BÀI #18 - PHÁT HIỆN TẤN CÔNG THỐNG KÊ

- **Thách thức trong phát hiện tấn công/xâm nhập**
- **Đánh đổi giữa khả năng phát hiện, bảo mật, quyền riêng tư, hiệu suất, v.v.**

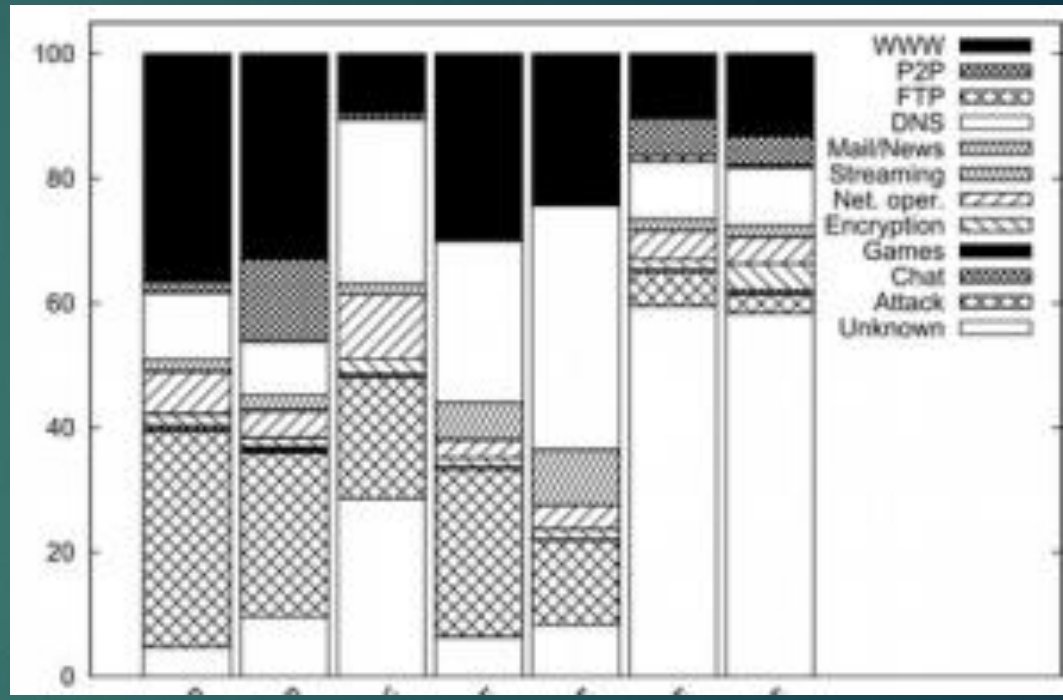
BÀI #18 - PHÁT HIỆN TẤN CÔNG THỐNG KÊ

TS. HOÀNG SỸ TƯƠNG

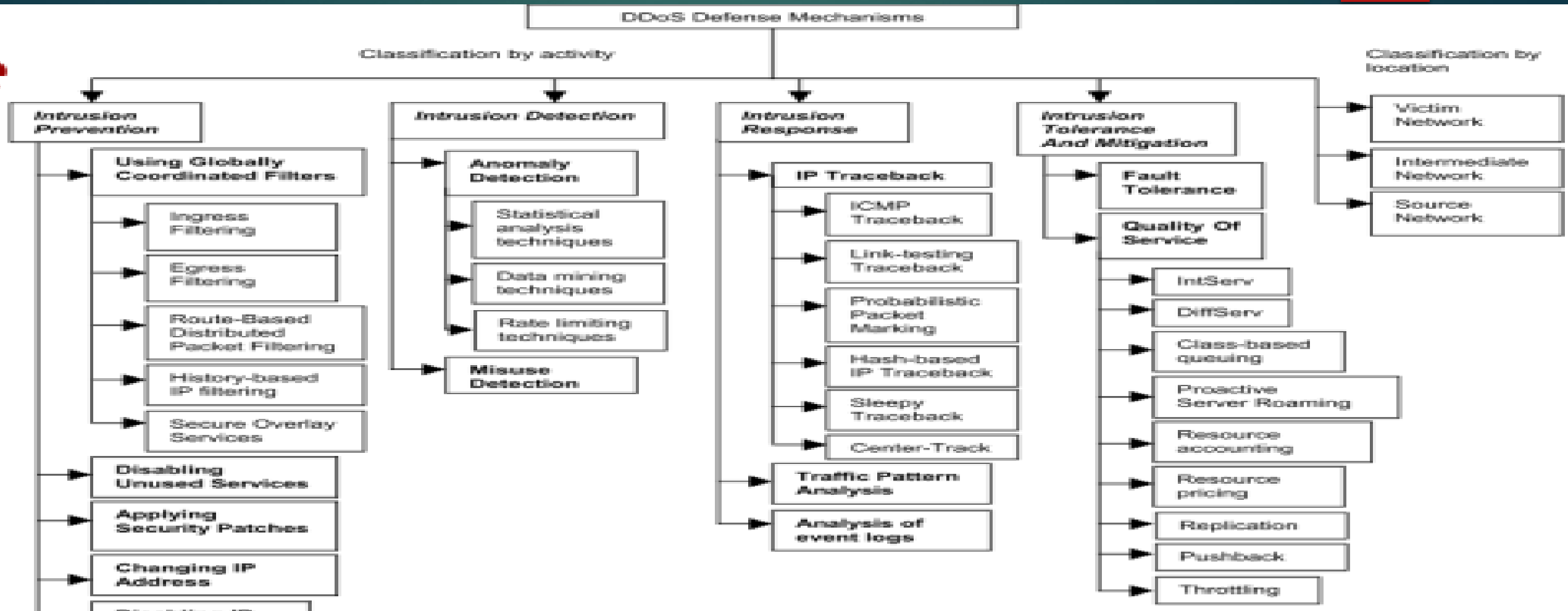
PHÁT HIỆN TẤN CÔNG/XÂM NHẬP

- Hầu hết công việc về phát hiện tấn công/xâm nhập mạng đều tập trung vào Internet

Bảng 2: Danh mục ứng dụng	
Danh mục	Ứng dụng/giao thức
web	http, https
p2p	FastTrack, eDonkey. BitTorrent, Ares Gnutella, WinMX, OpcnNap, MP2P SoulSeek. Direct connect, GoBoogy Soribada, PeerEnabler
ftp	ftp
Dns	Dns
Mail/news	smtp, pop, imap. identd, nntp
Streaming	mms(wmp), thực, quicklime, Shoutcast vbrick, netbios Video IM Logitech
vận hành mạng	Netbios, smb, snmp, ntp. …
Mã hóa	Ssh, ssl
Game	Quake, Halflife, Age of Empires
Chat	AIM, IRC, Yahoo Massenger…
Tấn công	Port scans, address scan



PHÒNG THỦ



From [Douligeris & Mitrokotsa, Computer Networks 2004]

THÁCH THỨC

- Nhiều mô hình và hệ thống phòng thủ kiểu Internet không chuyển thành mạng không dây, ngay cả những mạng là một phần của Internet
  - Các cuộc tấn công vào WiFi AP không giống như các cuộc tấn công vào bộ định tuyến Internet hoặc gateway có dây
  - Các cuộc tấn công được phát động từ các thiết bị di động qua LTE có thể giống nhau khi lưu lượng truy cập trên Internet, nhưng lại khác trong chính mạng LTE

THÁCH THỨC

- Tính cơ động phá vỡ nhiều giả định của các hệ thống phát hiện/phòng thủ truyền thống
  - Các đường dẫn thay đổi nhanh hơn nhiều, ngăn chặn việc in dấu chân của lớp mạng trong các phiên và làm phức tạp quá trình phân tích lưu lượng
  - Tuy nhiên, tính di động có thể cung cấp thông tin bổ sung, nếu máy dò đủ thông minh để tìm kiếm thông tin đó
    - *Ví dụ: nếu bộ phát hiện nằm trong lõi LTE, thì nó không biết nhiều về tính di động của thiết bị, trong khi nếu bộ phát hiện nhỏ nằm trong các trạm cơ sở thì có thể có thông tin về tính di động*

THÁCH THỨC

- Máy dò ở đâu?
  - Trong nhiều mô hình phát hiện/phòng thủ dựa trên mạng Internet truyền thống, các mạng được phân vùng độc đáo bằng cách sử dụng gateways, tường lửa, v.v. với bộ phát hiện (detector) dựa trên miền phía sau mỗi mô hình
  - Còn về mạng MANET/WSN thì sao?
    - Máy dò nên đi đâu? Nó cần bao nhiêu khả năng hiển thị?
    - Nó nên giám sát cái gì?

THÁCH THỨC

- Các biện pháp bảo mật ở các lớp khác nhau có thể ngăn chặn hoặc can thiệp vào việc phát hiện tấn công
  - Các mục tiêu bảo mật dữ liệu, quyền riêng tư của mạng, ẩn danh, v.v. xung đột trực tiếp với một số kỹ thuật phát hiện tấn công
  - Ví dụ: nhiều tập đoàn đang gặp khó khăn với việc áp dụng rộng rãi TLS/SSL/HTTPS vì nó phá vỡ các mô hình dựa trên kiểm tra gói của họ để phát hiện tấn công
  - Ví dụ: nếu các kỹ thuật phân tích chống lưu lượng truy cập làm cho tất cả lưu lượng truy cập giống nhau, làm thế nào để phân biệt lưu lượng truy cập bình thường và tấn công?

PHƯƠNG PHÁP PHỔ BIẾN

- Phát hiện tấn công phải phù hợp với ngữ cảnh
  - Ví dụ: trong một mạng cảm biến, lưu lượng truy cập mạng dự kiến sẽ ít khác biệt hơn nhiều, vì vậy việc phát hiện sự bất thường có thể dễ dàng hơn, có thể làm cho sự cân bằng trở nên hợp lý hơn
- Phát hiện tấn công có thể yêu cầu có sự cộng tác
  - Sự phụ thuộc giữa các tầng có nghĩa là phát hiện không phải là hoạt động theo tầng và có thể cần giám sát trên nhiều tầng khác nhau của ngăn xếp giao thức và các vị trí khác nhau trong mạng

CÂU HỎI MỞ

- Do có nhiều loại mạng và nhu cầu về các cơ chế phát hiện phù hợp với ngữ cảnh nên đây là một vấn đề khó.

1. Cơ chế phát hiện cụ thể nào là cần thiết cho các tình huống mạng/ứng dụng cụ thể?
2. Các cơ chế phát hiện có thể được khái quát hóa đến mức nào?
3. Lược đồ phát hiện có thể được học/đào tạo tại chỗ không?

BÀI 18:
BẢO MẬT & QUYỀN RIÊNG TƯ MẠNG VANET