UDC: 004.057.4 INFO M: str. 47-51

SIGURNOSNI ASPEKT FIX PROTOKOLA
SECURITY ASPECT OF FIX PROTOCOL

Marija Bogićević, Srđan Radojčić

REZIME: FIX protokol predstavlja standardizovani način elektronske razmene poruka koje se odnose na trgovanje hartijama od vrednosti. Predstojeća implementacija FIX protokola na Beogradskoj berzi poseban akcenat stavlja na sigurnosne aspekte i mehanizme implementacije protokola. FIX protokol definiše metode koji omogućuju autentikaciju, integritet i poverljivost poruke. U ovom radu biće izložen mehanizam zaštite poruka u FIX protokolu. Algoritmi koji se koriste za zaštitu podataka u FIX poruci su DES, PGP, PEM, dok se za digitalni potpis poruke koristi MD5.
KLJUČNE REČI: zaštita podataka, kriptografija, berza, fix protokol
ABSTRACT: FIX protocol is standardised method for exchanging electronic messages containing information about stock transactions. Future implementation of FIX protocol on Belgrade stock Exchange takes great concern on security and mechanism for protocol implementation. FIX protocol defines methods for authentication, integrity and confidentiality. This paper presents mechanism of data security in FIX protocol. Algorithms used for data security are DES, PGP, PEM. Additionally, MD5 is used for digital sigatures.
KEY WORDS: data security, cryptography, stock exchange, fix protocol

1. PROTOKOL

Protokol je unapred definisan način razmene podaka. U finansijskoj industriji rec "protocol" se odnosi na set pravila po kojima se šalju nalozi, primaju zaključnice i potvrđuje prijem istih. Takođe, banke koriste protokole za slanje novca oko sveta (npr."Swift"). Sam protokol je opis polja u kojima se nalaze relevantne informacije za dati podatak. Tako se bilo koji papirni formular može smatrati protokolom.

Potreba za jasno definisanim načinom razmene podataka potiče iz potrebe za brzinom razmene informacija i tačnošću istih u samoj finansijskoj industriji. Kako bi Beogradska berza vremenom prevazišla okvire lokalne berze i nastavila sa uspešnim poslovanjem i nakon završetka privatizacije, neophodno je uvesti odlike modernih, razvijenih tržišta.

Naravno, uvek je moguće rešiti problem komunikacije papirnim formularima ili korišćenjem aplikacija u koje korisnik mora da ukuca neophodne podatke, ali se na taj način smanjuje efikasnost i ograničava sloboda u poslovanju.

Uvođenje protokola omogućuje brokerima i vendorima da prave sopstvene aplikacije za trgovanje i da pri tome ne budu ograničeni operativnim sistemom ili programskim alatima. Samostalan razvoj aplikacija za trgovanje dovodi do poboljšanja samih aplikacija i do uvođenja višeg stepena konkurencije među brokerima jer im je omogućeno da razvijaju aplikacije koje nisu samo aplikacije za trgovanje već i inteligentni sistemi za analizu tržišta. Zbog poboljšanja kvaliteta i efikasnosti unošenja naloga dolazi do povećanja broja naloga a samim tim i produbljivanja tržišta.

2. OSNOVNI KONCEPTI FIX PROTOKOLA

FIX protokol je protokol koji je u ranim devedestetim ustanovljen kao standard za razmenu podataka koji se odnose na trgovinu hartijama od vrednosti između Salomon Brothers i Fidelity Investmentments institucija. U tom smislu se može porediti sa načinom razmene podataka između Beogradske berze i Centralnog Registra. Nakon prvobitne definicije formata podataka, FIX protokol je dobio na popularnosti i među drugim brokerima, tako da su u kasnim devedesetim i svetske berze počele da implementiraju "prevodioce" koji prevode i prihvataju naloge u FIX formatu.

FIX protokol se slikovito može opisati kao obrazac na kome brokeri prosleđuju nalog berzi. Na primer:

8 = FIX.4.19 = 6135 = A49 = BRKR56
= EXCH34 = 152 = 20000426 - 12:05:06

Prethodna poruka se tumači na sledeći način:

FIX polje sa vrednošću	Tumačenje
8 = FIX.4.1	Polje "8" označava verziju FIX protokola koja se koristi
9 = 61	Polje "9" označava dužinu poruke koja sledi, u ovom slučaju cela poruka se sastoji od šezdeset jednog karaktera
35 =A	Polje "35" je polje koje se zove "MsgType" i označava vrstu poruke ("obrasca") koji sledi. Polje "35" može imati različite vrednosti (npr. vrednost "D" znači da je prosleđena poruka nalog). U ovom slučaju prosleđena poruka je takozvani "Log on", tj. poruka kojom se brokeri prijavljuju na sistem.
49 = BRKR	Polje "49" je skraćeni naziv brokera koji šalje poruku. Npr. na Beogradskoj berzi u ovom polju bi stajala vrednost MVINV koja bi označavala M&V Investments.
56 = EXCH	Polje "56" je skraćeni naziv institucije kojoj je poruka upućena. Na Beogradskoj berzi vrednost ovog polja bi bila "BB" tj. "Beogradska berza".
34 = 1	Polje "34" označava redni broj poslate poruke. Kako je "Log on" poruka prva poruka koja se šalje u toku jedne sesije, vrednost ovog polja je "1". Svaka sledeća poruka dobija inkrementalno veći broj od prethodnog. Ovo polje se koristi da bi obe strane bile sigurne da nisu propustile ni jednu poruku.
52 = 20000426 - 12:05:06	Polje "52" označava vreme slanja poruke. Svetske berze praktikuju da odbiju poruke koje su starije od pet minuta jer je moguće da se situacija na tržištu promenila od trenutka slanja poruke. Ovo je posebno bitno u situacijama velike volatilnosti tržišta, kod kojih se naravno, dešava i opterećenje telekomunikacine mreze.

FIX nije software, niti je korišćenje FIX-a ograničeno od strane prvobitnih korisnika ili bilo koje druge institucije. Sam FIX definiše neprofitna organizacija "FIX Technical Committee", a pod vođstvom "Global Steering Committee"

i nekoliko radnih grupa. Sva pomenuta tela se sastoje iz predstavnika velikih svetskih banaka, brokerskih kuća i berzi koji su zainteresovane za unapređivanje poslovanja na finansijskim tržištima. Definicija polja i način njihovog korišćenja se nalaze na site-u www.fixprotocol.org. Sama definicija je prošla kroz nekoliko izdanja, kroz koje je nadgrađena tako da podržava većinu vrsta hartija (akcije, obveznice, više vrsta derivata).

FIX protokol se može najkraće definisati na sledeći način:

- To je standardni način za elektronsku razmenu informacija između institucija tržišta, samog tržišta i brokera.
- To je vrlo fleksibilno sredstvo za procesiranje svih vrsta informacija o trgovanju.
- Nezavistan je od računarske platforme, tako da radi sa više tipova računara i komunikacionih sistema.

Za njega se može reći da je specifikacija skupa poruka koji je razvijen kroz saradnju banaka, brokera, berzi, industrijskih asocijacija, institucionalizovanih investitora i softverskih kompanija u celom svetu. Svi ovi učesnici na tržištu kapitala delili su zajedničku viziju o jedinstvenom, globalnom jeziku za automatsko trgovanje hartijama od vrednosti. FIX je otvoren i slobodan za korišćenje i to nije softver. FIX je specifikacija na osnovu koje softverski razvojni timovi mogu kreirati komercijalne i besplatne aplikacije (open source). Kao vodeći protokol na tržištu kapitala FIX je inkorporiran u mnoge sisteme za trgovanje hartijama od vrednosti u svetu.

Većina svetskih berzi je pre uvođenja FIX-a koristila protokol koji je sama definisala. Neki od ovih protokola su postali popularni i na drugim berzama tako da sam FIX ima konkurenciju na svetskom tržištu (npr. STAMP, SWIFT). Međutim, uvidom u brojke, dolazi se do zaključka da je FIX ubedljivo najrasprostranjeniji standard i sve više berzi koristi upravo FIX kao glavni standard za razmenu podataka. Pomenućemo samo neke: London Stock Exchange, New York Stock Exchange, NASDAQ, Tokyo Stock Exchange, Deutsche Boerse AG, kao i mnoge manje berze. Lista korisnika govori da je FIX vodeći protokol, kako danas, tako i u budućnosti.

3. SUBJEKTI

Pri uvođenju FIX-a potrebno je učešće sledećih entiteta: Berza, brokeri, software provider-i i zakonodavna tela.

Komisija za implementaciju FIX-a koja tek treba da bude formirana bi bila zadužena za strateško planiranje i razvoj. Ovo telo bi bilo lider svih projekata koji se tiču FIX-a. Takođe, ova Komisija bi odigrala ključnu ulogu u komunikaciji sa zakonodavnim telima. Komisija treba da se sastoji od predstavnika Beogradske berze, Komisije za hartije od vrednosti, brokerskih kuća, predstavnika zakonodavnih tela kao i ostalih zainetersovanih institucija kao što su fakulteti i software proizvođači. Da bi delovanje ove Komisije bilo efikasno, potrebno je da se podeli na biznis i tehnički deo.

Berza je zadužena za pravljenje platforme za trgovanje, gateway-a za FIX i koordiniranje svih učesnika na tržištu. Takođe, zbog niskog stepena tehnološkog razvoja velikog broja brokerskih kuća, bilo bi poželjno da Berza razvije aplikaciju za trgovanje koja bi imala osnovne trgovačke funkcionalnosti.

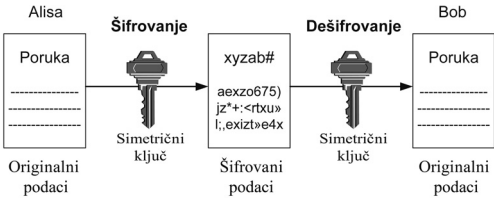
Brokerske kuće koje odluče da same razviju aplikaciju za trgovanje će biti odgovorne za ispravno funkcionisanje aplikacije. Sve brokerske kuće, bez obzira da li same razvijaju aplikaciju ili koriste aplikaciju spoljnih subjekata, su u obavezi da prilagode procedure poslovanja novom režimu (npr. Backoffice aplikacije).

Software proizvođači su softverske kuće koje bi pisale aplikacije za trgovanje na komercijalnom principu. Ova praksa je vrlo poželjna pri uvođenju FIX-a jer su profesionalne software-ske kompanije u boljoj poziciji nego Berza da kvalitetno opsluže brokere, i samim tim, da smanje pritiske na Berzu. Da bi učešće software-skih kuća bilo iskorišćeno na pravi način potrebno ih je uključiti u projekat pravovremeno i planski.

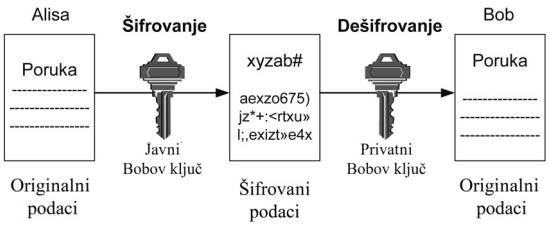
Zakonodavna tela bi bila aktivno uključena u realizaciju ovog projekta jer je neophodna izmena Zakona o hartijama od vrednosti koji definiše način unosa naloga koji FIX gateway ne bi ispoštovao. Takođe je neophodno prilagoditi zakon novonastaloj situaciji jer elektronski unos naloga značajno menja situaciju na tržištu i sa sobom donosi potencijalne probleme koji trenutnim zakonom nisu regulisani.

4. OSNOVNI KONCEPTI ZAŠTITE

Funkcionisanje FIX protokola mora biti zaštićeno odgovarajućim algoritmima, a najbolje rešenje je kriptografija. U okviru kriptografije kao izuzetno važne oblasti u sferi zaštite razlikuju se simetrični i asimetrični algoritmi. Simetrični algoritmi zahtevaju postojanje istog ključa i procesnog algoritma na oba kraja veze. Generišu tajni ključ koji se mora posebno zaštititi.



Dok asimetrični algoritmi koriste za šifrovanje i dešifrovanje podataka javni i privatni ključ. Javni ključ koristi pošiljalac radi šifrovanja poruke, dok se privatni ključ koristi na mestu prijema radi njenog dešifrovanja.



5. ZAŠTITA FIX PORUKE

Protokol definiše osnovna pravila po kojima se formira ključ sesije za vreme inicijalne logon sekvence. Ovaj ključ se koristi za enkripciju podataka u narednim porukama. Objašnjen je mehanizam digitalnog potpisa FIX poruke.

Postoje četiri vrste metoda za kriptovanje poruka zvanično podržanih od strane FIX protokola. To su: DES algoritam (Data Encryption Standard), kombinacija PKCS (Public Key Cryptography Standards) i DES, kombinacija PGP (Pretty Good Privacy), DES i MD5 (heš algoritam za generisanje digitalnog potpisa), kao i kombinacija PEM (Privacy Enhanced Mail), DES i MD5.

DES algoritam spada u grupu simetričnih kriptografskih algoritama koji koriste jedan tajni ključ za šifrovanje poruka. Sve ostale navedene tehnike koriste par ključeva (tajni i javni).

FIX protokol omogućava implementaciju bilo kog metoda, odnosno onog koji najviše odgovara u pogledu sigurnosnih zahteva. Odgovarajuće vrednosti za polje EncryptMethod su :

0 = None
2 = DES
3 = PKCS-DES
4 = PGP-DES-MD5
5 = PEM-DES-MD5.

Ukoliko je selektovano polje 0, tada se poruke šalju nekriptovane, odnosno nezaštićene. U tom slučaju nema ni zaštite integriteta sadržaja poruke. Ako se pojavi potpis podataka on se ignoriše. Ova opcija je krajne rizična, i u produkcionom okruženju neprihvatljiva, opravdanost njene upotrebe bi se mogla naći kada se poruke šalju u okviru fizički apsulutno zaštićene mreže.

U FIX protokolu definisana su četiri polja specijalno namenjena da podrže enkripciju kao i zaštitu integriteta. To su: Encrypted Data Length, Encrypted Data, Signature Data Length, and Signature Data. FIX protokol je prevashodno zasnovan na ASCII kodnom sistemu. Većina enkripcionih tehnika pri generisanju kriptovane poruke koristi svih 256 karaktera sa ciljem sprečavanja mešanja validnog graničnika FIX polja sa nekim enkriptovanim podatkom.

Svakom enkriptovanom polju mora prethoditi informacija o dužini podataka. Ovo omogućava FIX parseru da preskoči prethodni karakter koji je možda identičan sa karakterom graničnika FIX poruke, a kao polja graničnika uvršćena u enkriptovane podatke. Ovaj mehanizam se koristi i pri parsiranju polja koja služe za potpis podataka.

Kada enkriptovana poruka stigne na odredište, primalac parsira svako nekriptovano polje koje može biti uključeno u poruku. Ostatak poruke se zatim dekriptuje i re-parsira radi dobijanja kompletne dekriptovane FIX poruke.

Pošiljalac ima mogućnost da izabere koja će polja biti kriptovana, odnosno enkripciju celokupne poruke. FIX protokol definiše polja koja moraju biti uvek enkriptovana kada je enkripcija dozvoljena. Ova polja su : Sending Time, Sequence Number, Poss Dup Flag, SenderCompID, and TargetCompID. Enkripcijom pomenutih polja onemogućava se neovlašćeno dolaženje do FIX poruke, kao i modifikacija i fabrikacija poruka.

Enkricija podataka, i provera integriteta poruke zavise od verodostojne transmisije između dve strane. Ukoliko je enkripcija omogućena, gubitak ili dupliranje podataka će primorati sesiju da se restartuje. Ovo implicira da FIX podaci treba da budu poslati preko transportnog nivoa, poput TCP ili X.25. Podaci poslati korišćenjem nekog drugog protokola koji ne garantuje isporuku, moraju biti dostavljeni u korektnom stanju i bez ikakvih gapova (rupa).

6. RAZMENA KLJUČEVA

Problematika razmene ključeva ogleda se u potrebi uspostavljanja ključa za sesiju. Ukoliko je algoritam kritpovanja DES, pretpostavka je da je vrednost ključa poznata unapred za obe strane. Ključ ne može biti razmenjen između dve strane putem mreže bez preuzimanja treće strane. Enkripcija javnim ključem rešava ovaj problem, korišćenjem predefinisanog seta javnog i privatnog ključa. Svaka strana čini javni ključ dostupnim. Odgovarajući privatni ključ je dostupan samo njegovom vlasniku. Tokom logovanja strana koja pokreće sesiju random generiše ključ korišćenjem DES algoritma, koji se zatim enkritptuje javnim ključem primaoca poruke, i šalje kao deo LOGON poruke. Za autentifikaciju poruka je potpisana privatnim ključem pošiljaoca. Potpisana i enkriptovana poruka koristi PEM ili PGP standard.

7. ZAŠTITA FIX SESIJE

SessionInfo struktura sadrži 24 bajta. Prvih 8 bajtova u strukturi predstavljau DES_Key, DES ključ koji se koristi tokom sesije, generiše se slučajno, narednih 8 bajtova predstavlja inicijalni vektor (IV). Inicijalni vektor se koristi za DES-CBC[1] tip enkripcije, izbor vektora vrši se izborom slučajnih bajtova, poslednjih 8 bajtova su rezervisani za ChanBinding, ovo polje se koristi kako bi se onemogućio odgovor koji nije autentifikovan i autorizovan, ChinBinding polje sadrži broj porta brokerovog FIX engina, vrednost se čuva u ASCII kodu, pri čemu je potrebno da ima bar jedan vodeći prazan karakter. SessionInfo struktura se enkapsulira u Raw Data polje gde postaje deo podataka enkritpovan korišćenjem javnog ključa

Pri formiranju FIX LOGON poruke prvo se popunjava SessionInfo struktura koja se enkapsulira u RowData polje. Ovaj način konstruisanja poruke uslovljava potrebu da se RowDataLength polje postavi ispred RowData polja. Sva polja koja će biti enkritpovana se sastavljaju u baferu. Uključena su sledeća polja MsgSeqNum, SendingTime, SendingDate, RawDataLength and RawData. PEM/PGP poruka je konstruisana korišćenjem bafera kao ulaza.

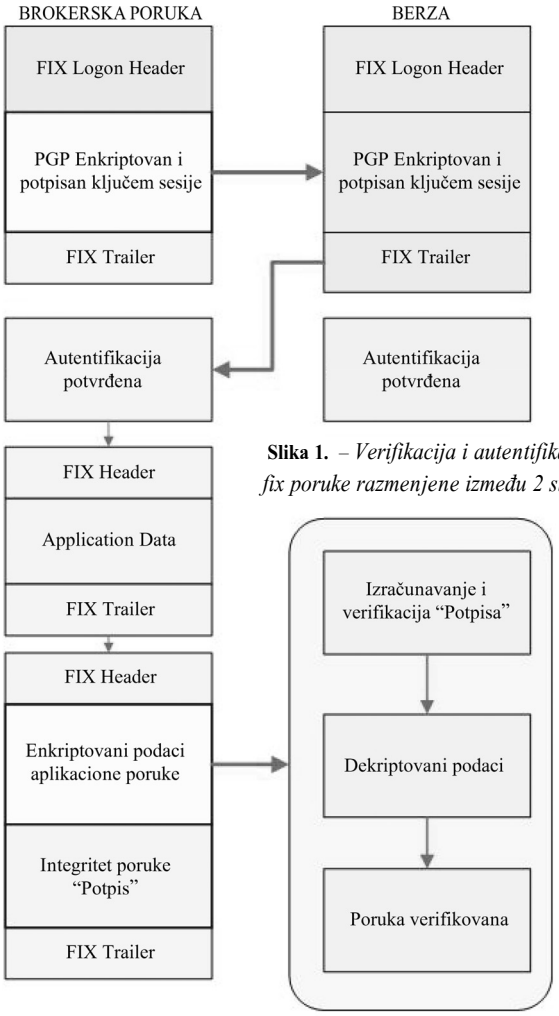
Enkriptovana poruka sadrži dovoljno informacija za autentifikaciju pošiljaoca primaocu te za uspostavljanje ključa koji će se koristiti tokom sesije. Za kriptovanje poruke koristi se javni ključ primaoca kako bi se osigurala privatnost i privatni ključ pošiljaoca, a s ciljem osiguranja autentičnosti pošiljaoca. Rezultat enkritpvoanja su podaci koji se konvertuju u ASCII tekst. Enkritpovani podaci su enkapsulirani u SercureData polju. SecureDataLen polje govori o dužini podataka. Ukoliko se radi o algoritmu enkripcije DES bufer je enkriptovan korišćenjem DES ključa prethodno razmenjenog između 2 strane. Kao javni ključ, DES ključ se koristi samo za enkripciju LOGON poruke.

Tag	Naziv polja	Tražen	komentar
	StandardHeader	Da	MsgType=A
98	EncryptMethod	Da	(Uvek nekriptovano)
108	HeartBtInt	Da	*Novo, samo u FIX 3.0*
90	SecureDataLength	Da	Dužina podatka koji
91	SecureData	Da	Sadži DES ključ sesije
	StandardTrailer	Da	

Zaglavlje LOGON poruke uvek sadrži SendingDate i SendingTime. Ova polja moraju biti enkriptovana PEM/PGP algoritmom. Fix engine na brokerskoj strani će odbiti sve logon zahteve ukoliko vreme i datum u tim poljima ne odgovaraju vremenu na lokalnoj mašini. Tolerancija od 10 minuta u oba smera se preporučuje.FIX protokol dozvoljava promenu ključa sesije tokom aktivne sesije. Nova LOGON poruka može biti inicirana sa obe strane. Poruka koristi novu strukturu DES ključa enkriptovanog na način sličan inicijalnoj LOGON poruci. Kako bi se sprečio napad u kojem se LOGON poruka šalje iz prethodne sesije poruka mora imati korektan broj sekvence i odgovarajući vremenski pečat. Svaka FIX poruka ima svoj broj sekvence koji se dobija inkrementiranjem prethodnog broja, brojevi sekvenci poruka ne smeju biti resetovani. Druga strana odgovora na ovu poruku pošiljaocu. Od ove tačke sve poruke će biti enkriptovane korišćenjem novog ključa. Potrebno je naglastiti da metod enkripcije u novoj LOGIN poruci ne mora da bude isti kao metod izabran u inicijalnoj poruci.

Signature polje nije potrebno za LOGON poruku u trejleru poruke. U koliko polje postoji, integritet poruke će biti proveren. DES ključ traži proveru integriteta poruke. Sve druge poruke moraju uključiti Signature polje. LOGOUT poruka takođe treba biti enkriptovana i zaštićena kao i sve druge FIX poruke.

1 DES-CBC - Data Encryption Standard- Cypher Block Chaining



Slika 1. – *Verifikacija i autentifikacija fix poruke razmenjene između 2 strane*

8. ENKRIPCIJA PORUKE KORIŠĆENJEM DES ALGORITMA

Ova sekcija opisuje enkripciju svih podataka u svim porukama osim LOGON poruke. Podaci koji će biti enkriptovani su prvo formatirani u baferu po specifikaciji FIX protokola. Bafer sadrži serije FIX polja, poslednji karakter u baferu mora biti FIX delimiter (SOH karakter ASCII vrednosti 0x01). Kako bi se popunila vrednost bafera koja mora biti deljiva sa 8 dodaju se random bajtovi. Vrednost takvog random podatka koji se dodaje može biti bilo šta osim SOH karaktera.

Baferisani podaci su kriptovani korišćenjem DES algoritma u CBC(Cypher Block Chaining) modu. Prvi bafer koji se enkriptuje koristi inicijalni vektor definisan u LOGON poruci. Svaki naredni bafer koristi poslednjih 8 bajtova kao inicijalni vektor. Ceo enkritpovatni bafer je enkapsuliran u SecureData polje. Ovom polju prethodi podatak o njegovoj dužini. SecureData polje će sadržati binarne karaktere. Na strani dekripcije, inicijalni vektor se takođe uzima iz LOGIN poruke. Svi naredni inicijalni vektori predstavljaju set od 8 poslednjih bajtova enkritpovane poruke, koje je prethodno dekriptovana.

Nakon dekripcije nepotrebni podaci koji su dodati na poruku (nakon poslednjeg SOH bajta) se odbacuju pre procesiranja FIX polja koja su dekriptovana. Ovi karakteri predstavljaju karaktere koji su dodati kako bi se dopunila dužina deljiva sa 8. Podaci se odbacuju kretanjem od poslednjeg karaktera bafera do pojave prvog SOH karaktera.

9. ZAŠTITA INTEGRITETA PORUKE

Svrha ovog koraka je zaštita integriteta poruke i neovlašćene izmene podataka. Nekriptovani heder i enkriptovani podaci će biti zaštićeni- Jednostavno enkritovana poruka sa DES algoritmom ne obezbeđuje uvek zaštitu integriteta poruke. Ukoliko je enkriptovana poruka promenjena rezultat dekriptovanja će biti nerazumljivi podaci, ali aplikacija možda neće uvek biti u mogućnosti da detektuje podatke koji nisu validni. Des ključ koji se uspostavlja tokom logon sekvence se koristi za zaštitu integriteta takođe.

MD5 Message Digest algoritam se koristi za konstruisanje sigurne provere integriteta. Cela poruka (uključujući zaglavlje i enkriptovano telo, bez trejlera) je zaštićena. Rezultujući checksum formira potpis poruke koji se smešta u trejler. Checksum nije povezana sa CheckSum poljem koje se pojavljuje u standardnoj FIX poruci.

Da bi se izračunao potpis, DES sesijski ključ je umetnut u MD5 engine kao prvih 8 bajtova. Bajtovi na najvišim pozicijama se prvi popunjavaju. Zatim se nekriptovani deo FIX zaglavlja prosleđuje. A onda se DES nekriptovani deo FIX poruke umeće. Na kraju, osam bajtova DES sesijskog ključa se umeću opet (s ciljem da zaštite poruku od napada). Izuzev StandardTrailer, cela poruka ima udela u digitalnom potpisu.

Rezultujućih 16 bajtova MD5 formira potpis poruke. Dužina ove vrednosti je smeštena u polju SignatureLength koja je praćena poljem Signature. Potpis se prenosi kao binarni podatak, stoga SignatureLength će sadržati vrednost 16.

Ovaj algoritam štiti od ponovnog slanja FIX poruke u sesiji, jer je DES Inicijalni vektor promenjen za svaku poruku. Duplirane poruke mogu biti odmah obrisane i uništene.

10. PRENOS PODATAKA

Seckure Socket Layer i Transport Layer Security su dva uobičajena protokola koji se koriste za prenos podataka između web klijenata i servera. SSL koristi kriptozaštitu podataka između dva sistema. Klijent inicira sesiju, dok server odgovara da je kriptozaštita potrebna i zatim usaglašavaju sisteme zaštite. TLS je protokol novijeg datuma, koji povezuje SSL sa drugim protokolima radi obezbeđenja kriptozaštite. SSL i TLS koriste port 443 i TCP za održavanje veze.

SSL/TLS biblioteke obavljaju verifikaciju sertifikata, komuniciraju sa TCP soketima. Biblioteka je crna kutija. SSLv3 je NETscape-ov protokol, a TLS je kompatibilan sa njim.

LITERATURA

[1] RFC1422: Privacy Enhancement for Internet Electronic Mail: Part II: Certificate-Based Key Management.
[2] Financial Information Exchange Protocol (FIX),
[3] Version 4.4, FIX Technical Committee, 30/04/2003,
[4] www.fixprotocol.org
[5] Data Formats -TRADING AND INFORMATION
[6] www.londonstockexchange.co.uk

Marija Bogićević
Fakultet Organizacionih nauka
Oblast Interesovanja: primena informacionih tehnologija, zastita racunarskih sistema

Srđan Radojčić
Fakultet Organizacionih nauka
Oblast Interesovanja: metodologija razvoja softvera, projektovanje poslovnih informacionih sistema, multimedijalne tehnologije