saznavanje svih poruka. Za šifarske sisteme koji se prostiru svetom ovo može biti obeshrabrujući zadatak, pa često kuriri ručno nose ključeve do njihovih destinacija; !Što više ljudi zna manja je bezbednost!

- **Ukoliko je ključ kompromitovan** (krađom, pogađanjem, iznuđivanjem, otimanjem, potkupljivanjem) napadač može dešifrovati sve poruke koje su tim ključem šifrirane. Može da se predstavi kao legalna strana u konverzaciji šaljući lažne poruke.

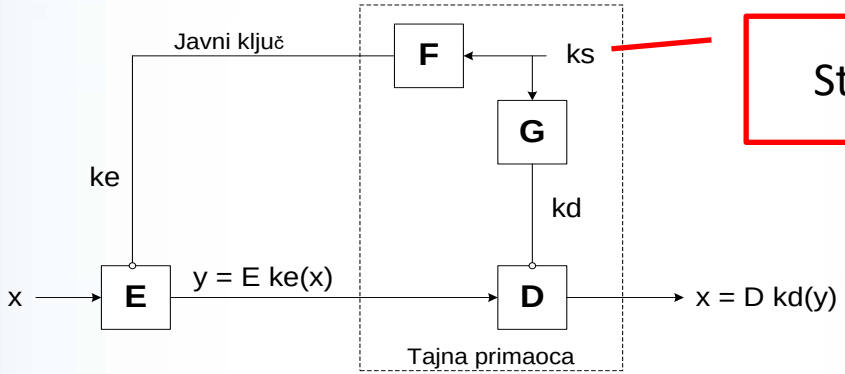
Asimetrični algoritmi

- Pošiljalac i primalac koriste različite, ali povezane ključeve (uparene ključeve), od kojih je samo jedan tajan.
- Primalac šifrovane poruke drži tajni ključ sa kojim je može dešifrovati, ali drugačiji ključ koristi pošiljalac da šifrira poruku i ovaj ključ može biti javan, bez opasnosti da će na bilo koji način kompromitovati sistem.
- Ovakav asimetričan sistem obezbeđuje **zaštićenu komunikaciju samo u jednom smeru**. Da bi se uspostavila zaštićena komunikacija i u drugom smeru potreban je drugi par ključeva.

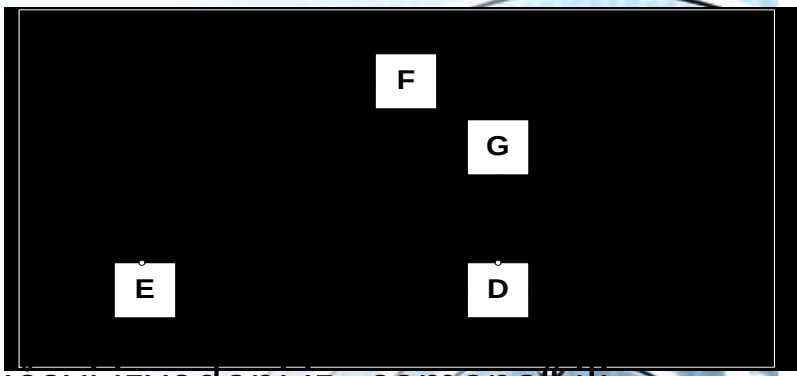
- Kod asimetričnih algoritama ključ potreban za dešifrovanje poruke razlikuje se od onog korišćenog za šifrovanje poruke.
- Ova dva ključa nisu potpuno nezavisna, već **su povezana u matematičkom smislu, tj. uzajamno su inverzni** i ne mogu biti matematički odvojeni entiteti.
- **Esencijalna karakteristika asimetričnih šifara /algoritama/** je da korisnik održava dva odvojena ključa, od kojih je jedan javni ključ (samo za šifriranje) i poznat je svima na sistemu i drugi tajni ključ (samo za dešifriranje), poznat jedino ovlašćenom (autorizovanom) primaocu.

- **Velika vrednost** kripto-sistema sa javnim ključem je da oni čine **nepotrebnim da se prenosi tajni ključ** između korespondenata A i B da bi se uspostavio zaštićen kanal. Znači, **reducira se problem upravljanja ključevima**, a to je značajno zbog činjenice da je transportovanje tajnog ključa veoma rizično i zbog mnogih potrebnih mera predostrožnosti ono može biti nezgodno i skupo.
- Skladištenje tajnog ključa takođe uključuje velike rizike, a u nekim primenama javnih ključeva ovi rizici su drastično reducirani. Kada jedan ključ mora biti smešten na mnogo mesta, uklanjanje potrebe za tajnošću je ogromno poboljšanje.
- Čist rezultat je da ako dve strane žele da međusobno komuniciraju ne postoji potreba za prethodnom razmenom ključeva. Svaka strana zna javni ključ druge strane. **Problem upravljanja ključevima se, dakle, reducira na problem zaštite korisnikovog privatnog ključa**.

Proces šifriranja i dešifriranja javnim ključem



- Pošiljalac za šifriranje primenjuje algoritam E i ključ za šifriranje **ke**, koji je ustvari **javni ključ** primaoca.
- Primalac za dešifriranje koristi algoritam D i ključ za dešifriranje **kd**, koji je ustvari njegov **tajni ključ**.
- **Oba algoritma su javna.**
- Dva ključa su specijalno kreirana za svaki novi zaštićen kanal i mogu biti menjani, slično svim ključevima.



- Da bi se mogao odraditi proces dešifriranja (inverzno šifriranje), evidentno je da dva ključa moraju biti povezana još u vreme njihovog izbora iz velikog univerzuma mogućih ključeva.
- Iz ovog razloga oni su na šemi prikazani kao ključevi izvedeni iz „semena" ili **startnog (početnog) ključa ks**, koji je izabran slučajno (random).
- Dva javna algoritma, F i G, se koriste za izračunavanje ključeva. Dve strane u asimetričnom šifriranju su pošiljalac i primalac.
- Samo primalac kome je namenjena informacija trebao bi biti u stanju da dešifruje poruku, zbog čega se ključ za dešifrovanje **kd** čuva tajno kod primaoca.
- Drugi ključ, **ke**, je javni i omogućava bilo kome da šifrira podatke za onog primaoca kojem taj ključ pripada. Da bi kreirao oba ključa i sačuvao tajnu primalac sam mora izvršiti izračunavanje F i G, nakon čega ključ **kd** mora čuvati striktno za svoje korišćenje.

- **Glavne prednosti kriptosistema s javnim ključem u**
- **poređenju sa simetričnim** su:
  - Nema potrebe za sigurnim komunikacionim kanalom za razmenu ključeva;
  - Za komunikaciju grupe od *N* ljudi potreno je 2*N* ključeva, za razliku od *N*(*N*-1)/2 ključeva kod simetričnog kriptosistema;
  - Mogućnost potpisivanja poruke
- Ipak, u stvarnosti kriptografija javnog ključa ne predstavlja zamenu za simetrične kriptosisteme. Ona se ne koristi za šifrovanje poruka, već za šifrovanje ključeva.
- **Naime, osobe A i B komuniciraju pomoću simetričnog kriptosistema s ključem koji su razmenili pomoću kriptosistema s javnim ključem.** To se zove ***hibridni kriptosistem***.
- Osnovni razlog zašto se javni ključ ne koristi za šifrovanje poruka je što su algoritmi s javnim ključem mnogo sporiji (oko 1000 puta) od modernih simetričnih algoritama.

U literaturi pojam asimetričnog kriptovanja se poistovećuje sa terminom *asymmetric-key* ili *public-key* kriptovanjem.

Razlika između simetričnih i asimetričnih algoritama je u tome što simetrični algoritmi koriste **isti ključ** za kriptovanje i dekriptovanje dok asimetrični algoritmi koriste **različite** ključeve za kriptovanje odnosno dekriptovanje.

Informacije koje su kriptovane javnim ključem mogu se dekriptovati samo tajnim ključem odnosno to može samo osoba koja je vlasnik tajnog asimetričnog ključa.

Oba ključa moraju biti povezana pomoću jedinstvene jednosmerne funkcije. Odnosno **ne sme se izračunati tajni ključ iz javnog ključa** ili se barem ne sme izračunati u razumnom vremenu.

Prednosti asimetričnog kriptovanja

1. Rešava nedostatake deljenja ključa kod simetričnih algoritama prilikom komunikacije između dve osobe (*A* i *B*). Kod simetričnog kriptovanja ključ se razmenjuje između dve osobe i ne može se koristiti ukoliko jedna od dve osobe želi komunicirati sa trećom osobom. Kod asimetričnih kriptosisitema svaka osoba kreira po dva ključa, jedan je tajni koji osoba čuva, a drugi je javni koji se razmenjuje sa drugima. Svaki od entiteta je nezavistan i svoj par ključeva može koristiti u komunikaciji sa bilo kime.
2. Druga prednost se ogleda u veoma velikom smanjenju broja ukupno potrebnih ključeva. U sistemu u kome komunicira milion korisnika, potrebno je samo 2 miliona ključeva, dok bi u slučaju korišćenja simetričnog kriptovanja bilo potrebno bar 500 milijardi ključeva.

Nedostaci asimetričnog kriptovanja

1. Najveći nedostatak je **kompleksnost algoritama** koji se koriste prilikom kriptovanja. Ako se želi efektno kriptovanje to povlači da algoritam koristi ogromne ključeve prilikom rada. Operisanje sa ogromnim brojevima zahteva mnogo vremena. Zbog toga asimetrični algoritmi nisu preporučljivi za rad sa velikim izvornim podacima. Može se reći da su asimetrični algoritmi mnogo efikasniji u radu sa kratkim porukama.

   Isto tako, ova vrsta algoritama zbog svoje složenosti nisu pogodni za hardversku implementaciju.
2. Drugi nedostatak je taj što se **komunikacija između dve strane i javni ključ moraju verifikovati**. Kako osoba *A* šalje svoj javni ključ osobi *B* putem elektronske pošte, osoba *B* na neki način mora biti sigurna da je dobijeni ključ upravo poslat od strane osobe *A*. Ovo je naročito važno ukoliko se radi o korišćenju asimetričnog kriptovanja prilikom identifikacije korisnika na neki sistem.

SIMETRIČAN

- način rada:
  - isti algoritam i isti ključ koriste se i za šifriranje i za dešifriranje
  - pošiljatelj i primatelj dele algoritam i ključ
- sigurnost:
  - očuvati tajnost ključa
  - nemoguće ili nepraktično dešifrirati poruku
  - poznavanje algoritma i dijelova šifrata mora biti nedovoljno za rekonstrukciju ključa
- 100-1000 puta brži

ASIMETRIČAN

- način rada:
  - jedan algoritam i par ključeva: jedan za šifriranje, jedan za dešifriranje
  - primatelj i pošiljatelj moraju imati po jedan od uparenih ključeva
- sigurnost:
  - jedan od dva ključa mora ostati tajan
  - nemoguće ili nepraktično dešifrirati poruku
  - poznavanje algoritma, jednog ključa i dijelova šifrata mora biti nedovoljno za rekonstrukciju ključa

Hibridni kriptosistemi

- Imajući u vidu da upotreba simetrične ili asimetrične kriptografije pati od izvesnih nedostataka javlja se potreba za sistemima koji kombinuju najbolje pojedinačne karakteristike oba sistema. Tako su nastali Hibridni kriptosistemi.
- Kombinovano koristi razne dosad navedene kriptografske algoritme u cilju jake i brze kriptozaštite.
- dobre strane simetričnih algoritama: brzina i manje računarski zahtevni
- dobre strane asimetričnih algoritama: upravljanje ključevima, distribucija i tajnost
- **hibridni pristup**:
  - **asimetričnu** kriptografiju koristiti za razmjenu **simetričnog** ključa
- Može se realizovati automatski preko već razvijenih sistema a može se i posebno birati kombinacija kriptografskih algoritama

Ponuda kriptosistema na tržištu

- Svakako treba ukazati da su brzom razvoju uređaja za šifriranja sa ugrađenim algoritmima u znatnoj meri doprineli i algoritmi za generisanje pseudo slučajnih nizova (PSN), tako da se iz dana u dan javlja sve više proizvođača koji nude ovakve uređaje „garantujući“ svojim kupcima potpunu zaštitu tajnosti informacija. Kripto uređaje i sisteme razvija i proizvodi više firmi koje se uglavnom nalaze u najrazvijenijim zemljama sveta (SAD, Nemačka, Švajcarska, Velika Britanija).

- Proizvođači se trude da obezbede visok stepen kriptološke zaštite, funkcionalnosti, kvaliteta, tehnoloških rešenja i pouzdanosti. Takođe obezbeđuju i tehnički servis, logističku podršku i obuku. Sve deluje vrlo primamljivo i obećavajuće. Međutim, kupovina zaštite je uvek, narodski rečeno, kupovina „mačke u džaku“, pa i u ovom slučaju postoji realna opasnost da se nabavi sistem sa nepoznatim i potencijalno opasnim slabostima.