BÀI 6.
AN TOÀN BẢO MẬT TRONG MẠNG TCP/IP

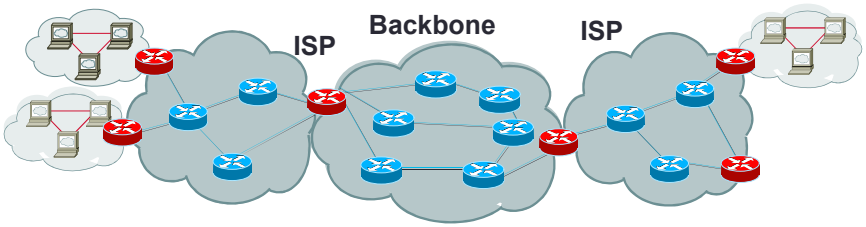
Bùi Trọng Tùng,
Viện Công nghệ thông tin và Truyền thông,
Đại học Bách khoa Hà Nội

Nội dung

- Tổng quan về mạng máy tính
- An toàn bảo mật tầng vật lý
- An toàn bảo mật tầng liên kết dữ liệu
- An toàn bảo mật tầng mạng
- An toàn bảo mật tầng giao vận
- An toàn bảo mật tầng ứng dụng

1. Tổng quan về mạng máy tính

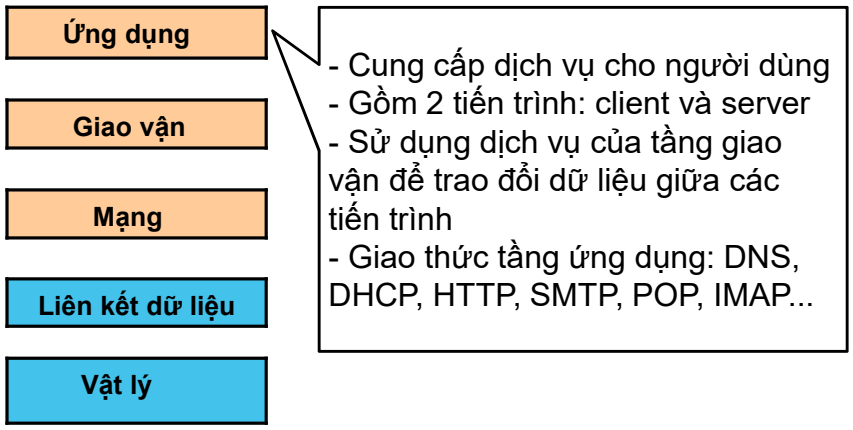
- Mạng máy tính là gì?
- Giao thức?
- Hạ tầng mạng Internet



3

3

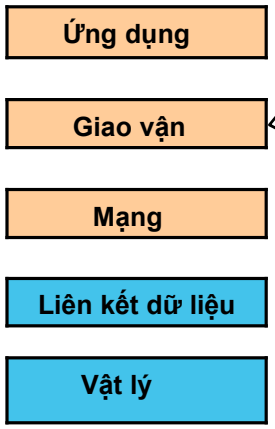
Kiến trúc phân tầng



4

4

Kiến trúc phân tầng (tiếp)

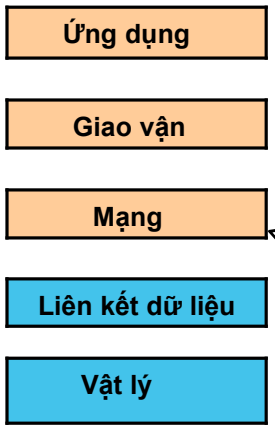


- Điều khiển quá trình truyền dữ liệu giữa các tiến trình.
- Dồn kênh/Phân kênh: số hiệu cổng dịch vụ
- TCP: hướng liên kết, tin cậy, truyền theo dòng byte
- UDP: hướng không liên kết, truyền theo bức tin (datagram)

5

5

Kiến trúc phân tầng (tiếp)

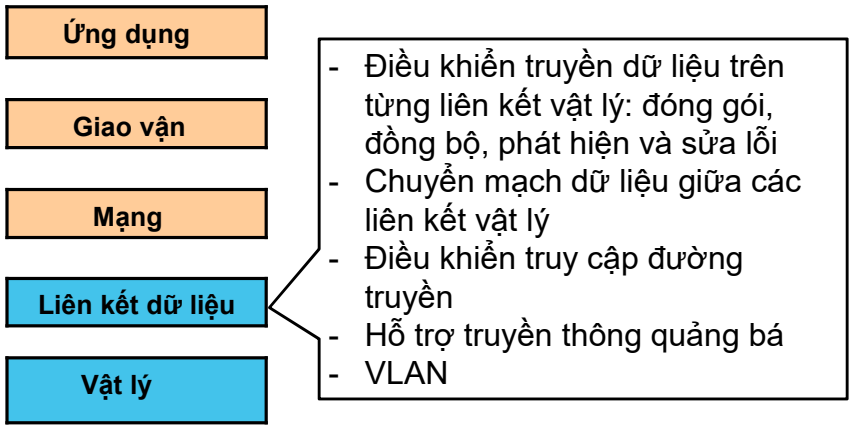


Kết nối liên mạng (Internetworking):
- Đóng gói, phân mảnh dữ liệu
- Định danh: địa chỉ IP
- Định tuyến
- Chuyển tiếp gói tin
- Đảm bảo chất lượng dịch vụ

6

6

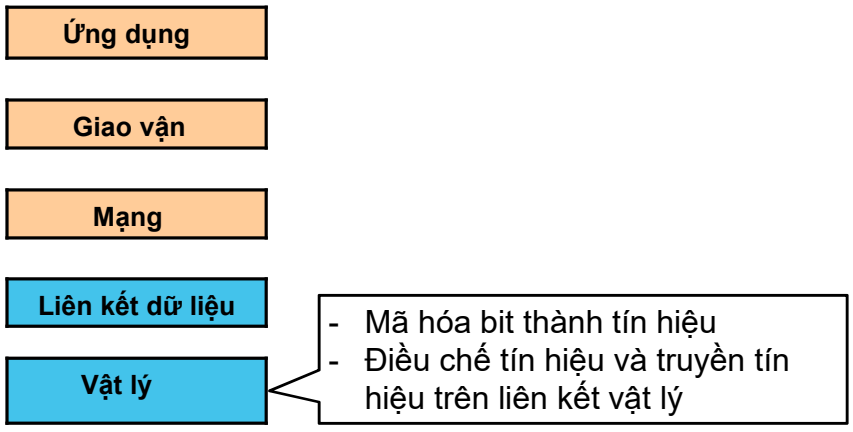
Kiến trúc phân tầng (tiếp)



7

7

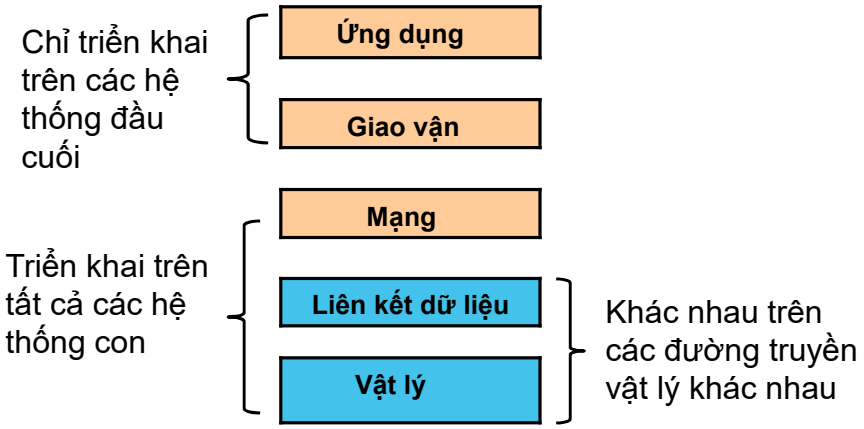
Kiến trúc phân tầng (tiếp)



8

8

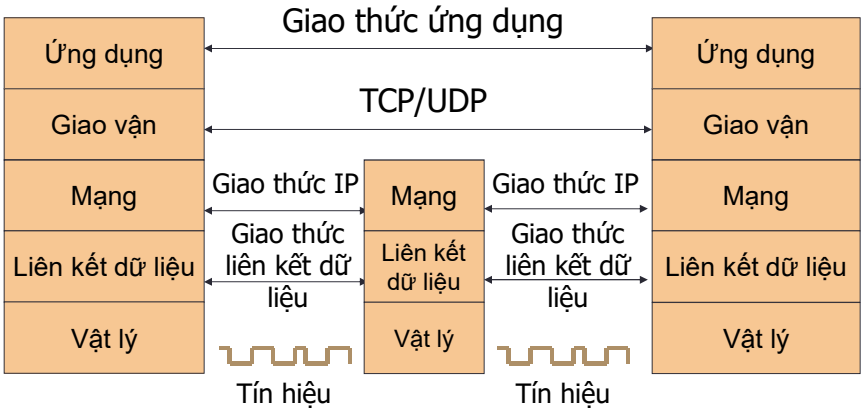
Kiến trúc phân tầng (tiếp)



9

9

Chồng giao thức (protocol stack)

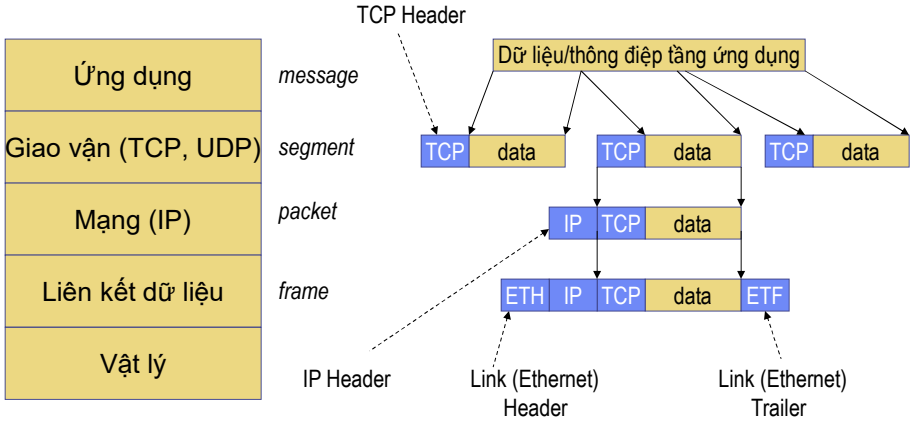


10

10

Đóng gói dữ liệu (TCP)

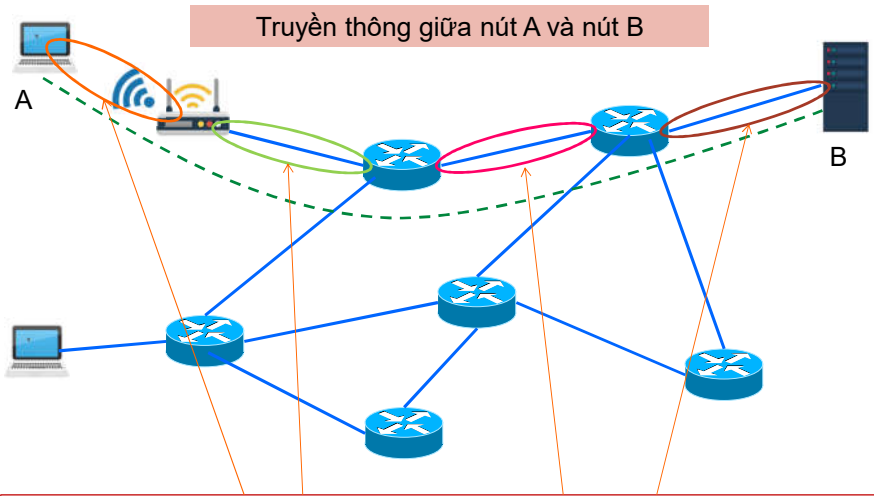
- Nút gửi: Thêm thông tin điều khiển (header)
- Nút nhận: Loại bỏ thông tin điều khiển



11

11

Hop-by-Hop vs End-to-End



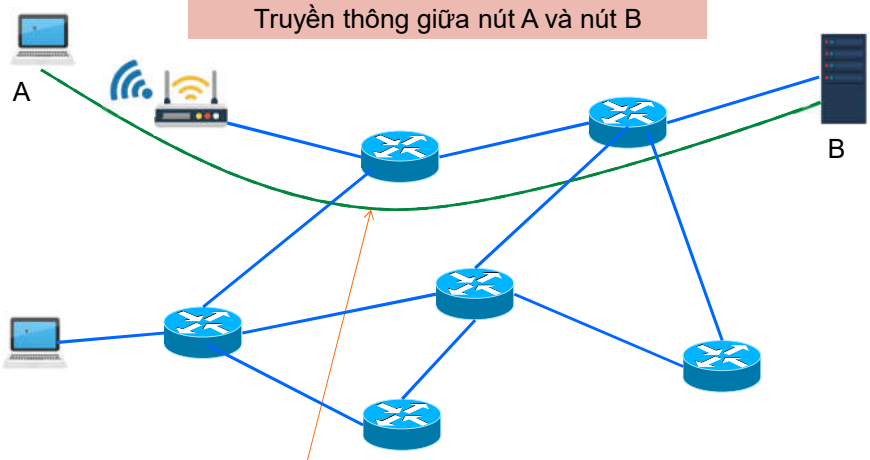
Hop-by-Hop: Lớp Vật lý và Liên kết dữ liệu có thể khác nhau

12

12

Hop-by-Hop vs End-to-End

Truyền thông giữa nút A và nút B



End-to-End: Lớp Mạng, Giao vận, Ứng dụng sử dụng giao thức giống nhau

13

13

Coffee Shop

1. Kết nối mạng WiFi

14

14

Coffee Shop

1. Kết nối mạng WiFi

Probe Response

HI, TÔI LÀ SSID.
HÃY KẾT NỐI VỚI
TÔI !!!

15

15

Coffee Shop

1. Kết nối mạng WiFi

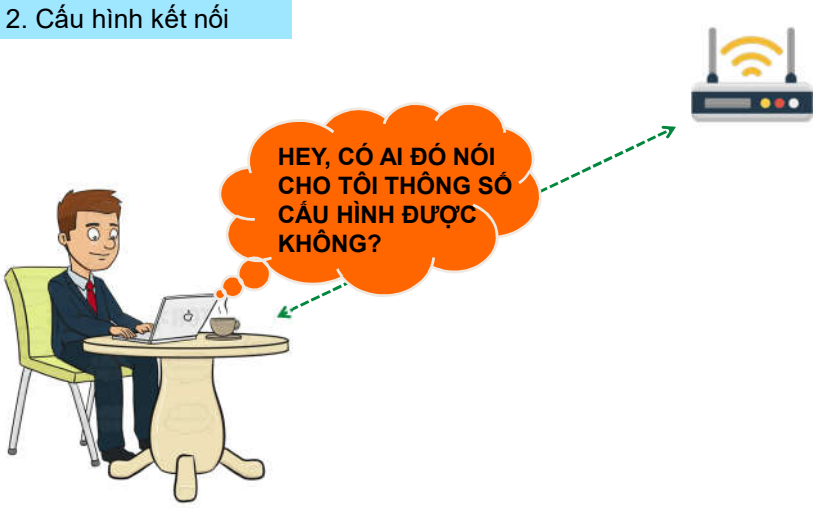
Thiết lập kết nối
(Có thể thực hiện các giao thức xác thực, mã hóa bảo vệ)

16

16

Coffee Shop

2. Cấu hình kết nối

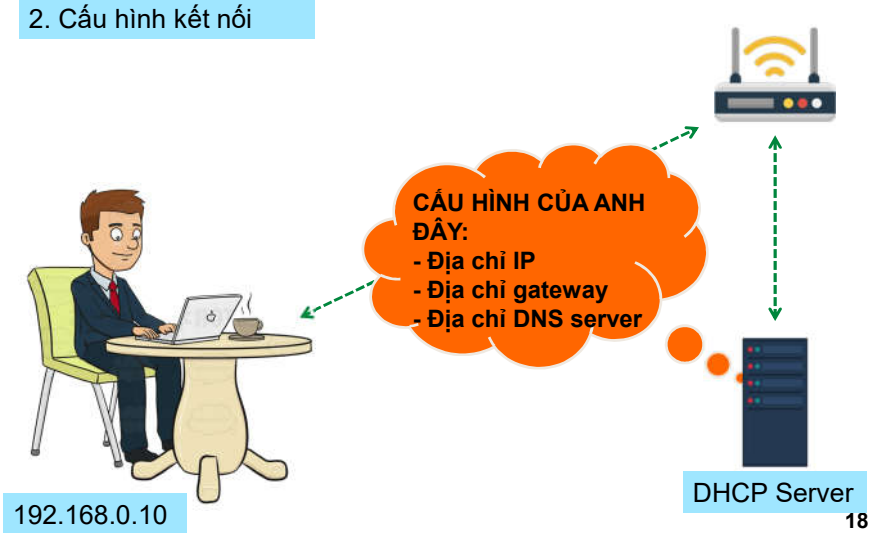


17

17

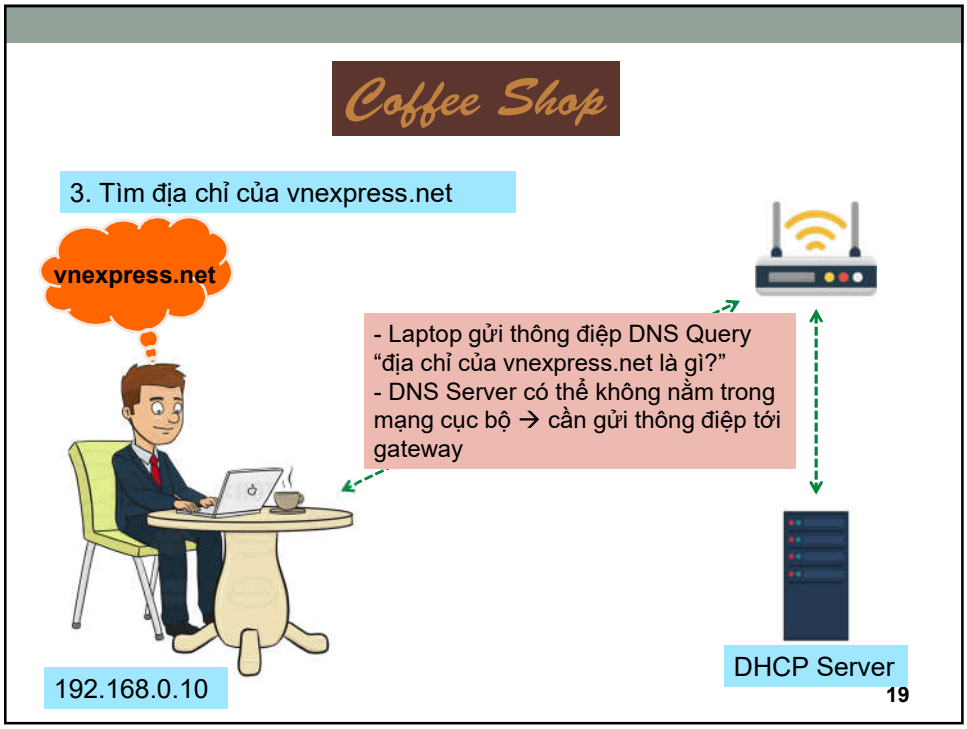
Coffee Shop

2. Cấu hình kết nối

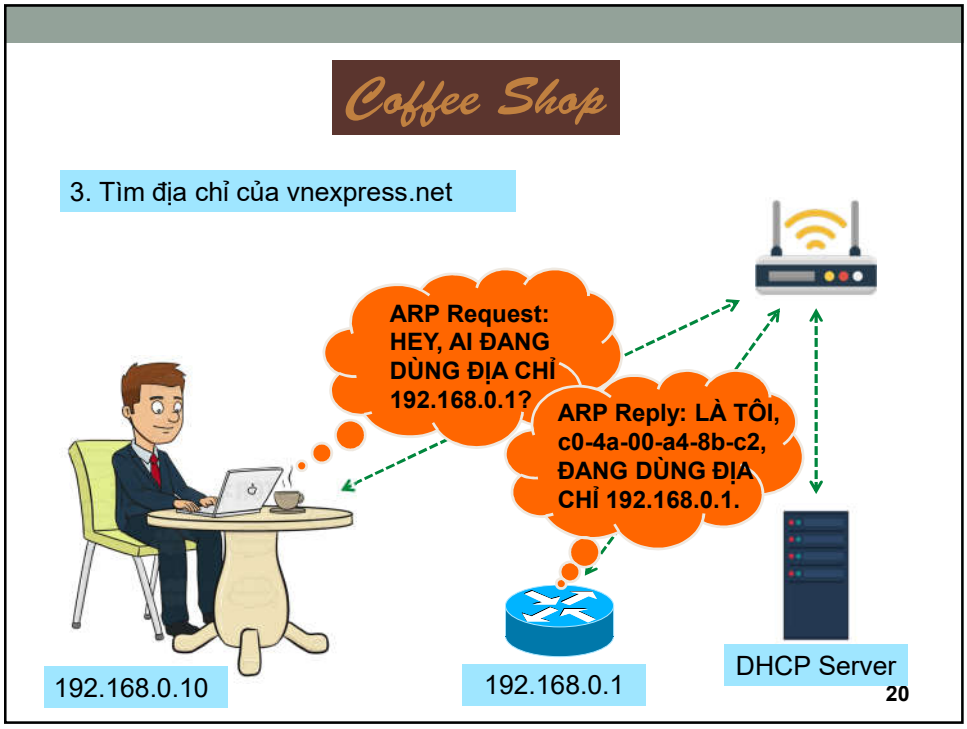


18

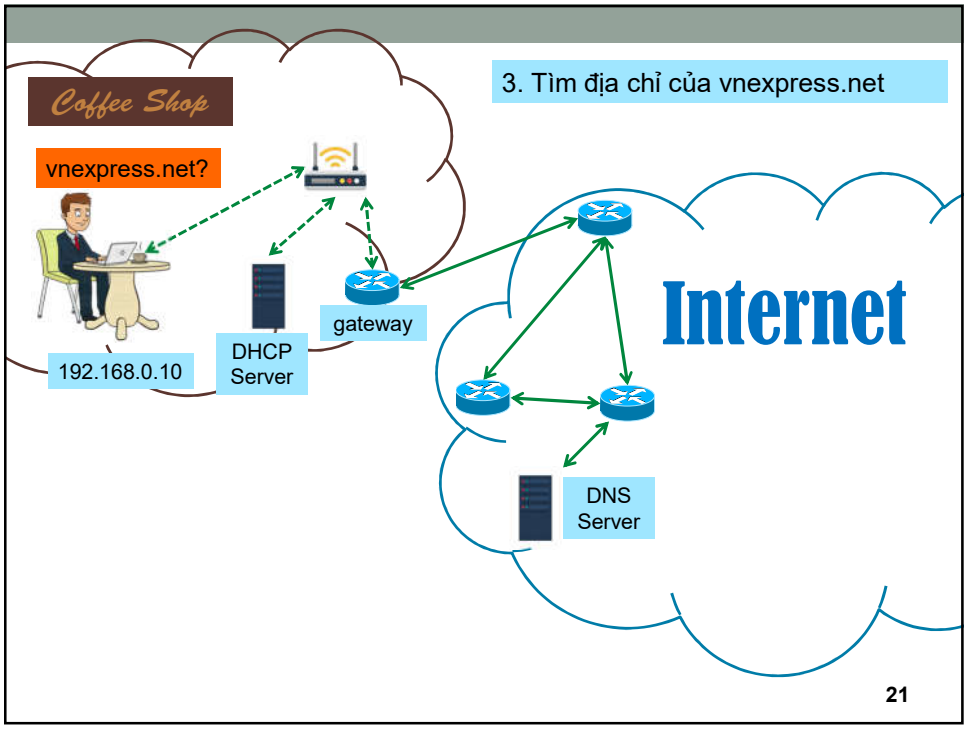
18


Coffee Shop
3. Tìm địa chỉ của vnexpress.net
vnexpress.net
- Laptop gửi thông điệp DNS Query "địa chỉ của vnexpress.net là gì?"
- DNS Server có thể không nằm trong mạng cục bộ → cần gửi thông điệp tới gateway
192.168.0.10
DHCP Server
19

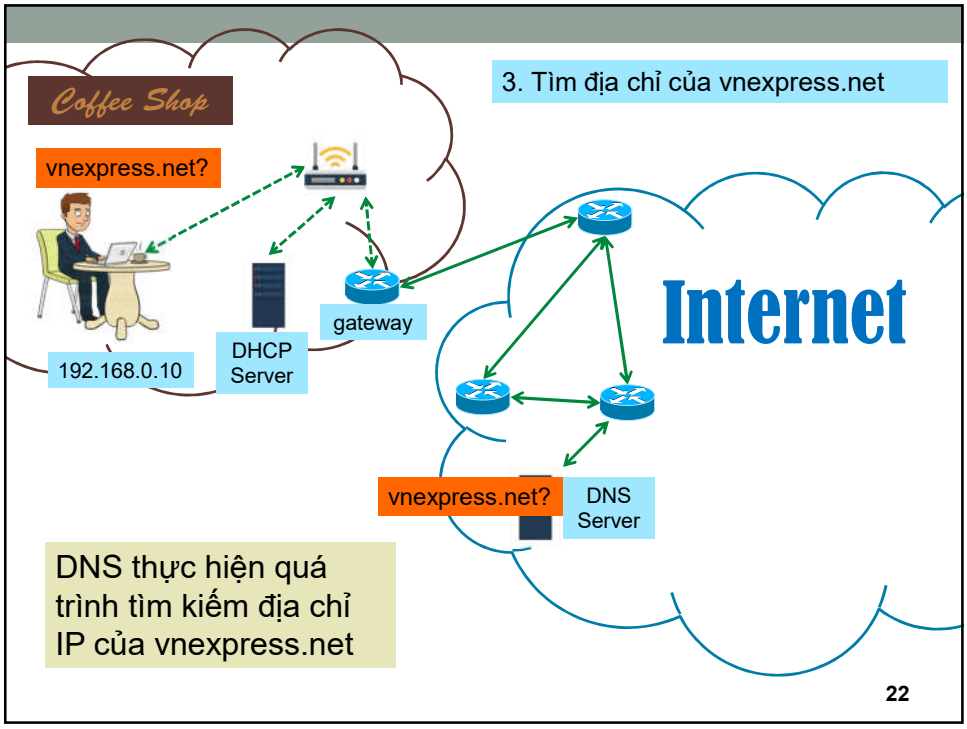
19


Coffee Shop
3. Tìm địa chỉ của vnexpress.net
ARP Request: HEY, AI ĐANG DÙNG ĐỊA CHỈ 192.168.0.1?
ARP Reply: LÀ TÔI, c0-4a-00-a4-8b-c2, ĐANG DÙNG ĐỊA CHỈ 192.168.0.1.
192.168.0.10
192.168.0.1
DHCP Server
20

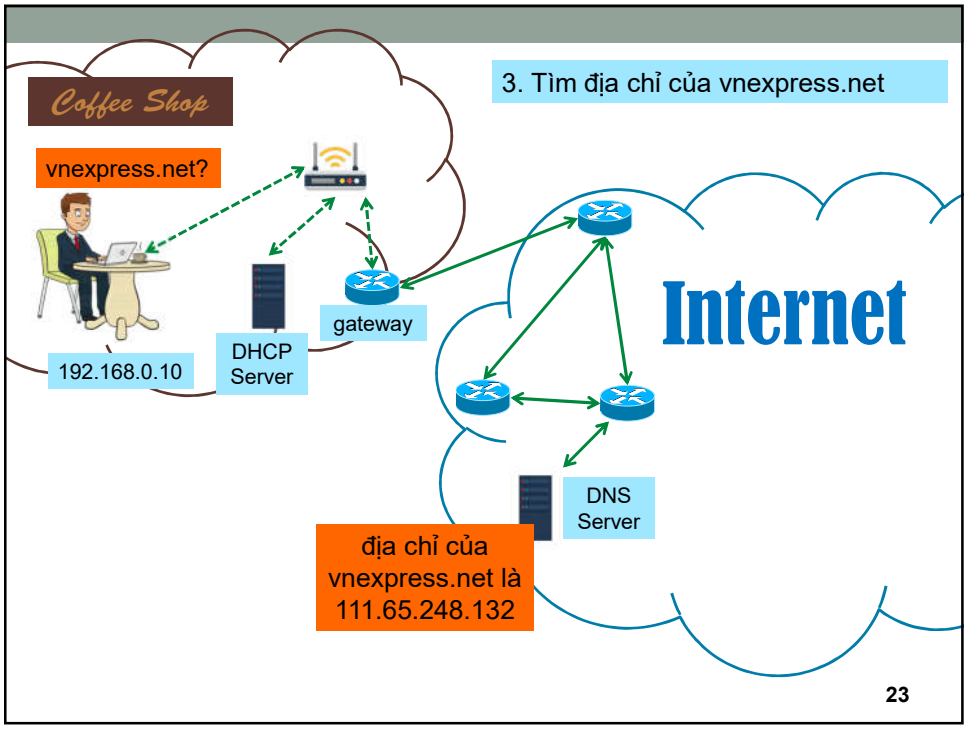
20


Coffee Shop
3. Tìm địa chỉ của vnexpress.net
vnexpress.net?
192.168.0.10
DHCP Server
gateway
Internet
DNS Server
21

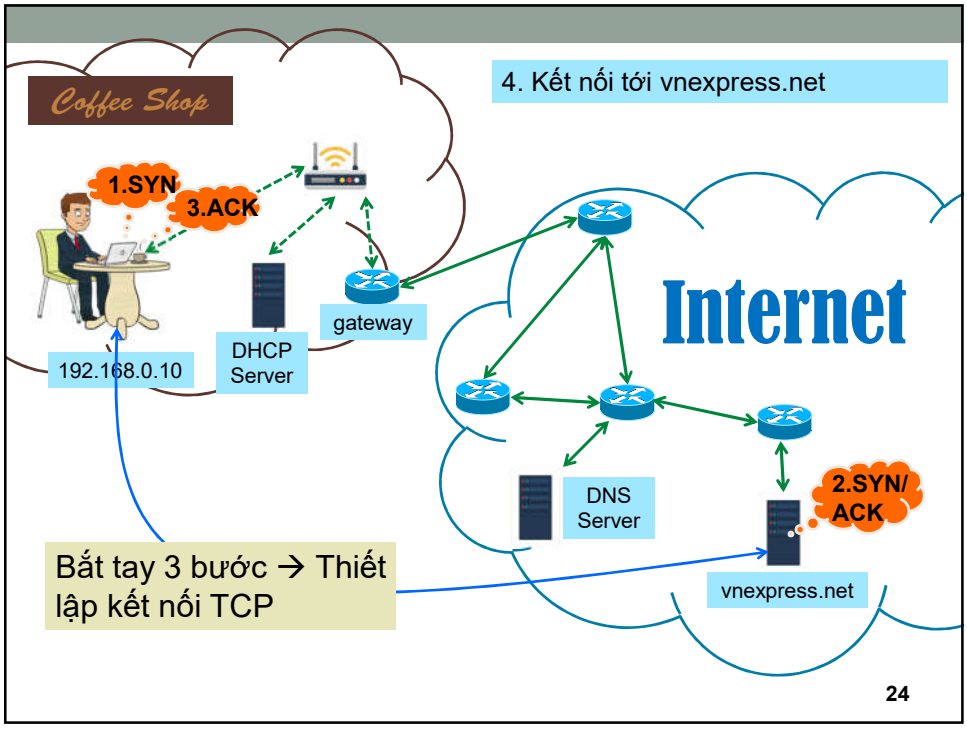
21


Coffee Shop
3. Tìm địa chỉ của vnexpress.net
vnexpress.net?
192.168.0.10
DHCP Server
gateway
Internet
vnexpress.net?
DNS Server
DNS thực hiện quá trình tìm kiếm địa chỉ IP của vnexpress.net
22

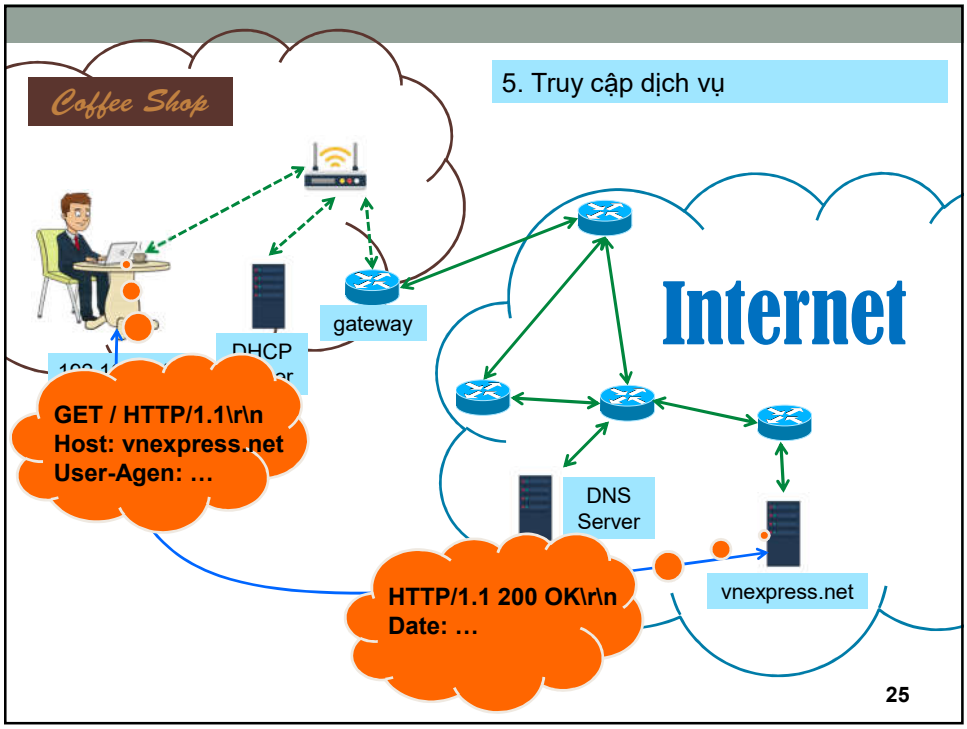
22


Coffee Shop
3. Tìm địa chỉ của vnexpress.net
vnexpress.net?
192.168.0.10
DHCP Server
gateway
Internet
DNS Server
địa chỉ của vnexpress.net là 111.65.248.132
23

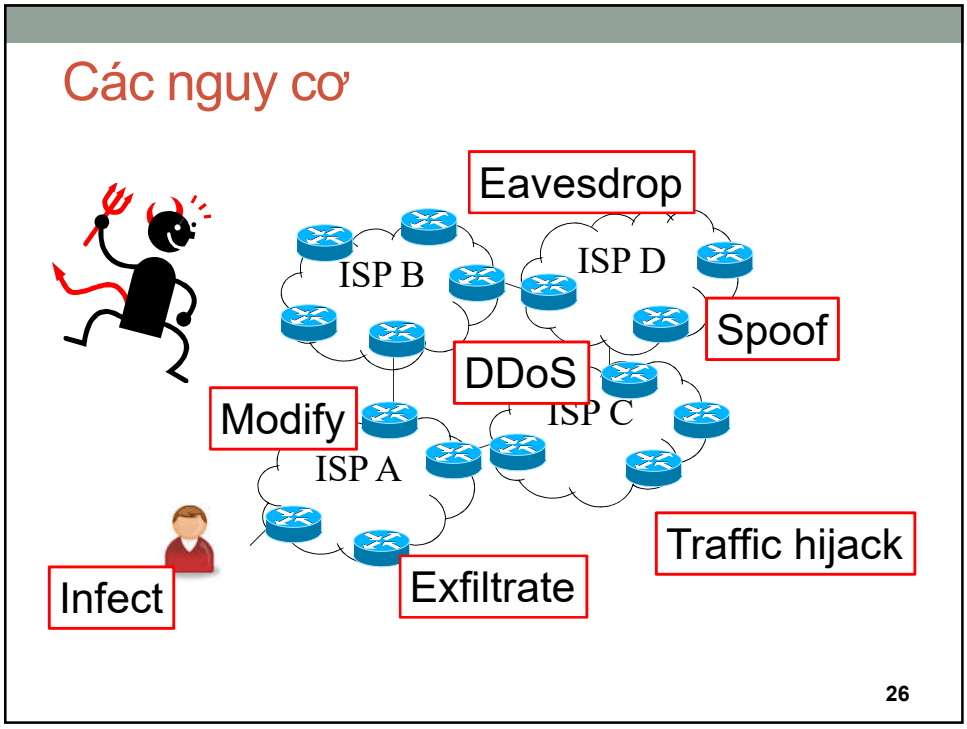
23


Coffee Shop
4. Kết nối tới vnexpress.net
1.SYN
3.ACK
192.168.0.10
DHCP Server
gateway
Internet
DNS Server
2.SYN/ ACK
vnexpress.net
Bắt tay 3 bước → Thiết lập kết nối TCP
24

24


Coffee Shop
5. Truy cập dịch vụ
gateway
DHCP
Internet
GET / HTTP/1.1\r\n
Host: vnexpress.net
User-Agen: …
DNS
Server
vnexpress.net
HTTP/1.1 200 OK\r\n
Date: …
25

25


Các nguy cơ
Eavesdrop
ISP B
ISP D
Spoof
DDoS
Modify
ISP C
ISP A
Traffic hijack
Infect
Exfiltrate
26

26

Những khó khăn với bài toán ATBM mạng máy tính (nhắc lại)

- Hệ thống mở
- Tài nguyên phân tán
- Người dùng ẩn danh
- TCP/IP được không được thiết kế để đối mặt với các nguy cơ ATBM
  - Không xác thực các bên
  - Không xác thực, giữ bí mật dữ liệu trong gói tin

27

27

"On the Internet, nobody knows you're a dog."

28

28

2. AN TOÀN BẢO MẬT TẦNG VẬT LÝ VÀ TẦNG LIÊN KẾT DỮ LIỆU

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

29

29

Các nguy cơ tấn công

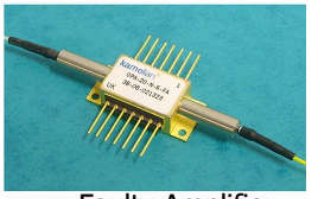
- Nghe lén:
  - Với các mạng quảng bá (WiFi, mạng hình trục, mạng sao dùng hub): dễ dàng chặn bắt các gói tin
  - Với các mạng điểm-điểm:
    - Đoạt quyền điều khiển các nút mạng
    - Chèn các nút mạng một cách trái phép vào hệ thống
  - Công cụ phân tích: tcpdump, Wireshark, thư viện winpcap, thư viện lập trình Socket
- Giả mạo thông tin: tấn công vào giao thức ARP, VLAN, cơ chế tự học MAC của hoạt động chuyển mạch
- Phá hoại liên kết: chèn tín hiệu giả, chèn tín hiệu nhiễu, chèn các thông điệp lỗi...
- Thông thường tấn công vào mạng LAN do kẻ tấn công bên trong gây ra.

30

30

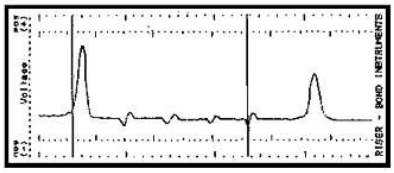
Tấn công nghe lén trên tầng vật lý

- Nghe trộm tín hiệu trên cáp đồng



Faulty Amplifier

Wire Tap

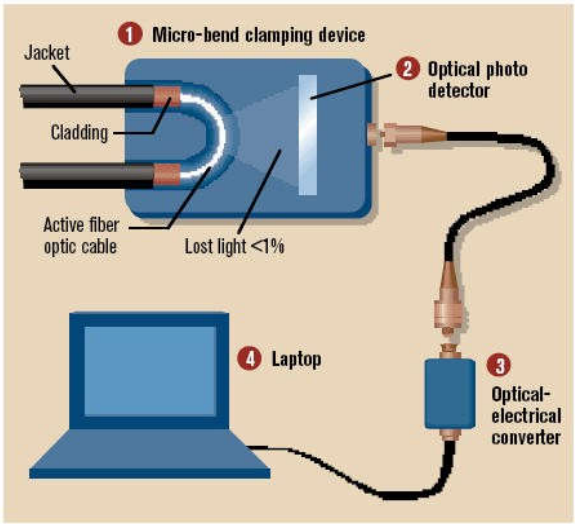


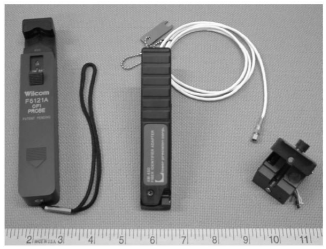
31

31

Tấn công nghe lén trên tầng vật lý

- Nghe trộm tín hiệu trên cáp quang





32

32

AN TOÀN BẢO MẬT MẠNG WLAN

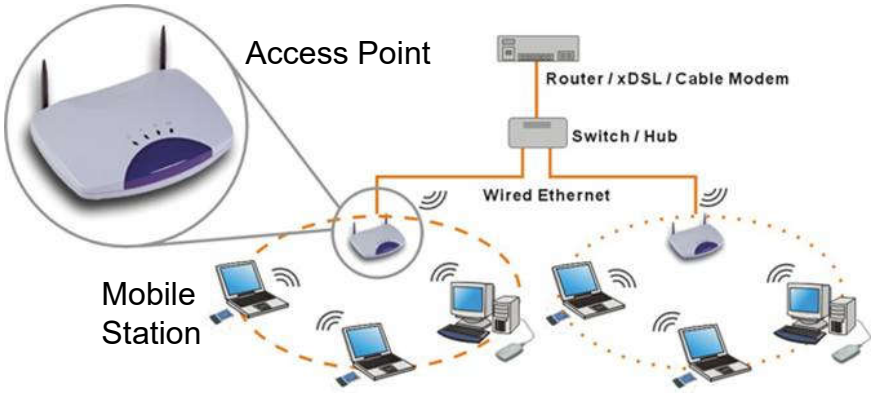
Bùi Trọng Tùng,
Viện Công nghệ thông tin và Truyền thông,
Đại học Bách khoa Hà Nội

Giới thiệu chung

- WLAN (Wireless Local Area Network) là mạng máy tính liên kết 2 hay nhiều thiết bị sử dụng môi trường truyền dẫn vô tuyến
- Chuẩn IEEE 802.11 gốc chính thức được ban hành năm 1997
- IEEE 802.11x (chuẩn WiFi) biểu thị một tập hợp các chuẩn WLAN được phát triển bởi ủy ban chuẩn hóa IEEE LAN/MAN (IEEE 802.11)
  - IEEE802.11a, IEEE802.11b, IEEE802.11g, IEEE802.11n các chuẩn quy định hạ tầng và công nghệ truyền dẫn
  - IEEE802.11i: chuẩn quy định về các giao thức bảo mật trong WLAN
  - …
- IEEE802.1X: điều khiển truy cập cho WLAN

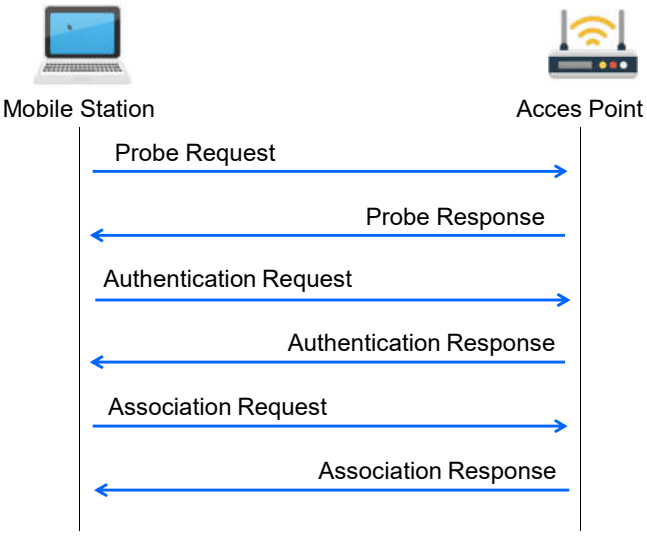
Cấu trúc của WLAN

- Một WLAN thông thường gồm có 2 phần: các thiết bị truy nhập không dây (Mobile Station-MS), các điểm truy nhập (Access Points – AP).



35

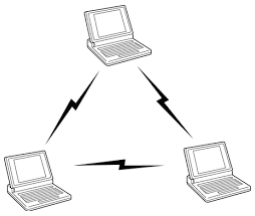
Giao thức kết nối mạng WLAN



36

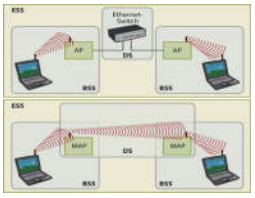
36

Các mô hình triển khai



Ad-hoc
- Không cần AP
- Kết nối ngang hàng

BSS
- Kết nối tập trung



ESS
- Kết nối tập trung
- Mở rộng bằng cách kết nối các BSS

37

Vấn đề ATBM trên mạng không dây

- Sử dụng sóng vô tuyến để truyền dẫn dữ liệu

→dễ dàng có thể thu bắt sóng và phân tích để lấy dữ liệu

→dễ dàng kết nối và truy cập

→dễ dàng can nhiễu

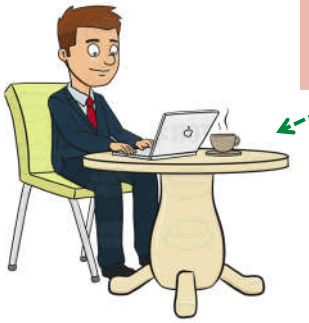
→dễ dàng để tấn công man-in-the-middle

38

Coffee Shop

1. Kết nối mạng WiFi

Thiết lập kết nối
(**Có thể** thực hiện các giao thức xác thực, mã hóa bảo vệ)



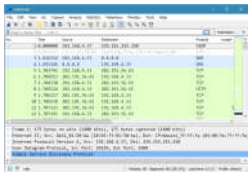
39

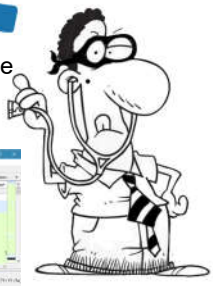
39

Coffee Shop

WEP Open:
Không thực hiện các giao thức xác thực, mã hóa bảo vệ

Dễ dàng nghe lén thông tin





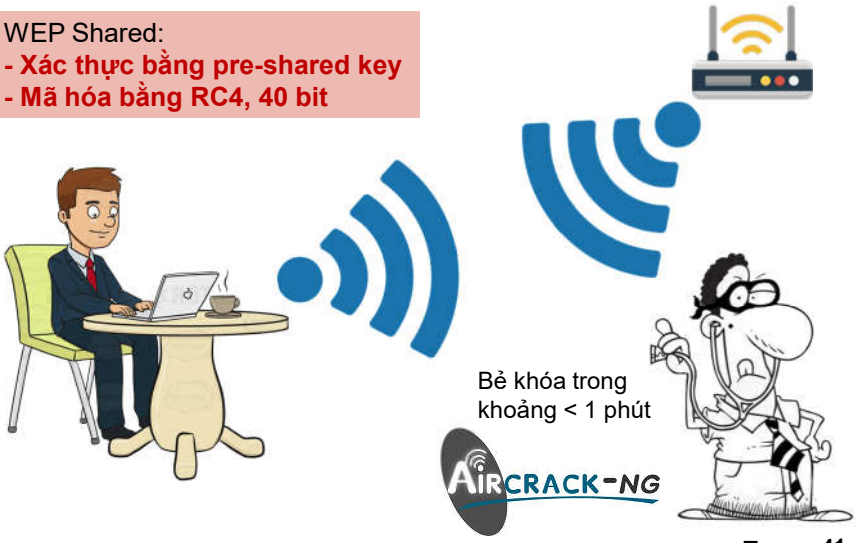
Eve

40

40

Coffee Shop

WEP Shared:
- **Xác thực bằng pre-shared key**
- **Mã hóa bằng RC4, 40 bit**



41

41

Coffee Shop

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

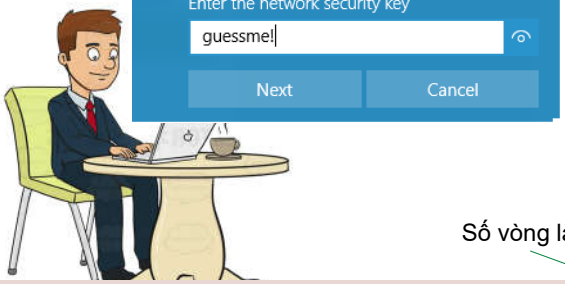
SSID: WifiStation
password: guessme!

42

42

Coffee Shop

WPA2 Personal



SSID: WifiStation
password: guessme!

Kích thước khóa

Số vòng lặp

Laptop và AP cùng tính toán:
K = PBKDF2(HMAC-SHA-1, password, SSID, SSID_length, 4096, 256)

43

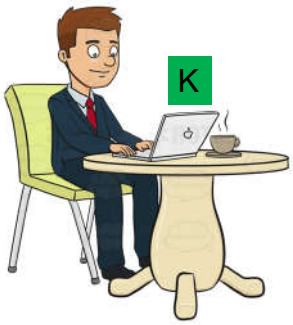
43

Coffee Shop

WPA2 Personal

K

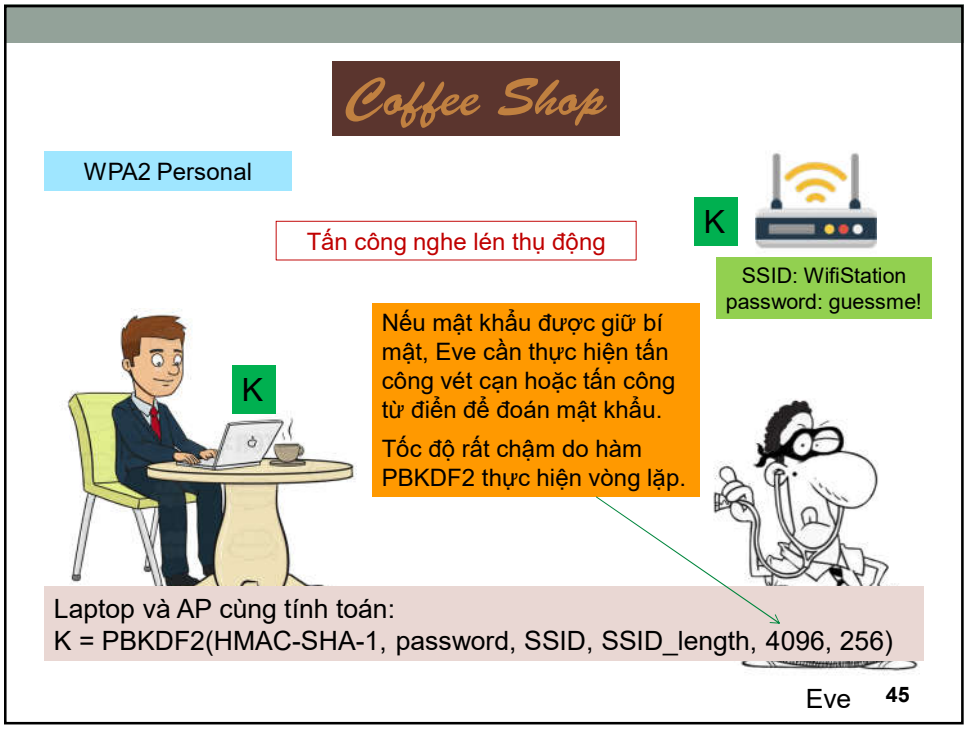
SSID: WifiStation
password: guessme!



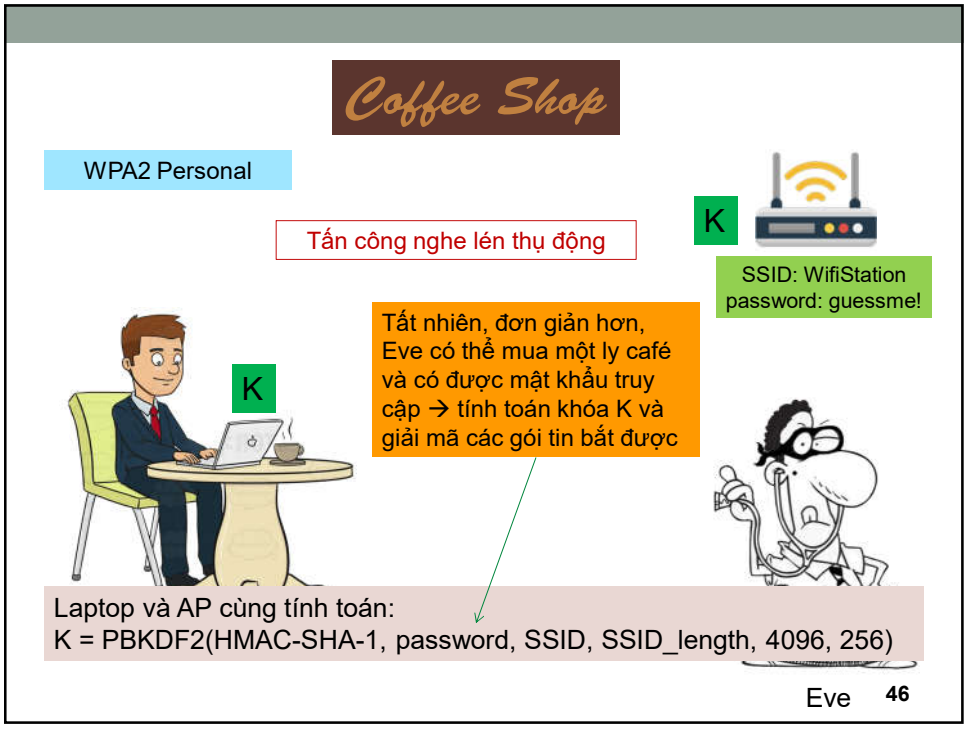
Laptop và AP cùng chia sẻ giá trị bí mật K. Giá này được sử dụng để sinh khóa dùng cho quá trình mã hóa và xác thực dữ liệu trao đổi giữa 2 bên

44

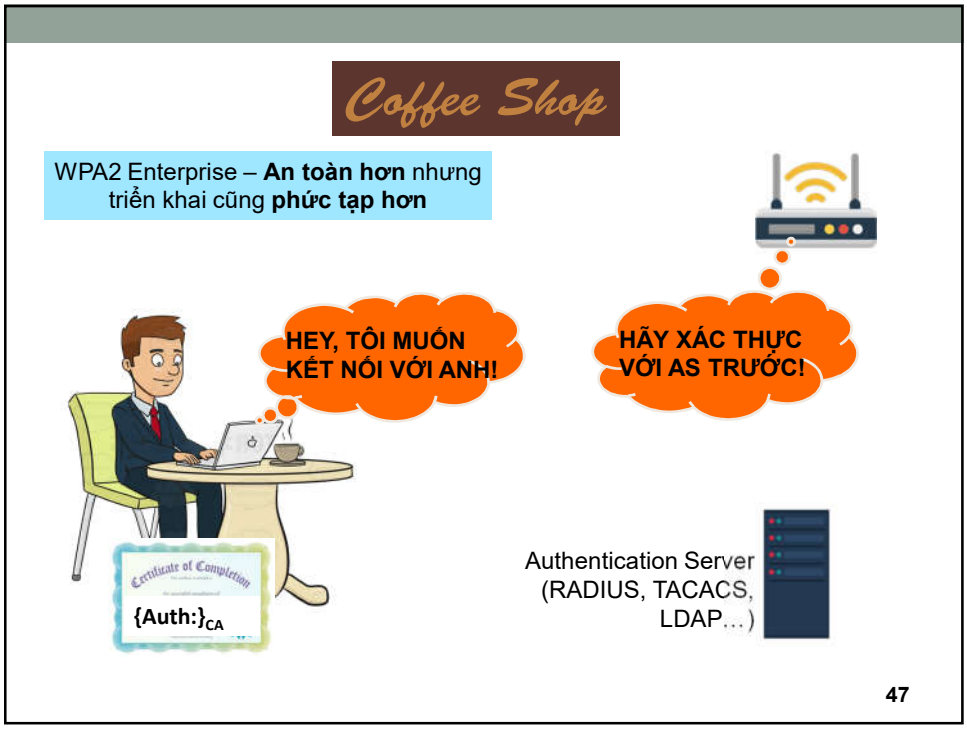
44


Coffee Shop
WPA2 Personal
Tấn công nghe lén thụ động
K
SSID: WifiStation
password: guessme!
K
Nếu mật khẩu được giữ bí mật, Eve cần thực hiện tấn công vét cạn hoặc tấn công từ điển để đoán mật khẩu.
Tốc độ rất chậm do hàm PBKDF2 thực hiện vòng lặp.
Laptop và AP cùng tính toán:
K = PBKDF2(HMAC-SHA-1, password, SSID, SSID_length, 4096, 256)
Eve
45

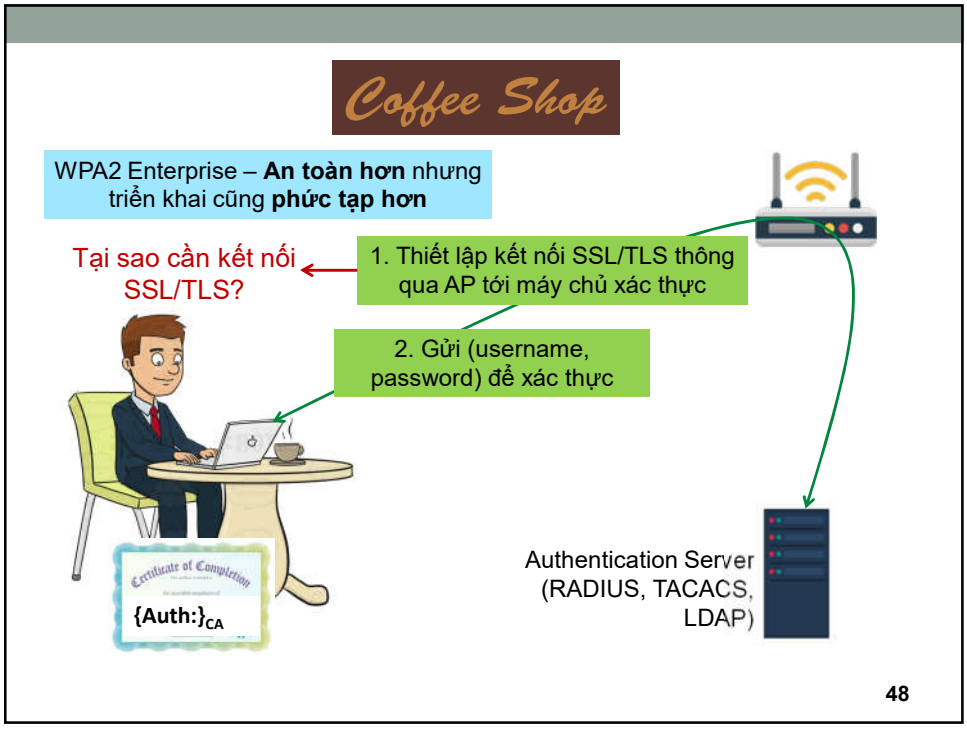
45


Coffee Shop
WPA2 Personal
Tấn công nghe lén thụ động
K
SSID: WifiStation
password: guessme!
K
Tất nhiên, đơn giản hơn, Eve có thể mua một ly café và có được mật khẩu truy cập → tính toán khóa K và giải mã các gói tin bắt được
Laptop và AP cùng tính toán:
K = PBKDF2(HMAC-SHA-1, password, SSID, SSID_length, 4096, 256)
Eve
46

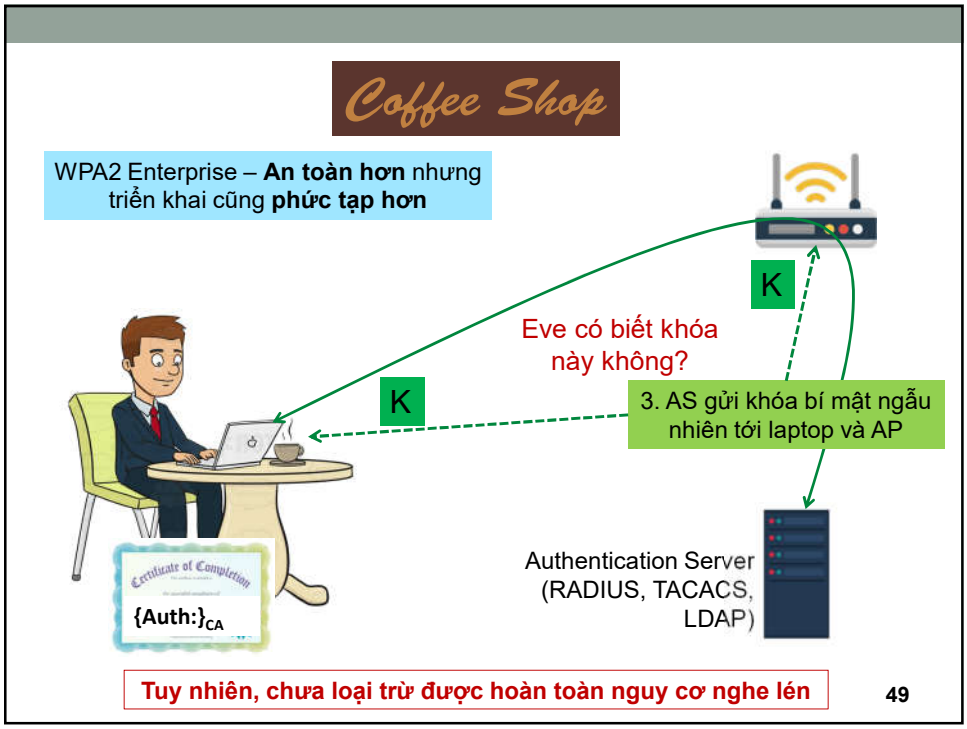
46


Coffee Shop
WPA2 Enterprise – An toàn hơn nhưng triển khai cũng phức tạp hơn
HEY, TÔI MUỐN KẾT NỐI VỚI ANH!
HÃY XÁC THỰC VỚI AS TRƯỚC!
Certificate of Completion
{Auth:}CA
Authentication Server (RADIUS, TACACS, LDAP…)
47

47


Coffee Shop
WPA2 Enterprise – An toàn hơn nhưng triển khai cũng phức tạp hơn
Tại sao cần kết nối SSL/TLS?
1. Thiết lập kết nối SSL/TLS thông qua AP tới máy chủ xác thực
2. Gửi (username, password) để xác thực
Certificate of Completion
{Auth:}CA
Authentication Server (RADIUS, TACACS, LDAP)
48

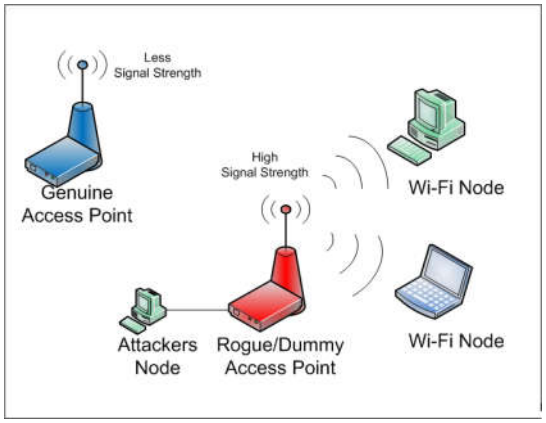
48



49

Các nguy cơ các trong mạng WLAN

- Chèn sóng (jamming): Cố tình gây nhiễu bằng cách phát ra tín hiệu cùng tần số với công suất lớn hơn
- Mục đích:
  - Giả mạo máy trạm
  - Giả mạo AP(Rogue AP)
  - DoS: phá kết nối giữa máy trạm và AP



50

50

Các nguy cơ khác trong mạng WLAN

- Disassociation: gửi disassociation frame tới máy trạm hoặc AP để ngắt kết nối đã được thiết lập
- Deauthentication attack: gửi deauthentication frame tới máy trạm để yêu cầu xác thực lại

→ Mục đích: kết hợp 2 loại tấn công:

- Bắt, phân tích tải để tìm SSID ẩn
- Đánh lừa máy trạm khi thực hiện kết nối lại sẽ kết nối với AP giả mạo

- Giả mạo AP (Rogue AP):
  - Thu thập thông tin xác thực giữa AP và máy trạm
  - Nghe lén chủ động
  - Tấn công man-in-the-middle
  - Phòng chống: sử dụng các công cụ quản trị mạng để phát hiện sự có mặt của thiết bị lạ

51

51

NGUY CƠ AN TOÀN BẢO MẬT TRONG MẠNG LAN

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

52

52

Tấn công trên VLAN

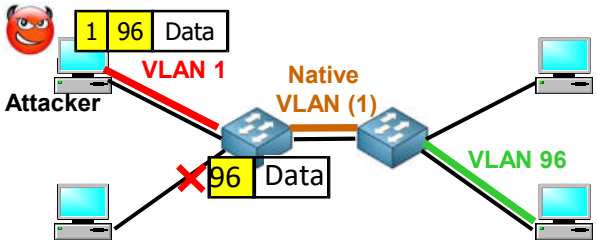
- VLAN: miền quảng bá logic trên các switch → phân tách các lưu lượng mạng ở tầng 2
- Các cơ chế ATBM có thể triển khai trên VLAN: điều khiển truy cập (access control), cách ly tài nguyên quan trọng
- Các VLAN được gán các dải địa chỉ IP khác nhau
- Các khung tin Ethernet được gắn thêm VLAN tag (802.1Q hoặc ISL)
- Chuyển mạch chỉ thực hiện trong 1 VLAN
- Trao đổi dữ liệu giữa các VLAN: định tuyến (inter VLAN routing)

53

53

Tấn công: VLAN hopping

- Mục đích: truy cập vào các VLAN khác từ Native VLAN
- Lỗ hổng: các dữ liệu chuyển trong Native VLAN không cần gắn tag
- Đánh lừa switch chuyển tiếp các gói tin vào VLAN
- Double-tag attack



- Phòng chống?

54

54

Tấn công VLAN: DTP và VTP

- Dynamic Trunking Protocol: tự động cấu hình chế độ trunking cho các cổng của VLAN
  - Tấn công giả mạo các gói tin DTP để lừa 1 switch kết nối vào VLAN của kẻ tấn công
- VLAN Trunking Protocol: tự động chuyển tiếp thông tin cấu hình VLAN từ VTP server tới các VTP client
  - Tấn công giả mạo các gói tin để xóa 1 VLAN (DoS) hoặc thêm 1 VLAN gồm tất cả các switch (tạo bão quảng bá – broadcast storm)
- Phòng chống?

55

55

Tấn công VLAN: DTP và VTP

- Dynamic Trunking Protocol: tự động cấu hình chế độ trunking cho các cổng của VLAN
  - Tấn công giả mạo các gói tin DTP để lừa 1 switch kết nối vào VLAN của kẻ tấn công
- VLAN Trunking Protocol: tự động chuyển tiếp thông tin cấu hình VLAN từ VTP server tới các VTP client
  - Tấn công giả mạo các gói tin để xóa 1 VLAN (DoS) hoặc thêm 1 VLAN gồm tất cả các switch (tạo bão quảng bá – broadcast storm)
- Phòng chống?

56

56

Tấn công giao thức STP

Spanning Tree Protocol: khử loop trên mạng kết nối switch có vòng kín

- Bầu chọn root:
  - Mỗi nút có giá trị priotity(mặc định là 38464)
  - Các nút trao đổi thông điệp BPDU chứa giá trị priority
  - Nút có priotity nhỏ nhất trở thành root
  - Nếu có nhiều switch cùng priority, switch có cổng địa chỉ MAC nhỏ nhất là root
- Thiết lập cây khung: các nút còn lại
  - Mỗi nút còn lại tìm đường đi ngắn nhất tới nút gốc (giá của liên kết xác định dựa trên băng thông)
  - Giữ cổng gần nút gốc nhất hoạt động, tạm ngắt các cổng "xa" nút gốc hơn
- STP không có cơ chế xác thực

57

57

Tấn công giao thức STP

- Tấn công vào STP: đoạt quyền root switch
  - DoS: black-hole attack, flooding attack
  - Chèn dữ liệu giả mạo vào luồng trao đổi thông tin
  - Tấn công man-in-the-middle
- Tấn công DoS: BPDU Flooding
- Phòng chống:
  - Root guard
  - BPDU guard
  - BPDU filtering

58

58

Tấn công cơ chế tự học MAC (chuyển mạch)

- Tấn công MAC flooding: gửi hàng loạt các gói tin với địa chỉ MAC nguồn là giả → bảng MAC bị tràn →Các gói tin thực sự bắt buộc phải chuyển tiếp theo kiểu quảng bá:
  - Gây bão quảng bá → chiếm dụng băng thông đường truyền, tài nguyên của các nút mạng khác
  - Nghe trộm thông tin
- Giả mạo địa chỉ MAC
- Phòng chống: Port Security

59

59

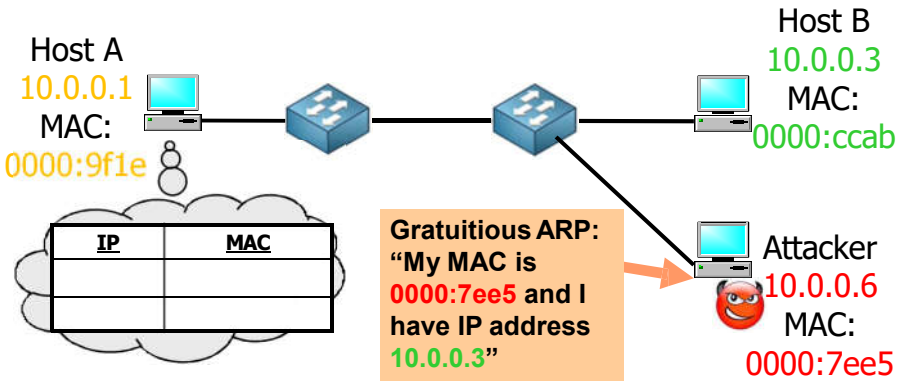
Tấn công giao thức ARP

- Address Resolution Protocol: tìm địa chỉ MAC tương ứng với địa chỉ IP
- Sử dụng phương thức quảng bá ARP Request:
  - Không cần thiết lập liên kết
- Không có cơ chế xác thực ARP Response
- Tấn công:
  - Giả mạo: ARP Spoofing
  - DoS
- Phòng chống: Dynamic ARP Inspection

60

60

ARP Spoofing



- Đặc biệt nguy hiểm khi đưa địa chỉ MAC giả mạo gateway router, Local DNS Server:
  - Nghe lén
  - Man-in-the-middle

61

61

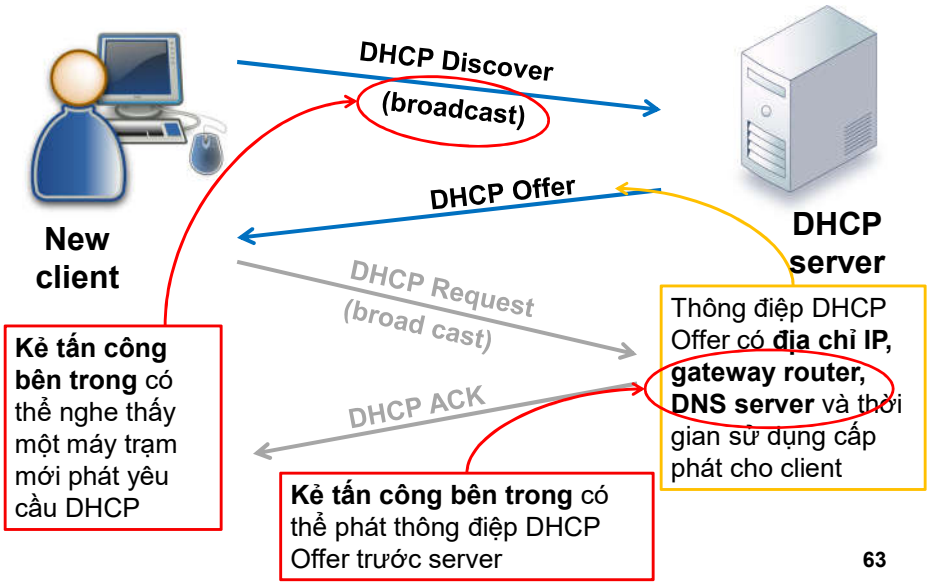
Tấn công dịch vụ DHCP

- Dynamic Host Configuration Protocol
- Cấp phát các cấu hình IP tự động cho máy trạm:
  - Địa chỉ IP
  - Địa chỉ gateway router
  - Địa chỉ DNS server
- Sử dụng UDP, cổng 67(server) và 68(client)

62

62

Hoạt động của DHCP



63

63

Các nguy cơ tấn công DHCP

- Lỗ hổng: Bất kỳ máy trạm nào yêu cầu cũng được cấp phát địa chỉ IP
  - Nguy cơ: Tấn công DoS làm cạn kho địa chỉ(DHCP Starvation)
- Lỗ hổng: Không xác thực cho các thông tin cấp phát từ DHCP server → DHCP Spoofing
  - Nguy cơ: Thay địa chỉ DNS server tin cậy bằng địa chỉ DNS của kẻ tấn công.
  - Nguy cơ: Thay địa chỉ default router, cho phép kẻ tấn công:
    - ✓ Chặn bắt, do thám thông tin
    - ✓ Tấn công phát lại
    - ✓ Tấn công man-in-the-middle
  - Phòng chống: DHCP Snooping

64

64

3. AN TOÀN BẢO MẬT TẦNG MẠNG

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

65

65

Giao thức IP và ICMP

- Internet Protocol:
  - Giao thức kết nối liên mạng
  - Hướng không kết nối (connectionless), không tin cậy
- Internet Control Message Protocol
  - Nằm trên giao thức IP
  - Hướng không kết nối (connectionless), không tin cậy
  - Kiểm tra trạng thái hoạt động của các nút mạng khác
- Vấn đề của giao thức IP và ICMP:
  - Không cần thiết lập liên kết: có thể lợi dụng để quét mạng
  - Dễ dàng giả mạo địa chỉ IP nguồn trên các gói tin
  - Có thể gửi liên tục với số lượng lớn các gói tin

66

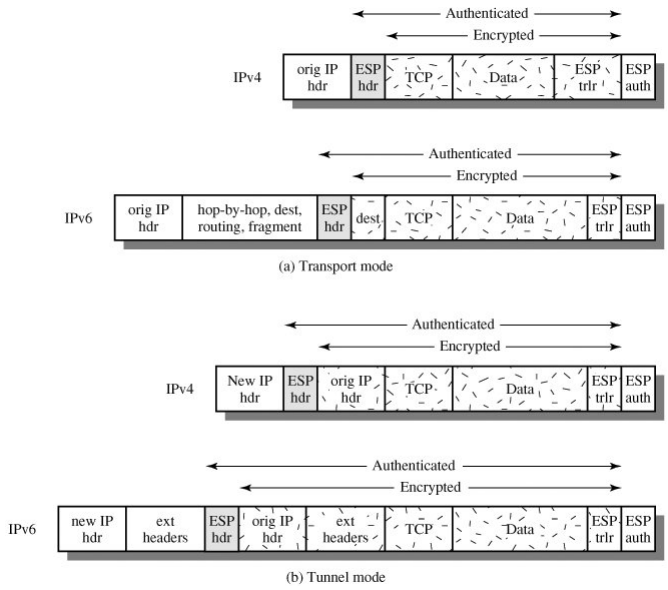
66

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

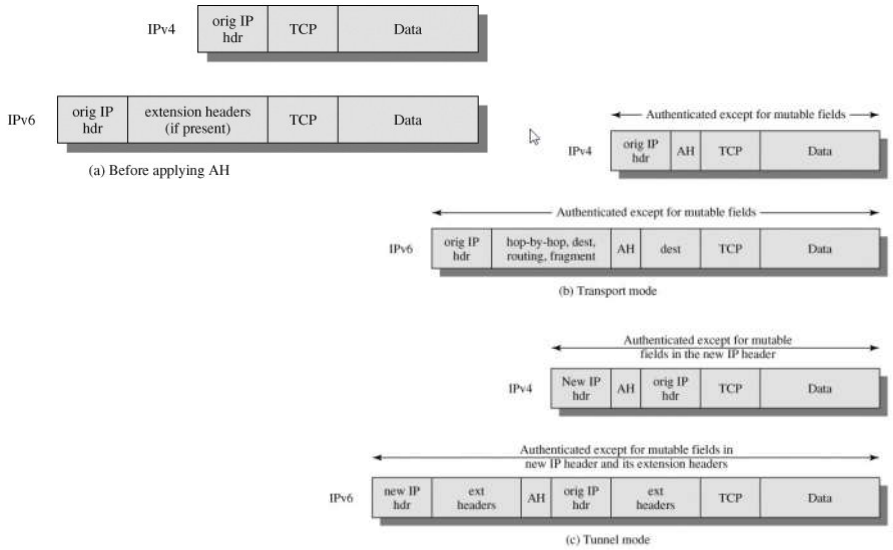
67

Đóng gói dữ liệu theo giao thức ESP



68

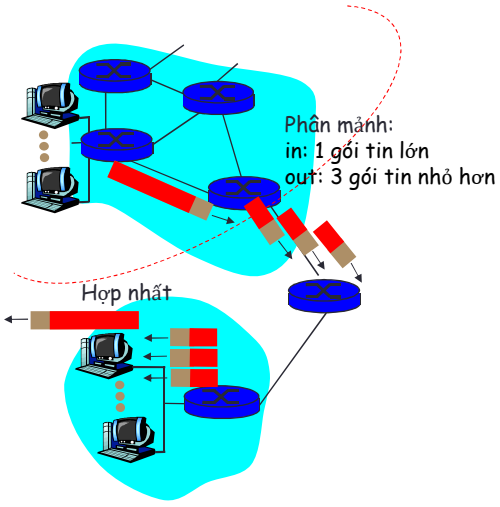
Đóng gói dữ liệu theo giao thức AH



69

Phân mảnh gói tin IP

- Đường truyền có một giá trị MTU (Kích thước đơn vị dữ liệu tối đa)
- Các đường truyền khác nhau có MTU khác nhau
- Một gói tin IP lớn quá MTU sẽ bị
  - Chia làm nhiều gói tin nhỏ hơn
  - Được tập hợp lại tại trạm đích

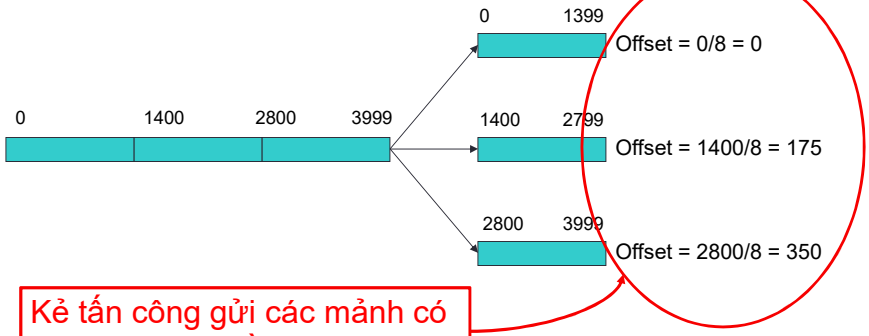


70

70

Nguy cơ tấn công vào giao thức IP (Tính sẵn sàng)

- Tấn công DoS – Teardrop: Lợi dụng cơ chế phân mảnh của giao thức IP
  - Offset cho biết vị trí của mảnh tin trong gói tin ban đầu



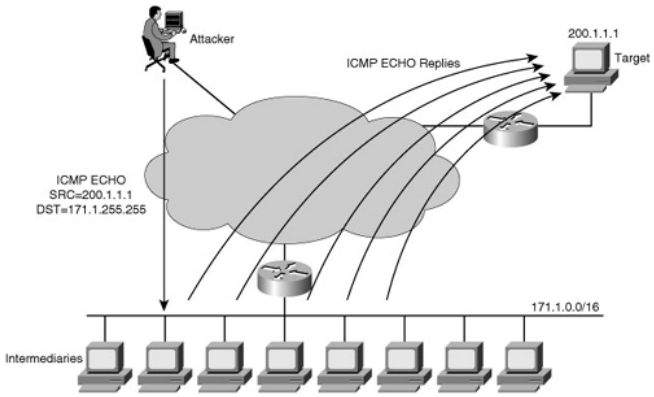
Kẻ tấn công gửi các mảnh có giá trị Offset chồng lên nhau

71

71

Nguy cơ tấn công vào giao thức ICMP (Tính sẵn sàng)

- Ping of Death: gửi liên tục các gói tin ICMP có kích thước tối đa (xấp xỉ 64 KB)
- Smurf attack



72

72

AN TOÀN BẢO MẬT CÁC GIAO THỨC ĐỊNH TUYẾN

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

73

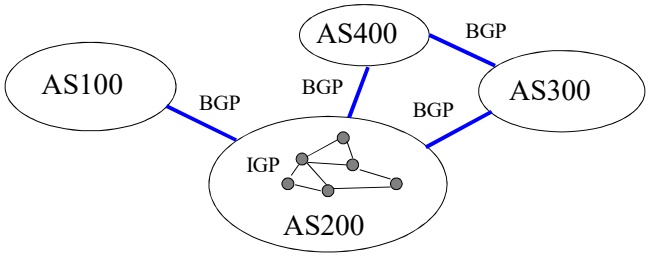
Giới thiệu chung về định tuyến

- Định tuyến: tìm ra đường đi ngắn nhất tới các mạng đích
  - Bảng định tuyến: lưu thông tin đường đi
- Định tuyến tĩnh: người dùng định nghĩa nội dung của bảng định tuyến → an toàn nhưng không cập nhật theo sự thay đổi trạng thái của các liên kết
- Định tuyến động: router tự động xây dựng nội dung bảng định tuyến
- Đặc điểm của định tuyến trong mạng IP:
  - Mỗi nút chỉ chắc chắn về các thông tin cục bộ
  - Các nút trao đổi thông tin định tuyến theo cơ chế flooding

74

Định tuyến trên mạng Internet

- Chia thành các vùng tự trị định tuyến AS
  - Thường được đăng ký và quản lý bởi ISP
- Phân cấp:
  - Định tuyến nội vùng(IGP): RIP, OSPF, IGRP, EIGRP
  - Định tuyến ngoại vùng(EGP): BGP



75

75

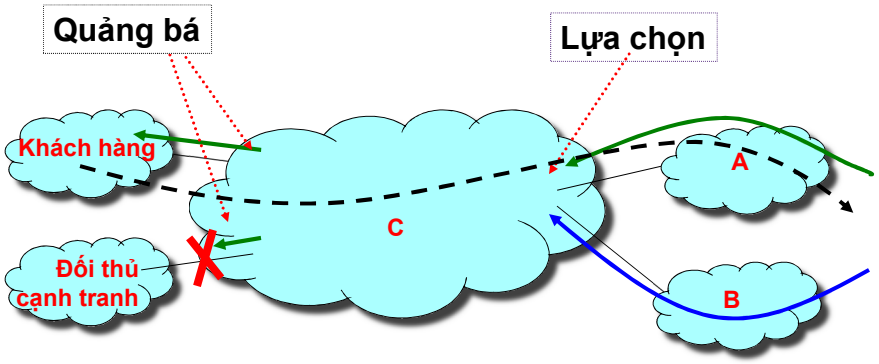
Hoạt động của BGP(tóm tắt)

- Hỗ trợ định tuyến không phân lớp
- Tìm đường tới các vùng tự trị (AS)
- Trao đổi thông điệp BGP với hàng xóm qua kết nối TCP
- Mỗi router quảng bá thông tin đường đi tới các router khác bằng bản tin UPDATE
  - Thông tin đường đi: danh sách các AS trên đường đi tới AS đích
- Thực hiện các chính sách trong quá trình chọn đường
  - Lựa chọn đường ra
  - Quảng bá đường vào
  - …

76

76

BGP: Chính sách lựa chọn-quảng bá

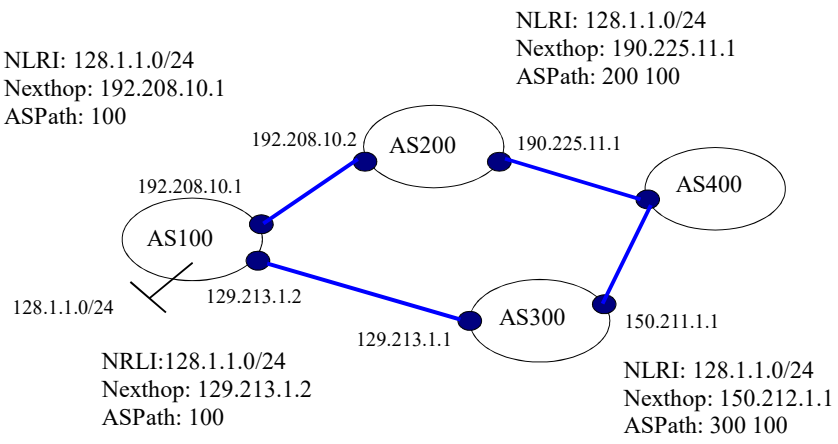


- **Lựa chọn**: Đường đi nào được dùng để chuyển dữ liệu tới AS đích?
  - Kiểm soát thông tin ra khỏi AS
- **Quảng bá**: Quảng bá cho AS khác đường đi nào?
  - Kiểm soát thông tin vào AS

77

77

Hoạt động của BGP – Ví dụ



78

78

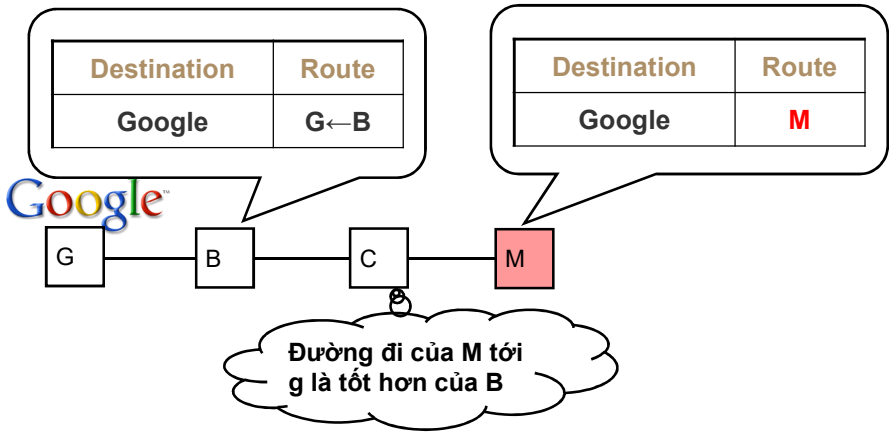
Tấn công các giao thức định tuyến

- RIPv1: không hỗ trợ các cơ chế xác thực thông tin trao đổi giữa các nút → khai thác tấn công thay đổi, giả mạo thông tin
- RIPv2, OSPF, BGP: hỗ trợ cơ chế xác thực sử dụng pre-shared key
  - Khóa không ngẫu nhiên, do người dùng lựa chọn
- OSPF: Lợi dụng cơ chế quảng bá thông tin LSA giả để tấn công DoS (black-hole attack)
- BGP: Giả mạo thông tin định tuyến để điều hướng dữ liệu → Hậu quả: tấn công từ chối dịch vụ, man-in-the-middle, thư rác...

79

79

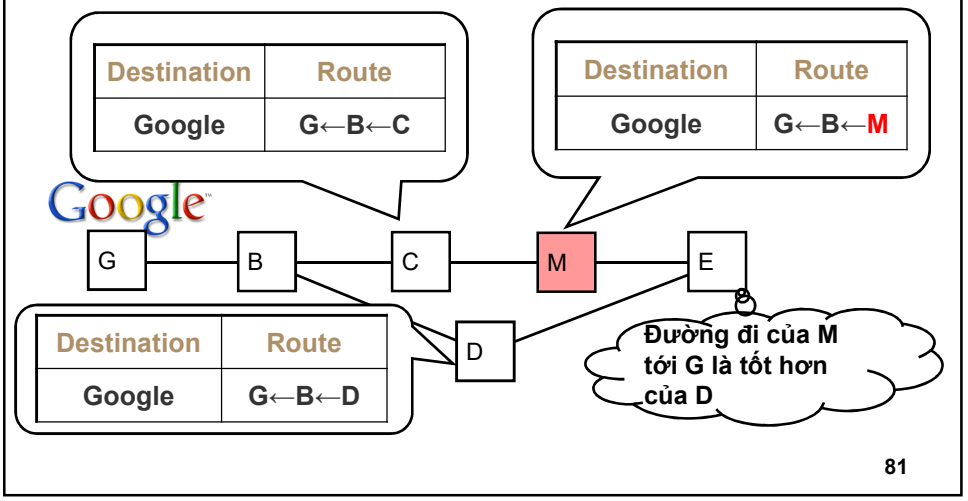
Tấn công BGP: Giả mạo thông tin đường đi



80

80

Tấn công BGP: Giả mạo thông tin đường đi

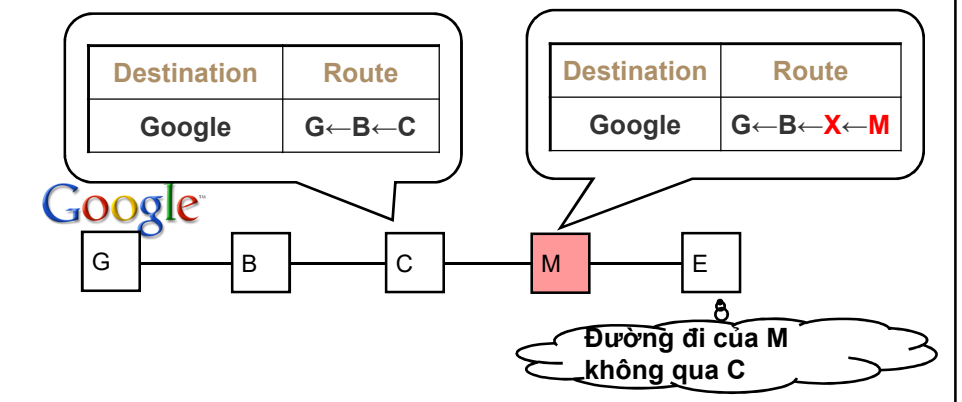


81

81

Tấn công BGP: Giả mạo thông tin đường đi

- Chính sách của E: Không lựa chọn đường đi qua C

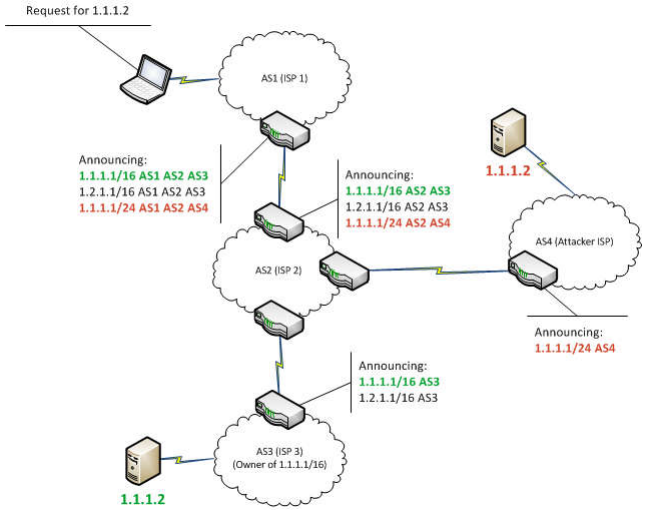


82

82

Tấn công BGP: Path hijack

- Lợi dụng cơ chế Longest Matching



83

83

BGP hijacking – Ví dụ

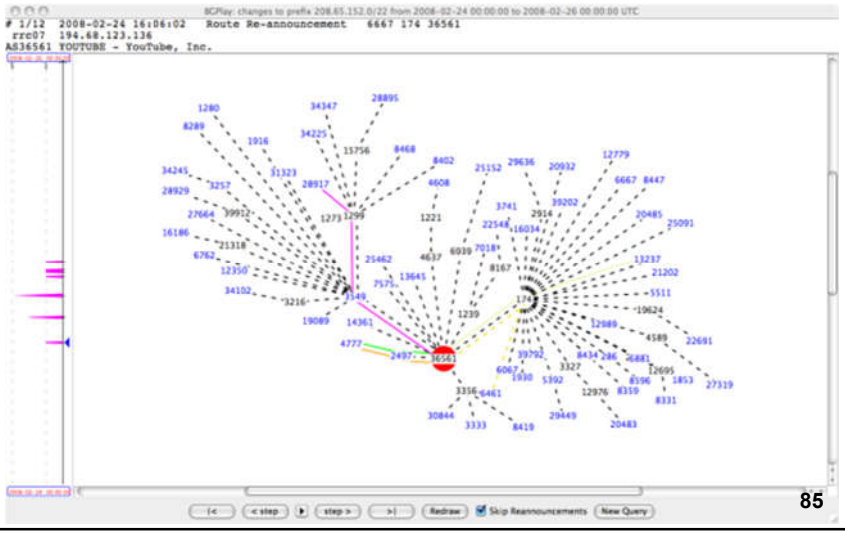
- Tháng 02/08: chính phủ Pakistan ngăn cản các truy cập vào trang Youtube:
  - Địa chỉ của Youtube: 208.65.152.0 /22
  - youtube.com: 208.65.153.238 /22
  - Pakistan Telecom loan báo một thông tin định tuyến BGP tới mạng 208.65.153.0 /24 → các router trên Internet cập nhật đường đi mới theo quy tắc longest matching → bị đánh lừa youtube.com nằm ở Pakistan → không thể truy cập youtube.com trong 2 giờ
- Tháng 03/2014: dịch vụ DNS của bị Google tấn công với địa chỉ 8.8.8.8/32
  - Không thể truy cập được từ một số nước ở Nam Mỹ trong 22 phút

84

84

BGP hijacking - Youtube

- AS36561(Youtube) loan báo về đường đi tới địa chỉ 208.65.152.0/22

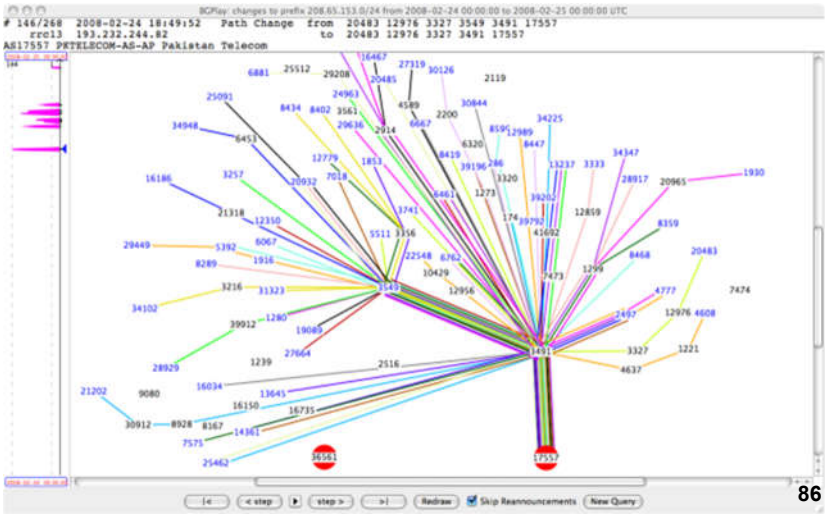


85

85

BGP hijacking - Youtube

- AS17557 (Pakistan Telecom) loan báo đường đi tới địa chỉ 208.65.153.0/24 trong 2 phút

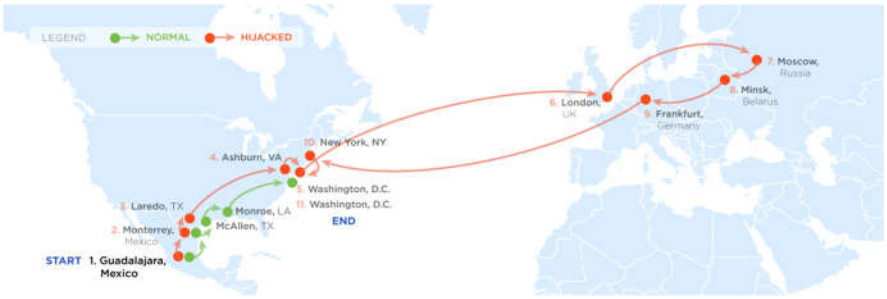


86

86

BGP hijacking – Ví dụ

- Tháng 2/2013: đường đi từ các AS Guadalajara tới WasingtonDC chuyển hướng qua Belarus trong vài giờ
  - Đường đi đúng: Alestra (Mexico) ⟶ PCCW (Texas) ⟶ Qwest (DC)



- Tương tự: tấn công tấn công Dell SecureWorks năm 2014, ISP của Italia vào 6/2015

87

87

Yêu cầu bảo mật với BGP

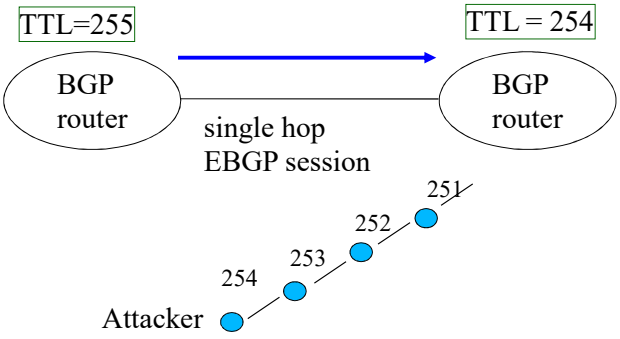
- Xác minh được "sự sở hữu" không gian địa chỉ: router BGP có thực sự kết nối tới AS sử dụng địa chỉ IP đó không?
- Xác thực giữa các AS
- Xác thực và ủy quyền cho các router trong AS
  - Quảng bá địa chỉ
  - Quảng bá đường đi
- Kiểm tra tính toàn vẹn, chính xác và tính đúng thời điểm của toàn bộ lưu lượng BGP

88

88

Phòng chống tấn công BGP

- Gửi thông điệp BGP cho hàng xóm với giá trị TLL trên gói tin IP là 255
- Từ chối tất cả các gói tin có TTL < 254
- Hạn chế: chỉ chống lại tấn công bằng giả mạo mà không xuất phát từ router hàng xóm



89

89

Phòng chống tấn công BGP

Xác thực với MD5 và pre-share-key

- Hai router hàng xóm được cấu hình để chia sẻ một giá trị bí mật

```
(config-router)# neighbor addr password passphrase
```

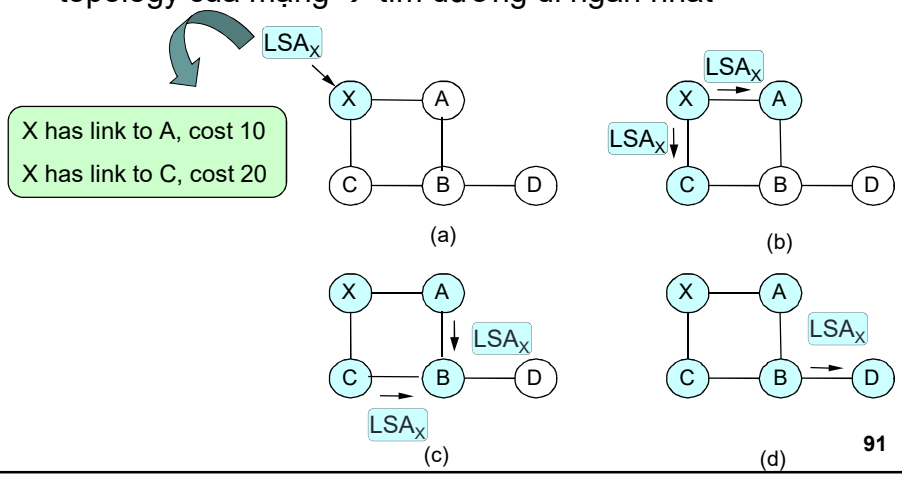
- Các gói tin TCP mang theo thông điệp BGP trường Options chứa mã băm *MD5(BGP message || passphrase)* để xác thực
- Chỉ chống lại tấn công giả mạo thông tin định tuyến từ bên ngoài
- Nguy cơ: không chống lại được tấn công giả mạo thông tin định tuyến từ router trong mạng

90

90

Hoạt động của OSPF(tóm tắt)

- Router quảng bá thông tin liên kết LSA trên mạng
- Mỗi router thu thập các thông tin LSA → xây dựng topology của mạng → tìm đường đi ngắn nhất



91

91

Các cơ chế ATBM trên OSPF

- Xác thực các bản tin LSA
  - Trên mỗi liên kết, 2 router chia sẻ một giá trị bí mật
  - Sử dụng hàm MAC để tạo mã xác thực:

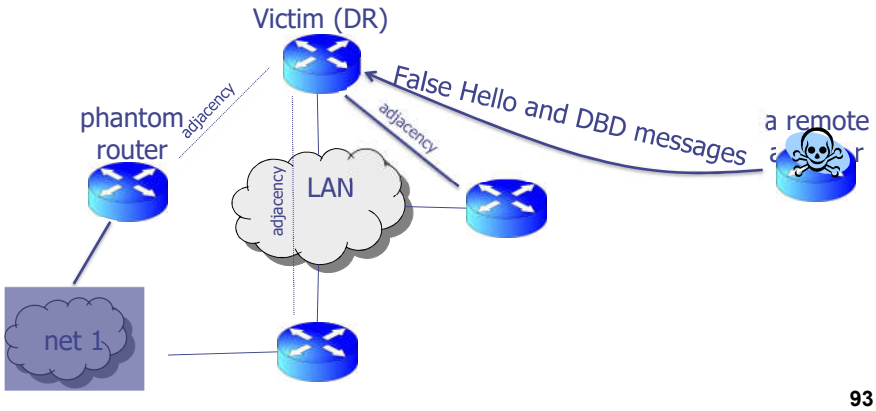
    MAC(k, m) = MD5(data || key || pad || length)
- Cơ chế "fight back": nếu router nhận được LSA của chính nó với giá trị timestamp mới hơn, ngay lập tức quảng bá bản tin LSA mới.

92

92

Tấn công giao thức OSPF

- Kẻ tấn công gửi thông tin LSA giả mạo để các router cập nhập đường đi ngắn nhất qua router không có thực
- Ví dụ



93

93

4. AN TOÀN BẢO MẬT TẦNG GIAO VẬN

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

94

94

Nhắc lại về TCP

- Transmission Control Protocol
- Hướng liên kết (connection-oriented), tin cậy:
  - Thiết lập liên kết: bắt tay 3 bước
  - Truyền dữ liệu
  - Kết thúc liên kết
- Báo nhận, phát lại
- Điều khiển luồng
- Điều khiển tắc nghẽn

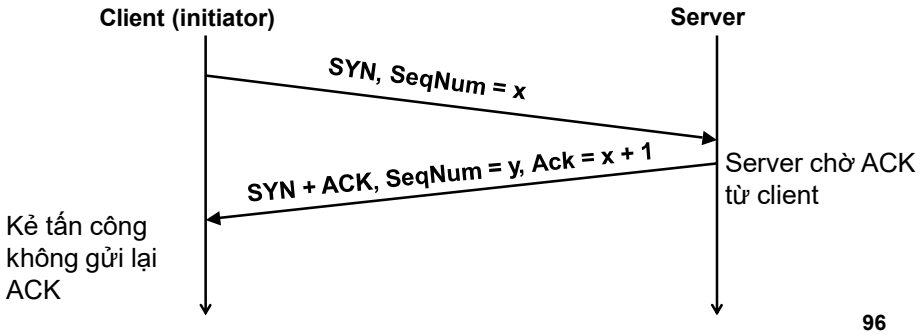
95

95

Nguy cơ ATBM với TCP (Tính sẵn sàng)

- Tấn công DoS – SYN Flooding
  - Kẻ tấn công gửi hàng loạt gói tin SYN với địa chỉ nguồn là các địa chỉ IP giả
  - Server gửi lại SYN/ACK, chuẩn bị tài nguyên để trao đổi dữ liệu, chờ ACK trong thời gian time-out

  → tấn công thành công nếu trong thời gian time-out làm cạn kiệt tài nguyên của ứng dụng, máy chủ vật lý



96

96

Tấn công can thiệp vào kết nối TCP

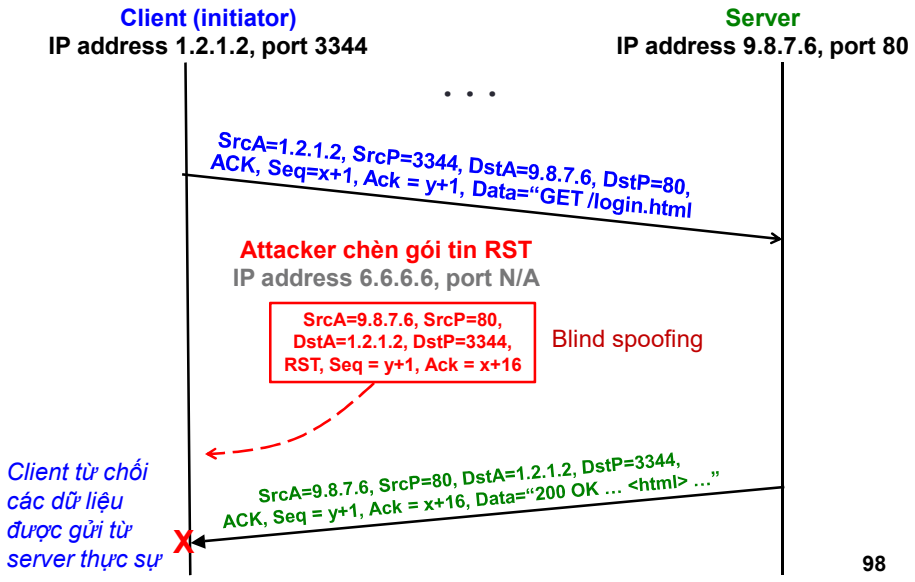
- Quá trình trao đổi dữ liệu kết thúc bình thường: giao thức TCP cho phép 2 bên đóng liên kết một cách độc lập (gửi gói tin FIN)
  - Tin cậy: chờ nhận ACK
  - Liên kết chỉ thực sự hủy khi 2 bên đã đóng
- Ngược lại, nếu quá trình trao đổi dữ liệu không thể kết thúc bình thường (tiến trình ứng dụng kết thúc đột ngột, các gói tin lỗi), gói tin RST (reset) được gửi đi:
  - Việc đóng liên kết xuất phát từ một bên
  - Không cần chờ ACK
  - Liên kết được hủy nếu Sequence Number là phù hợp

  → kẻ tấn công có thể ngắt kết nối đột ngột của người dùng nếu biết được thông tin về số hiệu cổng, Sequence Number

97

97

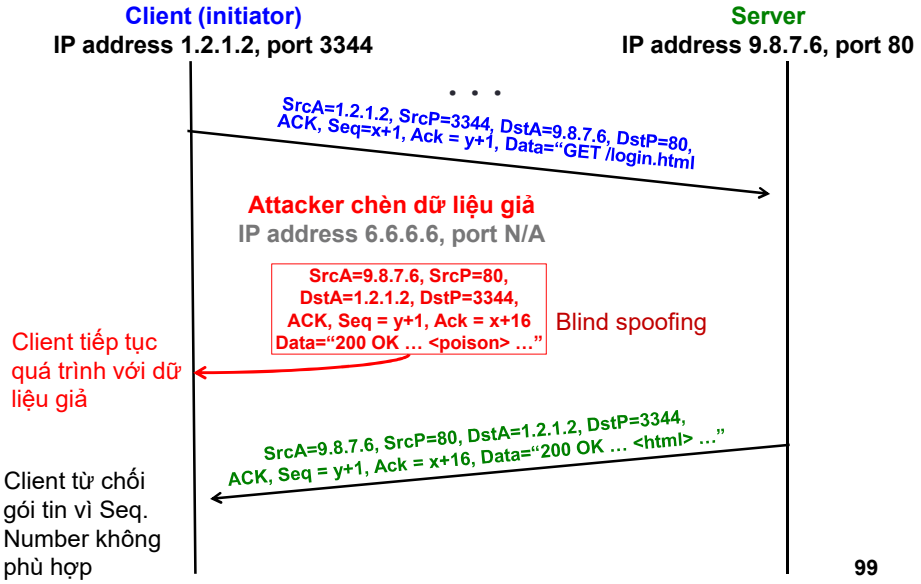
RST Injection



98

98

Data Injection



99

99

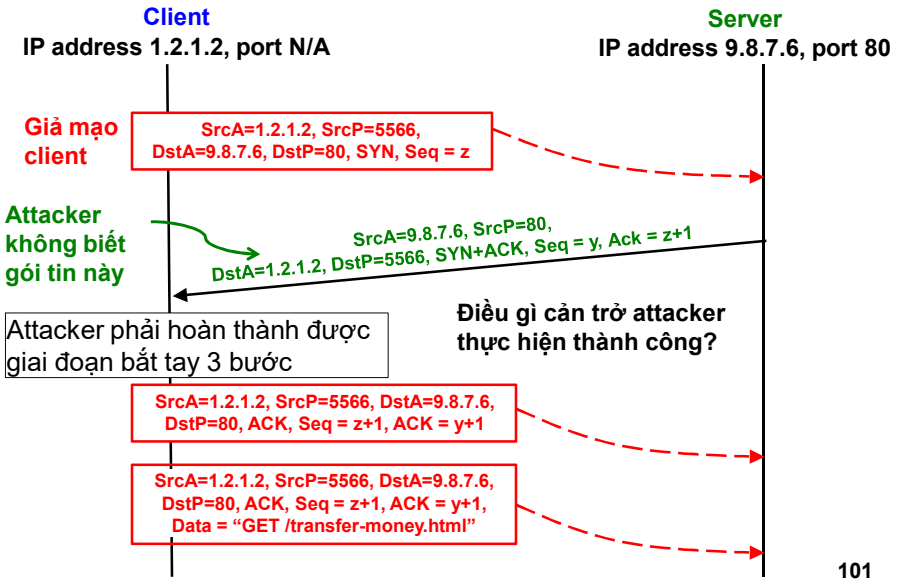
Tấn công kết nối TCP trong trường hợp không biết thông tin về kết nối

- Nhận xét: trong các kịch bản tấn công trên, kẻ tấn công cần phải theo dõi các thông số trên kết nối (cổng, Sequence Number...)
- Trong trường hợp không có các thông tin này, kẻ tấn công vẫn có thể thực hiện bằng cách đoán nhận → blind spoofing
- Hoặc đơn giản hơn: giả mạo kết nối TCP
- Phòng chống?

100

100

Tấn công giả mạo kết nối TCP



101

101

Kịch bản tấn công của Mitnick

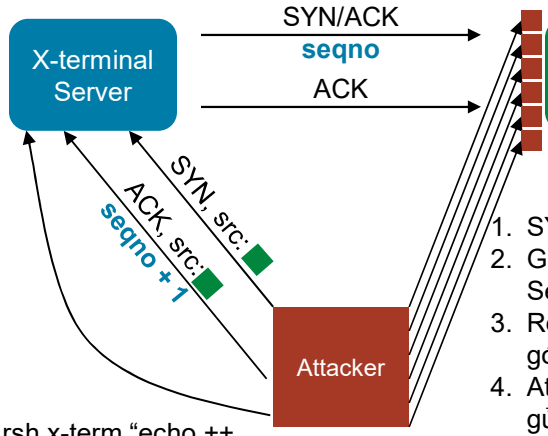
- Kevin Mitnick (1969) thực hiện cuộc tấn công vào hệ thống máy chủ của Tsutomu Shimomura(1964)
- Phát hiện lỗ hổng trên máy chủ X-terminal không sinh giá trị Seq ngẫu nhiên(= Seq_{i-1} + 128.000)
- Tấn công vào website của Shimomura và phát hiện danh sách các nút mạng được phép truy cập từ xa tới máy chủ X-terminal

→ tấn công giả mạo kết nối TCP(1992)

102

102

Kịch bản tấn công của Mitnick



Được phép truy cập tới X-terminal Server

1. SYN Flood tới Remote host
2. Gửi gói tin SYN tới X-terminal Server
3. Remote host không thể gửi gói tin RST
4. Attacker đoán nhận **seqno**, gửi gói tin ACK xác nhận thiết lập kết nối
5. Giành quyền truy cập vào X-terminal server
6. RST Flood tới Remote host

103

103

5. AN TOÀN BẢO MẬT TẦNG ỨNG DỤNG

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

104

104

5.1. GIAO THỨC SSL/TLS

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

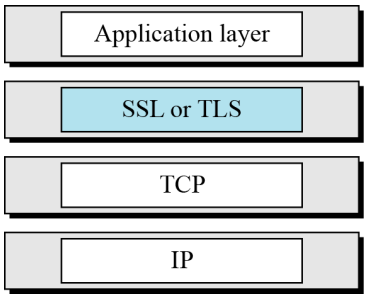
105

105

SSL/TLS là gì?

Sercure 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



106

106

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 + SSLT/TLS: Cổng 465
- FTPS = FTP + SSL/TLS: Cổng 990 và 989

107

107

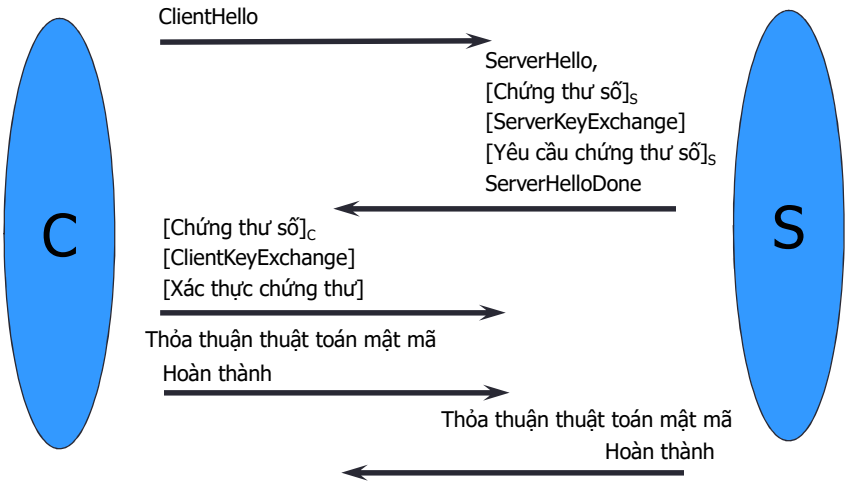
SSL/TLS là gì?

- 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

108

108

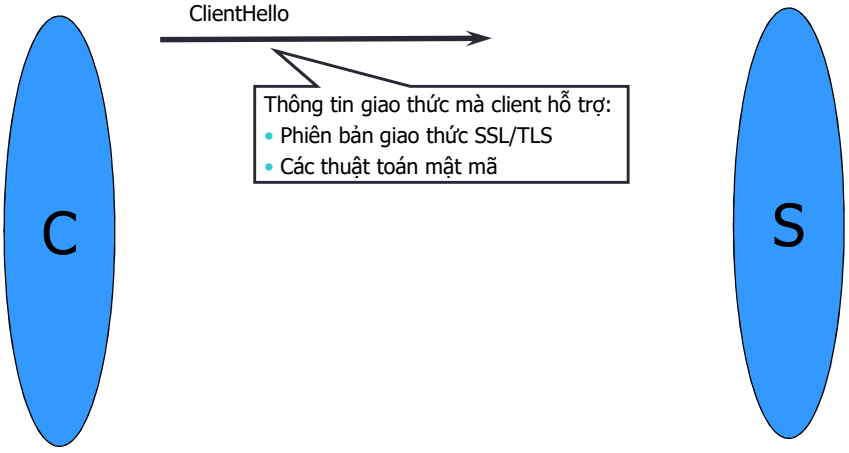
Giao thức bắt tay



109

109

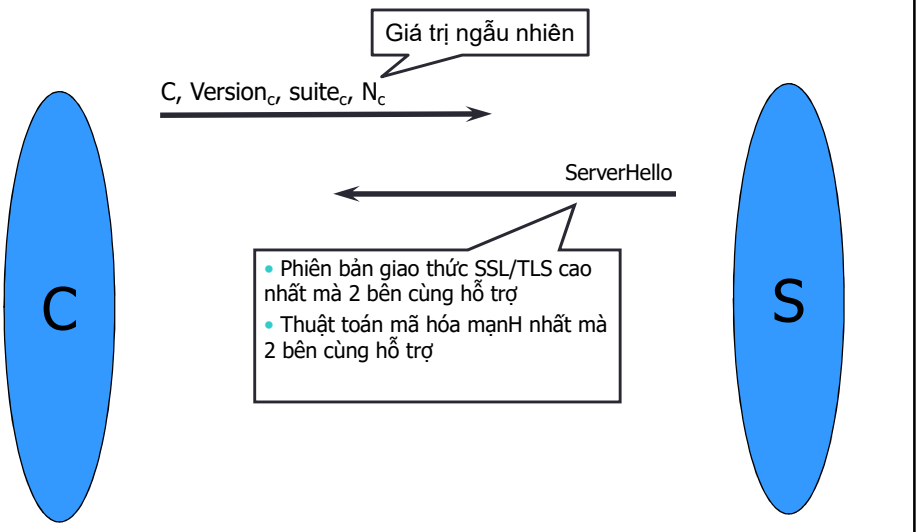
Client Hello



110

110

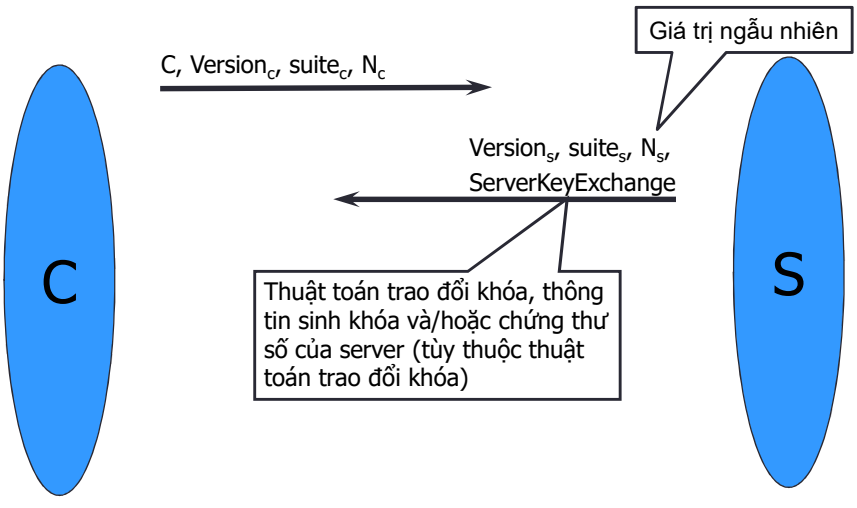
Server Hello



111

111

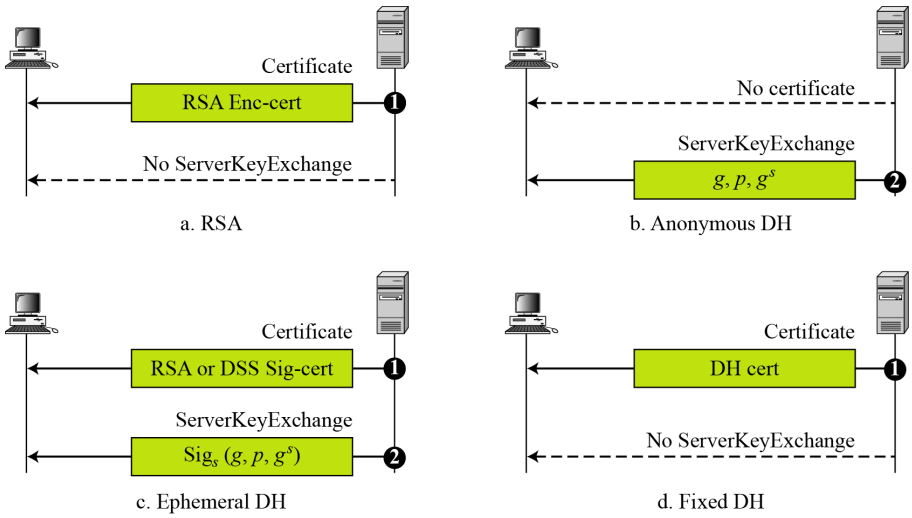
ServerKeyExchange



112

112

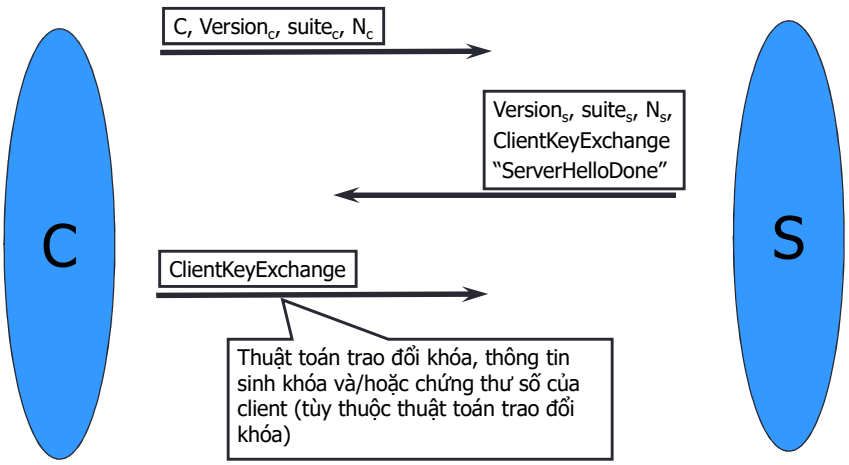
ServerKeyExchange



113

113

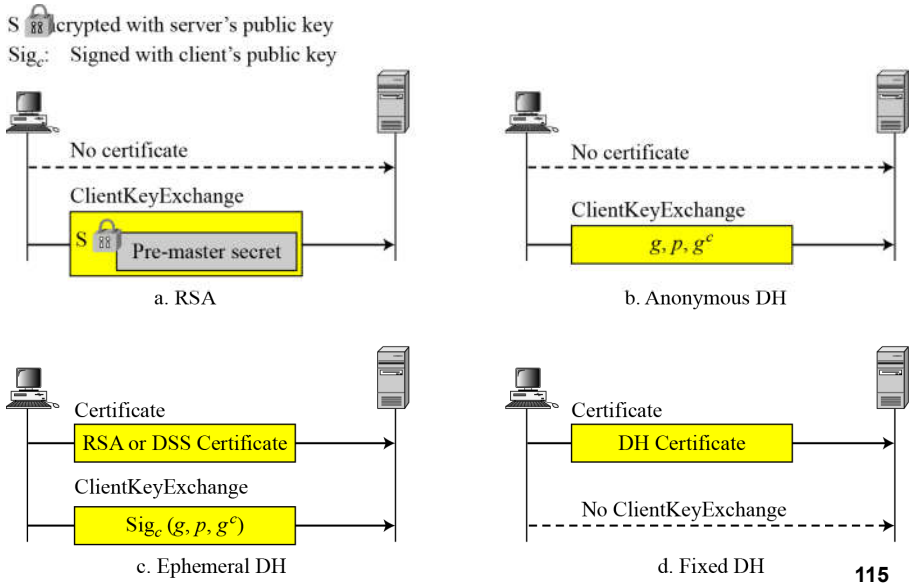
ClientKeyExchange



114

114

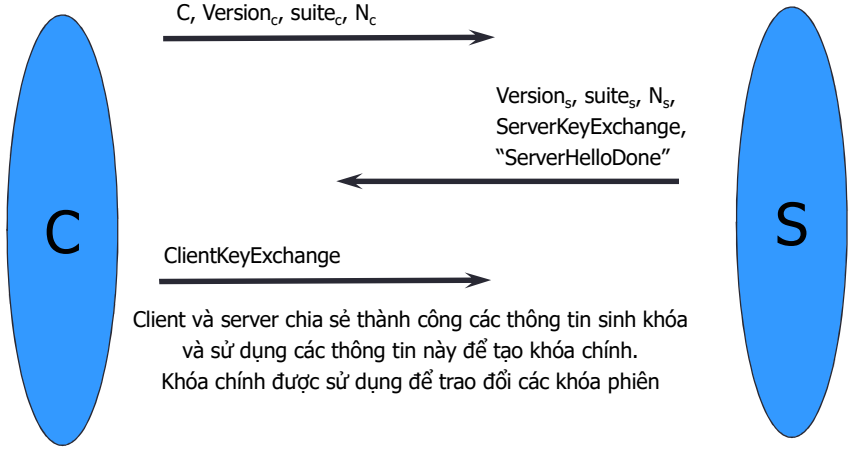
ClientKeyExchange



115

115

Hoàn tất giao thức bắt tay



Client và server chia sẻ thành công các thông tin sinh khóa và sử dụng các thông tin này để tạo khóa chính. Khóa chính được sử dụng để trao đổi các khóa phiên

116

116

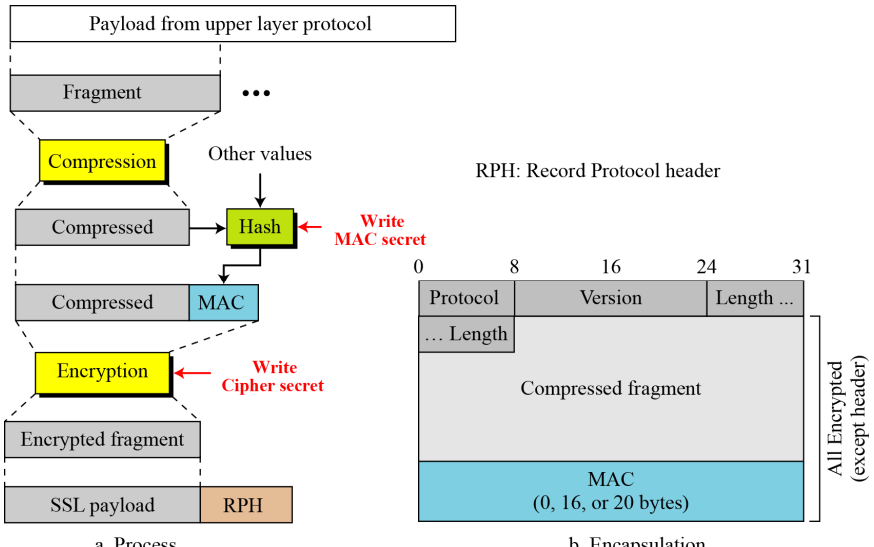
Các bộ thuật toán mã hóa trên TLS 1.0

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

117

117

Bảo vệ dữ liệu trên kênh SSL/TLS

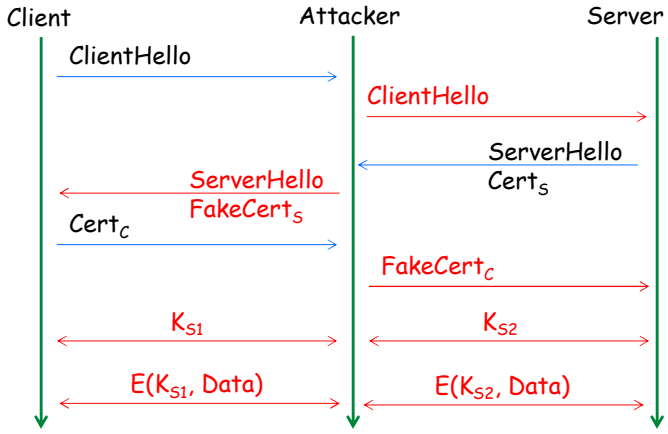


118

118

Tấn công man-in-the-middle

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



119

119

5.2. GIAO THỨC SSH

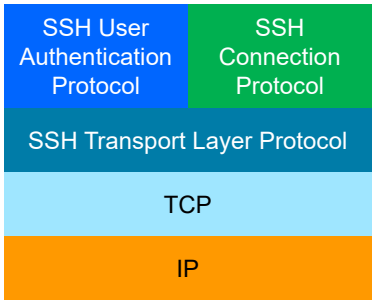
Bùi Trọng Tùng,
Viện Công nghệ thông tin và Truyền thông,
Đại học Bách khoa Hà Nội

120

120

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

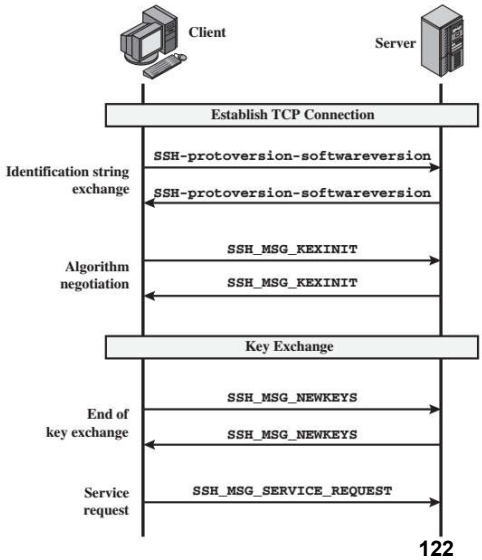


121

121

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)

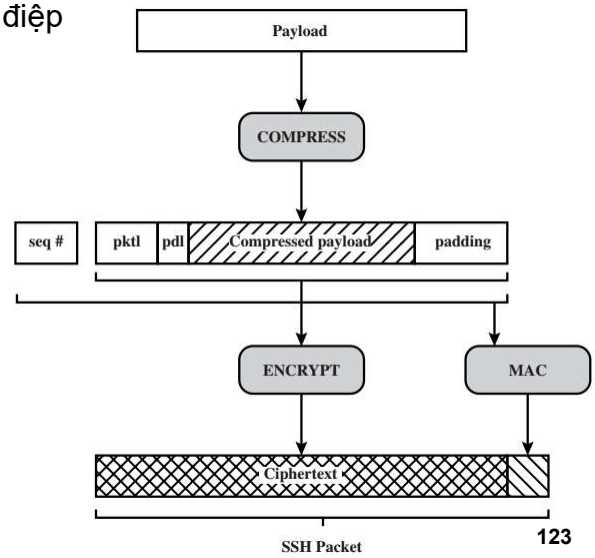


122

122

Transport Layer Protocol

- Khuôn dạng thông điệp



123

123

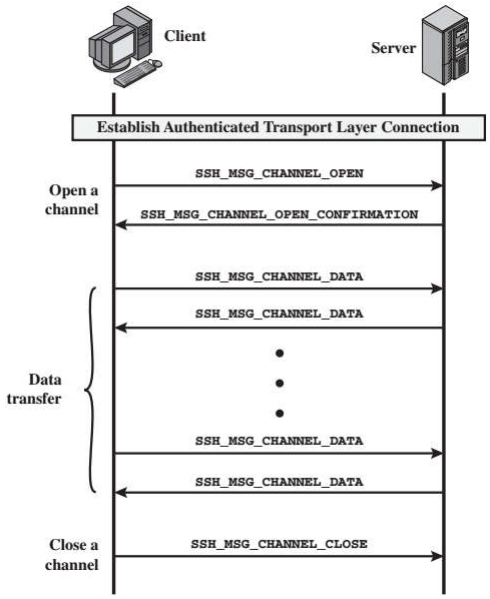
SSH User Authentication Protocol

- 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 snag 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

124

124

SSH Connection Protocol



125

125

An toàn bảo mật giao thức SSH

- Lỗ 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

126

126

5.3. AN TOÀN BẢO MẬT DỊCH VỤ DNS

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

127

127

Tổng quan về DNS

- Tên miền: định danh trên tầng ứng dụng cho các nút mạng
  - Trên Internet được quản lý tập trung
  - Quốc tế: ICANN
  - Việt Nam: VNNIC
- DNS(Domain Name System): hệ thống tên miền
  - Không gian thông tin tên miền
  - Gồm các máy chủ quản lý thông tin tên miền và cung cấp dịch vụ DNS
- Vấn đề phân giải tên miền sang địa chỉ IP
  - Người sử dụng dùng tên miền để truy cập dịch vụ
  - Máy tính và các thiết bị mạng không sử dụng tên miền mà dùng địa chỉ IP khi trao đổi dữ liệu

→Dịch vụ DNS: phân giải tên miền thành địa chỉ IP và ngược lại

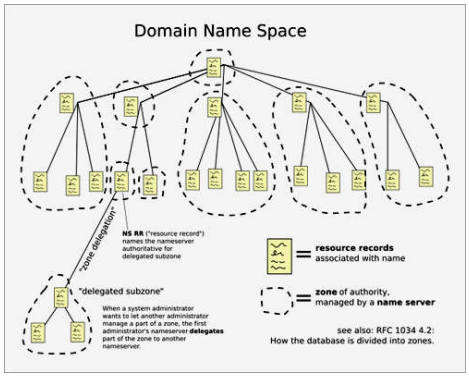
- UDP, cổng 53

128

128

Hệ thống tên miền

- Không gian tên miền
- Kiến trúc : hình cây
  - Root
  - Zone
- Mỗi nút là một tập hợp các bản ghi mô tả tên miền tương ứng với nút lá đó.
  - SOA
  - NS
  - A
  - PTR
  - CNAME



129

129

Hệ thống máy chủ DNS

- Máy chủ tên miền gốc (Root server)
  - Trả lời truy vấn cho các máy chủ cục bộ
  - Quản lý các zone và phân quyền quản lý cho máy chủ cấp dưới
  - Có 13 máy chủ gốc trên mạng Internet

130

130

Hệ thống máy chủ (tiếp)

- Máy chủ tên miền cấp 1 (Top Level Domain)
  - Quản lý tên miền cấp 1
- Máy chủ được ủy quyền (Authoritative DNS servers)
  - Quản lý tên miền cấp dưới
- Máy chủ của các tổ chức: của ISP
  - Không nằm trong phân cấp của DNS
- Máy chủ cục bộ: dành cho mạng nội bộ của cơ quan tổ chức
  - Không nằm trong phân cấp của DNS

131

131

Thông điệp DNS

- DNS Query và DNS Reply
  - Chung khuôn dạng
- QUESTION: tên miền cần truy vấn
  - Số lượng: #Question
- ANSWER: thông tin tên miền tìm kiếm được
  - Số lượng: #Answer RRs
- AUTHORITY: địa chỉ server trả lời truy vấn
- ADDITIONAL: thông tin phân giải tên miền cho các địa chỉ khác

SRC = 53	DST = 53
checksum	length
Identification	Flags
#Question	#Answer RRs
#Authority RRs	#Additional RRs
QUESTION	
ANSWER	
AUTHORITY	
ADDITIONAL	

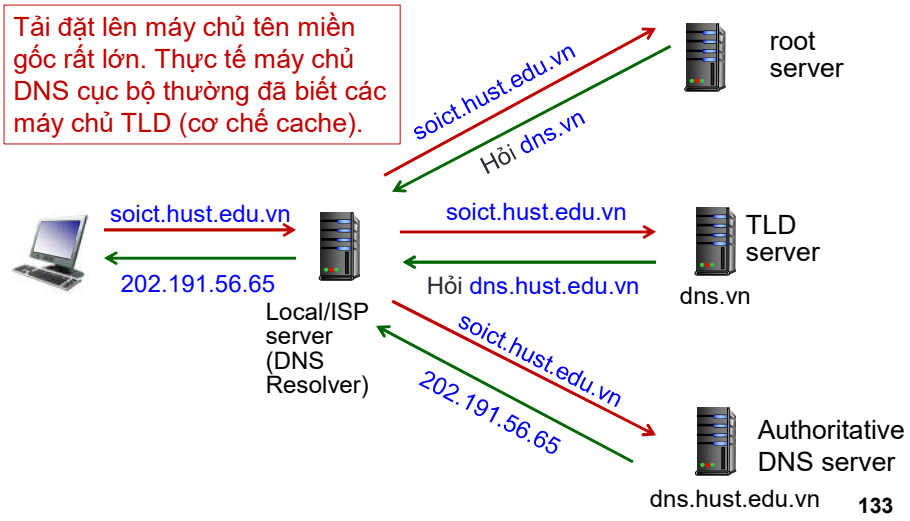
132

132

Phân giải tên miền

- Phân giải tương tác: Cơ chế mặc định trên các máy chủ DNS

Tải đặt lên máy chủ tên miền gốc rất lớn. Thực tế máy chủ DNS cục bộ thường đã biết các máy chủ TLD (cơ chế cache).

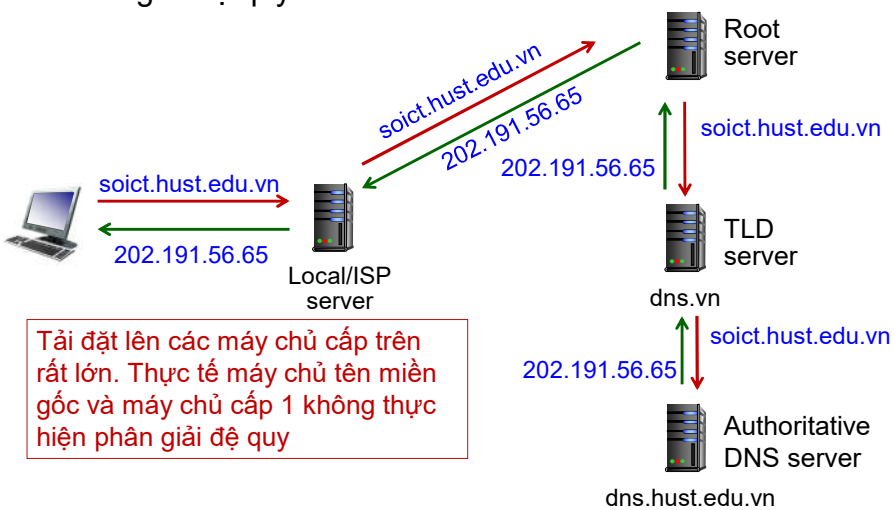


133

133

Phân giải tên miền

- Phân giải đệ quy



Tải đặt lên các máy chủ cấp trên rất lớn. Thực tế máy chủ tên miền gốc và máy chủ cấp 1 không thực hiện phân giải đệ quy

134

134

dig linux.com

```
; <> DiG 9.9.2-P1 <> linux.com
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 21655
;; flags: qr rd ra; QUERY: 1, ANSWER: 2, AUTHORITY: 2,
ADDITIONAL: 3
;; QUESTION SECTION:
;linux.com. IN A
;; ANSWER SECTION:
linux.com. 1786 IN A 140.211.167.51
linux.com. 1786 IN A 140.211.167.50
;; AUTHORITY SECTION:
linux.com. 86386 IN NS ns1.linux-foundation.org.
linux.com. 86386 IN NS ns2.linux-foundation.org.
;; ADDITIONAL SECTION:
ns1.linux-foundation.org. 261 IN A 140.211.169.10
ns2.linux-foundation.org. 262 IN A 140.211.169.11
```

TTL: thời gian(s) lưu giữ trả lời trong cache

135

135

dig linux.com

```
; <> DiG 9.9.2-P1 <> linux.com
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 21655
;; flags: qr rd ra; QUERY: 1, ANSWER: 2, AUTHORITY: 2,
ADDITIONAL: 3
;; QUESTION SECTION:
;linux.com. IN A
;; ANSWER SECTION:
linux.com. 1786 IN A 140.211.167.51
linux.com. 1786 IN A 140.211.167.50
;; AUTHORITY SECTION:
linux.com. 86386 IN NS ns1.linux-foundation.org.
linux.com. 86386 IN NS ns2.linux-foundation.org.
;; ADDITIONAL SECTION:
ns1.linux-foundation.org. 261 IN A 140.211.169.10
ns2.linux-foundation.org. 262 IN A 140.211.169.11
```

Tên các máy chủ DNS server trả lời truy vấn. Nếu phần ANSWER rỗng, DNS Resolver gửi truy vấn tới các máy chủ này

136

136

dig linux.com

```
; <> DiG 9.9.2-P1 <> linux.com
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 21655
;; flags: qr rd ra; QUERY: 1, ANSWER: 2, AUTHORITY: 2,
ADDITIONAL: 3
;; QUESTION SECTION:
;linux.com. IN A
;; ANSWER SECTION:
linux.com. 1786 IN A 140.211.167.51
linux.com. 1786 IN A 140.211.167.50
;; AUTHORITY SECTION:
linux.com. 86386 IN NS ns1.linux-foundation.org.
linux.com. 86386 IN NS ns2.linux-foundation.org.
;; ADDITIONAL SECTION:
ns1.linux-foundation.org. 261 IN A 140.211.169.10
ns2.linux-foundation.org. 262 IN A 140.211.169.11
```

Địa chỉ IP của các máy chủ trả lời truy vấn. Thông tin này được lưu vào cache

137

137

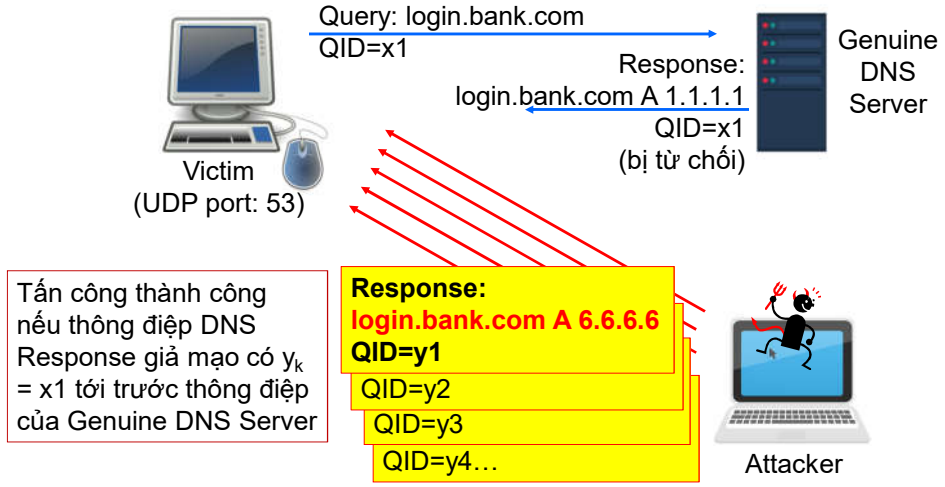
Một số dạng tấn công DNS

- Các vấn đề của DNS
  - Không có cơ chế xác thực thông tin phân giải
  - Không cần thiết lập kết nối
- Tấn công vào máy chủ cung cấp dịch vụ: DoS/DDoS, tấn công khai thác các lỗi phần mềm
- Tấn công vào giao thức DNS:
  - DNS cache poisioning
  - DNS spoofing
  - DNS rebinding
- Tấn công DDoS lợi dụng Open DNS Resolver
- DNS Amplification attack

138

138

DNS Spoofing

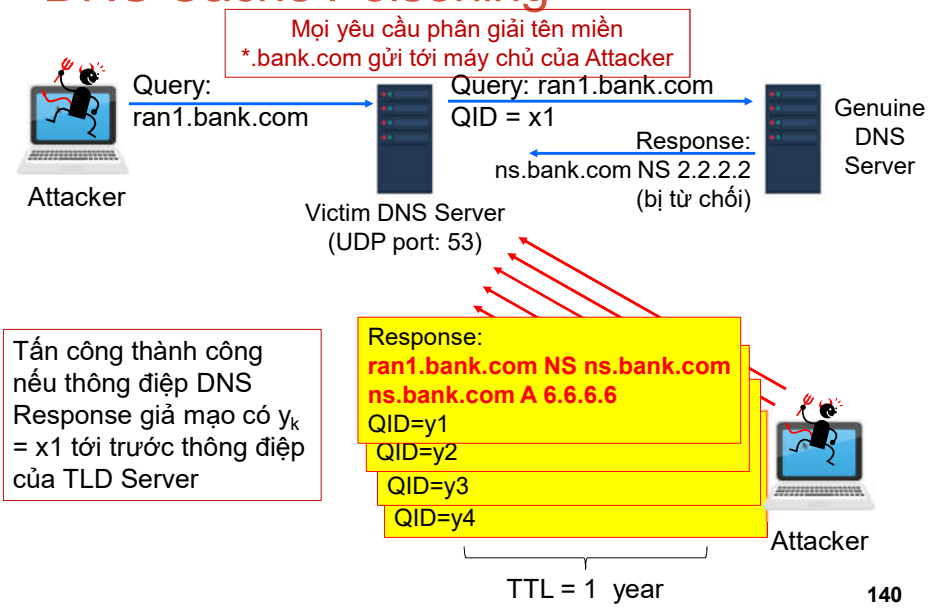


Tấn công thành công nếu thông điệp DNS Response giả mạo có y_k = x1 tới trước thông điệp của Genuine DNS Server

139

139

DNS Cache Poisoning



Tấn công thành công nếu thông điệp DNS Response giả mạo có y_k = x1 tới trước thông điệp của TLD Server

140

140

DNS cache poisioning

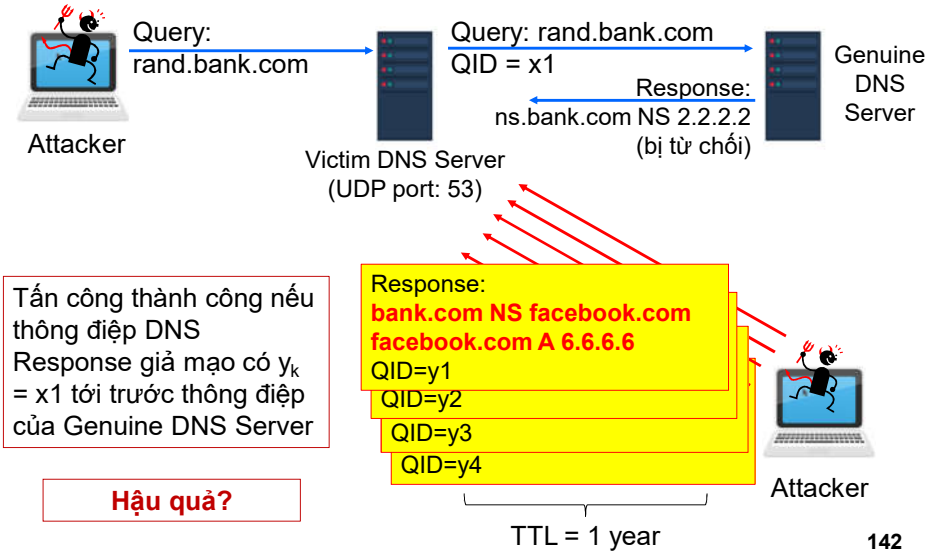
```
; <> DiG 9.9.2-P1 <> a.bank.com
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 21655
;; flags: qr rd ra; QUERY: 1, ANSWER: 0, AUTHORITY: 1,
ADDITIONAL: 1
;; QUESTION SECTION:
;a.bank.com. IN A
;; ANSWER SECTION:
;; AUTHORITY SECTION:
a.bank.com. 86386 IN NS ns.bank.com.
;; ADDITIONAL SECTION:
ns.bank.com. 261 IN A 6.6.6.6
```

Địa chỉ của máy chủ do kẻ tấn công điều khiển

141

141

DNS Cache Poisoning: cross-domain



Tấn công thành công nếu thông điệp DNS Response giả mạo có y_k = x1 tới trước thông điệp của Genuine DNS Server

Hậu quả?

142

142

dig rand.bank.com

```
; <> DiG 9.9.2-P1 <> rand.bank.com
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 21655
;; flags: qr rd ra; QUERY: 1, ANSWER: 0, AUTHORITY: 2,
ADDITIONAL: 2
;; QUESTION SECTION:
rand.bank.com. IN A
;; ANSWER SECTION:
;; AUTHORITY SECTION:
bank.com. 86386 IN NS ns.bank.com.
bank.com. 86386 IN NS facebook.com.
;; ADDITIONAL SECTION:
ns.bank.com. 261 IN A 140.211.169.10
facebook.com. 262 IN A 6.6.6.6
```

Tên miền bị tấn công

143

143

DNS cache poisioning (tiếp)

- Nếu giá trị QueryID được sử dụng là ngẫu nhiên, xác suất thành công của kẻ tấn công không cao:
  - $P = k/2^{16}$
  - Thông điệp giả mạo có giá trị QueryID phù hợp phải đến trước thông điệp của DNS server tin cậy
- Cải tiến:
  - Tấn công DoS vào máy chủ NS
  - Sử dụng kỹ thuật tấn công ngày sinh

144

144

DNS cache poisioning (D.Kaminsky '08)

- Kẻ tấn công gửi một loạt các yêu cầu truy vấn tên miền không tồn tại có cùng tên miền cấp trên với tên miền giả mạo
  - Ví dụ: random1.google.com, random2.google.com,…
- Gửi các thông điệp trả lời giả mạo với thông tin thêm vào phần Authority và Additional
- Phòng chống: DNS server sử dụng số hiệu cổng ngẫu nhiên khi gửi thông điệp truy vấn

145

145

DNS cache poisioning (D.Kaminsky '08)

```
;; QUESTION SECTION:
;randomX.google.com. IN A

;; ANSWER SECTION:
randomX.google.com. 21600 IN A don't matter

;; AUTHORITY SECTION:
google.com. 86386 IN NS mail.google.com.

;; ADDITIONAL SECTION:
mail.google.com. 86386 IN A 6.7.8.9
```

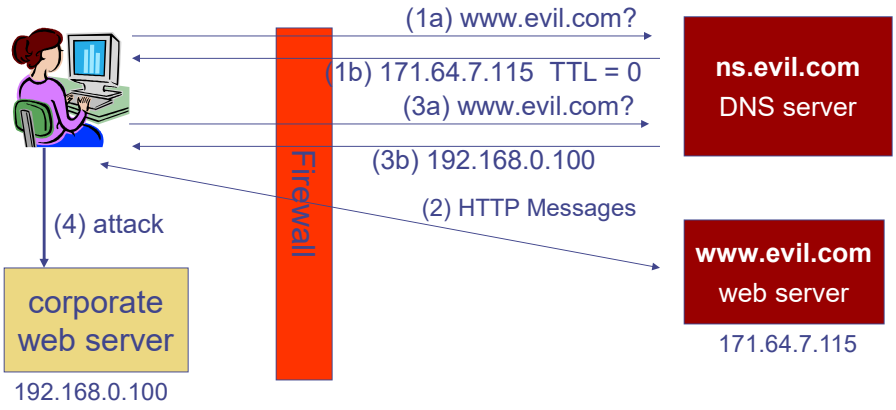
Hậu quả nếu kịch bản tấn công thành công, thông điệp trên được chấp nhận?

146

146

DNS Rebinding

<iframe src="**http://www.evil.com**">



147

147

Phòng chống tấn công DNS Rebinding

- Trình duyệt: DNS Pinning
  - Từ chối thay đổi ánh xạ tên miền sang địa chỉ IP khác trong một khoảng thời gian
  - Hạn chế tương tác với proxy, VPN, Dynamic DNS
- Máy trạm người dùng: sử dụng dịch vụ DNS tin cậy
- Máy chủ:
  - Từ chối các thông điệp HTTP request có trường Host là một tên miền không nhận diện được
  - Xác thực người dùng
- Firewall: chặn các thông điệp DNS Reponse phân giải tên miền thành 1 địa chỉ cục bộ

148

148

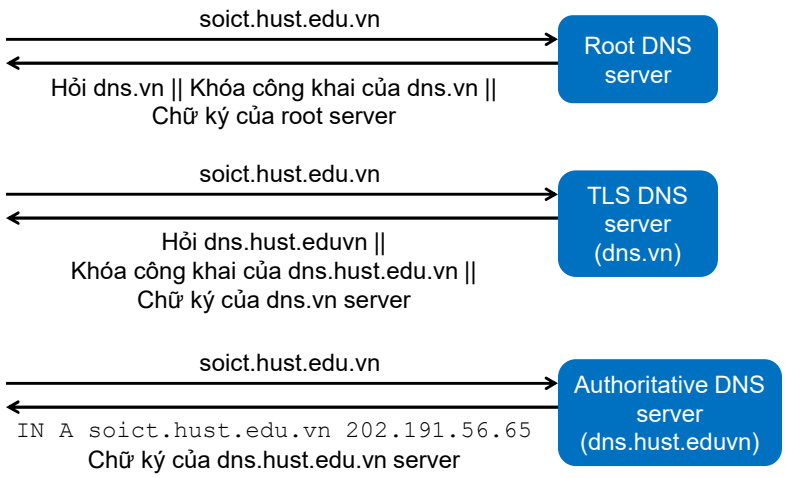
Làm thế nào để dịch vụ DNS an toàn hơn

- Ý tưởng cơ bản: sử dụng mật mã học
- Giải pháp 1: sử dụng kết nối SSL/TLS
  - Phân tích?
- Giải pháp 2: chứng thực bản ghi DNS
  - DNSSEC
  - Phân tích?

149

149

DNSSEC



150

150

5.4. AN TOÀN BẢO MẬT DỊCH VỤ EMAIL(TỰ HỌC)

Pretty Good Privacy

S/MIME

151

151

Bài giảng sử dụng một số hình vẽ và ví dụ từ các khóa học:

- Computer and Network Security, Stanford University
- Computer Security, Berkeley University
- Network Security, Illinois University

152

152