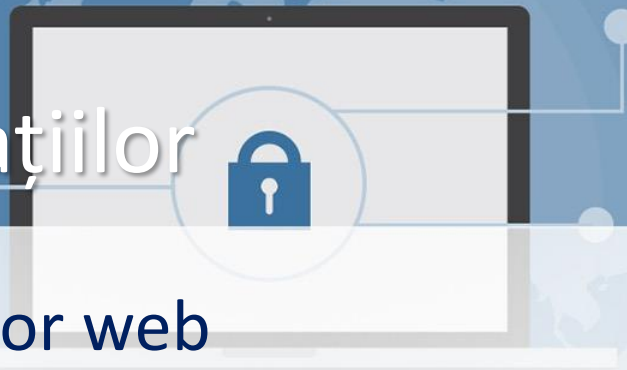
Criptografie și Securitate Cibernetică

RCC - CSC 5

Conținut

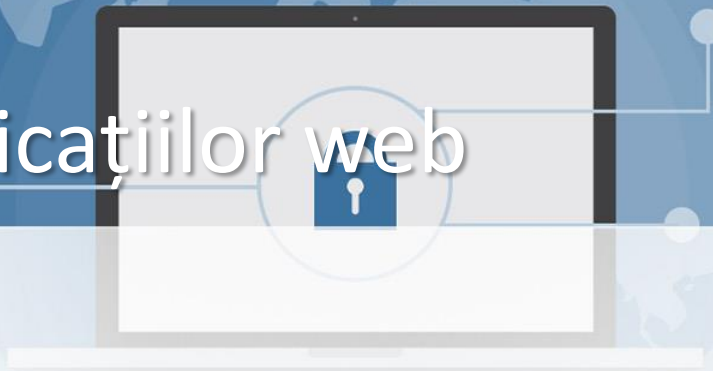
- Securitatea comunicațiilor
  - Securitatea comunicațiilor web
  - Protocoale de securitate
    - SSL TLS HTTPS SSH
- Securitatea rețelelor fără fir
  - Securitatea comunicațiilor wireless
  - Securitatea dispozitivelor mobile
  - Rețele wireless locale - IEEE 802.11
  - Standardul de securitate wireless - 802.11i

Securitatea comunicațiilor



- Securitatea comunicațiilor web
  - Protocoale de securitate
    - SSL
    - TLS
    - HTTPS
    - SSH

Securitatea comunicațiilor web



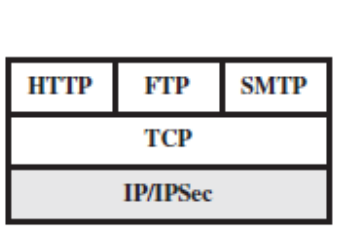
- Amenințări de securitate web
- Securitatea traficului web
- Protocoale de securitate web
  - SSL – Secure Sockets Layer
  - TLS – Transport Layer Security
  - HTTPS – HTTP over SSL
  - SSH – Secure SHell
- Securizarea componentelor (client, server, cod web)
- Compromiterea unui server web permite accesul în rețea
- Utilizatorii, de regulă, nu cunosc riscurile de securitate și nu au instrumente de protecție

Amenințări de securitate

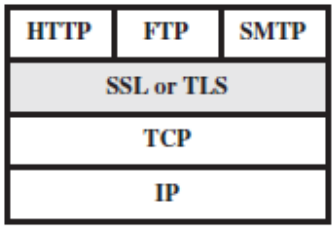
	Threats	Consequences	Countermeasures
Integrity	• Modification of user data • Trojan horse browser • Modification of memory • Modification of message traffic in transit	• Loss of information • Compromise of machine • Vulnerability to all other threats	Cryptographic checksums
Confidentiality	• Eavesdropping on the net • Theft of info from server • Theft of data from client • Info about network configuration • Info about which client talks to server	• Loss of information • Loss of privacy	Encryption, Web proxies
Denial of Service	• Killing of user threads • Flooding machine with bogus requests • Filling up disk or memory • Isolating machine by DNS attacks	• Disruptive • Annoying • Prevent user from getting work done	Difficult to prevent
Authentication	• Impersonation of legitimate users • Data forgery	• Misrepresentation of user • Belief that false information is valid	Cryptographic techniques

Niveluri de securitate

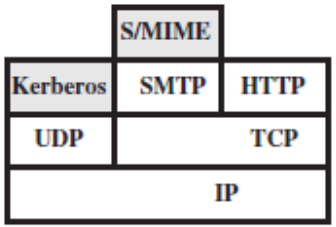
- Elemente de securitate în stiva de protocoale TCP/IP
  - Nivel rețea (IPSec - IP security)
  - Nivel transport (SSL, TLS)
  - Nivel aplicație



(a) Network level

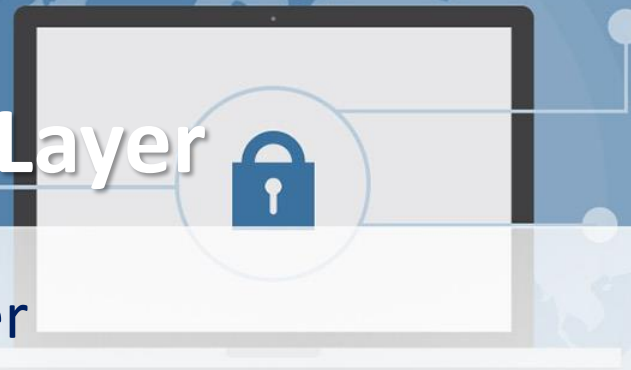


(b) Transport level



(c) Application level

SSL - **Secure Sockets Layer**

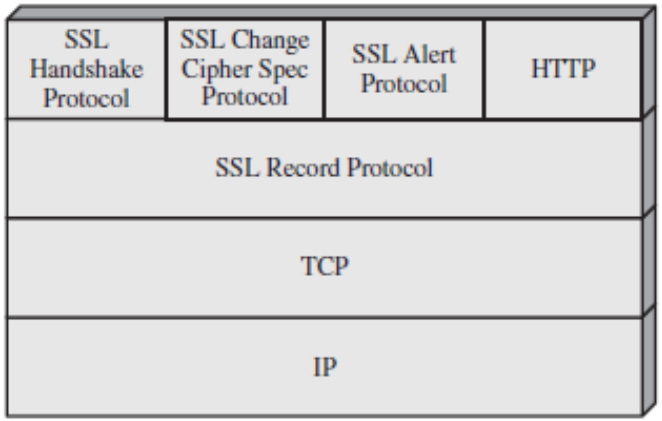


- SSL - Secure Sockets Layer
  - Unul dintre cele mai folosite protocoale de securizare
  - Serviciu de securizare
  - Implementat ca un set de protocoale pentru stiva TCP
    - Transparent (parte a unui protocol inferior din stiva)
    - Embedded (inclus în diferite aplicații – server web, browser)

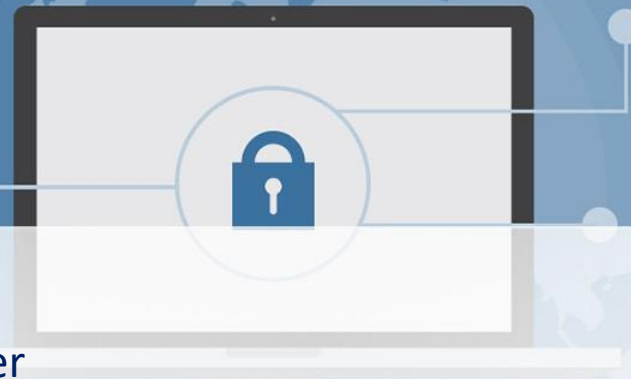
Arhitectura SSL

- Utilizează stiva TCP pentru activarea de servicii securizate
- 2 niveluri de protocoale
  - 1 protocol la nivel de bază
    - *SSL Record Protocol*

    furnizează servicii de securitate la nivelurile superioare
  - 3 protocoale la nivel superior
    - *Handshake Protocol*
    - *The Change Cipher Spec Protocol*
    - *Alert Protocol*

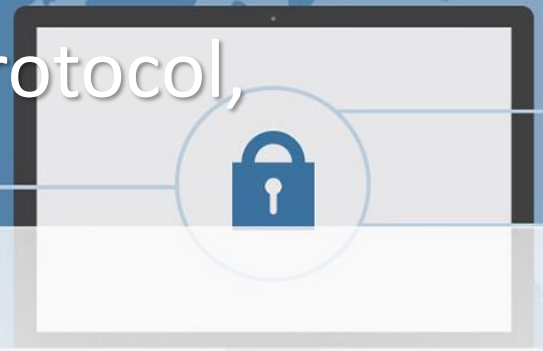


Concepte SSL



- Sesiunea SSL
  - Asocierea dintre client și server
  - Sesiunile sunt create de *Handshake Protocol*
  - Definește un set de parametri criptografici ce pot fi partajați la nivelul mai multor conexiuni
  - Folosite pentru a evita negocierea parametrilor de securitate pentru fiecare conexiune
- Conexiunea SSL
  - Sesiune de transport ce oferă o anumit tip de serviciu
  - Conexiune punct la punct
  - Conexiunile sunt tranzitorii
  - Fiecare sesiune este asociată cu o sesiune

SSL Handshake Protocol, Stări SSL



- Parametri specifici stărilor sesiune
  - Identificator de sesiune (secvență de identificare aleasă de server pentru identificarea unui status de sesiune activă sau reutilizabilă)
  - Certificat (certificat X509.v3, poate fi nul)
  - Metodă de compresie (algoritm de compresie, înainte de criptare)
  - Specificații de criptare (algoritmul de criptare – null, AES, etc.)
  - Cheie master (cheie secretă, partajată între client și server, 48 byte)
  - Indicator reutilizare (dacă sesiunea poate fi utilizată pentru a inițializa noi conexiuni)

SSL Handshake Protocol, Stări SSL

- Parametri specifici stărilor conexiune
  - Identificator server/client aleatoriu (secvență de octeți aleasă de client și server pentru fiecare conexiune)
  - Cheie MAC server (cheie secretă utilizată în operațiile la nivel MAC asupra datelor trimise de server)
  - Cheie MAC client (cheie secretă utilizată în operațiile la nivel MAC asupra datelor trimise de client)
  - Cheie server (cheie de criptare pentru datele criptate de server și decriptate de client)
  - Cheie client (cheia de criptare simetrică pentru datele criptate de client și decriptate de server)
  - Vectori de inițializare (menținut pentru fiecare cheie sau secvențial, preluat de la un bloc de criptare la următorul)
  - Numere de secvență (maxim 2^64 - 1)

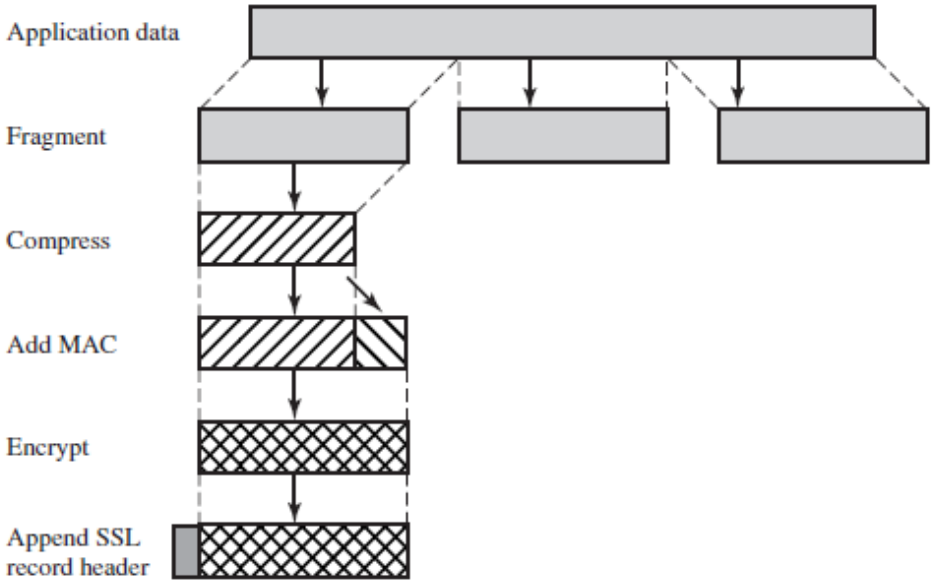
SSL Record Protocol

- Furnizează 2 servicii pentru conexiunile SSL
  - Confidențialitate

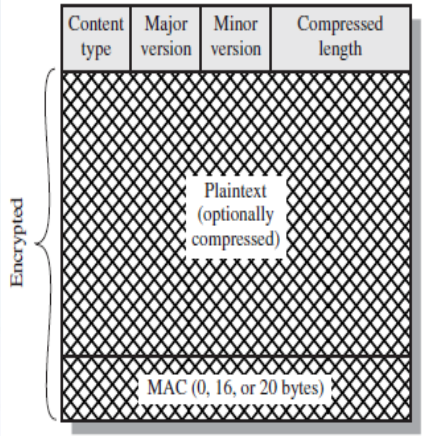
    Se definește o cheie secretă partajată, utilizată pentru criptarea SSL
  - Integritatea mesajului

    Se definește o cheie secretă partajată, utilizată pentru formarea unui MAC - *Message Authentication Code*

SSL Record Protocol



- Operații
  - Fragmentare
  - Compresia
  - Asociere MAC
  - Criptare
  - Asociere antet




```
hash(MAC_write_secret || pad_2 ||
    hash(MAC_write_secret || pad_1 || seq_num ||
    SSLCompressed.type || SSLCompressed.length ||
    SSLCompressed.fragment))
```

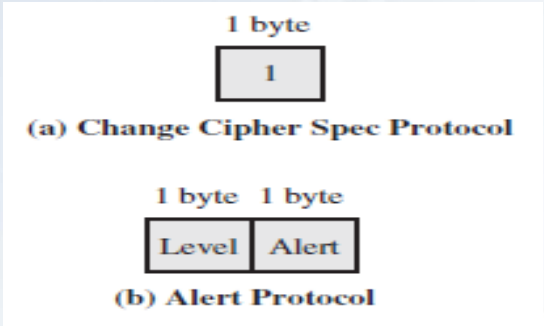
Block Cipher		Stream Cipher	
Algorithm	Key Size	Algorithm	Key Size
AES	128, 256	RC4-40	40
IDEA	128	RC4-128	128
RC2-40	40		
DES-40	40		
DES	56		
3DES	168		
Fortezza	80		

SSL Record Protocol Payload

- *SSL Record Protocol Payload*
  - *Change Cipher Spec Protocol*

    Determină copierea stării în așteptare în starea curentă, fapt ce determină actualizarea suitei criptografice utilizată la nivelul conexiunii
  - *Alert Protocol*

    Transmite mesaje specifice SSL către entități, mesajele sunt compresate și criptate, conform specificațiilor stării curente

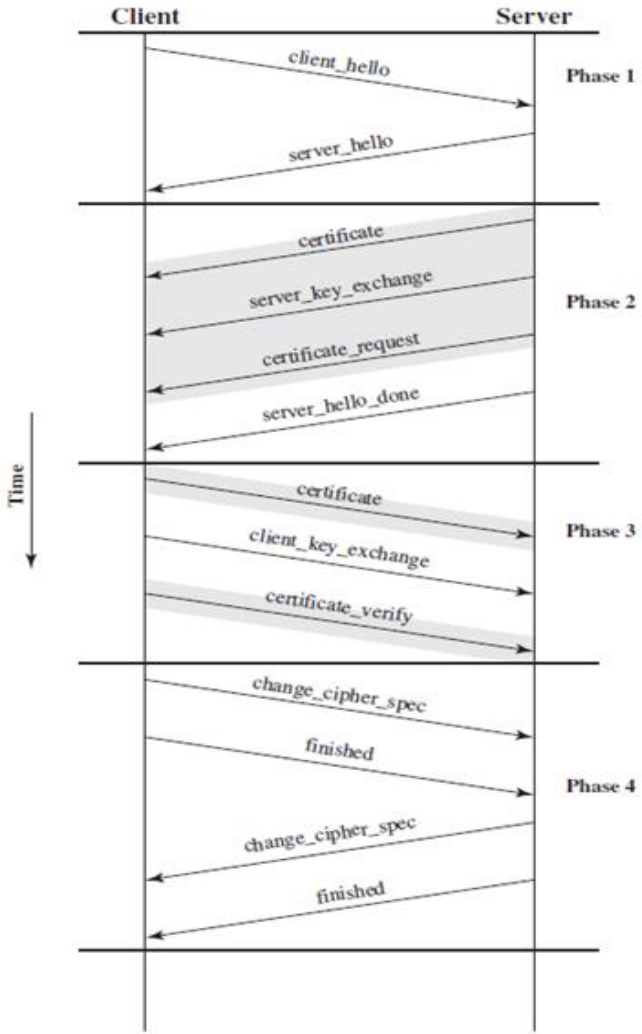


SSL Handshake Protocol, Mesaje

Message Type	Parameters
hello_request	null
client_hello	version, random, session id, cipher suite, compression method
server_hello	version, random, session id, cipher suite, compression method
certificate	chain of X.509v3 certificates
server_key_exchange	parameters, signature
certificate_request	type, authorities
server_done	null
certificate_verify	signature
client_key_exchange	parameters, signature
finished	hash value

Handshake Protocol, Acțiuni

- Etape
  - 1. Stabilirea capacităților de securitate, inclusiv versiunea de protocol, ID-ul de sesiune, suita criptografică, metoda de compresie, vectorul de inițializare.
  - 2. Serverul poate transmite certificatul, face schimbul de chei si solicita certificatul de securitate
  - 3. Clientul trimite certificat la solicitare, face schimbul de chei și poate trimite verificarea certificatului
  - 4. Se face schimbul de mesaje criptate și se finalizează protocolul



TLS - Transport Layer Security

- TLS
  - versiune standard SSL pentru Internet
  - RFC 5246 - Proposed Internet Standard
  - Foarte similar cu SSL v3
  - SSLv3.0 nu mai este sigur (vulnerabilitatea POODLE)
  - TLSv1.0 poate fi privit ca SSLv3.1

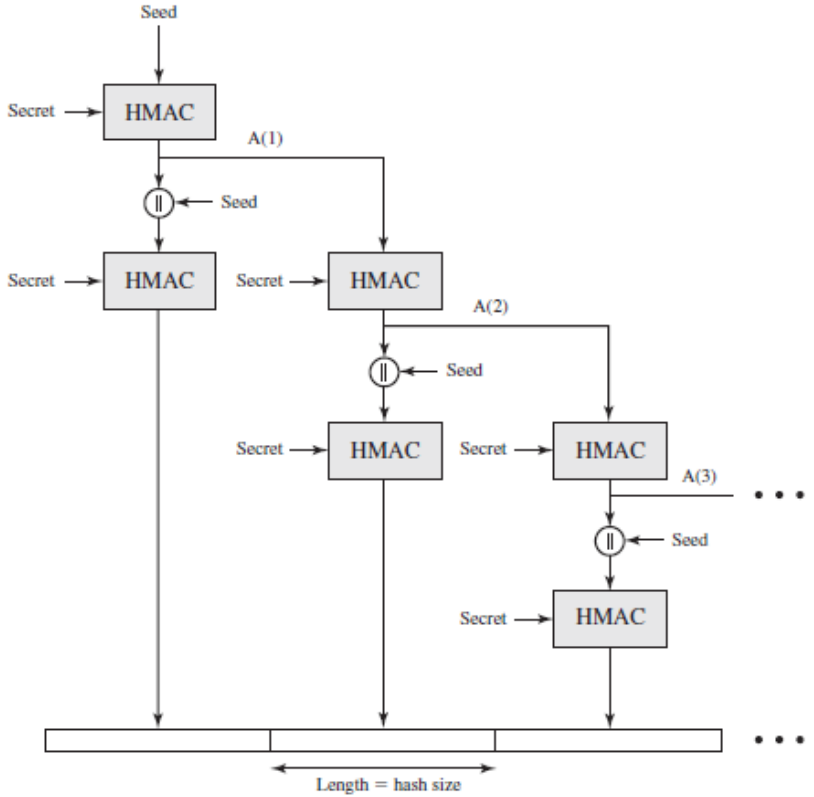
Funcția de criptare TLS

```
P_hash(secret, seed) = HMAC_hash(secret, A(1) || seed) ||
                       HMAC_hash(secret, A(2) || seed) ||
                       HMAC_hash(secret, A(3) || seed) || ...
```

where A() is defined as

$$A(0) = \text{seed}$$
$$A(i) = \text{HMAC\_hash}(\text{secret}, A(i-1))$$

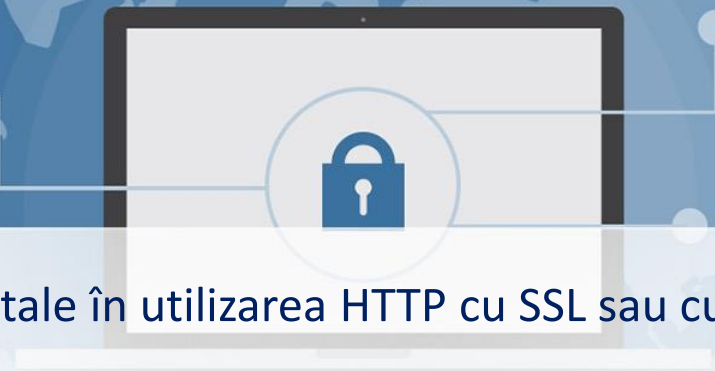
- Funcția de expandare a datelor



HTTPS

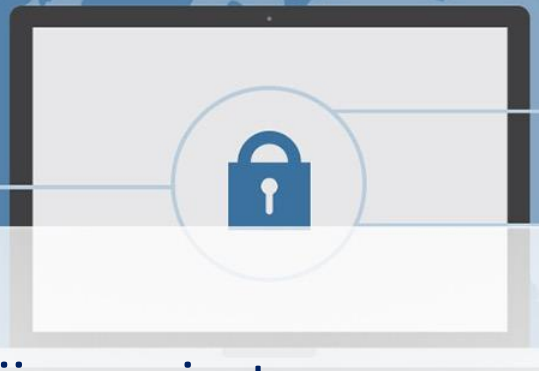
- HTTPS (HTTP over SSL) - RFC 2818
  - Combinația dintre HTTP și SSL pentru implementarea comunicațiilor securizate dintre clienții și serverele web
  - Caracteristicile HTTPS sunt incluse în browser
  - Folosirea depinde de server, dacă suportă/activ HTTPS
  - Diferențe URL (https:// vs. http://), port :443 vs. :80
  - Diferență Criptarea elementelor de comunicație
    - URL
    - Conținutul documentului web
    - Conținutul formelor web (completate de utilizator)
    - Cookie-urile
    - Conținutul antetului HTTP

Conexiuni HTTPS



- Nu există diferențe fundamentale în utilizarea HTTP cu SSL sau cu TLS (HTTPS)
- Inițierea conexiunilor
  - Clientul inițiază conexiunea către server (este și client TLS)
  - Cererea HTTP poate fi inițializată după protocol de handshake TLS
  - Toate datele HTTP sunt transmise ca și date TLS
- Închiderea conexiunilor
  - Conexiunile HTTP pot fi închise de client sau de server
  - Pentru închiderea HTTPS, trebui mai întâi închisă conexiunea TLS
  - Clienții HTTPS trebuie să facă față situației în care conexiunea TCP este terminată, fără încheierea protocolului de semnalizare

SSH - Secure Shell



- Secure Shell (SSH)
  - Protocol pentru comunicații securizate
  - Facilitate de conectare la distanță (înlocuiește TELNET)
  - Dispune de capabilități generale client/server care pot fi utilizate pentru diverse funcții de rețea
    - transfer de fișiere,
    - email,
    - vpn,
    - tunelare interfață grafică,
    - etc.

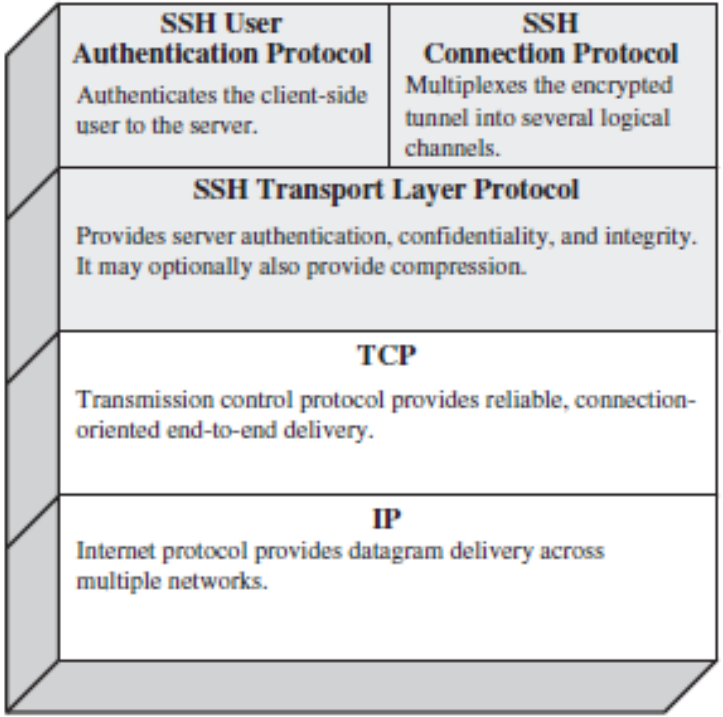
Protocoale SSH

- Stiva de protocoale SSH
  - ***Transport Layer Protocol***

    oferă autenticitatea serverului, confidențialitatea și integritatea datelor, opțional compresie
  - ***User Authentication Protocol***

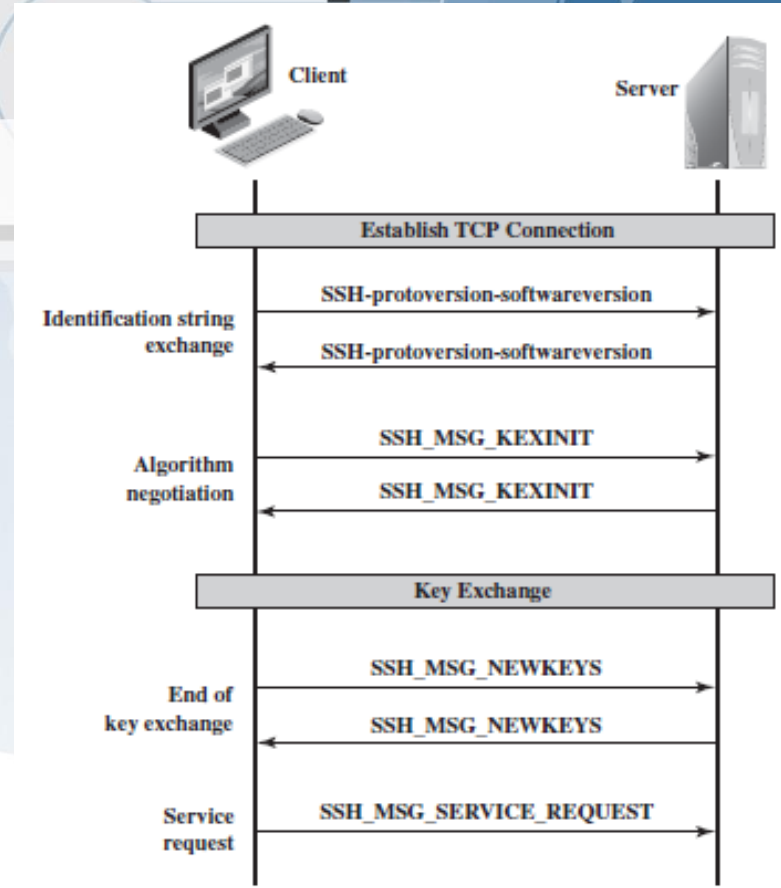
    asigură autentificarea utilizatorilor către server
  - ***Connection Protocol***

    multiplexează diferitele canale de comunicație logice la nivelul unei singure conexiuni SSH



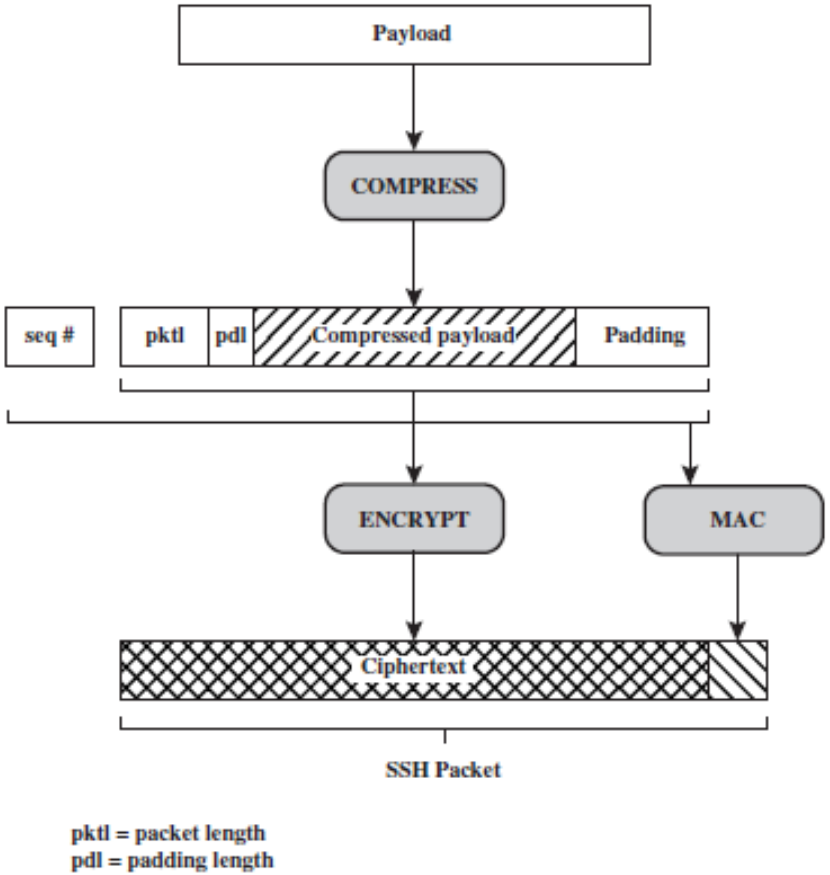
Schimbul de pachete SSH

- Mesajele specifice SSH *Transport Layer Protocol*
  - Stabilirea conexiunii
    - Identificare
    - Negociere algoritm
  - Schimbul de chei
    - Transferul de chei
    - Cererea de serviciu



Pachetul SSH

- Formatul pachetului SSH
  - Lungime pachet
  - Lungime biți de *padding*
  - Conținut efectiv (*payload*)
  - MAC (*Message Authentication Code*)



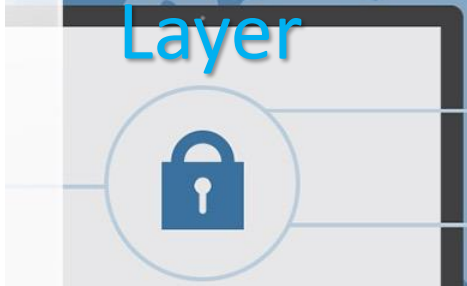
Algoritmi SSH Transport Layer

Cipher	
3des-cbc*	Three-key 3DES in CBC mode
blowfish-cbc	Blowfish in CBC mode
twofish256-cbc	Twofish in CBC mode with a 256-bit key
twofish192-cbc	Twofish with a 192-bit key
twofish128-cbc	Twofish with a 128-bit key
aes256-cbc	AES in CBC mode with a 256-bit key
aes192-cbc	AES with a 192-bit key
aes128-cbc**	AES with a 128-bit key
Serpent256-cbc	Serpent in CBC mode with a 256-bit key
Serpent192-cbc	Serpent with a 192-bit key
Serpent128-cbc	Serpent with a 128-bit key
arcfour	RC4 with a 128-bit key
cast128-cbc	CAST-128 in CBC mode

MAC algorithm	
hmac-sha1*	HMAC-SHA1; digest length = key length = 20
hmac-sha1-96**	First 96 bits of HMAC-SHA1; digest length = 12; key length = 20
hmac-md5	HMAC-MD5; digest length = key length = 16
hmac-md5-96	First 96 bits of HMAC-MD5; digest length = 12; key length = 16

Compression algorithm	
none*	No compression
zlib	Defined in RFC 1950 and RFC 1951

* = Required
** = Recommended



SSH User Authentication Protocol

- Metode de autentificare solicitate de server
  - Cu cheie publică

    Depinde de algoritmul cu cheie publică folosit
  - Cu parolă

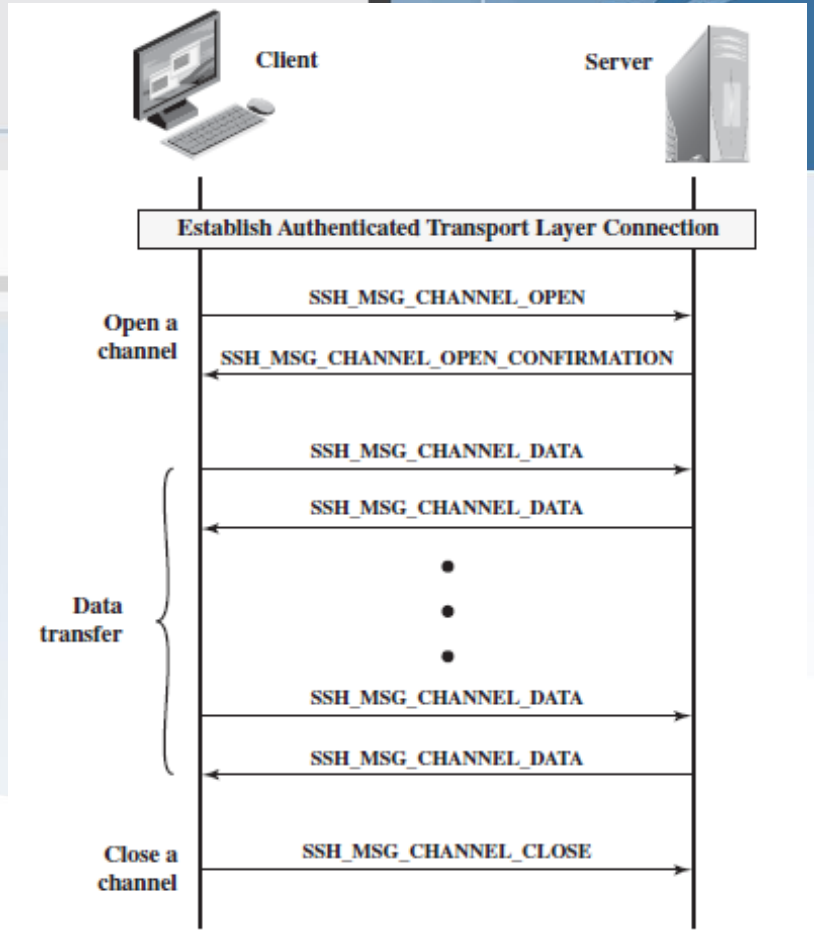
    Clientul trimite un mesaje cu parola, criptată de SSH Transport Layer Protocol
  - Pa bază de host

    Este autentificat un host (nu un utilizator)

    (pentru toți utilizatorii pe care i-ar putea avea)

Conexiune SSH

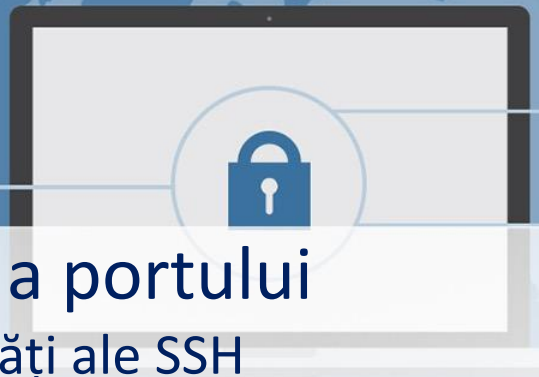
- Mesaje specifice SSH
  - Deschidere canal
  - Transfer de date
  - Închidere canal



SSH Connection Protocol

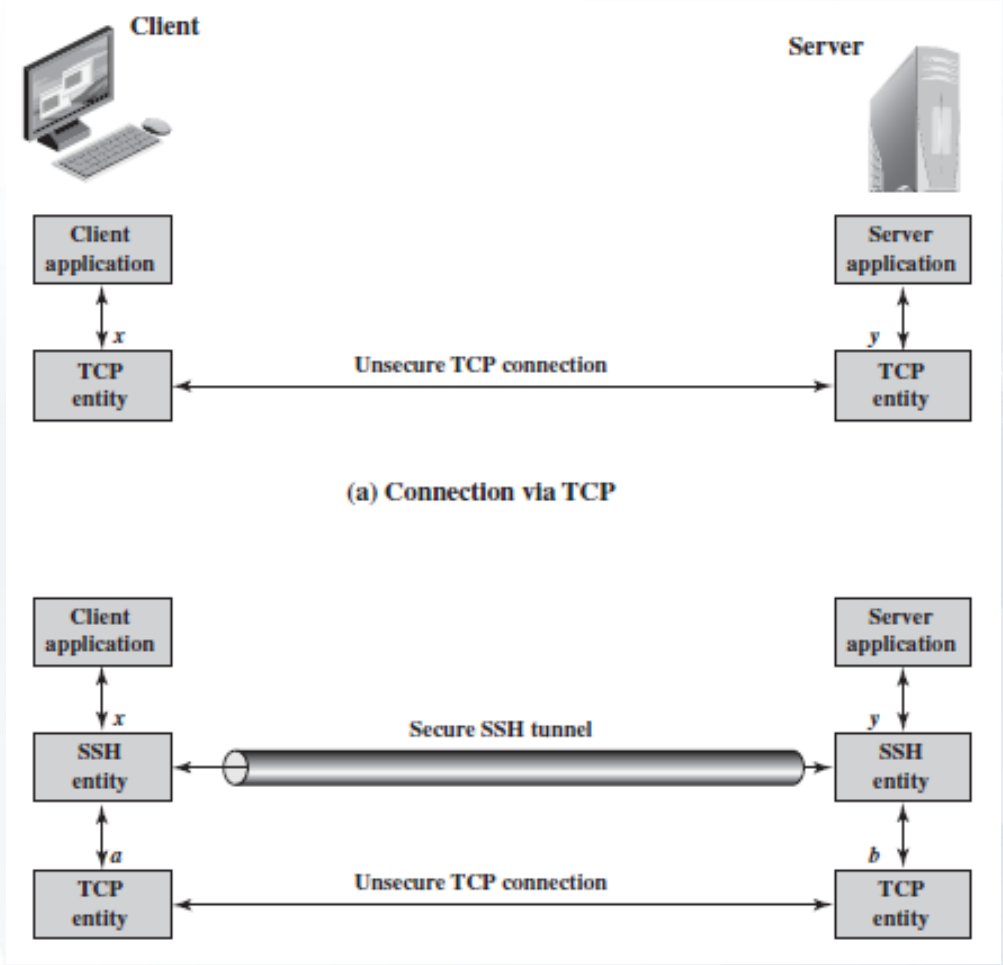
- Protocolul conexiune SSH
  - rulează deasupra nivelului Transport SSH
  - presupunând că este deja utilizată o conexiune securizată de autentificare, denumită tunel SSH
  - multiplexează conexiunile logice la nivelul tunelului SSH
- Tipuri de canale
  - Sesiune (execuția la distanță a unui program, shell, aplicație, comandă sistem sau sub-shell)
  - X11 (X Window System pentru aplicații GUI)
  - Forward tcp/ip (remote port forwarding,)
  - Direct tcp/ip (local port forwarding,)

SSH Port forwarding



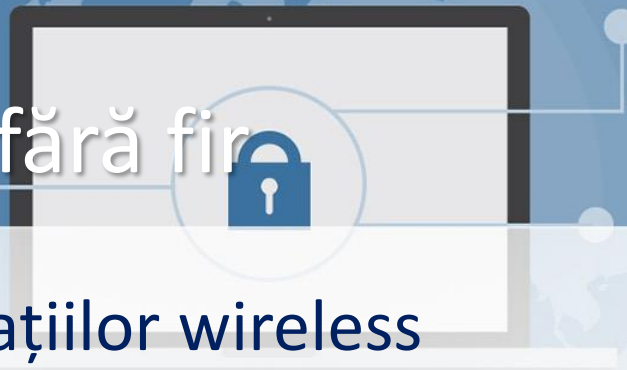
- Funcția de redirecționare a portului
  - Una dintre cele mai utile facilități ale SSH
  - Convertește orice conexiune TCP nesigură într-o conexiune securizată SSH
  - SSH tunneling
  - 2 tipuri de port forwarding
    - **Local** - permite clientului să creeze un proces de redirectare a unei conexiuni prin intermediul unui tunel SSH
    - **Remote** - clientul SSH al utilizatorului acționează în numele serverului, când se dorește utilizarea unui server din spatele unui firewall ce nu permite conexiuni SSH

Tunelare SSH



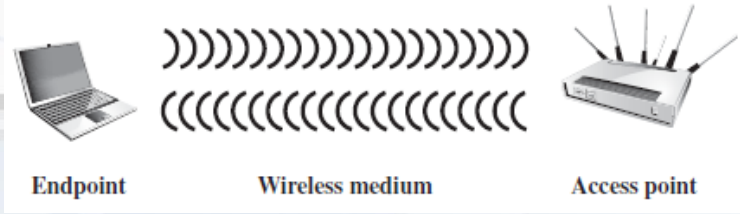
- Schimb de pachete SSH

Securitatea rețelelor fără fir



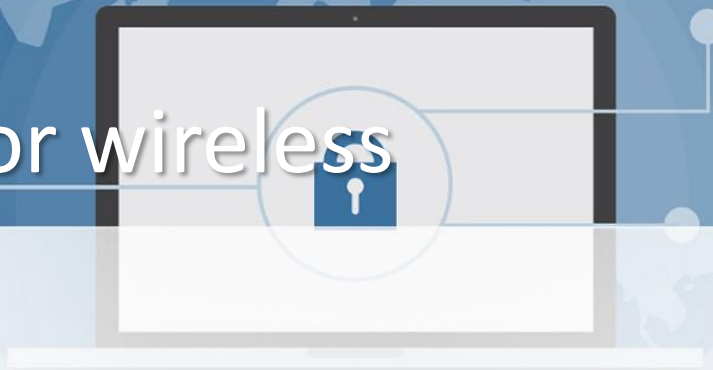
- Securitatea comunicațiilor wireless
- Securitatea dispozitivelor mobile
- Rețele wireless locale - IEEE 802.11
- Standardul de securitate wireless - 802.11i

Securitatea rețelelor wireless



- Canal de transmisiuni
  - Comunicații tip broadcast
  - Rețele sunt mai vulnerabile decât protocoalele
- Mobilitate
  - Dispozitivele wireless sunt adesea portabile
- Resurse
  - Dispozitivele wireless au sisteme de operare sofisticate, dar au resurse hardware limitate
- Accesibilitate
  - Dispozitivele wireless pot fi amplasate în locuri nesupravegheate

Securitatea rețelelor wireless

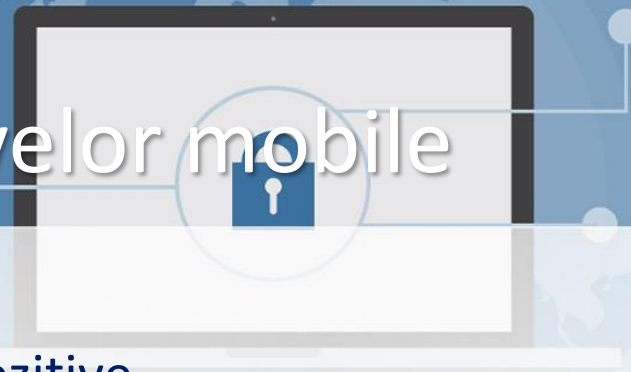


- Amenințări de securitate
  - Asocierea accidentală
  - Asocierea premeditată
  - Rețele ad-hoc
  - Rețele netradiționale
  - Furtul de identitate (MAC spoofing)
  - Atac man-in-the-middle
  - Atac tip Denial-of-service (DoS)
  - Injectarea de pachete în rețea

Securitatea rețelelor wireless

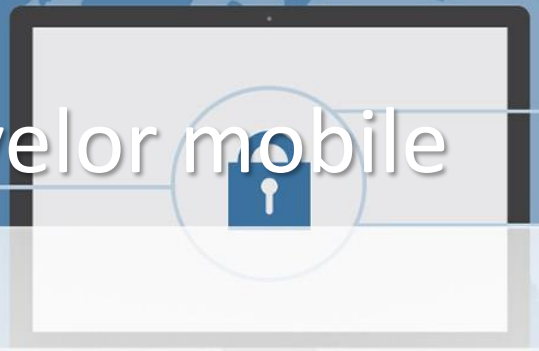
- Securizare transmisii wireless
  - Tehnici de ascundere a semnalului
    ascundere SSID, SSID codat, nivelului de semnal la minimul necesar, antene directive
  - Criptarea și protocoale de autentificare
- Securizare punct de distribuție (Access Point - AP)
  - Controlul accesului la nivel de port - IEEE 802.1X
- Securizare rețele wireless
  - Utilizare criptare (router)
  - Folosire firewall/antivirus (toate punctele rețelei)
  - Schimbarea numelui de SSID/user/parola implicite
  - Permiterea accesului în rețea pe baza adresei MAC

Securitatea dispozitivelor mobile



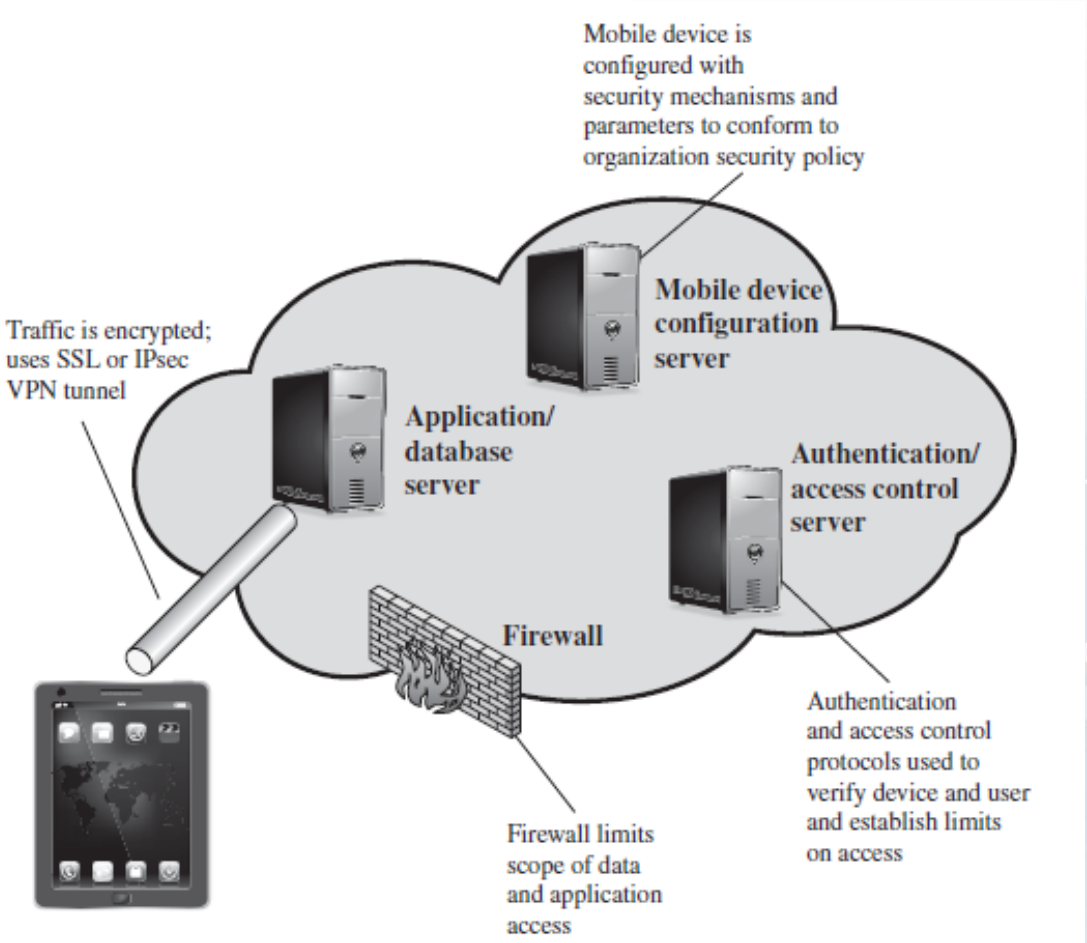
- Factori determinanți
  - Creșterea numărului de dispozitive
  - Utilizarea aplicațiilor din cloud
  - Imposibilitatea definirii stricte a perimetrelor rețelelor
  - Necesitatea permiterii accesului pentru echipamente externe (parteneri, vizitatori, locații la distanță)
- Politicile de securitate
  - Trebuie implementate la nivel organizațional
  - Facilități de securitate la nivelul dispozitivelor
  - Controlul securității la nivelul componentelor de rețea

Securitatea dispozitivelor mobile



- Amenințări de securitate
  - Lipsa controlului de securitate la nivel fizic
  - Utilizarea de dispozitive mobile nesigure
  - Utilizarea de rețele nesigure
  - Folosirea de aplicații de la producători neidentificabili
  - Interacțiunea cu alte sisteme
  - Accesarea de conținut nesigur
  - Utilizarea serviciilor de localizare

Elemente de securitate



- Accesul dispozitivelormobile

Securitatea dispozitivelor mobile

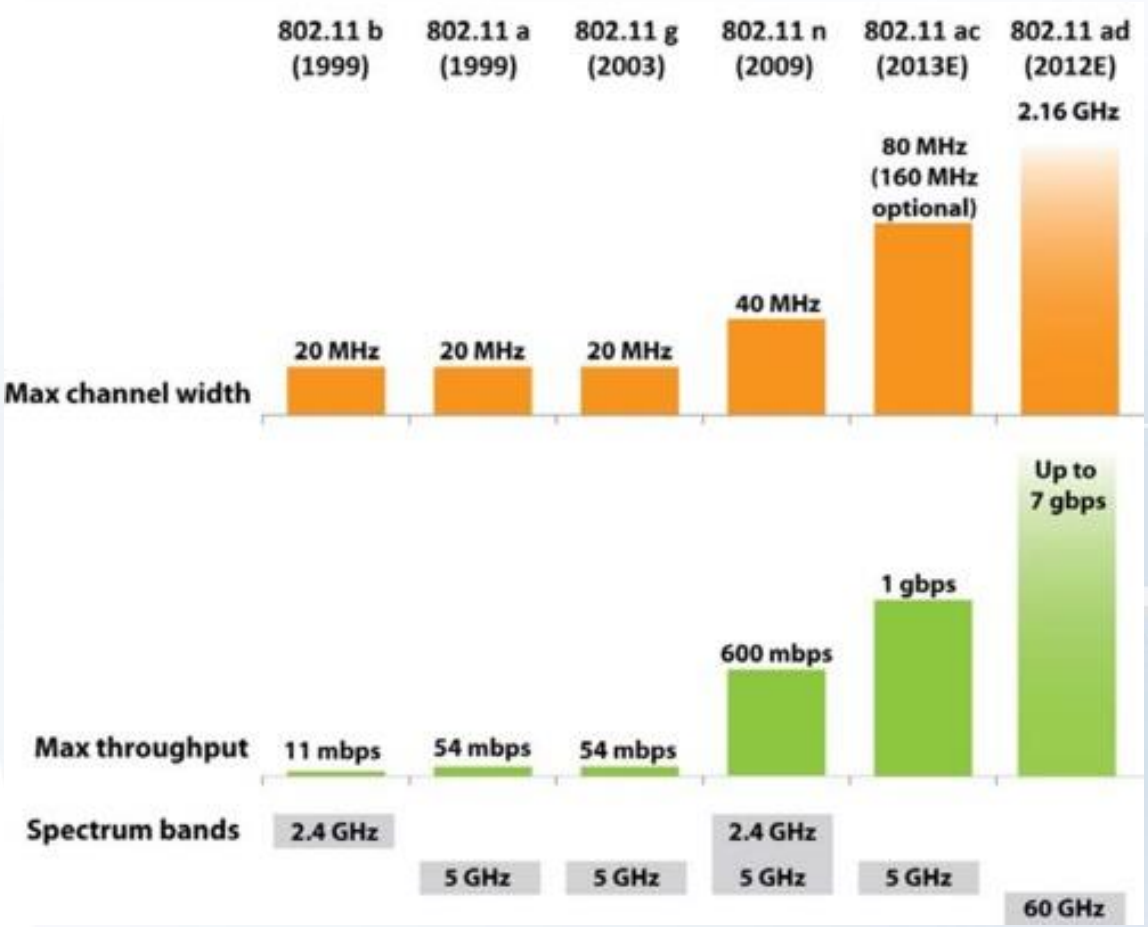
- Strategii de securitate
  - Securizarea dispozitivelor
    - Auto-lock, acces cu parolă/PIN,
    - Evitarea funcțiilor de auto-completare
  - Securitatea traficului
    - Mecanisme de criptare (SSL)
    - Sisteme de autentificare (VPN)
  - Securizarea limitelor de rețea
    - Mecanisme de protecție față de accesul neutorizat
    - Politici firewall
    - Sisteme de detecție și prevenire a intruziunilor

Wireless LAN

- Wi-Fi Alliance (Wireless Fidelity) ex. Wireless Ethernet Compatibility Alliance (WECA),
- Terminologie standard IEEE 802.11

Access point (AP)	Any entity that has station functionality and provides access to the distribution system via the wireless medium for associated stations.
Basic service set (BSS)	A set of stations controlled by a single coordination function.
Coordination function	The logical function that determines when a station operating within a BSS is permitted to transmit and may be able to receive PDUs.
Distribution system (DS)	A system used to interconnect a set of BSSs and integrated LANs to create an ESS.
Extended service set (ESS)	A set of one or more interconnected BSSs and integrated LANs that appear as a single BSS to the LLC layer at any station associated with one of these BSSs.
MAC protocol data unit (MPDU)	The unit of data exchanged between two peer MAC entities using the services of the physical layer.
MAC service data unit (MSDU)	Information that is delivered as a unit between MAC users.
Station	Any device that contains an IEEE 802.11 conformant MAC and physical layer.

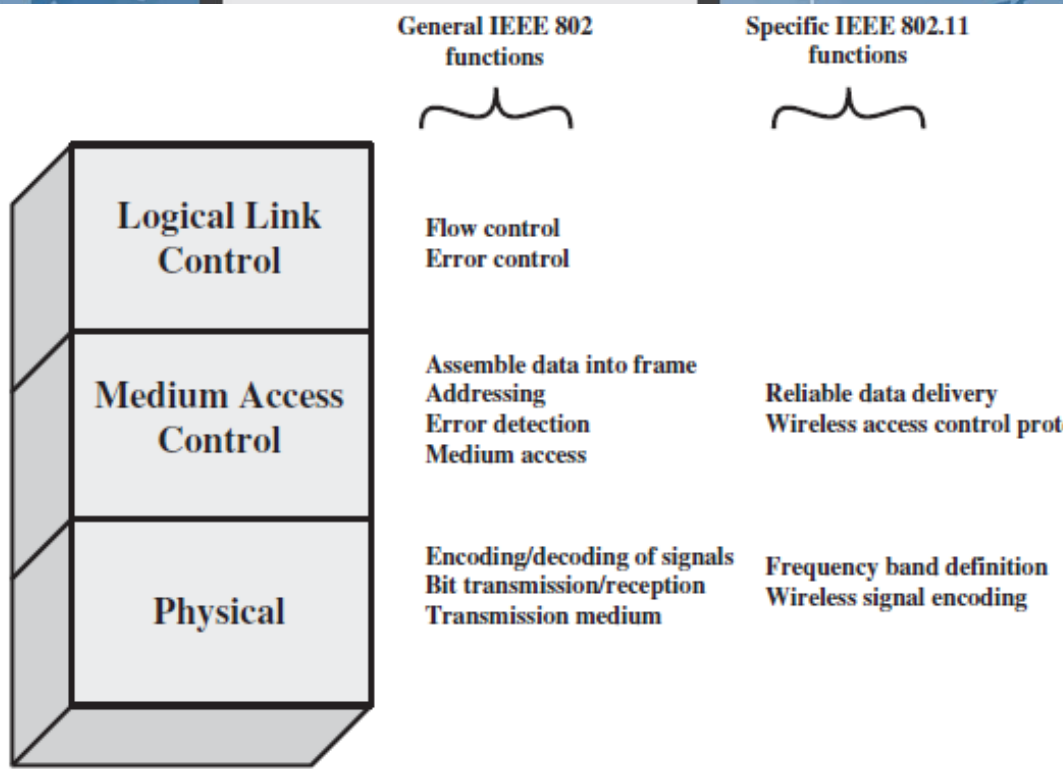
Evoluție 802.11



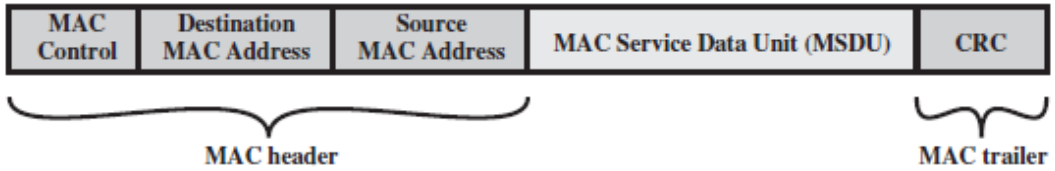
- Standard 802.11

Arhitectură 802.11

- Stiva de protocoale
- 802.11 vs. IEEE 802

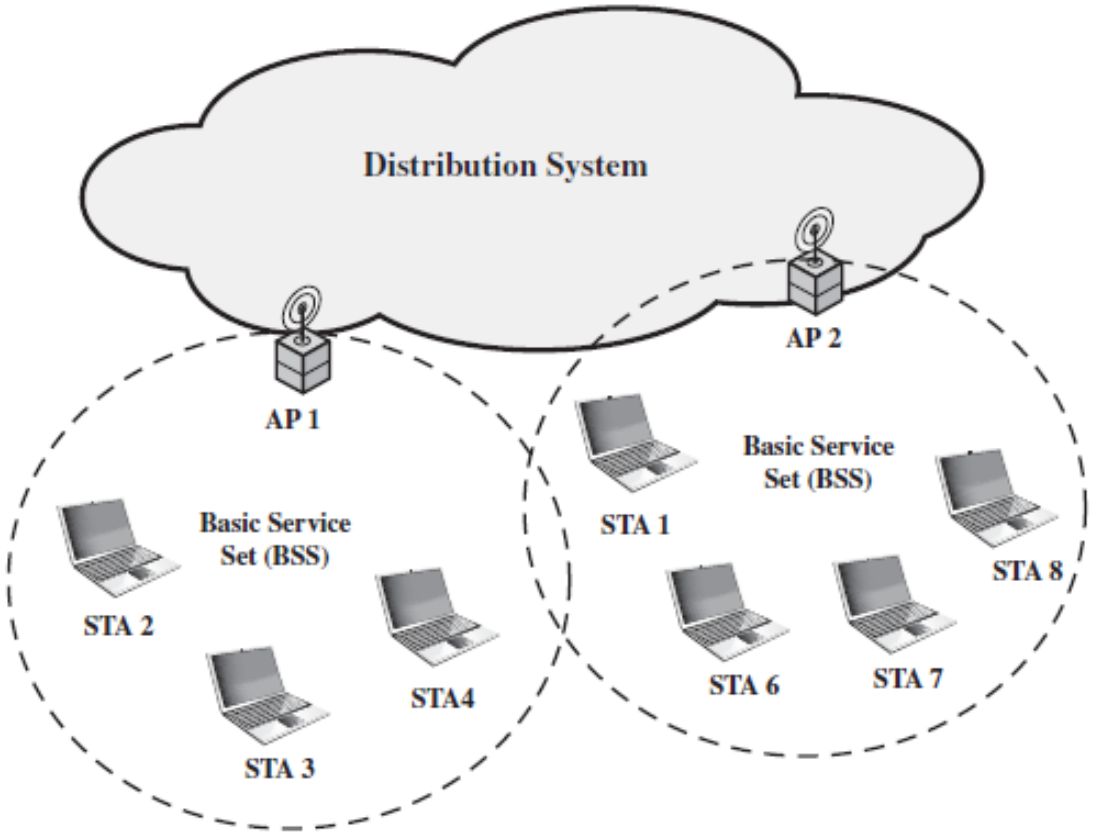


- Format MPDU



Model Arhitectural 802.11

- Componente rețea 802.11
  - BSS
  - AP
  - DS
  - ESS
  - IBSS



Servicii wireless

- 802.11 definește 9 servicii asigurate de o rețea WLAN
  - 3 pentru control
  - 6 pentru susținerea comunicației

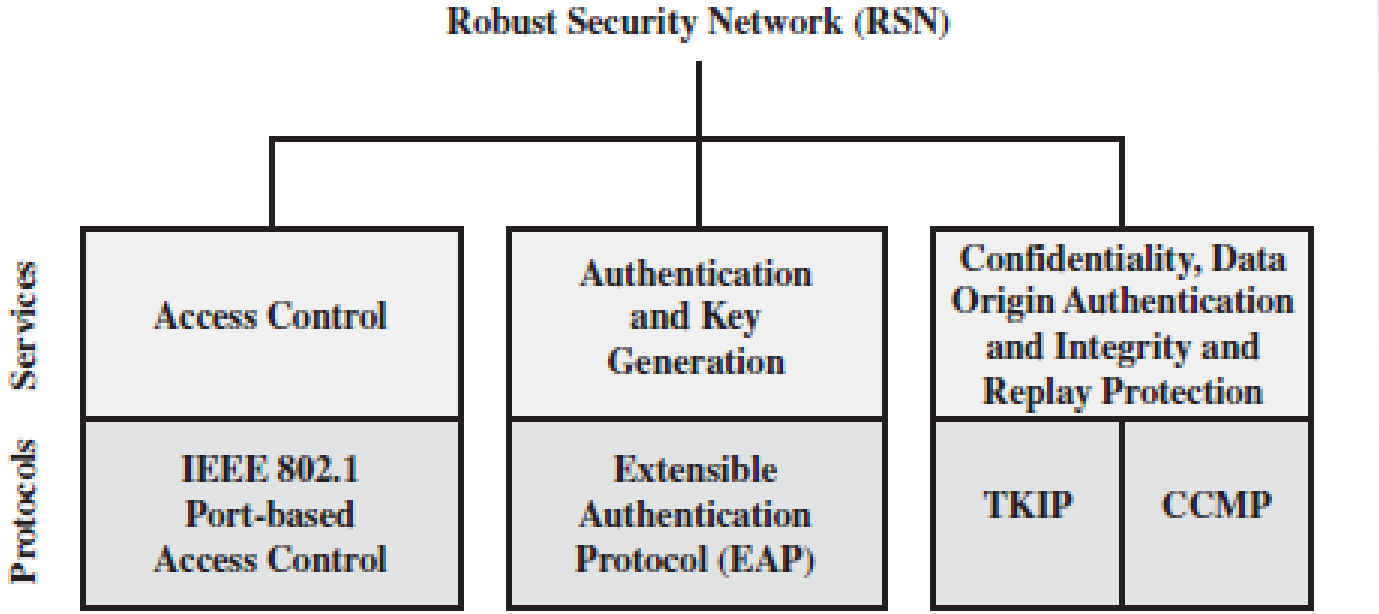
Service	Provider	Used to support
Association	Distribution system	MSDU delivery
Authentication	Station	LAN access and security
Deauthentication	Station	LAN access and security
Disassociation	Distribution system	MSDU delivery
Distribution	Distribution system	MSDU delivery
Integration	Distribution system	MSDU delivery
MSDU delivery	Station	MSDU delivery
Privacy	Station	LAN access and security
Reassociation	Distribution system	MSDU delivery

Securitatea rețelelor wireless

- Standardul 802.11i
  - Algoritmul WEP (Wired Equivalent Privacy)
  - Standardul WPA (Wi-Fi Protected Access)
  - Standard 802.11i - RSN (Robust Security Network) (WPA2)
    - Autentificare
    - Controlul accesului
    - Intimitate (criptare date la nivel MAC)
- Elemente 802.11i
  - Servicii și protocoale
  - Algoritmi criptografici

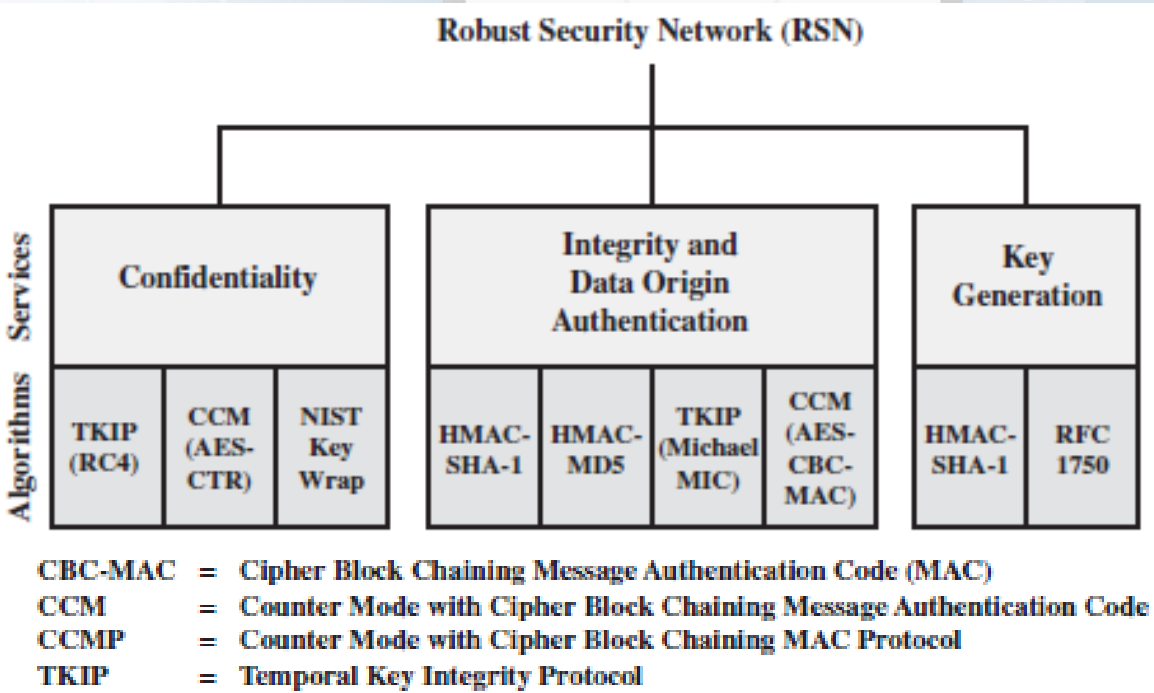
Servicii și protocoale

- RSN



Algoritmi criptografici

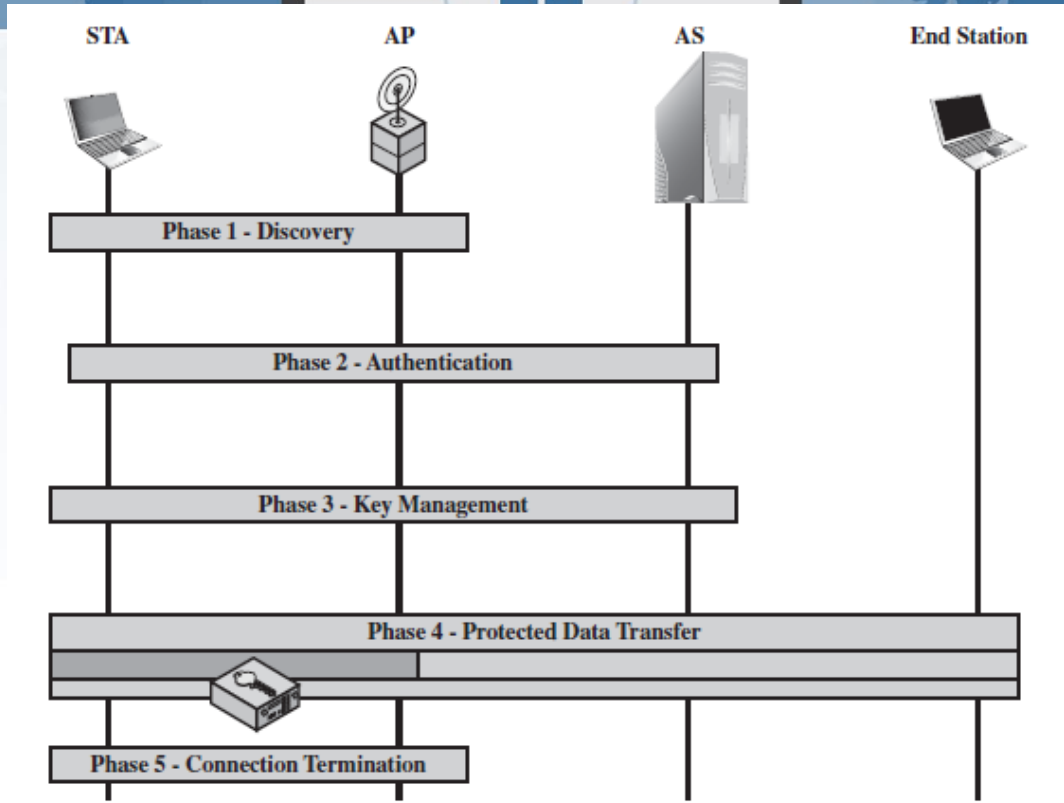
- RSN



Operațiuni specifice 802.11i

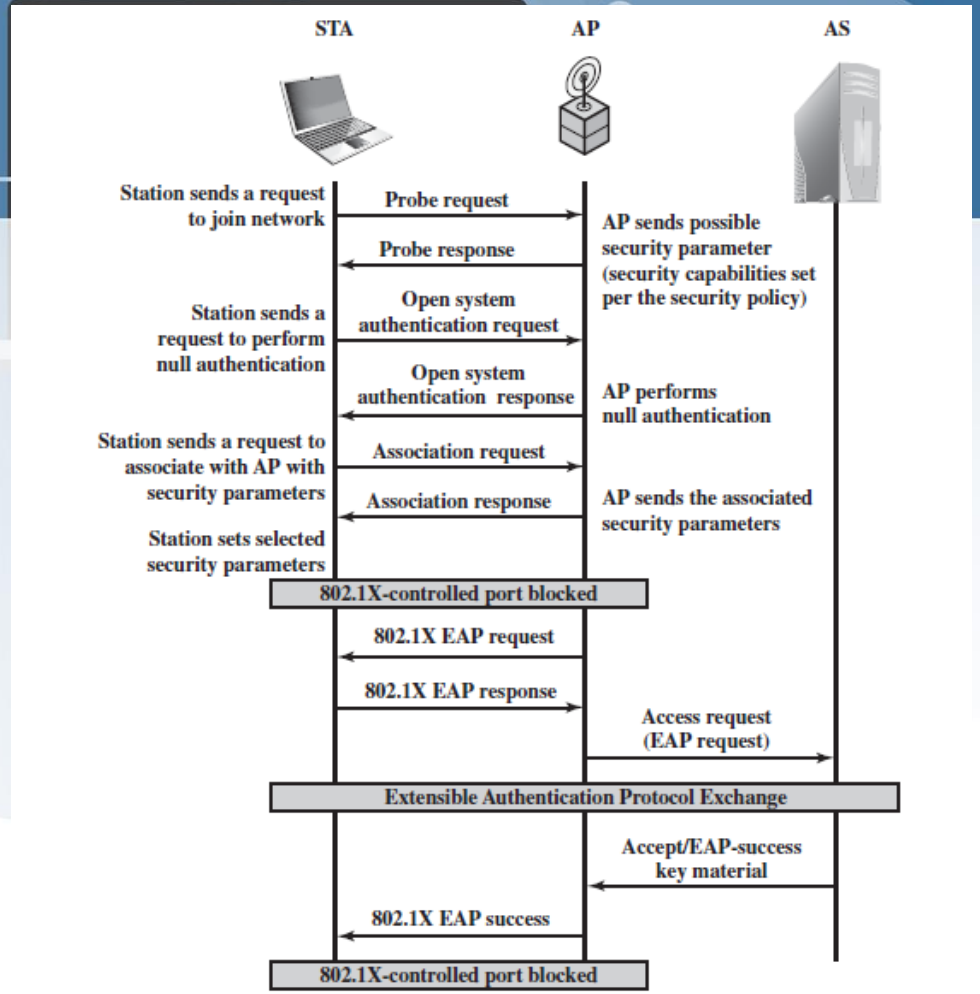
- Etape 802.11i

1. Identificare
2. Autentificare
3. Management chei
4. Transfer date
5. Terminare conexiune

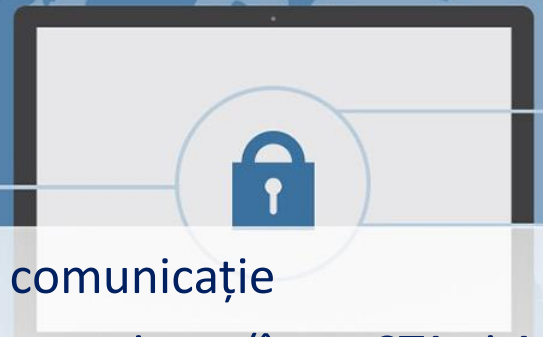


Etape de asociere 802.11i

- Detalii etape
  - Identificare (descoperire capacități)
  - Autentificare
  - Asociere

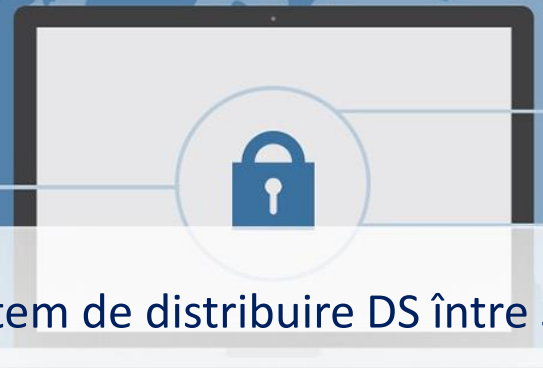


Identificarea



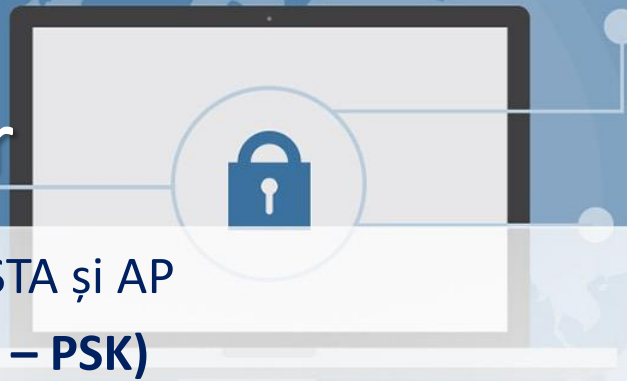
- Descoperirea capacităților de comunicație
  - Se stabilesc capabilități de securitate (între STA și AP)
    - tehnicile de asigurare a confidențialității
      - WEP (cheie 40/104biți), TKIP, CCMP
    - metoda de autentificare, AKM *(Authentication And Key Management)*
      - IEEE 802.1X, cheie secretă partajată
    - abordarea privind administrarea cheilor criptografice
  - Schimbul MPDU (*MAC Protocol Data Unit*)
    - Identificare resurse
    - Autentificare
    - Asociere

Autentificarea



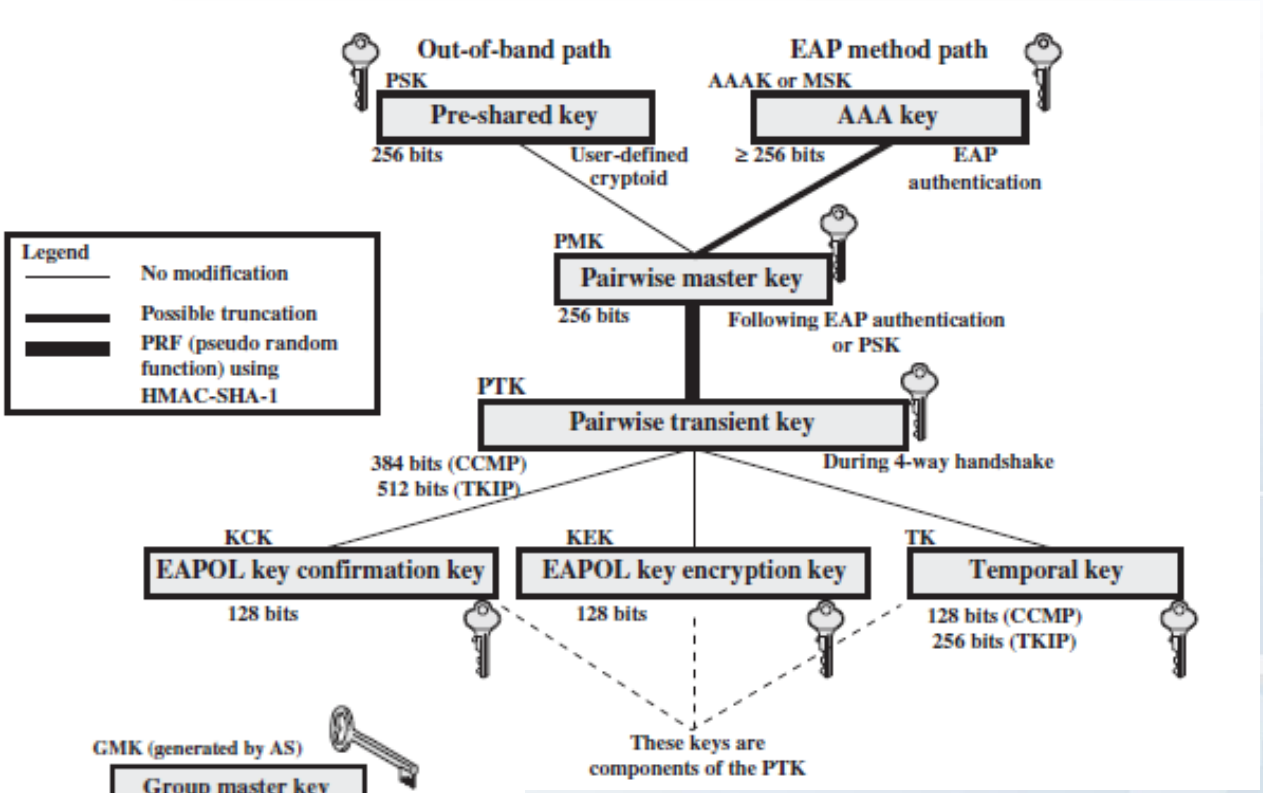
- Autentificare reciprocă la nivel de sistem de distribuire DS între STA și un AS
  - Controlul accesului prin 802.1X
  - Schimbul MPDU
    - (Conectare către AS - Schimbul EAP - Livrarea cheilor de securitate)
      - AS generează cheie master – *AAA (Authentication, Authorization, and Accounting)*
      - cheie care este trimisa către STA
      - cheile necesare STA pentru comunicația cu AP sunt generate pe baza AAA
  - Schimbul EAP (*Extensible Authentication Protocol*)
    - EAPOL sau RADIUS.

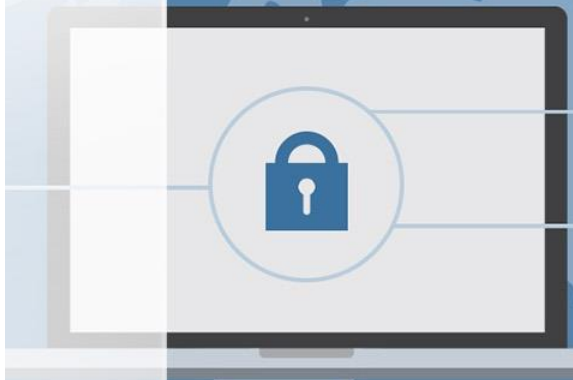
Administrarea cheilor



- Cheia unică de comunicație dintre STA și AP
  - Cheie partajată (**Pre-Shared Key – PSK)**
  - Cheie master (**Master Session Key (MSK**)
    - **Pairwise Master Key (PMK)** derivată din cheia master **Pairwise Transient Key (PTK)**, generată din PMK, are 3 componente:
      - **EAP Over LAN (EAPOL) Key Confirmation Key (EAPOL-KCK) -** cadrele de control
      - **EAPOL Key Encryption Key (EAPOL-KEK) -** protecția cheilor
      - **Temporal Key (TK) -** protecția efectivă a traficului utilizator
  - Grupuri de chei (comunicații multicast)
    - **group master key (GMK)**
    - **group temporal key (GTK)**.

Administrare chei

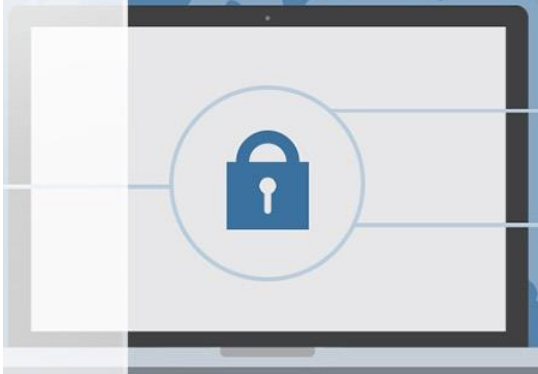




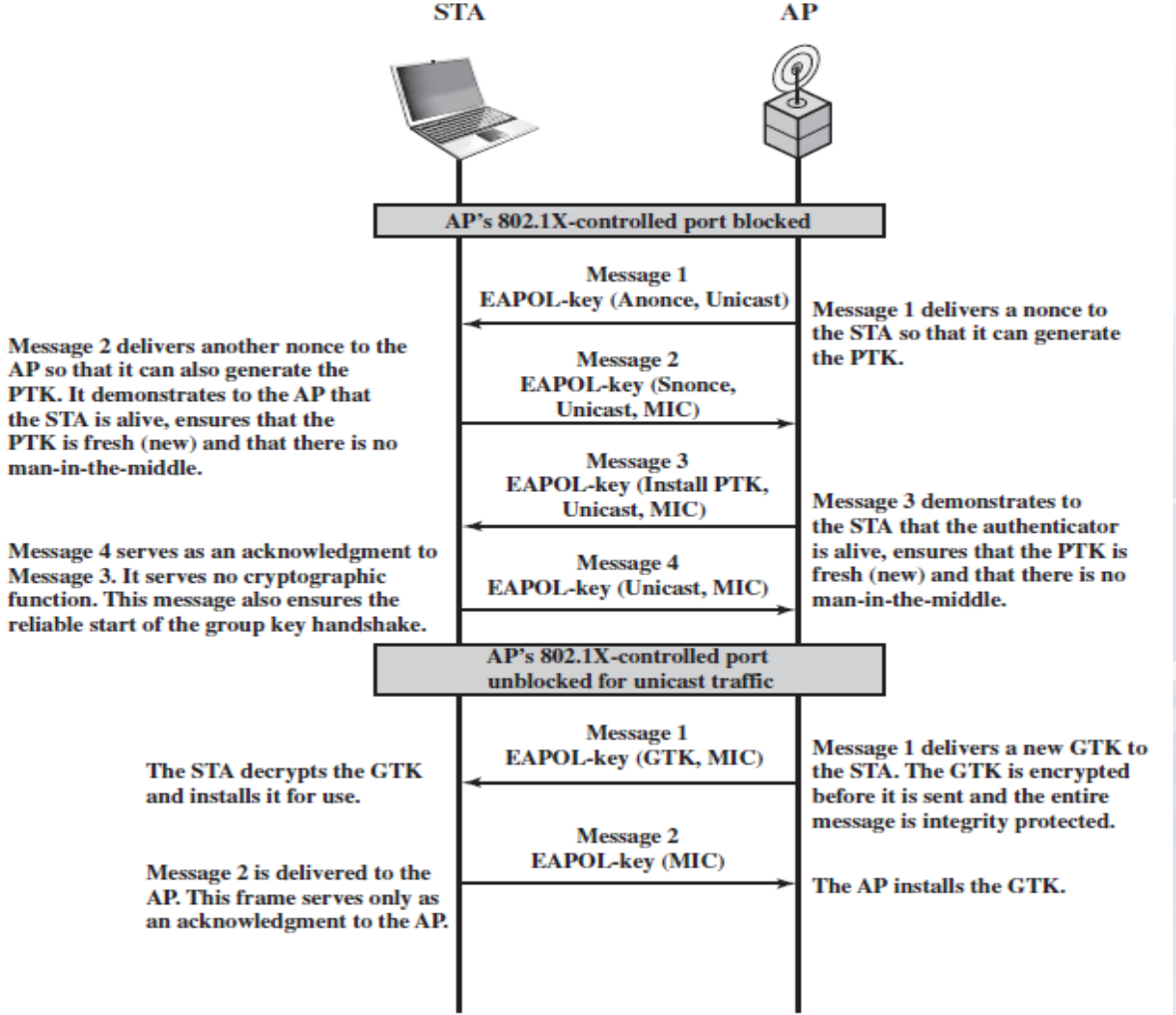
- Ierarhie chei

Chei și protocoale 802.11i

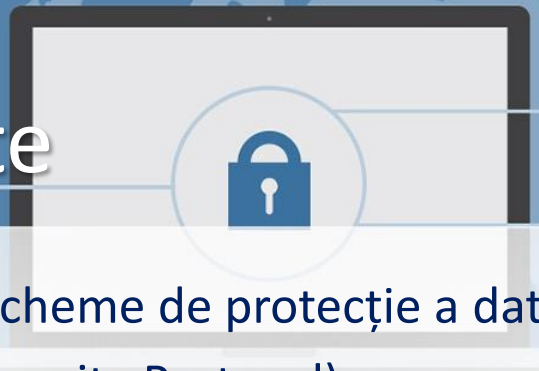
Abbrev-iation	Name	Description / Purpose	Size (bits)	Type
AAA Key	Authentication, Accounting, and Authorization Key	Used to derive the PMK. Used with the IEEE 802.1X authentication and key management approach. Same as MMSK.	≥ 256	Key generation key, root key
PSK	Pre-shared Key	Becomes the PMK in pre-shared key environments.	256	Key generation key, root key
PMK	Pairwise Master Key	Used with other inputs to derive the PTK.	256	Key generation key
GMK	Group Master Key	Used with other inputs to derive the GTK.	128	Key generation key
PTK	Pair-wise Transient Key	Derived from the PMK. Comprises the EAPOL-KCK, EAPOL-KEK, and TK and (for TKIP) the MIC key.	512 (TKIP) 384 (CCMP)	Composite key
TK	Temporal Key	Used with TKIP or CCMP to provide confidentiality and integrity protection for unicast user traffic.	256 (TKIP) 128 (CCMP)	Traffic key
GTK	Group Temporal Key	Derived from the GMK. Used to provide confidentiality and integrity protection for multicast/ broadcast user traffic.	256 (TKIP) 128 (CCMP) 40,104 (WEP)	Traffic key
MIC Key	Message Integrity Code Key	Used by TKIP's Michael MIC to provide integrity protection of messages.	64	Message integrity key
EAPOL-KCK	EAPOL-Key Confirmation Key	Used to provide integrity protection for key material distributed during the 4-Way Handshake.	128	Message integrity key
EAPOL-KEK	EAPOL-Key Encryption Key	Used to ensure the confidentiality of the GTK and other key material in the 4-Way Handshake.	128	Traffic key / key encryption key
WEP Key	Wired Equivalent Privacy Key	Used with WEP.	40,104	Traffic key



Distribuirea cheilor



Comunicații securizate



- IEEE 802.11i definește 2 scheme de protecție a datelor:
  - TKIP (Temporal Key Integrity Protocol)
    - Integritatea mesajelor (Message Integrity Code (MIC) – 64bit adăugat în frame-ul MAC)
    - Confidențialitatea datelor (criptare MPDU + MIC folosind RC4)
  - CCMP (Counter Mode-CBC MAC Protocol).
    - Integritatea mesajelor - folosind CBC-MAC (Cipher Block Chaining Message Authentication Code)
    - Confidențialitatea - folosind cifrul pe blocuri CTR (Counter) cu criptare AES.

Funcții de criptare 802.11i

- Pseudo-aleatoare

```
PRF(K, A, B, Len)
```

K = a secret key
A = a text string specific to the application (e.g., nonce generation or pair-wise key expansion)
B = some data specific to each case
Len = desired number of pseudorandom bits

```
PTK = PRF(PMK,"Pairwise key expansion",min(AP-
      Addr,STA-Addr) || max(AP-Addr,STA-Addr) || min
      (Anonce,Snonce) || max(Anonce,Snonce),384)
```