# Chương 1: Nội dung





# An ninh mạng

- Internet được thiết kế ban đầu không quan tâm nhiều đến vấn đề an ninh mạng
  - *Cách nhìn ban đầu:* "một nhóm người dùng tin tưởng lẫn nhau cùng sử dụng một hệ thống mạng trong suốt" ☺
  - Các nhà thiết kế giao thức Internet chọn phương pháp "catch-up"
  - Xem xét an ninh trong tất cả các tầng!
- Các vấn đề cần quan tâm:
  - Kẻ xấu có thể tấn công mạng máy tính như thế nào?
  - Chúng ta có thể bảo vệ mạng chống lại các tấn công như thế nào?
  - Có thể thiết kế kiến trúc mạng như thế nào để không bị tấn công?



# Kẻ xấu: đặt phần mềm độc hại vào các host qua Internet

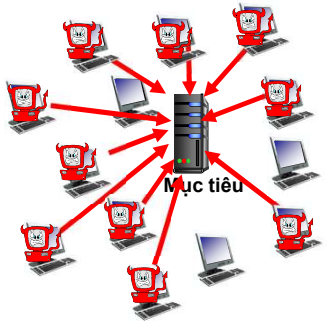
- Phần mềm độc hại (malware) có thể đi vào máy chủ từ:
  - *Vi rút:* lây nhiễm theo cách tự sao qua đối tượng nhận/thực thi (ví dụ: tệp đính kèm trong thư điện tử)
  - *Sâu mạng (worm):* lây nhiễm theo cách tự sao qua đối tượng nhận thụ động mà có thể được tự thực thi
- Phần mềm độc hại gián điệp (spyware malware) có thể ghi lại thao tác bàn phím, các trang web truy cập, và tải thông tin lên cho trang thu thập.
- Các host bị lây nhiễm có thể được ghi vào trong botnet, và được dùng để spam trong các cuộc tấn công DDoS.



# Kẻ xấu: tấn công server, cơ sở hạ tầng mạng

*Tấn công từ chối dịch vụ (Denial of Service - DoS):* kẻ tấn công làm cho các nguồn tài nguyên (máy chủ, băng thông) không còn có sẵn để phục vụ cho các lưu lượng hợp pháp bằng cách sử dụng áp đảo tài nguyên với những lưu lượng không có thật.

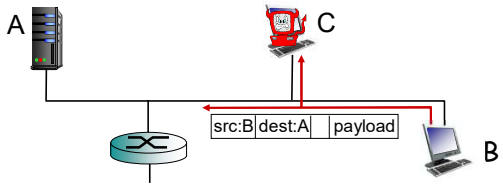
1. Lựa chọn mục tiêu
2. Đột nhập vào host trên toàn mạng (xem botnet)
3. Gửi các gói tin tới mục tiêu từ các host đã bị xâm nhập



## Kẻ xấu có thể bắt các gói tin

*Bắt gói tin (packet "sniffing"):*

- Đường truyền chung (quảng bá) (ethernet, chia sẻ không dây)
- Đọc/ghi lại tất cả các gói tin qua giao diện mạng ngẫu nhiên nào đó (ví dụ: bao gồm mật khẩu)

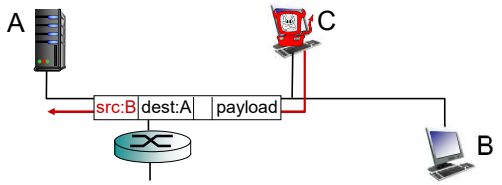



- Phần mềm wireshark (dùng trong thực hành môn học) có thể bắt gói tin (đây là phần mềm miễn phí).



## Kẻ xấu có thể giả mạo địa chỉ

*Giả mạo địa chỉ IP (IP spoofing):* gửi gói tin với địa chỉ nguồn sai




*… có rất nhiều vấn đề về an ninh mạng (xem thêm trong tài liệu)*



## Phòng chống tấn công

- Xác thực: chứng minh đúng người
  - Mạng di động cung cấp định danh phần cứng qua thẻ SIM; không có phần cứng hỗ trợ như vậy trong mạng Internet truyền thống
- Bảo mật: thông qua mã hóa
- Kiểm tra tính toàn vẹn: chữ ký số ngăn chặn/phát hiện giả mạo
- Hạn chế truy nhập: các VPN được bảo vệ bằng mật khẩu
- Tường lửa: "hộp trung gian" chuyên dụng trong mạng truy nhập và mạng lõi:
  - Chặn theo mặc định: lọc các gói đến để hạn chế người gửi, người nhận, ứng dụng
  - Phát hiện/phản ứng với các cuộc tấn công DOS



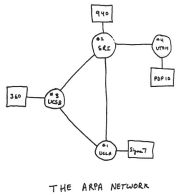
## Chương 1: Nội dung

## Lịch sử phát triển Internet

*1961-1972: Thời kỳ đầu của nguyên lý chuyển mạch gói*

- 1961: Kleinrock – lý thuyết hàng đợi cho thấy tính hiệu quả của chuyển mạch gói
- 1964: Baran – chuyển mạch gói trong các mạng quân đội
- 1967: ARPAnet được hình thành từ Mạng lưới cơ quan với các dự án nghiên cứu tiên tiến (Advanced Research Projects Agency) của Mỹ.
- 1969: Nút ARPAnet đầu tiên hoạt động

- 1972:
  - ARPAnet được công bố
  - NCP (Network Control Protocol) là giao thức quản lý mạng đầu tiên
  - Chương trình đầu tiên là thư điện tử
  - ARPAnet có 15 nút mạng






## Lịch sử phát triển Internet

*1972-1980: Liên mạng, các mạng riêng và mới*

- 1970: mạng vệ tinh ALOHAnet ở Hawaii
- 1974: Cerf and Kahn – kiến trúc cho hệ thống mạng toàn cầu
- 1976: Ethernet tại Xerox PARC
- Những năm 70: các mạng kiến trúc riêng: DECnet, SNA, XNA
- Cuối những năm 70: chuyển mạch cho các gói tin có độ dài cố định (tiền thân của ATM)
- 1979: ARPAnet có 200 nút mạng

Nguyên lý mạng toàn cầu của Cerf and Kahn's :

- Tính tối giản, tự chủ - không cần thay đổi nội bộ bên trong khi được yêu cầu kết nối các mạng
- Mô hình dịch vụ tốt nhất
- Các bộ định tuyến không trạng thái
- Điều khiển không tập trung

Xác định kiến trúc mạng Internet ngày nay!

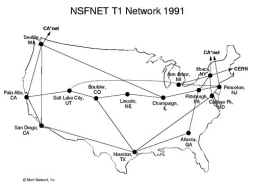


## Lịch sử phát triển Internet

*1980-1990: các giao thức mới, sự phát triển của mạng lưới*

- 1983: triển khai TCP/IP
- 1982: định nghĩa giao thức SMTP cho e-mail
- 1983: DNS được định nghĩa cho chuyển đổi tên miền – IP
- 1985: định nghĩa giao thức FTP
- 1988: Giao thức điều khiển tắc nghẽn TCP

- Các mạng quốc gia mới: Csnet, BITnet, NSFnet, Minitel
- 100.000 host được kết nối vào liên minh các mạng






## Lịch sử phát triển Internet

*Những năm 1990, 2000: thương mại hóa, Web, các ứng dụng mới*

- Đầu những năm 1990: ARPAnet ngừng hoạt động
- 1991: NSF dỡ bỏ các hạn chế đối với việc sử dụng NSFnet vì mục đích thương mại (ngừng hoạt động, 1995)
- Những năm đầu 1990: Web
  - Siêu văn bản [Bush 1945, Nelson 1960's]
  - HTML, HTTP: Berners-Lee
  - 1994: Mosaic, sau này là Netscape
  - Cuối những năm 1990: thương mại hóa trên Web

Cuối những năm 1990–2000:

- Nhiều ứng dụng mới: tin nhắn nhanh, chia sẻ file P2P
- An ninh mạng được đặt lên hàng đầu
- Ước tính có khoảng 50 triệu host, hơn 100 triệu người dùng
- Liên kết xương sống chạy với tốc độ Gbps

## Lịch sử phát triển Internet

*2005-nay: quy mô, SDN, di động, đám mây*

- Triển khai tích cực truy nhập băng thông rộng tại nhà (10-100 Mbps)
- 2008: Mạng được điều khiển bằng phần mềm (SDN)
- Tăng tính phổ biến của truy nhập không dây tốc độ cao: 4G/5G, WiFi
- Các nhà cung cấp dịch vụ (Google, FB, Microsoft) tạo ra các mạng riêng.
  - Bỏ qua Internet thương mại để kết nối "gần" với người dùng cuối, cung cấp quyền truy cập "tức thời" vào mạng xã hội, tìm kiếm, nội dung video,…
- Các doanh nghiệp chạy dịch vụ trên "đám mây" (ví dụ: Amazon Web Services, Microsoft Azure)
- Tăng điện thoại thông minh: thiết bị di động nhiều hơn thiết bị cố định trên Internet (2017)
- ~15B thiết bị được kết nối Internet (2023, statista.com)



## Lịch sử phát triển Internet Việt Nam

- 1991: Nỗ lực kết nối Internet không thành.
- 1996: Giải quyết các cản trở, chuẩn bị hạ tầng Internet
  - ISP: VNPT
  - Tốc độ 64kbps. Một đường kết nối quốc tế. Có một số người dùng.
- 1997: Việt Nam chính thức kết nối Internet.
  - 1 IXP: VNPT
  - 4 ISP: VNPT, Netnam (IOT), FPT, SPT
- 2007: "Mười năm Internet Việt Nam"
  - 20 ISP, 4 IXP
  - 19 triệu người dùng, chiếm 22,04% dân số
- 2022: "25 năm Internet Việt Nam": 70% dân số sử dụng Internet.



## Tổng kết

*Cần nắm vững các nội dung:*

- Khái quát về Internet
- Giao thức là gì?
- Phần cạnh, phần lõi của mạng, mạng truy nhập
  - So sánh chuyển mạch gói và chuyển mạch kênh
  - Cấu trúc mạng Internet
- Hiệu năng: mất mát, trễ, thông lượng
- Phân tầng, các mô hình dịch vụ
- An ninh mạng
- Lịch sử phát triển mạng

*Kiến thức thu được:*

- Bối cảnh, khái quát, "cảm nhận" về mạng
- Để hiểu sâu hơn, chi tiết trong *các phần sau*!



## Tham khảo


- Jim Kurose, Keith Ross, "*Computer Networking: A Top-Down Approach*" 8th edition, Pearson, 2020.