Khoa Công nghệ thông tin

Lớp: TH

Môn: Mã hóa thông tin và ứng dụng

Đề tài tìm hiểu: Wireless Security – WEP, WAP, WAP2

Sinh viên thực hiện:

# WEP

## Giới thiệu

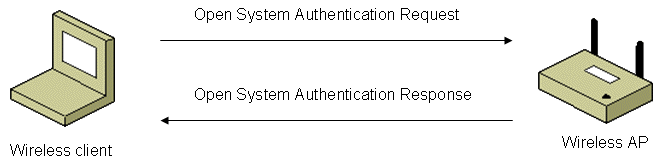
* WEP (Wired Equivalent Privacy, bảo mật tương đương mạng có dây), là một phần của chuẩn IEEE 802.11, được phê chuẩn vào 9/1999, sử dụng thuật toán RC4 (mã hóa đối xứng) để bảo mật thông tin và CRC-32 checksum để đảm bảo tính toàn vẹn của thông tin. Khóa WEP ở phía client dùng để chứng thực với Access Point, mã hóa và giải mã dữ liệu.
* Chuẩn 64-bit WEP (còn gọi là WEP-40) dùng 40 bit làm key, 24 bit làm IV (Initialization vector), chuẩn mở rộng 128-bit WEP (còn gọi là WEP-104) (chuẩn IEEE 802.11 không có nhưng nhiều nhà cung cấp hỗ trợ chuẩn này trong các thiết bị Access Point của họ) dùng key 104 bit. Đối với WEP-104, nó gồm một chuỗi 26 ký tự hexa (0-9, a-f), mỗi ký tự mô tả 4 bit của key, 26 \* 4 bit = 104 bit (cách tính tương tự cho các chuẩn WEP khác). Ngoài ra, một số nhà sản xuất cũng hỗ trợ 256-bit WEP trong một số sản phẩm của họ.

## Chứng thực

Trước khi truyền nhận dữ liệu với Access Point, client cần phải chứng thực mình là ai. Đối với WEP, có 2 cách chứng thực (Authentication) được dùng: Open System authentication and Shared Key authentication.

### Open System authentication

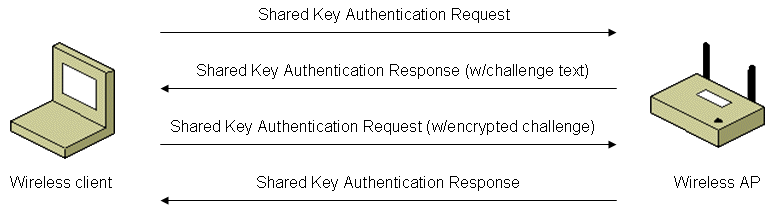
* Không cần chứng thực, client không cần cung cấp giấy ủy nhiệm (credentials) của nó cho Access Point trong quá trình chứng thực. Vì thế bất kỳ client nào cũng có thể chứng thực bản thân nó với Access Point và kết nối với Access Point mà không cần phải có khóa WEP. Sau quá trình chứng thực và kết nối với Access Point, WEP được dùng để mã hóa dữ liệu. Bắt đầu từ thời điểm này, client cần phải có khóa hợp lệ.
* Quá trình chứng thực theo Open System authentication
  1. Client gửi một thông điệp yêu cầu chứng thực theo kểu Open System Authentication, trong đó có chứa địa chỉ MAC của client.
  2. Access Point gửi lại một thông điệp cho biết việc chứng thực của client thành công hay thất bại.



* Một số Access Point cho phép cấu hình danh sách các địa chỉ MAC của client được phép kết nối đến Access Point. Nhưng với cách này, nó cũng không thể bảo vệ được mạng wireless, vì những kẻ tấn công có thể bắt gói tin của các client và lấy địa chỉ MAC của client đó. Dùng địa chỉ MAC của nạn nhân để truy cập vào mạng wireless.

### Shared Key authentication

* Access Point kiểm tra client có hợp lệ hay không thông qua một khóa được qui định trước giữa client và Access Point (Shared Key). WEP được dùng để chứng thực.
* Quá trình chứng thực gồm 4 bước:

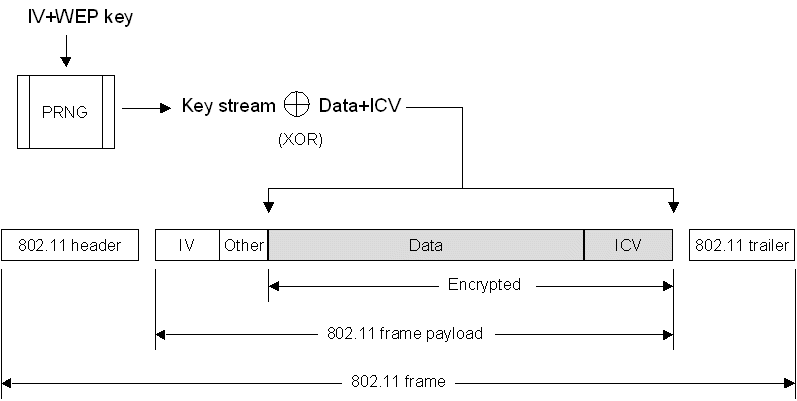
1. Client gửi một yêu cầu chứng thực cho Access Point.
2. Access Point gửi lại nonce (một chuỗi bit ngẫu nhiên dùng để thử thách client) cho client.
3. Client mã hóa nonce bằng cách dùng WEP và khóa WEP đã được cấu hình trước, và gửi lại 1 yêu cầu chứng thực khác bao gồm cả nonce đã mã hóa.
4. Access Point giải mã nonce đã mã hóa và so sánh với nonce mà nó đã gửi đi. Tùy vào kết quả so sánh mà Access Point sẽ trả lời là có hợp lệ hay không. Sau quá trình chứng thực và kết nối với Access Point, WEP được dùng để mã hóa dữ liệu.
   1. 

* Nhìn vào thì thấy rằng Shared Key authentication an toàn hơn Open System authentication, vì phải chứng thực trước khi kết nối với Access Point. Tuy nhiên, sự thật hoàn toàn ngược lại, hacker có thể lấy được khóa WEP bằng cách bắt 4 gói tin trong quá trình chứng thực.

## Mã hóa

Quá trình mã hóa diễn ra theo trình tự sau:

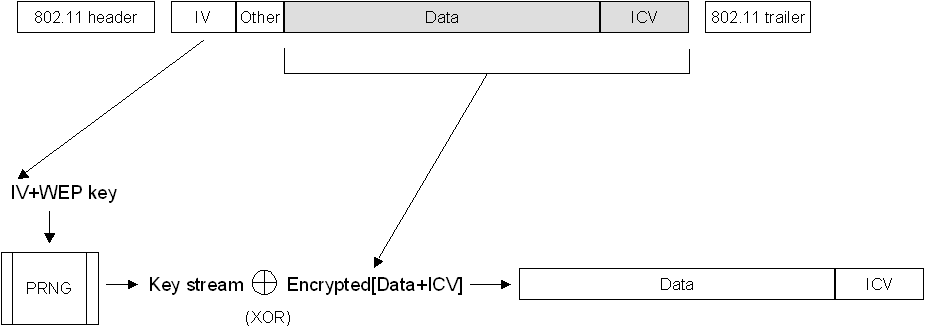
1. Tính ICV (32 bit, chính là checksum) từ dữ liệu cần mã hóa (data frame).
2. Thêm ICV vào cuối data frame.
3. Tạo IV (24 bit) và thêm nó vào khóa WEP.
4. [IV + khóa WEP] được dùng để tạo keystream (là một chuỗi các bit) bằng thuật toán RC4 (trong hình chính là PRNG, pseudo-random number generator), keystream có kích thước bằng với [data+ICV].
5. Lấy keystream XOR với [Data+ICV] tạo thành [Data+ICV] được mã hóa, nó là một phần của frame payload.
6. Để tạo frame payload, IV và trường khác được thêm vào trước [Data+ICV] đã được mã hóa.



## Giải mã

Quá trình mã hóa diễn ra theo trình tự sau:

1. Lấy được IV từ phần đầu của frame payload.
2. IV được thêm vào khóa WEP.
3. Dùng thuật toán RC4 (trong hình là PRNG) để tạo keystream từ [IV+khóa WEP], quá trình này dùng để tái tạo lại keystream.
4. Lấy keystream XOR với [Data+ICV] đã được mã hóa để giải mã ra phần [Data+ICV] ban đầu.
5. Tính lại ICV từ Data đã được giải mã, rồi đem so sánh với ICV nhận được từ payload, nếu 2 giá trị này bằng nhau thì dữ liệu nhận được là hợp lệ (không bị thay đổi trong quá trình truyền đi), ngược lại dữ liệu này được tự động loại bỏ (không hợp lệ).



## Vì sao sử dụng IV và checksum (CRC-32) trong gói tin của WEP

### Sử dụng IV

* Để chống lại reused key attack (tấn công bằng cách sử dụng lại khóa). Do WEP sử dụng khóa tĩnh trong cả quá trình chứng thực, mã hóa và giải mã thông điệp, và khóa WEP không thay đổi theo thời gian, theo từng phiên làm việc. Nên người tấn công chỉ cần bắt các gói tin và phân tích chúng ra thì có thể lấy khóa WEP.

Minh họa: E(A), E(B) là thông điệp đã được mã hóa; A, B là thông điệp cần gửi; C(K) là streamcipher, K là khóa WEP.

* E(A) = A xor C(K)
* E(B) = B xor C(K)
* E(A) xor E(B) = A xor B

🡺 Bằng cách làm như trên, chỉ cần bắt đủ gói tin, có thể lấy được khóa WEP nhờ các thuật toán phân tích.

* IV được thêm vào khóa WEP để tăng tính ngẫu nhiên cho khóa WEP, nên với 2 thông điệp giống nhau được gửi tại 2 thời điểm khác nhau sẽ có chuỗi mã hóa khác nhau, làm cho quá trình tấn công gặp khó khăn hơn.

### Sử dụng checksum (CRC-32)

* Để chống lại Substitution attack.
* Nếu không có CRC, người tấn công có thể thay đổi nội dung thông điệp truyền đi mà không cần biết khóa WEP.

Minh họa: giả sử kẻ tấn công biết rõ thông điệp có chứa một giá trị nào đó (ví dụ $1000.00), và người đó muốn sửa lại giá trị đó thành $9500.00, hoàn toàn làm được bằng cách:

* E(M) = C(K) xor “$1000.00”: thông điệp đã bị mã hóa, C(K) là streamcipher.
* Lấy E(M) xor “$1000.00” xor “$9500.00” thì thông điệp sẽ được đổi thành $9500.00.
* *(C(K) xor "$1000.00") xor "$1000.00" xor "$9500.00" = C(K) xor "$9500.00"*
* CRC sẽ tính toán ra một giá trị ứng với nội dung thông điệp được gửi, và giá trị này sẽ được tính lần nữa khi giải mã thông điệp để biết được thông điệp có bị thay đổi hay không.

## Ưu điểm

## Khuyết điểm

* Vẫn không chống lại được kiểu tấn công reused key attack mặc dù đã sử dụng IV. Vì IV chỉ có 24 bit nên khi khối lượng gói tin truyền đi nhiều (khoảng 5000 gói tin) thì IV bị lặp lại.
* Không có cơ chế thay đổi khóa tự động.
* Không thể tránh “weak IV”, “weak IV” là những IV có thể làm lộ nội dung thông điệp.
* Không ngăn được tấn công DoS (Denial of service).
* Không ngăn được việc thay đổi thông tin truyền đi dù đã sử dụng checksum.

## Tham khảo

* Nikita Borisov, Ian Goldberg, and David Wagner. [Intercepting Mobile Communications: The Insecurity of 802.11](http://www.seas.gwu.edu/%7Echeng/388/Readings/38.pdf). Proc. of ACM Mobicom, 2001.
* <http://en.wikipedia.org/wiki/Stream_cipher_attack>
* <http://en.wikipedia.org/wiki/Wired_Equivalent_Privacy>.
* Microsoft Corporation. IEEE 802.11 Wireless LAN Security with Microsoft Windows. 01/2007.
* <http://www.seas.gwu.edu/%7Echeng/388/LecNotes/WLANWEP.ppt>.

# WPA

## Giới thiệu

* WPA (Wi-Fi Protected Access), được ra đời vào tháng 4 năm 2003 bởi Wi-Fi Alliance nhằm khắc phục các điểm yếu của WEP.
* WPA được thiết kế để thay thế các mạng dùng WEP mà không cần nâng cấp phần cứng. Các nâng cấp miễn phí về phần mềm cho hầu hết các card mạng và điểm truy cập sử dụng WPA rất dễ dàng và có sẵn. Tuy nhiên, WPA không hỗ trợ các thiết bị cầm tay và máy quét mã vạch. Theo Wi-Fi Alliance, có khoảng 200 thiết bị đã được cấp chứng nhận tương thích WPA.
* WPA có sẵn 2 lựa chọn. Cả 2 lựa chọn này đều sử dụng giao thức TKIP, và sự khác biệt chỉ là khoá khởi tạo mã hoá lúc đầu.
  + WPA Enterprise (đòi hỏi một Radius Server) Dùng trong mạng doanh nghiệp. Nó sử dụng công nghệ 802.11x để xác thực người sử dụng thông qua một RADIUS server. Máy chủ xác thực và 802.1x cung cấp các khoá khởi tạo cho mỗi phiên làm việc.
  + WPA Personal (hay WPA-PSK (WPA-Pre Shared Key)) dùng trong các mạng gia đình và mạng văn phòng nhỏ. Khoá khởi tạo sẽ được sử dụng tại các thời điểm truy cập và thiết bị máy trạm. Mỗi người dùng phải nhập vào một passphrase (là một chuỗi password dùng để kết nối, giao dịch) để kết nối mạng.
* WPA dùng Temporal Key Intergrity Protocol (TKIP) để mã hoá và dùng 802.1X chứng thực với một trong các dạng của chuẩn Extensible Authentication Protocol (EAP) sẵn có hiện nay.
* WPA thay thế WEP ở các điểm sau: chứng thực, mã hóa, toàn vẹn thông tin.

## Chứng thực

Có 2 cách chứng thực trong WPA: Open system authentication và 802.1X

### Open system authentication

Đã trình bày ở phần WEP.

### 802.1X

WPA hỗ trợ 2 cấp hoạt động.

* WPA Enterprise là môi trường có hệ thống RADIUS và sử dụng chứng thực EAP.
* WPA Personal dành cho môi trường không có hệ thống RADIUS và sử dụng pre-shared key (khóa được cấp trước) để chứng thực

For 802.1X authentication using a RADIUS server, the PMK is mutually determined by the wireless client and the RADIUS server, which conveys the PMK to the wireless AP in the RADIUS Access-Accept message. After receiving the PMK, the wireless AP initiates the temporal key message exchange, which consists of the following:

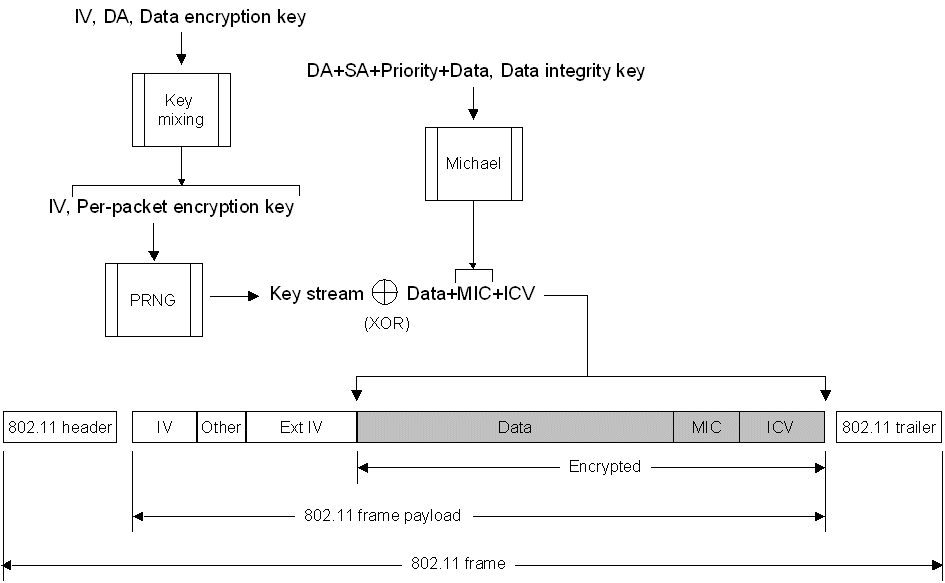
1. An EAPOL-Key message sent by the wireless AP that contains Nonce 1 and MAC 1. Because the temporal unicast keys are not yet determined, this message is sent as clear text and without message integrity protection. The wireless client now has all the elements needed to calculate the pairwise temporal keys.
2. An EAPOL-Key message sent by the wireless client that contains Nonce 2, MAC 2, and a MIC. Because the wireless client has calculated the pairwise temporal keys, it calculates a MIC using the derived EAPOL-Key integrity key. The wireless AP uses the Nonce 2 and MAC 2 values to derive the pairwise temporal keys and to validate the value of the MIC.
3. An EAPOL-Key message sent by the wireless AP that contains a MIC and a starting sequence number, indicating that the wireless AP is ready to start sending encrypted unicast and EAPOL-Key frames.
4. An EAPOL-Key message sent by the wireless client that contains a MIC and a starting sequence number, indicating that the wireless client is ready to start sending encrypted unicast and EAPOL-Key frames.

This set of messages exchanges the values needed to determine the pairwise temporal keys, verifies that each wireless peer has knowledge of the PMK (by verifying the value of the MIC), and indicates that each wireless peer is ready to begin encrypting and providing message integrity protection for subsequent unicast data frames and EAPOL-Key messages.

For multicast and broadcast traffic, the wireless AP derives a 128-bit group encryption key and a 128-bit group integrity key and sends these values to the wireless client using an EAPOL-Key message, encrypted with the EAPOL-Key encryption key and integrity-protected with the EAPOL-Key integrity key. The wireless client acknowledges the receipt of the EAPOL-Key message with an EAPOL-Key message.

## Mã hóa

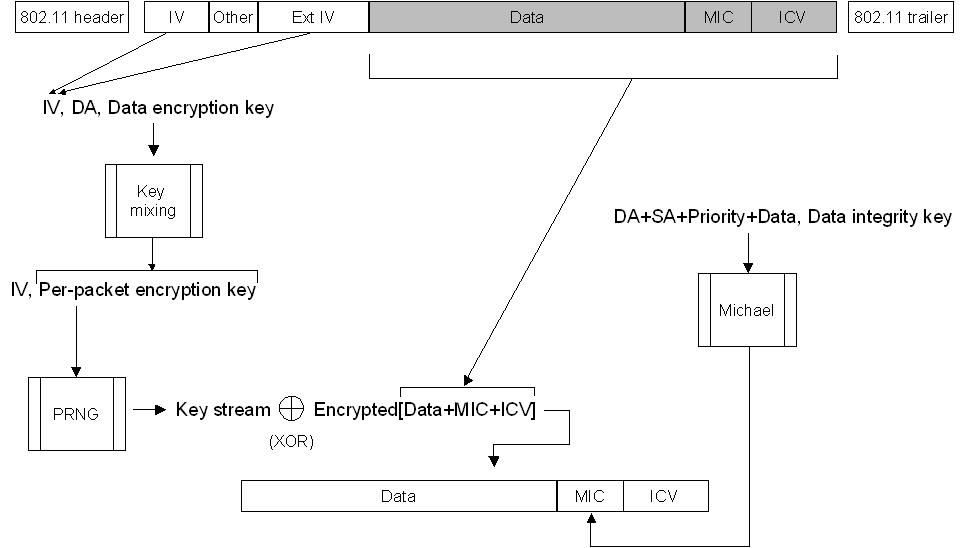
* WPA cần những giá trị sau để mã hóa và đảm bảo tính toàn vẹn của thông điệp truyền đi:
  + IV, bắt đầu từ 0 và tăng lên đối với những frame sau này.
  + Khóa mã hóa dữ liệu (dùng cho unicast traffic (kênh truyền giữa chính client với AP)) hoặc khóa mã hóa nhóm (dùng cho multicast traffic (nhiều kênh truyền) hoặc dùng cho broadcast).
  + Địa chỉ nơi nhận (DA, destination address) và địa chỉ nơi gửi (SA, source address) của frame.
  + Giá trị của trường Priority, có giá trị là 0 và được thay đổi lại cho những mục đích sau này.
  + Khóa toàn vẹn dữ liệu (dùng cho unicast traffic) hoặc khóa toàn vẹn nhóm (cho multicast hoăc broadcast traffic).
* Quá trình mã hóa cho gói dữ liệu unicast diễn ra theo trình tự sau:
  1. [IV, DA, khóa mã hóa dữ liệu] là đầu vào của hàm Key mixing, kết quả trả về là một khóa mã hóa cho từng gói dữ liệu (per-packet).
  2. [DA, SA, Priority, dữ liệu (chưa được mã hóa) và khóa toàn vẹn dữ liệu] là đầu vào của thuật toán Michael để tạo ra MIC (Message Integrity Check).
  3. ICV được tính từ CRC-32 checksum.
  4. [IV, khóa mã hóa dữ liệu] cho từng gói dữ liệu là đầu vào của thuật toán RC4 để tạo ra keystream, key stream có cùng kích thước với dữ liệu, MIC, và ICV.
  5. Keystream XOR với [dữ liệu, MIC, ICV] để tạo ra [dữ liệu, MIC, ICV] được mã hóa, nó là một phần của frame payload.
  6. Để tạo frame payload, IV, trường khác và IV mở rộng được thêm vào [dữ liệu, MIC, ICV] được mã hóa.



## Giải mã

Quá trình giải mã cho gói dữ liệu unicast diễn ra theo trình tự sau:

1. The IV value is extracted from the IV and Extended IV fields in the 802.11 frame payload and input along with the DA and data encryption key into the key mixing function, producing the per-packet encryption key.
2. The IV and the per-packet encryption key are input into the RC4 PRNG function to produce a key stream that is the same size as the encrypted data, MIC, and ICV.
3. The key stream is XORed with the encrypted data, MIC, and ICV to produce the unencrypted data, MIC, and ICV.
4. The ICV is calculated and compared to the value of the unencrypted ICV. If the ICV values do not match, the data is silently discarded.
5. The DA, SA, data, and the data integrity key are input into the Michael integrity algorithm to produce the MIC.
6. The calculated value of the MIC is compared to the value of the unencrypted MIC. If the MIC values do not match, the data is silently discarded. If the MIC values match, the data is passed to the upper networking layers for processing.



## Ưu điểm

* Không cần cài đặt phần cứng.
* WPA cũng mã hóa thông tin bằng RC4 nhưng chiều dài của khóa là 128 bit và IV có chiều dài là 48 bit.
* WPA sử dụng giao thức TKIP nhằm thay đổi khóa dùng Access Point và User một cách tự động trong quá trình trao đổi thông tin. Khóa sẽ thay đổi dựa trên người dùng, phiên trao đổi nhất thời và số lượng gói thông tin đã truyền.
* WPA sử dụng 802.1x/EAP để đảm bảo chứng thực lẫn nhau giữa Access Point và User nhằm chống lại tấn công kiểu man-in-middle.
* WPA sử dụng MIC (Michael Message Integrity Check) để tăng cường tính toàn vẹn của thông tin.

## Khuyết điểm

* Điểm yếu đầu tiên của WPA là nó vẫn không giải quyết được denial-of-service (DoS) attack. Kẻ phá hoại có thể làm nhiễu mạng WPA WiFi bằng cách gửi ít nhất 2 gói thông tin với một khóa sai (wrong encryption key) mỗi giây. Trong trường hợp đó, Access Point sẽ cho rằng một kẻ phá hoại đang tấn công mạng và Access Point sẽ cắt tất cả các nối kết trong vòng một phút để tránh hao tổn tài nguyên mạng. Do đó, sự tiếp diễn của thông tin không được phép sẽ làm xáo trộn hoạt động của mạng và ngăn cản sự nối kết của những người dùng được cho phép.
* WPA vẫn sử dụng thuật toán RC4, nó có thể dễ dàng bị bẻ vỡ bởi FMS attack, được đề nghị bởi những nhà nghiên cứu ở trường đại học Berkeley. Hệ thống mã hóa RC4 chứa đựng những khóa yếu (weak keys). Những khóa yếu này cho phép truy ra khóa encryption. Để có thể tìm ra khóa yếu của RC4, chỉ cần thu thập một số lượng đủ thông tin truyền trên kênh truyền không dây.
* WPA-PSK là một phiên bản yếu của WPA mà ở đó nó gặp vấn đề về quản lý password hoặc shared secret giữa nhiều người dùng. Khi một người trong nhóm (trong công ty) rời nhóm, một password/secret mới cần phải được thiết lập