NEKATERE APLIKACIJE ZA ZAGOTAVLJANJE VARNOSTNIH SERVISOV V ODPRTIH SISTEMIH

Tomaž Klobučar,
Laboratorij za odprte sisteme in mreže, Institut Jožef Stefan,
61111 Ljubljana, Jamova 39

Povzetek:

S hitrim razvojem računalniških mrež, njihovo vse večjo medsebojno povezanostjo ter množičnejšo uporabo komunikacijskih storitev rastejo tudi varnostne zahteve običajnega uporabnika. Prispevek seznanja bralca z osnovnimi mehanizmi za reševanje problemov varnosti pri izmenjavi podatkov in nekaterimi aplikacijami (PEM, PGP, Kerberos, DASS), ki so za to na voljo.

Abstract:

Security demands of a common user are growing along with rapid development and stronger connectivity of computer networks and widespread use of communication services. This paper presents basic mechanisms for solving security problems in data interchange and some applications (PEM, PGP, Kerberos, DASS) that are available for that purpose.

1. Uvod

V dokumentu ISO 7498-2 (1) so definirani naslednji varnostni servisi: zaupnost, overjanje, integriteta podatkov, preprečitev tajenja in kontrola dostopa. Našteti servisi, ki karakterizirajo varnostne zahteve v mrežah, so bili podrobno predstavljeni že v prejšnji številki (2), zato si jih bomo v nadaljevanju natančneje ogledali le toliko, kolikor bo to potrebno za razumevanje posameznih aplikacij. Za začetek omenimo nekaj najvažnejših varnostnih mehanizmov, ki jih uporabljamo za zagotovitev varnostnih servisov. Med drugimi spadajo sem tudi šifriranje, digitalno podpisovanje in protokoli za overjanje.

1.1 Šifriranje

Proces transformacije teksta (čistopis) v obliko, ki onemogoča njegovo razumevanje (tajnopis) imenujemo šifriranje, obraten proces pa dešifriranje. Transformaciji formalno opišemo s funkcijama dveh spremenljivk, ki poljubnemu paru (tekst, parameter) priredita nov tekst in sta med seboj tako povezani, da lahko pri izbiri poljubnega parametra ene izmed funkcij, ki ga ponavadi imenujemo ključ, najdemo tak ključ za drugo funkcijo, da kompozitum le-teh ohranja besedilo. Drugače povedano, pri izbranih parametrih sta funkciji inverzni druga drugi. Funkciji imata še to lastnost, da je iz tajnopisa in njemu pripadajočega čistopisa nemogoče ugotoviti pri katerem parametru smo ju uporabili. Algoritem za izračun funkcij (kriptoalgoritem) je ponavadi znan do podrobnosti vsakomur, zato je za zagotovitev tajnosti besedila potrebno skriti le ključ.

Množica vseh možnih ključev sestavlja skupaj s postopkoma za šifriranje in dešifriranje ter množicama mogočih tajnopisov in čistopisov kriptografski sistem (kriptosistem). V grobem ločimo dve vrsti kriptosistemov: simetrične in asimetrične. V simetričnih kriptosistemih (najpomembnejši predstavnik simetričnih kriptoalgoritmov je DES-Data Encryption Standard) (3)) uporabljamo za šifriranje in dešifriranje isti ključ. Poznavanje tega ključa omogoča sodelujočima v tajnem pogovoru enakovredno vlogo: oba lahko pošiljata šifrirane podatke in dešifrirata prejete. To pa lahko počne tudi kdorkoli drug, ki pozna njun skupni ključ, zato je največji problem v simetrični kriptografiji način podeljevanja oziroma izmenjave ključev. Vsaj pred začetkom prve vzpostavitve zveze si morata ključ izmenjati osebno, če želita ohraniti skrivnost zase. V današnjem času, ko komuniciramo z ljudmi po vsem svetu, je tak postopek seveda nesprejemljiv, v primeru, ko ljudi nadomeščajo računalniki, pa celo nemogoč.

Drugačen pristop je od leta 1976 (4) na voljo v asimetričnih kriptosistemih oziroma kriptosistemih javnih ključev, kjer ključa za šifriranje in dešifriranje nista enaka. Najpomembnejša lastnost takih kriptosistemov je ta, da iz enega ključa, brez poznavanja dodatnih informacij, ni mogoče določiti preostalega, zato lahko en ključ javno objavimo. Tak ključ imenujemo javni ključ, drugi ključ iz para pa skriti

ključ. Kdorkoli nam želi poslati sporočilo, ga šifrira z našim javnim ključem. Samo mi, ki edini poznamo skriti ključ, ki z javnim tvori par, pa lahko šifrirano sporočilo dešifriramo. Najbolj znan algoritem v kriptografiji javnih ključev je algoritem RSA (5).

Asimetrični kriptosistemi bistveno poenostavijo izmenjavo ključev, zmanjšajo pa tudi njihovo število. Potrebnih je namreč le toliko parov ključev kolikor je uporabnikov, ne pa toliko ključev kolikor je parov uporabnikov, kot je to v kriptografiji enega ključa v primeru, ko vsak želi tajno komunicirati z vsakim. Prednost asimetričnih kriptoalgoritmov je tudi v tem, da omogočajo elektronsko podpisovanje dokumentov. Edina slaba lastnost je večja časovna zahtevnost šifriranja, zato ponavadi v praksi uporabljamo kombinacijo obeh sistemov: simetrične za šifriranje podatkov, asimetrične pa za izmenjavo ključev.

Za boljšo predstavo o kriptografiji javnih ključev moramo odgovoriti še na dve vprasanji. Kje najdemo javni ključ osebe, ki ji želimo poslati šifrirano sporočilo, in kdo ali kaj nam zagotavlja, da je ključ res njen? Možna odgovora nudita globalni imenik X.500 (6) (ena izmed njegovih izvedb, ki nam je na voljo, se imenuje QUIPU in je bila razvita na University College of London) in sistem certifikatov (7). Direktorij X.500 je distribuirana baza, v kateri se hranijo in s pomočjo katere se razdeljujejo številni podatki, ki jih potrebujemo pri delu v računalniških mrežah. Najpomembnejši med njimi so prav gotovo drevesno strukturirana imena ("distinguished names"), ki enolično določajo uporabnika v globalnem odprtem sistemu, in certifikati, ki predstavljajo bistven del varnostne infrastrukture. Certifikat je potrdilo, ki veže uporabnika z njegovim javnim ključem. Sestavljen je iz množice informacij, ki med drugim vsebuje uporabnikovo ime in javni ključ, in digitalnega podpisa teh informacij, narejenega s skritim ključem ene izmed agencij za izdajanje certifikatov (Certfication Authority), ki so medsebojno povezane v hierarhično strukturo. Lastništvo javnega ključa uporabnika potrdimo tako, da preverimo podpis potrdila, ki ga najdemo v imeniku, z javnim ključem ustrezne agencije, ki je certifikat podpisala. Na enak način preverimo tudi certifikat te agencije, postopek pa nadaljujemo dokler ne naletimo na agencijo, ki ji sami zaupamo. Podrobnejšo razlago digitalnega podpisa si bomo pogledali v naslednjem razdelku.

1.2 Digitalni podpisi

Digitalni podpis predstavlja nadomestek lastnoročnega podpisa v elektronski izmenjavi podatkov. Običajno je digitalno podpisovanje povezano z asimetričnimi kriptosistemi, čeprav obstajajo tudi metode, ki uporabljajo simetrične kriptoalgoritme. V našem primeru se bomo omejili le na prve.

Podpisovanje poteka v dveh korakih. Najprej skrčimo podatke z eno izmed zgostitvenih funkcij, ki poljubno dolgo besedilo preslika v blok konstantne dolžine. Zgostitvenih funkcij je več vrst, za nas pa bodo zanimive le tiste, ki zadoščajo vsaj naslednjim zahtevam: nemogoče je najti sporočilo, ki ustreza dani vrednosti funkcije, nemogoče je najti dve različni sporočili, ki imata isto vrednost, in rezultat mora biti zadosti dolg. Danes se najpogosteje uporabljajo funkcije MD2 (8), MD4 (9) in MD5 (10), katerih vrednosti imajo dolžino 128 bitov. Dobljeni blok, ki predstavlja 'prstni odtis' besedila, nato šifriramo (v kriptografiji javnih ključev s svojim skritim ključem). Rezultat imenujemo digitalni podpis.

Tudi preverjanje podpisa je sestavljeno iz dveh delov. Najprej dešifriramo podpis z javnim ključem podpisnika. Nato sami izračunamo vrednost zgostitvene funkcije na besedilu in primerjamo bloka. Če se ujemata, je podpis pravi. Pri tem je verjetno potrebno omeniti, da zgostitvene funkcije ne vsebujejo nikakršnih skritih ključev ali drugih neznanih informacij, zato lahko podpis preveri kdorkoli.

Prednost digitalnega podpisovanja pred običajnim je v tem, da podpis poleg avtorstva besedila zagotavlja tudi njegovo integriteto, saj še tako majhna sprememba v besedilu, ki je morda sami ne bi niti opazili, povsem spremeni rezultat zgostitvene funkcije. Digitalni podpis, dobljen z javnimi ključi, omogoča tudi lažjo razsodbo v primeru, ko podpisnik zanika, da bi bil podpis njegov. Ker je praktično nemogoče določiti skriti ključ, ki je znan le lastniku, takega podpisa skoraj ne moremo ponarediti.

2. Varna pošta

Elektronska pošta je verjetno tista storitev, s katero se običajni uporabniki najprej seznanijo pri delu v računalniških mrežah in jo kasneje tudi najpogosteje uporabljajo. Večina izmed njih pa se se ne zaveda, da je, kar se tiče zasebnosti, pošiljanje pošte z računalnikom brez uporabe kriptografskih metod zaenkrat celo slabše kot pošiljanje običajnih razglednic oziroma dopisnic. Ne le, da lahko skoraj vsakdo bere našo pošto, sporočila se lahko tudi spremenijo, ne da bi to sami zaznali.

2.1 PEM

PEM (Privacy Enhanced Mail) (11) je Internetov standard za zagotavljanje varnostnih servisov pri prenašanju elektronske pošte v Internet okolju. Za vsako poslano sporočilo

- sprejemniku omogoča preverjanje izvora pošte oziroma identitete pošiljatelja,
- obema sodelujočima zagotavlja integriteto sporočila,
- pošiljatelju onemogoča tajenje avtorstva (v primeru uporabe asimetričnih kriptoalgoritmov).

Dodatno PEM nudi se možnost tajnosti pošte. Med problemi, povezanimi z varnostjo, ki jih PEM ne rešuje, so na primer kontrola dostopa, neavtorizirano spremljanje količine izmenjane pošte, potrditev prejema sporočil in preprečevanje podvajanja istih sporočil oziroma ponovnega pošiljanja od tretje osebe.

Procesiranje sporočil poteka v več korakih. Pri tem lah-

ko uporabljamo obe vrsti kriptosistemov: simetrične in asimetrične; najboljše je, če kombinacijo obeh:

1. Željeno besedilo napisemo v lokalnem naboru znakov.
2. Sporočilo pretvorimo v univerzalno kanonično obliko, podobno predstavitvi SMTP (Small Mail Transfer Protocol).
3. Besedilo v kanonični obliki digitalno podpišemo ('prstni odtis' oziroma MIC (Message Integrity Check) besedila lahko zaenkrat izračunamo s funkcijama MD2 in MD5). Če želimo zagotoviti še tajnost pošte, sporočilo dopolnimo z znaki, kot to zahtevajo določeni kriptoalgoritmi, in ga zašifriramo. V PEM so taka sporočila tipa ENCRYPTED. Zaenkrat imamo v ta namen na voljo le algoritem DES v načinu CBC (Cipher Block Chaining), odpira pa se možnost vključitve večkratnega šifriranja z DES (Triple-DES) s podvojeno dolžino ključa. Ključ za šifriranje generiramo vsakič na novo.
4. Besedilo, dobljeno na prejšnjem koraku, moramo v primeru, ko se bo spremenilo znotraj sistema za prenos sporočil MTS (Message Transfer System), dodatno zakodirati. Kodirana in podpisana (ne pa tudi šifrirana) sporočila so tipa MIC-ONLY, samo podpisana pa tipa MIC-CLEAR.

Sporočilo v PEM, ki je pripravljeno za prenos, je v bistvu niz ASCII znakov, zato ga lahko pošiljamo s poljubnim sistemom elektronske pošte, na primer X.400 ali SMTP.

Postopek branja pošte poteka v obratnem vrstnem redu kot pisanje. Najprej sporočilo dekodiramo, dešifriramo, preverimo digitalne podpise in iz kanonične oblike pretvorimo v lokalno. Za vse to potrebujemo dodatne informacije, ki jih najdemo v glavi sporočila. Glava med drugim vsebuje tip sporočila, informacijo o tem, s katerim algoritmom in ključem je bilo opravljeno podpisovanje oziroma šifriranje (ključi so zašifrirani z javnim ključem prejemnika pošte oziroma s skupnim skritim ključem), digitalni podpis, certifikat posiljatelja v primeru asimetrične kriptografije...

Običajnemu uporabniku seveda ni potrebno poznati podrobnosti procesiranja sporočil. Zadostuje pa, da ima svoj certifikat, in da pozna naslov osebe, ki ji želi pisati. Vse, razen pisanja pisma opravi namesto njega računalnik.

V uvodu smo videli, da mora biti za delovanje takega sistema na voljo način pridobivanja in preverjanja javnih ključev drugih uporabnikov. PEM podpira že omenjeni sistem certifikatov (7), čeprav se od njega nekoliko razlikuje predvsem v hierarhični strukturi agencij za izdajanje certifikatov in formatu seznamov za shranjevanje potrdil, ki niso več veljavna. Podrobnosti so opisane v (12, 13).

Danes obstaja v svetu več izvedb pošte PEM. V ZDA sta to na primer TIS/PEM iz Trusted Information Systems in izvedba z MIT (Massachusetts Institute of Technology). Glede na to, da seveda vsebujeta algoritme za šifriranje, velja za oba produkta prepoved izvoza (razen v Kanado). V Evropi so v okviru projekta Password (14) svoje rešitve razvili na UCL (University College of London), univerzi v Cambridgeu, GMD (Gesellschaft für Mathematik und Datenverarbeitung) v Nemčiji in INRIA v Franciji, na Švedskem pa obstaja komercialna različica z imenom COST-PEM.

V lanskem letu se je v projekt Password vključil tudi nas Laboratorij za odprte sisteme in mreže z Instituta Jožef Štefan. Poleg testiranja pilotskih aplikacij za zagotavljanje varnostnih servisov v odprtih sistemih smo razvili orodje, ki uporabniku omogoča lažje in hitrejše preverjanje javnih ključev oziroma certifikatov. Laboratorij zaenkrat predstavlja tudi vrhovno agencijo za izdajanje certifikatov za Slovenijo. Z vzpostavitvijo agencije je bil pri nas izpolnjen še zadnji potreben pogoj za izmenjavanje pošte PEM s preostalim svetom.

2.2 PGP

Drug program za zagotavljanje varne pošte, ki je prav tako kot večina izvedb PEM v javni lasti in ga lahko zastonj uporablja vsakdo, se imenuje PGP (Pretty Good Privacy). PGP ali kriptosistem javnih ključev za široke ljudske množice, kakor mu pravijo nekateri, se je v zadnjem času bliskovito razširil po vsem svetu. Šele z njim so mnogi spoznali, da za učinkovito kriptografsko zaščito datotek in pošte ne potrebujejo dragih naprav ampak le kratek in preprost program, čeprav PGP ni nič drugega kot skupek že davno znanih kriptografskih metod in kriptoalgoritmov. V primerjavi s PEM je manj formaliziran, pa tudi upravljanje s ključi zaenkrat ni dodelano za uporabo v globalnih sistemih. Kljub temu nudi dokaj visoko stopnjo zasebnosti za vsakogar.

Glavne razlike med PGP in PEM so:

1. PGP uporablja drugačen simetrični kriptoalgoritem: namesto DES nam je na voljo IDEA (International Data Encryption Algorithm), ki ima dolžino ključev 128 bitov, kar je precej več kot pri DES (56 bitov),
2. PGP sporočilo pred šifriranjem kompresira,
3. namesto agencij za izdajanje certifikatov si javne ključe uporabniki podpisujejo med seboj,
4. v okolju PEM obstajajo seznami za shranjevanje certifikatov, ki so bili preklicani pred iztekom časa veljavnosti.

Razliki, ki najbolj ločita PGP in PEM, sta predvsem zadnji dve. Certifikat v sistemu PGP vsebuje poleg javnega ključa in datuma izdelave še oznako ključa, ponavadi je to ime in priimek lastnika ter njegov naslov elektronske pošte, ki pa si jo uporabnik izbere sam in povsem poljubno. Ob nepazljivosti omogoča taka izbira številne zlorabe. Recimo, da nekdo označi svoje ključe s tujimi naslovi. Če osebe, ki ji želimo pisati, ne poznamo osebno, kako bomo potem z gotovostjo vedeli, kateri izmed ključev z enakim imenom je v resnici njen? Za reševanje takih problemov uporabniki drug drugemu podpisujejo certifikate, kar je drugače kot pri PEM, kjer to počnejo hierarhično urejene agencije. Vsak javni ključ lahko podpiše več ljudi in če med podpisniki najdemo nekoga, ki mu zaupamo ter smo prepričani, da je ključ, s katerim je

podpisan certifikat, res njegov, lahko verjamemo v verodostojnost ključa, ki smo ga našli. Tak decentraliziran način potrjevanja ključev je verjetno dober za manjše skupine, ki pelijo ostati ločene od drugih in v katerih se ljudje poznajo med seboj, ni pa primeren za velika, globalno povezana okolja.

3. Aplikacije za overjanje

Dokument ISO 7498-2 (1) loči overjanje podatkov in overjanje oseb, s katerimi smo vzpostavili zvezo. Preverjanje vira podatkov nam omogočajo digitalni podpisi, za ugotavljanje resnične identitete sogovornikov pa uporabljamo različne protokole. Vsakomur je verjetno poznano šibko overjanje, kjer je identiteta določena s poznavanjem gesla. Trenutno se gesla v mrežah prenašajo večinoma v nezaščiteni obliki, zato so lahka tarča za vsakogar, ki se želi dokopati do njih. Obstajajo načini prenosa gesel in dodatnih informacij (čas izdelave, naključna števila) za preprečevanje podvajanja, zaščitenih s funkcijami za katere je težko izračunati inverz, vendar so še vedno šlabši kot metode močnega overjanja s pomočjo poverilnic, dobljenih s kriptografskimi algoritmi, ki so običajno asimetrični. Prednost teh metod pred uporabo gesel je tudi ta, da nobena izmed obeh sodelujočih strani (seveda tudi nihče drug) pri overjanju ne dobi dovolj informacij, da bi se lahko kasneje izdajala za nasprotno stran.

3.1 Kerberos

Kerberos (15) je sistem za overjanje v odprtih računalniških mrežah. Razvit je bil na MIT (Massachusetts Institute of Technology) kot del projekta Athena, danes pa je v uporabi v številnih računalnikih Interneta. Kerberos temelji na simetrični kriptografiji in protokolu, ki sta ga leta 1978 predstavila R.Needham in M.Schroeder (16). V tem protokolu uporabljata osebi pri predstavitvi druga drugi tretjo stran, kateri v celoti zaupata. V primeru Kerberosa pri overjanju najpogosteje sodelujejo odjemalec (klient), strežnik in center za razdeljevanje ključev KDC (Key Distribution Center), ki predstavlja tretjo stran. Vsak sodelujoči (uporabnik, strežnik) ima pri sebi skrit ključ za simetrični kriptoalgoritem (DES), ključi vseh pa so znani KDC, ki je sestavljen iz dveh delov: AS (Authentication Server) in TGS (Ticket Granting Server). Očitno je seveda, da morajo biti ključi v KDC shranjeni tako, da do njih ne more nihče razen centra samega.

V nadaljevanju si bomo na kratko pogledali, kako poteka overjanje:

1. Klient se predstavi KDC ter mu pošlje namero za povezavo z določenim strežnikom.
2. KDC pošlje klientu naslednje podatke (poverilnico), zašifrirane s klientovim skritim ključem: začasni ključ za šifriranje ("session key"), katerega bosta klient in strežnik uporabljala za zagotovitev tajnosti pogovora, in karto ("ticket") za strežnik, katere šifrirani del, zašifriran s skritim ključem strežnika, vsebuje ime klienta, čas veljavnosti karte ter začasni ključ.
3. Pod pogojem, da se je predstavil s pravim imenom, klient dešifrira prejete podatke. Strežniku pošlje karto, ki jo je prejel od KDC, in overitelja ("authenticator"), ki med drugim vsebuje natančen čas izdelave ("timestamp") overitelja, ime klienta in začetne vrednosti za simetrične kriptoalgoritme, ki jih bosta obe strani uporabljali pri komunikaciji. Overitelj je zašifriran z začasnim ključem.
4. Strežnik s svojim skritim ključem dešifrira karto, iz nje izlušči začasni ključ in preveri ime klienta ter čas izdelave sporočila. Uspešno dešifriranje overitelja mu pove, da pošiljatelj pozna začasni ključ v karti, s preverjanjem časa pa izključi možnost, da bi prišlo do podvajanja enega izmed prejšnjih sporočil. Težava pri uporabi vključevanja časa izdelave za odkrivanje ponovljenih sporočil je potrebna sinhronizacija vseh ur v sistemu.

V praksi poteka na ta način v bistvu le začetna komunikacija z AS, v kateri klient zahteva karto (TGT-ticket granting ticket) za TGS. Pri nadaljnjih predstavitvah klient komunicira s TGS, vsa šifriranja s klientovim skritim ključem v zgornjem protokolu pa se nadomestijo s šifriranji z začasnim ključem iz TGT.

Izvedba Kerberosa z MIT, trenutna verzija ima številko 5, nima dovoljenja za uporabo zunaj ZDA in Kanade.

3.2 DASS

Drug znani sistem za overjanje se imenuje DASS (Distributed Authentication Security Service) (17) in je bil razvit v DEC (Digital Equipment Corporation). Za razliko od Kerberosa temelji na asimetrični kriptografiji in sistemu certifikatov.

Označimo s Ksx in Kpx skriti in javni ključ osebe X. Na začetku dela (ob priklopu na računalnik) si vsak uporabnik zgradi podatkovno strukturo, imenovano poverilnica ("credential"), ki mu do izklopa oziroma do izteka veljavnosti služi za predstavljanje sogovornikom. Z njo uporabnik v bistvu poveri računalniku nalogo, da opravlja različna dela v njegovem imenu.

Poverilnica vsebuje ime uporabnika, karto, na kateri je čas veljavnosti karte, začasni javni ključ uporabnika (Ktpx), blok (UID - unique identifier), v katerem so shranjene dodatne informacije o uporabniku in digitalni podpis teh treh stvari, narejen s Ksx, ter začasni skriti ključ (Ktsx). Uporabnika njegovo ime enolično določa v celotnem sistemu in je neodvisno od računalnika. Drugače povedano, nobena dvojica nima enakega imena za overjanje.

Predstavljanje osebe A osebi B z DASS poteka na naslednji način:

1. A v imeniku poišče javni ključ osebe B in ga preveri.
2. A pošlje B dokaz pristnosti ("authentication token"), ki vsebuje karto, začasni ključ za DES algoritem (označimo ga z Dek), zašifriran s Kpb, digitalni podpis

zašifriranega ključa Dek, dobljen s Ktsx, overitelja (natančen čas izdelave in podpis strukture, sestavljene iz časa in naslova računalnika) ter morebitne dodatne informacije.

3. B dešifrira ključ Dek, v direktoriju poišče certifikat osebe A, preveri njen javni ključ Kpa in vse digitalne podpise v prejetem sporočilu.
4. Pri vzajemnem overjanju B poslje A z Dek zašifriran čas izdelave overitelja.

Osebi v zgornjem protokolu lahko seveda nadomestimo tudi z računalnikoma. V odprtih sistemih ponavadi ni dovolj, da nas predstavlja samo računalnik na katerega smo se priklopili na začetku, saj le-ta za izvršitev naloge kliče druge računalnike, ki tudi delajo v našem imenu. V tem primeru pri predstavljanju nadomestimo digitalni podpis zašifriranega ključa Dek v dokazu pristnosti z začasnim skritim ključem Ktsx, zašifriranim z Dek. Naš predstavnik tako pozna oba začasna ključa. Podobne možnosti za delegiranje svojih predstavnikov obstajajo tudi pri Kerberosu.

Program overjanja s pomočjo javnih ključev se imenuje SPX.

4. Programske knjižnice

Večina kriptografskih algoritmov in metod je sprogramiranih in shranjenih v različnih programskih knjižnicah, ki so v javni lasti. Eden izmed takih programskih paketov je tudi SecuDe (Security Development Environment), ki je bil razvit na GMD (Gesellschaft für Mathematik und Datenverarbeitung) v Nemčiji. Podobna paketa so v okviru že omenjenega projekta PASSWORD razvili tudi v Franciji (TORQUEMADA/MAVROS) in Veliki Britaniji (OSISEC). Sistem SecuDe vsebuje različne algoritme za šifriranje (RSA, DES, IDEA), zgostitvene funkcije (MD, SHS (Secure Hash Standard)) ter metode za digitalno podpisovanje. V njem najdemo tudi modul za generiranje in razdeljevanje ključev, generiranje in upravljanje certifikatov in vzpostavljanje agencij za izdajanje certifikatov, modul za povezavo z direktorijem X.500, modul za upravljanje osebnega varnostnega okolja ter izvedbo standarda za varno pošto PEM.

5. Zaključek

Kljub temu, da je stanje na področju varnosti v odprtih računalniških mrežah danes še daleč od željenega, je uporabniku na voljo vse več aplikacij za zagotavljanje varnostnih zahtev pri izmenjavi podatkov. V prispevku smo si ogledali nekatere izmed njih, ki so namenjene za kriptografsko zaščito podatkov, varno pošto ter overjanje sporočil, ljudi in računalnikov. Predstavljene rešitve lahko v nekomercialne namene uporabljamo zastonj, večina izmed njih pa nam je na voljo tudi pri nas.

6. Literatura

1. International Standards Organization. ISO 7498-2: Information Processing Systems - Open Systems Interconnection - Basic Reference Model - Part 2: Security Architecture, 1988.
2. Jerman-Blažič B.: Varnost v računalniških mrežah z dodano vrednostjo, Uporabna informatika, letnik 1, st.2, 22-26, 1993.
3. National Bureau of Standards: Data Encryption Standard. Federal information processing standards publication 46 edition.
4. Diffie, Hellman: New directions in cryptography. Trans. IEEE on Information Theory, IT-22, No.6, 1976.
5. Rivest R., Shamir A., Adleman L.: A Method for obtaining digital signatures and public-key cryptosystems. Communications of the ACM, Vol. 21 (2), 120-126, Februar 1978.
6. International Standards Organization. ISO 9594-3: The Directory: Abstract Service Definition, 1988.
7. International Standards Organization. ISO 9594-8: The Directory: Authentication Framework, 1993.
8. Kaliski B.: The MD2 Message Digest Algorithm. RFC 1319, RSA Laboratories, 1992.
9. Rivest R.: The MD4 Message Digest Algorithm. RFC 1320, MIT and RSA Data Security, Inc., 1992.
10. Rivest R.: The MD5 Message Digest Algorithm. RFC 1321, MIT and RSA Data Security, Inc., 1992.
11. Linn J.: Privacy Enhancement for Internet Electronic Mail: Part 1 - Message Encipherment and Authentication Procedures. RFC 1421, Februar 1993.
12. Kent S.: Privacy Enhancement for Internet Electronic Mail: Part 2 - Certificate-Based Key Management. RFC 1422, Februar 1993.
13. Kaliski B.: Privacy Enhancement for Internet Electronic Mail: Part 4: Key Certification and Related Services. RFC 1424, Februar 1993.
14. Kirsten P.T., Williams P.: Piloting Authentication and Security Services in the Password Project, Proc. INET'93.
15. Kohl J., Neuman C.: The Kerberos Network Authentication Service (V5). RFC 1510, Digital Equipment Corporation, USC/ Information Sciences Institute, September 1993.
16. Needham R., Schroeder M.: Using Encryption for Authentication in Large Networks of Computers. Communications of the ACM, Vol. 21 (12), 993-999, December 1978.
17. Kaufman C.: Distributed Authentication Security Service. RFC 1507, Digital Equipment Corporation, September 1993.
18. Balenson D.: Privacy Enhancement for Internet Electronic Mail: Part 3: Algorithms, Modes and Identifiers. RFC 1423, Februar 1993.
19. Denning D., Sacco G.: Time stamps in Key Distribution Protocols, Communications of the ACM, Vol. 24 (8), 533-536, Avgust 1981.