An toàn Hệ thống Thông tin

Trần Đức Khánh
Viện CNTT&TT - ĐH BKHN

Thông tin chung

- Tên môn học:
  An toàn Hệ thống Thông tin
- Khối lượng: 2 TC
- Đánh giá
  - 70% điểm thi cuối kỳ
  - 30% điểm quá trình
- Giảng viên
  - Trần Đức Khánh
  - Viện CNTT&TT, P. 503, P.603 Nhà B1
  - khanhtd@soict.hut.edu.vn

Tài liệu tham khảo

- *Introduction to Computer Security.*
  Matt Bishop
- *Security in Computing, Fourth Edition.*
  Charles P. Pfleeger, Shari Lawrence Pfleeger
- *Handbook of Applied Cryptography.*
  A. Menezes, P. van Oorschot and S. Vanstone
- *Chuyên đề An toàn & Bảo mật*.
  Nguyễn Khanh Văn
- *Các Bài giảng về An toàn Máy tính.*
  ĐH Berkerley, MIT, ĐH Edinburgh

Mục tiêu sư phạm

- Sinh viên không ngủ gật
- Sinh viên nắm được kiến thức
- Sinh viên thích môn học

Mục tiêu môn học

- Nắm vững các khái niệm cơ bản trong an toàn HTTT: mối đe dọa, biện pháp ngăn chặn
- Nắm được cơ sở của lý thuyết mật mã
  - Các hệ mật mã
  - Ứng dụng: chữ ký số, xác thực, giao thức truyền thông bảo mật, thương mại điện tử,…
- Đánh giá độ tin cậy của các HTTT
- Hướng đến xây dựng chính sách và đề ra giải pháp an toàn bảo mật cho các HTTT

Nội dung

- Khái niệm cơ bản về an toàn thông tin
- Mật mã học
  - Mật mã cổ điển và các hệ mật mã hóa công khai
  - Chữ ký điện tử, kỹ thuật hàm băm
  - Giao thức mật mã và an toàn thông tin
- An toàn các HTTT
  - An toàn phần mềm
  - An toàn hệ điều hành
  - An toàn cơ sở dữ liệu
  - An toàn mạng, Web

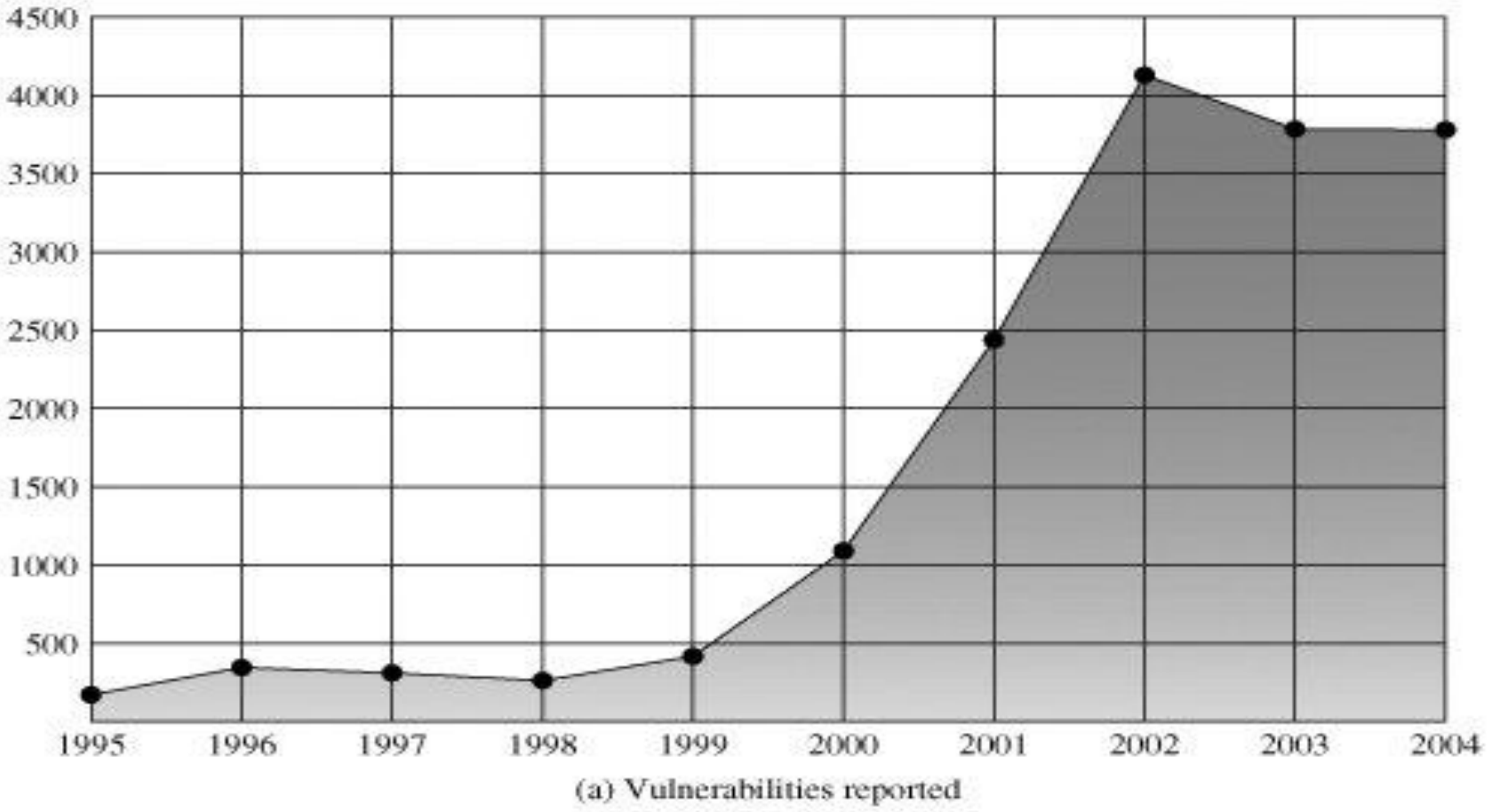
Sự cần thiết của An toàn HTTT

Thiệt hại an toàn HTTT

- Thiệt hại thời gian: theo viện SANS, máy tính không được bảo vệ chỉ "sống sót" < 20' trên internet
- Thiệt hại kinh tế: ~ tỷ USD hàng năm

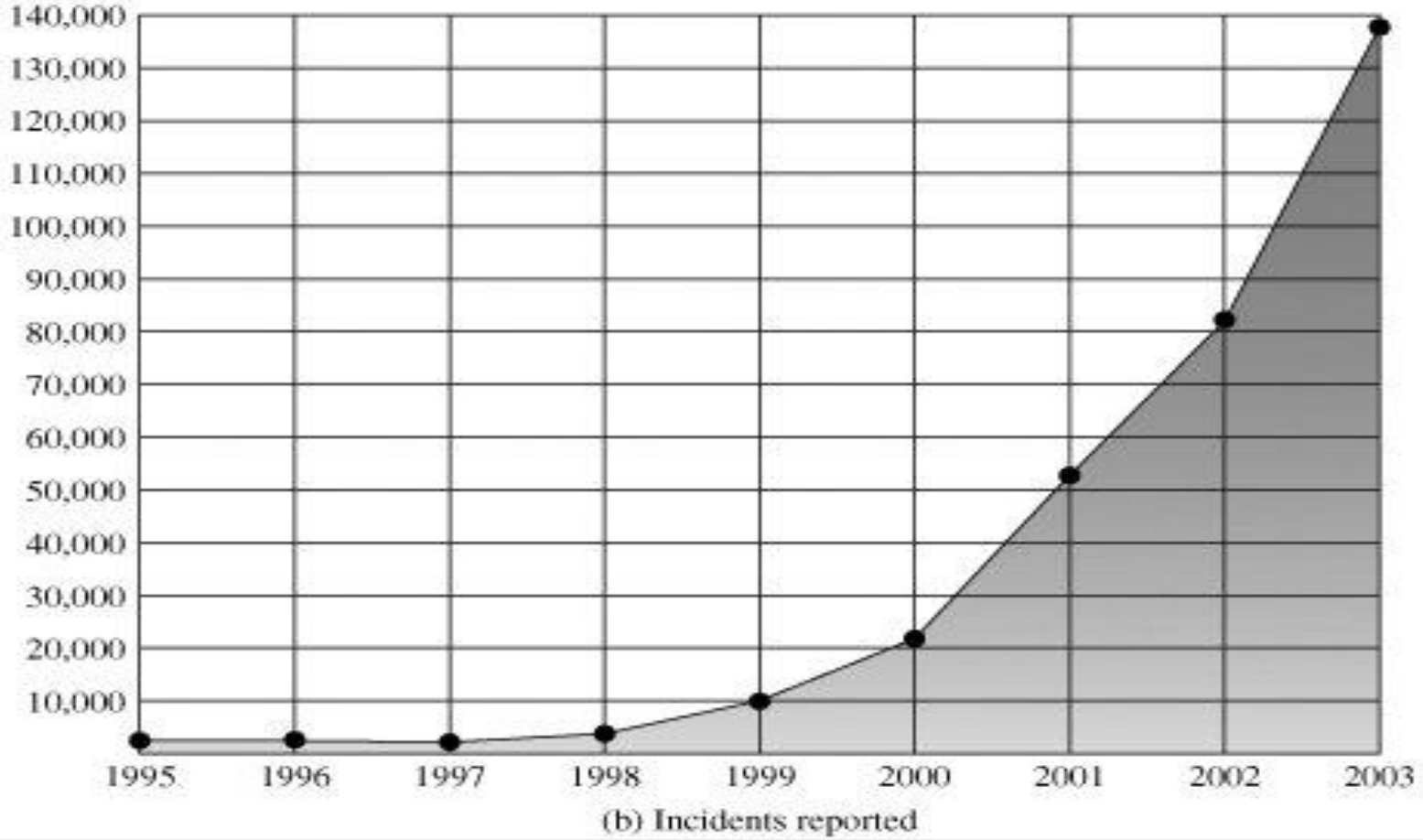
1. Vi rút
2. Từ chối dịch vụ
3. ……
4. ……

[CERT]: Mối nguy



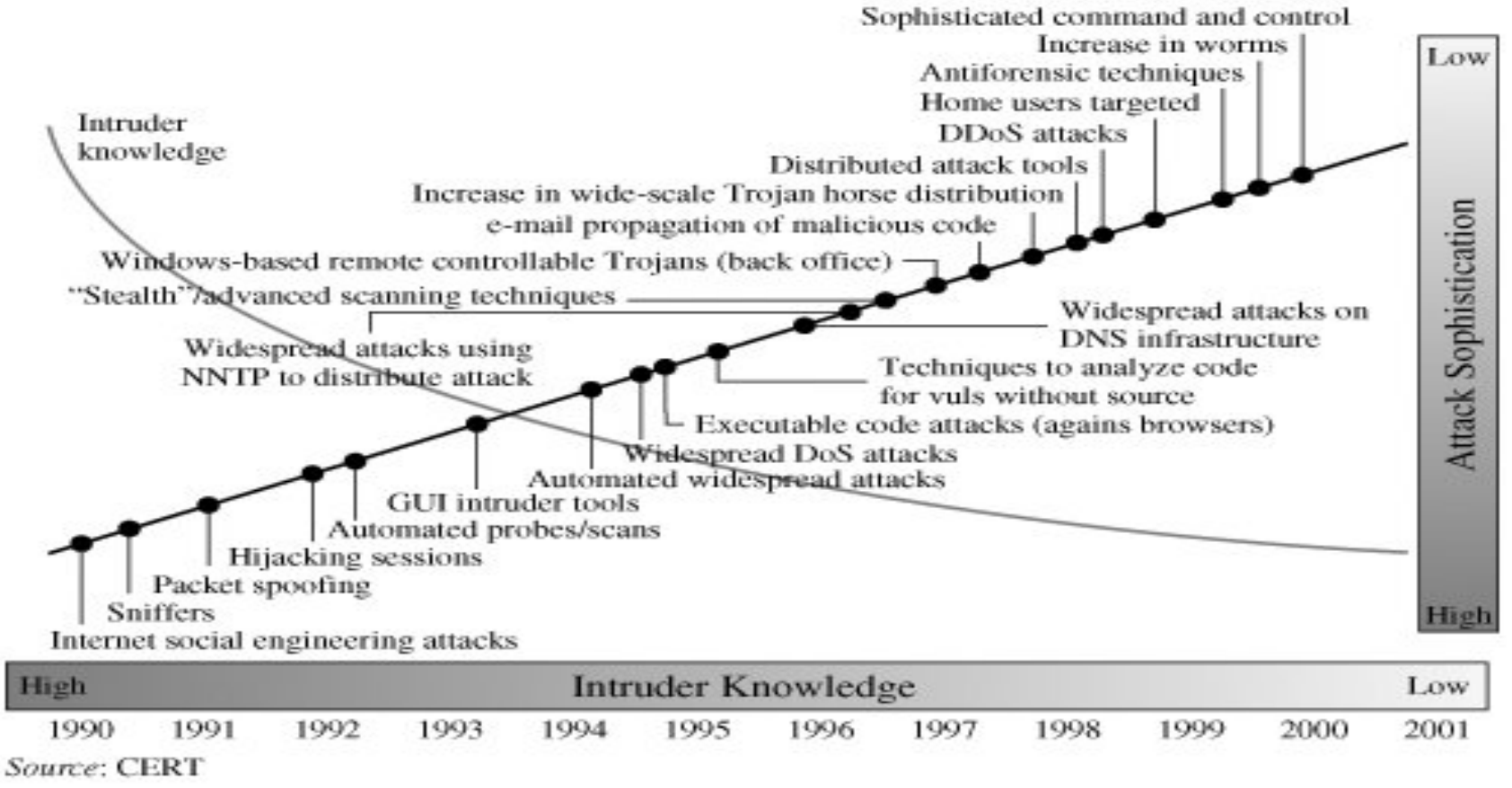
(a) Vulnerabilities reported

[CERT]: Sự cố



(b) Incidents reported

[CERT]: Quy mô, Tính phức tạp



Source: CERT

An toàn

Mục tiêu của an toàn là bảo vệ “tài sản” tránh khỏi các “mối đe dọa”, sử dụng các “biện pháp ngăn chặn”

- Tài sản nào?
- Mối đe dọa nào?
- Biện pháp ngăn chặn nào?

An toàn HTTT

- Tài sản: phần cứng, phần mềm, dữ liệu
- Mối đe dọa: phá hoại, can thiệp, sửa đổi
- Biện pháp ngăn chặn: mã hóa, kiểm soát thông qua phần mềm/phần cứng/các chính sách

An toàn HTTT

3 Mục tiêu:

- *Bí mật (Confidentiability):* tài sản chỉ được truy nhập bởi những người có quyền
- *Toàn vẹn (Intergrity):* tài sản chỉ được tạo/xóa/sửa đổi bởi những người có quyền
- *Sẵn dùng (Availability):* tài sản sẵn sàng để đáp ứng sử dụng cho những người có quyền

Hỏi/Đáp

Những biện pháp ngăn chặn nào đang được sử dụng trên máy tính cá nhân của bạn?

Các biện pháp này nhằm ngăn chặn những đe dọa nào?

An toàn HTTT - Mối đe dọa

- Phần mềm độc hại (Malware)
- Phishing
- Spam
- Từ chối dịch vụ (Denial of service)
- Truy nhập trái phép (Unauthorized access)
- Giao dịch gian lận (Fraudulent transaction)
- …

An toàn HTTT - Biện pháp

- Giao thức mã hóa
- Kiểm tra người sử dụng + mật khẩu
- Quét/diệt phần mềm ác tính
- Giới hạn truy nhập
- Phân quyền trong hệ điều hành
- Tường lửa
- Hệ thống phát hiện đột nhập
- Thẻ thông minh mã hóa
- Khóa
- …

Các chủ đề

- Mật mã học
- An toàn phần mềm
- An toàn hệ điều hành
- An toàn cơ sở dữ liệu
- An toàn mạng, Web

Các chủ đề (1)

- Mật mã học
  - Hệ Mật mã cổ điển
  - Hệ Mật mã khóa bí mật
  - Hệ Mật mã khóa công khai
  - Hàm băm, chữ ký số
  - Quản lý khóa, giao thức mật mã,…

Trộm ôtô bằng máy tính xách tay

- 2007, chiếc BMW X5 của David Beckham bị đánh cắp ở Madrid
- Kẻ cắp sử dụng máy tính xách tay, ăng ten và phần mềm để bẻ khóa
  - Ăng ten để thu sóng phát ra từ chíp RFID được cài trong khóa
  - Phần mềm được dùng để thử tất cả các khả năng mã hóa (hàng nghìn tỷ)

  Nguồn:

  http://www.msnbc.msn.com/id/13507939

- 2004, các nhà nghiên cứu của ĐH Johns Hopkins đã bẻ được khóa của một số xe đời mới
  - Texas Instruments, nhà sản xuất chip RFID, bỏ qua lời cảnh báo của nhóm nghiên cứu

Giải mã Enigma

- Máy mã hóa và giải mã phát minh bởi Arthur Scherbius cuối thế chiến thứ nhất
- Enigma được sử dụng trong quân đội Đức Quốc xã trong thế chiến thứ hai
- Công trình giải mã Enigma của quân Đồng minh được các sử gia đánh giá là rút gọn 2 năm thời gian thế chiến
- Một trong những lực lượng giải mã nổi tiếng là nhóm HUT 8 của Anh, do Alain Turing dẫn đầu

Các chủ đề (2) & (3)

- An toàn phần mềm
  - Các mối đe dọa
  - Các biện pháp an toàn
    - Soát lỗi
    - Kiểm định
    - Lập trình an toàn
- An toàn hệ điều hành
  - Các mối đe dọa
  - Các biện pháp an toàn
    - Phân quyền, Điều khiển truy nhập, Sandbox
    - Trusted computing

Tấn công iPhone

- 2007, các nhà nghiên cứu của Independent Security Evaluators phát hiện một lỗ hổng tạo điều kiện cho kẻ đột nhập kiểm soát iPhone
- Trình duyệt Safari của iPhone chạy với đặc quyền admin -> phần mềm độc hại chạy với đặc quyền admin
- Đột nhập thông qua
  - Điểm truy nhập không dây (wireless access point)
  - Các trang Web
  - Email, SMS có chứa các đường dẫn đến các trang web bị chiếm đoạt

Nguồn:

http://securityevaluators.com/content/case-studies/iphone//

Các chủ đề (5)

- An toàn mạng, Web
  - Các mối đe dọa
  - Tấn công từ chối dịch vụ
  - Spam
  - Phần mềm độc hại
  - Các công cụ bảo vệ

500 000 trang Web bị tấn công

- 2008, hơn nửa triệu trang Web, trong đó có cả các trang của Liên Hợp Quốc bị tấn công
- Tấn công dạng “SQL injection”
- Khai thác lỗ hổng trong SQL Server của Microsoft

Nguồn: http://www.computerworld.com/s/article/9080580/Huge_Web_hack_attack_infects_500_000_pages

Đột nhập hộp thư Gmail

- 2008, tại hội nghị Defcon hacker một nhà nghiên cứu demo một công cụ cho phép đột nhập vào hộp thư Gmail, ngay cả khi các phiên truy nhập hộp thư được mã hóa (https:// thay vì http://)
- Đột nhập thông qua việc đánh cắp Session Cookie
  - Session Cookie chứng nhận máy tính đã đăng nhập thành công
  - Session Cookie bị đánh cắp sẽ được sử dụng như một chứng nhận hợp lệ để truy nhập hộp thư Gmal

Nguồn: Washington Post

Các chủ đề (4)

- An toàn cơ sở dữ liệu
  - Các mối đe dọa
  - Các biện pháp an toàn

Tin tặc đoạt quyền kiểm soát Máy chủ của IMF

- 2011, chiến dịch tấn công vào Máy chủ IMF
- Tin tặc đánh cắp email, tài liệu
- Tin tặc đánh cắp một số thông tin tối mật về tình trạng tài chính của nhiều nước trên thế giới
- World Bank phải quyết định ngắt kết nối với IMF

Nguồn: http://www.profiforex.us/news/entry4000001548.html