Mục lục

[1. Các chuẩn mã hóa wifi 2](#_Toc530518880)

[Wired Equivalent Privacy (WEP) 2](#_Toc530518881)

[WiFi Protected Access (WPA) 3](#_Toc530518882)

[WiFi Protected Access II (WPA2) 3](#_Toc530518883)

[2. Các thuật toán mã hóa 4](#_Toc530518884)

[Mã hóa cổ điển 5](#_Toc530518885)

[Mã hóa một chiều 5](#_Toc530518886)

[Mã hóa đối xứng 6](#_Toc530518887)

[Mã hóa bất đối xứng 7](#_Toc530518888)

[Ứng dụng 8](#_Toc530518889)

[3. Các phương pháp tấn công 8](#_Toc530518890)

[MAC Spoofing: 8](#_Toc530518891)

[Denial of Service: 8](#_Toc530518892)

[Social Engineering: 9](#_Toc530518893)

[Encryption Cracking: 9](#_Toc530518894)

[Eavesdropping: 9](#_Toc530518895)

**Đề Tài: ĐIỀU TRA TẤN CÔNG WIRELESS**

# 1. Các chuẩn mã hóa wifi

## *Wired Equivalent Privacy (WEP)*

- Wired Equivalent Privacy (WEP) là thuật toán bảo mật WiFi được dùng nhiều nhất trên thế giới. Thực tế nó là thứ đầu tiên xuất hiện trong menu các chuẩn mã hóa của nhiều bộ định tuyến.

- WEP được phê chuẩn là phương thức bảo mật tiêu chuẩn dành cho WiFi vào tháng 9/1999. Phiên bản đầu tiên của WEP không hề mạnh, kể cả vào thời điểm nó được giới thiệu bởi việc chính phủ Mỹ cấm xuất khẩu nhiều công nghệ mã hóa khiến các nhà sản xuất chỉ bảo vệ thiết bị của họ với mã hóa 64 bit. Sau khi lệnh cấm được dỡ bỏ, chuẩn 128 bit được đưa vào sử dụng rộng rãi hơn. Thậm chí sau này kể cả khi mã hóa WEP 256 bit được giới thiệu, 128 bit vẫn là một trong những chuẩn được áp dụng nhiều nhất.

- Mặc dù các thuật toán được cải tiến và kích thước kí tự được tăng lên, qua thời gian nhiều lỗ hổng bảo mật được phát hiện trong chuẩn WEP khiến nó càng ngày càng dễ bị qua mặt khi mà sức mạnh của máy tính ngày càng được củng cố. Năm 2001, nhiều lổ hổng tiềm tàng đã bị phơi bày trên mạng Internet. Đến năm 2005, FBI công khai trình diễn khả năng bẻ khóa WEP chỉ trong một vài phút bằng phần mềm hoàn toàn miễn phí nhằm nâng cao nhận thức về sự nguy hiểm của WEP.

- Mặc dù nhiều nỗ lực cải tiến được tiến hành nhằm tăng cường hệ thống của WEP, chuẩn này vẫn đặt người dùng vào vị trí hết sức nguy hiểm và tất cả các hệ thống sử dụng WEP nên được nâng cấp hoặc thay thế. Tổ chức Liên minh WiFi chính thức cho WEP "về hưu" năm 2004.

## *WiFi Protected Access (WPA)*

- WiFi Protected Access là phương thức được Liên minh WiFi đưa ra để thay thế WEP trước những nhược điểm không thể khắc phục của chuẩn cũ. WPA được áp dụng chính thức vào năm 2003, một năm trước khi WEP bị loại bỏ. Phiên bản phổ biến nhất của WPA là WPA-PSK (Pre-Shared Key). Các kí tự được sử dụng bởi WPA là loại 256 bit, tân tiến hơn rất nhiều so với kí tự 64 bit và 128 bit có trong hệ thống WEP.

***-*** Một trong những thay đổi lớn lao được tích hợp vào WPA bao gồm khả năng kiểm tra tính toàn vẹn của gói tin (message integrity check) để xem liệu hacker có thu thập hay thay đổi gói tin chuyền qua lại giữa điểm truy cập và thiết bị dùng WiFi hay không. Ngoài ra còn có giao thức khóa toàn vẹn thời gian (Temporal Key Integrity Protocol – TKIP). TKIP sử dụng hệ thống kí tự cho từng gói, an toàn hơn rất nhiều so với kí tự tĩnh của WEP. Sau này, TKIP bị thay thế bởi Advanced Encryption Standard (AES).

- Tuy vậy điều này không có nghĩa là WPA đã hoàn hảo. TKIP, một bộ phận quan trọng của WPA, được thiết kế để có thể tung ra thông qua các bản cập nhật phần mềm lên thiết bị được trang bị WEP. Chính vì vậy nó vẫn phải sử dụng một số yếu tố có trong hệ thống WEP, vốn cũng có thể bị kẻ xấu khai thác.WPA, giống như WEP, cũng trải qua các cuộc trình diễn công khai để cho thấy những yếu điểm của mình trước một cuộc tấn công. Phương pháp qua mặt WPA không phải bằng cách tấn công trực tiếp vào thuật toán của nó mà là vào một hệ thống bổ trợ có tên WiFi Protected Setup (WPS), được thiết kế để có thể dễ dàng kết nối thiết bị tới các điểm truy cập.

## *WiFi Protected Access II (WPA2)*

- Đến năm 2006, WPA chính thức bị thay thế bởi WPA2. Một trong những cải tiến đáng chú ý nhất của WPA2 so với WPA là sự có mặt bắt buộc của AES và CCMP (Counter Cipher Mode with Block Chaining Message Authentication Code Protocol) nhằm thay thế cho TKIP. Tuy vậy, TKIP vẫn có mặt trong WPA2 để làm phương án dự phòng và duy trì khả năng tương tác với WPA.

-Hiện tại, lỗ hổng bảo mật chính của hệ thống WPA2 không thực sự lộ rõ. Kẻ tấn công phải có quyền truy cập vào mạng WiFi đã được bảo vệ trước khi có thể có trong tay bộ kí tự, sau đó mới có thể tiến hành tấn công các thiết bị khác trong cùng mạng. Như vậy, các lỗ hổng của WPA2 khá hạn chế và gần như chỉ gây ảnh hưởng đến các mạng quy mô lớn như của tập đoàn. Trong khi đó người dùng mạng tại nhà có thể yên tâm với chuẩn mới nhất này.

- Tuy nhiên không may là lỗ hổng lớn nhất trong bộ giáp của WPA vẫn còn tồn tại trong WPA2, đó là WPS. Mặc dù để thâm nhập được vào mạng lưới được bảo vệ bởi WPA/WPA2 bằng lỗ hổng trên cần tới 2-14 giờ hoạt động liên tục của một máy tính hiện đại, đây vẫn là một mối lo tiềm tàng. Vì thế tốt nhất WPS nên được tắt đi hoặc xóa bỏ hoàn toàn khỏi hệ thống thông qua các lần cập nhật firmware của điểm truy cập.

***\* Dưới đây là danh sách các chuẩn bảo mật dành cho WiFi, xếp theo khả năng bảo mật từ cao xuống thấp:***

- WPA2 + AES

- WPA + AES

- WPA + TKIP/AES (TKIP đóng vai trò là phương án dự phòng)

- WPA + TKIP

- WEP

- Mạng mở, không mã khóa

# 2. Các thuật toán mã hóa

- Thuật toán mã hóa là một thuật toán nhằm mã hóa thông tin của chúng ta, biến đổi thông tin từ dạng rõ sang dạng mờ, để ngăn cản việc đọc trộm nội dung của thông tin (Dù hacker có được thông tin đó cũng không hiểu nội dung chứa trong nó là gì).

- Thông thường các thuật toán sử dụng một hoặc nhiều key (Một chuỗi chìa khóa để mã hóa và giải mã thông tin) để mã hóa và giải mã (Ngoại trừ những thuật toán cổ điển). Bạn có thể coi key này như một cái password để có thể đọc được nội dung mã hóa. Người gửi sẽ dùng key mã hóa để mã hóa thông tin sang dạng mờ, và người nhận sẽ sử dụng key giải mã để giải mã thông tin sang dạng rõ. Chỉ những người nào có key giải mã mới có thể đọc được nội dung.

- Nhưng đôi khi "kẻ thứ ba" (hacker) không có key giải mã vẫn có thể đọc được thông tin, bằng cách phá vỡ thuật toán. Và có một nguyên tắc là bất kì thuật toán mã hóa nào cũng đều có thể bị phá vỡ. Do đó không có bất kì thuật toán mã hóa nào được coi là an toàn mãi mãi. Độ an toàn của thuật toán được dựa vào nguyên tắc:

+ Nếu chi phí để giải mã một khối lượng thông tin lớn hơn giá trị của khối lượng thông tin đó thì thuật toán đó được tạm coi là an toàn. (Không ai lại đi bỏ ra 50 năm để giải mã một thông tin mà chỉ mang lại cho anh ta 1000 đô).

+ Nếu thời gian để phá vỡ một thuật toán là quá lớn (giả sử lớn hơn 100 năm, 1000 năm) thì thuật toán được tạm coi là an toàn.

- Phân loại các thuật toán mã hóa:

* Mã hóa cổ điển
* Mã hóa một chiều
* Mã hóa đối xứng
* Mã hóa bất đối xứng

## *Mã hóa cổ điển*

- Đây là phương pháp mã hóa đầu tiên, và cố xưa nhất, và hiện nay rất ít được dùng đến so với các phương pháp khác. Ý tưởng của phương pháp này rất đơn giản, bên A mã hóa thông tin bằng thuật toán mã hóa cổ điển, và bên B giải mã thông tin, dựa vào thuật toán của bên A, mà không dùng đến bất kì key nào. Do đó, độ an toàn của thuật toán sẽ chỉ dựa vào độ bí mật của thuật toán, vì chỉ cần ta biết được thuật toán mã hóa, ta sẽ có thể giải mã được thông tin.

## *Mã hóa một chiều*

- Đôi khi ta chỉ cần mã hóa thông tin chứ không cần giải mã thông tin, khi đó ta sẽ dùng đến phương pháp mã hóa một chiều (Chỉ có thể mã hóa chứ không thể giải mã). Thông thường phương pháp mã hóa một chiều sử dụng một hàm băm (hash function) để biến một chuỗi thông tin thành một chuỗi hash có độ dài nhất định. Ta không có bất kì cách nào để khôi phục (hay giải mã) chuỗi hash về lại chuỗi thông tin ban đầu.

- Đặc điểm của hash function là khi thực hiên băm hai chuỗi dữ liệu như nhau, dù trong hoàn cảnh nào thì nó cũng cùng cho ra một chuỗi hash duy nhất có độ dài nhất định và thường nhỏ hơn rất nhiều so với chuỗi gốc, và hai chuỗi thông tin bất kì dù khác nhau rất ít cũng sẽ cho ra chuỗi hash khác nhau rất nhiều. Do đó hash function thường được sử dụng để kiểm tra tính toàn vẹn của dữ liệu.

- Ngoài ra có một ứng dụng mà có thể bạn thường thấy, đó là để lưu giữ mật khẩu. Vì mật khẩu là một thứ cực kì quan trọng, do đó ta không nên lưu mật khẩu của người dùng dưới dạng rõ, vì như vậy nếu bị hacker tấn công, lấy được CSDL thì hacker có thể biết được mật khẩu của người dùng. Do đó, mật khẩu của người dùng nên được lưu dưới dạng chuỗi hash, và đối với server thì chuỗi hash đó chỉnh là “mật khẩu” đăng nhập (lúc đăng nhập thì mật khẩu mà người dùng nhập cũng được mã hóa thành chuỗi hash và so sánh với chuỗi hash trong CSDL của server). Dù hacker có lấy được CSDL thì cũng không tài nào có thể giải mã được chuỗi hash để tìm ra mật khẩu của người dùng.

- Thuật toán mã hóa một chiều (hàm băm) mà ta thường gặp nhất là MD5 và SHA.

## *Mã hóa đối xứng*

- Mã hóa đối xứng (Hay còn gọi là mã hóa khóa bí mật) là phương pháp mã hóa mà key mã hóa và key giải mã là như nhau (Sử dụng cùng một secret key để mã hóa và giải mã). Đây là phương pháp thông dụng nhất hiện nay dùng để mã hóa dữ liệu truyền nhận giữa hai bên. Vì chỉ cần có secret key là có thể giải mã được, nên bên gửi và bên nhận cần làm một cách nào đó để cùng thống nhất về secret key.

- Để thực hiện mã hóa thông tin giữa hai bên thì:

* Đầu tiên bên gửi và bên nhận bằng cách nào đó sẽ phải thóa thuận secret key (khóa bí mật) được dùng để mã hóa và giải mã. Vì chỉ cần biết được secret key này thì bên thứ ba có thể giải mã được thông tin, nên thông tin này cần được bí mật truyền đi (bảo vệ theo một cách nào đó).
* Sau đó bên gửi sẽ dùng một thuật toán mã hóa với secret key tương ứng để mã hóa dữ liệu sắp được truyền đi. Khi bên nhận nhận được sẽ dùng chính secret key đó để giải mã dữ liệu.

- Vấn đề lớn nhất của phương pháp mã hóa đối xứng là làm sao để “thỏa thuận” secret key giữa bên gửi và bên nhận, vì nếu truyền secret key từ bên gửi sang bên nhận mà không dùng một phương pháp bảo vệ nào thì bên thứ ba cũng có thể dễ dàng lấy được secret key này.

- Các thuật toán mã hóa đối xứng thường gặp: DES, AES…

## *Mã hóa bất đối xứng*

- Mã hóa bất đối xứng (Hay còn gọi là mã hóa khóa công khai) là phương pháp mã hóa mà key mã hóa (lúc này gọi là public key – khóa công khai) và key giải mã (lúc này gọi là private key – khóa bí mật) khác nhau. Nghĩa là key ta sử dụng để mã hóa dữ liệu sẽ khác với key ta dùng để giải mã dữ liệu. Tất cả mọi người đều có thể biết được public key (kể cả hacker), và có thể dùng public key này để mã hóa thông tin. Nhưng chỉ có người nhận mới nắm giữ private key, nên chỉ có người nhận mới có thể giải mã được thông tin.

- Để thực hiện mã hóa bất đối xứng thì:

* Bên nhận sẽ tạo ra một gặp khóa (public key và private key). Bên nhận sẽ dữ lại private key và truyền cho bên gửi public key. Vì public key này là công khai nên có thể truyền tự do mà không cần bảo mật.
* Bên gửi trước khi gửi dữ liệu sẽ mã hóa dữ liệu bằng thuật toán mã hóa bất đối xứng với key là public key từ bên nhận.
* Bên nhận sẽ giải mã dữ liệu nhận được bằng thuật toán được sử dụng ở bên gửi, với key giải mã là private key.

- Điểm yếu lớn nhất của mã hóa bất đối xứng là tốc độ mã hóa và giải mã rất chậm so với mã hóa đối xứng, nếu dùng mã hóa bất đối xứng để mã hóa dữ liệu truyền – nhận giữa hai bên thì sẽ tốn rất nhiều chi phí.

- Do đó, ứng dụng chỉnh của mã hóa bất đối xứng là dùng để bảo mật secret key cho mã hóa đối xứng: Ta sẽ dùng phương pháp mã hóa bất đối xứng để truyền secret key của bên gửi cho bên nhận. Và hai bên sẽ dùng secret key này để trao đổi thông tin bằng phương pháp mã hóa đối xứng.

- Thuật toán mã hóa bất đối xứng thường thấy: RSA.

## *Ứng dụng*

- Khi cần bảo mật thông tin truyền đi giữa các ứng dụng chat, hoặc các ứng dụng có truyền nhận thông tin bí mật giữa client-server, thì ta có thể sử dụng kết hợp phương pháp mã hóa bất đối xứng và phương pháp mã hóa đối xứng để đảm bảo dữ liệu đó sẽ được bảo mật.

- Ta sẽ thực hiện bằng cách dùng phương pháp mã hóa bất đối xứng để truyền secret key từ bên gửi cho bên nhận, và dùng key này để mã hóa, giải mã thông tin.

- Ta có thể thực hiện theo quy trình sau:

* Bên nhận sinh ra cặp khóa public key và private key (dùng để mã hóa secret key của bên gửi) và gửi cho bên gửi một cách công khai, không cần bảo mật.
* Bên gửi sinh ra một secret key (dùng để mã hóa dữ liệu), mã hóa secret key này bằng thuật toán mã hóa bất đối xứng với key mã hóa là public key của bên nhận, sau đó truyền cho bên nhận.
* Bên nhận nhận dữ liệu và giải mã nó bằng thuật toán mã hóa bất đối xứng được sử dụng ở bên gửi, với key giải mã là private key. Khi đó sẽ ra được secret key dùng để mã hóa dữ liệu.
* Sau đó mỗi khi cần truyền dữ liệu thì bên gửi sẽ mã hóa dữ liệu đó bằng secret key trước khi gửi, và bên nhận cũng sẽ giải mã dữ liệu bằng secret key đó.

# 3. Các phương pháp tấn công

## *MAC Spoofing:*

+ Giả mạo địa chỉ MAC là điều cực kỳ dễ dàng để làm. Bởi vì điều này, sử dụng MAC để kiểm soát thiết bị là một việc không an toàn.

+ Tuy nhiên nó có thể được sử dụng kết hợp với các biện pháp bảo mật khác để xây dựng một kiến ​​trúc mạng an toàn hơn

## *Denial of Service:*

+ Thuật ngữ này bao gồm một số kĩ thuật khác nhau. Các cuộc tấn công DoS có thể xảy ra trên các lớp khác nhau.

+ Các cuộc tấn công lớp 1 được gọi là các cuộc tấn công gây nhiễu RF, và có thể là cả hai chủ ý và không chủ ý (chẳng hạn như lò vi sóng hoặc điện thoại không dây gây nhiễu sóng.

+ Các cuộc tấn công lớp 2 có thể xảy ra theo một số cách khác nhau. Ví dụ, kẻ tấn công có thể tràn ngập AP với các yêu cầu liên kết và phân ly giả mạo.

+ Có những giải pháp được sử dụng để phát hiện các loại tấn công này và cho phép bạn thực hiện các bước để ngăn chặn chúng.

## *Social Engineering:*

+ Trái ngược việc cần kĩ thuật cao , hầu hết các hack thành công đều không cần tool, không cần phần mềm độc hại mà vẫn có thể hack thông qua những thu thập từ những mạng xã hội hoặc thực tiễn tiếp xúc.

+ Đây là một kỹ thuật được sử dụng để thao túng mọi người cung cấp thông tin như mật khẩu máy tính hoặc thông tin sẽ giúp kẻ tấn công thu hẹp mật khẩu tiềm năng. Cách tốt nhất để đối phó với mối đe doạ này là đảm bảo rằng mọi người được giáo dục về các quy trình bảo mật như thay đổi mật khẩu thường xuyên và không chia sẻ thông tin cá nhân.

## *Encryption Cracking:*

+ Đây là nơi mà kẻ tấn công cố gắng để crack mã hóa trên mạng. Các mạng WEP dễ bị tấn công nhất, có thể dễ dàng bị nứt trong vòng 5 phút.

+ Điều quan trọng là đảm bảo rằng bạn sử dụng mã hóa an toàn nhất mà bạn có thể, và tránh sử dụng WEP nếu có thể.

## *Eavesdropping:*

+ Đây là nơi mạng không dây bị giám sát. Có hai loại nghe lén.

+ Đầu tiên, nghe trộm bình thường, hoặc đôi khi được gọi là khám phá WLAN, là nơi một máy khách không dây tích cực quét các điểm truy cập không dây.

+ Loại thứ hai, nghe trộm độc hại, là loại bất hợp pháp. Đây là nơi ai đó cố gắng lắng nghe dữ liệu được chuyển giữa khách hàng và điểm truy cập. Vì thế, yêu cầu đầu tien và cần thiêt là thông tin bạn cần phải được mã hoá trên đường truyền.