OpenPGP protokol in zaščita elektronske pošte

Aleš Zavec, Jaka Sodnik in Sašo Tomažič
Fakulteta za elektrotehniko
Univerza v Ljubljani
Tržaška 25, 1000 Ljubljana, Slovenija
ales.zavec@lkn.fe.uni-lj.si

OpenPGP protocol and e-mail security

This article presents the basics of cryptography used for e-mail protection in todays applications. E-mail is usually sent over the Internet as plain text. It can be read and altered by anyone whose server it passes through. Two basic features for E-mail security are: **Confidentiality** (The e-mail can only be read by the intended recipient. This is ensured using encryption.) and **Authentication** (The e-mail has been written and send by sender and has not been altered on its way to the recipient. This is achived with digital signatures.). OpenPGP specifies protocols to encrypt and digitally sign e-mail.

1. Uvod

Danes je elektronska pošta (e-pošta) ena od najpomembnejših in široko uporabljenih mrežnih internetnih aplikacij. Varnostna storitev je lahko dodana vsaki komunikacijski povezavi vzdolž poti oziroma poslanim podatkom tako, da je neodvisna od komunikacijskega mehanizma. Drugi pristop je t.i. ¨end-to-end¨ zaščita, ki je postala zelo pomemben uporabniški element. Dve osnovni značilnosti te vrste zaščite sta zaupnost - ¨confidentiality¨ (sporočilo lahko prebere samo tisti, kateremu je bilo namenjeno) in overjanje – ¨authentication¨ (prejemnik se lahko prepriča o identiteti pošiljatelja in celovitosti prejetega sporočila).
Samo zaščito e-pošte omogoča PGP aplikacija, ki temelji na OpenPGP protokolu. OpenPGP za zaščito uporabljata številne metode iz področja kriptografije in deluje na aplikacijskem nivoju TCP/IP protokolnega sklada.

2. Kriptografija

Kriptografija je znanost, ki uporablja matematiko za šifriranje in dešifriranje podatkov. Omogoča shranjevanje zelo občutljivih informacij ali njihov prenos preko nezavarovanega omrežja (kot je Internet), na tak način, da jih ne more prebrati nihče razen tistega, kateremu je informacija namenjena.

2.1. Osnovni pojmi

V kriptografski terminologiji osnovno sporočilo ponavadi imenujemo **čistopis** (plaintext, cleartext). **Šifriranje** (encryption) je metoda prikrivanja vsebine čistopisa. Z uporabo šifriranja želimo zavarovati informacijo tako, da je skrita vsem, ki jim ni namenjena, tudi tistim, ki lahko vidijo šifrirane podatke. Rezultat uporabe šifriranja nad čistopisom je nerazumljiv niz znakov, ki ga imenujemo **šifropis**. Postopek vrnitve šifriranega čistopisa nazaj v originalno obliko se imenuje **dešifriranje**. Za postopek šifriranja in dešifriranja uporabimo določene vrednosti, imenovane **ključ,** kot parametre v algoritmu. Ključ je začetna vrednost algoritma s katerim izvedemo šifriranje. Poznamo dva razreda šifrirnih algoritmov, ki temeljita na uporabi ključev: **simetrični** (*skrivni ključ* – secret key) in **asimetrični** (*javni ključ/tajni ključ* – public key/private key) algoritmi. Simetrični algoritmi uporabljajo isti ključ za šifriranje in dešifriranje. Asimetrični algoritmi uporabljajo različna ključa za šifriranje in dešifriranje sporočila: Pomembno je, da dešifrirnega ključa ni mogoče dobiti iz šifrirnega ključa.

2.2 Simetrično šifriranje

Pri simetričnem šifriranju, ki se imenuje tudi šifriranje s skrivnim ključem, se uporablja samo en ključ za šifriranje in dešifriranje podatkov. Prednost simetrične kriptografije je v tem, da je zelo hitra in je najbolj uporabna pri mirujočih podatkih, ki jih ni potrebno pošiljati. Uporaba simetrične kriptografije za oddajo varovanih podatkov je lahko zelo draga zaradi težavne varne distribucije ključev. Za varno komunikacijo pri uporabi simetričnega šifriranja, se morata pošiljatelj in prejemnik nekako sporazumeti glede ključa, ta pa mora ostati njuna skrivnost. Če se nahajata na različnih fizičnih lokacijah, morata distribucijo ključa zaupati kurirju ali kaki drugi vrsti varne komunikacije, ki preprečuje razkritje skrivnega ključa med prenosom. Kdorkoli prestreže ključ med prenosom, lahko pozneje prebere, spremeni ali ponaredi vse informacije zaščitene in overjene s tem ključem. Glavni problem simetričnega šifriranja je torej varna distribucija ključa.

2.3. Asimetrično šifriranje

Kriptografija z uporabo javnih in zasebnih ključev je asimetričen sistem, ki uporablja par ključev za šifriranje in dešifriranje. Javni ključ se uporablja za šifriranje podatkov, pripadajoči zasebni ključ, imenovan tudi tajni ključ, pa za njihovo dešifriranje. Vsak uporabnik tega sistema, objavi javno svoj javni ključ, medtem, ko zasebni ključ obdrži kot skrivnost. Vsi (tudi neznani pošiljatelji), ki razpolagajo z določenim javnim ključem, lahko zaščitijo informacijo. Ta je na voljo za branje le lastniku ustreznega zasebnega ključa.
Glavna prednost kriptografije z javnim ključem je v tem, da omogoča uporabnikom varno izmenjavo sporočil, brez predhodnega vzpostavljanja varne povezave. Potreba po izmenjavi skrivnih ključev preko varnih kanalov je izključena. Vse komunikacije obsegajo samo javne ključe in noben zasebni ključ ni nikoli prenešen ali deljen z drugo osebo.

2.4. Zgostitveni algoritmi

Zgostitveni algoritmi preslikajo poljubno dolg niz znakov v blok konstantne dolžine, ki je nekakšen prstni odtis oziroma povzetek vhodnega niza (message digest). Od zgostitvenega algoritma pričakujemo, da je nemogoče najti dve različni sporočili, ki bi ju preslikali v isti blok in da zgostitveni algoritem vedno preslika isto sporočilo v enak blok. Poleg tega iz zgostitvenega bloka ni mogoče restavrirati sporočila (od tu ime ¨one-way hash function¨). Vsaka sprememba v sporočilu povzroči spremembo zgostitvenega bloka. Rezultat mora torej enolično identificirati datoteko. Zaradi te lastnosti so povzetki postali nepogrešljivi pri digitalnem podpisovanju. Ne smemo pa teh algoritmov zamenjevati s kompresijskimi postopki (zip, rar, itd.), kjer lahko vedno iz zgoščene datoteke dobimo nazaj prvotno datoteko.
Najbolj znani zgostitveni algoritmi so:

- MD5,
- SHA (Secure Hash Algorithm).

Do leta 1996 se je večinoma uporabljal MD5, zdaj prevladuje uporaba SHA-1.

2.5. Digitalni podpisi

Digitalni podpis je majhna količina podatkov, ki predstavlja povzetek dokumenta narejenega z zgostitvenim (hash) algoritmom šifriran z avtorjevim zasebnim ključem po asimetričnem algoritmu. Pošiljatelj torej izračuna povzetek dokumenta z zgostitvenim algoritmom. Podpis naredi tako, da povzetek šifrira s svojim zasebnim ključem. Nato odpošlje dokument, ki mu priloži podpis. Naslovnik z javnim ključem pošiljatelja dešifrira podpis in dobi povzetek. Nato izračuna povzetek dokumenta z istim zgostitvenim algoritmom kot pošiljatelj. Če se ujemata, pomeni, da je dobil tak dokument, kot ga je pošiljatelj podpisal oz. poslal. Digitalni podpis torej omogoča prejemniku informacije overjanje njenega izvora in celovitosti sporočila. Kljub veliki varnosti, ki jo omogoča tak sistem, se pojavi še en bistven problem. Ali lahko verjamemo, da je pošiljatelj ali pa prejemnik res tisti, za kogar se izdaja? Kako naj vemo, da ni nekdo ponaredil (na primer) javnega ključa našega naslovnika? Ta problem rešujejo digitalna potrdila.

2.6. Digitalna potrdila

Digitalno potrdilo je digitalni dokument, ki potrjuje povezavo med javnim ključem in osebo, institucijo ali strežnikom. Digitalno potrdilo digitalno podpiše oseba ali institucija, ki ji zaupamo. Pri delu z javnimi ključi morajo uporabniki nenehno paziti na verodostojnost uporabljenih javnih ključev. V okolju javnih ključev je nujno potrebno, da zanesljivo vemo, da javni ključ s katerim šifriramo podatke, pripada predvidenemu naslovniku in da ni ponaredek.

2.6.1. Oblike digitalnih potrdil

V praski se za zaščito elektronske pošte večinoma uporabljata dve vrsti potrdil X.509v3 in PGP potrdila.

Oblika digitalnega potrdila po standardu ISO/IEC X.509v3:

- Verzija (zdaj do verzije 3).
- Serijska številka (enolična za potrdila posameznega overitelja).
- Algoritmi in parametri (npr. SHA-1 in RSA).
- Izdajatelj (overitelj javnih ključev).
- Datuma veljavnosti od – do.
- Prejemnik digitalnega potrdila (njegovo ime, drugi podatki).
- Podatki o njegovem javnem ključu:
    1. algoritem,
    2. parametri,
    3. javni ključ.
- Enolična oznaka uporabnika (samo v verzijah 2 in 3).
- Razširitve (verzija 3).
- Digitalen podpis teh podatkov, ki je narejen z zasebnim ključem CA.

PGP potrdila (OpenPGP RFC 2440):

- **Različico verzije PGP** – identificira katera verzija programa PGP je bila uporabljena pri ustvarjanju ključa povezanega s certifikatom.
- **Javni ključ lastnika certifikata** – javni del para ključev skupaj z algoritmom ključa: RSA, RSA Legacy, DH (Diffle-Hellman) ali DSA (Digital Signature Algorithm).
- **Informacijo o lastniku certifikata** – ta je sestavljena iz informacij o identiteti uporabnika: ime, identifikacijska številka, elektronski naslov, ICQ številka, fotografija, itd.

- **Digitalni podpis lastnika certifikata** – imenovan tudi lastnoročni podpis. To je podpis, ki uporablja pripadajoči tajni ključ, iz para ključev povezanih s certifikatom.
- **Obdobje veljavnosti certifikata** – začetni datum/čas in končni datum/čas certifikata. Tako vemo, kdaj bo pretekla veljavnost certifikata. Če par vsebuje podključe, potem je opredeljen tudi datum prenehanja veljavnosti podključev.
- **Izbran prioritetni simetrični algoritem za šifriranje ključa** – naznanja kateremu šifrirnemu algoritmu daje lastnik certifikata prednost.

3. PGP in OpenPGP

Na PGP lahko gledamo kot na protokol in aplikacijo. Trenutno je najnovejša verzija PGP 8.0.2. Sama PGP aplikacija temelji na OpenPGP protokolu, ki je opisan v OpenPGP Message Format, RFC 2440, med tem, ko je MIME pakiranje za OpenPGP opisano v MIME Security with Pretty Good Privacy, RFC 3156.

3.1. Osnovne značilnosti PGP aplikacije

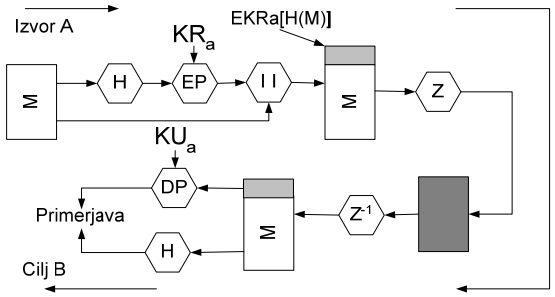
PGP je aplikacija, ki omogoča storitev zaupnosti (confidentiality) in overjanja (authentication). Te storitve se uporablja za shranjevanje datotek in za zaščito elektronske pošte. PGP uporablja za overjanje obe predhodno omenjeni obliki potrdil. X509v3 je hierarhičen model, kjer nam potrdilo izda priznani overitelj potrdil (CA Certification Authorithy), po drugi strani predstavlja PGP model mrežno zaupanje, kjer vsak uporabnik nastopa v vlogi overitelja in s tem odpade potreba po glavni CA. Mrežno zaupanje uporablja neposredno zaupanje in hierarhično zaupanje. Potrdilu lahko zaupamo neposredno ali pa ima zaupanje nekega člena v verigi, ki je povezan z izvornim overiteljem. Če kdorkoli od uporabnikov podpiše drug ključ, postane ta uporabnik overitelj tega ključa. Z nadaljevanjem tega procesa se vzpostavi mrežno zaupanje. Pri izdelavi PGP potrdila omogoča aplikacija uporabniku izbiro vrste algoritma in velikost šifrirn-ega(ih) ključ-a(ev). PGP potrdilo je bolj primerno za osebno uporabo, X509v3 pa za poslovne sisteme.

3.2. PGP opis delovanja

Dejansko delovanje PGP aplikacije je sestavljeno iz petih storitev: overjanja, zaupnosti, kompresije, združljivosti elektronske pošte in segmentacije.

3.2.1. Overjanje

Overjanje je torej storitev, ki omogoča digitalni podpis sporočila. V primeru overjanja se šifrira povzetek sporočila (dobljen z zgostitvenim algoritmom SHA-1) z avtorjevim tajnim ključem. Šifriran povzetek se nato pripne čistopisu. Celoten postopek je prikazan na sliki.

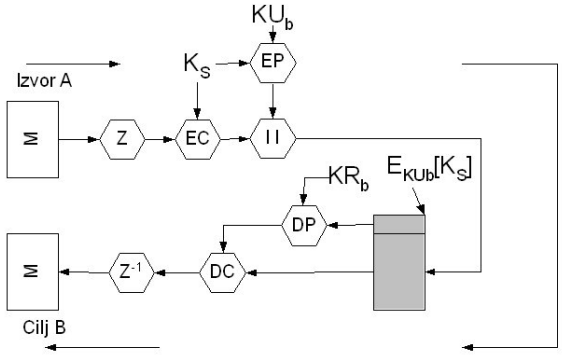


Slika 1: Overjanje sporočila.

Legenda za overjanje:
M - Sporočilo, **H** - Zgoščevalna funkcija, **EP** - Šifriranje z javnim ključem, **KRa** - Tajni ključ uporabnika A, **II** - Spojitev, **Z** - Kompresija, $\mathbf{Z^{-1}}$ – Dekompresija, **DP** - Dešifriranje s tajnim ključem, **KUa** - Javni ključ uporabnika A.

3.2.2. Zaupnost

Zaupnost dosežemo s šifriranjem sporočila. Sporočila šifriramo s simetričnim algoritmom, za vsako sporočilo se generira nov ključ. Na voljo so sledeči algoritmi: CAST (128 bitni), IDEA (128 bitni), 3DES (168 bitni), AES (256 bitni) in Twofish (256 bitni). Simetričen ključ je šifriran s prejemnikovim javnim ključem (RSA ali DSS) in pripet sporočilu.



Slika 2: Zaupnost sporočila.

Legenda za zaupnost:
M - Sporočilo, **Z** - Kompresija, **EC** - Simetrično šifriranje, **EP** – Šifriranje z javnim ključem, **Ks** – simetrični ključ, **II** – Spojitev, **DP** – Dešifriranje s tajnim ključem, **DC** – Simetrično dešifriranje, $\mathbf{Z^{-1}}$ – Dekompresija, **KUb** - Javni ključ uporabnika B, **KRb** - Tajni ključ porabnika B.

3.2.3. Overjanje in zaupnost

V praksi se večinoma uporabljata obe storitvi hkrati, pri tem je zelo pomemben vrstni red operacij. Kot prvo se izvede overjanje, saj se mora podpis izračunati iz čistopisa sporočila. V nasprotnem primeru bi prejemnik sporočila potreboval tudi simetrični ključ (Ks) za preverjanje podpisa. Če primerjamo predhodni storitvi na obeh slikah, lahko združimo celotni proces

na mestu kompresije (Z) - podpisovanju sledi šifriranje in obratno na mestu dekompresije (Z^{-1}) - dešifriranju sledi preverjanje podpisa.

3.2.4. Kompresija in segmentacija

PGP aplikacija opravi kompresijo sporočila po podpisu sporočila in pred njegovim šifriranjem (na sliki 1 in 2 kompresijo in dekompresijo predstavljata Z in Z^{-1}). Podpis se generira pred kompresijo iz dveh razlogov:
- ker to zadostuje za shranjevanje navadnega teksta (čistopis) in podpisa, za kasnejšo verifikacijo,
- ker PGP kompresijski algoritem ni deterministične; različne izvedbe algoritma dosežejo različne hitrosti in stopnjo kompresije.

S šifriranjem sporočila po opravljeni kompresiji povečamo kriptografsko varnost, saj ima kompresirano sporočilo manj redundance, kar oteži kriptoanalizo.
PGP avtomatično razdeli sporočila v segmente, ki so dovolj majhni za pošiljanje preko elektronske pošte. Na sprejemni strani se avtomatično izvede ponovna sestava sporočil.

3.2.5. Združljivost elektronske pošte

Mnogo sistemov elektronske pošte dovoljuje uporabo blokov, ki vsebujejo samo ASCII tekst. PGP standard uporablja Radix-64 pretvorbo za pretvarjanje zaporedja v ASCII znakovno obliko, primerno za tiskanje. Šifrirani deli sporočila tvorijo zaporedje 8-bitnih oktetov, dolžina sporočila po pretvorbi preko ACSII tabele naraste za 33,3% (iz 24 bitov na 32 bitov).

Vhodni Podatki	01000 |11 0101 |1100 10 |010001
Radix-64	01001001 00110001 011110001 01010010
ASCII	1lyR

3.3. PGP glavne lastnosti in prednosti

Sama aplikacija se je od prve verzije, (1991) brez grafičnega vmesnika, razvila v aplikacijo z obsežnim grafičnim vmesnikom, ki omogoča uporabniku zelo enostavno upravljanje z vsemi razpoložljivimi funkcijami, poleg same zaščite elektronske pa ima na voljo še dodatne varnostne mehanizme.
PGP aplikacija sestoji iz treh glavnih komponent. **PGP Keys** (ta komponenta omogoča uporabniku ustvarjanje osebnih ključev ter upravljanje z javnimi ključi drugih oseb), **PGP Mail** (omogoča šifriranje in dešifiranje sporočil) in **PGP Disk** (s to komponento lahko šifriramo celoten ali le del trdega diska oziroma USB diska in s tem popolnoma zaščitimo podatke tudi v primeru kraje ali izgube diska).
Dodatni varnostni mehanizni omogočajo še zaščito ICQ komunikacij, popolno brisanje datotek brez možnosti povrnitve izbrisanih podatkov in ustvarjanje arhivov, ki se lahko sami dešifrirajo.

Zelo pomenben dejavnik je tudi ta, da je na domači strani (www.pgp.com) na voljo popolna izvorna koda zadnje verzije PGP aplikacije. Namen objave izvorne kode je v tem, da to omogoča zainteresiranim posameznikom pregled celotne kode za pravilnost implementacije (šifriranje s prevedeno izvorno kodo nam mora dati enak šifropis kot šifriranje z originalno aplikacijo), poleg tega se uporabniki lahko prepričajo, da niso vgrajena stranska vrata, ki bi omogočala poznavalcu te bližnjice, enostaven obhod katerekoli zaščite. Za končne uporabnike pomeni to dodatno zagotovilo na področju varnosti PGP aplikacije.

Uporabniku so na voljo tri različne verzije aplikacije: PGP Personal, PGP Desktop in PGP Enterprise. PGP Personal je namenjena individualnim uporabnikom in ima vse zgoraj naštete lastnosti. Omogoča integracijo v Outlook Express, Outlook in Eudoro. PGP Desktop je namenjena manjšim skupinam, ki ne potrebujejo administracijske inštalacije in podpore in dodaja integracijo v sisteme elektronske pošte (Miocrosoft Exchange, Lotus Notes in Novell GroupWise). Tretja verzija PGP Enterprise je namenjena večjemu številu uporabnikov (korporacije), ki potrebujejo centralni nadzor, konfiguracijo in upravljanje, kar je omogočeno z dodatno komponento **PGP Admin**.

4. Zaključek

Že dolgo časa je javna skrivnost, da se izvaja nadzor nad elektronsko pošto pri njenem prenosu preko javnega omrežja (Internet). Ta se bo verjetno s časom še povečeval, zato bosta potreba in tudi zanimanje za zaščito elektronske pošte naraščala.
Sama PGP aplikacija, ki je trenutno na voljo, ob pravilni uporabi zagotavlja zadovoljivo zaščito naših sporočil in podatkov. Čeprav so možne napake v sami programski opremi in uporabljenih algoritmih, se je v praksi izkazalo, da je prav uporabnik sam najšibkejši člen celotnega varnostnega sistema in najpogostejši vzrok za odpoved izbrane zaščite sistema.

Literatura

[1] A. Zavec, Protokoli za zaščito elektronske pošte, Diplomska naloga, Ljubljana, 2002

[2] PGP Corporation, www.PGP.com, 2003

[3] S. Tomažič, Varnost v telekomunikacijah in kako jo zagotoviti, Zbornik 14. delavnice VITEL 2003, str. 9-14, Brdo pri Kranju, Slovenija, 2003