

BÀI 11. MỘT SỐ GIAO THỨC MẬT MÃ TRONG MẠNG TCP/IP

Bùi Trọng Tùng,
Viện Công nghệ thông tin và Truyền thông,
Đại học Bách khoa Hà Nội

1

1

Nội dung

- Một số dạng tấn công quá trình truyền tin (nhắc lại)
- IPSec
- SSL/TLS
- SSH
- Các giao thức mật mã trong WLAN

2

2

1. MỘT SỐ DẠNG TẤN CÔNG

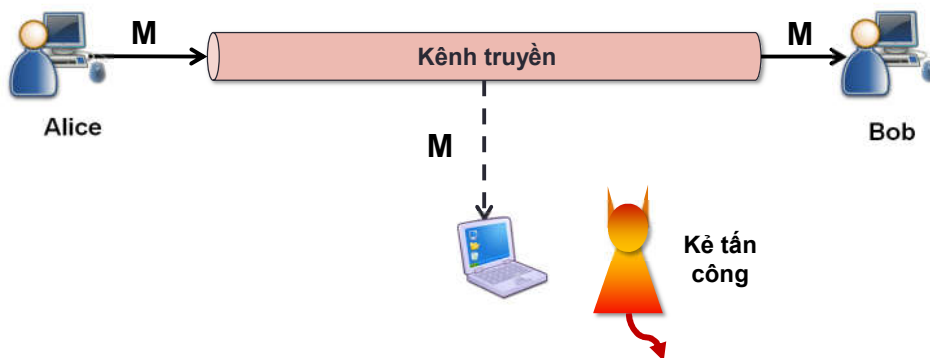
Bùi Trọng Tùng,
Viện Công nghệ thông tin và Truyền thông,
Đại học Bách khoa Hà Nội

3

3

Nghe lén

- Thu nhận trái phép các thông tin trong quá trình truyền
→ tấn công vào tính bí mật của thông tin

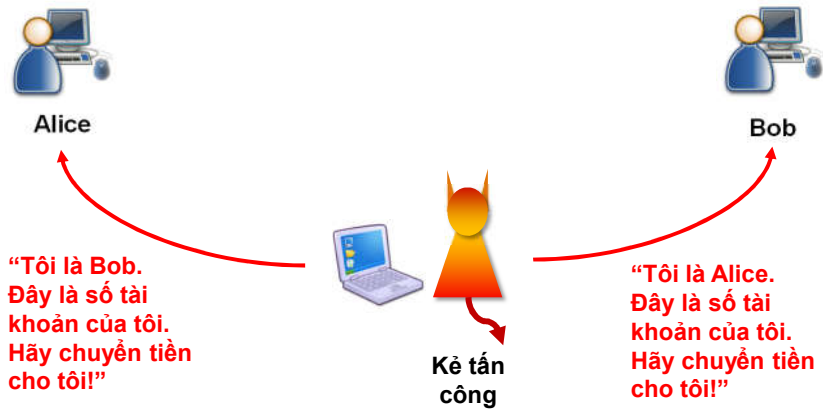


4

4

Mạo danh

- Kẻ tấn công mạo danh một bên và chuyển các thông điệp cho bên kia.

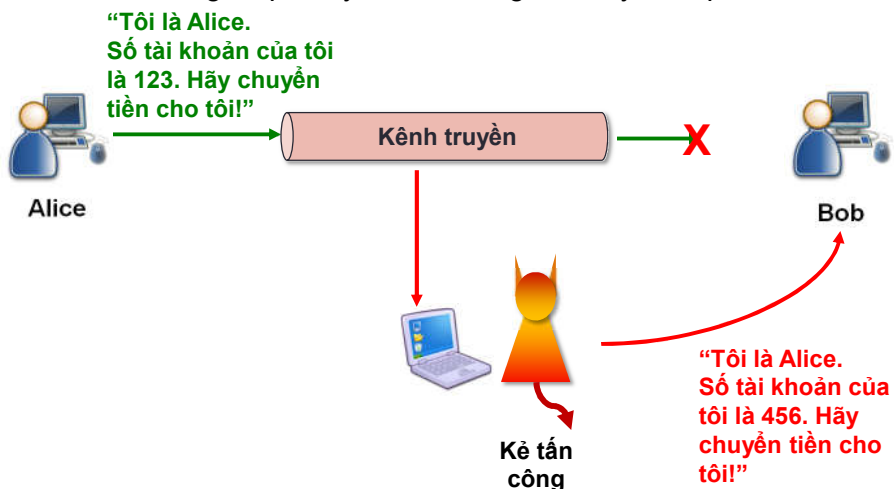


5

5

Thay đổi nội dung thông điệp

- Chặn thông điệp, thay đổi nội dung và chuyển tiếp cho bên kia

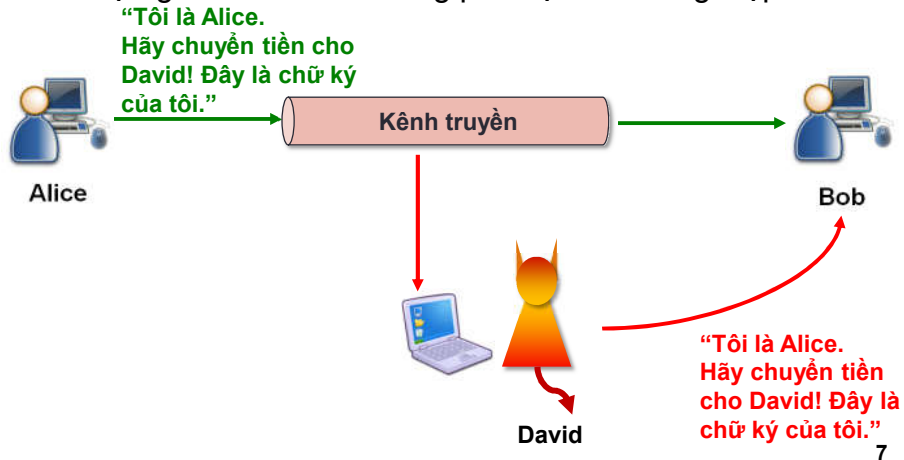


6

6

Phát lại thông điệp

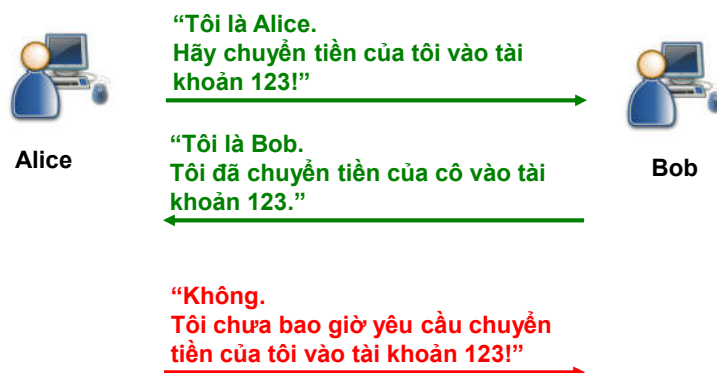
- Lỗi hồng: trên các thông điệp có dấu hiệu xác thực tính tin cậy, nhưng không có giá trị xác định thời điểm thông điệp được gửi đi → kẻ tấn công phát lại các thông điệp cũ



7

Tấn công phủ nhận gửi

- Bên gửi phủ nhận việc đã gửi đi một thông tin

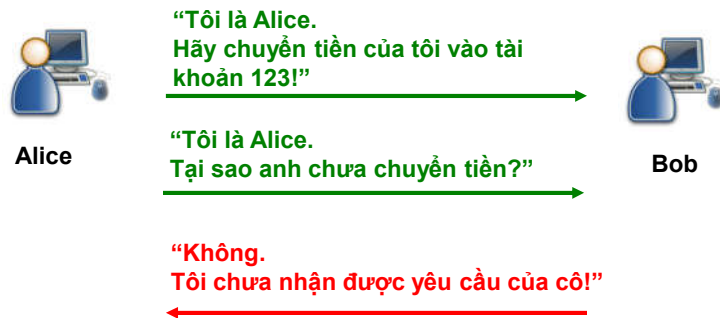


8

8

Tấn công phủ nhận nhận

- Bên nhận phủ nhận đã nhận được thông tin



9

9

2. IPSEC

Bùi Trọng Tùng,
Viện Công nghệ thông tin và Truyền thông,
Đại học Bách khoa Hà Nội

10

10

Giao thức IPSec

- Bộ giao thức bảo mật mở rộng cho IPv4 và IPv6 (mô tả chi tiết trong RFC 4301 và >30 RFC khác ☺)
- Các dịch vụ:
 - Bảo mật: DES, 3DES, AES
 - Xác thực: HMAC MD-5, HMAC SHA-1
 - Chống tấn công phát lại
 - Xác thực các bên
 - Kiểm soát truy cập
- Giao thức đóng gói dữ liệu :
 - AH : Xác thực thông điệp
 - ESP : Bảo mật thông điệp
 - ESP-ICV: Bảo mật và xác thực thông điệp

11

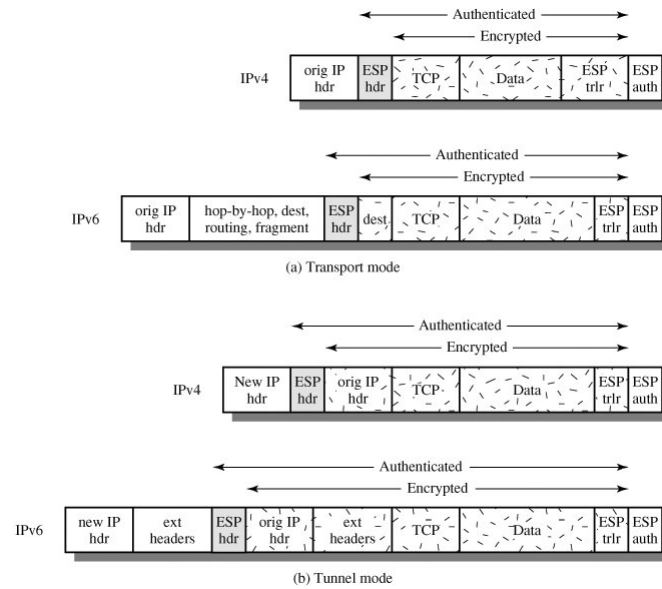
Tiến trình trao đổi dữ liệu qua IPSec VPN

1. Một trong 2 bên khởi tạo
2. Thiết lập kết nối điều khiển: ISAKMP/IKE
Phase 1:
 - Các chính sách trao đổi khóa
 - Diffie-Hellman
 - Xác thực thiết bị và xác thực người dùng
3. ISAKMP/IKE Phase 2 : thỏa thuận các tham số thiết lập kết nối bảo mật để truyền dữ liệu
4. Trao đổi dữ liệu
5. Làm mới các kết nối nếu quá thời gian quy định cho 1 phiên

12

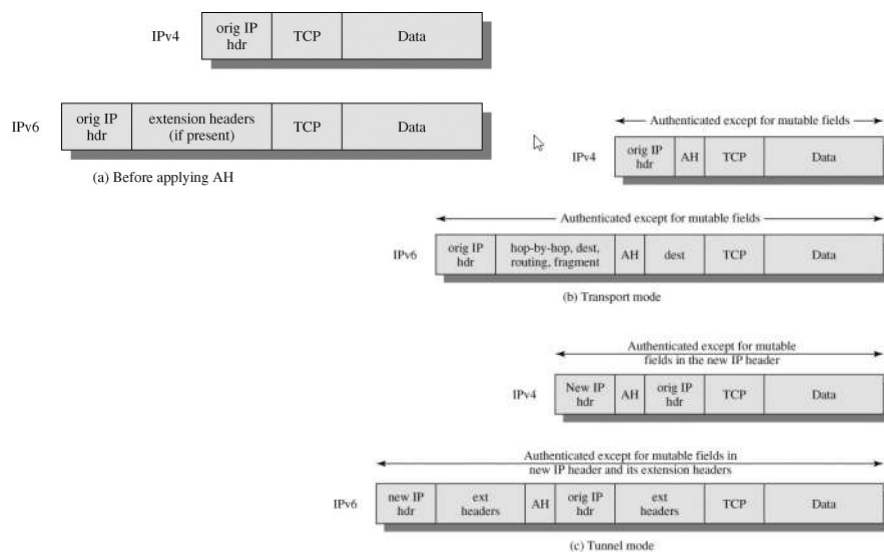
12

Đóng gói dữ liệu theo giao thức ESP



13

Đóng gói dữ liệu theo giao thức AH



14

2. GIAO THỨC SSL/TLS

Bùi Trọng Tùng,
Viện Công nghệ thông tin và Truyền thông,
Đại học Bách khoa Hà Nội

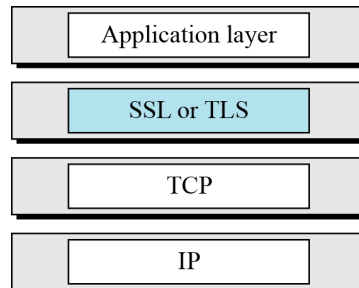
15

15

SSL/TLS là gì?

Secure Socket Layer/Transport Layer
Security

- Nằm giữa các giao thức tầng giao vận và tầng ứng dụng
- Cung cấp các cơ chế mã mật và xác thực cho dữ liệu trao đổi giữa các ứng dụng
- Các phiên bản: SSL 1.0, SSL 2.0, SSL 3.0, TLS 1.0 (phát triển từ SSL 3.0)
- Sử dụng giao thức tầng giao vận TCP
- DTLS: Phiên bản tương tự trên nền giao thức UDP



16

16

SSL và các giao thức tầng ứng dụng

- HTTPS = HTTP + SSL/TLS: cổng 443
- IMAP4 + SSL/TLS: Cổng 993
- POP3 + SSL/TLS: Cổng 995
- SMTP + SSL/TLS: Cổng 465
- FTPS = FTP + SSL/TLS: Cổng 990 và 989

17

17

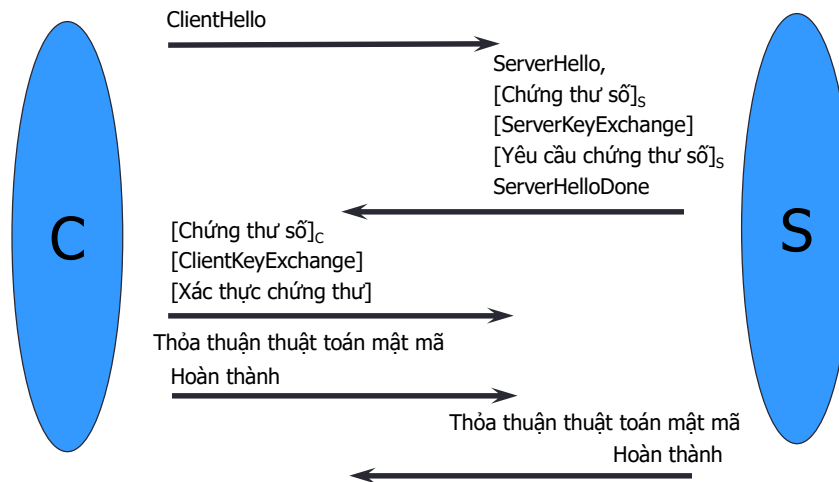
SSL/TLS là gì?

- Gồm 2 giao thức con
- Giao thức bắt tay(handshake protocol): thiết lập kết nối SSL/TLS
 - Sử dụng các phương pháp mật mã khóa công khai để các bên trao đổi khóa bí mật
- Giao thức bảo vệ dữ liệu(record protocol)
 - Sử dụng khóa bí mật đã trao đổi ở giao thức bắt tay để bảo vệ dữ liệu truyền giữa các bên

18

18

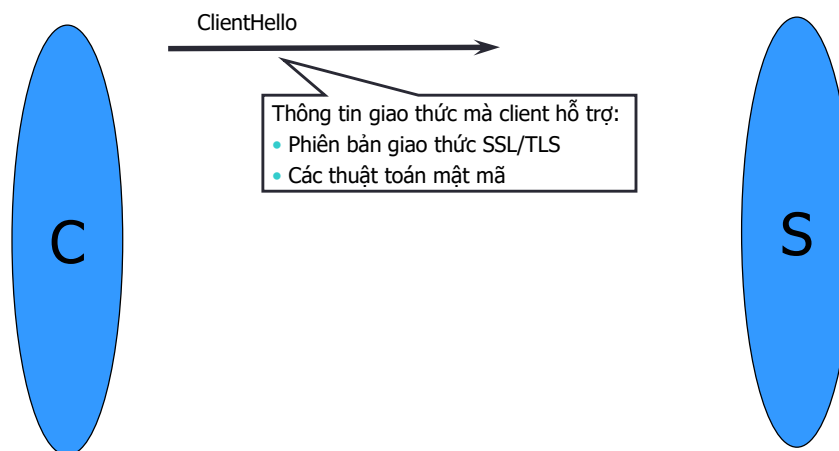
Giao thức bắt tay



19

19

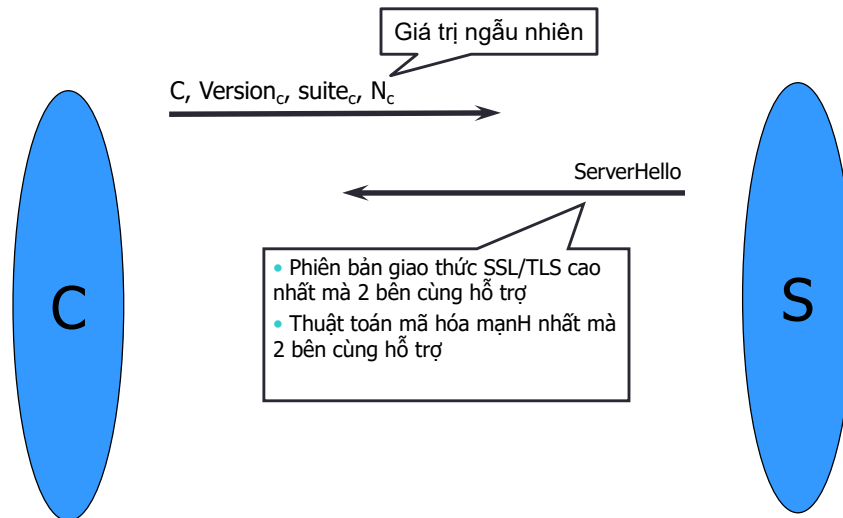
Client Hello



20

20

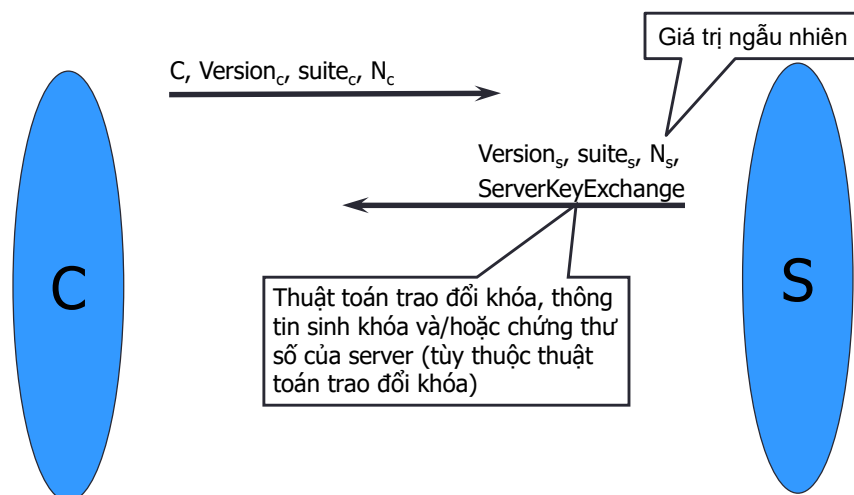
Server Hello



21

21

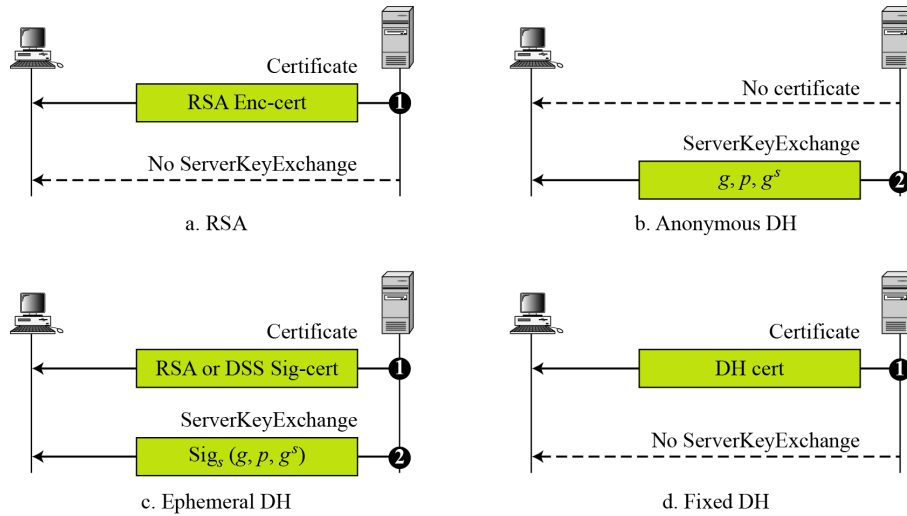
ServerKeyExchange



22

22

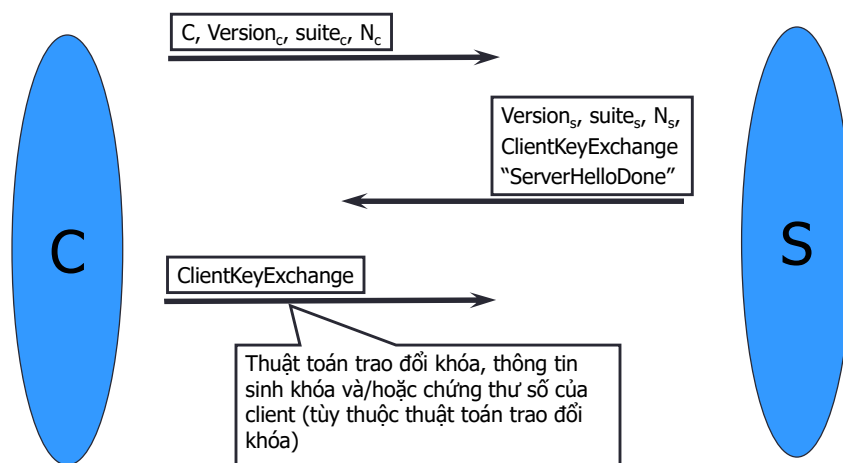
ServerKeyExchange



23

23

ClientKeyExchange

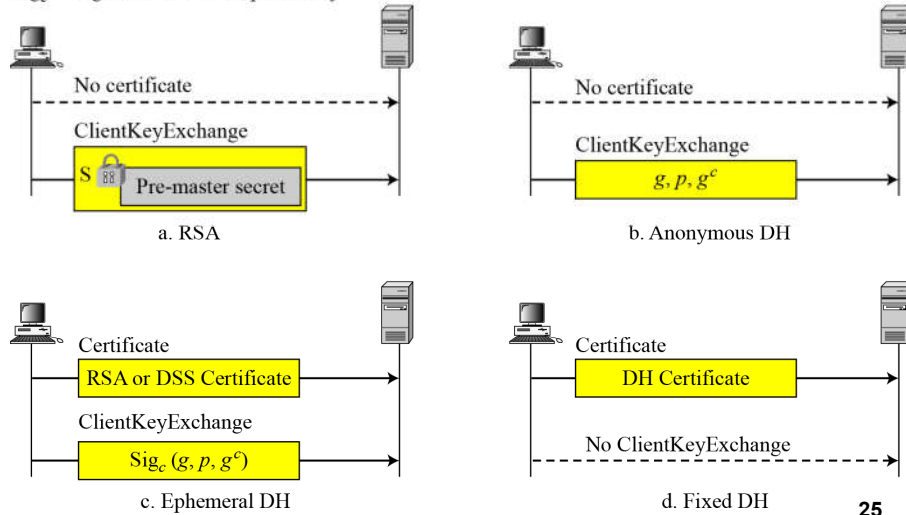


24

24

ClientKeyExchange

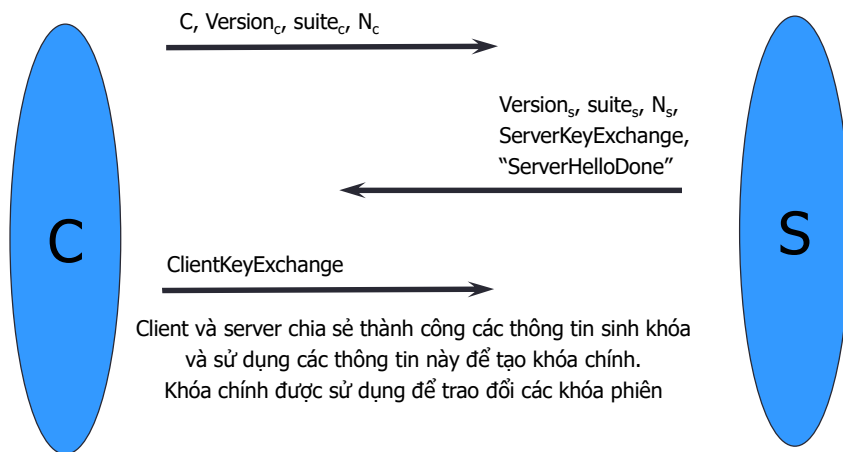
S encrypted with server's public key
 Sig_c: Signed with client's public key



25

25

Hoàn tất giao thức bắt tay



26

26

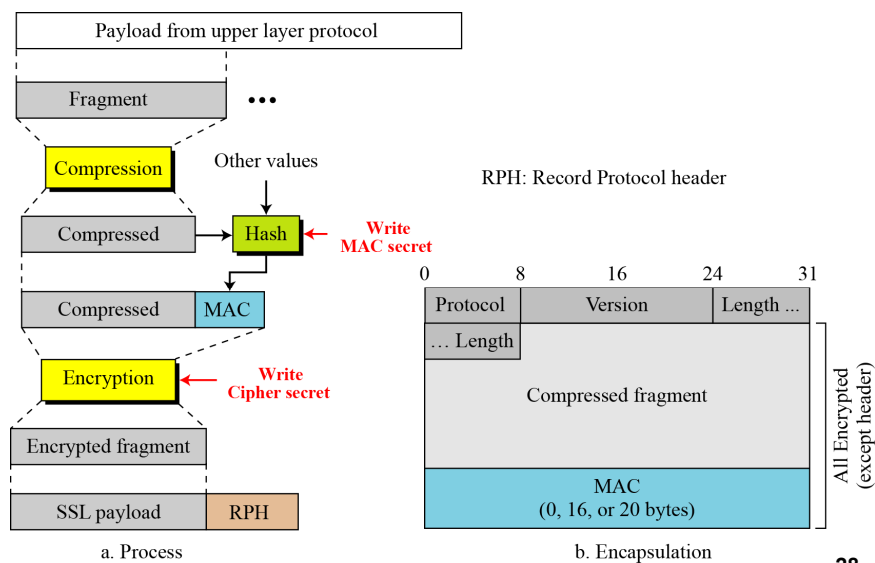
Các bộ thuật toán mã hóa trên TLS 1.0

Cipher suite	Key Exchange	Encryption	Hash
TLS_NULL_WITH_NULL_NULL	NULL	NULL	NULL
TLS_RSA_WITH_NULL_MD5	RSA	NULL	MD5
TLS_RSA_WITH_NULL_SHA	RSA	NULL	SHA-1
TLS_RSA_WITH_RC4_128_MD5	RSA	RC4	MD5
TLS_RSA_WITH_RC4_128_SHA	RSA	RC4	SHA-1
TLS_RSA_WITH_IDEA_CBC_SHA	RSA	IDEA	SHA-1
TLS_RSA_WITH_DES_CBC_SHA	RSA	DES	SHA-1
TLS_RSA_WITH_3DES_EDE_CBC_SHA	RSA	3DES	SHA-1
TLS_DH_anon_WITH_RC4_128_MD5	DH_anon	RC4	MD5
TLS_DH_anon_WITH_DES_CBC_SHA	DH_anon	DES	SHA-1
TLS_DH_anon_WITH_3DES_EDE_CBC_SHA	DH_anon	3DES	SHA-1
TLS_DHE_RSA_WITH_DES_CBC_SHA	DHE_RSA	DES	SHA-1
TLS_DHE_RSA_WITH_3DES_EDE_CBC_SHA	DHE_RSA	3DES	SHA-1
TLS_DHE_DSS_WITH_DES_CBC_SHA	DHE_DSS	DES	SHA-1
TLS_DHE_DSS_WITH_3DES_EDE_CBC_SHA	DHE_DSS	3DES	SHA-1
TLS_DH_RSA_WITH_DES_CBC_SHA	DH_RSA	DES	SHA-1
TLS_DH_RSA_WITH_3DES_EDE_CBC_SHA	DH_RSA	3DES	SHA-1
TLS_DH_DSS_WITH_DES_CBC_SHA	DH_DSS	DES	SHA-1
TLS_DH_DSS_WITH_3DES_EDE_CBC_SHA	DH_DSS	3DES	SHA-1

27

27

Bảo vệ dữ liệu trên kênh SSL/TLS



28

28

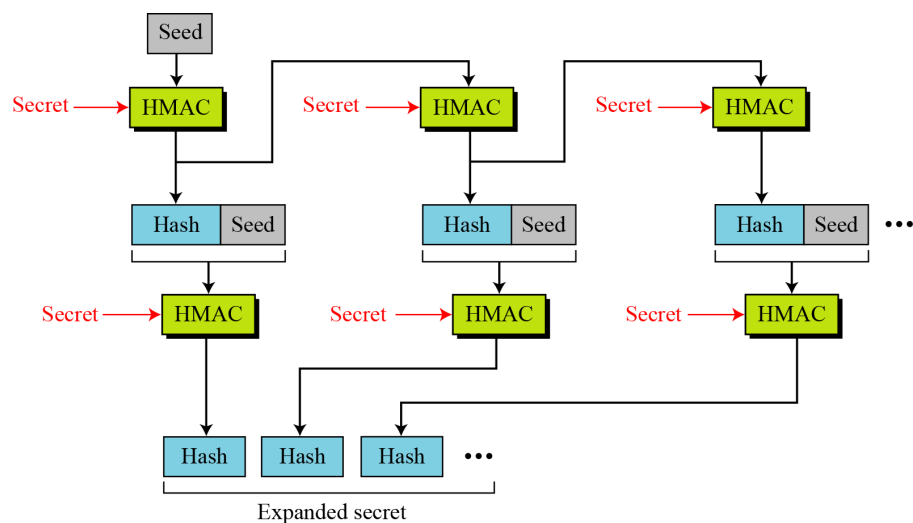
Một số cải tiến trên TLS 1.0

- Thuật toán sinh khóa an toàn hơn: sử dụng 2 hàm
 - Mở rộng giá trị bí mật
 - Hàm giả ngẫu nhiên kết hợp 2 hàm băm MD5 và SHA-1 để sinh thông tin tạo khóa
- Sử dụng các hàm HMAC thay thế cho MAC

29

29

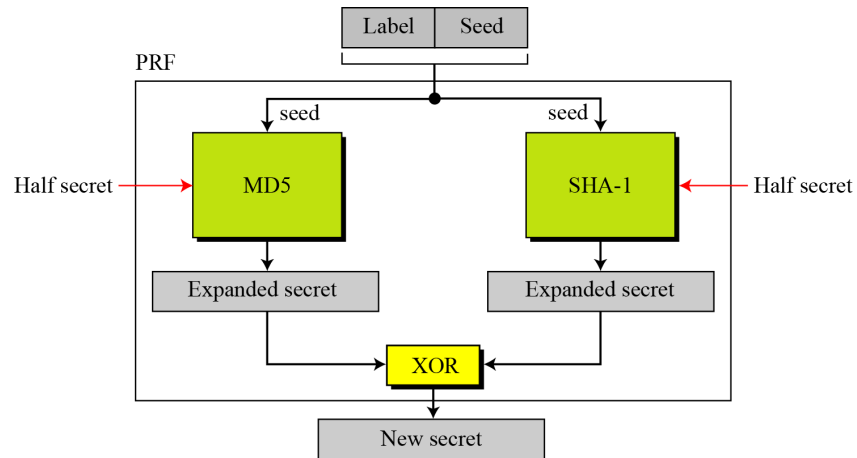
Hàm mở rộng giá trị bí mật



30

30

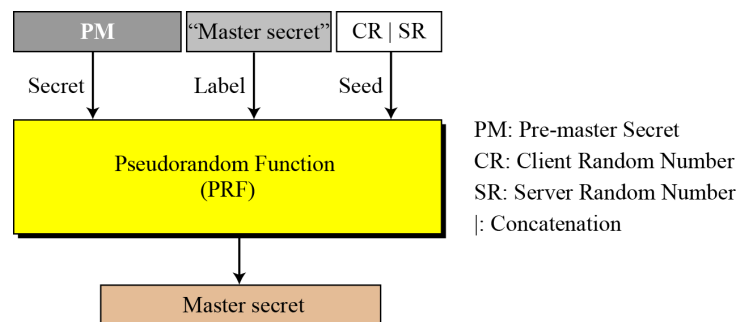
Hàm giả ngẫu nhiên PRF



31

31

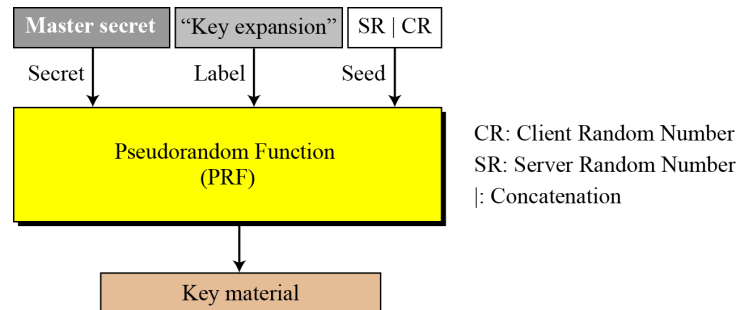
Sinh giá trị master-secret



32

32

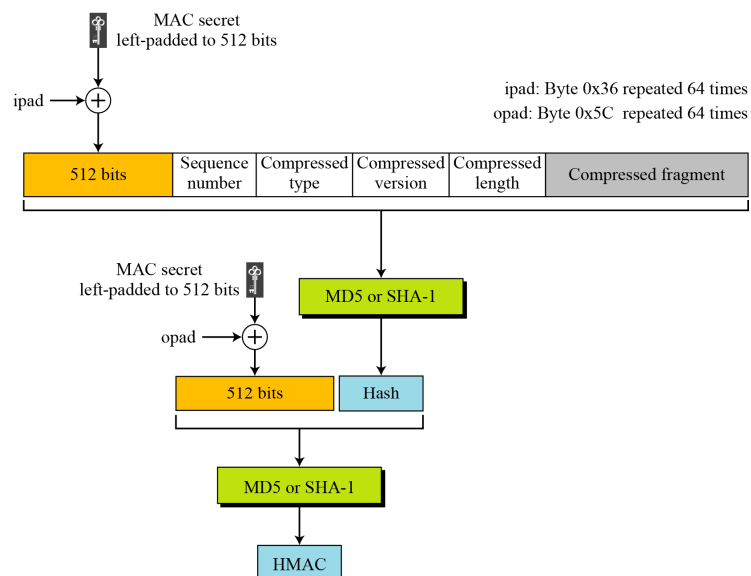
Sinh thông tin tạo khóa



33

33

Hàm HMAC trong TLS 1.0

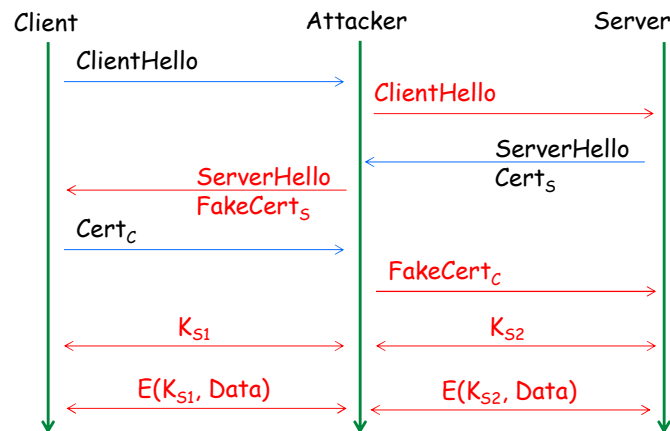


34

34

Tấn công man-in-the-middle

- Lợi dụng lỗ hổng các bên không kiểm tra tính hợp lệ của chứng thư số
- Kịch bản:



35

35

3. GIAO THỨC SSH

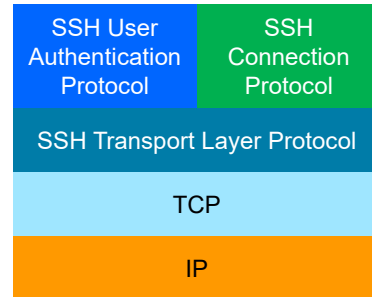
Bùi Trọng Tùng,
Viện Công nghệ thông tin và Truyền thông,
Đại học Bách khoa Hà Nội

36

36

SSH là gì?

- Secure Shell: nằm trên tầng ứng dụng
- Phiên bản hiện tại: SSH2 (RFC4250 đến RFC 4256)
- Gồm 3 giao thức con:
 - SSH Transport Layer Protocol: cung cấp kết nối xác thực, bảo mật
 - SSH User Auth. Protocol: Xác thực phía client với server
 - SSH Connection Protocol: dồn kênh truyền dữ liệu bí mật trên kết nối SSH

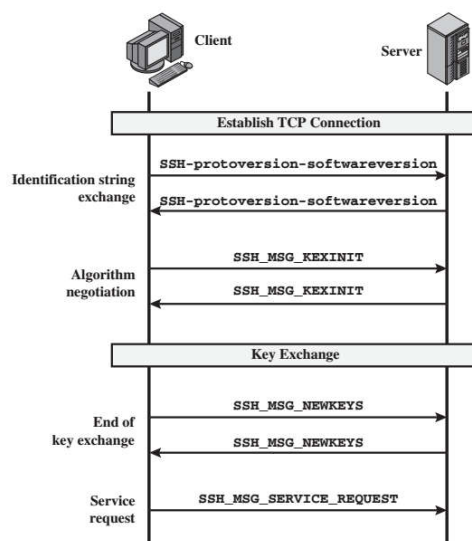


37

37

Transport Layer Protocol

- Xác thực server dựa trên chứng chỉ số
- Client duy trì bảng ánh xạ địa chỉ server và chứng chỉ số của server đó
- Trao đổi khóa: sử dụng giao thức trao đổi khóa IKE dựa trên sơ đồ Diffie-Hellman (RFC 2409)

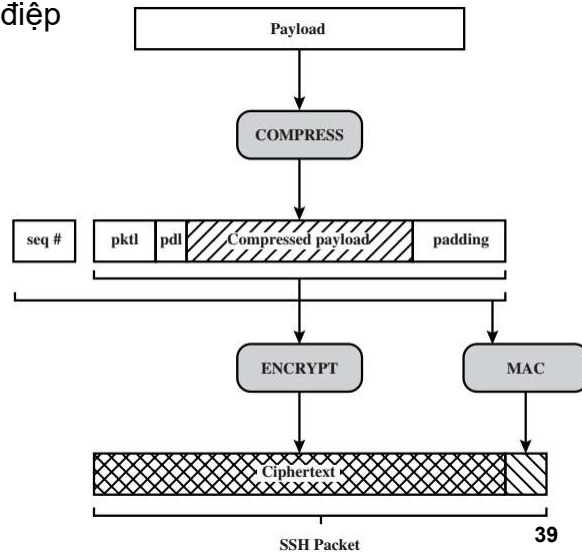


38

38

Transport Layer Protocol

- Khuôn dạng thông điệp



39

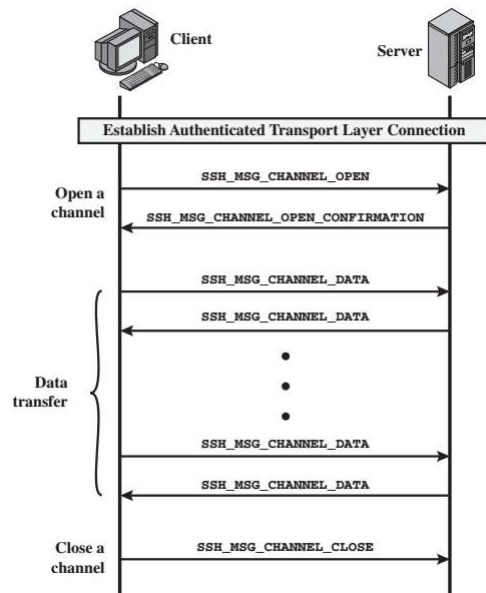
SSH User Authentication Protocol

- B1: Client gửi thông điệp MSG_USERAUTH_REQUEST với thông tin tài khoản và phương pháp xác thực đề nghị
- B2: Server kiểm tra tài khoản người dùng. Nếu không hợp lệ gửi thông điệp MSG_USERAUTH_FAILURE. Ngược lại chuyển sang bước 3
- B3: Server gửi MSG_USERAUTH_FAILURE nếu không hỗ trợ phương pháp xác thực mà client yêu cầu kèm theo danh sách các phương pháp mà server đề nghị
- B4: Client lựa chọn phương pháp xác thực mà server hỗ trợ và gửi lại MSG_USERAUTH_REQUEST
- B5: Nếu xác thực thành công và cần thêm các bước xác thực khác, quay lại bước 3
- B6: Server gửi thông điệp MSG_USERAUTH_SUCCESS báo xác thực thành công

40

40

SSH Connection Protocol



41

41

An toàn bảo mật giao thức SSH

- Lỗi hổng: client không kiểm tra đầy đủ tính hợp lệ của chứng chỉ mà server cung cấp
- Nguy cơ: giả mạo sever và tấn công man-in-the-middle
 - Tương tự nguy cơ trên giao thức SSL/TLS

42

42

3. GIAO THỨC BẢO MẬT WLAN

Bùi Trọng Tùng,
Viện Công nghệ thông tin và Truyền thông,
Đại học Bách khoa Hà Nội

43

43

Coffee Shop

WPA/WPA2:

- **Xác thực:** Tùy thuộc chế độ
- **WPA:** Mã hóa bằng RC4, 128 bit
- **WPA2:** Mã hóa bằng AES-128



SSID: WifiStation
password: guessme!



44

44

Coffee Shop

WPA2 Personal



SSID: WifiStation
password: guessme!



WifiStation
Connecting

Enter the network security key

guessme!

Next
Cancel

Kích thước khóa

Số vòng lặp

Laptop và AP cùng tính toán:

$$K = \text{PBKDF2}(\text{HMAC-SHA-1}, \text{password}, \text{SSID}, \text{SSID_length}, 4096, 256)$$

45

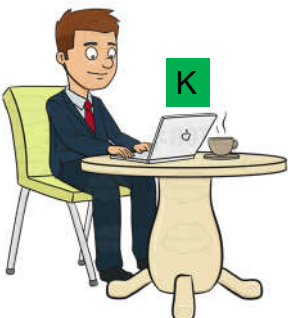
45

Coffee Shop

WPA2 Personal



SSID: WifiStation
password: guessme!



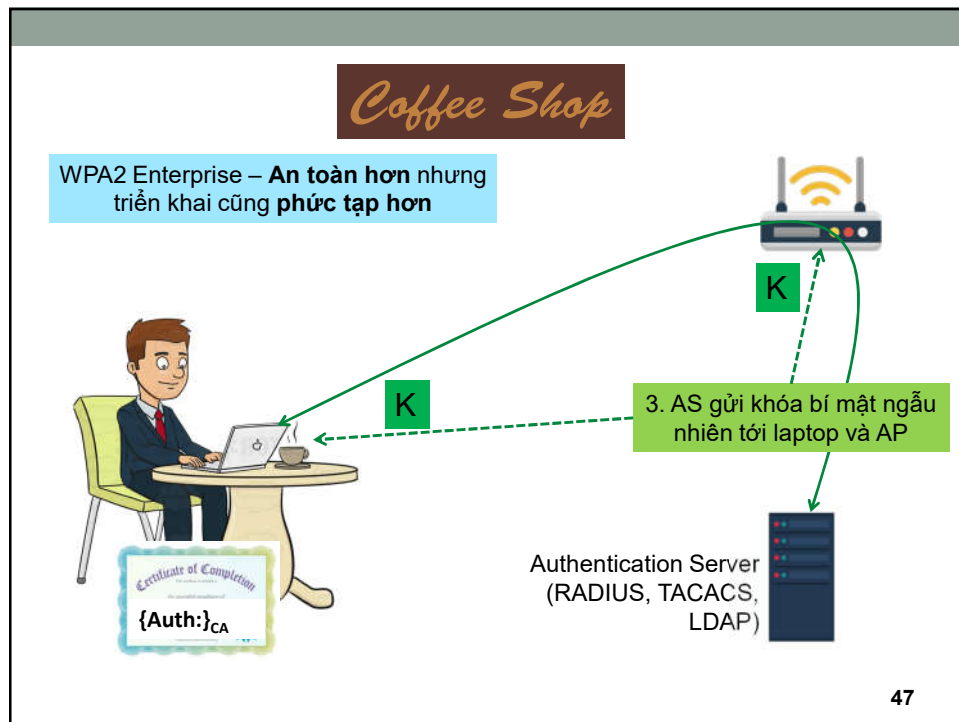
K

K

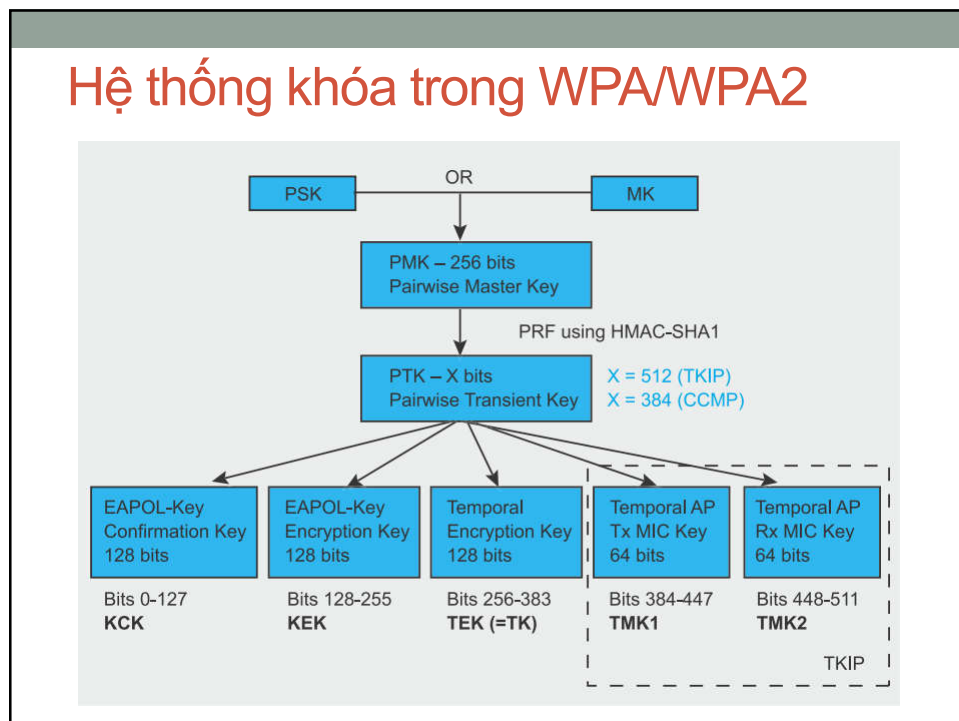
Laptop và AP cùng chia sẻ giá trị bí mật K. Giá này được sử dụng để sinh khóa dùng cho quá trình mã hóa và xác thực dữ liệu trao đổi giữa 2 bên

46

46



47



48

Hệ thống khóa trong WPA/WPA2

- PSK(Pre-shared Key): khóa được sinh từ mật khẩu chia sẻ trước
- MK(Master Key): khóa do máy chủ RADIUS, phân phối cho MS và AP
- PMK(Pairwise Master Key): khóa dùng để phân phối các khóa phiên:
 - WPA/WPA2 Personal: PMK = PSK
 - WPA/WPA2 Enterprise: PMK = MK
- PTK (Pairwise Transient Key): bộ khóa phiên gồm các khóa KCK, KEK, TK, TMK dùng cho truyền thông unicast
- GTK: bộ khóa phiên dùng cho truyền thông multicast

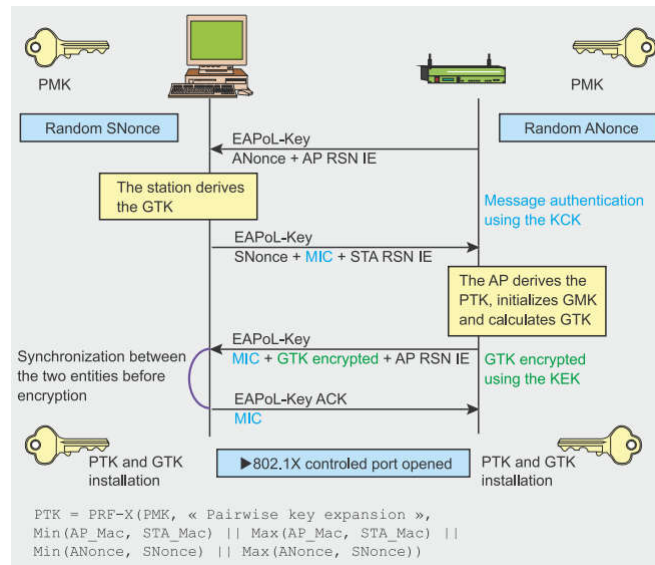
49

Hệ thống khóa trong WPA/WPA2

- KCK(Key Confirmation Key): khóa dùng để xác thực khi bắt tay 4 bước phân phối khóa PTK và GTK
- KEK(Key Confirmation Key): khóa dùng để mã hóa bảo mật khi bắt tay 4 bước phân phối khóa PTK và GTK
- TK/TEK (Temporary Key/Temporary Encryption Key): khóa dùng để mã hóa bảo mật của dữ liệu trong giao thức TKIP(WPA) và CCMP(WPA2)
 - Trong WPA2, TEK còn được sử dụng để xác thực dữ liệu
- TMK(Temporary MIC Key): khóa dùng để xác thực dữ liệu trong TKIP

50

Phân phối khóa PTK và GTK



51

Phân phối khóa PTK và GTK

- Sử dụng các thông điệp EAPoL-Key(EAP over LAN)
- Bước 1.
 - AP khởi tạo ngẫu nhiên giá trị ANonce
 - Gửi ANonce cho Client
- Bước 2.
 - Client khởi tạo giá trị ngẫu nhiên SNonce
 - Khởi tạo MIC và gửi cho AP.
 - Sử dụng PMK, SNonce, ANonce, MAC của Client và AP để tính toán PTK.

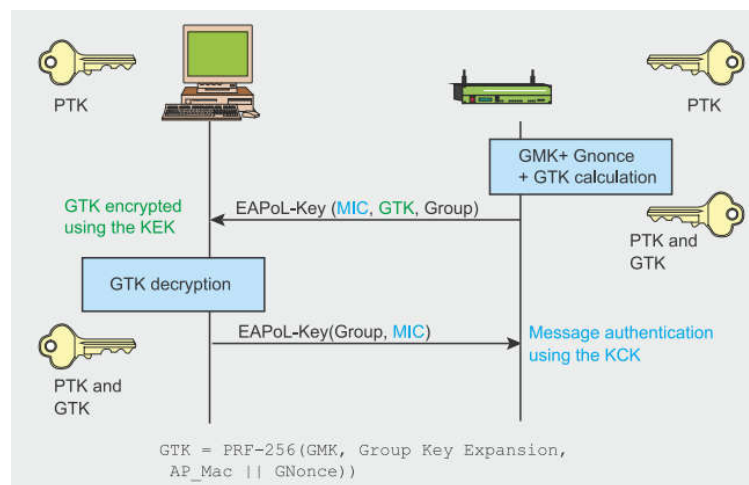
52

Phân phối khóa PTK và GTK

- Bước 3.
 - Dựa vào PMK, ANonce, MAC của Client và AP, và S Nonce vừa nhận được, AP tính toán PTK.
 - Xác thực MIC.
 - Khởi tạo GMK để tính toán GTK (128 bit với CCMP).
 - Tạo MIC mới. Gửi MIC và GTK cho Client
- Bước 4.
 - Báo cáo hoàn thành kết nối.
 - Client cài đặt GTK, tính toán giá trị MIC để chắc chắn rằng AP biết PMK.
- **Chú ý:** Khóa GTK sẽ được làm mới bởi quá trình Group Key Handshake.

53

Làm mới khóa GTK



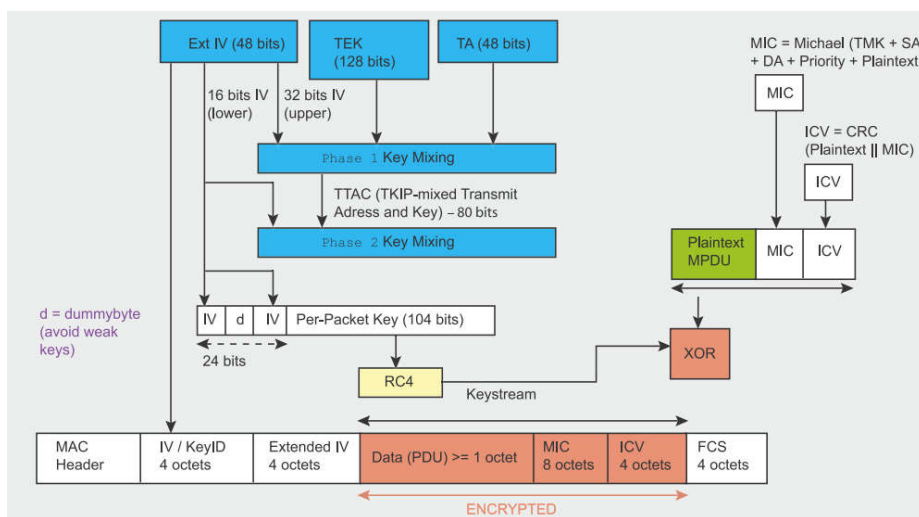
54

Làm mới khóa GTK

- Bước 1.
 - AP khởi tạo ngẫu nhiên Gnonce, cộng với GMK đã có, tính toán GTK mới, được mã hóa lại bằng KEK.
 - Gửi giá trị GTK, MIC tới AP.
- Bước 2.
 - Client giải mã GTK, xác thực MIC.
 - Gửi giá trị MIC cho AP.
 - Sau khi xác thực MIC thành công, AP cài đặt GTK mới.

55

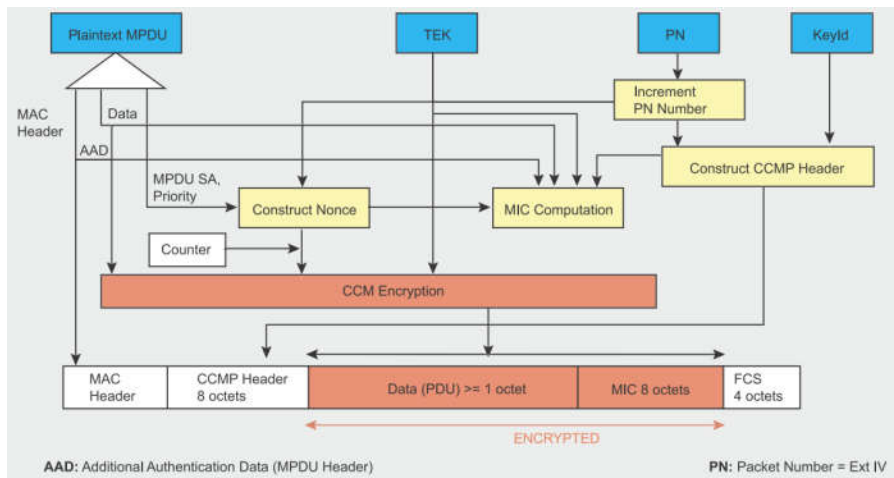
Option 1: Trộn khóa và mã hóa TKIP



56

56

Option 2: Mã hóa CCMP



57