Đề tài 12. Tìm hiểu về các lỗ hổng bảo mật trên mạng không dây và lựa chọn tìm hiểu các công cụ: WEPCrack, AirSnort, Aircrack

**I. Mạng không dây**

***I.1. Mạng không dây***

Mạng không dây (hay còn gọi là mạng Wireless, mạng Wi-Fi, 802.11) là mạng kết nối các thiết bị có khả năng thu phát sóng (như laptop, smartphone, etc.) lại với nhau không sử dụng dây dẫn mà sử dụng sóng vô tuyến được truyền dẫn trong không gian thông qua các trạm thu phát sóng.

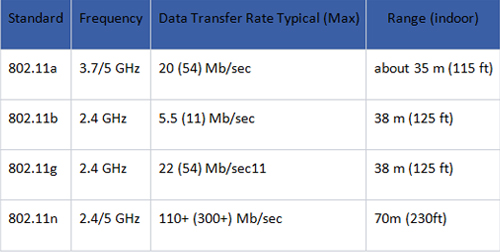


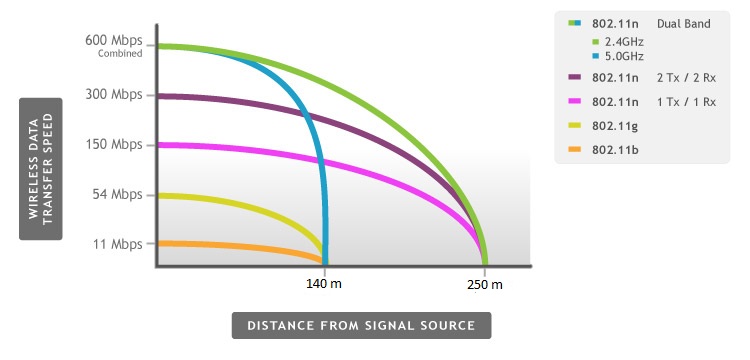
Điển hình về mạng không dây là mạng Wi-Fi, mạng 4G, mạng Bluetooth, mạng truyền thông vệ tinh, mạng cảm biến không dây.

***I.2. Mạng Wi-Fi***

Wi-Fi (Wireless Fidelity) – công nghệ kết nối không dây phổ biến nhất hiện nay, thường bị lạm dụng để chỉ kết nối không dây nói chung.

Ưu điểm của kết nối Wi-Fi là khả năng hoạt động hiệu quả trong phạm vi vài chục đến vài trăm mét của các mạng WLAN. Việc thiết lập kết nối Wi-Fi cũng rất dễ dàng và không đòi hỏi nhiều kiến thức chuyên môn. Về mặt tốc độ, công nghệ Wi-Fi ngày càng được cải thiện để đáp ứng nhu cầu ngày càng cao của người dùng. Được hiệp hội Wi-Fi xây dựng dựa trên bộ giao thức IEEE 802.11, chúng ta có thể thấy sự tiến bộ của công nghệ này theo thời gian trong bảng sau đây.





Ngoài những ưu điểm tính tiện dụng, linh hoạt, kết nối Wi-Fi cũng có những nhược điểm của riêng mình. Phương pháp truyền tín hiệu broadcast trong các công nghệ không dây đòi hỏi phải có các biện pháp bảo mật phù hợp đi kèm để tránh thất thoát thông tin. Phương pháp mã hóa WEP (Wired Equivalent Privacy) hiện đã quá cũ kĩ và dễ dàng bị bẻ khóa; các công nghệ WPA, WPA2 mới hơn và đang được sử dụng rộng rãi cho các nhu cầu gia đình hoặc doanh nghiệp.

Một nhược điểm nữa là việc sử dụng dải tần 2.4GHz khiến sóng Wi-Fi dễ bị ảnh hưởng bởi nhiều yếu tố như sóng Bluetooth, lò vi sóng và các thiết bị điện khác trong nhà làm giảm đáng kể hiệu quả hoạt động của mạng.

**II. Các lỗ hổng của mạng không dây trên các giao thức mã hóa mạng**

***II.1. Các lỗ hổng của mạng không dây***

*II.1.1. Hạn chế về khả năng quản trị*

Bất kỳ thiết bị điện tử nào nằm trong vùng phủ sóng đều có thể kết nối mạng không dây. Chính vì thể các đối tượng xấu có thể xâm nhập vào mạng để tấn công những người dùng khác nếu biết cách đột nhập.

*II.1.2. Khả năng mã hóa dữ liệu*

Mặc dù thông tin truyền trên mạng đã được mã hóa nhằm ngăn chặn việc truy cập bất hợp pháp, nhưng các hacker có thể sử dụng các thiết bị để chặn dữ liệu rồi giải mã chúng, tìm kiếm khóa. Sau đó truy cập trái phép vào mạng và các máy tính gia nhập mạng.

Mới đây, mã hóa WPA2 đã bị bẻ khóa sử dụng KRACK. Bản chất của KRACK là lỗ hổng trong hệ thống giao thức kết nối WPA2 giữa điểm phát sóng và thiết bị. Sử dụng nó, hacker có thể đọc được thông tin mã hóa trên mạng Wifi, chặn những thông tin nhạy cảm như số thẻ tín dụng, mật khẩu, ảnh, tin nhắn.

*II.1.3. Xác thực quyền người dùng*

Lỗ hổng trong quá trình xác thực người dùng giúp cho kẻ tấn công có thể tấn công vào mạng không dây. Chẳng hạn, kẻ tấn công có thể giả mạo khách hàng gửi thông điệp yêu cầu truy cập mạng đến Access Point (AP). Sau đó điểm truy cập sẽ trả lời bằng một thông điệp và chờ người dùng xác nhận, nhưng kẻ tấn công không xác nhận lại mà dựa vào bản tin AP gửi cho và có thể sử dụng các công cụ để tìm ra khóa và tấn công vào mạng.

***II.2. Các giao thức mã hóa mạng và lỗ hổng***

Wi-Fi sử dụng nhiều chuẩn mã hóa khác nhau nhằm bảo vệ tránh sự truy cập trái phép, vì tính đặc thù của kết nối không dây là không thể giới hạn về mặt vật lý truy cập đến đường truyền, bất cứ ai trong vùng phủ sóng đều có thể truy cập được.

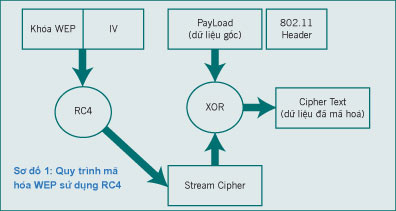
Bài báo cáo sẽ trình bày sơ lược về 3 loại chính gồm: WEP, WPA, WPA2

*II.2.1. WEP*

WEP (Wired Equivalent Privacy) là kiểu mã hóa ra đời sớm nhất và được hỗ trợ phổ biến nhất bởi các nhà sản xuất thiết bị Wi-Fi. WEP cung cấp tính bảo mật và toàn vẹn của thông tin trên mạng không dây, đồng thời được xem như một phương thức kiểm soát truy cập. Một máy nối mạng không có khóa WEP chính xác sẽ không thể truy cập đến Access Point (AP) và cũng không thể giải mã cũng như thay đổi dữ liệu đường truyền.

WEP sử dụng thuật toán đối xứng RC4 cho phép chiều dài của khóa thay đổi lên tới 256 bit. Chuẩn 802.11 bắt buộc các thiết bị WEP phải hỗ trợ chiều dài khóa tối thiểu là 40 bit. Hiện nay, đa số các thiết bị không dây hỗ trợ WEP với ba chiều dài khóa: 40 bit, 64 bit, và 128 bit.

Thuật ngữ: Phương thức mã hóa dòng (stream cipher) là phương thức mã hóa dữ liệu theo từng bit, đối nghịch với phương thức mã hóa khối (block cipher), mã hóa dữ liệu theo từng khối (thường là 64 bit)



\* Lỗ hổng WEP và cách tấn công

WEP sử dụng RC4, một thuật toán sử dụng phương thức mã hóa dòng, nên cần một cơ chế đảm bảo hai dữ liệu giống nhau sẽ không cho kết quả giống nhau sau khi được mã hóa hai lần khác nhau nhằm tránh sự suy đoán của hacker. Để đạt mục đích trên, một giá trị có tên là Initialization Vector (IV) được sử dụng để cộng thêm với khóa WEP nhằm tạo ra khóa khác nhau mỗi lần mã hóa. IV là một giá trị có chiều dài 24 bit và được chuẩn IEEE 802.11 đề nghị khác nhau mỗi lần mã hóa.

Do khi thiết bị gửi tạo ra IV một cách ngẫu nhiên, nên IV bắt buộc phải được gửi đến thiết bị nhận ở dạng không mã hóa trong header của gói dữ liệu 802.11 nên bất cứ ai “tóm” được dữ liệu trên mạng đều thấy được. Với độ dài 24 bit, giá trị của IV dao động trong khoảng 16.777.216 trường hợp, nếu hacker bắt giữ đủ một số lượng package nào đó thì hoàn toàn có thể phân tích các IV này để đoán ra khóa WEP.

Hơn nữa, ba nhà phân tích mã hóa Fluhrer, Mantin, và Shamir (FMS – Đại học Berkeley) đã phát hiện những điểm yếu của thuật toán tạo IV cho RC4 và vạch ra một phương pháp phát hiện và sử dụng những IV lỗi nhằm tìm ra khóa.

Cả 2 phương pháp nêu trên đều mang tính chất thụ động. Có nghĩa là kẻ tấn công chỉ cần thu nhận các gói dữ liệu trên đường truyền mà không cần liên lạc với Access Point. Điều này khiến khả năng phát hiện các tấn công tìm khóa WEP đầy khó khan và gần như không thể phát hiện được. Hiện nay, trên Internet đã có sẵn nhưng công cụ có khả năng tìm khóa WEP như AirCrack, AirSnort, WepCrack,…

*II.2.2. WPA và WPA2*

WPA (Wi-Fi Protected Access) là một giải pháp bảo mật được đề nghị bởi Wi-Fi Alliance nhằm khắc phục những hạn chế của WEP.

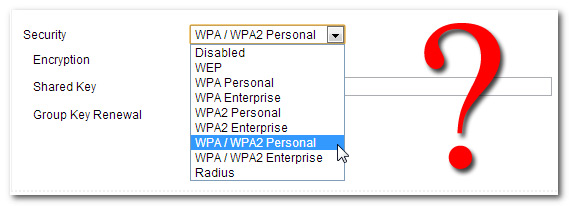
WPA sử dụng một khóa động mà được thay đổi một cách tự động nhờ vào giao thức TKIP (Temporal Key Integrity Protocol). TKIP dùng một khóa nhất thời 128 bit kết hợp với địa chỉ MAC của user host và IV để tạo ra mã khóa. Mã khóa này sẽ được thay đổi sau khi 10000 gói thông tin được trao đổi.

Phiên bản phổ biến nhất là WPA-PSK (pre-shared key) là sẽ dùng một password (Master Key) chung cho AP và client devices. Thông tin authentication giữa user và server sẽ được trao đổi thông qua giao thức 802.1x/EAP (Extensible Authentication Protocol).

WPA sử dụng MIC (Message Integrity Check) để kiểm tra tính toàn vẹn của gói tin. MIC là một message 64 bit được tính dựa trên thuật tóan Michael. MIC sẽ được gửi trong gói TKIP và giúp người nhận kiểm tra xem thông tin nhận được có bị lỗi trên đường truyền hoặc bị thay đổi bởi kẻ phá hoại hay không.

\* Lỗ hổng WPA

Hacker có thể lợi dụng điểm yếu ở thuật toán mã hóa của TKIP, nhưng TKIP sau đó được thay thế bằng AES (Advanced Encryption Standard). Lỗ hổng phổ biến nằm ở một hệ thống bổ sung được phát hành cùng WPA là WPS (Wi-Fi Protected Setup) – một hệ thống giúp liên kết thiết bị với các điểm truy cập một cách dễ dàng.



\* WPA2: sử dụng một thành phần mới thay thế cho TKIP có tên là CCMP, đồng thời yêu cầu sử dụng thuật toán AES. WAP2 + AES đang là chuẩn an toàn lý tưởng nhất hiện nay.

Tuy nhiên, mới đây, một lỗ hổng của WPA2 được khai thác bởi KRACK (Key Reinstallation Attack). Bản chất của KRACK là lỗ hổng trong hệ thống giao thức kết nối WPA2 giữa điểm phát sóng và thiết bị. Hiện tại các nhà cung cấp thiết bị mạng đã bắt đầu tung ra các bản vá để khắc phục lỗi này.

**III. Công cụ WEPCrack, AirSnort, Aircrack**

Công cụ dùng để penetration testing mạng không dây, crack wep và dò khóa wpa/wpa2-psk.

APPENDIX

[1] KRACK (Key Reinstallation Attack)

http://time.com/4983720/krack-attack-wpa2-wifi/

https://www.krackattacks.com/

[2] Tham khảo

<http://www.vnpro.vn/so-luoc-ve-mang-khong-day/>

<http://www.vnpro.vn/tong-quan-lo-hong-bao-mat-va-mot-so-ky-thuat-tan-cong-vao-mang/>

<http://genk.vn/do-choi-so/khai-quat-ve-mang-khong-day-2013011411154296.chn>

<http://greennet.vn/tin-tuc/do-khoa-wep-cua-mang-wifi-va-cach-bao-ve-2/>

<http://www.pcworld.com.vn/articles/cong-nghe/cong-nghe/2006/03/1188349/wep-bao-mat-cho-mang-khong-day/>