Ch1

1. *Каков тип на активни напади може да постојат? Објасни ги!
   - Masquerade - напаѓачот се преправа дека е друг корисник и испраќа порака до примачот. Пр. Напаѓачот испраќа порака до Алис, но се преправа, односно изгледа како да ја испратил Боб
   - Модификација на пораки - кога Боб сака да испрати порака до Алис, напаѓачот ја пресретнува пораката, ја подифицира и и ја праќа изменетата на Алис
   - Denial od service - Боб нема пристап до сервисите кои ги нуди серверот бидејќи се вмешува напаѓачот
   - Replay - напаѓачот ги зима пораките од Боб кои се наменети за Алис и отпосле и праќа одговор на Алис.
2. *Каков тип на пасивни напади може да постојат?
   - The release of message contents
   - Traffic analysis
3. *Да се објаснат трите различни површини на напад (network attack surface, software attack surface, human attack sudrface)

   - Network attack surface •
     - This category refers to vulnerabilities over an enterprise network, wide-area network, or the Internet
   - Software attack surface
     - Vulnerabilities in application, utility, or operating system code
   - • Human attack surface
     - Refers to vulnerabilities created by personnel or outsiders, such as social engineering, human error, and trusted insiders
4. Светото тројство:
   - Доверливост на податоците - Уверува дека приватните или доверливите информации не се достапни или откриени на неовластени лица
   - Интегритет на податоците - Уверува дека информациите и програмите се менуваат само на одреден и овластен начин
   - Достапност - Уверува дека системите работат навремено и дека услугата не е одбиена за овластени корисници
5. OSI Security Architecture
   - Безбедносен напад - Секое дејство што ја загрозува безбедноста на информациите во сопственост на организацијата
   - Безбедносен механизам - процес (или уред кој вклучува таков процес) кој е дизајниран да открие, спречи или закрепнува од безбедносен напад
   - Безбедносна услуга - услуга за обработка или комуникација која ја подобрува безбедноста на системите за обработка на податоци и преносот на информации на организацијата

Ch2

2.1 Кои се основните состојки на една симетрична шифра?

- Обичен текст, алгоритам за криптирање, таен клуч, шифриран текст, алгоритам за декриптирање.

2.2 Кои се двете основни функции што се користат во алгоритмите за криптирање?

- Пермутација и замена.

2.3 Колку клучеви се потребни за две лица да комуницираат со помош на симетрична шифра?

- Еден таен клуч.

2.4 Која е разликата помеѓу блок шифра и шифрирање на поток (stream cipher)?

- Шифрирањето на проток шифрира дигитален поток на податоци еден бит или еден бајт во
исто време. Шифрирањето со блок е начин во кој блок на едноставен текст се третира како
целина и се користи за производство на шифрирани текстови со еднаква должина.

*Да се објасни како функционира шифрирање на поток (stream cipher), прикажано на сликата? Кој е најпознат алгоритам за шифрирање на поток?

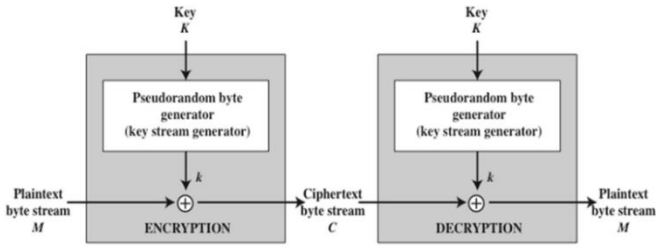


Figure 2.7 Stream Cipher Diagram

Шифрирањето на проток шифрира дигитален поток на податоци еден бит или еден бајт во исто време.

На сликата, на псевдорандом бит генератор на влез му се дава клуч и се произведува стрим од 8-битни броеви кои што се рандом. Излезот од генераторот се прави XOR со plaintext, бит по бит. На излез се добива крипто-текст, на кој потоа му се прави декрипција со истата псевдорандом секвенца.

Најпознат алгоритам е RC4

2.5 Кои се двата општи пристапа за напад врз шифра?

- Криптоанализа и брутална сила (brute force).

2.6 Зошто некои режими на работа на блок-шифри користат само криптирање, додека други
користат и криптирање и декриптирање?

- Во некои режими, обичниот текст не поминува низ функцијата за криптирање, но се прави
XOR операција со излезот на функцијата за криптирање. Математиката открива дека за декриптирање во овие случаи, функцијата за криптирање исто така мора да се користи.

*2.7 Што е тројно криптирање и како функционира? Објаснете зошто е подобро од единечното.

- Со тројно криптирање, обичен блок е шифриран со тоа што тој поминува преку алгоритам за криптирање; резултатот потоа се пренесува повторно преку истиот алгоритам за криптирање; резултатот од второто криптирање поминува низ истиот алгоритам за криптирање трет пат, Каде за секоја егзекуција се користат три клуча. Обично, втората фаза го користи алгоритмот за декриптирање отколку алгоритмот за криптирање.
C=E(K 3 , D(K 2 , E(K 1 , P))) — P - порака, E(K,X) - енкрипција на X со клуч K, Ki - клуч, C - криптиран текст, D – декрипција

2.8 Зошто средниот дел на 3DES е декриптирање наместо криптирање?
- Нема криптографско значење за употребата на декриптирање за
втората фаза. Единствената предност е тоа што им овозможува на корисниците на 3DES да
ги декриптираат податоците шифрирани од корисниците на постариот DES со повторување
на клучот.

Ch3

Message authentication is a procedure that allows
communicating parties to verify that received messages are
authentic
3.1 Наведете три пристапи за автентикација на пораките.
- Шифрирање на пораки, код за автентикација на пораки, hash функција .
3.2 Што е код за автентикација на пораката?
- Автентикатор кој е криптографска функција и на податоците што треба да бидат автентицирани и на тајниот клуч.

*Да се објасни сликата во која е претставена автентикација на пораки со MAC код?

Со помош на MAC, се уверува приемникот дека пораката не е изменета, дека е од соодветниот испраќач и ако пораката вклучува низа од броеви, дека е правилната. Тоа се прави така што со употреба на таен клуч се генерира MAC код, кој се додава на пораката. Тоа се прави со помош на таен клуч кој го споделуваат, на пр А и В, клучот К АВ. Кога А испраќа порака до В, MAC се пресметува како функција од пораката и клучот F(K AB, M). Пораката и кодот се пренесуваат заедно до примачот. Примачот ја врши истата пресметка за да го добие нов

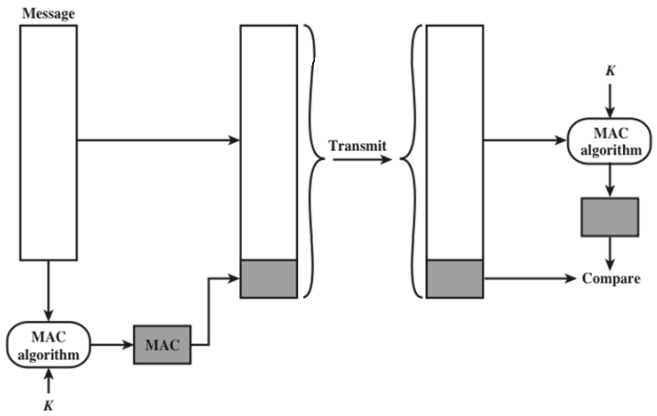


Figure 3.1 Message Authentication Using a Message Authentication Code (MAC)

MAC код со помош на истиот таен клуч. Применият MAC се споредува со пресметаниот MAC, за да се потврди автентичноста.

3.3 Накратко опишете ги трите шеми прикажани на слика 3.2.

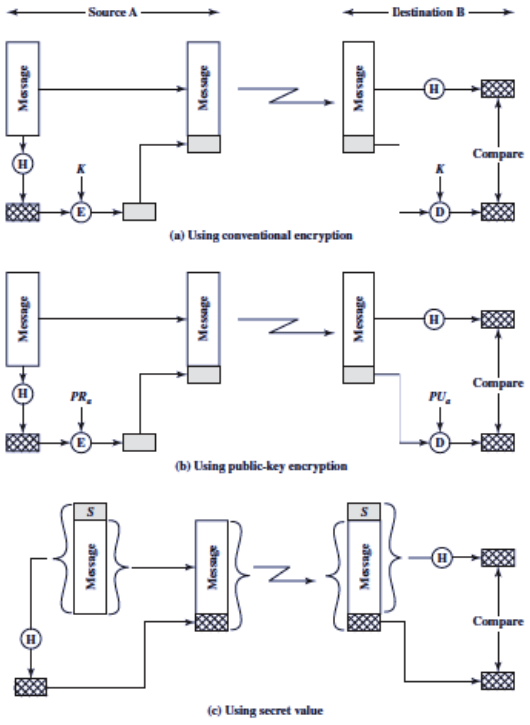


Figure 3.2 Message Authentication Using a One-Way Hash Function

(а) Hash кодот се пресметува од изворната порака,шифрирана со употреба на симетрично криптирање и таен клуч и се прилепува на пораката. Кај примачот се пресметува истиот hash
код. Влезниот код е декриптирани со користење на истиот клуч и спореден со пресметаниот hash
код.
(б) Ова е иста постапка како во (а), освен што тука
се користи криптирање со јавен клуч; испраќачот
го криптира hash кодот со неговиот
приватен клуч и приемникот го декриптира хаш-кодот со јавен клуч на испраќачот.
(в) Тајна вредност се додава на пораката, а потоа а
hash кодот се пресметува со употреба на пораката
плус тајната вредност како влез.
Тогаш пораката (без тајната вредност) и hash-

кодот се пренесени. Примачот додава иста тајна вредност на порака и ја пресметува hash вредноста над пораката плус тајна вредност. Ова потоа се споредува со применият hash-код.

3.4 Кои својства мора да ги имаат hash функциите да бидат корисни за автентикација на пораката?

1. H може да се примени на блок на податоци со која било големина.
2. H произведува излез со фиксна должина.
3. H (x) е релативно лесно да се пресмета за дадено x, со што и двете имплементации на хардвер и софтвер се практични.
4. За која било дадена вредност h, пресметковно е неостварливо да се најде x таков каде H (x) = h. Ова понекогаш се споменува во литературата како еднонасочно својство.
5. За кој било даден блок x, пресметковно е немерливо да се најде y ≠ x каде H (y) = H (x).
6. Пресметковно е неизводливо да се најде кој било пар (x, y) така што H (x) = H (y).

3.5 Во контекст на hash функција, која е функцијата за компресија?

-Функцијата за компресија е основен модул, или основниот градбен блок, на hash функција.

Функцијата hash се состои од повторувана примена на функцијата за компресија.

There are two approaches to attacking a secure hash function:

1.Cryptanalysis - Involves exploiting logical weaknesses in the algorithm

2.Brute force attack - The strength of a hash function against this attack depends solely on the length of the hash code produced by the algorithm

3.6 Кои се главните состојки на криптосистемот со јавен клуч?

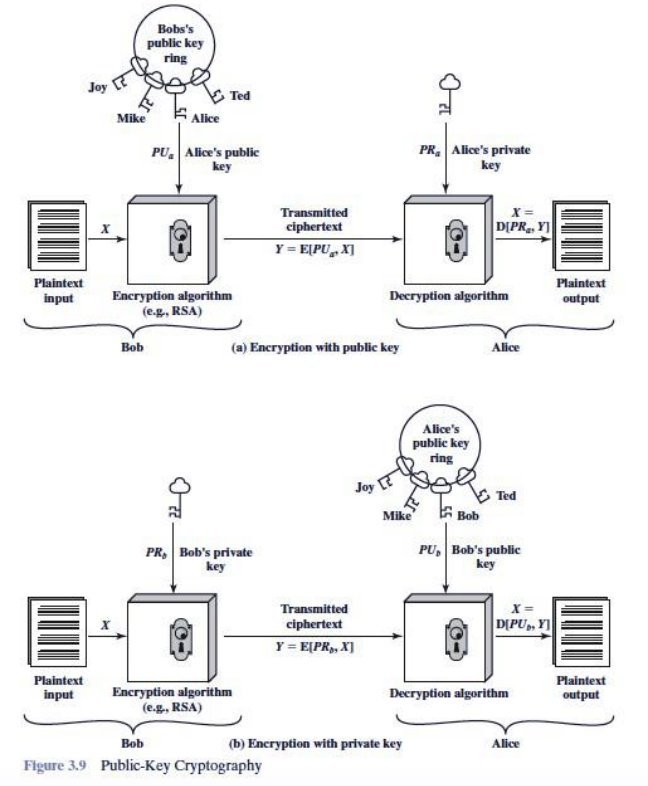


Figure 3.9 Public-Key Cryptography

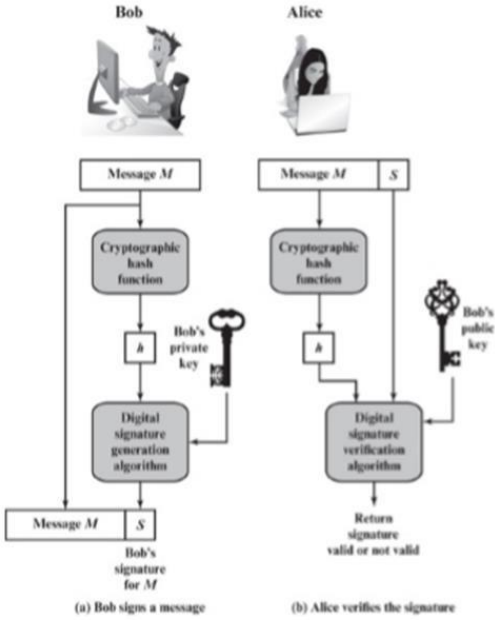
- Plaintext: Ова е читлива порака или податоци што се внесуваат во алгоритмот како влез.
-Алгоритам за криптирање: Алгоритмот за криптирање извршува разни трансформации на едноставен текст (plaintext).
-Јавни и приватни клучеви: Ова е пар клучеви кои се избрани така што ако едниот се користи за криптирање, другиот се користи за декриптирање. Трансформациите извршени од алгоритмот за криптирање зависат од јавниот или приватниот клуч што е даден како влез.
-Криптиран текст (ciphertext): Ова е измешана порака произведена како излез. Таа зависи од обичниот текст и клучот. За дадена порака, два различни клучеви ќе произведат две различни шифрирања.
-Алгоритам за декрипција: Овој алгоритам прифаќа ciphertext и клуч кој што се совпаѓа и се произведува оригиналниот јасен текст (plaintext).

3.7 Наведете и накратко дефинирајте три употреби на криптосистемот со јавен клуч.
-Енкрипција / декрипција: Испраќачот шифрира порака со јавниот клуч на примателот.
-Дигитален потпис: Испраќачот „потпишува“ порака со неговиот приватен клуч. Потпишувањето се постигнува со криптографски алгоритам применет на пораката или на мал блок на податоци што е функција од пораката.
-Размена на клучеви: Двете страни соработуваат за размена на клуч за сесија. Можни се неколку различни пристапи, вклучувајќи ги приватен клуч (еви) на едната или двете страни.

3.8 Која е разликата помеѓу приватен клуч и таен клуч?
- Клучот што се користи при конвенционалното шифрирање обично се нарекува таен клуч.
Двата клучеви што се користат за криптирање со јавен клуч се наведени како јавен клуч и приватен клуч.

*3.9 Што е дигитален потпис? Објасни ја сликата

- Дигитален потпис е механизам за автентикација што овозможува сопственикот на пораката да закачи код што делува како потпис. Потписот се формира со земање на hash пораката и криптирање на истата со приватниот клуч на сопственикот. Потписот го гарантира изворот и интегритетот на пораката.



- Бог сака да испрати порака до Алис, и да го остави својот потпис за Алис да знае дека пораката е испратена од него. Прво Боб генерира хеш вредност, користејќи ја хеш функцијата и пораката која сака да ја испрати. Потоа, со помош на својот приватен клуч и хеш вредноста, прави енкрипција, со што се добива дигиталниот потпис. Потоа, на приемнтата страна, кај Алис, таа на пораката ја употребува истата хеш функција на пораката и добива хеш вредност, а исто така прави декрипција на потписот со приватниот клуч на Боб, и се добива друга хеш вредност. Тие хеш вредност се споредуваат и ако се исти, тогаш Алис со сигурност знае дека Боб ја испратил пораката.

*Што е man-in-the-middle напад? Објаснете ја сликата на која е прикажан ваков напад!

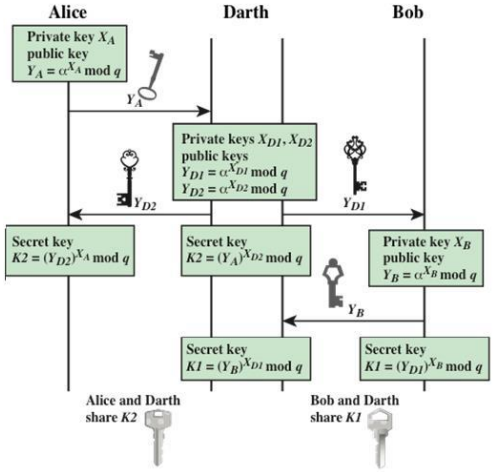


Fig. 3.14 Man-in-the-Middle Attack

Да претпоставиме дека Алис и Боб сакаат да разменат клучеви, а Darth е натрапникот. 1. Darth се спрема за напад така што генерира два рандом приватни клучеви X D2 X D1, а од нив ги добива клучевите Y D2 и Y D1. 2. Алис го праќа клучот Y A до Боб. 3. Darth го пресретнува клучот и го испраќа Y D1 на Боб, во меѓубреме го пресметува K2=(Y A) X D2 mod q. 4. Боб го добива клучот Y D1 и го калкулира K1=(Y D1) X B mod q. 5. Боб го праќа Y B на Алис. 6. Darth го пресретнува и го испраќа Y D2 на Алис. Дарт го калкулира K1= (Y B) X D1 mod q. 7. Алис го добива Y D2 и калкулира K2=(Y D2) X A mod q.
Вака Боб и Алис мислат дека делат таен клуч, но всушност Боб и Дарт делат таен клуч K1 и Алис и Дарт делат таен клуч K2

RSA -

RC4 -

Ch4

4.1 Наведете начини на кои можат да се дистрибуираат тајните клучеви на две страни што комуницираат.

To provide keys for link encryption, option 1,2,3 are used
To provide keys for end to end encryption (over a network), option 4 is preferable

- За две страни А и Б, дистрибуцијата на клучеви може да се постигне на повеќе начини:
1. А може да избере клуч и физички да го достави до Б.
2. Трето лице може да го избере клучот и физички да го достави до А и Б.
3. Ако А и Б претходно и неодамна користеле клуч, една страна може пренесе новиот клуч на другиот, шифриран со употреба на стариот клуч.
4. Ако А и Б имаат шифрирани врски со трето лице Ц, Ц може да достави клуч на шифрираните врски до А и Б

-за четвртата опција се користат два типови на кличеви :
-sesion key;
-permanent key

4.2 Која е разликата помеѓу клучот за сесии и мастер клучот?

- Сесиски клуч е привремен клуч за шифрирање што се користи помеѓу две странки за време на траењето на ниваната логичка конекција која претходно треба да биде воспоставена.

Master клуч е долготраен клуч што се користи помеѓу центар за дистрибуција на клучеви и странка за кодирање на преносот на сесиски клучеви. Обично, мастер клучевите се дистрибуираат на некриптографски начин.

4.3 Што е центар за дистрибуција на клучеви? нз

- Центар за дистрибуција на клучеви е систем кој е овластен да пренесува привремени клучеви за сесија на странките. Секој клуч за сесија се пренесува во шифрирана форма, со користење на master клуч кој дистрибутивниот центар на клучеви го споделува со главната странка.

1. When host A wishes to set up a connection to host B, it transmits a connection request packet to the KDC.
The communication between A and the KDC is encrypted using a master key shared only by A and the KDC.
2. If the KDC approves the connection request, it generates a unique one time session key.
It encrypts the session key using the permanent key it shares with A and delivers the encrypted session key to A.
Similarly , it encrypts the session key using the permanent key it shares with B and delivers the encrypted session key to B.
3. A and B can now set up a logical connection and exchange

messages and data, all encrypted using the temporary
session key.

*Да се објасни како се врши дистрибуција на клучеви наменети за криптирање на крај-крај мрежна конекција помеѓу хост А и Б, доколку тие имаат криптирана конекција со трет уред С!
С може да им достави клуч на енкриптираните линкови А и Б, при што се користат два типа на клучеви: сесиски (кога два система сакаат да комуницираат, тие креираат логичка конекција-сесија и притоа целите податоци се енкриптираат со тој клуч во текот на таа сесија, при завршување на сесијата се уништува клучот) и траен (клуч кој се користи да дистрибуција на сесиски клучеви). Исто така, потребен е и дистибутивен центар (KDC) кој одлучува кои системи смеат да комуницираат помеѓу себе. Кога два система имаат дозвола за конекција, KDC им дава сесиски клуч за таа конекција.

4.4 Кои ентитети се дел од целосната Керберос околина?
- Целосна Керберос околина се состои од Керберос сервер, број на клиенти и голем број апликациски сервери.

. The Kerberos server must have the user ID and hashed
passwords of all participating users in its database. All users
are registered with the Kerberos server
2. The Kerberos server must share a secret key with each
server. All servers are registered with the Kerberos server.

4.5 Во контекст на Керберос, што е царство (realm)? нз
- Царство е околина во која:
1. Керберос серверот мора да го има идентификаторот на корисникот (UID) и хешираните лозинки на сите учесници во неговата база на податоци. Сите корисници се регистрирани на серверот Керберос.
2. Серверот Керберос мора да споделува таен клуч со секој сервер. Сите сервери се регистрирани на серверот Керберос.
4.6 Кои се главните разлики помеѓу верзијата 4 и верзијата 5 на Керберос?
- Верзијата 5 надминува некои недостатоци во околината и некои технички недостатоци во верзија 4.
4.7 Што е nonce?
- Nonce е вредност што се користи само еднаш, како што е временска ознака (timestamp), а
бројач или случаен број; минималниот услов е да се разликува со секоја трансакција.
4.8 Кои се две различни намени на криптографијата со јавен клуч поврзани со дистрибуцијата на клучеви?
- 1. Дистрибуцијата на јавни клучеви.
2. Употреба на public-key криптирање за дистрибуција на тајни клучеви

4.9 Кои се основните состојки на директориумите со јавен клуч? нз

- 1. Авторитетот чува директориум со записи {име, јавен клуч} за секој учесник.
2. Секој учесник регистрира јавен клуч со овластување на авторитетот. Регистрацијата треба да биде лична или со некоја форма на сигурна потврдена комуникација.
3. Учесникот може да го замени постојниот клуч со нов во секое време, поради негова лична желба да се замени јавниот клуч кој веќе се користи во голема мерка податоци, или затоа што соодветниот приватен клуч е компромитиран на некој начин.
4. Периодично, авторитетот го објавува целиот директориум или ажурирања на директориумот. На пример, може да се објави верзија слична на телефонски именик или надградбите би можеле да бидат наведени во широко распространетите медиуми.
5. Учесниците можат да имаат пристап до директориумот по електронски пат. За таа цел, безбедна автентицирана комуникација од авторитетот до учесникот е задолжителна.

*4.10 Што е public-key сертификат,што се содржи во него и на кој начин се објавуваат сертификати за јавни клучеви?
- Сертификатот за јавен клуч содржи јавен клуч и User ID ос сопственикот на клучот, е креиран од овластен орган за сертификати и се дава на учесникот со соодветниот приватен клуч. Учесникот ги пренесува своите клучни информации до друг со пренесување на својот сертификат. Притоа, другите учесници можат да потврдат дека сертификатот е создаден од надлежен орган.

4.11 Кои се барањата за употреба на шема на public-key сертификати?
-1. Секој учесник може да прочита сертификат за да го утврди името и јавниот клуч на сопственикот на сертификатот.
2. Секој учесник може да го потврди дека сертификатот потекнува од овластувањето за сертификати и не е фалсификуван.
3. Само органот за сертификати може да креира и ажурира сертификати.
4. Секој учесник може да ја потврди валутата на сертификатот.

4.12 Која е целта на стандардот X.509? нз
- X.509 дефинира framework за давање услуги за автентикација од страна на директориумот X.500 на своите корисници. Директориумот може да послужи како складиште на сертификати од јавен клуч. Секој сертификат го содржи јавниот клуч на корисникот и е потпишан со приватниот клуч на доверлив орган за сертификати.

4.13 Што е ланец од сертификати? нз
- Синџирот на сертификати се состои од низа сертификати создадени од различни органи за овластување (CA) во кои секоја последователниот сертификат е сертификат од еден CA што го потврдува јавниот клуч на следниот CA во ланецот.

4.14 Како се одзема сертификатот X.509?
- Сопственикот на јавниот клуч може да издаде список за поништување на сертификати кој
одзема еден или повеќе сертификати.

A certificate policy is a named set of rules that indicates the applicability of a certificate to a particular community and/or class of application with common security requirements

*Што значи отповикување на сертификати за јавни клучеви и во кој случај се прави тоа?

Секој сертификат има период на валидност, и нов сертификат се креира пред да истече стариот сертификат. Но, може да се отповика сертификатот кога:

1. Приватниот клуч на корисникот се смета за компромитиран
2. Кога корисникот веќе не е сертифициран од тој CA, на пр ако се промени името на субјектот
3. Кога се смета дека CA сертификатот е компромитиран

ch5

*5.1 Дајте кратка дефиниција за контрола на пристап до мрежата.

• Термин за управување со пристап до мрежа; врши автентикација на корисниците кои се најавуваат во мрежата и одредува до кои податоци можат да пристапат и активности што можат да ги извршат

• Исто така, го испитува и здравјето на компјутерот или мобилниот уред на корисникот

NAC системите се занимаваат со три категории на компоненти:

- Барател за пристап (Access Requester - AR)
  - Јазол што се обидува да пристапи до мрежата и може да биде кој било уред со кој управува NAC системот, вклучувајќи работни станици, сервери, печатари, фотоапарати и други уреди со можност за IP (исто така се нарекуваат барателиили клиенти)
- Сервер за полиси (Policy server)
  - • Одредува каков пристап треба да се даде
  - • Често се потпира на позадинските системи, антивирусни програми, управување со верзии или директориуми, за да се утврди состојбата на домаќинот.
- *Сервер за мрежен пристап (Network Access Server - NAS)
  - • Функционира како точка за контрола на пристап за корисниците на оддалечени локации што се поврзуваат со внатрешната мрежа на претпријатието/фирмата • Може да има свои сервиси за автентикација

или да се потпира на посебна услуга за автентикација од серверот за полиси

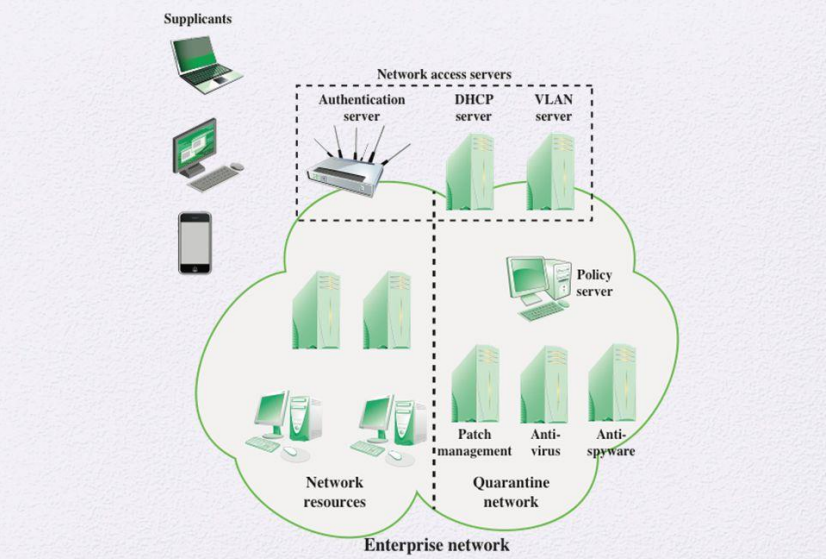


Figure 16.1 Network Access Control Context

1. Различни клиенти (AR) бараат пристап до мрежа на претпријатија со примена на некој вид NAS. Првиот чекор е генерално да се автентицира AR.
   • Автентикацијата може да ја изврши NAS, или NAS може да посредува во постапката за автентикација (преку сервер за полиси).
   • Го верификува идентитетот на подносителот на барањето кој што потврдува дека е негово
2. Серверот за полиси или серверот за поддршка вршат проверки на AR за да утврдат дали треба да му се дозволи интерактивна конекција за далечински пристап.
   • Овие проверки - понекогаш наречени здравствени, бараат од софтверот на системот на корисникот да потврди усогласеност со одредени барања од основната конфигурација на организацијата
   • На пример, antimalware софтверот на корисникот мора да биде ажуриран, оперативниот систем мора да биде целосно заштитен (patched), а оддалечениот компјутер мора да биде во сопственост и контролиран од организацијата.
   • Врз основа на резултатите од овие проверки, организацијата може да утврди дали на далечинскиот компјутер треба да му биде дозволено да користи интерактивен далечински пристап.
   • Ако корисникот има прифатливи овластувања за овластување, но оддалечениот компјутер не ја помине здравствената проверка, на корисникот и на далечинскиот компјутер треба да му биде одземен мрежен пристап или да има ограничен пристап до т.н. карантинска мрежа за да може овластениот персонал да ги отстрани безбедносните недостатоци.

3. Откако AR е автентициран и има одредено ниво на пристап до мрежата на претпријатието, NAS може да му овозможи на AR да комуницира со ресурсите во мрежата на претпријатието. • NAS може да посредува во секоја размена за спроведување на безбедносна политика за овој AR, или може да користи други методи за ограничување на привилегиите на AR.

5.2 Што е EAP (Extensible Authentication Protocol)? • EAP обезбедува услуга за транспорт за размена на информации за автентикација помеѓу систем на клиенти и сервер за автентикација • Основната услуга за транспорт на EAP е проширена со употреба на специфичен протокол за автентикација, инсталиран и во EAP клиентот и во серверот за автентикација

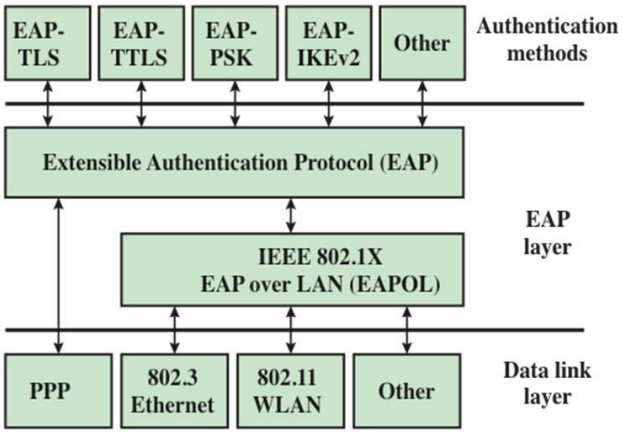


Figure 5.2 EAP Layered Context

Three layers of the
EAP layered context are summarized in Fig. 5.2.

1. Authentication methods are illustrated at the top, including EAP TLS , EAP TTLS , EAP PSK ,EAP IKEv2 , and other.
2. The EAP layer below has communication from Extensible Authentication Protocol (EAP) with each method above, and with IEEE 802.1 X EAP over LAN EAPOL).
3. The data link layer includes PPP , communicating with EAP above, and 802.3 Ethernet, 802.11 WLAN , and other, each communicating with EAPOL above.

5.3 Наведете ги и накратко дефинирајте четири методи за автентикација на EAP.
•EAP Transport Layer Security -EAP-TLS (RFC 5216) дефинира како TLS протоколот (опишан во Поглавје 6) може да се вклучи во EAP пораките.
•EAP Tunneled TLS - Слично на EAP-TLS, освен тоа што само серверот има сертификат со кој најпрвин се автентицира на клиентот. Серверот потоа може да ја користи воспоставената безбедна врска („тунел“) за да се автентицира клиентот. •EAP Generalized Pre-Shared Key -EAP-GPSK, дефиниран во RFC 5433, е EAP метод за взаемна автентикација и правење на сесиски клуч со употреба на претходно споделен клуч (PSK).
•EAP-IKEv2 -Дефинирана во RFC 5106; заснована на Internet Key Exchange protocol version 2 (IKEv2); Поддржува взаемна автентикација и воспоставување сесии со клучеви со користење на различни методи.

5.4 Што е EAPOL?Да се објасни слиаката!5.5 Основниот елемент дефиниран во 802.1X е протокол познат како EAPOL (EAP преку LAN). • EAPOL работи во мрежните слоеви и користи на IEEE 802 LAN, како што е Етернет или Wi-Fi, на link ниво. • EAPOL му овозможува на клиентот да комуницира со автентикатор и ја поддржува размената на EAP пакетите за автентикација. • Кога подносителот на барањето најпрво ќе се поврзе со LAN, не ја знае MAC адресата на автентикаторот. Со испраќање на пакетот EAPOL-Start на специјална адреса за групен мултикаст резервирана за IEEE 802.1X автентикатори, подносителот на барањето може да утврди дали е постои таков автентикатор и да му каже на истиот дека барателот е подготвен. • Во многу случаи, автентикаторот веќе ќе биде известен дека новиот уред е поврзан од известување за хардвер. На пример, hub ќе знае дека кабелот е вклучен пред уредот да испрати какви било податоци. Во овој случај, автентикаторот може да ја активира пораката за започнување со своја порака. • И во двата случаи, автентикаторот испраќа порака за EAP Request Identity, енкапсулирана во пакетот EAPOL-EAP. • EAPOL EAP е тип EAPOL рамка што се користи за транспорт на EAP пакети. • Автентикаторот го користи пакетот EAP-Key за да испрати криптографски клучеви до барателот откако ќе одлучи да го прифати во мрежата. • Типот на пакет EAP-Logoff означува дека подносителот на барањето сака да биде исклучен од мрежата.

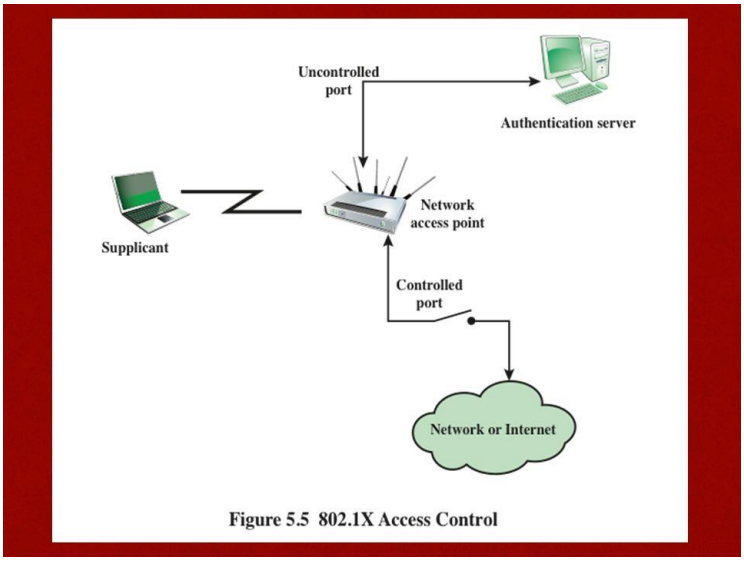


Figure 5.5 802.1X Access Control

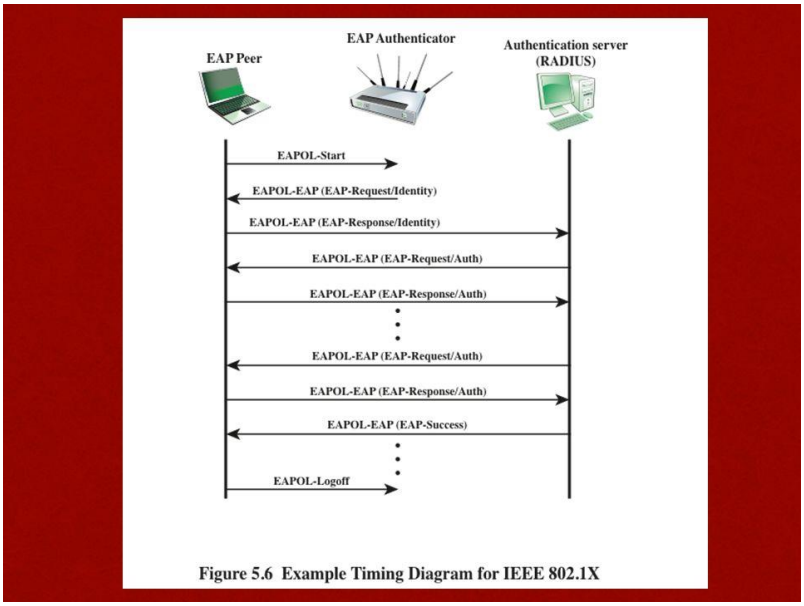


Figure 5.6 Example Timing Diagram for IEEE 802.1X

5.5 Којафункцијата на IEEE 802.1X?

• Контролата на пристап до мрежа врз основа на порти IEEE 802.1X е дизајнирана да обезбеди функции за контрола на пристапот за LAN. • Додека AS не го автентицира подносителот на барањето (со користење на протокол за автентикација), автентикаторот испраќа само пораки за контрола и автентикација помеѓу барателот и AS; Контролниот канал 802.1X е деблокиран, но каналот за податоци 802.11 е блокиран. • Откако барателот ќе биде автентициран и ќе се обезбедат клучеви, автентикаторот може да пренасочува податоци од подносителот на барањето; под овие околности, каналот за податоци е деблокиран.

5.6 Дефинирајте што е пресметување во облак(cloud computing).
Модел за овозможување сеприсутен, удобен мрежен пристап до заедничка група на ресурси што можат да се конфигурираат (на пр. Мрежи, сервери, складирање, апликации и услуги) кои можат брзо да се обезбедат и да се ослободат со минимален напор за управување. Ваквиот облак модел промовира достапност и е составен од пет основни карактеристики, три модели на услуги и четири модели на deployment .

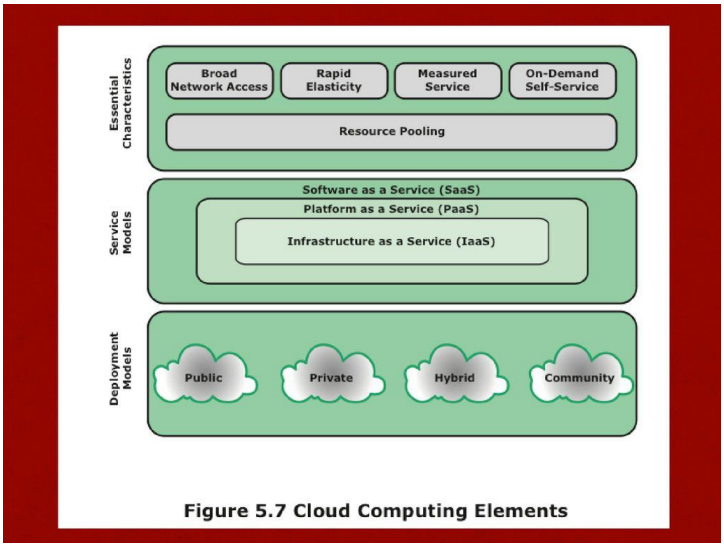


Figure 5.7 Cloud Computing Elements

5.7 Наведете ги и накратко дефинирајте три модели на услуга на облак (service models). (2)

- Софтвер како услуга (Saas): Способноста што му е дадена на потрошувачот е да ги користи апликациите на давателот на услуги кои работат на облачна инфраструктура. Апликациите се достапни од различни уреди со клиенти преку тенок клиентски интерфејс, како што е вебпрелистувач. Наместо да добие лиценца за работна површина и сервер за софтверски производи што ги користи, едно претпријатие ги добива истите функции од услугата cloud. SaaS ја зачувува комплексноста на инсталирање, одржување, надградба и закрпи на софтвер. •
- Платформа како услуга (PaaS): PaaS често обезбедува услуги во стилот на Middleware, како што се база на податоци и услуги за компоненти за употреба од апликации. Всушност, PaaS е оперативен систем во облакот. •

- Инфраструктура како услуга (IaaS): Способноста што му е дадена на потрошувачот е да обезбеди обработка, складирање, мрежи и други основни компјутерски ресурси каде потрошувачот е во состојба да распореди и да управува произволен софтвер, кој може да вклучува оперативни системи и апликации. IaaS им овозможува на клиентите да комбинираат основни компјутерски услуги, како што се складирање на податоци, за да градат високо адаптибилни компјутерски системи.

The essential characteristics of cloud computing (1)
include the following

•
Broad network access: Capabilities are available over the network and accessed through standard mechanisms that promote use by heterogeneous thin or thick client platforms (e.g., mobile phones, laptops, and PDAs)

•
Rapid elasticity: Cloud computing gives you the ability to expand and reduce resources according to your specific service requirement. For example, you may need a large number of server resources for the duration of a specific task. You can then release these resources upon completion of the task

•
Measured service: Cloud systems automatically control and optimize resource use by leveraging a metering capability at some level of abstraction appropriate to the type of service (e.g., storage, processing, bandwidth, and active user accounts). Resource usage can be monitored, controlled, and reported, providing transparency for both the provider and consumer of the utilized service.

•
On demand self service: A consumer can unilaterally provision computing capabilities, such as server time and network storage, as needed automatically without requiring human interaction with each service provider.

•
Resource pooling: The provider’s computing resources are pooled to serve multiple consumers using a multi tenant model, with different physical and virtual resources dynamically assigned and reassigned according to consumer demand

NIST defines four deployment(3)
models:

•
Public cloud: The cloud infrastructure is made available to the general public or a large industry group and is owned by an organization selling cloud services . The cloud provider is responsible both for the cloud infrastructure and for the control of data and operations within the cloud

•
Private cloud: The cloud infrastructure is operated solely for an organization. It may be managed by the organization or a third party and may exist on premise or off premise. The cloud

provider (CP) is responsible only for the infrastructure and not for the control

•

Community cloud: The cloud infrastructure is shared by several organizations and supports a specific community that has shared concerns (e.g., mission , security requirements, policy, and compliance considerations). It may be managed by the organizations or a third party and may exist on premise or off premise.

•

Hybrid cloud: The cloud infrastructure is a composition of two or more clouds (private, community, or public) that remain unique entities but are bound together by standardized or proprietary technology that enables data and application portability (e.g., cloud bursting for load balancing between clouds

5.8 Која е референтната архитектура за компјутерски облак?

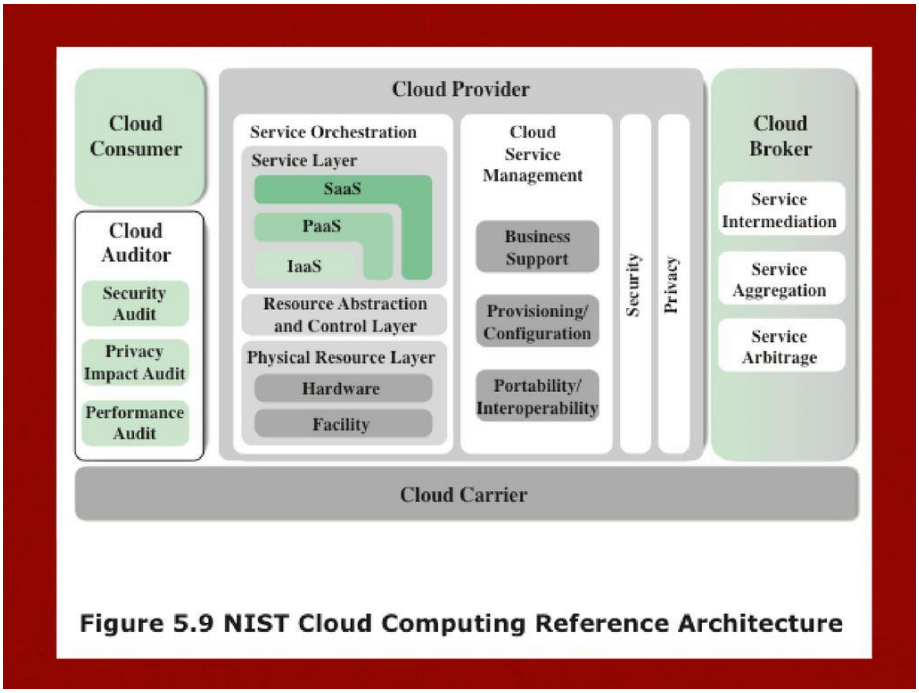


Figure 5.9 NIST Cloud Computing Reference Architecture

Cloud consumer: Едно лице или организација што одржува деловен однос и користи услуги од провајдери на облак.

• Снабдувач на облак (CP): Лице, организација или субјект одговорен за достапноста на услугата за заинтересираните страни

• Cloud auditor: Страна што може да спроведе независна проценка на услугите на облак, работењето на информацискиот систем, перформансите и безбедноста на имплементацијата на облак.

• Cloud broker: Ентитет кој управува со употреба, перформанси и испорака на cloud услуги и преговара за односите помеѓу CP и потрошувачите на облак.

• Носач на облак: посредник кој обезбедува поврзаност и транспорт на услуги од облак од CP до потрошувачи на облак.

Figure 5.8 illustrates the typical cloud service context.

•

An enterprise maintains workstations within an enterprise LAN or set of LANs, which are connected by a router through a network or the Internet to the cloud service provider.

•

The cloud service provider maintains a massive collection of servers, which it manages with a variety of network management, redundancy, and security tools.

•

In the figure, the cloud infrastructure is shown as a collection of blade servers, which is a common architecture.

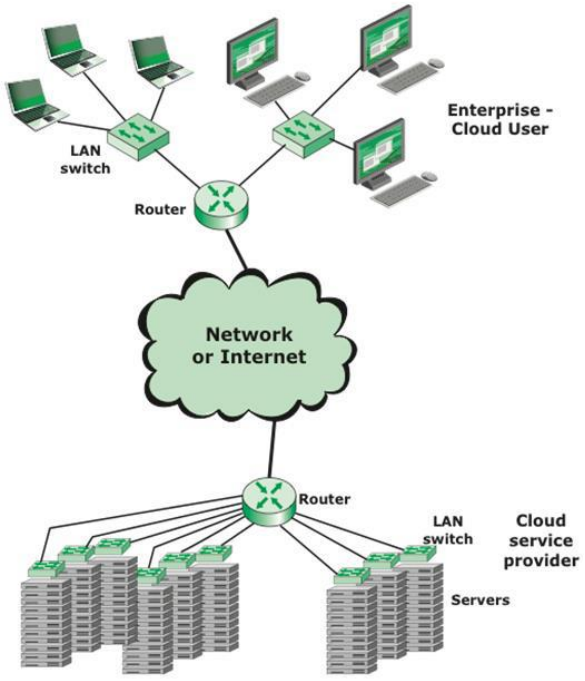


Figure 5.8 Cloud Computing Context

5.9. Опиши ја енкрипцијата на база на податоци во облак

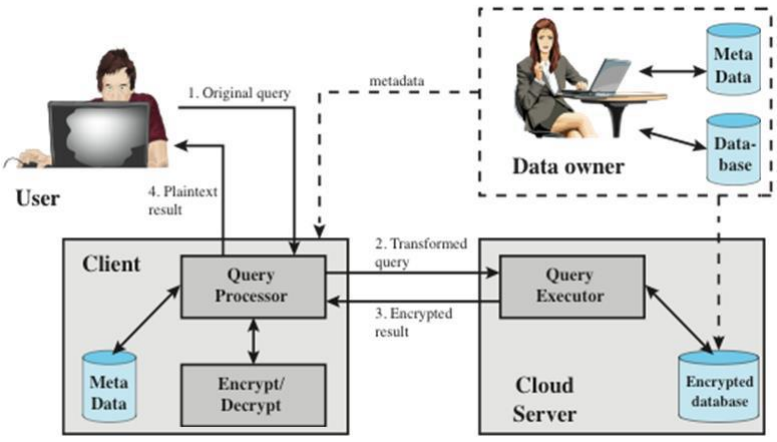


Figure 5.10 An Encryption Scheme for a Cloud-Based Database

1.Оригиналното query, од корисникот до процесорот за пребарување на query на клиентот, кој комуницира со метаподатоци на клиентот и криптирање / декрипција.
2.Трансформирано барање од процесор за пребарување на клиентот до извршител на барањето за облак-сервер, кој комуницира со криптираната база на податоци од облак.

Шифрираната база на податоци вклучува метаподатоци и комуникација со базата на податоци со сопственикот на податоците.
3.Енкриптиран резултат од извршителот на барањето до процесорот за пребарување.
4.Plaintext резултат од пребарувањето до корисник.
Вклучени се четири субјекти:

• Сопственик на податоци: Организација која произведува податоци што ќе бидат достапни за контролиран пристап или во рамките на организацијата или на надворешните корисници.

• Корисник: Човечки субјект што доставува барања (прашања) до системот. Корисникот може да биде вработен во организацијата на која му е овозможен пристап до базата на податоци преку серверот, или корисник надворешен од организацијата на која, по автентикација, му се дозволува пристап.

• Клиент: Frontend што ги трансформира барањата од корисникот во прашања за шифрираните податоци зачувани на серверот.

• Сервер: Организација што ги прима шифрираните податоци од сопственикот на податоците и ги прави достапни за дистрибуција на клиенти. Серверот всушност може да биде во сопственост на сопственикот на податоците, но, обично е објект во сопственост и одржуван од надворешен провајдер. (cloud систем)

Ch6

6.1 Кои се предностите на секој од трите пристапи прикажани на слика 5.1?

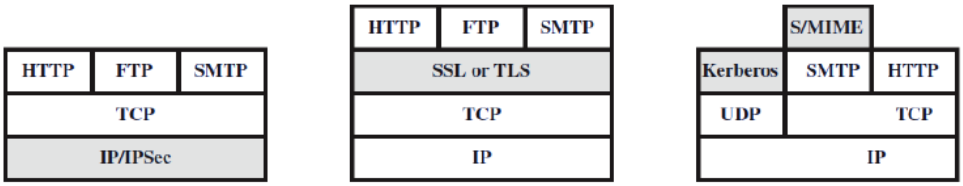


Figure 5.1 Relative Location of Security Facilities in the TCP/IP Protocol Stack

Предност на користењето на IPSec (Слика 5a) е што е транспарентен до крајните корисници и апликации и дава решение за општа намена. Понатаму, IPSec вклучува можност за филтрирање на пакети. Предност на користење SSL е тоа што ги користи механизмите за сигурност и контрола на проток на TCP. Предноста на безбедносните услуги специфични за апликациите (Слика 5c) е дека услугата може да биде прилагодена на специфичните потреби на дадена апликација.

6.2 Кои протоколи се состојат во SSL? (samo da se nabrojat)
Протокол за ракување со SSL(SSL handshake protocol);
Протокол за промена на шифрирање SSL (SSL change cipher spec protocol);
Предупредувачки SSL протокол (SSL alert protocol);
SSL record protocol.

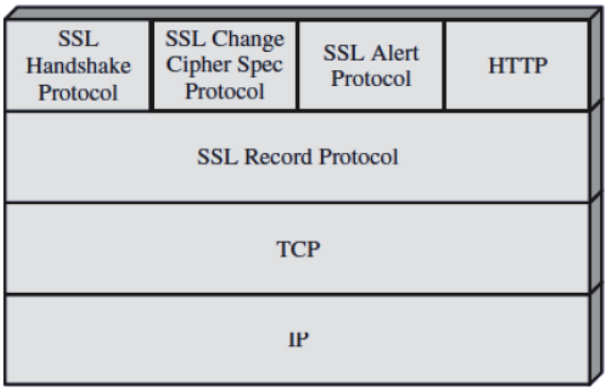


Figure 5.2 SSL Protocol Stack

6.3 Која е разликата помеѓу SSL-врска (connection) и SSL-сесија (session)?
Врска: Врската е транспорт што обезбедува соодветен вид на услуга. За SSL,врските се врски peer-to-peer. Секоја врска е поврзана со една сесија.
Сесија: SSL сесијата е асоцијација помеѓу клиент и сервер.Сесиите се создадени со протоколот за ракување (handshake). Сесиите дефинираат криптографски безбедносни параметри кои можат да бидат споделени меѓу повеќекратни врски. Сесиите се користат за да се избегнат скапите преговори за нови безбедносни параметри за секоја врска.

6.4 Наведете ги и накратко дефинирајте ги параметрите што дефинираат состојба на SSL сесија.
Идентификатор на сесија: произволна низа за бајти избрана од серверот за да се идентификува активна или обновена состојба на сесијата.
Сертификат за peers: X509.v3 сертификат за peers.
Метод на компресија: Алгоритмот кој се користи за компресирање на податоците пред криптирањето.
Шифрирање: Го одредува алгоритмот за шифрирање на податоците (како што се DES, итн.) и hash алгоритмот (како што се MD5 или SHA-1) што се користи за пресметување MAC (Message Authentication Code). Исто така дефинира криптографски атрибути како што е hash_size.
Master тајна: 48-бајтна тајна споделена помеѓу клиентот и серверот.
Is resumable: Знаменце што означува дали може да се користи истата сесија за нови Врски.

6.5 Наведете ги и накратко дефинирајте ги параметрите што дефинираат SSL врска.
Сервер и клиент random: Бајтни секвенци што ги избираат серверот и клиентот за секоја врска.
Server write MAC secret: Таен клуч што се користи во MAC операциите на податоците испратени од серверот.
Client write MAC secret: Тајниот клуч што се користи во MAC операциите на податоците испратени од клиентот.
Клуч за запишување на серверот (Server write key): Конвенционален клуч за

криптирање
за податоци шифрирани од серверот и декриптирани од клиентот.
Клуч за запишување на клиентот (Client write key): Конвенционален клуч за криптирање за податоци шифрирани од клиент и декриптирани од серверот.
Вектори за иницијализација: Кога се користи блок шифра во CBC режим, векторот за иницијализација (IV) се одржува за секој клуч.
Секвентни броеви: Секоја страна одржува посебна секвенца на броеви за пренесени и примени пораки за секоја врска. Кога страната испраќа или прима порака за спецификација на шифрирање, соодветниот секвентен број е поставен на нула. Броевите на секвенци не смеат да надминат 2^64 – 1.

6.6 Кои услуги се обезбедени со протоколот за евиденција за SSL (SSL Record Protocol)?
Доверливост: Протоколот за ракување дефинира споделен таен клуч што се користи за конвенционално криптирање на SSL payloads.
Интегритет на порака: Протоколот за ракување дефинира и заеднички таен клуч што се користи за да се формира код за автентикација на порака (MAC).

6.7 Кои чекори се вклучени во преносот на SSL Record ? (bi trebalo da znam, da go nacrtam)
Фрагментација; компресија; додавање на MAC; шифрирање; додавање SSL заглавје

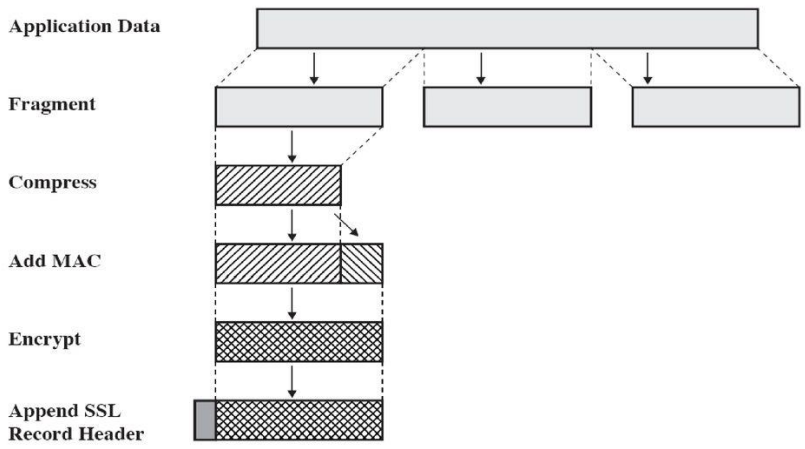
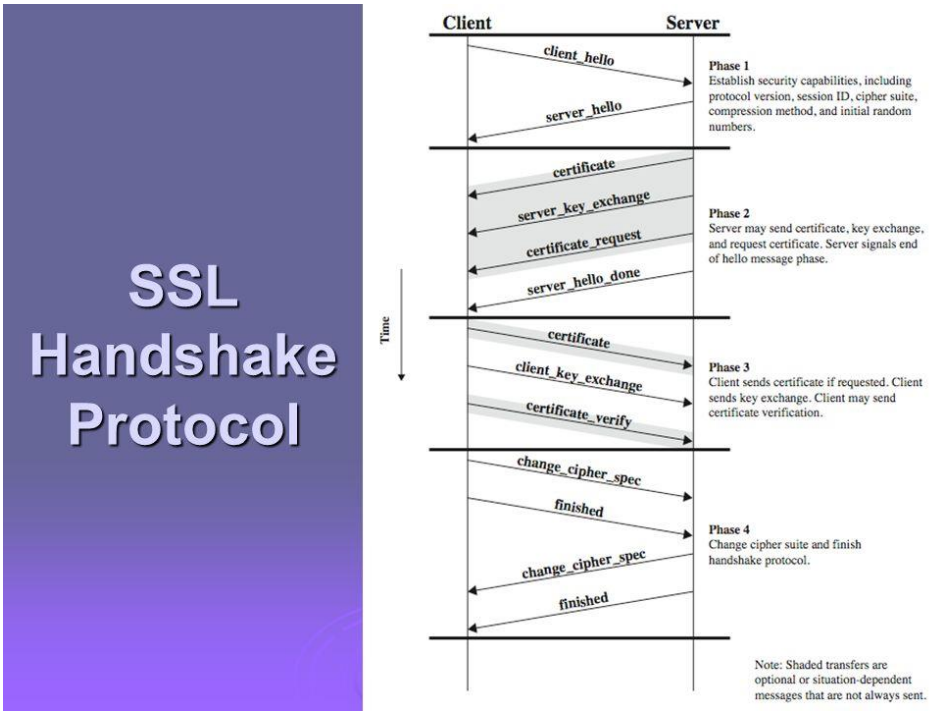


Figure 5.3 SSL Record Protocol Operations



6.8 Која е целта на HTTPS?

HTTPS (HTTP преку SSL) се однесува на комбинацијата на HTTP и SSL на спроведување на безбедна комуникација помеѓу веб-прелистувач и веб сервер. Главната разлика може да ја видиме во Web прелистувачите (https:// наместо http://). Нормална HTTP врска ја користи портата 80, додека HTTPS ја користи портата 443, што го активира SSL.

6.9 За кои апликации е корисен SSH?

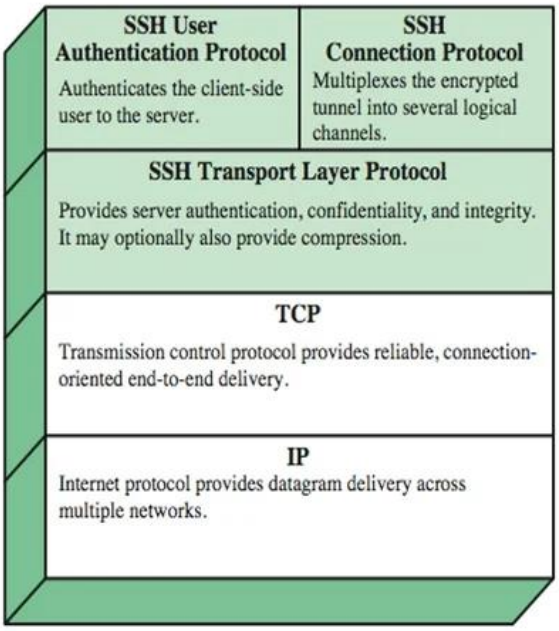
Првичната верзија, SSH1 била фокусирана на обезбедување на безбедно далечинско управување на објекти со цел да ги замени TELNET и другите шеми за далечинска најава кои не биле безбедни. SSH исто така обезбедува поопшти клиент / сервер можности и може да се користи за мрежни функции како пренос на датотеки и е-пошта.

6.10 Наведете ги и накратко дефинирајте ги протоколите на SSH.

Протокол за транспорт на слој: Обезбедува автентикација на податоците на серверот, доверливост на податоци и интегритет на податоци со обезбедена тајност (т.е., ако клучот е компромитиран во текот на една сесија, знаењето на истиот не влијае безбедноста на претходните сесии). Транспортот слој може по избор да обезбеди компресија.

Протокол за автентикација на корисникот: Го автентицира корисникот до серверот.

Протокол за поврзување: Мултиплексира повеќекратни логички комуникациски канали преку една основна SSH врска.



4.2. There are three typical ways to use nonces as challenges. Suppose Na is a nonce generated
by A,A and B share key K, and f() is a function (such as increment).The three usages are

Usage 1	Usage 2	Usage 3
(1) A → B: N_a (2) B → A: E(K, N_a)	(1) A → B: E(K, N_a) (2) B → A: N_a	(1) A → B: E(K, N_a) (2) B → A: E(K, f(N_a))

- All three really serve the same purpose. The difference is in the vulnerability. In Usage 1, an attacker could breach security by inflating Na and withholding an answer from B for future replay attack, a form of suppress-replay attack. The attacker could attempt to predict a plausible reply in Usage 2, but this will not succeed if the nonces are random. In both Usage 1 and 2, the messages work in either direction. That is, if N is sent in either direction, the response is E[K, N]. In Usage 3, the message is encrypted in both directions; the purpose of function f is to assure that messages 1 and 2 are not identical. Thus, Usage 3 is more secure.

4.4 Let us consider the case of the interchange of C_1 and C_2. The argument will be the same for any other adjacent pair of ciphertext blocks. First, if C_1 and C_2 arrive in the proper order:

$$P_1 = E[K, C_1] \oplus IV$$
$$P_2 = E[K, C_2] \oplus C_1 \oplus P_1 = E[K, C_2] \oplus C_1 \oplus E[K, C_1] \oplus IV$$
$$P_3 = E[K, C_3] \oplus C_2 \oplus P_2 = E[K, C_3] \oplus C_2 \oplus E[K, C_2] \oplus C_1 \oplus E[K, C_1] \oplus IV$$

Now suppose that C_1 and C_2 arrive in the reverse order. Let us refer to the decrypted blocks as Q_i.

$$Q_1 = E[K, C_2] \oplus IV$$
$$Q_2 = E[K, C_1] \oplus C_2 \oplus Q_1 = E[K, C_1] \oplus C_2 \oplus E[K, C_2] \oplus IV$$
$$Q_3 = E[K, C_3] \oplus C_1 \oplus Q_2 = E[K, C_3] \oplus C_1 \oplus E[K, C_1] \oplus C_2 \oplus E[K, C_2] \oplus IV$$

The result is that $Q_1 \neq P_1$; $Q_2 \neq P_2$; but $Q_3 = P_3$. Subsequent blocks are clearly unaffected.

ШТО Е OSI СИГУРНОСНАТА АРХИТЕКТУРА?

OSI сигурносната архитектура е framework кој обезбедува систематски начин за дефинирање на барањата за безбедност и карактеризирање на
пристапи кон задоволување на овие барања.
Документот дефинира безбедносни напади, механизми и услуги и врски меѓу
овие категории.
За 2.1
Лесно запамтување: Мемориските зборови се лесни за запамтување и употреба, особено ако се користат зборови кои се познати или лесни за асоцирање.
Отпорност на криптоанализа: Користењето на мемориски зборови како клучеви може да го затрудни процесот на криптоанализа, особено ако се користат зборови кои не се лесно поврзани со историски или културни контексти.
Поедноставување на управувањето со клучеви: Заместо користење на сложени или долги клучеви, мемориските зборови овозможуваат едноставно запамтување и пренос на клучевите.
Иако оваа техника има свои предности, не е секогаш соодветна за сите ситуации. На пример, ако е потребно високо ниво на

безбедност, како во случаи на воена или финансиска комуникација, можеби ќе се предпочита користење на напредни алгоритми за шифрирање со долги и случајно генерирани клучеви.
Osnovno
In active attacks, the intruder attempts to alter system resources or data, disrupt services, or impersonate users to gain unauthorized access to systems or networks.

- Masquerade
- Replay
- Modification of messages
- Denial of Service

Passive attacks are more subtle and involve monitoring and eavesdropping on communication channels or data transmissions without actively altering them.

- The release of message contents
- Traffic analysis