SAVREMENI KRIPTOGRAFSKI PROTOKOLI

Ermila Džogović
Univerzitet " Ukshin Hoti", Fakultet kompjuterskih nauka – Prizren
ermila.dzogovic@gmail.com

Muzafer Saračević
Univerzitet „Ukshin Hoti" Fakultet Kompjuterskih nauka,- Prizren
muzafer.saracevic@uninp.edu.rs

Abstract

In this paper we describe the basics of cryptography, how to protect the confidentiality of information. Symmetric and asymmetric algorithms that provide security by using a secret key are defined.
The basics of security are defined, the possibility of authentication of messages, authorization, validation, intransigence, anonymity, etc. An important security feature is that the data is readable only to those to whom it is intended, while those for whom it is not intended will not be legible and can not be used.
Finally, basic cryptographic protocols are provided that provide protection on all layers of the OSI reference model.

Keywords: cryptography, protocol, authorization, integrity, non-authenticity, anonymity, authentication, keys, security

Apstrakt

U ovom radu opisane su osnove kriptografije, kako zaštititi tajnost informacija. Definisani su simetrični i asimetrični algoritmi koji pružaju sigurnost primjenom tajnog ključa.
Definisane su osnove bezbjednosti, mogućnost autentifikacije poruka, autorizacija, validacija, neporečivost, anonimnost i dr. Značajna stavka bezbjednosti je da podaci budu čitljivi samo onima kojima su namijenjeni, dok za one kojima nisu namijenjeni neće biti čitljivi i ne mogu se upotrijebiti.
Na kraju predstavljeni su osnovni kriptografski protokoli koji pružaju zaštitu na svim slojevima OSI referentnog modela.

Ključne riječi: Kriptografija, protokol, autorizacija, integritet, neporečivost, anonimnost, autentifikacija, ključevi, sigurnost.

UVOD

Zaštita u mobilnoj mreži se bazira na autentifikaciji i anonimnosti korisnika i šifrovanju podataka koji se prenose.

Protokol predstavlja niz pravila koji omogućavaju komunikaciju između dva lica, a to mogu biti korisnici, proces ili računarski sistemi.

Ukoliko je u komunikaciji deo poruke šifrovan, taj protokol se može smatrati kriptografskim.

Kriptografski protokoli pružaju sigurnost komunikacije putem mreža i distribuiranih sistema.

Glavna namjena kriptografskih protokola je da obezbijede kompanijama i pojedincima sigurnosne usluge neporečivosti, poverljivosti i integriteta.

Kriptografskim protokolima se vrši izbor algoritma šifrovanja i dešifrovanja, vrši se izbor ključeva i dogovaraju drugi kriptografski parametri. Protokoli moraju obezbijediti osnovne sigurnosne usluge povjerljivosti, neporečivosti i integriteta kao i mehanizme za provjeru identiteta, autorizaciju i upravljanje ključevima (što uključuje generisanje, čuvanje i razmjenu ključeva).

OSNOVE KRIPTOGRAFIJE

Poruka je otvoren tekst (eng. *plaintext*) (ili čist tekst, eng. *cleartext*). Šifrovanje (engl. *encryption*) proces je maskiranja poruke koji za rezultat ima sakrivanje njene sadržine.

Šifrovana poruka je šifrat (engl. *ciphertext*). Dešifrovanje predstavlja povratak na prvobitan otvoreni tekst.

Slika 1. Šifrovanje i dešifrovanje

Kriptografija (engl. cryptography) je proces šifrovanja, odnosno,

postupak transofrmacije čitljivog teksta u oblik koji nije čitljiv za onoga kome taj tekst nije namijenjen.

Glavni zadatak kriptografije je očuvanje tajnosti informacija.

Najčešće korišćene tehnike u kriptografiji predstavljene su preko matematičkih transformacija koje posmatraju poruku kao skup algebarskih elemenata. Čitljiva poruka transformiše se u tekst koji nije čitljiv i dostupan entitetu kome nije namijenjen.

Kriptoanalitičari bave se kriptoanalizom, umjetnošću provaljivanja šifrata (tj. pogled iza maske).

Kriptologija je nauka koja se bavi proučavanjem algoritama i metoda za zaštitu podataka i informacija odnosno, šifrovanje, ali pored toga bavi se pronalaženjem i analizom metoda za otkrivanje šifrovanih informacija.

Podjela kriptologije:

- Kriptozaštita
- Kriptoanaliza

Kriptozaštita predstavlja dio kriptologije čiji je osnovni zadatak baziran na izradi metoda za šifrovanje informacija.

Pored toga bavi se i izradom ključeva koji se koriste u procesu šifrovanja informacija.

Osnovni zadatak kriptoanalize je proučavanje metoda za otkrivanje šifrovanih informacija, odnosno, otkrivanje tajnog ključa.

Cilj kriptografije je zaštita poruke od :

- pogrešnog primaoca
- pogrešnog emitovanja

Slika 2. Cilj kriptografije

PODJELA KRIPTOGRAFIJE

Na osnovu toga kriptografija se dijeli na simetričnu i asimetričnu kriptografiju.

Razlika između simetrične i asimetrične kriptografije je u primjeni ključa, jedna koristi isti ključ za kriptovanje i dekripciju, dok druga koristi različite ključeve.

Slika 3. Podjela kriptografije

SIMETRIČNA KRIPTOGRAFIJA

Simetrična kriptografija transformiše tekst gdje se koristi isti ključ za kriptovanje i dekripciju.

Glavni problem kod ovog vida kriptografije je da prilikom prijenosa šifrovane poruke prenosimo i ključ.

Tada se može pojaviti problem jer prilikom prijenosa se može presresti ključ pa se sadržaj poruke može pročitati. Pa to predstavlja glavni problem kriptografije.

ASIMETRIČNA KRIPTOGRAFIJA

Kao što je već definisano, pored simetrične kriptografije razlikujemo i asimetričnu kriptografiju.

Kod simetrične kriptografije imamo primjenu istog ključa za enkripciju i dekripciju, dok kod asimetrične kriptografije primjenjuju se dva ključa, a to su javni i privatni ključ.

Prilikom izrade ključeva oba ključa se izrađuju u isto vrijeme. Javni ključ se dodjeljuje svim osobama koje šalju određene podatke, dok privatni ključevi se dodjeljuju samo osobama koje primaju podatke.

SAVREMENI KRIPTOGRAFSKI PROTOKOLI

Klasifikacija savremenih kriptografskih protokola se može razvrstati u pet kategorija a to su:

- Bezbjednost na Web-u (SSH, SSL)
- Bezbjednost na IP sloju (IPSec)
- Bezbjednost u distribuciji simetričnih ključeva (Kerberos)
- Bezbjednost na bežičnim mrežama (WEP, WPA)
- Bezbjednost mobilnih uređaja (GSM, 3GPP)

PROTOKOLI ZA BEZBJEDNOST NA WEB-U

Na Internetu se koristi veliki broj protokola od kojih je svaki specijalizovan za svoj poseban zadatak. Neki od njih su namjenjeni za obezbeđenje specijalnih komunikacionih servisa, kao što je na primjer elektronska pošta ili pristup sistemu sa udaljenog terminala. Drugi su opšte namjene i koriste se u različitim vidovima komuniciranja.

Dominantan protokol na Webu je SSL (Secure Socket Layer). Služi za šifrovanje komunikacija opšte namjene između pretraživača (browser) i servera.

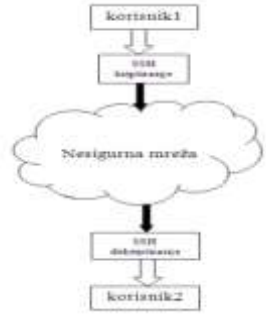
Protokol SSL se nalazi na transportnom nivou protokola TCP/IP, jedan nivo ispod nivoa aplikacija (kao na primjer NTTP(news), HTTP (Web), SMTP (elektronska pošta) ili TELNET).

Protokol sadrži sljedeće funkcionalnosti:

- Autentifikacija servera
- Autentifikacija korisnika
- Kriptovana SSL veza

SSH (eng. Secure Shell) protokol je nastao 90-ih godina prošlog vijeka kao zamjena za druge, nesigurne, protokole, poput rlogin, rsh, TELNET i FTP, koji putem računarske mreže razmjenjuju podatke. SSH za razliku od postojećih protokola uvodi zaštitu tajnosti podataka.

Naime, kod drugih sličnih protokola podaci se kroz mrežu šalju u otvorenom (nekriptovanom) obliku i bilo koji korisnik može ih presresti, pročitati ili čak mijenjati. SSH podatke kriptuje prije slanja i dekriptuje nakon prijema čime se onemogućuje njihovo otkrivanje dok se kreću mrežom.



Slika 4. SSH komunikacija
Izvor: CCERT-PUBDOC-2009-08-272

BEZBJEDNOST NA IP SLOJU (IPSEC)

Potreba za zaštitom podataka dok se transportuju kroz nezaštićenu mrežu je razvojem komunikacionih mreža postajala sve veća. Ranjivost računarskih mreža je sve veća pa je potrebno definisati određene tehnike zaštite, a to je moguće ostvariti primjenom protokola IP sloja.

Zaštita na mrežnom sloju, je veoma važna i nipošto ne smije se zanemarivati, jer bez te zaštite bi se moglo reći da zaštita uopšte ni ne postoji.

IPSec radi na mrežnom sloju OSI referentnog modela i za razliku od SSH i SSL protokola on pored aplikativnog dijela predstavlja i dio Operativnog sistema.

IPSec implementira šifrovanje i autentifikaciju u mrežnom sloju, osiguravajući tako sigurnu komunikaciju od početka do kraja unutar mrežne infrastrukture.

IPSec se sastoji od dva glavna dijela:

- IKE(Internet Key Exchange)
- ESP/AH (Encapsulating Security Payload / Autentification Header)

BEZBJEDNOST U DISTRIBUCIJI SIMETRIČNIH KLJUČEVA (KERBEROS)

Nakon generisanja ključeva, isti se mogu koristiti na različitim lokacijama i sa različitom opremom. Da bi se dopremili do udaljenih lokacija, ključevi se po pravilu transportuju preko nezaštićenih komunikacionih linija.

Ako se ključevi tokom transporta ne zaštite, mogu biti „ukradeni“, što cio sistem za kriptovanje čini nesigurnim. Preporučljivo rješenje je da se za prijenos ključeva koriste sigurne linije, kao što je na primjer dostavljanje ključa

korisnicima putem pošte.

Kerberos protokol se satoji od dva dijela:

- TTP
- KDC

Slika 5. Podjela kerberosa

BEZBJEDNOST NA BEŽIČNIM MREŽAMA

Iako se u standardima definiše nekoliko sigurnosnih elemenata, činjenica je da su bežične mreže najslabija sigurnosna karika unutar neke organizacije.

Standardi ne uspijevaju da zadovolje tri osnovna sigurnosna zahtjeva: pouzdanu provjeru identiteta korisnika, zaštitu privatnosti i autorizaciju korisnika.

WEP protokol

Standard 802.11 propisuje sigurnosni protokol WEP na nivou sloja podataka.

Sigurnost lokalnih mreža temelji se prije svega na fizičkoj sigurnosti prostora u kojem se mreža nalazi.

Bežične lokalne mreže ne mogu se fizički zaštiti jer je širenje signala teško ograničiti.

WEP obezbeđuje autentifikaciju i šifrirovanje komunikacije između klijenata i pristupne tačke. Algoritam za šifrovanje koristi 40-bitni tajni ključ i dodaje 24-bitni inicijalizovani vektor kako bi se kreirao 64-bitni inicijalizovani vektor.

WPA (Wi-Fi protected Access)

Organizacija Wi-Fi Alliance projektovala je WPA u okviru IEEE 802.11 standarda u namjeri da otkloni nedostatke uočene u WEP standardu, a da pri tome zadrži kompatibilnost s postojećom mrežnom opremom.

Unapređena su sva tri dijela WEP-a tj. provjera identiteta, privatnost i

integritet podataka. I dalje se koriste RC4 sistem za kriptovanje podataka i to uz 128-bitnim ključem i 48-bitni inicijalizovani vektor. Prednost u odnosu na WEP se odnosi u korišćenju:

- TKIP protokola (*Temporal Kez Integritz Protocol)* za šifrovanje,
- Standard 802.1x i neke od uobičajenih EAP protokola za provjeru identiteta,
- MIC (Message Integritz Check) za sprječavanje lažiranja paketa.

BEZBJEDNOST MOBILNIH UREĐAJA (GSM, 3GPP)

Zaštita u mobilnoj mreži se bazira na autentifikaciji i anonimnosti korisnika i šifrovanju podataka koji se prenose. Šifrovanje se vrši kako bi se onemogućilo napadaču da razumije komunikaciju između korisnika.

Naravno, nije moguće spriječiti napadača da prisluškuje, ali je šifrovanjem moguće spriječiti da napadač razumije podatke koje je prikupio. Anonimnost se ogleda u tome da korisnik mreži nikada ne šalje lične podatke, već ekvivalent u vidu jedinstvenih brojeva.

Razlog za to je da se napadaču oteža da identifikuje korisnike koji učestvuju u komunikaciji. SMART kartica u mobilnom uređaju sadrži jedinstveni International Mobile Subscriber Identity (IMSI) broj, koji služi za identifikaciju korisnika.

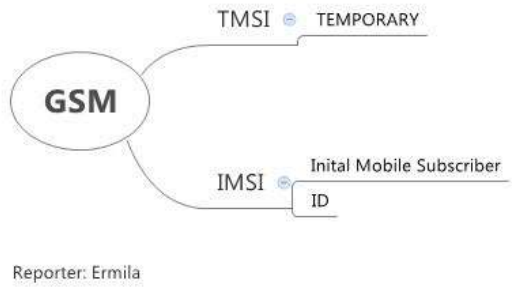
GSM

GSM (engl. *Global System for Mobile Communications*) predstavlja tehnologiju koja je rasprostranjena u Evropi. Prvi put se pojavljuje 80-tih godina u Švedskoj i polako je počeo osvajati Evropu, a kasnije i cijeli svijet.

Predstavlja tehnologiju koja omogućava pokretnu komunikaciju, sa oko 60 miliona korisnika širom svijeta.

GSM arhitektura se sastoji od sljedećih stavki:

- Mobilni uređaj – telefon
- Bazna stanica
- Kontroler baznih stanica
- Fiksna linija
- Mrežni operator
- GSM protokol se bazira na sljedećim komponentama:



Slika 6. GSM komponente

IMSI komponenta se koristi za inicijalnu identifikaciju korisnika, a TMSI predstavlja slučajno generisanje ID korisnika, koji se često mijenja i kada se šalje uvijek se šifruje.

TREĆA GENERACIJA PROTOKOLA – 3GPP

Na osnovu svih ranjivosti GSM-a došlo je do pojave 3G bezbjednosnog protokola.

Prilikom izrade protokola programeri su otklonili sve ranjivosti GSM-a.

Na primjer, *3GPP* uključuje uzajamnu autentifikaciju i zaštitu integriteta (kao što je komanda započni šifrovanje) između bazne stanice i mobilnog uređaja. Ovo poboljšanje eliminiše napad umetanjem lažnih baznih stanica.

Šifrovanje se obavlja od mobilnog uređaja pa do kontrolera bazne stanice (BSC).

ZAKLJUČAK

Računarske sisteme je danas sve teže zaštititi, jer svakim danom broj korisnika znatno raste pa je potrebno primjenjivati značajne tehnike zaštite.

Danas, sve se više javlja opasnost od pristupa informacijama od strane neovlašćenih entiteta, koji jednostavno mogu izmijeniti date podatke ili informacije i podmetnuti lažne.

Sve češće, informacije se prijenose različitim nesigurnim komunikacijskim kanalima, pa se pristup tim komunikacionim kanalima mora fizički zaštititi kako napadač ne bi narušio sigurnost sistema.

Kako bismo povećali zaštitu neophodno je, da se poruke prilikom

prijenosa kriptuju, što predstavlja najdjelotvorniji način ostvarenja sigurnosti.

Pored svih ovih tehnika zaštite, trka u razvoju novih mehanizama bezbjednosti se uveliko nastavlja.

LITERATURA

- [1] Milan Milosavljević, Saša Adamović (2014): Kriptologija II, Osnove za analizu i sintezu šifarskih sistema, Beograd.
- [2] Ćamil Sukić (2012): Sigurnost računarskih sistema, Novi Pazar.
- [3] Bruce Schneier, Primjenjena Kriptografija, prevod drugog izdanja.
- [4] Danilo Damjanović (2015): Kriptografski mehanizmi zaštite i digitalna forenzika, Podgorica.
- [5] Sinkovski Stevan, Lučić Branislav: Informaciona bezbednost i kriptografija, Beograd.
- [6] Saša Mrdović (2014): Sigurnost računarskih sistema, Sarajevo.
- [7] Kovačević Vladimir (2010): Zaštita podataka primenom kriptografskih metoda, Niš.
- [8] Branislav Veljković (2015): Kriptografski aspekti zaštite mreže za upravljanje telekomunikacionim sistemima.
- [9] Aleksandar Milošević (2011): Osnovi kriptografije, Niš.
- [10] Hamza Hadžić (2016): Kriptografski algoritmi i njihova analiza, Novi Pazar.
- [11] http://web.zpr.fer.hr/ergonomija/2005/rebac/asimetrCrypto.html
- [12] http://nasport.pmf.ni.ac.rs/materijali/2263/Zastita%20podataka.pdf
- [13] http://www.cis.hr/www.edicija/LinkedDocuments/CCERT-PUBDOC-2003-02-05.pdf
- [14] http://www.cert.hr/sites/default/files/CCERT-PUBDOC-2009-08-272.pdf
- [15] http://www.etf.ucg.ac.me/materijal/1353966929Sigurnosni-protokoli.pdf