ЗАШТИТА ПОДАТАКА У РАЧУНАРСКИМ МРЕЖАМА

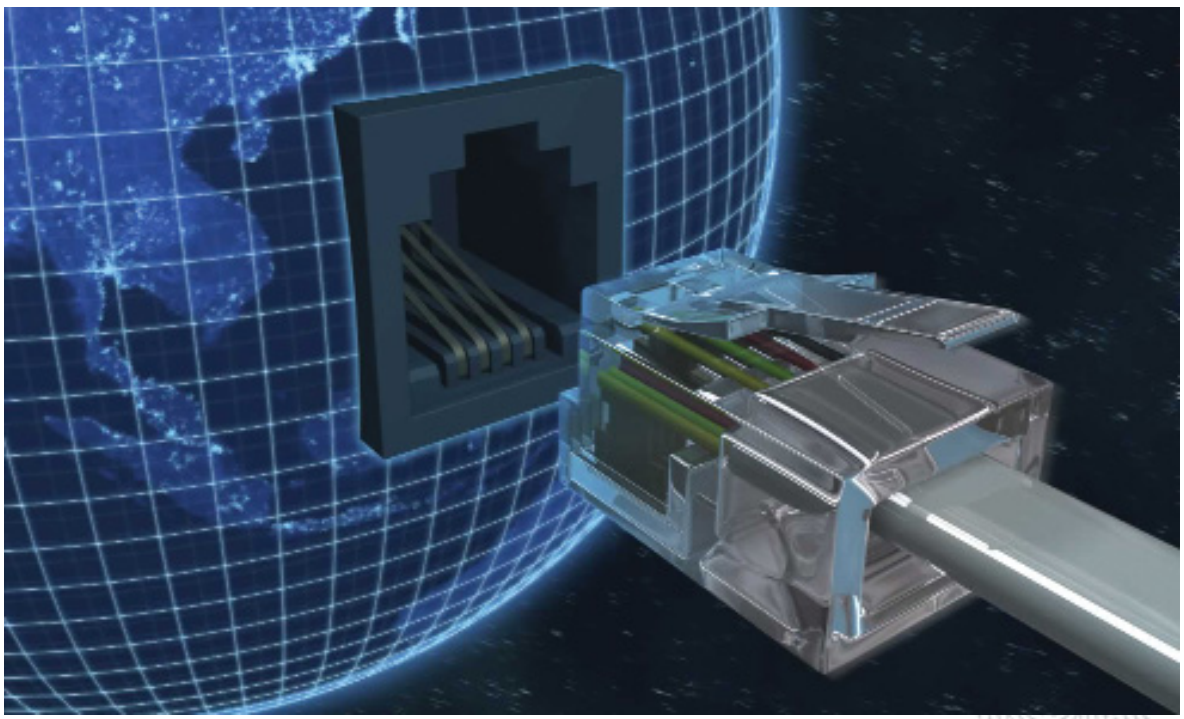
Капетан *Бориша* Јовановић,
Поручник *Ненад* Томић, Поручник *Велибор* Цекић

Током првих неколико деценија постојања рачунарске мреже су, углавном, користили истраживачи са универзитета за размену порука електронске поште и запослени у предузећима да би користили у то време скупе заједничке ресурсе кроз систем дељења, као, на пример, канцеларијске штампаче. У тим околностима мало ко је обраћао пажњу на безбедност. Али, данас, када милиони људи користе мреже за банкарске трансакције, за куповину или за попуњавање пореских пријава, безбедност на мрежи почиње да представља велики проблем. У овом раду обрађени су разни аспекти безбедности рачунарских мрежа и објашњени основни концепти и протоколи заштите рачунарских мрежа.

*Аутори раде у Центру за примењену математику и електронику, Управа за телекомуникације и информатику (J-6), ГШ ВС

Безбедносни проблеми на мрежи могу се грубо сврстати у четири повезане категорије: тајност, провера идентитета, немогућност порицања и контрола интегритета. Тајност, позната и као поверљивост, води рачуна о томе да информације не доспеју у руке неовлашћених особа. Провера идентитета остварује се ради утврђивања идентитета учесника у комуникацији, и неопходна је пре откривања осетљивих података или предузимања пословног подухвата. Немогућност порицања своди се на примену неког од постојећих метода дигиталног (електронског) потписивања: како доказати да је купац стварно, електронским путем, наручио десет милиона јединица неког производа, по цени од 89 динара, ако он касније буде тврдио да је цена била 69 динара? Купац може да тврди и да ништа није ни поручио. Најзад, како бити сигуран да је примљену поруку стварно послао купац, а не нека трећа страна која је пресрела дату поруку, намерно је изменила (нарушила њен интегритет) и тако измењену послала?

Када се говори о савременим рачунарским мрежама и функционалностима које оне пру-



жају, било са комуникационог или безбедносног аспекта, постоје два логичка референтна модела која се користе за описивање могућности рачунарских мрежа. Оба модела су слојевите структуре где се функционалности које пружа слој усложавају од најнижег логичког слоја ка највишем. Сваки слој енкапсулира одређени број функционалности за које је само он задужен, и те функционалности пружа слоју изнад себе кроз интерфејс услуга које се могу користити са вишег слоја. Стандардизовани референтни модел Open Systems Interconnection (OSI) настао је под окриљем ITU (енгл. ITU – International Telecommunication Union) који се састоји од седам логичких слојева: физичког слоја, слоја везе података, мрежног слоја, транспортног слоја, слоја сесије, презентационог слоја и апликативног слоја. Transmision Control Protocol/Internet Protocol (TCP/IP) јесте референтни модел настао развојем интернета и представља најзаступљенији мрежни модел који се користи у рачунарским мрежама данашњице. У раду ће се користити овај мрежни модел како би се објаснили безбедносни аспекти у оквиру рачунарских мрежа.

Пре анализе самих решења заштите у рачунарским мрежама треба рећи нешто о томе где се безбедносни механизми налазе у скупу мрежних протокола. То место није јединствено, већ би безбедносни механизми мреже требало да буду тако конципирани да сваки слој даје свој допринос укупној безбедности. У физичком слоју OSI модела, повезивање на жицу (физички медијум) може се спречити ако се преносни водови сместе у херметички затворену цев, испуњену гасом који је под притиском. Сваки покушај бушења цеви изазваће ослобађање гаса и снижење притиска, што аутоматски активира сигнал за узбуну. У слоју везе података OSI модела, пакети се на линијама од тачке до тачке могу шифровати на једном крају, а дешифровати на другом. Све се то може реализовати на нивоу слоја везе, без знања виших слојева. Такво решење је неадекватно ако пакет пролази кроз више рутера, јер се на сваком рутеру мора дешифровати, а тада постаје рањив на нападе из самог рутера. Описано решење такође не дозвољава да само неке сесије буду заштићене (нпр. само оне које се односе на куповину преко мреже помоћу кредитне картице). Ипак, шифровање везе (енгл. link encryption), како се назива ова техника, може се остварити у свакој мрежи и често је корисно. На мрежном слоју могу се инсталирати заштитне баријере које ће у мрежу пуштати само „добре" пакете, а оне „лоше" задржавати напољу. На транспортном слоју могу се шифровати читаве везе од једног до другог краја, тј. од једног процеса до другог, од клијента до сервера. За максималну безбедност потребно је применити шифровање на свим слојевима OSI модела. На крају, провера идентитета и немогућност порицања могу се остварити само у слоју апликација.

Имајући у виду слојевиту структуру савремених рачунарских мрежа, намеће се идеја да је за реализацију поузданог система заштите неопходно осмислити и применити вишеслојну архитектуру. На шеми 1 приказани су TCP/IP мрежни модел и предложени систем заштите. Увођењем додатних заштитних слојева повећава се укупна безбедност рачунарске мреже, а самим тим и безбедност система у целости.

Требало би да се систем заштите рачунарских мрежа састоји од следећа три независна безбедносна нивоа:

Заштита на апликативном нивоу, заштита „с краја на крај" (енгл. end-to-end security) заснива се на примени технологије дигиталног потписа на бази асиметричних криптографских алгоритама и заштите тајности података применом симетричних криптографских алгоритама. Применом овог нивоа зашти-

Шема 1. *TCP/IP мрежни модел предложеног система заштите*

те обезбеђује се: провера аутентичности корисника сервиса мреже, како у процесу успостављања комуникације (енгл. end-user authentication), тако и у процесу контроле приступа (енгл. access control) ресурсима мреже, заштита интегритета података, заштита од могућности накнадног порицања о слању порука, као и заштита тајности података.

Најпознатији протоколи заштите на апликативном нивоу, који се примењују у TCP/IP мрежама, јесу: S/MIME (енгл. S/MIME – Secure Multipart Internet Mail Extensions), Kerberos, SET (енгл. SET – Secure Electronic Transactions) и други. Ти системи се базирају на примени асиметричних и симетричних криптографских алгоритама и примени дигиталних сертификата, као једнозначних параметара идентификације страна у комуникацији. Протокол SET намењен је за заштиту финансијских трансакција, на бази примене кредитних картица, између клијената и банке. У савременој криптографији за заштиту електронске поште се, уместо PGP (енгл. PGP – Pretty Good Privacy) протокола, чешће користи S/MIME протокол. Kerberos је протокол који на бази симетричних криптографских алгоритама, посредством активне треће стране од поверења, реализује размену сесијских кључева и аутентикацију учесника у комуникацији.

Заштита на транспортном нивоу представља заштиту тајности података применом симетричних криптографских алгоритама и узајамне провере идентитета субјеката комуникације. Овај ниво штити комуникацију субјеката од интерних и екстерних напада применом криптографских тунела (заштићених сесија) између чворова комуникационог сегмента мреже на бази симетричних криптографских система и применом процедуре „јаке" аутентикације (енгл. strong authentication) између субјеката комуникације. Додатном применом симетричних криптографских система на транспортном нивоу реализују се функције заштите интегритета података који се преносе кроз мрежу.

Најпознатији коришћени протоколи су: SOCKS (енгл. SOCKS – SOCKet Secure), SSH (енгл. SSH – Secure Shell), SSL (енгл. SSL – Secure Sockets Layer), TLS (енгл. TLS – Transport Layer Security) и WTLS (енгл. WTLS – Wireless Transport Layer Security). Протокол SSH користи се за реализацију безбедног удаљеног приступа рачунару (енгл. remote login), извршења команди на датом рачунару и копирање датотека између рачунара који комуницирају. Најчешће се користи протокол SSL и састоји се од две фазе: аутентикације која се базира на примени асиметричних криптографских алгоритама и размени дигиталних сертификата, у којој се проверава аутентичност страна у комуникацији и размена сесијског кључа, и криптографског тунела који се базира на примени симетричног алгоритма са сесијским кључем који је размењен и израчунат у фази аутентикације. Протокол WTLS је бежична варијанта SSL протокола и служи за заштиту на транспортном нивоу између WAP (енгл. WAP – Wireless Application Protocol) мобилних телефона и WAP сервера на истим принципима (аутентикација и криптографски тунел), као и SSL протокол.

Заштита на мрежном нивоу обезбеђује заштиту између мрежних чворова и штити читав дистрибуирани рачунарски систем од спољашњих напада коришћењем:

– заштитних механизама које пружа стандардна комуникациона опрема,

– поступака заштите применом мрежних ба–ријера (енгл. firewall),

– заштитних механизама на мрежном нивоу које пружа оперативни систем,

– физичких мера заштите приступа рутерима и серверима и

– примена криптографских техника и протокола.

На мрежном нивоу врши се заштита интегритета, тајности и аутентикација IP пакета. Заштита интегритета и аутентикација IP пакета најчешће се реализује применом криптографских компресионих функција са употребом тајног кључа (енгл. MAC – Message Authentication Code), док се заштита тајности остварује применом симетричних криптографских алгоритама. Најпознатији протокол заштите на мрежном нивоу јесте IPSec протокол (енгл. IPSec – Internet Protocol Security).

ЗАШТИТА НА АПЛИКАТИВНОМ НИВОУ – S/MIME ПРОТОКОЛ

Један од најчешће коришћених апликативних сервиса је електронска пошта. Скуп TCP/IP протокола има за циљ да обезбеди међусобну размену електронске поште између највећег могућег броја рачунарских мрежа и система. Да би то било могуће, TCP/IP дели своје стандарде за пошту на два дела. Један стандард прописује формат поштанских порука (RFC 822), а други стандард одређује детаље размене електронске поште између два рачунара. На овај начин, раздвајањем два стандарда електронске поште, омогућава се изградња поштанских мрежних пролаза који повезују TCP/IP мреже са системом за испоруку поште неког другог испоручиоца, задржавајући при томе исти формат порука за оба механизма.

Multipurpose Internet Mail Extension (MIME) јесте интернет стандард који проширује формат поруке електронске поште како би омогућио да се произвољни подаци кодирају у ASCII формату и преносе као стандардне поруке електронске поште.

Secure/Multipurpose Internet Mail Extension (S/MIME) јесте стандардни протокол за шифровање и дигитално потписивање MIME података. Он представља вероватно један од најкоришћенијих протокола заштите на апликативном нивоу. S/MIME апликације уграђују се у софтверске пакете који су данас најдоминантнији на тржишту, као што су: Netscape Communicator, Microsoft Outlook, Lotus Notes, Novell итд. S/MIME се базира на популарном интернет MIME стандарду – проширењу. Он обезбеђује одређене криптографске услуге по питању сигурности за апликације типа електронске размене порука. То су: аутентикација, интегритет поруке и непорецивост (користећи дигитални потпис), и тајност података (дигиталну енвелопу).

S/MIME могу користити традиционални кориснички поштански агенти (енгл. MUA – Mail User Agents), како би се пошти, која је послата, додале криптографске безбедносне услуге, и како би се интерпретирале криптографске безбедносне услуге у пошти која је примљена. S/MIME није ограничен само на електронску пошту; може се користити са било којим транспортним механизмом који транспортује MIME податке, као што је HTTP (енгл. HTTP – HyperText Transfer Protocol). Осим тога, S/MIME може бити примењен у агентима аутоматизованог преноса порука који користе криптографске безбедносне услуге које не захтевају било какву интервенцију човека, као што је потписивање софтверски-генерисаних докумената и енкрипцију fax порука које се шаљу преко Интернета. Претходно је наглашено да MIME стандард пружа генералну структуру садржаја Интернет порука и одобрава екстензије за апликације новог садржаја.

S/MIME спецификација дефинише како креирати део MIME тела који је криптографски унапређен према CMS-у (енгл. CMS – Cryptographic Message Syntax – RFC 3852), који је изведен према PKCS-7 стандарду. CMS је Интернет стандард који дефинише структуру заштићене електронске поште. CMS се заснива на Rivest-Shamir-Adelman (RSA) стандарду асиметричног шифарског система и PKCS-7 форматом поруке, али CMS такође додаје типове података и семантику везану за њих. Ова спецификација такође дефинише application/PKCS7-MIME MIME тип који се може користити за пренос тих делова MIME тела. Кроз спецификацију, постоје захтеви и препоруке како агенти примаоци рукују са долазећим порукама. Постоје одвојени захтеви и препоруке како агенти трансмитери креирају одлазеће поруке.

Од Service Release 1 верзије Microsoft-овог пакета за пријем и слање електронске поште Outlook, побољшања везана за заштићено слање порука унапређена су тако да одговарају CMS и S/MIME стандарду. Ова побољшања укључују:

– подршку за слање и примање порука са следећим типом садржаја: SignedData, EnvelopedData i Data,

– подршку за примање порука са неограниченим угнеждавањем CMS типова садржаја,

– могућност валидације дигиталних потписа са неограниченим угнеждавањем CMS типова садржаја,

– могућност коришћења Ephemeral-Static Diffie-Hellman криптографског алгоритма, и

– могућност коришћења DSA (енгл. DSA – Digital Signature Algorithm) алгоритма за потписивање.

Порука са подацима спакованим у коверту

Порука са подацима спакованим у коверту (енгл. EnvelopedData) садржи шифровани еквивалент отвореног текста – шифрат, који је намењен одређеном скупу примаоца. Отворени текст се шифрује применом криптографског кључа, користећи симетрични криптографски алгоритам, као што је RC2 или 3DES. Примењени криптографски кључ се преноси заједно са подацима спакованим у коверту, и он је посебно шифрован јавним кључем сваког примаоца, тако да њега могу дешифровати само примаоци применом својих приватних кључева. Порука са подацима спакованим у коверту садржи:

– скуп структура везаних за информације о примаоцу (енгл. RecipientInfo), где свака структура садржи кључ шифрата и идентификацију сертификата примаоца, коришћеног за шифровање (по једном кориснику постоји један RecipientInfo),

– шифрат и

– информације о коришћеним алгоритмима шифровања.

Порука са потписаним подацима

Порука са потписаним подацима (енгл. SignedData) садржи отворени текст, плус један или више дигиталних потписа. Сваки дигитални потпис садржи сертификат потписника и криптографски отисак поруке (енгл. message digest) који је шифрован приватним кључем потписника, и остале информације, као што је, на пример, време потписивања. Дешифровање криптографског отиска поруке врши се јавним кључем потписника поруке. По дешифровању дигиталног потписа прималац поруке изврши исти поступак добијања отиска над добијеном поруком. Ако је добијени отисак поруке идентичан са дешифрованом вредношћу отиска, верификација је успела, у противном верификација је негативна. На овај начин, при-

малац може са сигурношћу тврдити да (1) порука није мењана од када је потписник потписао, и (2) да је порука заиста потписана од ентитета/особе идентификоване у поруци (претпостављајући да је сертификат потписника коректно верификован и да његов издавач има пуно поверење примаоца)[3]. Порука са потписаним подацима садржи:

– отворени текст,

– скуп сертификата коришћених у процесирању поруке,

– скуп структура везаних за информације о потписнику (енгл. SignerInfo), где свака структура садржи идентификацију потписника (показивач на сертификат потписника), дигиталне потписе и остале атрибуте,

– за S/MIME поруке, атрибут који специфицира S/MIME, укључујући алгоритам шифровања пошиљаоца и идентификацију сертификата који пошиљалац преферира да се користи приликом слања шифроване поште назад ка кориснику и

– информације о коришћеним алгоритмима.

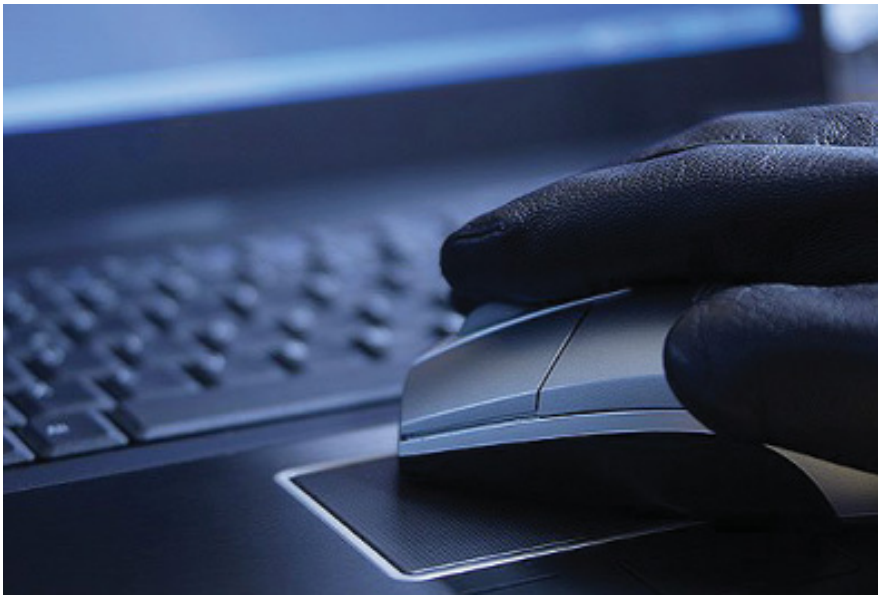
С обзиром на то да поруке са потписаним подацима могу да садрже информације о сертификату, оне се могу користити за прост транспорт сертификата. У овом случају порука не садржи отворени текст и SignerInfo структуре.

ЗАШТИТА НА ТРАНСПОРТНОМ НИВОУ – SSL ПРОТОКОЛ

Сигурности преноса података у TCP/IP мрежама, којима припада и глобална мрежа интернет, већ се дуже време посвећује велика пажња. Интересовање и потреба за сигурним преносом података знатно је порасла у новије време, када су тенденција броја и врсте садржаја, те услуга доступних на мрежи у наглом порасту. Постојећи механизми за сигурни пренос података у IP мрежама су добри и поуздани. Два најпознатија механизма за заштиту IP преноса података су SSL протокол и IPSec протокол. SSL протокол најчешће се користи за осигуравање комуникације код World Wide Web апликација које користе HTTP протокол за пренос података. IPSec протокол настао је као резултат настојања да се изради јединствени сигурносни протокол у оквиру скупа TCP/IP протокола, независан од протокола са виших нивоа.

Secure Sockets Layer (SSL) протокол изворно је развио Netscape Communications Corporation, а касније је постао општеприхваћен за аутентичну и криптолошки заштићену комуникацију између клијентских и серверских рачунара код World Wide Web апликација. На темељу SSL протокола, касније је IETF (енгл. IETF – Internet Engineering Task Force) издао стандард под називом TLS (енгл. TLS – Transport Layer Security) који је тако постао стандардни протокол за сигурну комуникацију у оквиру World Wide Web апликација. TCP/IP скуп протокола има улогу преноса и усмеравања података у IP мрежама и на интернету. Остали протоколи виших нивоа (апликативни ниво), као што су HTTP (енгл. HTTP – Hyper Text Transport Protocol), LDAP (енгл. LDAP – Lightweight Directory Access Protocol), IMAP (енгл. IMAP – Internet Messaging Access Protocol) и

слични, користе функционалности TCP/IP протокола за пренос и усмеравање података, док истовремено пружају подршку захтевима апликација, као нпр. приказ web страница, слање електронске поште итд. SSL протокол налази се изнад TCP протокола, а испод протокола са апликативног нивоа у вишеслојном моделу архитектуре TCP/IP мрежа, као што је приказано на шеми 1.



SSL протокол омогућава серверу, који га користи, да докаже свој идентитет клијенту, омогућује клијенту доказивање идентитета серверу и успоставу сигурне – криптолошки заштићене комуникације између клијента и сервера. То су уједно и три основне фазе сваке комуникације успостављене према SSL протоколу. Основни елемент за доказивање аутентичности код SSL протокола јесте дигитални сертификат који издаје трећа страна од поверења – сетификационо тело.

Алгоритам	Опис и примена криптографског алгоритма
DES	Data Encryption Standard
DSA	Digital Signature Algorithm
KEA	Key Exchange Algorithm, алгоритам за размену симетричних кључева
MD5	Message Digest version 5, hash функција и алгоритам за дигитално потписивање података
RC2 i RC4	Rivest Ciphers, симетрични криптографски алгоритми које је развио Рон Риверст
RSA	Асиметрични алгоритам за шифровање и аутентикацију
RSA key exchange	Алгоритам за размену симетричних кључева код SSL протокола заснован на RSA алгоритму
SHA-1	Secure Hash Algorithm, hash функција
Triple-DES	DES алгоритам примењен три пута над истим подацима

Табела 1. *Криптографски алгоритми коришћени код комуникације SSL протоколом*

SSL аутентикација сервера омогућава клијенту да се увери у аутентичност сервера са којим намерава да успостави везу. Користећи стандардне методе криптографије јавних кључева, програмска подршка за управљање SSL протоколом на рачунару клијента проверава ваљаност дигиталног сертификата датог сервера. Ваљани дигитални сертификат мора бити издат од треће стране од поверења.

SSL аутентикација клијента омогућује серверу да се увери у аутентичност клијента који са њим намерава да успостави везу. Користећи једнаке методе као и код аутентикације сервера, програмска подршка за управљање SSL протоколом на рачунару сервера проверава ваљаност дигиталног сертификата клијента.

Сви подаци који се размењују између клијента и сервера криптолошки се обрађују (шифрују) одговарајућом програмском подршком на рачунару пошиљаоцу, а дешифрују се на рачунару примаоцу, пружајући притом висок ниво тајности. Осим шифровања, подаци се пре слања дигитално потписују и на тај начин се постиже заштита интегритета података.

– SSL протокол користи два потпротокола:


Снимио М. АТЛАГИЋ

– SSL протокол записа порука (енгл. *SSL record protocol*) и

– SSL протокол договарања параметара сесије (енгл. *SSL handshake protocol*).

– SSL протоколом записа порука дефинишу су формати порука које се користе при преносу података. SSL протокол договарања параметара сесије користи се за размену порука састављених према SSL протоколу записа порука између SSL клијента и SSL сервера када се између њих по први пут успоставља SSL веза. Циљеви размене порука су аутентикација сервера клијенту, омогућавање клијенту и серверу да изаберу криптографски алгоритам који оба подржавају и који ће бити коришћен у комуникацији, аутентикација клијента серверу (ова активност није обавезна и остављена је серверу на избор), коришћење метода шифровања јавним кључевима за размену тајних симетричних кључева, и на крају успостављање сигурне – криптолошки заштићене SSL везе.

Криптографски алгоритми коришћени код SSL протокола

SSL протокол подржава више различитих криптографских алгоритама који се користе у поступцима међусобне аутентикације клијента и сервера, размене дигиталних сертификата и успоставе тајних симетричних кључева, односно кључева сесије. Програмска подршка на клијентском и серверском рачунару може се разликовати по томе који скуп криптографских алгоритама подржава, зависно од верзије SSL протокола коју подржава, и безбедносној политици организације о минимално прихватљивој дужини криптографских кључева. Поред осталих функција, SSL протокол договарања параметара сесије одређује на који начин клијент и сервер договарају скуп криптографских алгоритама и припадајућих кључева коришћених током SSL сесије. Криптографски алгоритми коришћени код комуникације SSL протоколом приказани су у табели 1.

Алгоритам Опис и примена криптографског алгоритма DES Data Encryption Standard DSA Digital Signature Algorithm KEA Key Exchange Algorithm, алгоритам за размену симетричних кључева MD5 Message Digest version 5, hash функција и алгоритам за дигитално потписивање података RC2 i RC4 Rivest Ciphers, симетрични криптографски алгоритми које је развио Рон Риверст RSA Асиметрични алгоритам за шифровање и аутентикацију RSA key exchange Алгоритам за размену симетричних кључева код SSL протокола заснован на RSA алгоритму SHA-1 Secure Hash Algorithm, hash функција Triple-DES DES алгоритам примењен три пута над истим подацима

Алгоритми за размену кључева, KEA (енгл. KEA – Key Exchange Algorithm) и RSA key exchange, одређују начин на који клијент и сервер договарају симетрични кључ који ће се користити током SSL сесије. У највећем броју случајева користи се RSA key exchange алгоритам. Током успостављања SSL сесије, односно у фази договарања криптографских параметара, клијент и сервер бирају најјачи скуп криптографских алгоритама који оба истовремено

подржавају, па тако договорени скуп алгоритама користе током SSL сесије.

SSL ПРОТОКОЛ ДОГОВАРАЊА ПАРАМЕТАРА СЕСИЈЕ

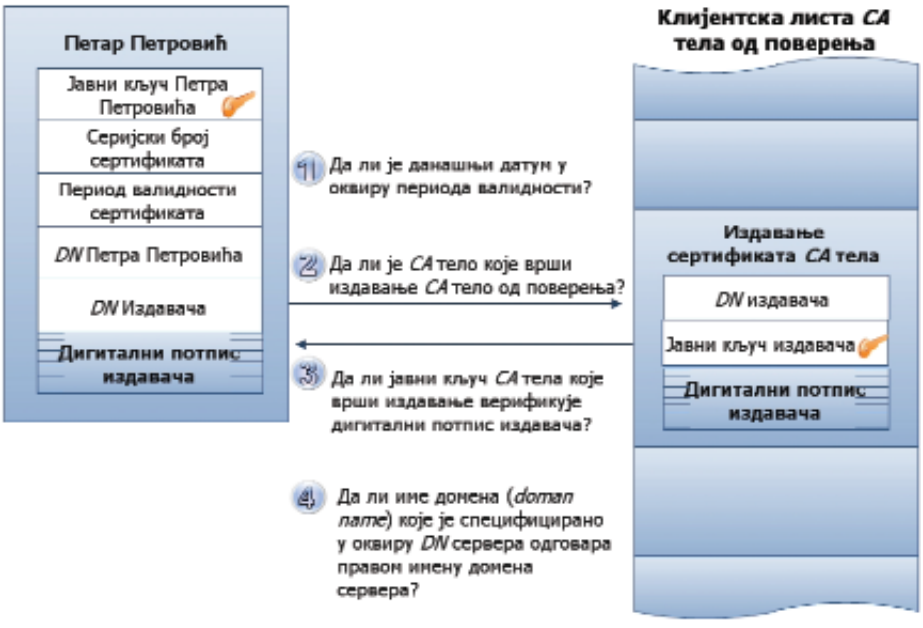
SSL сесија између клијента и сервера увек започиње разменом порука која је позната под називом SSL протокол договарања параметара сесије (енгл. SSL Handshake protocol). SSL протокол договарања параметара сесије омогућује кориснику да изврши аутентикацију сервера коришћењем метода криптографије са јавним кључевима. Такође, омогућава клијенту и серверу да заједно суделују у стварању и избору симетричног тајног кључа сесије који ће користити за шифровање, дешифровање и дигитално потписивање порука током SSL сесије. Ако сервер то захтева, SSL протокол договарања параметара сесије омогућава да и сервер изврши аутентикацију клијента. Ток размене порука код SSL протокола договарања параметара сесије је следећи:

1. Клијент шаље серверу верзију SSL протокола коју подржава његова софтверска подршка, наводи најјачи скуп криптографских алгоритама који је спреман да прихвати случајно генерисане податке и, по потреби, остале податке који су серверу потребни за комуникацију са клијентом, користећи SSL протокол.

2. Сервер шаље клијенту верзију SSL протокола коју је подржала серверска софтверска подршка, наводи најјачи скуп криптографских алгоритама који је спреман да прихвати властити дигитални сертификат, случајно генерисане податке и, по потреби, остале податке који су клијенту потребни за комуникацију са сервером коришћењем SSL протокола.

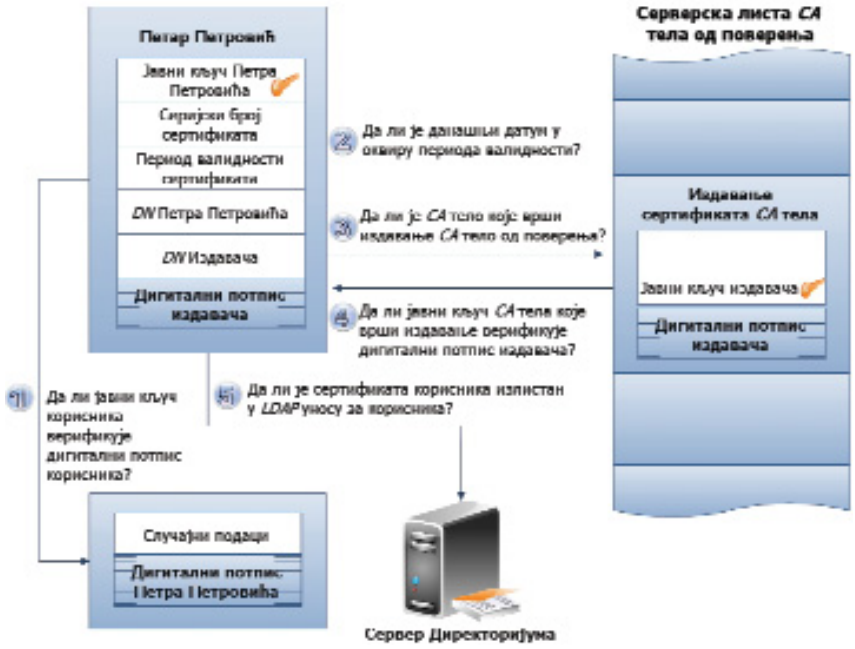
3. Податке примљене од сервера у кораку 2. клијент користи за аутентикацију сервера. Детаљи поступка SSL аутентикације сервера описани су у наставку рада. У случају да поступак аутентикације сервера резултира негативним исходом, сервер се обавештава о насталим проблемима и сигурна – криптолошки заштићена SSL веза не може бити успостављена. Уколико клијент изврши успешно аутентикацију сервера, поступак се наставља кораком 4.

4. Користећи све досад генерисане и размењене податке, клијент, у договору са сервером а у зависности од договорених криптографских алгоритама, ствара привремени тајни кључ (енгл. premaster secret). Привремени тајни кључ шифрује јавним кључем сервера. Јавни кључ сервера клијент добија из примљеног дигиталног сертификата сервера, који му је сервер послао у кораку 2. Овај привремени тајни кључ клијент шифрује и шаље серверу.



Шема 2. *Поступак SSL аутентикација сервера*

5. Ако сервер захтева аутентикацију клијента, клијент дигитално потписује податке произашле из досадашње размене порука, везане искључиво за ту сесију које су познате само клијенту и серверу. У том случају клијент серверу, осим шифрованог привременог



Шема 3. Поступак SSL аутентикације клијента

тајног кључа, шаље и властити клијентски дигитални сертификат и дигитално потписане податке.

6. Уколико се захтева аутентикација клијента, сервер у овом кораку најпре покушава да утврди аутентичност клијента. Детаљи поступка аутентикације клијента наведени су у наставку рада. Ако сервер не успе да потврди аутентичност клијента, сесија се прекида и сигурна – криптографски заштићена комуникација се не успоставља. Уколико је поступак аутентикације клијента успешно завршен, користи властити тајни кључ за дешифровање привременог тајног кључа. На основу привременог тајног кључа клијент и сервер израчунавају главни тајни кључ (енгл. master secret). Главни тајни кључ још увек није коначни симетрични кључ који се користи током SSL сесије.

7. Клијент и сервер користе главни тајни кључ за израчунавање кључа сесије (енгл. session key). Кључ сесије је симетрични кључ који се током SSL сесије користи за шифровање и дешифровање порука које се размењују током комуникације, као и за њихово дигитално потписивање.

8. Клијент шаље серверу поруку којом потврђује да ће све будуће поруке бити шифроване кључем сесије. Након тога шаље шифровану поруку којом серверу шаље обавештење да је протокол договарања параметара сесије на клијентовој страни завршен.

9. Овим кораком клијенту се шаље одговор на поруке из претходног корака. Сервер шаље кориснику поруку којом му потврђује да ће све будуће поруке бити шифроване кључем сесије. Након тога шаље шифровану поруку којом обавештава клијента да је протокол договарања параметара сесије и на страни сервера завршен.

10. SSL протокол договарања параметара сесије је завршен и SSL сесија је почела. Клијент и сервер користе кључ сесије за шифровање, дешифровање и проверу интегритета података које међусобно размењују.

Пре почетка SSL сесије, сервер може проверити да ли за дигитални сертификат клијента постоји запис у LDAP директоријуму издавача дигиталног сертификата. То је један од начина на који сервер може проверити да ли дигитални сертификат клијента није повучен из употребе.

Током поступка договарања параметара сесије, клијент и сервер користе својства асиметричне криптографије за шифровање и дешифровање порука које размењују. У случају аутентикације сервера, клијент шифрује привремени тајни кључ јавним кључем сервера. Само одговарајући тајни кључ може правилно дешифровати привремени тајни кључ. Клијенту се на тај начин гарантује да заиста комуницира са сервером чији је јавни кључ употребио за шифровање. У супротном, сервер не би био у могућности да дешифрује привремени тајни кључ и да израчуна главни тајни кључ и кључ сесије, па не би дошло до успостављања сесије. У случају аутентикације клијента, клијент случајно генерисане податке дигитално потписује својим тајним кључем. Јавним кључем из дигиталног сертификата

клијента може се утврдити исправност дигиталног потписа само ако је за потписивање употребљен одговарајући тајни кључ који је познат само власнику дигиталног сертификата. Уколико дигитални потпис није успешно верификован, сервер прекида договарање параметара и не допушта успоставу сесије. У наставку су детаљније описани поступци SSL аутентикације сервера и клијента.

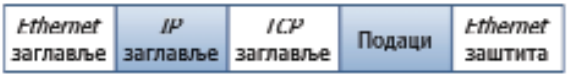
SSL аутентикација сервера

Клијентска софтверска подршка при успостави SSL сесије увек захтева аутентикацију сервера. За утврђивање аутентичности сервера клијент користи дигитални сертификат сервера који сервер шаље у кораку 3. протокола договарања параметара сесије. Да би се доказала аутентичност сервера, тј. веза између јавног кључа уписаног у дигитални сертификат и имена сервера уписаног у дигитални сертификат, корисник мора добити потврдан одговор на четири постављена питања, као што је приказано на шеми 2. Уколико је одговор на неко од неведених питања негативан, аутентикација се сматра неуспешном. Последње питање није део SSL протокола, али је препоручљиво да га клијентска софтверска подршка подржава, јер служи као заштита од напада пресретањем комуникације (енгл. *Man-in-the-Middle Attack*).

Након спроведеног поступка аутентикације сервера, сервер мора да искористити свој тајни кључ за дешифровање привременог тајног кључа. То је додатно осигурање клијенту да идентитет сервера, представљен дигиталним сертификатом, припада серверу са којим је клијент успоставио везу.

SSL аутентикација клијента

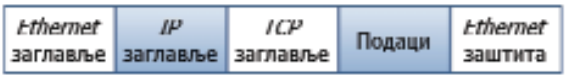
Приликом успостављања SSL везе са клијентом сервер може од клијента захтевати да



Шема 4. Структура IP пакета података за пренос путем Ethernet мрежа

докаже своју аутентичност. Ако корисник прими захтев за доказивањем аутентичности, он серверу шаље свој дигитални сертификат и одређену количину података које дигитално потписује. Примљене дигитално потписане податке сервер користи за проверу јавног кључа у дигиталном сертификату клијента и аутентичности идентитета коју представља сертификат.

За доказивање везе између јавног кључа и идентитета особе или организације коју дати дигитални сертификат представља, односно



Шема 5. Структура IPSec пакета података за пренос преко Ethernet мрежа

за реализацију поступка аутентикације клијента, сервер мора добити потврдан одговор на прва четири питања приказана на шеми 3. Уколико је одговор на неко од наведених питања негативан аутентикација се сматра неуспешном. Последње питање није део SSL протокола и служи као провера да ли дигитални сертификат клијента није повучен из употребе.

ЗАШТИТА НА МРЕЖНОМ НИВОУ – IPSec ПРОТОКОЛ

Већина рачунарских мрежа, укључујући и интернет као глобалну светску мрежу, за комуникацију користи TCP/IP скуп протокола. У основи се ради о две врсте протокола, TCP протоколу, задуженом за пренос података, и IP протоколу, који има основну улогу усмеравања пакета података кроз мрежу од изворишног до одредишног рачунара. Скуп IP протокола показује добра комуникацијска својства у смислу скалабилности, прилагодљивости и отворености према различитим архитектурама рачунара и мрежној опреми, те је због тога широко распрострањен комуникациони протокол. Највећи недостатак IP протокола је што не пружа подршку за очување тајности, аутентичности и интегритета пренесених података. Пренос осетљивих података у IP мрежама по-

требно је осигурати на вишим нивоима комуникације, на транспортном и апликативном нивоу. Пример безбедносног механизма који делује између апликативног и транспортног слоја је поменути SSL протокол. Недостатак таквог приступа је што постоји велики број различитих протокола са апликативног слоја за које је потребно засебно развијати сигурносне *механизме.*

IP Security (IPSec) протокол настао је као резултат иницијативе да се развије јединствени сигурносни механизам за заштићени пренос података у IP мрежама. Развила га је Internet Engineering Task Force (IETF) група и представља проширење основног IP протокола. IPSec протокол је саставни део мрежног слоја.

Физички слој и слој везе података су најнижи слојеви у вишеслојном моделу рачунарских мрежа. Физички слој састоји се од електричних каблова, мрежних картица, радио-предајника и пријемника за бежичну комуникацију, као и од остале опреме потребне за пренос електричних сигнала између два или више рачунара. Слој везе података пружа подршку једноставним протоколима за пренос података на нивоу електричних импулса које користе виши слојеви. Различити делови рачунарске мреже могу за пренос података да користе различите врсте физичких медијума, па је подршка за физички пренос података раз-

Ethernet заглавље	*IP* заглавље	*ESP* (укључује *TCP* заглавља и податке)	*Ethernet* заштита

Шема 6. *Структура IPSec пакета података уз коришћење ESP потпротокола у Ethernet мрежама*

Шема 7. *Структура ESP поља IPSec пакета података*

двојена од остатка мрежне инфраструктуре и обједињена у овом слоју.

Изнад физичког слоја и слоја везе података налази се мрежни слој. Задатак мрежног слоја је прикупљање података о стању мреже од мрежних чворишта и усмеравање пакета података између мрежних чворишта, како би се пренели од изворишног до одредишног рачунара. Мрежни слој користи функционалности физичког слоја и слоја везе података за пренос података, док за усмеравање пакета користи властиту логику. У IP мрежама овај слој се назива IP слој, а усмеравање пакета кроз мрежу обавља се према IP протоколу.

Значајно својство IP мрежа је потпуна хомогеност мрежног, односно IP слоја, док у осталим слојевима постоји одређени степен разноврсности. Апликативни слој пружа подршку за више протокола апликативног нивоа, а физички слој и слој везе података подржавају различите методе физичког преноса података. Истовремено, IP слој користи јединствени IP протокол. Независно од употребљеног протокола апликативног слоја и начина на који је остварена физичка веза између мрежних чворишта, сви подаци који се преносе мрежом морају проћи кроз мрежни слој где се подвргавају IP протоколу. Својство хомогености IP слоја

битно поједностављује увођење јединственог сигурносног механизма у IP мреже. Осигуравањем комуникације на нивоу IP протокола осигурава се целокупна мрежна комуникација. Протокол за осигуравање комуникације у мрежном, односно IP слоју, назива се IPSec протокол.

IPSec протокол задржава компатибилност с постојећим IP протоколом и омогућава мрежној опреми заснованој на IP протоколу транспарентност у односу на IPSec протокол. Само два крајња учесника у комуникацији, пошиљалац и прималац, морају имати подршку за комуникацију IPSec протоколом. Мрежа чворишта и рутера између крајњих учесника, због компатибилности IPSec протокола са IP протоколом, не мора бити опремљена програмском подршком за IPSec протокол. На шеми 4. приказана је структура TCP/IP пакета података за комуникацију преко Ethernet мрежа.

Ethernet заглавље и Ethernet заштиту користе физички слој и слој везе података. За правилан рад мрежног слоја и IP протокола битно је IP заглавље. У IP заглавље су, поред осталог, уписане изворишна и одредишна адреса IP пакета које су потребне за усмеравање пакета кроз мрежу. Остали делови TCP/IP пакета, TCP заглавље и подаци, припадају вишим слојевима и за IP слој они представљају обичне податке које је потребно пренети кроз мрежу. Да би се задржала компатибилност IPSec протокола са IP протоколом потребно је да у структури IPSec пакета података остане очувано IP заглавље. IPSec протокол стога обавља криптографске акције над заглављима и подацима виших слојева. Структура IPSec пакета података за комуникацију у Ethernet мрежама приказана је на шеми 5. Поље са IPSec заглављем и подацима укључује TCP заглавље, као и сва остала заглавља и податке виших слојева у шифрованом облику.

IPSec протокол омогућава стварање структуре сигурне виртуалне приватне мреже (енгл. VPN – Virtual Private Network) изграђене на инфраструктури постојеће јавне IP мреже, односно интернета, у којој нису задовољени захтеви у погледу сигурности комуникације.

За осигуравање тајности, аутентичности, интегритета и непорецивости пренесених података, IPSec протокол користи три потпротокола који заједнички представљају заштиту од свих тренутно познатих сигурносних напада. Потпротоколи се разликују по структури и намени IPSec заглавља и података. Разликују се три врсте IPSec заглавља и података:

– енкапсулирани шифровани подаци,
– заглавље за аутентикацију,
– заглавље за размену кључева.

Шема 8. *Структура IPSec пакета података уз коришћење AH потпротокола у Ethernet мрежи*

Шема 9. *Структура заглавља за аутентикацију AH потпротокола код IPSec пакета података*

IPSec пакет са енкапсулираним шифрованим подацима (енгл. ESP – Encapsulating Security Payload) користи се у случајевима када је битно очувати тајност пренесених података. Уз тајност, ESP поље IPSec пакета чува аутентичност и интегритет података. За стварање ESP поља података користе се симетричне криптографске технике у спрези са методама за проверу аутентичности поруке – HMAC (енгл. HMAC – Hash Message Authentication Code).

Заглавље за аутентикацију (енгл. AH – Authentication Header) користи се за проверу идентитета пошиљалаца података и откривање нарушавања интегритета података током преноса кроз мрежу. Аутентикација је базирана на примени метода за проверу аутентичности поруке. Заглавље за аутентикацију не чува тајност података и користи се само у случајевима када је битна аутентичност и интегритет података, а не и њихова тајност.

Заглавље за размену кључева користи се код потпротокола за размену кључева (енгл. IKE – Internet Key Exchange) као једног од три IPSec потпротокола. IKE је прилагодљив протокол за успостављање метода аутентикације, криптографских алгоритама и дужина кључева,

као и за размену самих кључева између учесника комуникације.

Потпротокол за шифровање података

Потпротокол са енкапсулацијом шифрованих података користи се у случајевима када су подаци који се размењују поверљиве природе и потребно је очувати тајност информација. ESP потпротокол чува тајност података применом симетричних криптографских алгоритама на садржај IP пакета. Замишљен је да подржи било који од симетричних криптографских алгоритама, а за обезбеђивање минималног нивоа заштите између учесника комуникација предложен је стандардни 56-битни DES алгоритам. Основна градивна јединица IPSec пакета у случају употребе ESP потпротокола јесте поље корисних шифрованих података или ESP поље. На шеми 6. приказан је IPSec пакет података за пренос Ethernet мрежама, док је на шеми 7 приказана структура ESP поља.

Грађење IPSec пакета података одвија се поступно, проласком података кроз слојеве мрежне хијерархије, од апликативног према физичком нивоу, у следећим корацима:

1. На заглавља и податке виших апликативних нивоа додаје се TCP заглавље, стварајући тако TCP пакет.

2. Овако настали TCP пакет се енкапсулира у IP пакет.

3. Гради се ESP поље. Целокупни IP пакет (укључујући и заглавље и TCP податке) шифрује се и чини корисне податке у ESP пољу. Корисним подацима додају се потребна ESP заглавља према шеми 7.

4. Испред ESP поља додаје се IP заглавље. Тиме је створен IP пакет података.

5. Испред IP пакета додаје се Ethernet заглавље, а на крај заштитна Ethernet сума (реч је о кодовима за детекцију и корекцију грешке).

Саставни делови ESP поља су индекс безбедносних параметара, редни број пакетаМ, корисни подаци, допуна до пуног блока, величина допуне до пуног блока и ознака протокола који следи након ESP поља. Индекс безбедоносних параметара (енгл. SPI – Security Parameter Index) је 32-битни број којим су одређени криптографски алгоритми, кључеви, трајање кључева и остали безбедоносни параметри коришћени у комуникацији. Прималац ову вредност користи да би за дешифровање података употребио параметре који су коришћени за шифровање. Редни број пакета (енгл. Sequence Number) јесте бројач који се увећава за један приликом сваког слања пакета на исту одредишну адресу, уз коришћење истог индекса безбедоносних параметара. Користи се да би се пакети на одредишту могли правилно поређати, као и за спречавање напада понављањем истих пакета. Корисни подаци (енгл. Payload Data) представљају стварну корисну информацију која се преноси мрежом. Допуна до пуног блока (енгл. Padding) јесте количина 0–255 бајтова података који се додају да би се блок корисних података допунио до вишеструке величине пуног блока коју користи криптографски алгоритам. Величина допуне до пуног блока (енгл. Pad Length) садржи податак о броју бајтова који су додати за допуњавање корисних података до пуног блока. Ознаком протокола који следи након ESP поља (енгл. Next Header) назначава се присуство података за аутентикацију на крају ESP поља. Подаци за аутентикацију нису обавезни део ESP поља и могу се изоставити. Ознака протокола означава да ли су подаци за атентикацију саставни део ESP поља.

Прва два дела у ESP пољу, индекс безбедносних параметара и редни број пакета, кроз мрежу се преносе у отвореном облику, јер су примаоцу потребни пре него што обави дешифровање. Остали делови су шифровани. Након ознаке протокола који следи након ESP поља може се налазити поље са подацима за аутентикацију. Дужина поља за аутентикацију зависи од алгоритама који су коришћени за креирање отиска поруке. У креирању отиска поруке учествују сви претходно наведени делови ESP поља, укључујући индекс безбедносних параметара и редни број пакета. Алгоритми за креирање отиска поруке који се користе за проверу аутентикације података у IPSec протоколу су MD5, SHA-1 и SHA-2.

Потпротокол за аутентикацију

Код примене IPSec протокола за утврђивање аутентичности пошиљалаца података и провере интегритета послатих података, а да притом тајност података није битна, користи се

потпротокол за аутентикацију (енгл. AH – Authentication Header). Потпротокол за аутентикацију може бити примењен као самостални потпротокол IPSec протокола или у спрези са ESP потпротоколом. Самостални AH потпротокол осигурава аутентичност и интегритет пренесених података, док спрега AH и ESP потпротокола осигурава аутентичност, интегритет и тајност пренесених података. Разлика између AH потпротокола и поља података за аутентикацију код ESP потпротокола је у томе што AH потпротокол, осим ESP поља, или TCP пакета, ако се не користи ESP, аутентикује и IP заглавље.

Основна градивна јединица IPSec пакета у случају коришћења AH као самосталног потпротокола је заглавље за аутентикацију. На шеми 8 приказан је IPSec пакет података за пренос Ethernet мрежом кад се као потпротокол користи само AH.

Заглавље за аутентикацију AH потпротокола у IPSec пакету налази се иза IP заглавља, а испред TCP заглавља, или ESP поља ако се користи спрега AH и ESP. На шеми 8 AH дигитално потписује сва поља IPSec пакета осим Ethernet заглавља и заштитне суме. Детаљи структуре заглавља за аутентикацију приказани су на шеми 9.

Саставни делови заглавља за аутентикацију слични су онима код ESP поља. Заглавље за аутентикацију састоји се од дужине заглавља, ознаке протокола који следи након AH потпротокола, резервисаног поља, индекса безбедоносних параметара, редног броја пакета и података за аутентикацију. Дужина заглавља је 8-битни број који садржи дужину података за аутентикацију на крају заглавља. Ознаком протокола који следи након AH потпротокола одређен је протокол који следи након заглавља за аутентикацију. Иза заглавља за аутентикацију може се налазити ESP поље ако се AH користи у спрези с ESP потпротоколом, или TCP заглавље ако се AH користи као самостални потпротокол. Ознака протокола одређује врсту AH потпротокола и протокол који следи након AH заглавља у структури IPSec пакета података. Резервисано поље тренутно није у употреби и увек је испуњено нулама. Предвиђено је за каснија проширења протокола. Индекс безбедоносних параметара SPI користи се, као и код ESP потпротокола, за означавање коришћених криптографских параметара. Редни број пакета такође има исту функцију као и код ESP потпротокола. Увећава се за један са сваким послатим пакетом са истим индексом безбедоносних параметара на исту одредишну адресу. Омогућава правилан поредак пакета на одредишту и спречава напад понављањем истих пакета. Подаци за аутентикацију представљају отисак IP заглавља и података који припадају протоколу који следи након AH потпротокола, ESP или TCP. Да би се увек осигурао минимални ниво међусобног деловања учесника у комуникацији који користе IPSec протокол, предложено је да све верзије AH потпротокола за креирање отиска поруке који се користе за проверу аутентикације података користе MD5, SHA-1 i SHA-2 алгоритме. Међутим, потребно је напоменути да су могући и други алгоритми.

Потпротокол за размену кључева

Потпротоколи AH и ESP користе симетричне криптографске алгоритме за заштиту података. За сврсисходну примену AH и ESP потпротокола потребно је имати сврсисходан начин размене тајних кључева за шифровање података симетричним алгоритмима. Осим тога, пре почетка комуникације AH или ESP потпрото-

колом, две стране које учествују у комуникацији морају договорити и остале безбедоносне параметре: криптографске алгоритме, алгоритме за дигитално потписивање, дужине кључева, учесталост измене кључева и слично. Потпротокол за размену кључева (енгл. *IKE – Internet Key Exchange*) служи за договарање безбедоносних параметара IPSec комуникације и размену симетричних кључева.

За договарање параметара безбедне комуникације, IKE потпротокол уводи концепт безбедносне асоцијације (енгл. Security Association), која обједињује све потребне податке који су учесницима потребни за комуникацију IPSec протоколом. Безбедносном асоцијацијом одређени су врста и начин рада алгоритма за дигитално потписивање података и коришћених кључева, врста и начин рада криптографског алгоритма за шифровање података код ESP потпротокола и коришћених кључева, спровођење или изостављање поступка синхронизације код криптографских алгоритама, као и параметри синхронизације, протокол за утврђивање аутентичности података (AH или ESP), животни век кључева, учесталост промене кључева, животни век безбедносне асоцијације, изворишна адреса безбедносне асоцијације и степен осетљивости преношених података. Безбедносна асоцијација може се сматрати врстом сигурног комуникацијског канала кроз несигурне мрежне путеве између два учесника који комуницирају IPSec протоколом. Својства таквог сигурног канала одређена су параметрима безбедносне асоцијације. Безбедносна асоцијација на тај начин представља разреде сигурних комуникационих канала. Један учесник може, за комуникацију с различитим учесницима, користити различите безбедносне асоцијације, односно сигурне комуникационе канале различитих разреда.

Безбедносна асоцијација је представљена индексом безбедносних параметара SPI. SPI је 32-битни број који једнозначно одређује безбедносну асоцијацију. Пошиљалац података током договарања безбедносних параметара шаље примаоцу SPI који тренутно не користи и који није користио у недавној прошлости. Од тог тренутка, до истека времена важности договорене безбедносне асоцијације, та два учесника за комуникацију договореном безбедносном асоцијацијом увек користе размењени SPI. Учесник који прима податке најпре анализира SPI. Утврђује која је безбедносна асоцијација придружена примљеном SPI и применом безбедносних параметара које одређује безбедносна асоцијација дешифрује примљене податке или верификује дигитални потпис. Задатак IKE потпротокола је да омогући договарање безбедносних параметара, као и њихово повезивање у безбедносну асоцијацију и придруживање SPI безбедносној асоцијацији.

Потпротокол IKE обезбеђује договарање протокола, алгоритама и кључева између учесника у комуникацији, проверава аутентичност учесника који учествују у поступку договарања, омогућава размену података на основу којих ће се генерисати кључеви и управља изменом кључева. Овај потпротокол обавља се у две фазе. У првој фази два учесника успостављају безбедни комуникацијски канал којим ће се обавити договарање безбедоносних параметара и размена кључева. Договарање параметара и размена кључева, односно успостава безбедоносне асоцијације, обавља се у другој фази.

Закључак

Убрзани развој технологије, како у погледу хардвера, тако и у погледу софтвера, умногоме отежавају целокупни систем безбедности и заштите рачунарских мрежа. Подаци и информације које се преносе путем рачунарске мреже сваког дана су све рањивији и неопходно је постојање свеобухватног, одбрамбено оријентисаног, вишеслојно организованог механизма заштите и очувања безбедности рачунарских мрежа.

Литература

[1] Oppliger, R. Internet and Intranet Security, Artech House, 1998.

[2] Rodić, B. Đorđević G., *Da li ste sigurni da ste bezbedni*, Jugoslovenski zavod za produktivnost rada, 2004.

[3] Oppliger, R. Secure Messaging With PGP and S/MIME, Artech House, 2000.

[4] Stallings, W. Cryptography and Network Security Principles and Practices, Fourth Edition, Prentice Hall, 2005.

[5] Oppliger, R. SSL and TLS Theory and Practice, Artech House, 2009.

[6] Rescola, E. SSL and TLS Designing and Building Secure Systems, Addison Wesley, 2008.

[7] Doraswamy, N., Harkins D., IPSec: The New Security Standard for the Internet, Intranets, and Virtual Private Networks, Second Edition, Prentise Hall PTR, 2003.

[8] Frankel, S. Demystufying the IPSec Puzzle, Artech House, 2001.