Varnost v telekomunikacijah in kako jo zagotoviti

Sašo Tomažič[1]

Povzetek — V predavanju je opredeljen pojem varnosti v telekomunikacijah kot zagotavljanje celovitosti prenašanih sporočil. Različne vidike celovitosti, to so zasebnost, verodostojnost in avtentičnost, je mogoče zagotoviti z ustrezno uporabo šifrirnih postopkov. Kako uporabimo šifrirne postopke za zagotavljanje celovitosti je določeno z ustreznimi protokoli. Četudi v protokolu uporabimo zelo zanesljive šifrirne postopke, se lahko zgodi, da so v protokolu šibkosti, ki omogočajo potencialnemu napadalcu zlorabo.

Telekomunikacijski sistem predstavlja zgolj infrastrukturo informacijskega sistema in sam po sebi ne more zagotavljati tudi varnosti informacijskega sistema. Za varnost informacijskega sistema mora poskrbeti uporabnik – upravljalec informacijskega sistema z ustrezno varnostno politiko. Ponavadi so najšibkejši člen pri zagotavljanju varnosti informacijskega sistema uporabniki tega sistema, zato je izobraževanje uporabnikov izrednega pomena.

Ključne besede — varnost, telekomunikacije, informacijski sistem, celovitost podatkov, šifriranje, zasebnost, verodostojnost, avtentičnost.

Abstract — In this lecture we define the term security in telecommunications as integrity of transmitted messages. Different aspects of integrity, i.e., privacy, credibility and authenticity, can be achieved with proper use of cartographic algorithms in communications protocols. The protocols can be vulnerable to different attacks even when strong cryptographic algorithms are used.

Telecommunication systems represent the infrastructure of information systems and cannot for themselves provide security to information systems connected to them. The security of information systems depends on proper security policy established by the managers of the information systems. The weakest link in the security are usually users of the information system.

Keywords — security, telecommunications, information system, data integrity, privacy, credibility, authenticity, cryptography

I. Uvod

Začetek 21. stoletja je neločljivo povezan s pojmom informacijska družba, to je družba v kateri postaja informacija najpomembnejša tržna dobrina. Človeška dejavnost na vseh področjih njegovega delovanja je vse bolj povezana z njegovo zmožnostjo pridobivanja oziroma izmenjave različnih informacij. Zelo pomembno je, da je *prava* informacija *pravočasno* na *pravem* mestu, to pa omogočajo sodobni telekomunikacijski sistemi, ki zato predstavljajo osnovno infrastrukturo informacijske družbe.

Vedno večja povezanost informacijskih sistemov na eni strani in njihova vedno večja javna dostopnost na drugi strani omogočata velikemu številu uporabnikov, da brez svoje fizične prisotnosti dostopajo do informacij in/ali te informacije tudi spreminjajo, kar pa obenem povečuje možnost zlorab. Vedno pomembnejši vidik pri načrtovanju telekomunikacijskih sistemov je zato njihova varnost.

Pojem varnost je zelo širok in subjektiven. Kar nekomu predstavlja varnost lahko pomeni nevarnost za nekoga drugega. *Varne* komunikacije ene strani v vojskovanju nedvomno pomenijo *nevarnost* za nasprotno stran. Ravno tako bi lahko trdili, da je za večino državljanov mnogo *varneje*, če imajo organi prisile možnost prisluškovanja telefonskim pogovorom, čeprav to lahko krši njihovo pravico po zasebnosti, obenem pa je ta možnost zelo *nevarno* za tiste, ki bi radi uporabili telekomunikacijski sistem za nezakonito dejavnost. Zelo *nevarna* utegne biti tudi uporaba mobilnega telefona medtem ko vozimo avto, vendar tega problema ponavadi ne obravnavamo v sklopu varnih komunikacij. Vidimo, da je potrebno pojem varnosti v telekomunikacijah natančneje opredeliti.

V telekomunikacijah imamo opravka s prenosom sporočil. Sporočila so lahko namenjena končnemu uporabniku in imajo kot taka sama po sebi neko vrednost ali pa so to sistemska sporočila, ki omogočajo dostop do in upravljanje z oddaljenimi sistemi oziroma delovanje samega telekomunikacijskega sistema. Vrednost teh sporočil je posredna. V obeh primerih lahko povzroči nepooblaščen dostop do teh sporočil oziroma njihovo nepooblaščeno uporabniku telekomunikacijskega sistema večjo ali manjšo škodo. Naloga varnega telekomunikacijskega sistema je preprečiti tovrstne zlorabe. Pomen pojma varnosti v telekomunikacijah zato zožimo na sposobnost telekomunikacijskega sistema, da zagotavlja čimbolj zanesljivo dostavo sporočil njegovemu naslovniku in hkrati zagotavlja njihovo celovitost.

[1] Sašo Tomažič je zaposlen na Univerzi v Ljubljani, Fakulteta za elektrotehniko
E-pošta: saso.tomazic@fe.uni-lj.si

II. ZAGOTAVLJANJE CELOVITOSTI

Pod pojmom celovitost sporočil razumemo predvsem:

- zasebnost (oziroma tajnost), ki zagotavljala, da je vsebina sporočila dostopna samo njegovemu naslovniku,
- verodostojnost, ki zagotavlja, da je sprejeto sporočilo enako oddanemu in
- avtentičnost, ki zagotavlja, da je identiteta izvora sporočila znana in/ali, da tega kasneje ni mogoče zanikati.

Ko slišimo pojem *varne komunikacije* ponavadi pomislimo zgolj na prvi vidik celovitosti, to je zasebnost. Kot uporabniki telekomunikacijskega sistema namreč ne želimo, da bi nekdo prisluškoval našim pogovorom ali bral našo elektronsko pošto. Vendar sta v določenih primerih druga dva vidika enako pomembna ali celo precej pomembnejša od zasebnosti.

Vzamemo za primer elektronsko bančništvo. Tu je veliko bolj kritično, če se lahko nekdo predstavi v našem imenu (avtentičnost) in nato tudi v našem imenu izvede poljubno transakcijo ali pa prestreže našo transakcijo ter spremeni ciljni račun in znesek našega nakazila (verodostojnost), kot če transakcijo zgolj opazuje in izve komu in kakšen znesek smo nakazali (zasebnost).

Posamezne vidike celovitosti sporočil je mogoče v telekomunikacijskih sistemih zagotavljati na več načinov. Zasebnost in avtentičnost lahko zagotovimo tako, da onemogočimo dostop do terminalne in prenosne opreme in tudi dostop do prenosnih poti. Verodostojnost lahko zagotavljamo z uporabo zanesljivih prenosnih poti in zanesljivih kodirnih in dekodirnih postopkov, ki omogočajo detekcijo oziroma odpravljanje napak pri prenosu, vendar so tovrstni postopki pogosto neuporabni. Pri mobilnih komunikacijah namreč ne moremo preprečiti dostopa do prenosne poti, ravno tako pa je lahko dostop do terminalne dokaj preprost (npr. izguba mobilnega telefona).

Vse vidike celovitosti podatkov je mogoče zagotoviti z ustrezno uporabo šifrirnih postopkov. Pri tem pa se moramo zavedati,

- da noben telekomunikacijski sistem sam po sebi ne more zagotoviti popolne celovitosti in,
- da je mogoče zagotoviti popolno celovitost le z uporabo šifrirnih postopkov na končnih točkah komunikacije (end to end) in to le za uporabniška sporočila. Za nekatera sistemska sporočilom ni mogoče zagotoviti vseh vidikov celovitosti.

A. Šifrirni postopki

Šifrirni postopek je postopek, ki razumljivo sporočilo (čistopis) preslika v nerazumljivo sporočilo (šifropis) tako, da je obratna preslikava mogoča le, če poznamo neko skrivno informacijo (ključ). Pri tem želimo, da sta postopka šifriranja in dešifriranja splošno znana in je tajen le ključ[2]. Glede na vrsto ključev ločimo dve vrsti šifrirnih postopkov:

- simetrične in
- asimetrične šifrirne postopke.

A.I. Simetrični postopki

Pri simetričnih šifriramo in dešifriramo z istim ključem, zato morajo udeleženci komunikacije preden začno komunicirati ta ključ med seboj na nek varen način izmenjati. Ključ predstavlja skupno skrivnost.
Simetrične šifrirne postopke dalje delimo na pretočne in bločne. Pri pretočnih postopkih šifriramo sporočilo sproti, tako da izvajamo XOR operacijo med posameznimi biti sporočila in biti ključa. Dolžina ključa mora biti enaka dolžini sporočila ali pa moramo uporabiti nek postopek, ki krajši ključ podaljša na dolžino sporočila.
Pri bločnih postopkih razdelimo sporočilo na krajše bloke (običajno dolžine 64 bitov), ki jih nato drugega za drugim šifriramo, tako da uporabimo zaporedje zamenjav (substitucij) in premikov (transpozicij), ki so določene s tajnim ključem.

A.II. Asimetrični postopki

Pri asimetričnih postopkih imamo par ključev: šifrirni ključ in dešifrirni ključ. S šifrirnim ključem lahko sporočilo šifriramo, ne moremo pa ga z njim tudi dešifrirati. Da bi lahko sporočilo dešifrirali, moramo poznati njegov par, to je dešifrirni ključ.
Ker s šifrirnim ključem sporočila ne moremo dešifrirati, tudi ni potrebe, da bi bil šifrirni ključ tajen, zato ga imenujemo tudi javni ključ. Ključ za dešifriranje mora ostati skrivnost in ga imenujemo tudi tajni ključ. Ker za šifriranje ne potrebujemo tajnega ključa, tu tudi ni potrebe po predhodni varni izmenjavi ključev.
Asimetrični postopki so zasnovani na tako imenovani enosmerni funkciji s stranskim vhodom (one way trapdoor function). Enosmerna funkcija je funkcija, ki jo je relativno preprosto izvesti (šifriranje), obraten postopek (dešifriranje) pa je matematično zelo zahteven (praktično neizvedljiv), če ne poznamo stranskega vhoda (dešifrirnega ključa).
Postopek šifriranja z javnim ključem bi lahko primerjali s poštnim nabiralnikom. Pri tem naslov in številka nabiralnika predstavljata javni ključ. Vsakdo, ki pozna ta ključ, lahko vrže pismo v nabiralnik, ne more pa ga iz njega vzeti. Pismo lahko vzame iz nabiralnika le lastnik nabiralnika, ki ima njegov ključ.

[2] Tega pravila pri načrtovanju GSM niso upoštevali. Tu je namreč šifrirni postopek tajen.

A.III. Varnost šifrirnih postopkov

Ko govorimo o šifrirnih postopkih, je ključnega pomena njihova varnost, to je odpornost proti različnim kriptografskim napadom. Napadalec lahko skuša:

- dešifrirati neko določeno sporočilo in na ta način priti do uporabnih informacij,
- odkriti tajni ključ, kar mu omogoči dešifriranje vseh sporočil, ki so šifrirana s tem ključem ali
- odkriti šibkost samega šifrirnega postopka, kar mu omogoči dešifriranje vseh sporočil, šifriranih s tem postopkom.

Napadi na šifrirne postopke se razlikujejo glede na to, kaj ima napadalec ob napadu na voljo. Ločimo predvsem:

- napad na osnovi enega ali več šifropisov,
- napad, pri katerem ima napadalec na voljo enega ali več parov čistopisa in šifropisa,
- napad pri katerem ima napadalec na voljo šifropise poljubnega števila izbranih čistopisov.

Odpornost šifrirnih postopkov na napade pada od prvega proti zadnjemu. Pri postopkih z javnim ključem je vedno možna tretja vrsta napada, saj lahko napadalec, ki pozna javni ključ, sam ustvari poljubno število parov čistopisa in šifropisa.

Glede na varnost, ki jo nudijo šifrirni postopki ločimo:

- teoretično varne postopke, ki jih je nemogoče razbiti, ne glede na vložen čas in sredstva ter
- praktično varne postopke, za katere je verjetnost, da bi jih razbili v omejenem času z omejenimi sredstvi dovolj majhna.

Edini znan teoretično varen postopek je postopek z enkratno uporabo ključa (one time key pad). To je pretočni postopek pri katerem je ključ popolnoma naključen in enak dolžini sporočila. S preizkušanjem vseh ključev bi napadalec dobil vsa možna sporočila vendar ne bi imel nobenega podatka o tem, katero od teh sporočil je pravo.

Na osnovi znanega para čistopisa in šifropisa je pri tem postopku sicer preprosto priti do ključa, vendar to napadalcu ne pomaga, saj se vsak ključ uporabi samo enkrat. Zaradi velike dolžine ključa, zahteve, da je ta popolnoma naključen in, da se vedno uporabi nov ključ, je tak postopek nepraktičen in se uporablja zgolj za varovanje najstrožje zaupnih sporočil.

Za praktično varne simetrične postopke mora veljati, da sam postopek ne vsebuje šibkosti, kar pomeni, da je za tak postopek edini način napada preizkušanje vseh možnih ključev. Varnost postopka je potem odvisna le od bitne dolžine ključa B. Da bi preskusil vse ključe, bi moral napadalec 2^B krat izvesti šifrirni postopek. Tudi če bi imel na voljo računalnik sposoben preizkusiti milijardo ključev na sekundo, bi lahko v milijardi milijard tisočletij preskusil le deset odstotkov 128 bitnih ključev. Simetrični šifrirni postopek s 128 bitnim ključem lahko zato štejemo za praktično varen postopek.

Pri asimetričnem postopku napadalcu ni potrebno preizkusiti vseh možnih ključev. Zadošča, da uspe iz javnega ključa izračunati njegov par, to je tajni ključ.

V trenutno znanih asimetričnih postopkih je javni ključ produkt dveh velikih praštevil, prafaktorja, ki to število sestavljata, pa sta tajna in predstavljata tajni ključ. Tajni ključ lahko torej napadalec pridobi s faktorizacijo javnega ključa. Če tak šifrirni postopek nima šibkosti, je to tudi najpreprostejši način napada. Kako varen je postopek je torej odvisno od dolžine ključa in učinkovitosti algoritmov za faktorizacijo. Ker se algoritmi za faktorizacijo stalno izboljšujejo, je skladno s tem potrebna tudi vse večja dolžina ključa. Trenutno zagotavlja 2048 bitni ključ pri asimetričnih postopkih približno enako varnost kot 128 bitni ključ pri simetričnih postopkih.

B. Protokoli za zagotavljanje celovitosti

Šifrirni postopki sami po sebi še ne zagotavljajo celovitosti sporočil. Da bi z njimi lahko zagotovili različne vidike celovitosti, jih moramo uporabiti v ustreznih komunikacijskih protokolih.

Šifrirni postopki so relativno varni, zato je ponavadi napadalcu precej lažje odkriti šibkosti v protokolu kot šibkosti v samem šifrirnem postopku. Kljub temu, da danes štejemo danes DES (data encryption standard) s 56 bitnim ključem za šibak šifrirni postopek, zaenkrat ni znanih zlorab, do katerih bi prišlo zaradi šibkosti DESa. Napadalci so pri različnih zlorabah, predvsem vdorih v sisteme, običajno izkoristili šibkosti v protokolu ali pa neprevidno obnašanje in napake, ki so jih naredili uporabniki sistema.

B.I. Zasebnost

Zasebnost je vidik celovitosti, ki ga lahko najbolj neposredno zagotovimo z uporabo ustreznega šifrirnega postopka.

Ker so asimetrični postopki računsko precej zahtevnejši od simetričnih postopkov, uporabljamo za zagotavljanje zasebnosti ponavadi simetrične šifrirne postopke. Računska zahtevnost je še posebej pomembna v mobilnih komunikacijah, kjer je imajo mobilni terminali močno omejeno računsko zmogljivost.

Pri simetričnih postopkih je potrebna predhodna varna izmenjava tajnega ključa. Ker večkratna uporaba istega ključa olajšuje kriptoanalizo, je zaželeno, da se za vsako sejo komunikacije tvori nov ključ (sejni ključ) ali pa, da se celo med samo sejo večkrat zamenja.

Za zgled si oglejmo preprost protokol, pri katerem je za izmenjavo sejnega ključa uporabljen asimetrični

šifrirni postopek. Uporabnik **A** želi poslati uporabniku **B** zaupno sporočilo, zato:

- **A** sporoči svojo namero **B**.
- **B** pošlje **A** svoj javni ključ jK_B.
- **A** tvori naključen sejni ključ *S* in z njim simetrično šifrira svoje sporočilo. Z javnim ključem JK_B nato še asimetrično šifrira sejni ključ *S* in ga skupaj s šifriranim sporočilom pošlje **B**.
- **B** s svojim tajnim ključem tK_B dešifrira sejni ključ *S* in potem s pomočjo *S* dešifrira še sporočilo.

Zgornji protokol je naveden zgolj kot zgled protokola in v resnici ni uporaben. Vsebuje namreč šibkost, ki bi jo lahko izkoristil napadalec **C**, če bi imel možnost prestrezanja vseh sporočila med **A** in **B**. Opisani protokol namreč ne zagotovljena avtentičnost javnega ključa JK_B. Če bi se v komunikacijo med **A** in **B** vmešal napadalec **C**, bi komunikacija lahko potekala na naslednji način:

- **C** prestreže zahtevo po komunikaciji ki jo pošlje **A,** in jo nespremenjeno posreduje **B**.
- **B** pošlje javni ključ jK_B uporabniku **A**, vendar ga **C** prestreže in posreduje naprej lažni ključ $jK_B^{'}$.
- **A** tvori ključ *S* in z njim šifrira sporočilo. Ker ne ve da je $jK_B^{'}$ lažen, ga uporabi za šifriranje sejnega ključa *S*, in vse skupaj pošlje **B**.
- C prestreže tudi to sporočilo. Ker pozna tajni ključ $tK_B^{'}$, ki je par lažnemu javnemu ključu $jK_B^{'}$, lahko dešifrira ključ *S* in s pomočjo tega ključa tudi sporočilo.
- C nato šifrira *S s* pravim javnim ključem jK_B, ga priloži šifriranemu sporočilu in pošlje naprej do **B**.
- **B** s svojim tajnim ključem tK_B dešifrira *S* in ga uporabi za dešifriranje sporočila.

V gornjem primeru je napadalec **C** izrabil šibkost v protokolu in prebral zaupno sporočilo, ne da bi uporabnika **A** in **B** to sploh opazila.
Obstaja veliko število različnih protokolov za izmenjavo ključev. Nekateri med njimi so zasnovani na asimetričnih šifrirnih postopkih, drugi na simetričnih postopkih, med tem ko uporabljajo tretji za tvorjenje sejnega ključa enosmerne funkcije brez stranskih vrat, kot je to primer pri Diffie - Hellman-ovi eksponentni izmenjavi ključev.

B.II. Verodostojnost

Verodostojnost pri prenosu sporočil pomeni, da lahko z veliko gotovostjo trdimo, da so sprejeta sporočila enaka oddanim. Želimo torej preprečiti možnost, da bi prišlo pri prenosu sporočila do spremembe vsebine, tako namerne kot nenamerne, ne da bi to opazili.

Nenamerno spreminjanje sporočil lahko preprečimo z redundančnim kodiranjem. Originalnemu sporočilu dodamo krajše sporočilo, ki predstavlja nekakšen prstni odtis tega sporočila, in ga dobimo tako, da sporočilo zgostimo z neko zgoščevalno (hash) funkcijo, ki različna sporočila preslika v različne prstne odtise. Pri tem mora biti verjetnost, da bi imeli dve sporočili enak prstni odtis, zelo majhna.
Prejemnik sporočila tudi sam izračuna prstni odtis sporočila in izračunan prstni odtis primerjamo s prstnim odtisom, ki je priložen sporočilu. Če sta enaka, lahko z veliko gotovostjo sklepa, da pri prenosu sporočilo ni bilo spremenjeno. Primera takega kodiranja sta dodajanje paritetnega bita in dodajanje ciklične redundančne kode (CRC).
Z redundančnim kodiranjem pa ne moremo zaščititi sporočila pred zlonamernimi spremembami. Napadalec lahko potem, ko spremeni sporočilo, izračuna nov prstni odtis in z njim nadomestil starega. Take spremembe prejemnik sporočila ne more odkriti. Da bi to preprečili, je potrebno prstni odtis, preden ga priložimo sporočilu, šifrirati z nekim tajnim ključem. Ker napadalec tega ključa ne pozna, tudi ne more zamenjati starega prstnega odtisa z novim.
Za šifriranje prstnega odtisa sporočila lahko uporabimo simetrični ali asimetrični šifrirni postopek. Če uporabimo za šifriranje simetrični postopek, je potrebna vnaprejšnja izmenjava tajnega ključa. Bolj priročna je uporaba asimetričnega postopka, kjer za šifriranje prstnega odtisa uporabimo tajni ključ, pri sprejemu pa prstni odtis dešifriramo z javnim ključem pošiljatelja, tako da izmenjava ključev ni več potrebna. S tajnim ključem šifriran prstni odtis sporočila imenujemo digitalni podpis.

B.III. Avtentičnost

Avtentičnost sporočila pomeni, da lahko z veliko gotovostjo ugotovimo identiteto izvora oziroma avtorja sporočila. Včasih je potrebno, da poznamo tudi točen čas nastanka sporočila kot tudi, da avtor sporočila ne more zanikati, da je sporočilo ustvaril ali pa, da je bil z njim seznanjen in se z njim strinja.
Avtentičnost sporočil je zelo pomembna pri sistemskih sporočilih, ki omogočajo uporabnikom dostop do oddaljenih sistemov. Da bi bil uporabniku odobren dostop do oddaljenega sistema, mora najprej dokazati svojo identiteto.
Preprost sistem dokazovanja identitete uporabnika je s pomočjo uporabniškega gesla. Uporabniško geslo je skrivnost, ki jo delita sistem in uporabnik. Sistem prepozna uporabnika po uporabniškem imenu in geslu. Uporabniško ime je lahko javno, geslo pa mora biti tajno. Kdorkoli pozna uporabniško ime in geslo se lahko prevzame identiteto uporabnika, zato je tajnost gesla izredno pomembna. Pri dostopu do oddaljenega sistema se geslo preko telekomunikacijskega sistema

prenaša kot sistemsko sporočilo, zato je nujno zagotoviti celovitost tega sporočila. Sistemi, ki temeljijo na preprostem prenosu gesla imajo veliko pomanjkljivosti:

- Uporabniki pogosto izbirajo zelo preprosta gesla, da bi si jih lažje zapomnili. Taka gesla potencialni napadalec zelo lahko ugane. Temu se da izogniti, če sistem zahteva določeno, minimalno dolžino gesla in/ali, da geslo vsebuje črke in številke. Nekateri sistem sami generirajo gesla in jih predlagajo uporabniku.
- Ker večina uporabnikov dostopa do različnih sistemov, potrebuje tudi večje število gesel, ki si jih je težko zapomniti. Pogosto jih zapišejo na lahko dostopnih mestih.
- Gesla se pogosto prenašajo nešifrirano, tako da jih lahko napadalec prestreže in pridobi lažno identiteto. Zgolj šifriranje gesel pri tem ne pomaga, kajti napadalec lahko prestreže šifrirano geslo in s pomočjo šifriranega gesla prevzame lažno identiteto.

Različni protokoli avtentikacije odpravljajo zgornje pomanjkljivosti. Pri avtentikaciji na osnovi izziva in odgovora (challenge and response) sistem in uporabnik delita skupno skrivnost (tajno geslo), vendar se to geslo nikoli ne prenaša preko telekomunikacijskega sistema. Namesto tega sistem izzove uporabnika tako, da mu pošlje neko naključno sporočilo. Uporabnik odgovori tako, da šifrira to s sporočilo s tajnim geslom, in ga pošlje nazaj. Sistem, ki pozna tajni ključ, šifrira svoje sporočilo in ga primerja s sporočilom, ki ga je prejel od uporabnika. Če sta enaka je identiteta uporabnika potrjena. Na enak način lahko tudi uporabnik preveri identiteto sistema, čeprav v praksi le redki sistemi omogoča takšno preverjanje.

Drug način avtentikacije je možen s pomočjo digitalnega podpisa, ki smo ga omenili že v prejšnjem razdelku. Uporabnik s svojim digitalnim podpisom podpiše sprejeto sporočilo in ga pošlje nazaj. Identiteto uporabnika sistem preveri s pomočjo javnega ključa uporabnika, zato tu ni potrebno, da bi imela sistem in uporabnik skupno skrivnost, zagotovljena pa mora biti avtentičnost javnega ključa.

V določenih primerih ne zadošča, da sistem zgolj preveri identiteto uporabnika, ampak mora biti poskrbljeno tudi za to, da kasneje uporabnik ne more zanikati sporočil, ki jih je poslal, ker za ta sporočila tudi odgovarja. Tak primer je elektronsko bančništvo. To, da uporabnik z digitalnim podpisom podpisanih sporočil ne more zanikati, je mogoče zagotoviti samo, če uporabnik prej podpiše dogovor, v katerem potrjuje veljavnost svojega digitalnega podpisa (overi svoj javni ključ) in prevzame odgovornost za uporabo svojega digitalnega podpisa, to je uporabo tajnega ključa, ki je par overjenemu javnemu ključu.

Nalogo overjanja ključev lahko prevzame tudi neka ustanova – urad za overjanje (certification authority), ki overjene ključe podpiše s svojim digitalnim podpisom in s tem zagotavlja avtentičnost javnega ključa. S pomočjo urada za overjanje (ki mu morajo vsi uporabniki zaupati) je mogoča avtentikacija brez kakršne koli predhodne izmenjave sporočil med udeleženci v komunikaciji.

Pri asimetričnih postopkih je tajni ključ veliko praštevilo, ki si ga uporabnik ne more zapomniti, zato mora imeti nekje shranjenega. Pri shranjevanju je potrebno ključ zavarovati s simetričnim postopkom, tako da ga je mogoče dešifrirati samo s pomočjo tajnega gesla ali osebne identifikacijske številke (personal identification number). Če ima uporabnik na izbiro uporabo osebne številke ali gesla, je veliko bolje izbrati dolgo gesla, ki si ga lažje zapomniti kot dolgo številko.

Izbira ustreznega, za uporabnika atipičnega gesla, ki ga napadalec ne more uganiti, je pri tem zelo pomembna. Največ vdorov v sisteme s prevzemanjem lažne identitete je namreč narejenih z ugibanjem gesel. Dokaj varno geslo, ki si gaje lahko zapomniti in ga je hkrati zelo težko uganiti, dobimo, če za geslo vzamemo prve črke nekega dolgega stavka.

Tajni ključ je smiselno še dodatno zavarovati, tako da ga na shranjujemo prenosljivem mediji (magnetna kartica, pametna kartica, USB disk, ...). Da bi prišel do ključa, bi moral napadalec najprej pridobiti medij, na katerem je ključ shranjen in nato še razbiti šifrirni postopek, s katerim je ključ šifriran.

III. VARNOSTNA POLITIKA

Poslovanje podjetij in različnih ustanov je vse bolj odvisno od njihovih informacijskih sistemov. Običajno so ti informacijski sistemi povezani z drugimi informacijskimi sistemi in tudi v globalno omrežje Internet. Povezava v Internet prinaša veliko prednosti, kot je to dostop do oddaljenih informacijskih virov, uporaba Internetnih storitev, kot je to elektronska pošta, dostop do notranjih virov iz poljubne lokacije preko fiksnih in mobilnih terminalov, delo od doma in podobno. Povezava informacijskega sistema v Internet pa hkrati omogoča velikemu številu napadalcev (hackerjev), da skušajo vdreti v informacijski sistem. Poleg tega da lahko takšni vdori napadalcem prinesejo velike koristi je vdiranje v informacijske sisteme postalo tudi športna disciplina, ki napadalcem sicer ne prinaša koristi, podjetju pa lahko kljub temu povzroči veliko škodo. S tako rekoč 100% gotovostjo lahko trdimo, da bodo napadalci skušali vdreti v vsak sistem ki je vključen v Internet. Zgolj na domač osebni računalnik avtorja tega članka je bilo na primer v zadnjem letu narejenih preko dva tisoč poskusov vdora. Informacijski sistem pred takimi vdori zagotovo najučinkoviteje zaščitimo tako, da ga ne vključimo v javno omrežje, vendar je ta ugotovitev podobna ugotovitvi, da je najbolje imeti avto brez motorja in volana, ker je tak avto zelo težko ukrasti.

Če želimo vključiti informacijski sistem v javno omrežje, je torej nujno da ga zaščitimo pred morebitnimi vdori. Pri tem se moramo zavedati, da lahko ponudnika Internet storitev in telekomunikacijskih storitev le v zelo omejenem obsegu pripomoreta k zaščiti uporabnikovega informacijskega sistema, v največji meri, mora to storiti uporabnik sam.

Da bi sistem uspešno zaščitili proti različni napadom, je potrebno izdelati ustrezno varnostno politiko, zato pa moramo najprej oceniti:

- kako je informacijski sistem ogrožen in kdo ga ogroža,
- koliko so vredni podatki ki jih želimo zaščititi,
- kako trajna je vrednost zaščitenih podatkov,
- kolikšno škodo lahko povzročijo napadalci,
- kako in v kolikšni meri je za poslovanje pomembna odprtost sistema do javnega omrežja,
- in kakšne stroške bi imeli z uvedbo ustreznih zaščitnih ukrepov, pri čemer moramo upoštevati neposredne kot tudi posredne stroške.

Na osnovi gornje analize lahko izdelamo varnostno politiko, ki določa:

- kateri deli informacijskega sistema so posebno vitalni in jih je potrebno bolj zaščititi,
- kateri uporabniki sistema imajo pravico dostopa do javnega omrežja in kakšne so te pravice,
- kateri uporabniki imajo pravico dostopa iz javnega omrežja in kakšne so te pravice,
- kakšne zaščitne ukrepe bomo uvedli (požarni zid, protivirusna zaščita, ločitev delov omrežij, ...) in
- določiti pravila obnašanja uporabnikov sistema.

Pri načrtovanju varnostne politike moramo paziti, da stroški vzpostavljanja varnosti ne presežejo potencialne škode, ki bi nastala ob vdoru v sistem. Pri tem moramo upoštevati tako neposredne in posredne stroške kot tudi neposredno in posredno škodo.

Kadar nimamo dovolj sredstev, da bi sistem zaščitili z vsemi najsodobnejšimi sredstvi, igrajo ključno vlogo pri zagotavljanju varnosti pravila obnašanja uporabnikov. Večina škode namreč v takih primerih povzroče uporabniki z neprevidnim obnašanjem, ko je to nameščanje sumljive programske opreme, ignoriranje varnostnih opozoril zaščitne programske opreme, slaba izbira ali slabo varovanje dostopnih gesel oziroma in podobno. Osveščanje in izobraževanje uporabnikov informacijskega sistema je torej ključnega pomena pri zagotavljanju njegove varnosti.

IV. Zaključek

Ugotovili smo, da je zaščita podatkov, ki se prenašajo preko telekomunikacijskih sistemov, predvsem pa zaščita informacijskih sistemov, ki so vključeni v javna omrežja, danes nujna.

Ponudniki telekomunikacijskih storitev lahko zavarujejo celovitost sporočil pri prenosu skozi telekomunikacijski sistem (npr. zaščita radijskega dela pri mobilnih komunikacijah), ne morejo pa popolnoma zaščititi informacijskih sistemov, ki so priključeni v javno omrežje. To ostaja naloga uporabnikov, ki se v javni sistem vključujejo.

Kadar so sredstva, ki jih lahko uporabniki vložijo v zaščito svojega sistema omejena, igra najpomembnejšo vlogo obnašanje uporabnikov pri uporabi informacijskega sistema, zato ima izobraževanje uporabnikov, njihovo seznanjanje s potencialnimi nevarnostmi, pravilno uporabo sistemov in možnostmi zaščite, ključno vlogo v varnosti telekomunikacijsko informacijskih sistemov.

V. Viri

[1] A. Menezes, P. Van Oorschot, S. Vanstone, Handbook of Applied Cryptography, CRC Press, 1996

[2] Seangwon Lee, Seong-Min Hong, Hyunsoo Yoon and Yookun Cho, Accelerating Key Establishment Protocols for Mobile Communication, 1999

[3] G. J. Simmons (editor), Contemporary Criptology, The Science of Information Integrity, IEEE Press, 1991

[4] Stallings W., "Network and Internetwork Security, Priciples and Practice." 1995, IEEE Press, Prentice –Hall.

[5] Rivest R., Shamir A. and Adleman L., "A Method for Obtaining Digital Signatures and Public Key Cryptosistems", Communications of the ACM, February 1978.

[6] Smith P., "LUC Public Key Encryption: A Secure Alternative to RSA." Dr. Bobb's Journal, January 1993.

[7] Knuth D., "The Art of Computer Programming, Volume 1: Fundamental Algorithms." Addison – Wesley, 1981.

Sašo Tomažič je doktoriral leta 1991 na Univerzi v Ljubljani, s področja telekomunikacij. Je profesor Fakulteti za elektrotehniko v Ljubljani, predstojnik Laboratorija za komunikacijske naprave in predstojnik Katedre za telekomunikacije. Bil je nacionalni koordinator za področje telekomunikacij na Ministrstvu za šolstvo, znanost in šport in svetovalec za področje telekomunikacij na Ministrstvu za obrambo. Njegovo sedanje delo obsega raziskave na področju obdelave signalov, varnosti v telekomunikacijah, elektronskega poslovanja in porazdeljenih informacijskih sistemov.