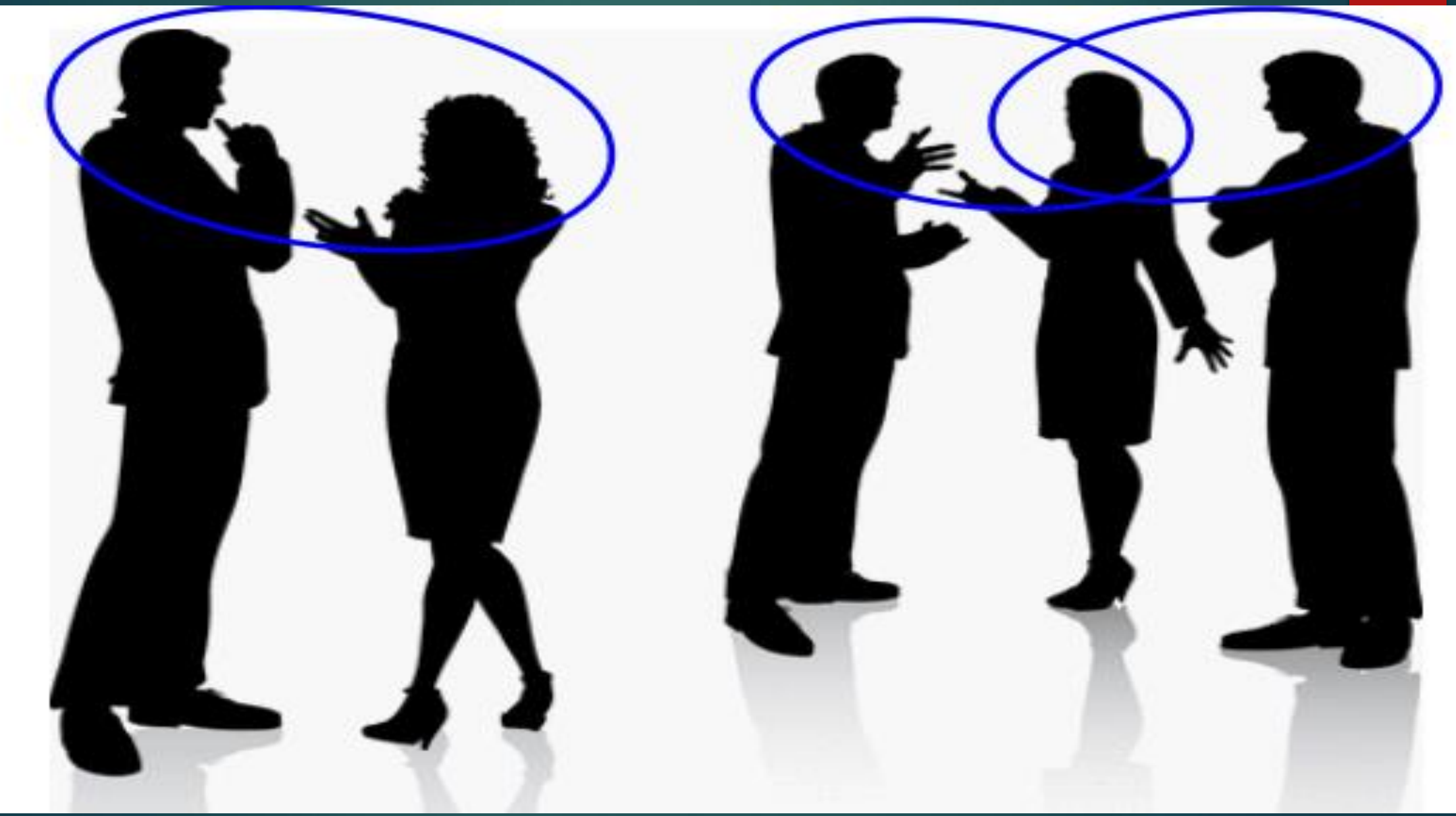
BÀI #6 – CÁC MỐI ĐE DỌA Ở TẦNG LIÊN KẾT; BẢO MẬT WI-FI

- Tổng quan bảo mật tầng liên kết
- Bảo mật mạng WLAN/Wifi
- Lỗ hổng wifi

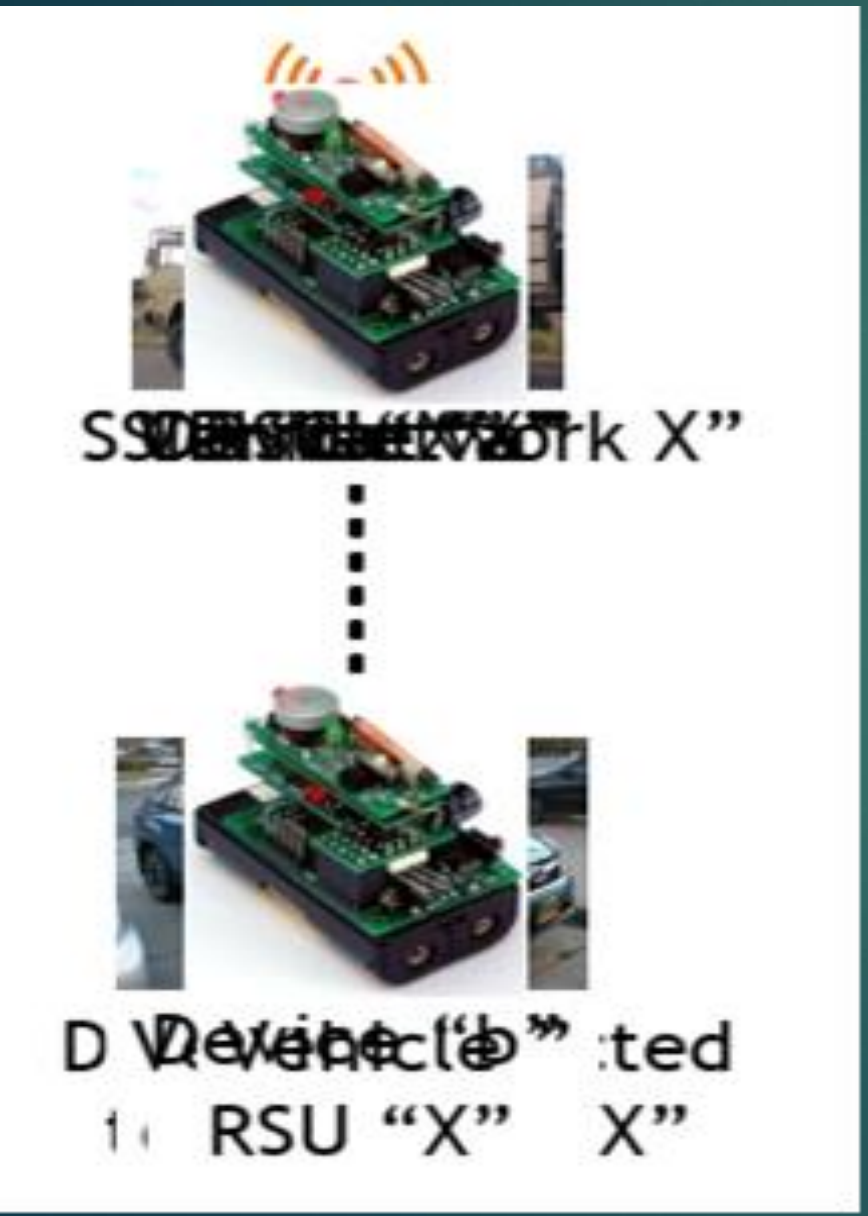
WIRELESS LINKS



CHỨC NĂNG TẦNG LIÊN KẾT

- Tầng liên kết không dây chịu trách nhiệm chính trong việc thiết lập và quản lý các liên kết điểm-điểm giữa các nút lân cận
- Ngoài ra, truyền khung dữ liệu đến/từ tầng vật lý PHY và tầng mạng

CÁC LOẠI LIÊN KẾT KHÔNG DÂY



- WiFi: AP — máy chủ
- Viễn thông: di động — BTS
- V2I: xe ↔ RSU
- V2V: xe ↔ xe
- V2C: xe ↔ cat

  - Không hẳn...

- D2D: thiết bị — thiết bị
- .....

PHÂN TÍCH DỊCH VỤ - SERVICE BREAKDOWN

- **Thiết lập liên kết:**
  - **– Khám phá hàng xóm**
  - **– Định địa chỉ**
  - **– Thiết lập/đồng bộ kênh**
  - **- Uỷ quyền/ xác thực**
- **Quản lý liên kết:**
  - **– Kiểm soát truy cập trung bình (MAC), tính khả dụng**
  - **- Bảo mật, toàn vẹn, v.v.**
  - **– Xếp hàng & lập lịch trình**
- **Dịch vụ phân tầng:**
  - **– PHY: tránh va chạm, cảm biến sóng mang, sửa lỗi, báo hiệu, v.v.**
  - **– NET: chuyển tiếp, chuyển mạch, v.v.**

CÁC NGUY CƠ TẦNG LIÊN KẾT

Về cơ bản, mọi dịch vụ ở lớp liên kết đều có các mối đe dọa tương ứng

KHÁM PHÁ MỐI ĐE DỌA

- Khám phá có thể bị ảnh hưởng bởi các thiết bị độc hại ngăn chặn các thiết bị lành tính tìm và kết nối với nhau
- Ví dụ:

  – *Trong mạng WiFi, một thiết bị độc hại có thể giả mạo điểm truy cập WiFi, thu hút những người dùng cả tin kết nối với kẻ tấn công thay vì mạng dự định kết nối*

  – *Trong MANET/VANET, kẻ tấn công Sybil có thể đưa ra nhiều danh tính mạng, thu hút các thiết bị bị giới hạn kết nối để lãng phí dung lượng trong bảng tra cứu*

CÁC MỐI ĐE DỌA TRUY CẬP MẠNG

- Quyền truy cập mạng có thể bị ảnh hưởng theo hai cách:
  1) Ngăn chặn quyền truy cập của các thiết bị hợp lệ và
  2) Giành quyền truy cập cho các thiết bị không hợp lệ
- Ví dụ:

– Ngăn chặn truy cập bằng DoS, cưỡng bức ngắt kết nối, v.v.

– Truy cập trái phép hoặc mức truy cập nâng cao, đạt được bằng cuộc tấn công dựa trên crypto, chiếm quyền điều khiển phiên, chiếm đoạt phiên trong quá trình chuyển giao, v.v. dựa trên các giao thức xác thực/ủy quyền

CÁC MỐI ĐE DỌA INFOSEC

- Tính bảo mật/bí mật có thể bị xâm phạm bằng cách tấn cryto hoặc các giao thức bảo mật được sử dụng để bảo vệ dữ liệu các chuyến bay
  - *Đặc biệt nếu cryto yếu được sử dụng*
- Tính toàn vẹn có thể bị tổn hại
  - *Cryto yếu hoặc thiết kế giao thức toàn vẹn không tốt*

MỐI ĐE DỌA TÍNH KHẢ DỤNG

- Tính khả dụng có thể bị đe dọa theo nhiều cách khác nhau từ việc khám phá, cụ thể là kẻ tấn công có thể cho phép bạn khám phá và kết nối, nhưng không có/dịch vụ kém

  – *Các mối đe dọa ở lớp PHY như nhiễu/gây nhiễu có thể ảnh hưởng đến quản lý kết nối với một AP được phát hiện*

  – *Gian lận thường có thể xảy ra ở lớp MAC do giả định rằng mọi người chơi tốt với nhau*

CÁC MỐI ĐE DỌA QUYỀN RIÊNG TƯ

• Quyền riêng tư của thiết bị/người dùng có thể gặp rủi ro do tiếp xúc/trao đổi thông tin nhận dạng có trong quá trình hình thành liên kết và quản lý

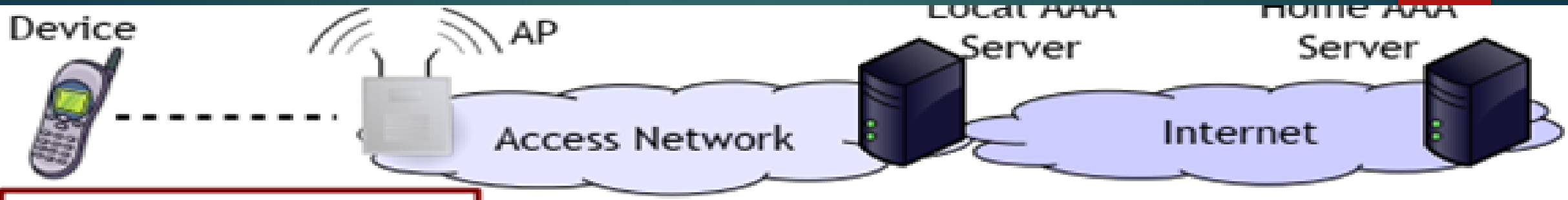
• Ví dụ:

– Trong WiFi (và hầu hết các thiết bị khác), các thiết bị được yêu cầu phát địa chỉ MAC xác định chúng

• *thậm chí Ngay cả khi MAC không được liên kết với danh tính cá nhân, các thông báo/vị trí tiếp theo có thể được liên kết với nhau*

CHI TIẾT HƠN VỀ MẠNG WIFI

MẠNG WIFI RIÊNG



Device needs to discover available AP to connect to

Network servers store credentials, identity, etc.

Device authenticates to AAA server

Server provides cryptographic material to AP

Device ↔ AP secure channel

AP ↔ Server / Internet secure channel

PHÁT HIỆN WI-FI

- Để thiết bị khách kết nối với AP, thiết bị cần phát hiện ra sự hiện diện/tồn tại của AP
- Hai cách để làm điều này:
  - AP có thể tự thông báo cho tất cả các thiết bị xung quanh
    - *Không thể làm điều này thường xuyên, vì vậy các thiết bị cần đợi – cũng cần kiểm tra nhiều kênh, vì các AP có thể di chuyển → chậm*
  - Khách hàng có thể gọi cho các AP đã biết - "WiFi Probing"
    - *Nếu máy khách đã kết nối trước đó, nó sẽ biết cách cấu hình AP nên có thể tìm thấy nó rất nhanh*
    - *Nhưng, ...*

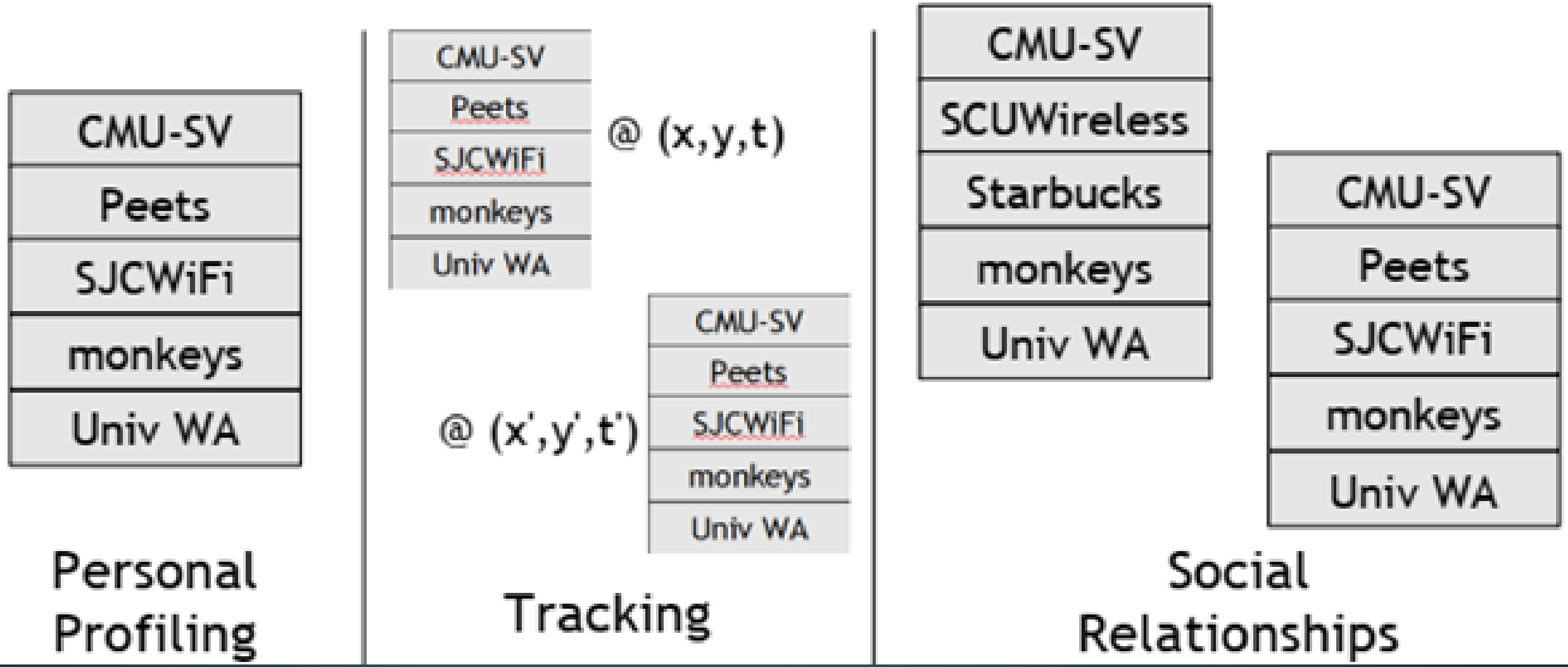
SỰ CỐ THĂM DÒ WIFI

Filter: (wlan.fc.type_subtype == 0x04) Expression...

Time	Source	Type	SSID
401.697011000	54:26:	Probe Request	
401.707384000	Apple_	Probe Request	
401.855865000	bc:cf	Probe Request	
401.868368000	Apple	Probe Request	
402.093322000	Apple_	Probe Request	Hooters
402.094443000	Apple_	Probe Request	Internet
402.095695000	Apple_	Probe Request	HarborLink - Buffalo Wi
402.096939000	Apple_	Probe Request	NetScout
402.098059000	Apple_	Probe Request	Rosen Guest Wireless
402.099190000	Apple_	Probe Request	Student
402.100310000	Apple_	Probe Request	Guest
402.101568000	Apple_	Probe Request	Gdaycreations
402.106317000	Apple_	Probe Request	cactusmoon_public
402.107442000	Apple_	Probe Request	NOTanIphone
402.108690000	Apple_	Probe Request	Gentleman Joes 3
402.109815000	Apple_	Probe Request	MISSION PRIVATE

CÁC MỐI ĐE DỌA DỰA TRÊN SSID

- Bất cứ khi nào thiết bị di động phát ra thông báo thăm dò, chúng tôi có thể tìm hiểu bộ SSID có liên quan của thiết bị đó



BẢN SỬA LỖI TIỀM NĂNG

- Vì nhiều mối đe dọa dựa trên các cặp MAC-SSID nên có thể sử dụng tên giả MAC

  – *Ngụ ý có một bên thứ ba đáng tin cậy để xử lý bút danh, yêu cầu phải có mối quan hệ từ trước*

- Thông tin MAC hoặc SSID có thể được mã hóa

  – *Yêu cầu tính toán hoặc tìm kiếm trên thiết bị di động và/hoặc AP để khám phá khóa nào sẽ được sử dụng để giải mã, yêu cầu mối quan hệ có sẵn*

- Không sử dụng thăm dò trực tiếp

  - *Chậm*

QUẢN LÝ TÊN GIẢ GSM - GSM PSEUDONYM

• Định danh người dùng và thiết bị:

– IMEI: ID thiết bị di động quốc tế - thiết bị

– IMSI: ID thuê bao di động quốc tế - người dùng

– TMSI: ID thuê bao di động tạm thời – bút danh

BUỔI 6.1:

THUYẾT TRÌNH GIỚI THIỆU DỰ ÁN