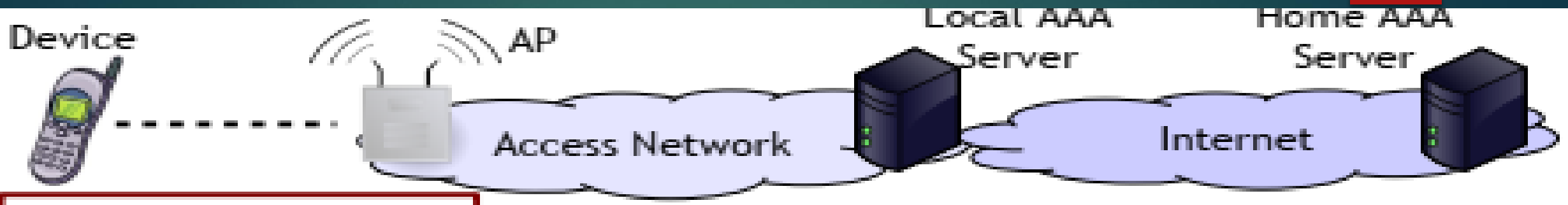
BÀI #7 BẢO MẬT WI-FI

TIẾP TỤC BẢO MẬT WIFI

TS. HOÀNG SỸ TƯƠNG

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

BẢO MẬT LIÊN KẾT WIFI

- Bảo mật liên kết WiFi tập trung chủ yếu vào kiểm soát truy cập và mã hóa

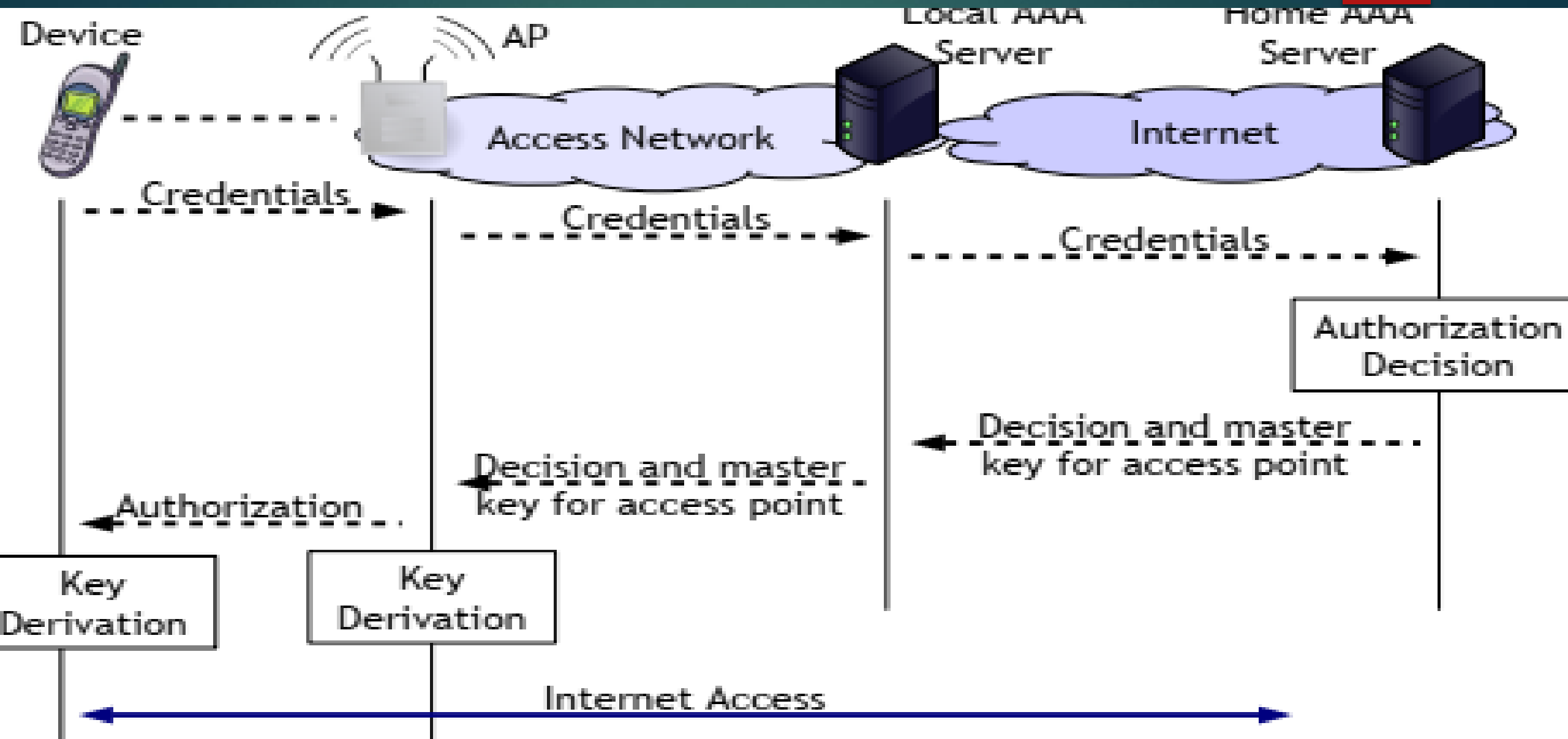
  - Trong các hệ thống WiFi riêng, quyền truy cập được kiểm soát bằng khóa dùng chung, thông tin xác thực danh tính hoặc bằng chứng thanh toán

  - Thông thường, xác thực chỉ dành cho người dùng/thiết bị, nhưng xác thực lẫn nhau có thể được một số người dùng/thiết bị mong muốn/yêu cầu

  - Bảo mật và toàn vẹn qua liên kết không dây

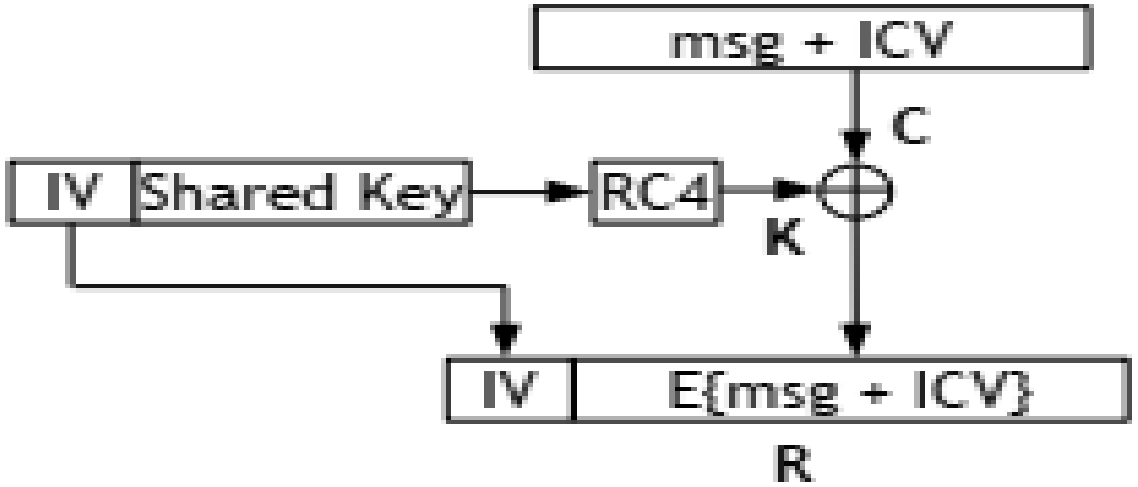
  - Phương tiện được chia sẻ giữa những người dùng WiFi không đáng tin cậy

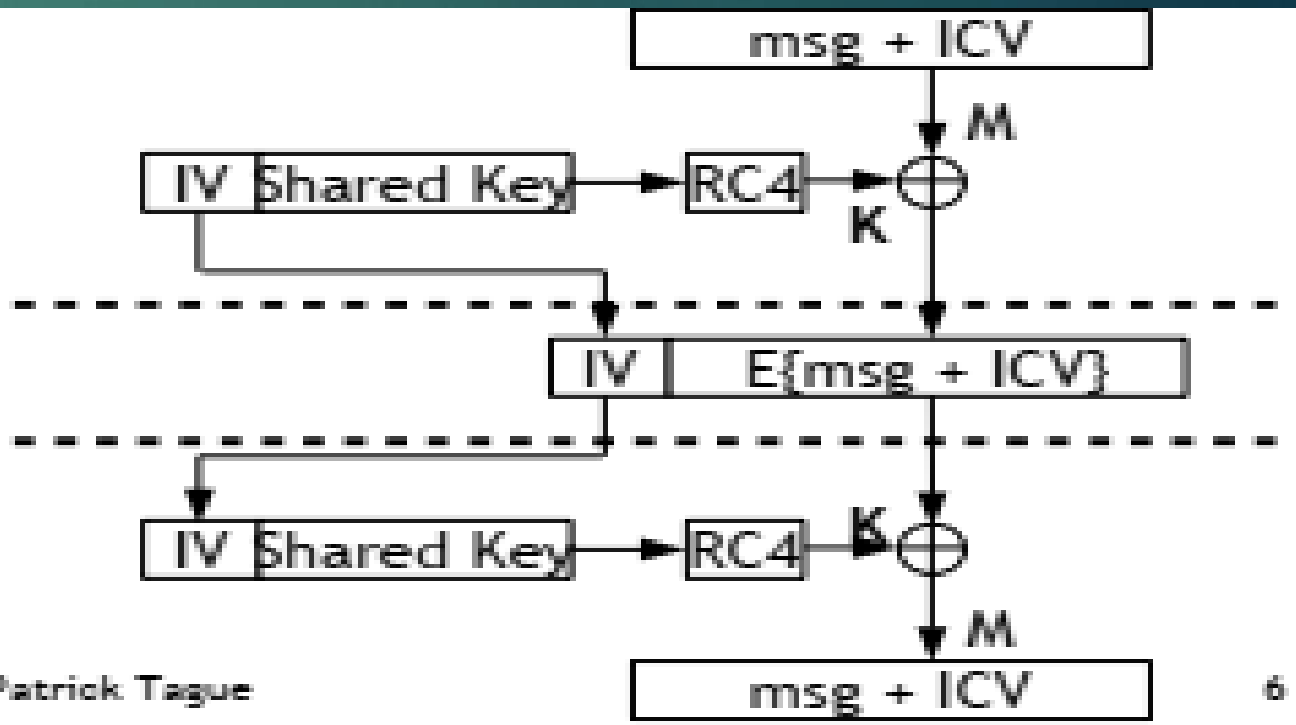
MẠNG WIFI RIÊNG



QUYỀN RIÊNG TƯ TƯƠNG ĐƯƠNG CÓ DÂY WEP - WIRED EQUIVALENT PRIVACY

- WEP nhằm mục đích làm cho nhiệm vụ dễ dàng truy cập mạng WLAN trở nên khó khăn hơn nhiều, như trong mạng có dây.
- WEP cung cấp mã hóa và xác thực
- Xác thực là phản hồi/thách thức để chứng minh kiến thức về khóa bí mật dùng chung
- Mã hóa dựa trên mã dòng RC4 sử dụng cùng một khóa





XÁC THỰC WEP

- Xác thực phản hồi/thách thức (Challenge-response) w/XOR

- Vấn đề 1: auth không tương hỗ

- Vấn đề 2: auth + enc sử dụng cùng khóa bí mật

- Vấn đề 3: auth chỉ xảy ra trên kết nối ban đầu

- Vấn đề 4: RC4 w/XOR

- *Kẻ tấn công có thể nhận được C và R = C XOR K, do đó nhận được K*
- *Có thể xác thực trong các phiên tương lai bằng cách sử dụng cùng một IV từ R*
- *Vì khóa bí mật được chia sẻ nên kẻ tấn công có thể giả mạo bất kỳ ai*

BẢO VỆ TÍNH TOÀN VẸN WEP

- Bảo vệ tính toàn vẹn dựa trên Giá trị kiểm tra tính toàn vẹn (ICV) dựa trên CRC

  - Tin nhắn được mã hóa là (M || CRC(M)) XOR K

  - CRC tuyến tính, nghĩa là CRC(X XOR Y) = CRC(X) XOR CRC(Y)

$$
\begin{aligned}
&((M \,||\, CRC(M)) \text{ XOR } K) \text{ XOR } (\Delta M \,||\, CRC(\Delta M)) \\
&= ((M \text{ XOR } \Delta M) \,||\, (CRC(M) \text{ XOR } CRC(\Delta M))) \text{ XOR } K \\
&= ((M \text{ XOR } \Delta M) \,||\, CRC(M \text{ XOR } \Delta M)) \text{ XOR } K
\end{aligned}
$$

  - Ngoài ra, WEP không cung cấp bảo vệ phát lại

TÍNH BÍ MẬT WEP

• Tính bí mật được xử lý bởi WEP IV

- **Vấn đề 1:** IV 24bit lặp lại vài giờ một lần cho mỗi người dùng

  • *Tất cả người dùng có cùng khóa bí mật...*

- **Vấn đề 2:** IV = 0; cho mỗi gói: IV++;

  • *Trình tự giả ngẫu nhiên giống nhau đối với mọi người dùng*

  • *Kẻ tấn công có thể chèn tin nhắn đúng lúc*

- **Vấn đề 3:** Sử dụng RC4 không phù hợp

  • *"Khóa yếu" là hạt giống RC4 cho phép suy luận các bit khóa*

• **Chuyên gia:** luôn vứt bỏ 256B đầu tiên của đầu ra RC4

  • *WEP không làm điều này + số lượng IV nhỏ = khóa yếu gặp phải kẻ tấn công có thể khôi phục toàn bộ khóa bí mật*

VÌ VẬY, WEP BỊ PHÁ VỠ HOÀN TOÀN.

CHÚNG TA ĐÃ GIẢI QUYẾT VẤN ĐỀ WEP NHƯ THẾ NÀO?

IEEE 802.11 i

- Thông số kỹ thuật của IEEE cho bảo mật mạng mạnh mẽ

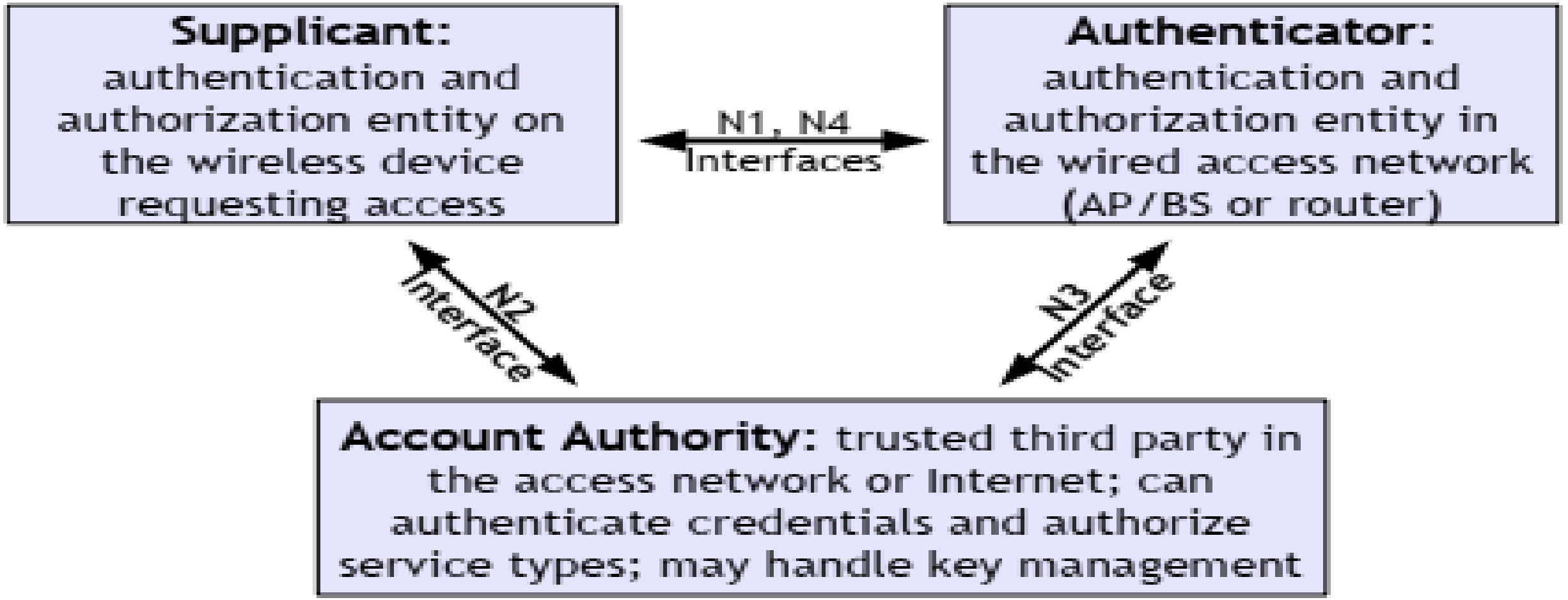
  - Xác thực và kiểm soát truy cập dựa trên 802.1x

  - Cơ chế bảo vệ toàn vẹn và bí mật dựa trên AES để thay thế RC4

802.1x

- Chuẩn xác thực và kiểm soát truy cập

- Được thiết kế cho mạng LAN có dây, nhưng được mở rộng sang mạng WLAN



GIAO THỨC NAC

- Các giao thức liên quan đến NAC

  - Giao thức xác thực mở rộng (EAP)

    - *Xác thực đầu cuối giữa thiết bị và trình xác thực tài khoản*

    - *Hỗ trợ nhiều phương thức xác thực client-server*

  - IEEE 802.1x (mở rộng đến 802.11i)

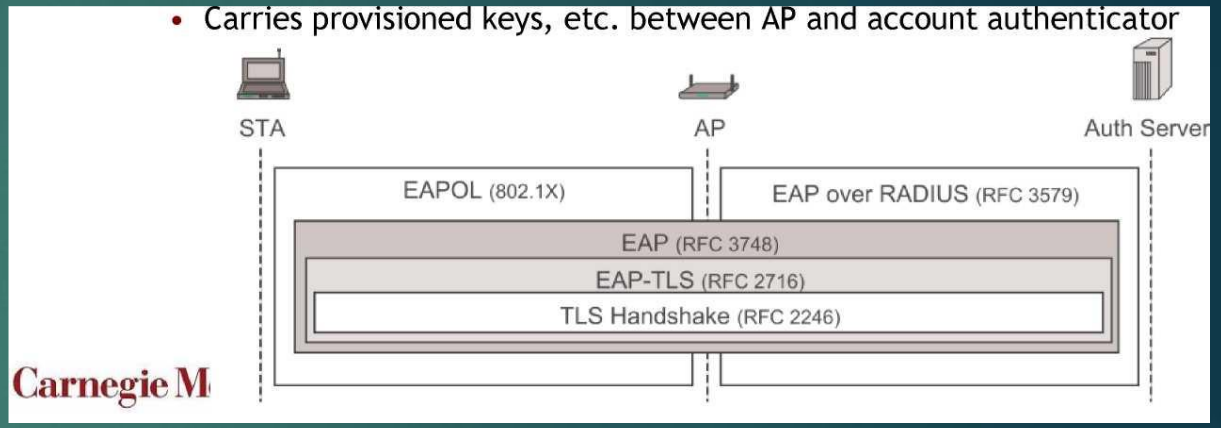
    - *Mang EAP qua liên kết mạng LAN không dây (EAPoL) giữa thiết bị và AP*

    - *802.11i yêu cầu khóa phiên trên mỗi trạm, không phải trong mạng có dây do cổng trên mỗi dây*

  - Radius

    - *Vận chuyển EAP giữa AP và trình xác thực tài khoản*

    Mang khóa được cung cấp, v.v. giữa AP và trình xác thực tài khoản



NGOÀI KHÓA ĐƯỢC CHIA SẺ

- STA và AP chia sẻ khóa chính theo cặp (PMK) được sử dụng để lấy khóa tạm thời theo cặp (PTK)

  - PTK = khóa mã hóa dữ liệu (DEK), khóa toàn vẹn dữ liệu (DIK), khóa mã hóa khóa (KEK), khóa toàn vẹn khóa (KIK)

  - Bắt tay bốn bước sử dụng nonces

    - *AP gửi nonce tới STA, STA tính toán PTK*

    - *STA gửi nonce và MIC sử dụng KIK tới AP*

    - *AP tính toán PTK, xác minh MIC, gửi MIC + SN (để bảo vệ phát lại) tới STA, sẵn sàng*

    - *STA xác minh MIC và ACK để sẵn sàng*

- AP và tất cả các STA cũng chia sẻ một khóa tạm thời của nhóm (GTK)

TUY NHIÊN, RC4 VÀ AES ĐÃ ĐƯỢC TRIỂN KHAI TRONG PHẦN CỨNG NÊN VIỆC NÂNG CẤP KHÔNG THỂ DIỄN RA TRONG MỘT SỚM MỘT CHIỀU

TRUY CẬP WIFI ĐƯỢC BẢO VỆ

- Giao thức về Tính toàn vẹn Key Temporal

  - TKIP 802.11i sử dụng RC4 thay vì AES

  - Cho phép nâng cấp firmware ngay lập tức để sử dụng TKIP

  - WPA là tập hợp con của 802.11i được hỗ trợ thông qua TKIP

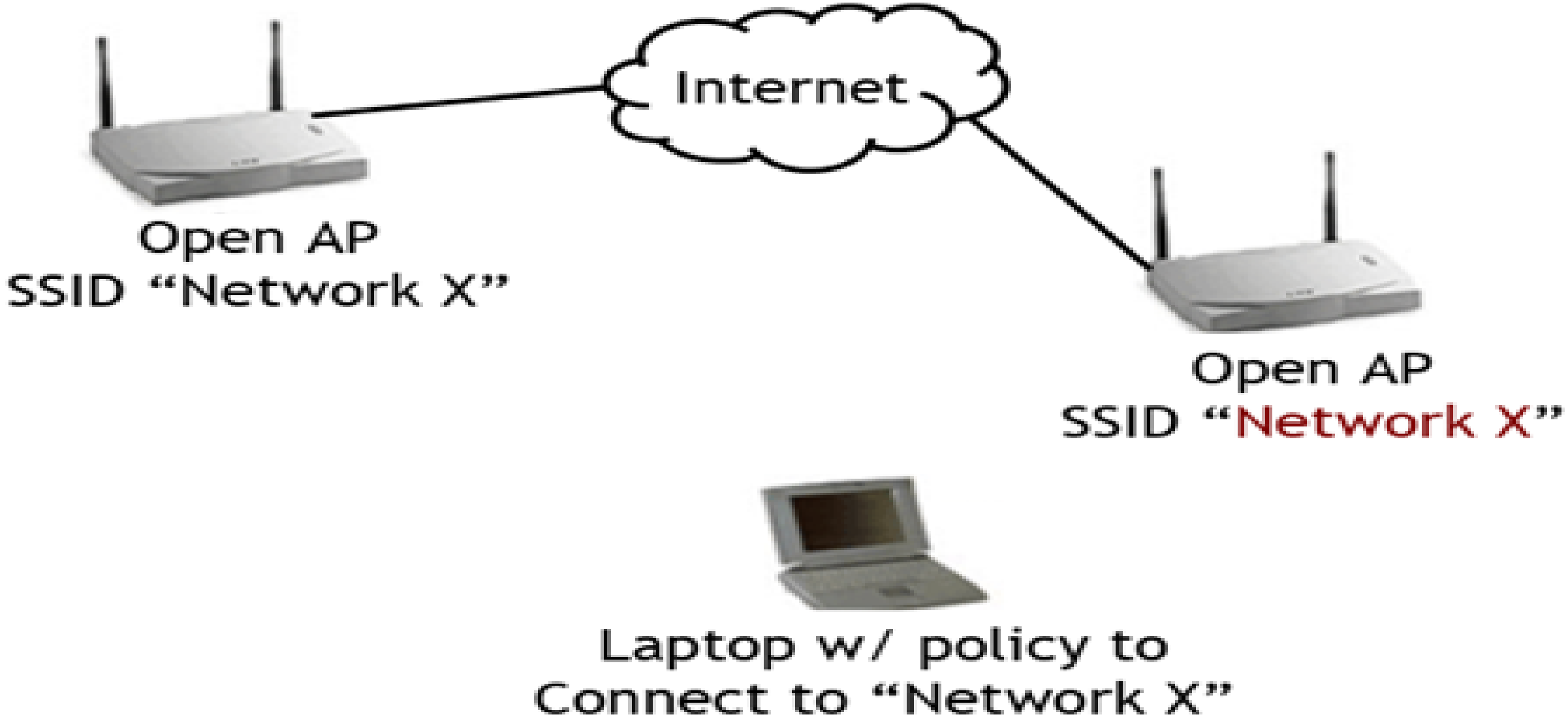
    - *Xác thực và kiểm soát truy cập trong WPA và 802.11i giống nhau*

    - *Tính toàn vẹn và bảo mật dựa trên TKIP*

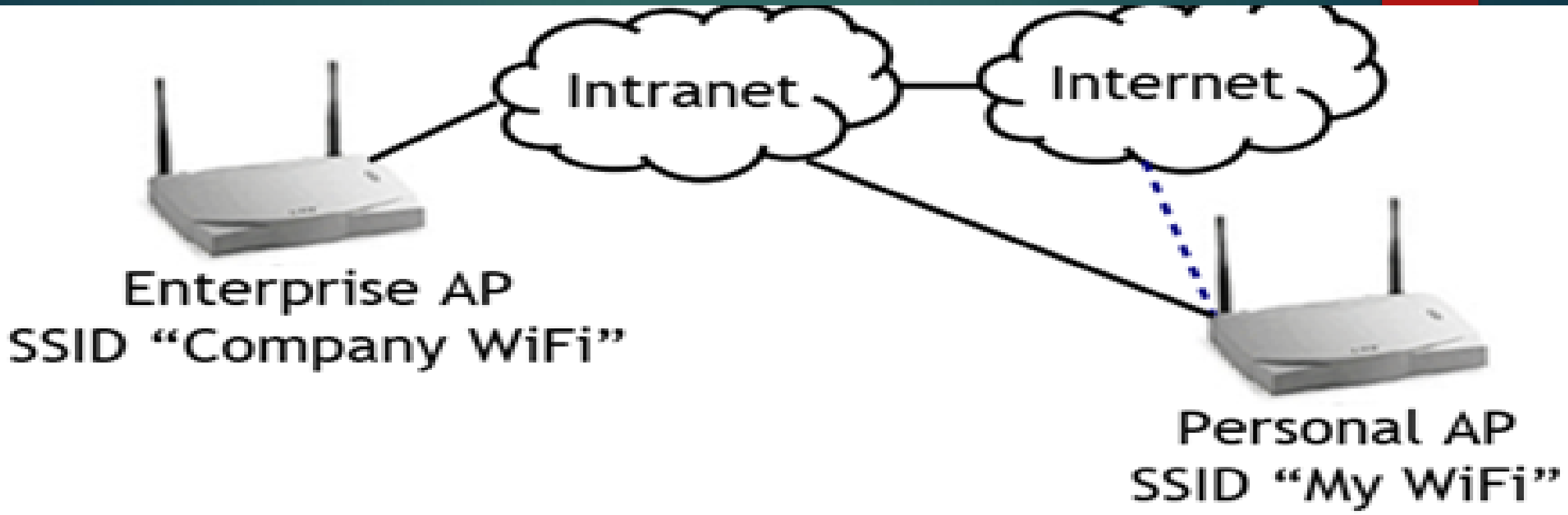
- WPA2 triển khai đầy đủ 802.11i

  - WPA2 vẫn còn một số điểm yếu.

VÌ VẬY, NHỮNG DẠNG TẤN CÔNG CÓ THỂ XẢY RA LÀ GÌ?


Internet
Open AP
SSID "Network X"
Open AP
SSID "Network X"
Laptop w/ policy to
Connect to "Network X"

CÁC MỐI ĐE DỌA AP GIẢ MẠO TRONG DOANH NGHIỆP



MỘT SỐ TẤN CÔNG THÚ VỊ KHÁC

- Nghịch đảo chiến tranh [Beetle & Potter, shmoo.com]

  - Wardrive đang sử dụng ứng dụng khách WiFi để tìm các AP đang mở để nhận dịch vụ Internet miễn phí

  - Inverse Wardrive đang sử dụng Fake AP để tìm các ứng dụng khách WiFi sẽ kết nối với nó

    - *Nếu máy khách có lỗ hổng chưa được vá thì sao?*

    - *IW có thể được sử dụng để định vị các máy khách dễ bị tấn công và khai thác chúng*

    - *Ví dụ: lây nhiễm mã độc cho chúng*

  - Tạo Fake AP rất dễ dàng, đặc biệt là sử dụng các công cụ như Airsnarf ....

CÒN CÁC MỐI ĐE DỌA NỘI BỘ THÌ SAO?

LỖ HỔNG HOLE196

- Được phát hiện vào năm 2010 bởi Md. Sohail Ahmad của AirTight Security

- Được đặt tên theo số trang trong IEEE 802.11-v2007

- Những kẻ nội gián ác ý có thể lạm dụng GTK

  - *Ví dụ: Đầu độc ARP bằng cách sử dụng GTK cho phép người trong cuộc tự quảng cáo cổng, lừa họ chuyển hướng dữ liệu của họ tới người trong cuộc thông qua AP*

[Image from AirTight Networks whitepaper]

LỖ HỔNG HOLE196 DOS

- Hole196 cũng liên quan đến lỗ hổng DoS

  - Người dùng nội bộ có thể sử dụng khung bảo vệ phát lại trong WPA2 để DoS một thiết bị khác

  - Phát gói mã hóa GTK có số thứ tự cao hơn giá trị bộ đếm hiện tại

  - Tất cả khách hàng sẽ cập nhật bộ đếm của họ lên giá trị mới

  - Tất cả các quảng bá hợp pháp có số thứ tự thấp hơn giá trị của kẻ tấn công sẽ bị loại bỏ

CÁC VẤN ĐỀ KHÁC VỀ HOLE196

- Người trong cuộc có thể khởi động một số cuộc tấn công khác bằng cách sử dụng lỗ hổng Hole196

  - Bao gồm một payload độc hại khác trong các gói được mã hóa GTK giả mạo có thể dẫn đến khai thác lớp cao hơn

    - *Ví dụ: Tấn công lớp IP vào một địa chỉ IP cụ thể, đặt lại TCP, chuyển hướng TCP, thao túng DNS, quét cổng, tiêm phần mềm độc hại, leo thang đặc quyền*

  - Xem sách trắng của AirTight Networks để biết chi tiết

VÁ LỖI 196 (1)

- Cách ly máy khách

  - Một số bộ điều khiển và AP có thể tách biệt các máy khách với nhau một cách hợp lý, ngăn chặn lưu lượng dữ liệu từ nạn nhân đến nội bộ khi cả hai được kết nối với cùng một AP hoặc miền của bộ điều khiển

  - Không phải là một giải pháp hoàn chỉnh, vì các biến thể của đầu độc ARP và MitM có thể vượt qua sự cô lập của máy khách

  - Không được tiêu chuẩn hóa, vì vậy việc triển khai là độc quyền và có thể khác nhau giữa các nhà cung cấp

VÁ LỖI 196 (2)

- Không sử dụng GTK

  - Hầu hết các kiến trúc mạng WLAN dựa trên bộ điều khiển không sử dụng GTK cho bất kỳ mục đích gì, vì AP không truyền lưu lượng quảng bá

  - Các nhà cung cấp có thể khắc phục lỗ hổng bằng cách thay thế GTK bằng một giá trị (ngẫu nhiên) duy nhất cho mỗi máy khách

  - Vô hiệu hóa lỗ hổng Hole196 mà không có chi phí liên quan

- Nếu AP gửi lưu lượng quảng bá, nó sẽ phải được mã hóa bằng cách sử dụng các giá trị duy nhất và không phát sóng

VÁ LỖI 196 (3)

- WIPS
  - Các hệ thống ngăn chặn xâm nhập không dây có thể cung cấp một lớp bảo vệ để phát hiện các cuộc tấn công dựa trên GTK và ngăn chặn chúng cho đến khi lỗ hổng được vá

TÓM TẮT

BẢO MẬT WIFI ĐÃ KHÁ PHÁT TRIỂN, NHƯNG VẪN CHƯA ĐƯỢC HIỂU RÕ HOÀN TOÀN, MỘT PHẦN DO TÍNH PHỔ BIẾN VÀ MỘT PHẦN DO ĐỘ PHỨC TẠP

BUỔI 7.1:

THUYẾT TRÌNH GIỚI THIỆU DỰ ÁN

BUỔI 8:

BẢO MẬT PHÁT SÓNG QUẢNG BÁ & QUẢN LÝ KHÓA.