UNIVERZA V LJUBLJANI
FAKULTETA ZA ELEKTROTEHNIKO

SEMINARSKA NALOGA IZ KRIPTOGRAFIJE IN RAČUNALNIŠKE VARNOSTI

ELEKTRONSKO BANČNIŠTVO V SLOVENIJI

Avtor: Kotnik Samo

Ljubljana, julij 2000

KAZALO

1. Uvod

Z razvojem interneta in podatkovnih komunikacij se je povečala potreba po čim lažjem poslovanju z bankami. Ko so bile zagotovljene možnosti za dokaj varno poslovanje, se je začel razmah elektronskega bančništva v svetu in malo kasneje tudi v Sloveniji.

Samo elektronsko bančništvo omogoča:

- Opravljanje bančnih storitev preko interneta.
- Uporabniku ponuja hiter in varen način poslovanja z banko, saj lahko bančne storitve opravlja vedno in povsod, kjer ima na voljo računalnik z dostopom do interneta.
- Takšno poslovanje pa prinaša tudi številne prednosti kot so:
  - prihranek časa
  - stalen pregled na računih
  - neodvisnost od poslovnega časa bančnih enot
  - zasebnost

Za realizacijo elektronskega bančništva je potrebno zadostiti tudi določenim pogojem. Z uporabnikovega stališča mora biti vsekakor sistem elektronskega bančništva varen in zanesljiv. Samo varnost se zagotavlja na različne načine in mora biti dokaj visoka, ker se v nasportnem primeru potencijalni uporabniki ne bodo odločali za elektronske storitve.

Varnost se zagotavlja s pomočjo naslednjih mehanizmov:

- **overjanje** uporabnikov sistema elektronskega bančništva

S pomočjo overjanja se uporabnik sistema predstavi nato pa sistem preveri identitieto uporabnika. Če sistem uporabnika pozna mu dovoli dostop do storitev, v nasprotnem primeru pa mu opravljanje le teh prepreči. Za overjanje se lahko uporabljajo različni mehanizmi kot so uporabniška imena in gesla, razne pametne kartice, pa tudi biometrično overjanje s pomočjo prsnih odtisov, glasu,...

- **avtorizacije** transakcij uporabnikov

Pri izvedbi vsake transakcije je potrebno preveriti ali jo uporabnik lahko izvede ali ne. Prav tako je potebno preveriti, ali se pogovarjajo sistemi, ki so se prej overili in podobno.

- **zaupnost** podatkov

Podatki morajo biti »nepovabljenim« očem skriti, ker to omogoča dodatno varnost. Zaupnost podatkov se zagotavlja s pomočjo šifriranja podatkovnega toka. Uporabljene tehnologije obsegajo šifriranje na aplikativni ravni, pa vse do omrežne plasti interneta, kjer samo šifriranje omogočajo razni internet standardi kot je IPSEC.

- **celovitost** in **nespremenljivost** podatkov

Sami podatki o transakciji morajo biti varni pred spreminjanjem. Zagotoviti je potrebno tudi, da se podatek ne drobi po omrežju, ker bi lahko to spet zmanjšalo varnost. Za preprečevanje spreminjanja podatkov se uporabljajo razne zgoščevalne funkcije, ki omogočajo dobro zaščito pred spreminjanjem. Najpogosteje se uporabljajo funkcije SHA-1 in MD5, ter podobne.

2. Elektronsko bančništvo v Sloveniji

V Sloveniji se število bank, ki ponujajo elektronsko bančništvo povečuje iz dneva v dan. Ponujene storitve se rahlo razlikujejo od banke do banke, prav tako pa je tudi za varnost poskrbljeno na različne načine.

Slovenske banke, ki ponujajo elektronske storitve so:

a) Nova Kreditna Banka Maribor - Bank@Net
b) Nova Ljubljanska Banka - Klik
c) SKB banka - SKB Net
d) Banka Koper - I-Net

Glavne značilnosti posameznih e-bank:

a) Bank@Net bo podrobneje opisan v nadaljevanju.

b) Klik Nove Ljubljanske banke je pričel z delovanjem v letu 1999. Za zagotavljanje identitete, zaupnosti in celovitosti transkacij uporablja standandard SSL (Secure Socket Layer). Poleg tega pa vsebuje tudi dodatne mehanizme, kot so:
   - Varnostni sistem na podlagi identifikacije z osebnim geslom
   - Varnostni sistem na podlagi identifikacije z osebnim certifikatom
   - Varnostni sistem na podlagi pametne kartica ActiveCard Gold
   - Varnostni sistem samodejne odjave po določenem času neaktivnosti

c) SKB Net je pričel z obatovanjem leta 1999. Za zagotavljanje identitete, zaupnosti in celovitosti transakcij prav tako skrbi standard SSL. Uporabljeni dodatni varnostni mehanizmi pa so:

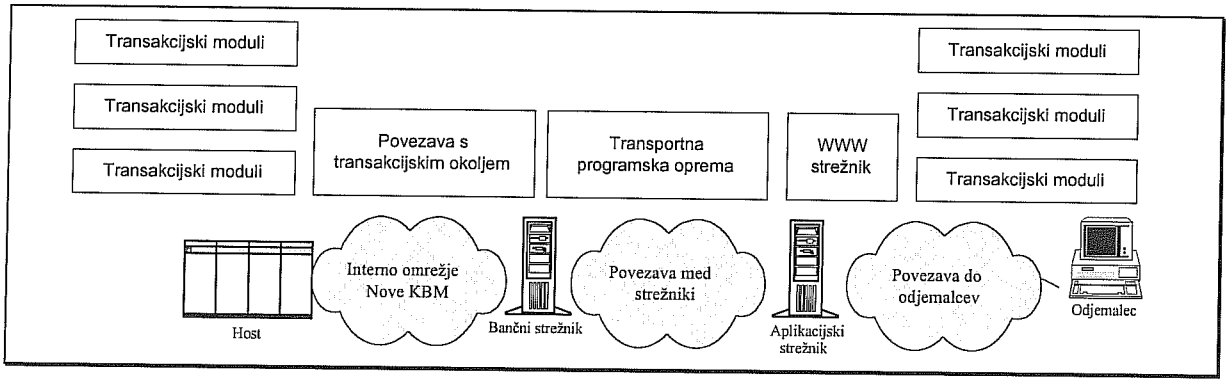
   - Varnostni sistem na podlagi identifikacijske kartice
   - Varnostni sistem proti ugibanju osebnega gesla
   - Varnostni sitem na podlagi pametne kartice ActiveCard

d) Tudi I-Net uporablja standard SSL za zagotavljanje identitete, zaupnosti in celovitosti transakcij. Poleg SSL-a pa uporablja še naslednje varnostne mehanizme:

   - Varnostni sistem na podlagi tajne številke (PIN)
   - Varnostni sistem proti ugibanju tajne številke
   - Varnostni sistem proti poskusu več hkratnih prijav
   - Varnostni sistem samodejne odjave

3. Podrobna analiza varnosti Bank@Net

Osnovno shemo sistema elektronskega bančništva prikazuje spodnja slika:



Slika 1: Osnovna shema sistema elektronskega bančništva

Ker odjemalci sistema dostopajo do posebnega aplikacijskega strežnika elektronskega bančništva in ne neposredno v bančno okolje, varnostne mehanizme delimo v grobem na dve skupini:

- varnostne mehanizme pri transakcijah med odjemalcem in aplikacijskim (Internetovim) strežnikom
- varnostne mehanizme pri posredovanju transakcij v bančno okolje

3.1. Varnostni mehanizmi za varen dostop odjemalcev

Odjemalski del sistema temelji na Internetovih tehnologijah, ki omogočajo množično in preprosto uporabo sistema uporabnikom Interneta brez dodatne programske opreme. V ta namen je odjemalski del izveden znotraj Internetovega pregledovalnika (*browser*-ja), ki dostopa do Internetovega strežnika sistema elektronskega bančništva NKBM. Ker komunikacija poteka preko omrežja zunaj bankinega nadzora (Interneta), je potrebno zagotoviti vrsto varnostnih mehanizmov, ki onemogočajo zlorabo sistema na načine, ki so na omrežju Internet dovolj preprosto izvedljivi (lažno predstavljanje, prisluškovanje transakcijam, sprememba transakcij,...).

3.1.1. Overjanje Internetovih uporabnikov

Overjanje omogoča, da nedvoumno ugotovimo identiteto uporabnika, ki preko globalnega omrežja dostopa do sistema elektronskega bančništva. Klasično overjanje v omrežnih aplikacijah, ki temelji na sistemu navadnih gesel, je za varnostne potrebe sistema elektronskega bančništva prešibko, zato je v sistemu elektronskega bančništva NKBM uporabljen sistem enkratnih gesel SecurID, ki temelji na t.i. dvodejavniškem overjanju (*two-factor authentication*). Pri tej vrsti overjanja se uporabnik sistemu predstavi z dvema neodvisnima dokazoma identitete:

- z nečim, kar uporabnik **ima** (kartica s časovno spreminjajočim se geslom);
- z nečim, kar uporabnik **ve** (številka PIN).

Dokaz identitete potuje do bančnega strežnika v notranjem omrežju, ki ima varno shranjene informacije o uporabnikih sistema in lahko preko *strežnika overjanja* v notranjem omrežju potrdi identiteto oddaljenega uporabnika in mu s tem omogoči uporabo storitev elektronskega bančništva. To overjanje se izvaja takrat, ko uporabnik sproži izvajanje transakcije. V primeru, da uporabnik ne izvaja transakcij, pa zadostuje vpis uporabniškega imena in večkratnega gesla. Za zaščito proti ugibanju gesel je poskrbljeno, saj se uporabniški račun zaklene po treh neuspešnih poskusih.

3.1.2. Overjanje Internetove seje

Poleg seje med uporabnikom in bančnim strežnikom je seja med Internetovim odjemalcem in Internetovim strežnikom NKBM prav tako overjena. Overjanje se v tem primeru izvaja z mehanizmi, vgrajenimi v Internetov standard SSL (Secure Sockets Layer) in v osnovni izvedbi omogoča overjanje strežnika s pomočjo certifikatne infrastrkture X.509 in pripadajočem sistemu javnih ključev za elektronsko podpisovanje, ki ga omogoča protokol SSL. Prav tako je v prihodnje možna integracija overjanja uporabnika (odjemalca), ki uporablja certifikat X.509 za dostop do Internetovega strežnika. Trajanje seje je zaradi varnostnih razlogov omejeno, zato se po petih minuta neaktivnosti uporabnika seja prekine.

3.1.3. Avtorizacija Internetovih uporabnikov

Na podlagi pridobljenega znanja o identiteti oddaljenega uporabnika lahko sistem elektronskega bančništva posameznemu uporabniku dodeli ustrezne pravice uporabe sistema. Do aplikacije na Internetovem strežniku lahko seveda dostopajo le ustrezno overjeni uporabniki. Internetovi uporabniki nikoli ne smejo dostopati do strežnika, ki je priključen neposredno v omrežje NKBM (bančni strežnik, strežnik overjanja).

3.1.4. Zagotavljanje zaupnosti in celovitosti transakcij

Seja med odjemalcem in Internetovim strežnikom poteka preko omrežja Internet in mora biti ustrezno zaščitena pred priskuškovanjem in spremembo podatkov. V ta namen se uporablja šifriranje podatkovne seje, preko katere si odjemalec in Internetov strežnik izmenjujeta podatke preko protokola HTTP. Šifriranje seje poteka preko storitev protokola SSL, ki temelji na certifikatni infrastrukturi za izvedbo mehanizma varne izmenjave šifrirnih sejnih ključev in simetričnih algoritmih za šifriranje podatkov. Tako je vsak prenos podatkov med odjemalcem (uporabnikom) in Internetovim strežnikom šifriran, kar omogoča zaupnost, celovitost in nespremenljivost bančnih transakcij, ki ji po prenosu preko omrežja Internet Internetov strežnik NKBM posreduje bančnemu strežniku NKBM.

3.2. Varnostni mehanizmi za varno komunikacijo z bančnim okoljem

Pri dostopu Internetovega strežnika do bančnega strežnika znotraj omrežja NKBM se uporablja dodatne varnostne mehanizme, ki omogočajo visoko stopnjo varnosti pri prenosu transakcij proti produkcijskem okolju banke.

3.2.1. Varnost Internetovega strežnika

Internetov strežnik temelji na tehnologiji Lotus Domino, ki zagotavlja visoko varnost aplikacijskega strežnika. Ker se podatki in aplikacija sama neposredno ne nahajata v datotečnem sistemu (shranjeni so v bazah Lotus Notes, ki so dostopne samo preko strežnika Domino), so zaščiteni z močnimi mehanizmi nadzora dostopa sistema Notes, ki tako s kriptografsko močnim overjanjem in na njem temelječim nadzorom dostopa omogoča želeno stopnjo varnosti.
Internetov strežnik je pred napadi na operacijski sistem strežnika iz omrežja Internet zaščiten z elementi požarnega zidu NKBM, ki z obrambo na omrežnem, transportnem in aplikacijskem sloju omogoča povezljivost le za najnujnejše storitve Internetovega strežnika.

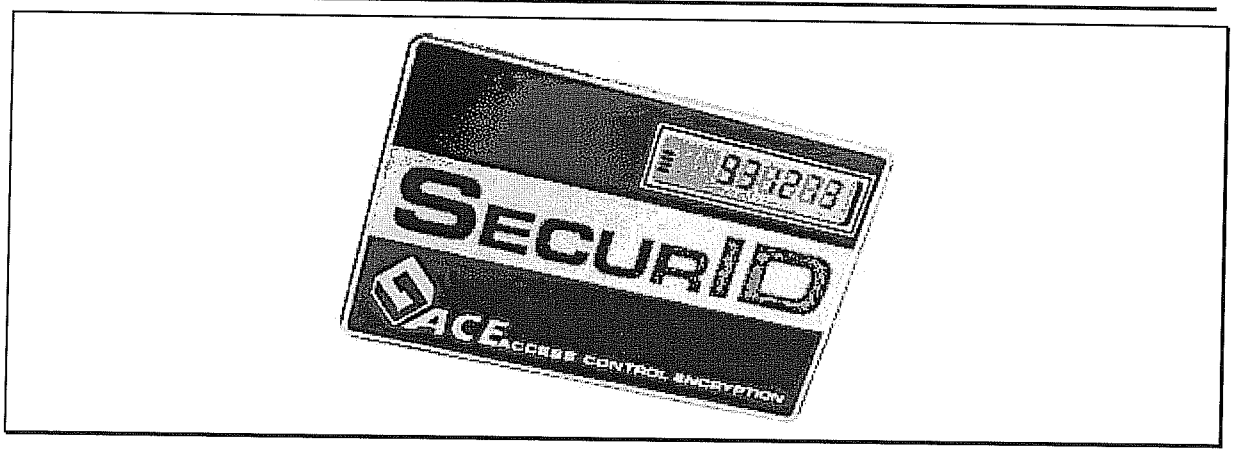
3.2.2. Varnost komunikacije med Internetovim ter bančnim strežnikom

Podatkovna seja med Internetovim in bančnim strežnikom poteka preko lastnih mehanizmov okolja Lotus Notes, zato se lahko zagotavi:

- overjanje seje Notes med strežnikoma z mehanizmi, enakovrednimi mehanizmom, ki jih uporablja protokol SSL (sistem javnih ključev, elektronsko podpisovanje);
- šifriranje seje Notes, ki zagotavlja zaupnost in celovitost podatkov.

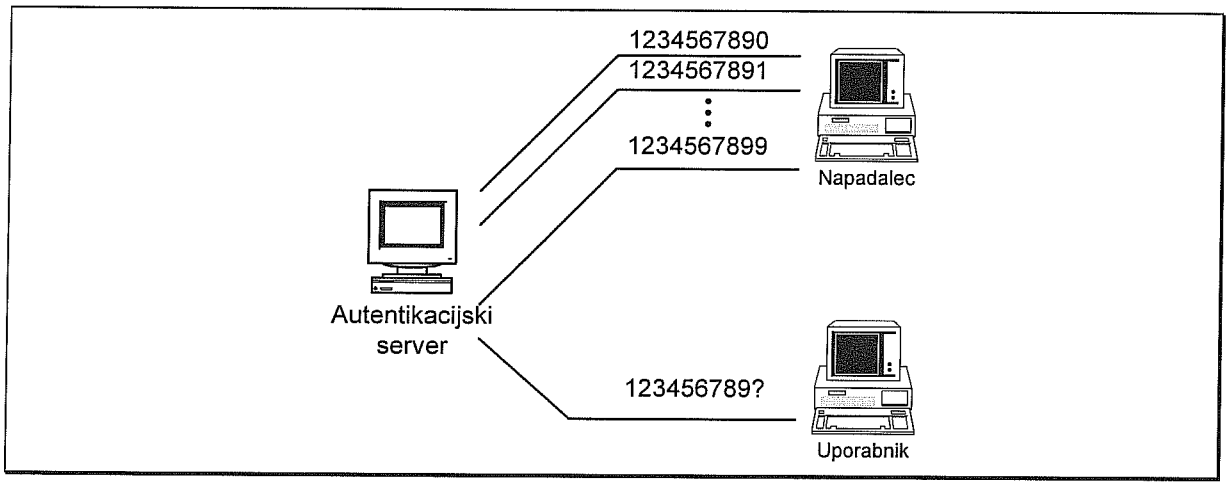
Na omrežnem, transportnem in aplikacijskem sloju omrežja je omogočena zelo omejena komunikacija med Internetovim in bančnim strežnikom, saj se le-ta odvija preko sistema požarnega zidu NKBM. V ta namen je požarni zid ustrezno varno nastavljen in omogoča kar najmočnejše varovanje notranjega omrežja (dopuščene so le nujne vhodne seje sistema elektronskega bančništva, torej seje, ustvarjene med strežnikoma Domino).
Bančni strežnik sistema elektronskega bančništva dostopa do *strežnika overjanja* ACE/Server v notranjem omrežju, ki overja oddaljene uporabnike sistema, ki se sistemu predstavijo z mehanizmom enkratnih gesel SecurID. Zasnova sistema elektronskega bančništva je taka, da ta strežnik ne potrebuje nikakršne povezljivosti z omrežjem Internet in je tako lahko izoliran od omrežij z nižjo stopnjo varnosti.

3.3. SecurID in možen napad



Slika 2 – SecureID kartica

Zaščita s SecurID temelji na enkratnem geslu, ki se generira na podlagi 64-bitnega "semena" in močnega algoritma, ki vsako minuto generira enkratno geslo. Geslo se izpiše na ekrančku kartice. Server prav tako izvaja identičen algoritem in na podlagi primerjave izhodov odloči ali je geslo pravilno ali ne. Možna je še dodatna zaščita z uporabo PIN kode, ki onemogoči uporabo kartice nepooblaščenim. Ker je generirana koda nepredvidljiva (neodvisna) od prejšnje kode, je praktično nemogoče uganiti naslednjo kodo na podlagi prejšnje. Vsaj proizvajalec trdi, da naj bi generirana gesla zadostila kriterijem PFS (Perfect Forward Secrecy), kar pomeni, da je naslednji izhod generatorja gesel res popolnoma neodvisen od prejšnjih. Če je temu kriteriju zadoščeno, je vsako naslednje geslo enako verjetno in zato ga je nemogoče ugotoviti. Seveda, pa ni mogoče zanesljivo trditi, da je to tudi resnica, ker bi potem lahko mirno odkrili algoritem, ki se uporablja za generiranje gesla, pa je le-ta se vedno zelo varovana poslovna skrivnost.
Obstaja tudi napad na SecureID. Kot vemo je enkratno geslo konstantne dolžine in sicer šestih (6) znakov. Če še temu geslu dodamo štiri (4) mestno PIN kodo, dobimo geslo dolžine desetih (10) znakov. V določenih pogojih pa obstaja tekmovalni napad na SecurID. Ti pogoji so izpolnjeni, če je možno "prisluškovati" liniji in ima uporabnik terminalnski emulator, ki pošilja podatke znank za znakom in ne vsako vrstico skupaj. V tem primeru je možno slediti seji, ki sta jo vzpostavili "stranki". Napadalec prisluškuje in si odpre deset sej z avtentikacijskim strežnikom. Na vsaki seji ponavlja znak za znakom do predzadnjega znaka. Predpostavimo, da je SecurID številka enaka 1234567890, torej smo do sedaj izvedeli številke 123456789 in nam manjka samo še zadnja številka. Kombinacij je samo deset, zato preprosto priredimo vsaki seji eno od kombinacij. Če smo bili dovoj hitri, da smo prehiteli lastnika kartice nas bo server autenticiral kot le-tega in dovolil opravljanje storitev. Obramba pred napadom je realizirana tako, da server ne dovoljuje toliko zaporednih prijavljanj za istega uporabnika. Vendar še vedno obstaja verjetnost 1/10, da se kljub temu prijavimo prej kot uporabnik in z pravim geslom.



Slika 3 – Poskus napada na SecureID

4. Zaključek

Za zagotavljanje varnosti se uporablja vrsto mehanizmov, pa vendar se moramo vprašati ali je zaščita dovoj dobra. Moje mnenje je, da je trenutno zaščita zadovoljiva. Prav vsak varnostni mehanizem ima sicer "luknje", ki pa so tako zasnovane, da bi jih v zglednem času težko odkrili. Velikokrat se torej zanašamo na "nemoč" današnjih računalnikov, da bi konkreten problem (ki se razlikuje od realizacije do realizacije) lahko rešili v doglednem času.
Pri načrtovanju varnih sistemov se je potrebno zavedati tudi pravila najšibkejšega člena verige, ki pravi, da je veriga močna toliko, kot je močan njen najšibkejši člen. Nima smisla vlagati ogromne denarje v najbolj moderno opremo, če recimo lahko najdemo geslo za vstop v zaščiten del omrežja napisano na monitorju nekega uslužbenca.
Statistika pravi, da je 10-15 % zlorab izvršenih znotraj banke (če upoštevamo, da se za veliko zlorab sploh ne razve, lahko ta procent mirno še povečamo) in smo 3%-5% preko interneta.
Za varnost je torej potrebno najprej izobraževati ljudi, ki prihajajo v direkten stik z varovanim procesom, kajti ti so najpogosteje najšibkejši člen v verigi.
Trendi razvoja elektronskega bančništva in elektronskega poslovanja so v smeri čimvečjega prometa po elektronskih medijih in seveda čimvečje varnosti poslovanja. Glede na to, da smo trenutno šele na začetku razvoja, lahko pričakujemo še ogromne spremembe in veliko novih storitev. Z razvojem se bodo seveda pojavljali še novi (stari) problemi po zasebnosti, ki jo je zelo težko zagotoviti v povezavi z varno izmenjavo podatkov, kar elektronsko bančništvo in poslovanje pravzaprav tudi je. Uveljavljajo se nove tehnologije, ki omogočajo šifriranje in zaščito podatkov že na tretjem nivoju OSI omrežnega modela, kar rešuje še vrsto problemov. Primer takšne tehnologije je IPSEC, ki omogoča enkripcijo do te mere, da ni možno ugotoviti, kdo pošilja določeno informacijo in komu, kar občutno zmanjša možnost napada. Prav tako prihaja tehnologija VPN-ov (Virtual Private Networks), ki omogoča gradnjo varnih omrežij neodvisno od fizične topologije omrežja, ampak samo na podlagi logične razdelitve posameznih uporabnikov v VPN omrežje, le ti pa so lahko fizično na različnih koncih sveta.
Tako kot se izboljšujejo tehnologije zaščite, pa se tudi izboljšujejo tehnike napada, zato mislim, da se bo ta boj nadaljeval še dolgo oziroma najbrž nikoli ne bo končnega zmagovalca.

5. PRILOGA – Diagram poteka uporabe Bank@Net