Fakulteta za matematiko in fiziko
Podiplomski študij iz matematike - izobraževalna smer

Kriptografija

PRODAJA SISTEMOV ZA VARNOST PODATKOV

Ljubljana, maj 2000

MOJCA KOMAR

POVZETEK

Pričujoči članek se dotika precej aktualne teme - prodaje sistemov za zaščito informacij. Živimo v času, ki je naklonjen razvoju podjetij za zaščito informacij. Informacija, podatek z določeno vrednostjo, je v zadnjem času zopet pridobila na vrednosti. Če se je minula leta trg predvsem ukvarjal s strojno in programsko opremo, je sedaj čas, ko je potrebno to opremo uporabiti za nekaj koristnega - jo usmisliti in ji dati vsebino. Relativno hitro so se tega zavedli mediji, založbe in druga podjetja, ki se ukvarjajo s ponujanjem različnih vrst podatkov. Seveda so se hitro zavedla tudi dejstva, da bi bilo dobro te podatke zaščititi predvsem pri prenosu le teh (opaziti je namreč povečan medmrežni kriminal). Če nas je še do včeraj zanimalo pri programski ali strojni opremi, če "deluje", se zdaj z upravičenjem lahko vprašamo, če "deluje varno". Z razvojem novih tehnologij se je razvil tudi nov tip kriminala (elektronski kriminal), katerega smo priča vsak dan. Zaščita podatkov se je izkazala v preteklosti kot nuja ob ključnih momentih, naprimer preteča nevarnost vojne. Tako je lahko tudi razumeti, da se je v obdobju vojn rodilo obilo podjetij, ki so ponujala "najboljšo" zaščito. Žal so povečini vsa podjetja propadla, saj so imela premajhen trg, ali pa je njihov izdelek prišel na trg prepozno, torej v obdobju finančnih kriz. Zaradi velikega povpraševanja so današnja podjetja, ki se ukvarjajo z zaščito podatkov, povečini dobro stoječa.

UVOD

Si lahko predstavljate jutro, ko bi odšli od doma, vhodna vrata pa bi pustili odklenjena? Najbrž bi se ves dan spraševali "Kaj pa, če mi kdo odnese TV, računalnik ali pa celo kitajski porcelan?" Si lahko predstavljate, da bi prišli domov in bi videli, da je nekdo, ki ga sploh ne poznate ležal v vaši postelji? Najbrž ne! Pa se to vseeno dogaja. Podobno kot vam lahko ukradejo televizor iz nezakljenjenega stanovanja, vam lahko ukradejo tudi nezaščiteno informacijo. Radovednost sosedov in zanimanje za tuje stvari mnogokrat pripelje do nasprotij, pretepov, pa tudi do vojn. In ravno čas vojn predstavlja izziv za kriptografe.

PRODAJA ZAŠČITE INFORMACIJ MED VOJNAMA

Leta 1917 je ameriško podjetje AT&T dalo svojemu uslužbencu Gilbertu S. Vernamu zanimivo nalogo. Preveril naj bi varnost prenosa podatkov preko teleprinterja (takrat so ga imenovali še printer na daljavo). Na njihovo začudenje je kmalu dokazal, da je varnost zelo slaba in, da lahko prebere besedilo poslano po teleprinterju takorekoč vsakdo, ki je imel teleprinter. Sam je kmalu začel iskati novo rešitev in jo tudi našel. V pomoč mu je bila Baudotova koda (to je različica Morseove abecede za teleprinter), kjer vsak črka čistopisa dobi pet električnih impulzov ali izostankov tega impulza. Tako spremenjenemu besedilu je dodal ključ enake dolžine tako, da je bil nastali tajnopis sestavljen iz impulzov, ki so bili vsote čistopisa in ključa po modulu 2. Pokazal je, da je tak sistem v katerem za vsako poslano besedilo vzamemo drug (nov) ključ enake dolžine, varen. S tem je tudi iz kriptografskega procesa odstranil človeka - šifranta, in tako uvedel šifriranje v živo. Zelo kmalu so tudi vodilni v AT&T ugotovili prednost Vernamove ideje. Žal so po začetnem navdušenju ugotovili, da je število dnevno poslanih sporočil preveliko in poteka prehitro, da bi lahko hkrati proizvajali ravno tako število različnih ključev ustrezne dolžine. Zato so naredili kompromis med potrebo po pošiljanju sporočil in varnostjo le teh in Vernamovo idejo upoštevali le delno. Kljub temu, da je ideja tehnično uspela, je komercialno propadla. Vernam se je še naprej ukvarjal z raziskavami na tem področju, vendar brez uspeha. Umrl je reven. Kljub temu, da bi pričakovali, da bo čas obeh vojn pospešil prodajo tovrstnih izumov, je enako usodo doživelo še več njegovih naslednikov:

- Hill je izumil šifriranje sporočil s pomočjo reševanja sistema enačb po modulu 26, pa njegovega izuma ni kupil nihče.
- Kar štirje kriptografi so takorekoč istočasno izumili šifriranje s ključem na rotorju. Tudi ta izum ni bil odkupljen.
- Edward Hugh Hebern je uporabil ključ na petih rotorjih in v velikem zanosu ustanovil podjetje *Hebern Electronic Code.* Ker je prodajal preveč lastnih delnic, prodaja pa je občutno padala (prodal je samo 12 naprav), je podjetje kmalu odšlo v stečaj.
- Alex Koch je svoje patente vložil v podjetje *Geheimschrijfmachine,* vendar je zaradi družinskih problemov vse patente prodal Scherbiousu.
- Scherbious je na podlagi teh patentov naredil Enigmo, ki je prav tako propadla, vendar pa jo je Hitler uporabil v svoji vojski po njegovi smrti.
- Damm[12] ustanovil podjetje, ki je proizvajalo naprave podobne Enigmi, vendar so pri sami proizvodnji naredili preveč napak, zato je bila tudi prodaja slaba.

Boris Hagelin, eden izmed delničarjev Dammovega podjetja, predlaga izboljšave naprav in jih proda Švedski (model B-21). Medtem Damm umre, Hagelin pa s podobnimi idejami

vodi podjetje in postane nesramno bogat. Svoje nove modele proda Franciji, ZDA, ... (Converter M-209, C-25), ki jih koristno uporabijo med drugo svetovno vojno. Za Hagelina lahko rečemo, da je imel več materialne koristi od kriptografije kot kdorkoli in kjerkoli na svetu. Tudi po koncu vojne je ostal aktiven na tem področju, takorekoč do prihoda interneta. Sedaj pa si poglejmo kakšno je danes stanje na tem področju.

PRODAJA SISTEMOV ZA VARNOST PODATKOV

Ena aktualnejših tem je v tem trenutku varnost podatkov na Internetu in brezžični komunikaciji. Ko povezujemo krajevno računalniško omrežje v internet, se moramo zavedati, da s tem postanemo del globalnega omrežja, ki je lahko dostopno vsem uporabnikom. To omogoča možnost nezaželenih dostopov in zlorab. Nevarnosti za uporabnika so:

- vdori z namenom pridobiti podatke ali računalniške vire, do katerih uporabnik (notranji ali zunanji) nima pravic. Pri vdorih vlomilci izkoriščajo nepopolne varnostne mehanizme ali zelo dobro poznajo pomanjkljivosti v operacijskih sistemih. Opisane slabosti so lahko tudi rezultat slabe ali pomanjkljive varnostne politike ter nedoslednosti sistemskih administratorjev. Povzročena neposredna škoda običajno ni velika, zato pa je lahko toliko večja posredna (izdaja zaupnih informacij konkurenci, izguba zaupanja pri strankah, ...);
- računalniški vdori z namenom onesposobitve normalnega delovanja računalnikov in komunikacijske opreme, povzročitev škode s spreminjanjem vsebine datotek ali oviranje pristopa rednim uporabnikom. Te vrste vlomov ponavadi nimajo namena pridobitve materialnih koristi, zato pa lahko povzročajo znatno neposredno škodo, saj onemogočajo normalno poslovanje podjetja;
- možnost vnosa virusov prek elektronske pošte ali skupaj z datotekami iz interneta;
- različne možnosti za lažno predstavljanje na podlagi podatkov, uporabljenih v internetu (številka kreditne kartice, identifikacijska koda, uporabniško ime, ...);
- prestrezanje podatkov pri sporazumevanju med vozlišči ali uporabniki v internetu.

Možne rešitve so:

- Požarna pregrada (*Firewall*) je omrežna komunikacijska enota, ki skrbi za varno povezavo več računalniških vozlišč med seboj. Z njegovo postavitvijo lahko nadzorujemo in upravljamo sporazumevanje med posameznimi vozlišči: določamo možne uporabnike, predvidimo protokole itd. Osnovno načelo pri njegovi postavitvi je, da imajo vsi uporabniki krajevnega omrežja nadzorovan, vendar čim bolj neoviran dostop do interneta, iz omrežja pa v krajevno prepuščamo le tiste, ki prihajajo z določenih naslovov. Od požarnega zidu pa običajno zahtevamo še popolno in izčrpno beleženje vseh aktivnosti, alarmiranje sistemskega administratorja ob poskusih vdora ali prepogostih kršitvah postavljenih pravil in varovanje strežnika pred možnimi vdori.
- Protivirusna zaščita je ena izmed osnovnih načinov varovanja računalnikov v krajevnem omrežju. Protivirusno ščitimo sestavne dele, ki sodelujejo v prometu z internetom: požarni zid, dohodna vrata za elektronsko pošto, strežnike in delovne postaje v krajevnem omrežju. Protivirusna zaščita za požarne zidove preverja ves promet, ki prihaja iz interneta v krajevno omrežje ter samodejno odstranjuje nezaželene dele. Zaščita za dohodna vrata elektronske pošte preverja vse prilepke v elektronski pošti ter odstranjuje morebitne viruse, še preden povzročijo škodo in se

začnejo širiti. Strežnike in delovne postaje ščitimo tudi pred virusi, ki izvirajo iz samega omrežja (nepazljivi uporabniki pri prenosu podatkov z disketami, uporaba nepreverjenih virov pri nabavi programske opreme, ...).

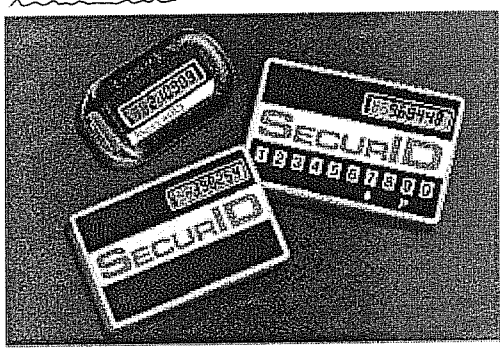
- Šifriranje podatkov pri sporazumevanju med uporabniki v internetu, med posameznimi krajevnimi omrežji ali oddaljenimi uporabniki ter centralo se v večini primerov že izvaja samodejno, saj so v programski opremi vključeni sistemi za šifriranje podatkov pri prenosu
- Za določitev istovetnosti ter popolnega prenosa podatkov se pri uporabniškem sporazumevanju uporabljajo tudi sistem gesel in uporabniških imen.
- Uporaba elektronskega podpisa (skupaj z uporabo sistema javnih ključev) ter avtorizirani sistem javnih in skrivnih gesel.
- Testiranje varnostnih pomanjkljivosti lahko opravimo z različnimi programskimi paketi. Le-ti sami prepoznajo operacijski sistem ciljnega računalnika in preverjajo vse najpogostejše postopke za vdore v sistem. Pri tem upoštevajo znane pomanjkljivosti ciljnega operacijskega sistema. Testiranja se lahko izvedejo na ravni internetnih strežnikov ali na ravni posameznih postaj v krajevnem omrežju (možnost vnosa škodljivih programov v postajo v krajevnem omrežju). Testiranje se izvede ob vsaki izvedeni spremembi v sistemu.

Pri zaščiti krajevnega omrežja uporabimo možne elemente v skladu z načinom uporabe priklopa v internet v podjetje ter v skladu z oceno možnih nevarnosti, ki posameznemu podjetju dejansko lahko povzročijo škodo. Pri tem je potrebno upoštevati dejstvo, da **100% varnost v poslovanju ne obstaja!**

Sedaj si pobliže poglejmo ponudbo nekaterih podjetij, ki se ukvarjajo z varnostjo na internetu, pametnimi karticami, varnostjo brezžične komunikacije ...

Security Dynamics Technologies

Security Dynamics Technologies je vodilno podjetje na področju dvofaktorske istovetnosti - večina varnostnih pomanjkljivosti v informacijskih sistemih je namreč posledica neustreznih (prekratkih in prelahko uganljivih) gesel. Security Dynamics je začetnik tehnologije enkratnih gesel in kot tak obvladuje približno 70 % trga strogega preverjanja istovetnosti uporabnikov.

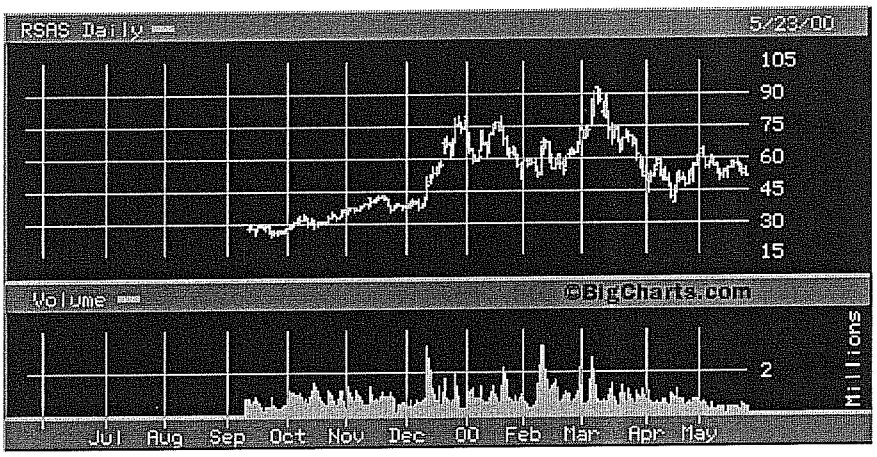


Osnova sistema so kartice, na katerih se geslo spreminja vsako minuto. V tem časovnem obdobju se lahko z isto številko prijavi le en uporabnik. Na ta način ne moremo gesla ponovno uporabiti, četudi bi ga npr. zajeli z omrežnimi analizatorji. Poleg tega pa mora uporabnik dodatno vtipkati še štirištevilčno kodo, ki je poznana le njemu.
Preverjanje na podlagi posedovanja dveh faktorjev (nekaj, kar veš in nekaj, kar imaš) se imenuje dvofaktorska istovetnost. Zagotavljanje pristnosti osebe je ključnega pomena pri vzpostavljanju elektronskega poslovanja.

V zadnjem času pa z nakupi neodvisnih podjetij zaokrožuje ponudbo tudi ponudbo na ostalih varnostnih področjih: ugotavljanje varnostnih pomanjkljivosti, digitalni certifikati, enkratno logiranje v omrežje, ... Med najbolj znanimi podjetji, ki so jih kupili, je podjetje RSA, katerega tehnologije za šifriranje podatkov (npr. DES)?? uporablja v različnih programskih paketih nekaj milijonov uporabnikov. Na področju elektronske pošte pa je na voljo požarna pregrada za elektronsko pošto World Secure Server: pregledovanje vsebine elektronske pošte, obveščanje pristojnih ali pa uporabnika o neustreznosti vsebine, ki jo pošilja (na podlagi ključnih besed), protivirusna zaščita,...

RSA

RSA je podjetje, ki ima visoko stopnjo zaupanja pri svojih uporabnikih. Že skoraj 20 let se pojavlja kot ponudnik elektronske varnosti predvsem na področjih izobraževanja, energetike, zdravstvene oskrbe, proizvodnje, telekomunikacij, medijev in zabave. Najnovejša je družina rešitev imenovanih RSA Keon. Sistemi preverjanja istovetnosti uporabnikov na osnovi infrastrukture javnih ključev je ena izmed tehnologij, ki se v zadnjem času najbolj razvija in se ji v strokovnih medijih posveča tudi največ pozornosti. Kot rezultat razvoja SDT in povezanih podjetij (RSA in Dynasoft) je Security Dynamics pripravil naslednika izdelka BoKS ter nadgradnjo tehnologij za šifriranje in digitalno podpisovanje podjetja RSA. Njihove izdelke uporablja na miljone ljudi (naprimer: tehnologijo RSA SecurID uporablja približno 6 miljonov uporabnikov, medtem ko so prodali preko 500 miljonov kopij RSA BSAFE).



slika 1

Velik odjemalec njihove tehnologije je vlada Združenih držav Amerike, med katerimi je urad predsednika ZDA, ministrstva, zvezne agencije, senat in sodišča, prav tako pa uporabljajo njihovo tehnologijo nekateri spletni brkljalniki in spletna programska oprema.
Nakup njihovih rešitev je varna odločitev, podobno velja tako tudi za nakup njihovih delnic. Tako kot v mnogih podjetjih (npr. Certicom), je tudi delnica podjetja RSA Security občutno rasla do letošnjega marca, ko je nenadno padla (slika 1 prikazuje gibanje delnice v zadnjem letu).

Internet security Systems - ISS

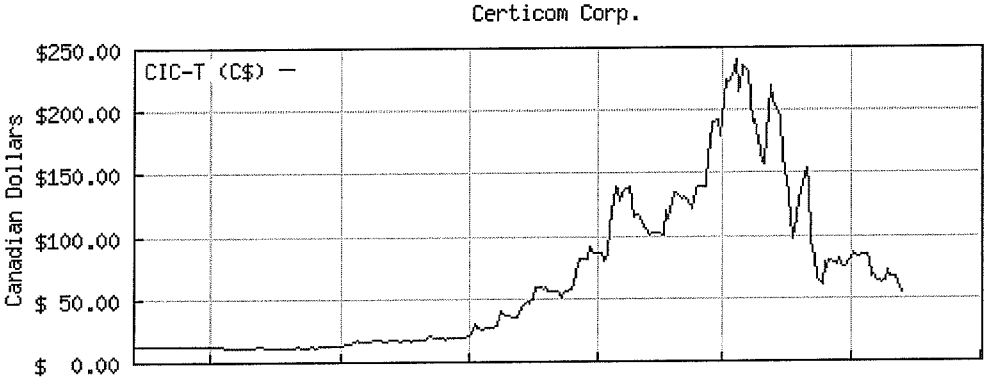
Podjetje Internet Security Systems je vodilni ponudnik programske opreme za testiranje varnosti omrežja in njegovo nadziranje. Programi, kot sta Internet Scanner ter Real Secure, dobivajo v strokovni literaturi najvišje ocene. Ugotavljanje varnostnih pomanjkljivosti ni enkraten dogodek. Dosledna varnostna politika zahteva stalno spremljanje na novo odkritih varnostnih pomanjkljivosti ter njihovo sprotno odpravljanje. V ISS ta proces imenujejo Adaptive Security Management (*prilagodljiva varnostna politika*). S spreminjajočim se okoljem se spreminjajo tudi načini zlorab informacij ali vdorov v informacijski sistem, za kar so potrebna orodja, ki omogočajo nenehno spremljanje s kar najmanjšo porabo časa.

ICSA

Podjetje ICSA (*International Computer Security Association*) je bilo ustanovljeno leta 1989. Je neodvisno in vodilno globalno združenje varnosti v informatiki z razvojem storitev s področja varnosti v internetu. Med ponudniki varnostnih storitev pa kot prvo ponuja tudi zavarovanje pred vdori in povzročenimi škodami, ki so posledica varnostnih incidentov. ICSA razvija varnostne izdelke in izvaja storitve najvišjega kvalitetnega razreda, že leta pa zagotavlja standarde in izvaja certificiranje proizvajalcev programske opreme (antivirusni programi, požarne pregrade, kriptografija, biometrija, filtriranje, IPSec) preko zahtevnih programov za certificiranje izdelkov in vodi več konzorcijev s področja varnosti v informatiki. Vsak dan ICSA izmenjuje informacije z razvijalci in proizvajalci varnostnih rešitev, strokovnjaki za varnost v informatiki, akademijami in korporacijami. Integracija teh informacij iz vseh virov jim zagotavlja najširši pregled v industriji, tehnično odličnost, ter omogoča integracijo v metodologijo neprestanega zagotavljanja varnosti – TruSecure!

Certicom

Kanadsko podjetje Certicom, ustanovljeno leta 1985, se s približno 100 zaposlenimi ukvarja z razvojem, izdelavo in prodajo tehnologij, izdelkov in drugih storitev s področja zaščite podatkov. Njihovi izdelki segajo na področje uvajanja industrijskih standardov v mobilne in brezžične aplikacije. Večino časa se podjetje ukvarja s kodirno tehnologijo in njeno uporabo v različnih orodjih in strojni opremi. Razvili so svojo tehnologijo imenovano ECC (*elliptic curve cryptography* - kriptografija s pomočjo eliptičnih krivulj), ki omogoča močno zaščito podatkov z javnim ključem na prenosnih aparatih. Ponujajo tudi dobre izvedbe standardnih varnostnih protokolov (npr. SSL Plus, WTLS Plus). Ukvarjajo se tudi s čisto specifičnimi problemi kot so npr. kodiranje sporočil po faksu (CertiFax). Njihova tehnologija in znanje so vgrajeni v mnoge znane produkte npr. Palm VII, družina Hawlett Packard OpenView, nekateri aparati GSM. Delnica podjetja Certicom prinaša svojim vlagateljem lep dobiček. Do letošnjega marca, ko se je rast umirila, je vrednost delnice nepretrgoma rasla (slika 2).



slika 2

Counterpane

Podjetje se, kot že ime pove, ukvarja z varnim prenosom podatkov na Internetu. Osredotočili so se na varni priklop elektronskega poslovanja. Sami ne prodajajo izdelkov za povečevanje varnosti, prav tako jih ne nameravajo nadomestiti. Njihov namen je narediti že obstoječo tehnologijo bolj učinkovito, zato tudi pogosto stojijo za trditvijo: "Varnost je proces, ne produkt.". So pobudniki partnerstva med posameznimi podjetji, ki se ukvarjajo s tehnologijo za varovanje podatkov. Tako so v ta program že vstopila mnoga podjetja, med njimi tudi: Exodus Communications Inc., Foundstone Inc., Network Flight Recorder, Open Source Group, PricewatershouseCoopers, Secure Computing, Security Inc., ... Podjetje Counterpane nudi tako predvsem usluge, kot so npr. opazovanje (24x7), odkrivanje in preprečevanje vdorov v sisteme.

Zgornja podjetja tudi v Sloveniji ponujajo svoje storitve preko svojih partnerjev (npr: Atlantis d.o.o., Nil Data Communications, Pronet d.o.o.,..). Dejavnosti podjetij obsegajo svetovanje, načrtovanie. izvedbo. asistenco pri delovanju omrežij ter izobraževanje.

ZAKLJUČEK

Nič še ne kaže, da bi se razvoj v tej smeri končal. Z uvajanjem računalnikov v vsakdanje življenje in glede na čedalje hitrejši razvoj, postaja informacija - odkrivanje in skrivanje le teh čedalje pomembnejša za uspeh. Torej imajo tovrstna podjetja velik še neizkoriščen trg. Tudi se ni bati, da bi podjetja propadla zaradi medsebojne konkurence, saj je trg porabnikov ogromen in tudi možnosti razvoja se še odpirajo. Pomembno je, da podjetja stremijo k izbiri najboljših kadrov, veliko je povpraševanje po matematikih. Zaključimo lahko, da se bo razvoj v tej smeri samo še nadaljeval.

VIRI:

- *David Kahn:* Šifranti protiv špijuna (druga knjiga, poglavje: Tajnost na prodaju), Centar za informaciju I publicitet, Zagreb, 1979)
- Spletni naslovi:
  www.britannica.com
  www.certicom.com
  www.r3.ch
  www.nsa.gov
  www.cdt.org
  www.computerprivacy.com
  www.cryptography.com
  www.rsasecurity.com
  www.counterpane.com