



Bài 9. An toàn an ninh mạng

ONE LOVE. ONE FUTURE.

1

Nội dung

- Tổng quan về mạng máy tính
- An toàn bảo mật các giao thức trong TCP/IP
- Tấn công từ chối dịch vụ

2

1. Tổng quan về mạng máy tính

ONE LOVE. ONE FUTURE.

3

Mạng máy tính là gì?

- Tập hợp các máy tính điện tử kết nối với nhau

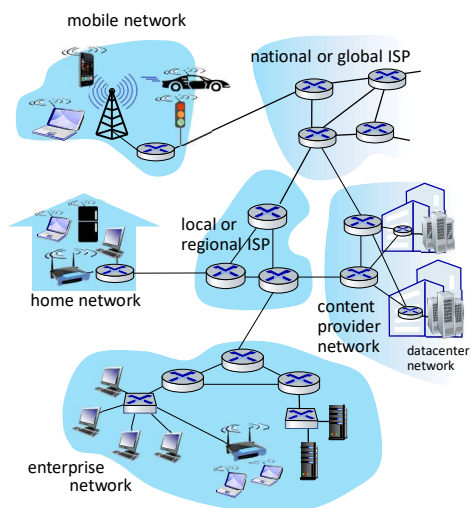
- Máy tính đầu cuối (nút mạng)



- Thiết bị mạng



- Sử dụng các loại đường truyền khác nhau để kết nối
- Triển khai theo một kiến trúc mạng nào đó



Nguồn: "Computer Networking: A Top Down Approach", J.Kurose

4

Mạng máy tính là gì?

- Phương tiện truyền: đường truyền vật lý:
 - Hữu tuyến: cáp đồng, cáp quang
 - Vô tuyến: sóng hồng ngoại, sóng radio
- Kiến trúc mạng:
 - Hình trạng mạng: cách thức các máy tính kết nối bằng đường truyền vật lý với nhau
 - Giao thức mạng: cách thức các máy tính trao đổi dữ liệu với nhau như thế nào?
- Hoạt động cơ bản trên hệ thống mạng máy tính: truyền thông tin từ máy tính này sang máy tính khác
 - Tương tự như con người trao đổi thư tín qua hệ thống bưu điện
 - Máy nguồn: gửi dữ liệu
 - Máy đích: nhận dữ liệu

5

Truyền thông tin trên mạng máy tính?

- Thông tin được tổ chức như thế nào?
 - Cú pháp?
 - Ngữ nghĩa?
- Định danh – đánh địa chỉ: Phân biệt các máy với nhau trên mạng?
- Tìm đường đi cho thông tin qua hệ thống mạng như thế nào?
- Làm thế nào để thông tin gửi đi không bị lỗi?
- Làm thế nào để thông tin gửi đi không làm quá tải đường truyền, quá tải máy nhận?
- Làm thế nào để chuyển dữ liệu thành tín hiệu?
- Làm thế nào để biết thông tin đã tới đích?
- ...

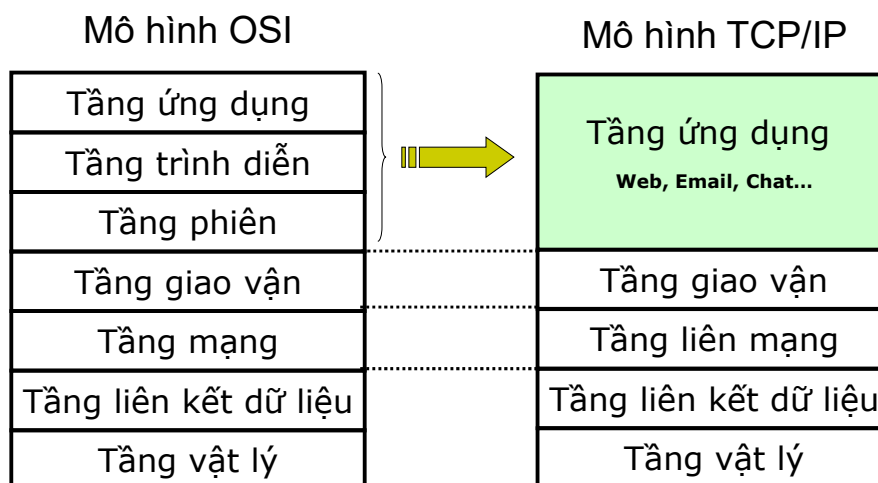
6

Kiến trúc phân tầng

- Để truyền thông tin từ máy này sang máy khác: cần giải quyết rất nhiều vấn đề → hệ thống mạng cần rất nhiều chức năng
- Kiến trúc phân tầng: chia các chức năng của hệ thống mạng thành các tầng. Các chức năng ở mỗi tầng được thực hiện/điều khiển bởi một hoặc nhiều giao thức
 - Dễ dàng xây dựng và thiết kế
 - Dễ dàng nâng cấp, thay đổi từng thành phần
- Các mô hình tiêu biểu:
 - Mô hình OSI: có ý nghĩa tham chiếu
 - Mô hình TCP/IP: được sử dụng trên thực tế

7

Mô hình OSI và mô hình TCP/IP



8

Mô hình TCP/IP – Tầng ứng dụng

- Cung cấp dịch vụ mạng cho người dùng
- Phối hợp hoạt động của chương trình client và chương trình server
 - Client: cung cấp giao diện cho người dùng
 - Server: đáp ứng dịch vụ
- Một số dịch vụ tiêu biểu: Web, Email, Lưu trữ và chia sẻ file (FTP)...
- Mô hình cung cấp dịch vụ:
 - Client/Server
 - Ngang hàng
 - Mô hình lai
- Máy chủ cung cấp dịch vụ thường được định danh bằng tên miền

9

Mô hình TCP/IP – Tầng giao vận

- Điều khiển quá trình trao đổi dữ liệu giữa các chương trình của tầng ứng dụng trên các hệ thống đầu-cuối
- Hai giao thức:
 - TCP: tin cậy
 - Chỉ gửi khi máy đích sẵn sàng nhận
 - Kiểm tra chắc chắn dữ liệu đã tới máy đích
 - Gửi lại dữ liệu khi có lỗi hoặc khi mất dữ liệu
 - UDP: không tin cậy, gửi ngay dữ liệu, không quan tâm đến tình trạng máy đích và hệ thống trung gian

10

Mô hình TCP/IP - Tầng liên mạng

- Cung cấp các cơ chế để kết nối các hệ thống mạng với nhau (internetworking)
 - Mạng của các mạng
- Giao thức IP : Internet Protocol
 - Định danh: sử dụng địa chỉ IP để gán cho các nút mạng (máy trạm, máy chủ, bộ định tuyến)
 - Khuôn dạng dữ liệu
- Định tuyến(chọn đường): tìm các tuyến đường tốt nhất qua hệ thống trung gian để gửi thông tin
- Chuyển tiếp: quyết định gửi dữ liệu qua tuyến đường nào

Mô hình TCP/IP – Tầng liên kết dữ liệu

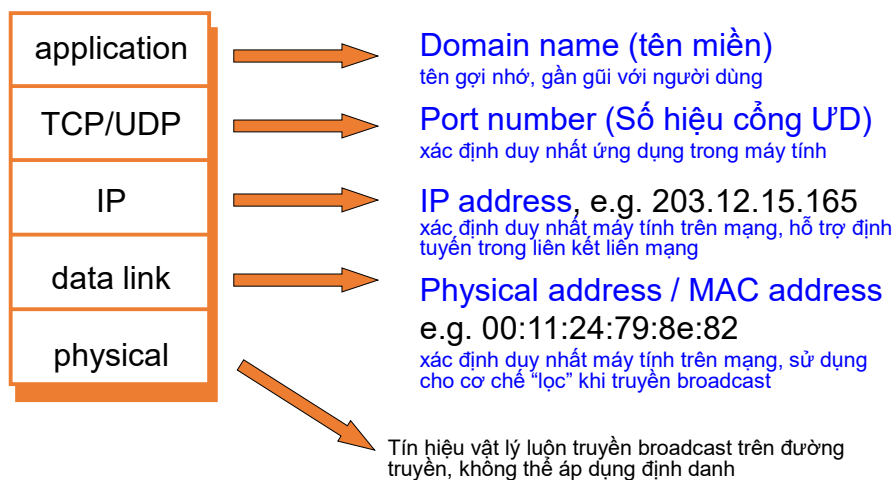
- Điều khiển truyền tin trên liên kết vật lý giữa các nút mạng
 - Thiết lập kênh truyền
 - Điều khiển truy nhập kênh truyền khi có nhiều nút mạng dùng chung đường truyền:
 - Khi nào được gửi dữ liệu lên đường truyền
 - Phát hiện và xử lý tranh chấp khi có nhiều nút mạng cùng gửi dữ liệu lên đường truyền
 - Độ ưu tiên của các nút mạng
 - Điều khiển luồng: tốc độ gửi dữ liệu trên nút nguồn phù hợp với nút đích
 - Phát hiện và sửa lỗi trên gói tin
- Chuyển tiếp dữ liệu từ liên kết vật lý này sang liên kết vật lý khác

Mô hình TCP/IP – Tầng vật lý

- Quy định cách thức điều chế các bit thành tín hiệu số (xung vuông)
- Quy định cách thức điều chế tín hiệu số thành tín hiệu tương tự để truyền đi
- Một số chuẩn phổ biến hiện nay cho mạng LAN:
 - Cáp xoắn đôi: 100-BASE-T, 1000-BASE-T
 - Cáp quang: 1000-BASE-SX, 1000-BASE-LX
 - Không dây: WiFi (a/b/g/n)

13

Định danh trên kiến trúc phân tầng



14

Định danh trên kiến trúc phân tầng

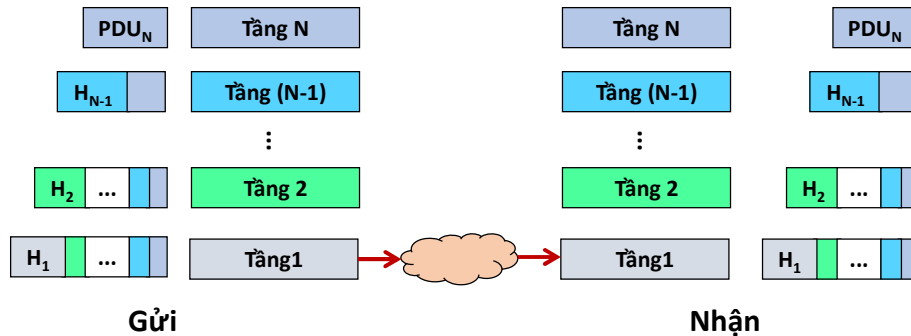
- Tầng ứng dụng : **tên miền** định danh cho máy chủ cung cấp dịch vụ
 - Tên miền: chuỗi ký tự dễ nhớ với người dùng. Thiết bị mạng không dùng tên miền khi truyền tin
 - Ví dụ: hust.edu.vn (máy chủ Web của ĐHBK Hà Nội)
- Tầng giao vận: **số hiệu cổng** định danh cho các dịch vụ khác nhau
 - Số hiệu cổng: từ 1-65535
 - Ví dụ: Web-80, DNS-53, Email(SMTP-25, POP-110, IMAP-143)

Định danh trên kiến trúc phân tầng

- Tầng mạng: **địa chỉ IP** định danh cho các máy trạm, máy chủ, bộ định tuyến
 - Có thể dùng trong mạng nội bộ và mạng Internet
 - Địa chỉ IPv4: 32 bit
 - Địa chỉ IPv6: 128 bit
- Tầng liên kết dữ liệu: **địa chỉ MAC** định danh cho các máy trạm, máy chủ, thiết bị mạng
 - Kích thước: 48 bit
 - Biểu diễn bằng dạng hexa
 - Chỉ dùng trong mạng nội bộ

Truyền thông trong kiến trúc phân tầng

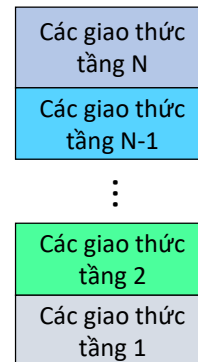
- Bên gửi: thêm tiêu đề chứa thông tin phục vụ cho việc xử lý dữ liệu tại tầng tương ứng và chuyển cho tầng dưới (Đóng gói dữ liệu - Encapsulation)
- Bên nhận: xử lý dữ liệu theo thông tin trong phần tiêu đề, tách tiêu đề và chuyển dữ liệu cho tầng trên



17

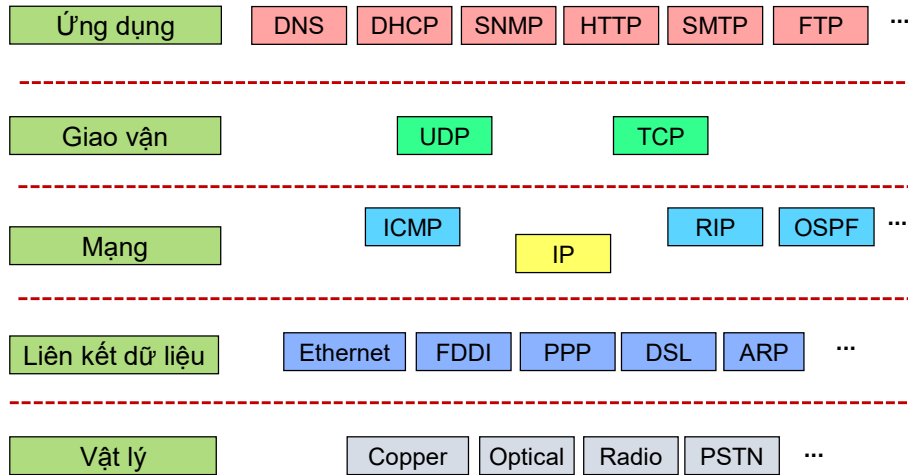
Chồng giao thức (Protocol stack)

- Các chức năng được phân chia cho các tầng
 - Mỗi tầng có nhiều cách thức để thực hiện các chức năng → sinh ra các giao thức khác nhau
- chồng giao thức: ngăn xếp các giao thức truyền thông trên kiến trúc phân tầng
- Giao thức mỗi tầng bao gồm:
- Gọi dịch vụ nào của giao thức tầng dưới
 - Và cung cấp dịch vụ cho giao thức tầng trên như thế nào



18

Chồng giao thức TCP/IP



19

Một số giao thức trong TCP/IP

ONE LOVE. ONE FUTURE.

20

Giao thức IP

- Internet Protocol
- Các phiên bản: IPv4, IPv6
- Là giao thức thuộc tầng liên mạng
- Cung cấp chức năng để điều khiển truyền dữ liệu giữa các mạng khác nhau
 - Thống nhất định danh: sử dụng địa chỉ IP
 - Thống nhất cách thức đóng gói và xử lý dữ liệu
 - Không phụ thuộc vào hạ tầng vật lý
 - Cho phép các dịch vụ tầng trên triển khai trên mọi hệ thống mạng

Giao thức ICMP

- Internet Control Message Protocol
- Giao thức thuộc tầng liên mạng
- Giao thức điều khiển hoạt động báo lỗi khi chuyển tiếp gói tin IP
- Lệnh ping
 - Sử dụng để kiểm tra kết nối
 - Gửi gói tin ICMP echo request
 - Bên nhận trả về ICMP echo reply

Các giao thức định tuyến

- Chức năng chính: tìm các tuyến đường tốt nhất trên hệ thống trung gian để gửi dữ liệu
- Triển khai trên các bộ định tuyến
- Hoạt động chính:
 - Các bộ định tuyến trao đổi thông tin với nhau:
 - Các tuyến đường đã biết
 - Hoặc các thông tin về liên kết vật lý
 - Thu thập các thông tin nhận được từ bộ định tuyến khác và tìm tuyến đường.
- Một số giao thức định tuyến: RIP, OSPF, BGP

23

Giao thức UDP

- Giao thức nằm trên tầng giao vận
- Truyền thông hướng không liên kết: Dữ liệu được gửi đi ngay
- Điều khiển truyền dữ liệu theo mô hình không tin cậy:
 - Không phát lại khi có lỗi
- Vì sao cần UDP?
 - Nhanh
 - Đơn giản
 - Phù hợp các dịch vụ không cần độ tin cậy cao, chấp nhận mất mát một số gói tin mà không ảnh hưởng tới chất lượng dịch vụ
 - Một số dịch vụ không thể thiết lập liên kết trước khi cung cấp. Ví dụ: DHCP, SNMP (Giao thức quản trị mạng)

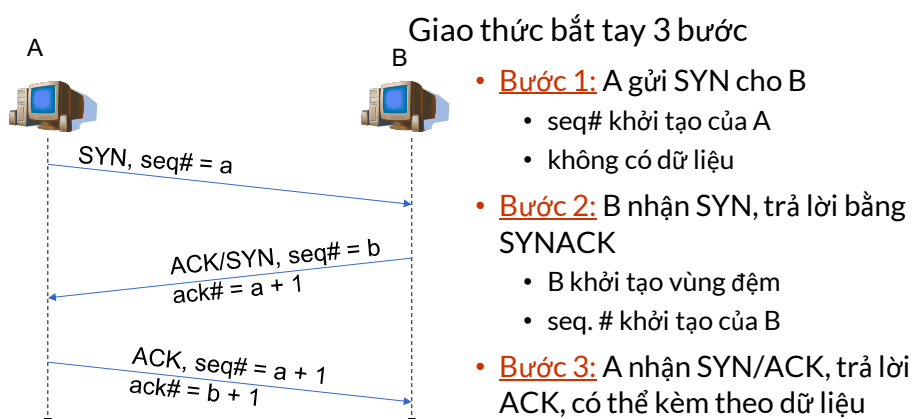
24

Giao thức TCP

- Giao thức nằm trên tầng giao vận
- Giao thức truyền thông hướng liên kết:
 - Thiết lập liên kết: bắt tay 3 bước
 - Truyền dữ liệu
 - Đóng liên kết
- Điều khiển truyền dữ liệu theo mô hình tin cậy:
 - Phát hiện mất gói tin
 - Phát hiện lỗi dữ liệu
 - Sử dụng cơ chế báo nhận phát lại

25

Thiết lập liên kết TCP



26

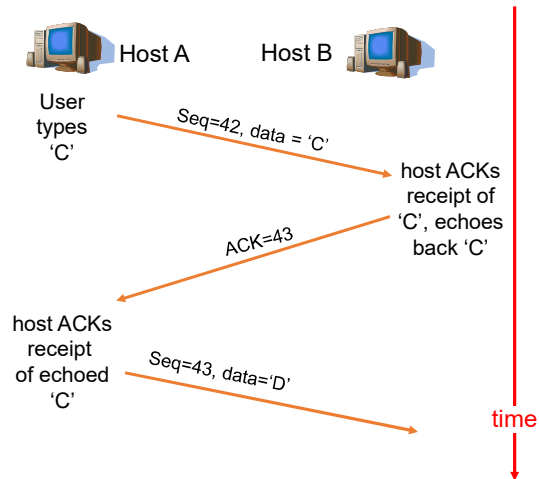
Cơ chế báo nhận trong TCP

Seq. #:

- Số hiệu của byte đầu tiên của đoạn tin trong dòng dữ liệu

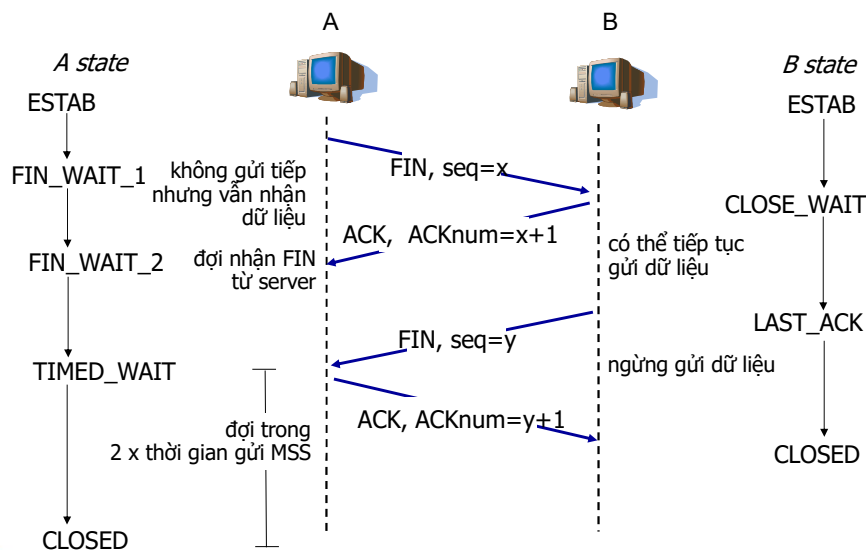
ACK:

- Số hiệu byte đầu tiên mong muốn nhận từ đối tác



27

Đóng liên kết



28

Giao thức DNS

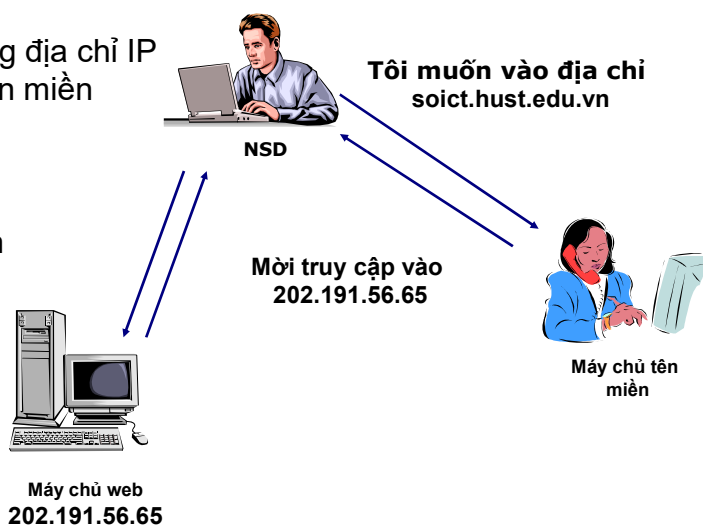
- Điều khiển dịch vụ tên miền
 - Giao thức giao vận: UDP/TCP
 - Số hiệu cổng dịch vụ: 53
- Máy trạm yêu cầu dịch vụ có thể gửi ngay thông điệp truy vấn tên miền
 - Không cần máy chủ DNS cho phép
 - Không cần kiểm tra trạng thái của máy chủ
- Máy trạm không kiểm tra tính tin cậy của câu trả lời từ máy chủ
- Câu trả lời từ máy chủ có thể được sử dụng lại cho những lượt khác

29

Phân giải tên miền và ví dụ

- Máy tính dùng địa chỉ IP
- NSD dùng tên miền

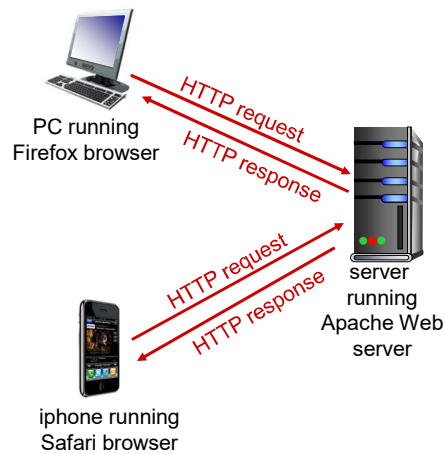
↓
Cần có chuyển đổi địa chỉ



30

HTTP và Web

- WWW: World Wide Web
 - trao đổi dữ liệu siêu văn bản HTML (HyperText Markup Language) trên mạng
- HTTP: HyperText Transfer Protocol
 - Mô hình Client/Server
 - Client yêu cầu truy nhập tới các trang web (chứa các đối tượng web) và hiển thị chúng trên trình duyệt
 - Server: Nhận yêu cầu và trả lời cho client



Hình ảnh từ: "Computer Networking: A Top Down Approach", Jim Kurose

Hoạt động của HTTP

- Thiết lập liên kết TCP
 - Server mở một TCP socket chờ yêu cầu kết nối tại cổng 80 (mặc định)
 - Client khởi tạo một liên kết TCP tới server
 - Server chấp nhận yêu cầu, tạo liên kết
- Trao đổi thông điệp HTTP (giao thức ứng dụng)
 - HTTP Request: Thông điệp yêu cầu
 - HTTP Response: Thông điệp trả lời
- Đóng liên kết TCP

Khuôn dạng HTTP request

- Mã ASCII (dễ dàng đọc được dưới dạng văn bản)

Dòng yêu cầu

Các dòng tiêu đề

Báo kết thúc tiêu đề

```
GET /~tungbt/index.htm HTTP/1.1\r\nHost: soict.hust.edu.vn\r\nUser-Agent: Mozilla/5.0\r\nAccept: text/html,application/xhtml+xml\r\nAccept-Language: en-us,en;q=0.5\r\nAccept-Encoding: gzip,deflate\r\nAccept-Charset: ISO-8859-1,utf-8;q=0.7\r\nKeep-Alive: 115\r\nConnection: keep-alive\r\n\r\n
```

33

Khuôn dạng HTTP response

Dòng trạng thái trả lời

Các dòng tiêu đề

Dữ liệu đáp ứng yêu cầu

```
HTTP/1.1 200 OK\r\nDate: Thu, 31 Jul 2014 00:00:14 GMT\r\nServer: Apache/2.2.15 (CentOS)\r\nLast-Modified: Wed, 30 Jul 2014 23:59:50 GMT\r\nETag: "17dc6-a5c-bf716880"\r\nAccept-Ranges: bytes\r\nContent-Length: 2652\r\nConnection: close\r\nContent-Type: text/html; charset=UTF-8\r\n\r\ndata data data data data ...
```

34

2. An toàn bảo mật trong mạng TCP/IP

ONE LOVE. ONE FUTURE.

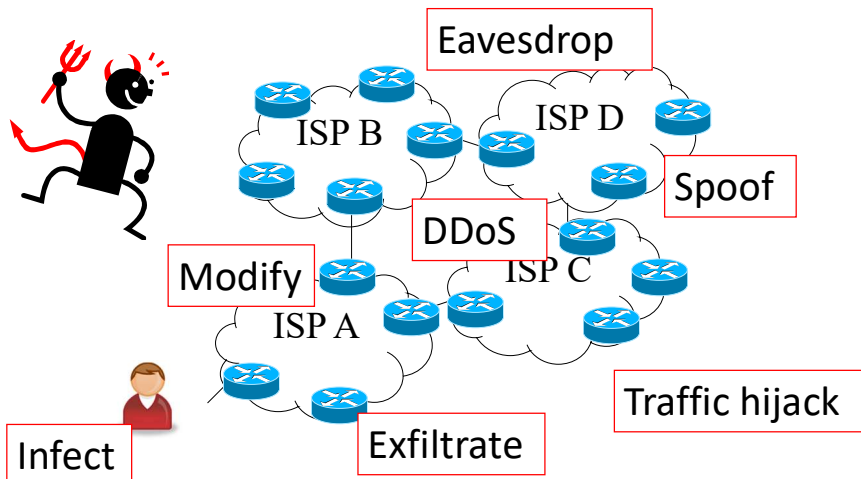
35

Vấn đề an toàn bảo mật

- Giao thức IP không sử dụng các cơ chế bảo vệ dữ liệu
- Không mã hóa giữ bí mật nội dung gói tin
 - Đe dọa tấn công: Nghe lén dữ liệu
- Không có mã xác thực toàn vẹn nội dung
 - Đe dọa tấn công: Sửa đổi dữ liệu
- Không xác thực địa chỉ nguồn
 - Đe dọa tấn công: Gửi gói tin với địa chỉ IP tùy ý để giả danh
- Phần lớn các giao thức khác cũng giống giao thức IP

36

Các mối đe dọa



37

Tấn công các giao thức định tuyến

- RIPv1: không hỗ trợ các cơ chế xác thực thông tin trao đổi giữa các nút
- 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,

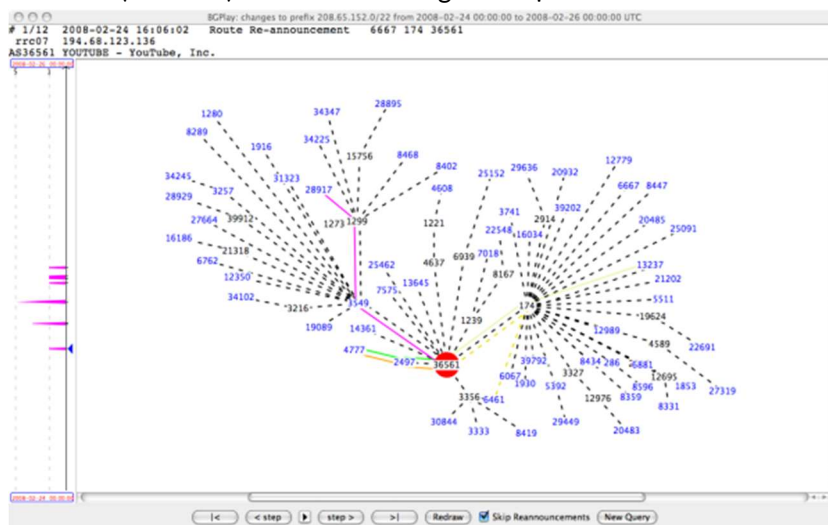
38

Ví dụ: Tấn công BGP hijacking

- 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

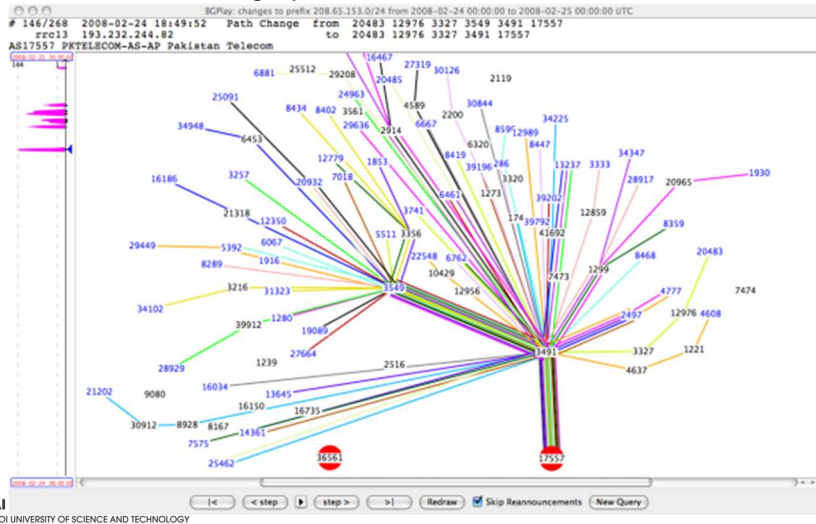
BGP hijacking – Tấn công Youtube

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



BGP hijacking – Tấn công Youtube

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



41

41

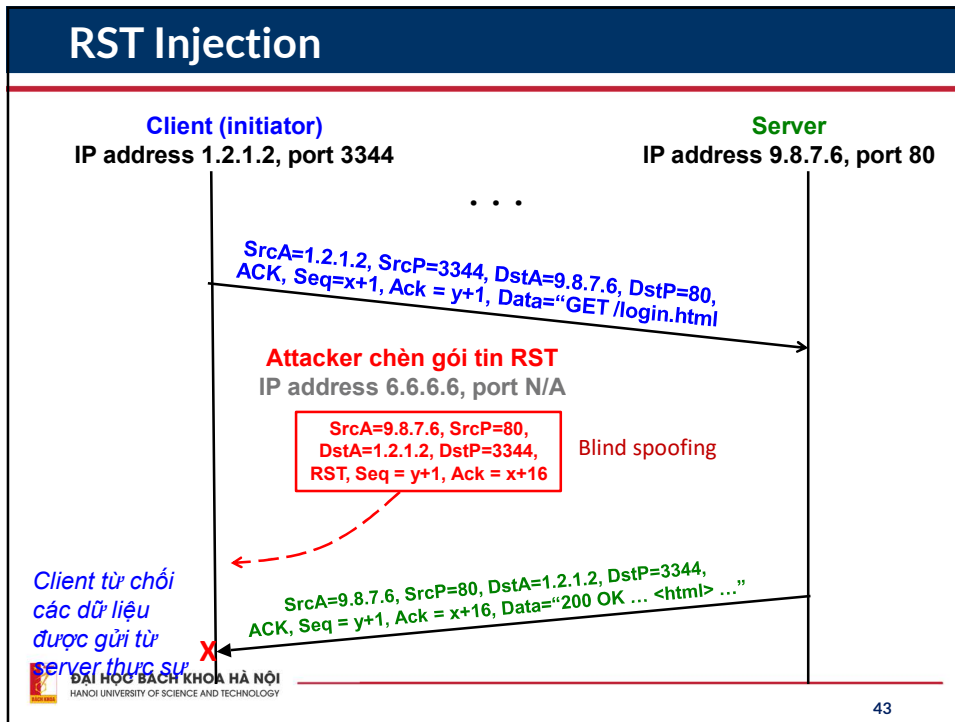
Tấn công can thiệp vào kết nối TCP

- 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

42

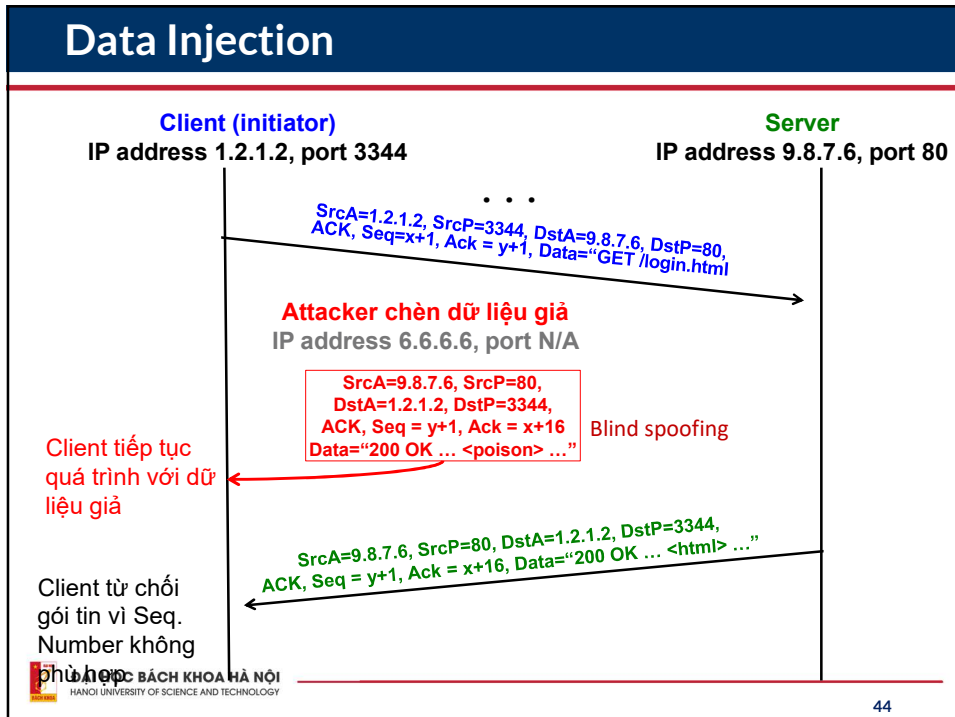
42

RST Injection



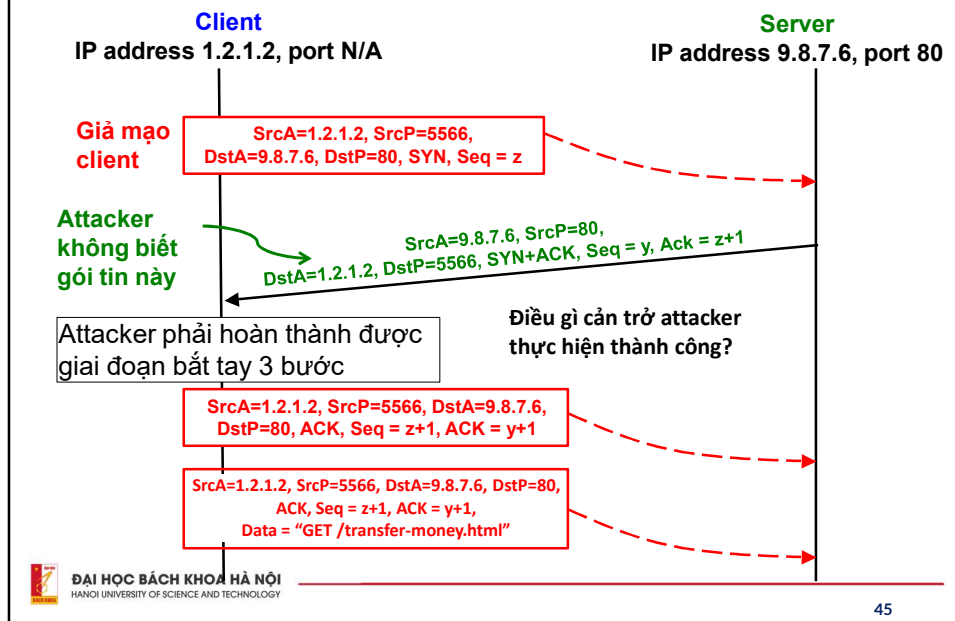
43

Data Injection



44

Giả mạo kết nối TCP (TCP Spoofing)



45

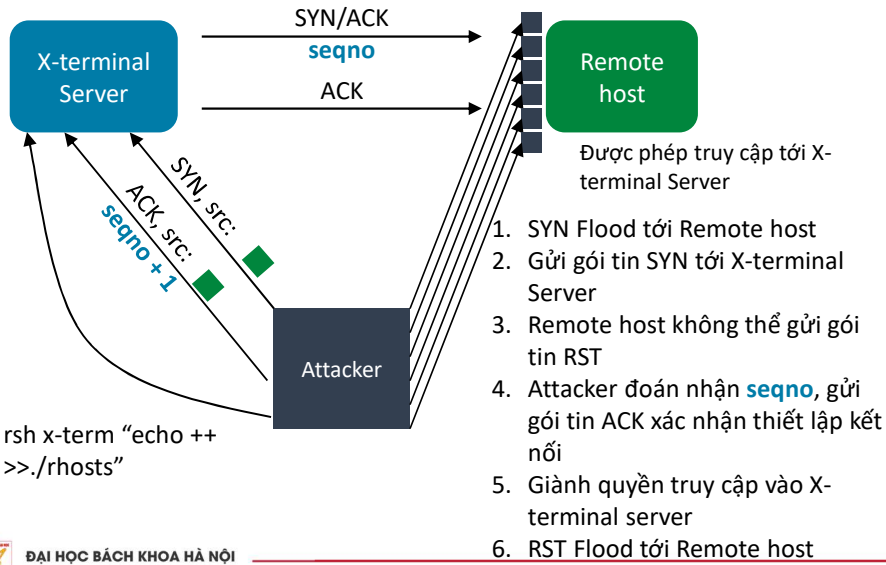
Kịch bản tấn công của Mitnick

- 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)



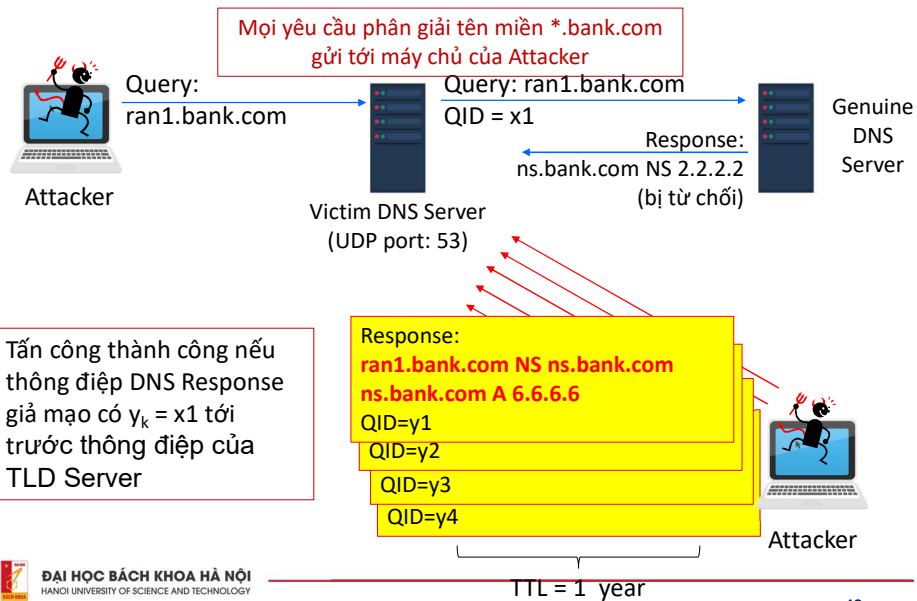
46

Kịch bản tấn công của Mitnick

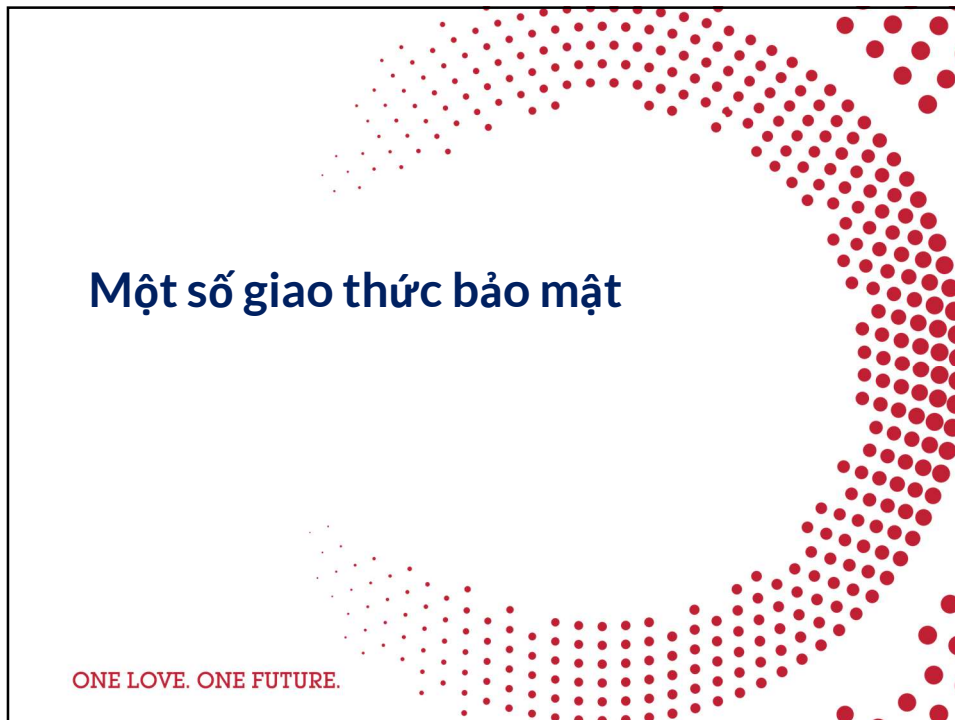


47

Tấn công DNS Cache Poisoning



48



49

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

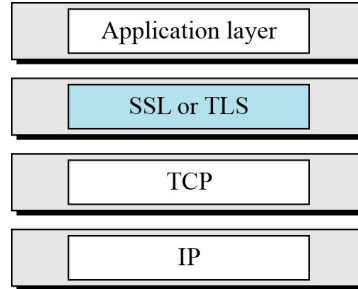


50

Giao thức SSL/TLS

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



Giao thức SSL/TLS

- 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

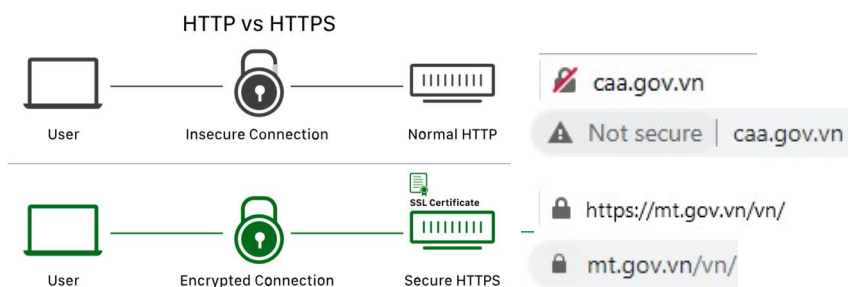
SSL và các giao thức tầng ứng dụng

- 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

53

Giao thức HTTPS

- HTTPS = HTTP + SSL/TLS



- Trình duyệt kiểm tra “danh tính” thực sự của Website thông qua chứng chỉ số mà website đó sử dụng

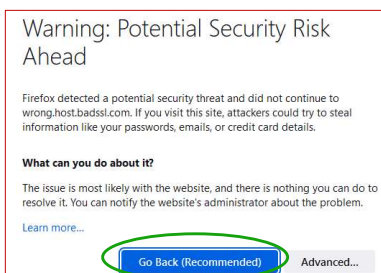
54

Hoạt động của HTTPS

- (1) Trình duyệt truy cập tới website
- (2) Máy chủ dịch vụ gửi chứng thư số khóa công khai của website cho trình duyệt
- (3) Trình duyệt kiểm tra chứng thư
 - Chứng thư phát hành cho tên miền của website
 - Chứng thư được phát hành bởi tổ chức tin cậy
 - Chứng thư còn hạn sử dụng
 - Chứng thư còn được phép sử dụng
 - Chứng thư không phải là giả mạo
- (4) Nếu chứng thư hợp lệ, trình duyệt và máy chủ trao đổi dữ liệu của website và người dùng:
 - Dữ liệu được mã hóa giữ bí mật
 - Dữ liệu được kiểm tra nguyên bản, không bị giả mạo, sửa đổi

HTTPS không phải là lá chắn vạn năng

- HTTPS chỉ bảo vệ dữ liệu khi truyền
- HTTPS giảm thiểu nguy cơ truy cập Website giả mạo nếu sử dụng đúng cách



Warning: Potential Security Risk Ahead

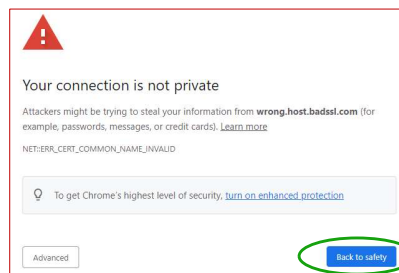
Firefox detected a potential security threat and did not continue to wrong.host.badssl.com. If you visit this site, attackers could try to steal information like your passwords, emails, or credit card details.


What can you do about it?

The issue is most likely with the website, and there is nothing you can do to resolve it. You can notify the website's administrator about the problem.

[Learn more...](#)


[Go Back \(Recommended\)](#) [Advanced...](#)



 Your connection is not private

Attackers might be trying to steal your information from wrong.host.badssl.com (for example, passwords, messages, or credit cards). [Learn more](#)

NET:ERR_CERT_COMMON_NAME_INVALID

 To get Chrome's highest level of security, [turn on enhanced protection](#)

[Advanced](#) [Back to safety](#)

- HTTPS không phải là sự đảm bảo cho thấy Website là an toàn

3. Tấn công do thám

ONE LOVE. ONE FUTURE.

57

Khái niệm

- Là các hành vi mà kẻ tấn công thực hiện nhằm thu thập thông tin về tổ chức và hệ thống
 - Thăm dò chủ động: có tương tác với mục tiêu
 - Thăm dò bị động: không có tương tác với mục tiêu
- Kẻ tấn công có cái nhìn chi tiết hơn và sâu hơn về hệ thống: các dịch vụ cung cấp, các cổng dịch vụ đang mở, địa chỉ IP, hệ điều hành và phần mềm...
- Trích xuất thông tin từ giai đoạn này cho phép kẻ tấn công lên kế hoạch chi tiết để thực hiện tấn công

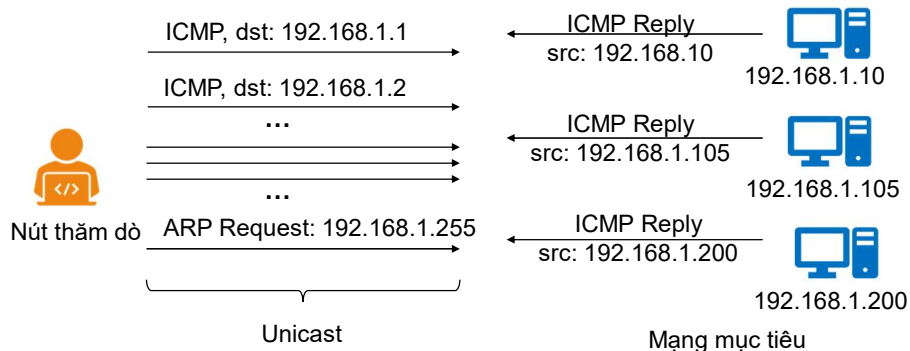
58

Cách thức do thám

- Sử dụng các công cụ tìm kiếm: Google, Shodan, Censys
- Thông tin từ mạng xã hội: FB, Twitter, LinkedIn
- Thông tin từ website của đối tượng: Burp Suite, ZAP, Web Spider, Web Mirroring
- Thăm dò hệ thống email
- Thăm dò tên miền: WHOIS, DNS
- Thăm dò kết nối mạng: trace route
- Sử dụng kỹ nghệ giao tiếp xã hội
- Xác định các nút mạng kết nối: Ping Sweep
- Kiểm tra các cổng dịch vụ đang mở: TCP Scanning, UDP Scanning
- Xác định thông tin hệ điều hành trên hệ thống mục tiêu: ID Serve, Netcraft

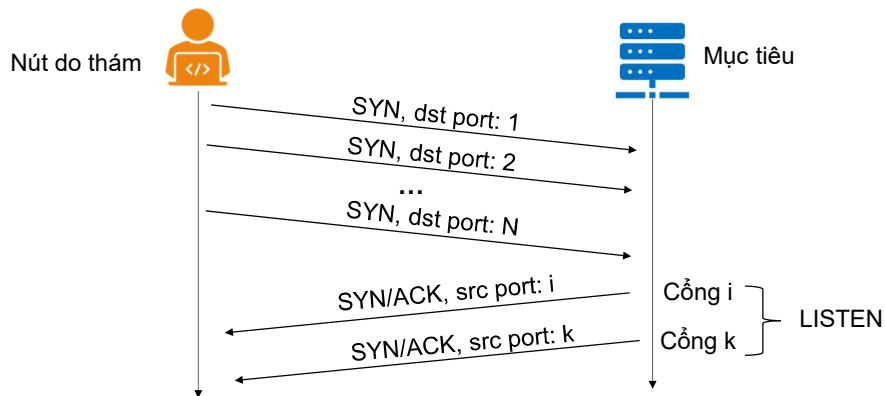
Quét mạng: ICMP Ping Scan

- Nút quét gửi một loạt gói tin ICMP Echo Request tới các địa chỉ IP trong mạng mục tiêu
- Nếu nút mạng đang hoạt động, gửi gói tin ICMP Echo Reply trả lời



Quét cổng dịch vụ

- Port scanning: thăm dò nút mạng đang cung cấp dịch vụ nào
- Cách thức thực hiện: TCP SYN Scan



4. Tấn công từ chối dịch vụ

DoS là gì?

- Denial of Service: Ngăn cản dịch vụ cung cấp tới người dùng trong mạng
- Denial of Service: Ngăn cản dịch vụ cung cấp tới Cách thức thực hiện:
 - Phá hủy hạ tầng phần cứng
 - Gửi lượng dữ liệu đủ lớn làm quá tải nút thắt cổ chai (bottleneck) của hệ thống
 - Lưu lượng tấn công lớn hơn băng thông của mục tiêu, hoặc
 - Số lượng gói tin lớn hơn khả năng xử lý của mục tiêu
 - Khai thác lỗ hổng phần mềm cung cấp dịch vụ
- Có thể xảy ra với mọi thành phần của hệ thống

Phân loại

- Tấn công vật lý: gây ra sự cố nguồn điện, kết nối mạng
- Tấn công băng thông: gửi liên tục một lượng lớn các gói tin làm tràn ngập băng thông của nạn nhân
 - Thường sử dụng các kỹ thuật khuếch đại
 - Ví dụ: Ping of Death, Smurf attack, DNS Amplification, UDP Flood
- Tấn công tài nguyên hệ thống: Gửi một lượng lớn yêu cầu làm cạn kiệt tài nguyên của nạn nhân
 - Thường khai thác điểm yếu của giao thức
 - Ví dụ: Tear drop, TCP SYN Flood, HTTP Flood, DHCP Starvation
- Tấn công dựa trên khai thác lỗ hổng phần mềm
 - Buffer Overflow
 - Integer Overflow
 - Format String

Một số cuộc tấn công DoS điển hình

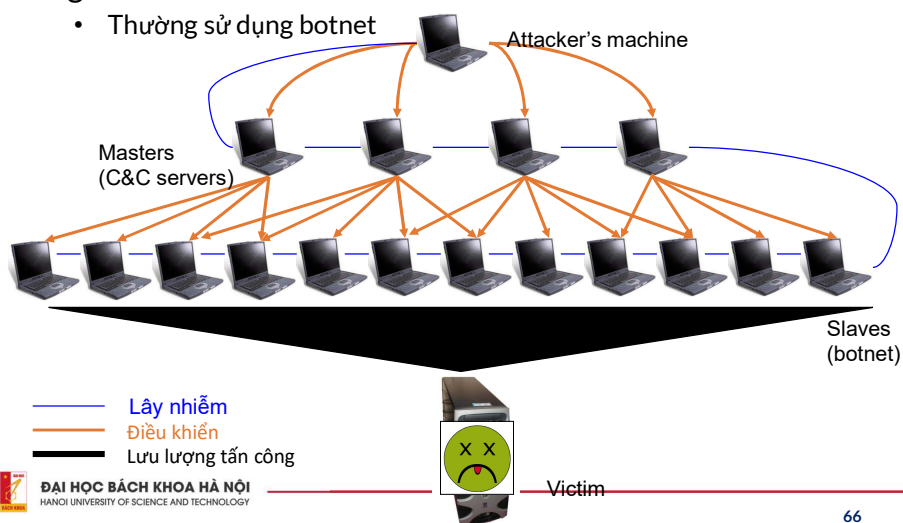
Thời gian	Mục tiêu	Lưu lượng	Kỹ thuật
03/2013	Spamhaus	~300 Gbps	DNS Amp. Attack
09/2016	Blog của Brian Krebs	~600 Gbps	SYN, GET, POST Flooding
09/2016	OVH Công ty hosting tại Pháp	~1 Tbps	Multiple type
03/2018	Đối tác của Arbor Network	~ 1.7 Tbps	Memcached amplification
02/2020	Amazon Web Service	~2.3 Tbps	Multiple type

65

DDoS

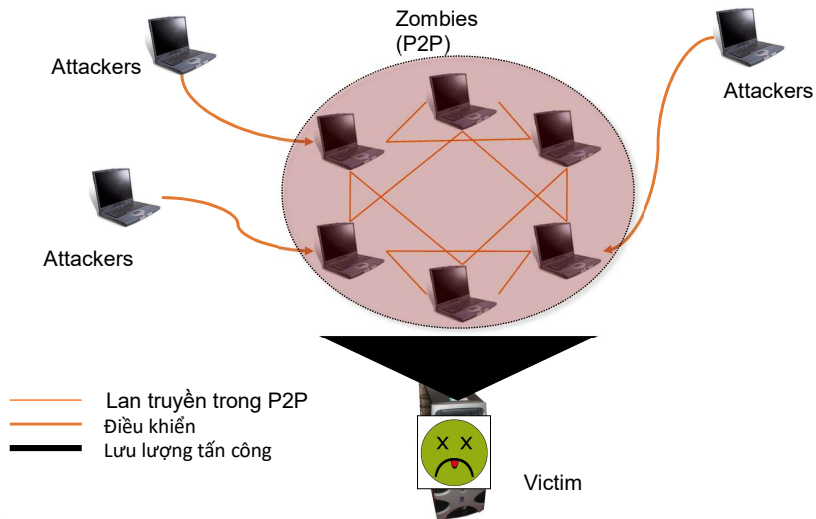
- DDoS-Distributed DoS: tấn công được thực hiện bởi nhiều nguồn khác nhau:

- Thường sử dụng botnet



66

DDoS sử dụng P2P botnet

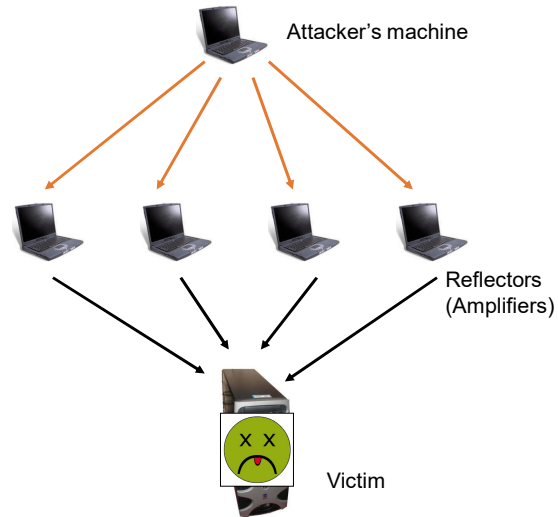


Distributed Reflection DoS (DRDoS)

- Reflector: nút mạng có khả năng gửi hồi đáp khi nhận được thông điệp yêu cầu
 - Trên lý thuyết, tất cả các giao thức có hồi đáp đều có thể lợi dụng
- DRDoS gửi yêu cầu tới reflector với địa chỉ nguồn là địa chỉ nạn nhân
 - Reflector gửi thông điệp hồi đáp cho nạn nhân
- DRDoS thường sử dụng các giao thức mà thông điệp hồi đáp có kích thước lớn hơn nhiều thông điệp yêu cầu
 - khuếch đại lưu lượng
- Tại sao DRDOS nguy hiểm?
 - Che giấu nguồn tấn công
 - Không cần đòi hỏi số lượng bot lớn

DRDoS

1. Kẻ tấn công gửi các gói tin giả mạo nạn nhân tới mạng khuếch đại
2. Mạng khuếch đại gửi dữ liệu trả lời cho nạn nhân
3. Nạn nhân bị đánh sập do phải xử lý lượng dữ liệu cực lớn

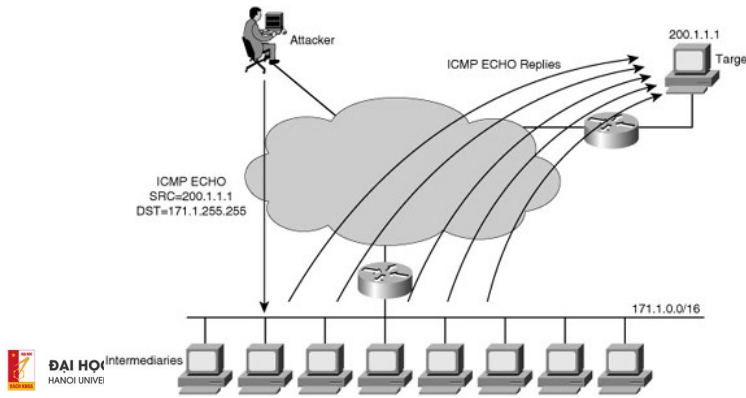


Tại sao DoS rất khó phòng chống?

- Kỹ thuật tấn công đơn giản
- Mạng Internet không được thiết kế để chống lại tấn công DoS
- Dễ dàng để xâm nhập và điều khiển máy tính của người dùng đầu cuối
 - 2010: BredoLab(30tr. bot), Mariposa(12tr.), Conficker(10tr.)
 - Xu hướng mới: sử dụng các thiết bị IoT (VD: Mirai-300K)
- Rất khó phân biệt lưu lượng tấn công và lưu lượng người dùng thông thường
- Thiếu sự phối hợp giữa các ISP
- Rất khó để triển khai các biện pháp phòng chống

Tấn công lợi dụng giao thức ICMP

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

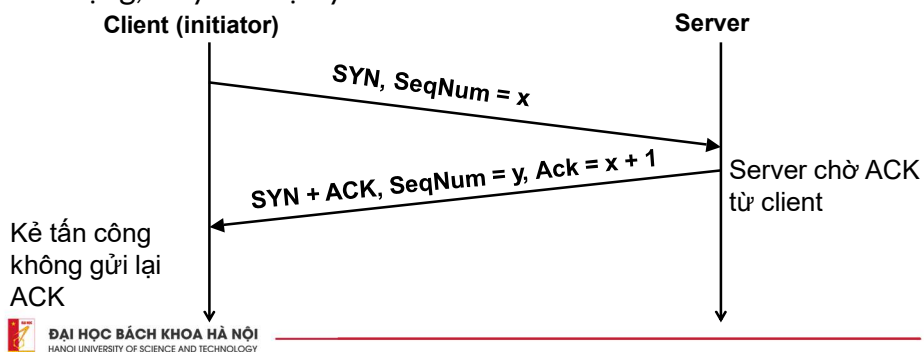


71

71

TCP SYN Flooding

- Kẻ tấn công gửi hàng loạt gói tin SYN để yêu cầu thiết lập kết nối nhưng không hoàn thành bước 3.
- Server gửi lại SYN/ACK, chuẩn bị tài nguyên để trao đổi dữ liệu, chờ ACK trong thời gian time-out
- Khi số lượng gói tin đủ lớn làm cạn kiệt tài nguyên của ứng dụng, máy chủ vật lý

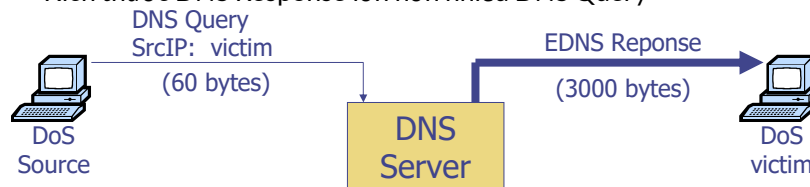


72

72

DNS Amplification

- Lợi dụng:
 - DNS sử dụng giao thức UDP không cần thiết lập kết nối
 - Kích thước DNS Response lớn hơn nhiều DNS Query



- 2006: 580 nghìn DNS resolver miễn phí trên Internet
- 2013: 21.7 triệu DNS resolver miễn phí
- Thực hiện tương tự với các dịch vụ: NTP(x557), SNMPv2(x6.3), NetBIOS(3.8), SSDP(x30.8)...

Tấn công HTTP Flood

- Gửi một lượng lớn các yêu cầu HTTP Request
- Basic HTTP Floods: gửi yêu cầu truy cập liên tục tới các trang giống nhau
- Randomized HTTP Floods: gửi yêu cầu truy cập tới các trang một cách ngẫu nhiên
 - Cache-bypass HTTP Floods: sử dụng các kỹ thuật vượt qua các cơ chế cache trên máy chủ
 - WordPress XMLRPC Floods: lợi dụng có chế pingback trên WordPress để thực hiện kỹ thuật tấn công phản hồi

Phòng chống tấn công DoS

- Chống tấn công DoS vào phần cứng
 - Hệ thống cất giữ: Phòng máy, tủ mạng, camera...
- Chống tấn công DoS khai thác lỗ hổng phần mềm:
 - Kiểm thử xâm nhập (Penetration Testing)
 - Cập nhật, vá lỗ hổng phần mềm
- Chống tấn công DoS vào tài nguyên tính toán:
 - Triển khai firewall, IDPS
 - Thiết lập thông số cấu hình hệ thống
 - Sử dụng các kỹ thuật thách đố (Ví dụ: CAPTCHA)

Phòng chống tấn công DoS

- Chống tấn công DoS vào băng thông:
 - Mở rộng băng thông
 - Cân bằng tải (Load Balancing)
 - Đối với ISP: Chống tấn công từ nguồn
 - Triển khai firewall, IDPS
- Phát hiện nguồn tấn công:
 - Truy vết nguồn tấn công
 - Phát hiện và ngăn chặn mã độc botnet: triển khai IDPS, firewall

5. Các hệ thống phòng chống tấn công mạng

ONE LOVE. ONE FUTURE.

77

Tường lửa

- Là hệ thống có khả năng ngăn chặn các truy cập không hợp lệ và **đã biết** từ bên ngoài và trong khu vực tài nguyên cần bảo vệ
- Tường lửa có thể triển khai ở nhiều vị trí, tùy thuộc cách thức định nghĩa, phạm vi tài nguyên cần bảo vệ:
 - Mạng ngoại vi
 - Mạng nội bộ } Network-based firewall
- Nút mạng(Host-based firewall)
- Ứng dụng(Application-based firewall)

78

Tường lửa có thể làm gì?

- Thi hành các chính sách an toàn bảo mật: hoạt động như một hệ thống cảnh vệ(traffic cop) cho phép/từ chối lưu lượng mạng nào đó **đi qua** tường lửa dựa trên các đặc điểm(giao thức, địa chỉ, nội dung...) **đã xác định**
- Hạn chế các hành vi tấn công vào mạng
 - Từ mạng bên ngoài(Internet) vào mạng nội bộ
 - Từ phân vùng mạng nội bộ này tới những phân vùng mạng nội bộ khác
- Lưu nhật ký các lưu lượng mạng

Tường lửa không thể làm gì?

- Không bảo vệ được tài nguyên trước các mối nguy cơ từ bên trong
- Không kiểm soát được các lưu lượng mạng không đi qua
- Không kiểm soát đầy đủ đối với các lưu lượng đã được mã hóa
- Không ngăn chặn được các truy cập tấn công chưa biết
- Không chống lại được hoàn toàn các nguy cơ từ phần mềm độc hại
- Do đó cần được:
 - Triển khai ở nhiều vị trí khác nhau
 - Kết hợp với các giải pháp khác: phòng chống phần mềm độc hại, IDS/IPS, điều khiển truy cập, kiểm toán(auditing)
 - Cập nhật liên tục các chính sách mới

Các kiến trúc tường lửa(1)

- Network-based firewall: Kiểm soát lưu lượng mạng giữa các phân vùng mạng
- Ưu điểm: Phạm vi kiểm soát rộng
- Nhược điểm:
 - Không kiểm soát được lưu lượng trong từng phân vùng
 - Không kiểm soát đầy đủ lưu lượng đã được mã hóa

Các kiến trúc tường lửa(2)

- Host-based firewall: Kiểm soát lưu lượng mạng đến và đi từ một nút mạng
- Ưu điểm: Kiểm soát được lưu lượng tới nút mạng từ những nguồn trong cùng phân vùng mạng
- Nhược điểm:
 - Chỉ bảo vệ được cho một mục tiêu đơn lẻ
 - Không kiểm soát đầy đủ lưu lượng đã được mã hóa

Các kiến trúc tường lửa(3)

- Application firewall: Kiểm soát lưu lượng mạng của một dịch vụ cụ thể
- Ưu điểm: Kiểm soát được toàn bộ lưu lượng mạng tới dịch vụ, kể cả lưu lượng đã mã hóa
- Nhược điểm:
 - Bộ luật phức tạp
 - Cần phải cài đặt nhiều phần mềm tường lửa nếu trên máy chủ cung cấp các dịch vụ khác nhau

83

Hệ thống IDPS

- Intrusion Detection and Prevention System: hệ thống có khả năng theo dõi, giám sát, phát hiện và ngăn chặn các hành vi tấn công, khai thác trái phép tài nguyên được bảo vệ
- IDPS vs tường lửa:
 - Tường lửa: xử lý từng gói tin trên lưu lượng mạng
 - IDPS: có khả năng theo dõi, giám sát chuỗi các gói tin, hành vi để xác định có phải là hành vi tấn công hay xâm nhập hay không
 - Các thiết bị tường lửa thế hệ mới thường trang bị tính năng IDPS

84

Các phương pháp phát hiện tấn công

- Phát hiện lạm dụng: sử dụng dữ liệu về các dạng tấn công đã biết
 - Phát hiện dựa trên dấu hiệu (signature-based)
 - Phát hiện dựa trên lỗ hổng (vulnerability signature)
- Phát hiện dựa trên bất thường: xây dựng mô hình các hành vi bình thường. Đánh dấu nghi ngờ và đo lường các hành vi nằm ngoài mô hình.
 - Phát hiện dựa trên ngưỡng
 - Phát hiện dựa trên thống kê
 - Phát hiện dựa trên học máy