BẢO MẬT MẠNG LOCAL AREA NETWORK DỰA TRÊN TIÊU CHUẨN 802.1X

Nguyễn Bá Nhiệm *

Tóm tắt

Ngày nay các ứng dụng, dịch vụ trên các hệ thống mạng gia tăng với nhiều sự phức tạp và rủi ro cho người quản trị hệ thống mạng. Do đó, chúng ta cần thực hiện, triển khai các biện pháp bảo mật tốt hơn, tiêu chuẩn 802.1X mà bài viết muốn giới thiệu, một tiêu chuẩn chứng thực người dùng để giải quyết vấn đề bảo mật trên cơ sở hạ tầng mạng LAN và WLAN (Wireless LAN). Tiêu chuẩn 802.1X được định nghĩa bởi IEEE, hỗ trợ việc điều khiển truy cập phương tiện truyền dẫn, khả năng cho phép hay cấm sự kết nối mạng, điều khiển truy cập VLAN và triển khai chính sách lưu lượng truyền dựa trên sự nhận dạng tài khoản người dùng hoặc xác định thiết bị. Chuẩn 802.1X thực hiện theo giao thức chứng thực EAP (Extensible Authentication Protocol) được định dạng theo khung Ethernet trên mạng LAN với tên gọi EAPOL (Extensible Authentication Protocol Over LAN) đồng thời hỗ trợ nhiều phương pháp chứng thực khác nhau như PPP, MD5, TLS, CHAP và RADIUS có thể triển khai trên hệ thống mạng LAN và cả WLAN. Bài viết trình bày chi tiết tiêu chuẩn 802.1X, EAP và EAPOL để cung cấp thêm kiến thức giải quyết các vấn đề bảo mật cho việc thiết kế và triển khai một hệ thống mạng.

Từ khóa: tiêu chuẩn 802.1x, EAP, EAPoL, giao thức chứng thực mở rộng, gia tăng bảo mật mạng LAN với tiêu chuẩn 802.1x.

Abstract

Today, the increasing of applications and services on the network system has brought network administrators plenty of difficulties and risks. Therefore, the designing network security should be effectively implemented by network administrators. One of security standards is 802.1X which is a user authentication standard to address security issues on LAN and WLAN (Wireless LAN) infrastructure.The 802.1X standard, is defined by IEEE, supports access control for transmission medium, the ability to allow or prohibit network connection, VLAN access control and implementation of transmission policies based on identity user accounts or devices determined. The 802.1X standard is done by Extensible Authentication Protocol (EAP) and has the Ethernet frame format on the LAN called Extensible Authentication Protocol Over LAN (EAPOL), and supports various authentication methods such as PPP, MD5, TLS , CHAP and RADIUS which can be deployed on a LAN system, even WLAN. The paper will discuss in detail about the 802.1X standard, EAP and EAPOL to provide more knowledge to solve security issues for the design and implementation of a network system.

Keywords: The standard 802.1x, EAP, EAPOL, Extensible Authentication Protocol, The enhanced security of LAN with 802.1x standard.

1. Giới thiệu 802.1X, EAP và EAPOL

IEEE 802.1X là một chuẩn điều khiển truy cập mạng dựa trên cổng (port), nghĩa là sự chứng thực của tầng 2 trên mô hình OSI. Nó được triển khai bất kỳ của một cổng trên mạng Ethernet (IEEE 802). Phần lớn các việc triển khai truy cập mạng dựa trên cổng là truy cập đến các mạng không dây (WLAN) và truy cập các mạng có dây (LAN) dựa trên một nhóm thiết bị Switch. Mặc nhiên các cổng ở trạng thái "đóng", nghĩa là sự truy cập không được cho phép luồng dữ liệu đi ngang qua, ngay cả sự kết nối vật lý được thiết lập. Sau khi người dùng (user) hoặc thiết bị truy cập yêu cầu chứng thực bản thân nó, khi đó trạng thái cổng được thay đổi "mở", nghĩa là luồng dữ liệu thông thường được phép đi ngang qua cổng. IEEE 802.1X hạn chế các máy trạm (clients) không được xác thực kết nối đến hạ tầng mạng LAN hoặc WLAN dùng bởi sự điều khiển truy cập dựa trên máy chủ (Server) và máy trạm với giao thức chứng thực.

Chuẩn 802.1X định nghĩa ba thành phần chính tham gia trong mô hình điều khiển truy cập như sau:

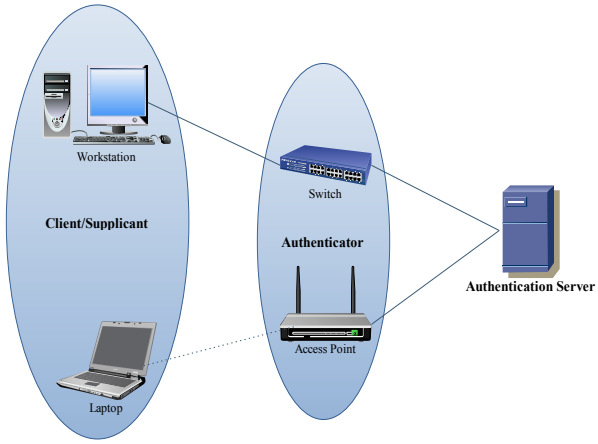
* *Thạc sĩ, Khoa Kỹ thuật & Công nghệ - Trường Đại học Trà Vinh*

- Client hoặc Supplicant: Thiết bị cần truy cập hay yêu cầu truy cập hạ tầng mạng LAN/WLAN hoặc các dịch vụ thiết bị thuộc tầng 2. Các thiết bị được hỗ trợ phần mềm 802.1X phục vụ cho máy trạm để nó có thể trả lời yêu cầu từ thiết bị thuộc tầng 2.

- Authenticator: Nhiệm vụ của thiết bị này chuyển tiếp thông tin giữa máy chủ chứng thực và máy trạm (Supplicant). Authenticator là thiết bị mạng thuộc tầng 2 hoạt động như một điểm trung gian hoặc proxy giữa máy trạm và máy chủ chứng thực bởi thực hiện yêu cầu xác nhận thông tin từ máy trạm, kiểm tra thông tin đó với máy chủ chứng thực và thực hiện hồi đáp lại của máy chủ chứng thực đến máy trạm.

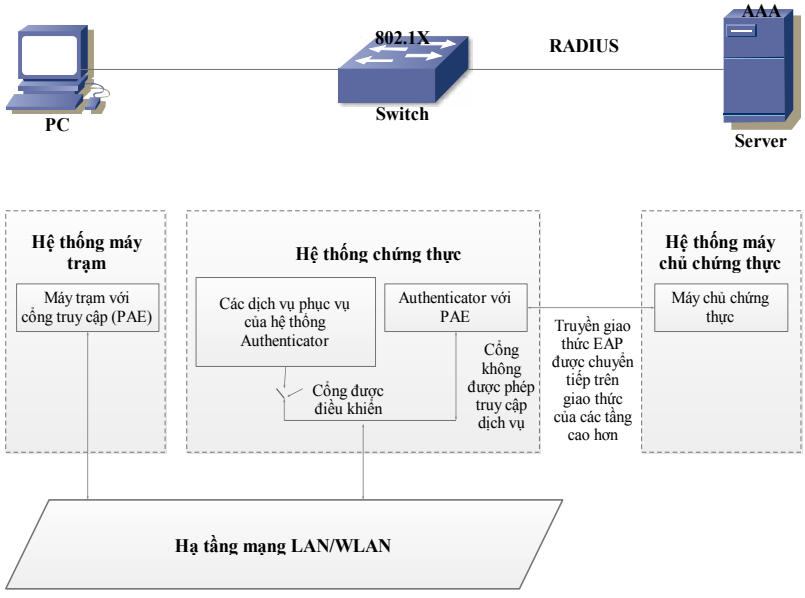
- Authentication Server: Thiết bị đảm nhận việc thực hiện chứng thực và cho phép Authenticator phục vụ hay từ chối phục vụ cho máy trạm. Máy chủ chứng thực phê chuẩn thông tin nhận dạng của máy trạm và thông báo cho thiết bị mạng thuộc tầng 2 đang hoạt động như Authenticator chuyển tiếp thông tin đến máy trạm.

Trong Hình 1 đưa ra mô hình mạng dựa trên các sự kết nối khác nhau.



Hình 1. Sự kết nối triển khai trên các thiết bị sử dụng chuẩn 802.1X

Các thành phần của Hình 2 cung cấp khái niệm chung về kiến trúc của chuẩn 802.1X và đưa ra Supplicant, Authenticator, Authentication Server trong mạng LAN hoặc WLAN dùng chuẩn 802.1X trong đó nó yêu cầu mỗi cổng trên Authenticator là cổng điều khiển cho phép hay không cho phép luồng dữ liệu đi qua.



Hình 2. Sơ đồ kiến trúc của chuẩn 802.1X

PAE (Port Access Entity) trình bày trong Hình 2 dùng cho các thiết bị mạng thực hiện thuật toán của chuẩn 802.1X và hoạt động giao thức. Một cổng là một điểm độc lập kết nối đến cơ sở hạ tầng mạng LAN. Trong trường hợp mạng LAN, một Switch quản lý các cổng logic. Mỗi cổng logic đó giao tiếp với một cổng của máy trạm.

RADIUS (remote access dial in user service) một chuẩn cung cấp các dịch vụ Authentication, Authorization, Accounting (AAA) cho hệ thống mạng. Mặc dù giao thức RADIUS hỗ trợ là tùy chọn trong IEEE 802.1X. Nhiều Authenticator sử dụng chuẩn 802.1X đóng vai trò như các máy trạm RADIUS.

EAP (Extensible Authentication Protocol) là một giao thức chính được sử dụng kiểm tra thông tin chứng thực giữa máy trạm và máy chủ chứng thực.

IEEE 802.1X định nghĩa sự đóng khung của EAP dựa trên IEEE 802 và được biết đến như EAP sử dụng mạng LAN (EAP over LANs hay EAPOL). EAPOL đã thiết kế cho mạng Ethernet nhưng đã được phát triển thêm để phù hợp cho việc triển khai các mô hình mạng khác nhau như mạng Wireless, mạng FDDI (Fiber Distribution Data Interface).

EAP là một giao thức chứng thực, không những chỉ định bắt buộc sự chứng thực trong hệ thống, nó còn cung cấp vài chức năng chung và lựa chọn các phương pháp chứng thực gọi là các phương pháp EAP (EAP methods). Các phương pháp EAP hỗ trợ nhiều loại chứng thực khác nhau như thẻ bài (token card), chứng nhận (certificates), mật khẩu (passwords) và sự chứng thực khóa công cộng (public key authentication).

Bài viết trình bày hai giao thức EAP và EAPOL để hiểu tốt hơn về chúng trước khi chúng ta triển khai chúng trong hệ thống mạng thực tế.

2. Giao thức chứng thực mở rộng (Extensible Authentication Protocol -EAP)

EAP là một nền tảng sự chứng thực cho các thiết bị trong hệ thống mạng mà nó hỗ trợ nhiều phương pháp chứng thực. Về cơ bản, EAP cho phép hai thực thể trong hệ thống mạng trao đổi thông tin được chỉ định phương pháp chứng thực, các thực thể đó muốn sử dụng. Nội dung của sự chứng thực đó chỉ định bởi các phương pháp không được định nghĩa trong EAP.

Đây là một giao thức đem lại nhiều thuận lợi được đưa ra kiến trúc EAP và mang tính chất mềm dẻo. Authenticator không cần cập nhật để hỗ trợ các phương pháp chứng thực khác nhau hay các phương pháp chứng thực mới chỉ máy trạm (client/supplicant) và máy chủ chứng thực có thể thực hiện một vài hay tất cả các phương pháp chứng thực.

Ngày nay, có nhiều phương pháp chứng thực hoặc các phương pháp chứng thực đang sử dụng trong thực tế, trong số các phương pháp được định nghĩa của IETF RFCs như EAP-MD5, EAP-OTP, EAP-GTC, EAP-TLS và ngoài ra còn các phương pháp khác do các nhà sản xuất thiết bị chỉ định như PEAP, LEAP, EAP-TTLS.

EAP chỉ định bốn thông điệp truyền đi trên mạng:

- **Request (0x01):** Được dùng để gửi các thông điệp từ Authenticator đến máy trạm (Supplicant).

- **Response (0x02):** Được dùng để gửi các thông điệp từ máy trạm đến Authenticator.

- **Success (0x03):** Được gửi bởi Authenticator chỉ định sự truy cập được chấp thuận.

- **Failure (0x04):** Được gửi bởi Authenticator chỉ định sự truy cập bị từ chối.

Hình 3 minh họa định dạng thông điệp EAP và liệt kê, mô tả các thành phần thông điệp.

Code	Identifier	Length	Data

Hình 3. Định dạng thông điệp EAP

- **Code:** Trường Code chiếm một byte chỉ ra loại thông điệp (Request, Response, Success, Failure).

- **Identifier:** Trường Identifier chiếm một byte chứa đựng một số nguyên dương dùng để kiểm tra trùng khớp các thông điệp request với các thông điệp response. Mỗi thông điệp request mới sử dụng một số identifier mới.

- **Length:** Hai byte cho trường Length chỉ ra tổng số byte trong toàn bộ gói tin (packet).

- **Data:** Giá trị của biến Length (bao gồm byte 0) của trường Data định nghĩa cách làm thế nào để trường Data thông dịch dữ liệu.

Định dạng thông điệp EAP trình bày trong Hình 3 được sử dụng để gửi đi.

- EAP request
- EAP response
- EAP success
- EAP failure

Thêm một trường nữa được giới thiệu là trường Type thể hiện trong Hình 4. Trường này dùng một byte để định nghĩa loại thông điệp EAP request hoặc EAP response. Chỉ một trường Type được sử dụng trong mỗi gói tin và Type hồi đáp trùng khớp với yêu cầu.

Code	Identifier	Length	Type	Request/Response Data

Hình 4. Thông điệp Request/Response EAP

Các thông điệp EAP Success và EAP Failure thể hiện trong trường Data là các byte 0 và cấu trúc duy trì trong Hình 4. Trước khi bắt đầu thực hiện, các thông điệp EAP Request và EAP Response được chia nhỏ ra dùng trong trường EAP Type. Có vài loại EAP chung sau đây:

- Identity (1)
- Notification (2)
- NAK (3)
- MD5-Challenge (4)
- One-Time Password (OTP) (5)
- Generic Token Card (6)
- LEAP (17)
- EAP-TTLS (21)
- PEAP (25)
- EAP-FAST (43)

Phần quan trọng đã định nghĩa trước trong trường Type là Identity *(Type = 1)* bởi điều này sử dụng như một phần việc phân tích thông điệp EAP:

- **EAP-Request/Identity** *(Code = 1, Type = 1):* gửi bởi Authenticator đến một Supplicant mới.

- **EAP-Response/Identity** *(Code = 2, Type = 1):* hồi đáp đến EAP-Resquest/Identity, Supplicant phản hồi với thông điệp này chứa đựng tài khoản người dùng (username) hoặc vài thông tin xác nhận khác mà sẽ được hiểu bởi máy chủ chứng thực.

Để tìm hiểu chi tiết các loại EAP khác, vui lòng tham khảo tài liệu EAP RFC (RFC 2284).

3. Giao thức chứng thực mở rộng cho mạng LAN (Extensible Authentication Protocol Over LAN - EAPOL)

EAP RFC không chỉ rõ làm thế nào các thông điệp trao đổi được với nhau. Vậy để trao đổi các thông điệp EAP, chúng ta cần tìm hiểu cách trao đổi và định dạng của chúng. Để giải thích vấn đề này, IEEE 802.1X đã định nghĩa một giao thức gọi là EAPOL (EAP over LAN) để giúp hiểu các thông điệp EAP trao đổi giữa máy trạm (Supplicant) và Authenticator. EAPOL được thiết kế trước tiên cho Ethernet nhưng mở rộng phù hợp cho các chuẩn mạng khác nhau.

Hình 5 mô tả định dạng khung EAPOL

Ethernet MAC Header	Protocol Version	Packet Type	Paket Body Length	Packet Body

Hình 5. Định dạng khung EAPOL

Có năm loại thông điệp của EAPOL như sau:

- **EAP-Packet (0):** chứa đựng khung EAP đã định dạng

- **EAP-Start (1):** Một máy trạm (Supplicant) có thể gửi một khung EAP-Start thay vì chờ đợi sự thách thức từ Authenticator (EAP-Packet [EAP-Identity/Resquest]).

- **EAP-Logoff (2):** Dùng để trả về trạng thái của cổng không được phép truy cập khi máy trạm đã kết thúc sử dụng mạng.

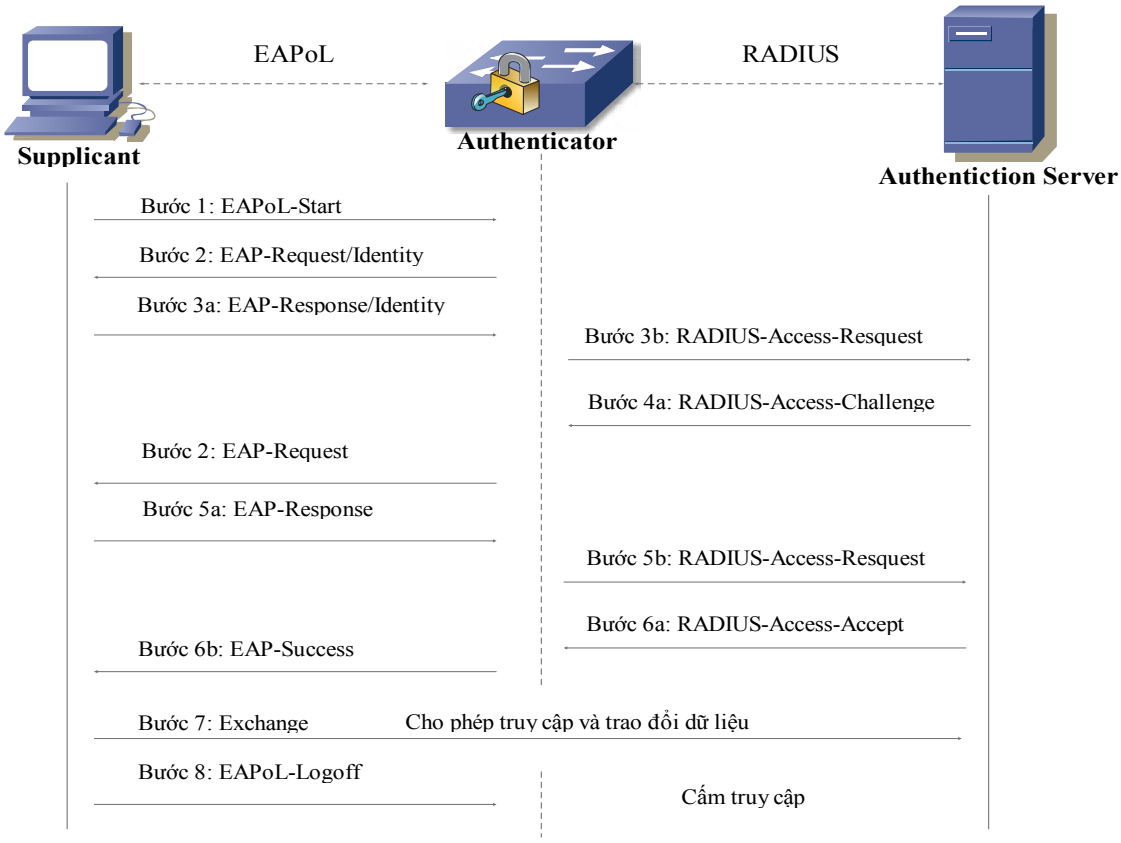
- **EAP-Key (3):** Dùng trao đổi thông tin khóa bảo mật.

- **EAP-Encapsulatated-ASF-Alert (4):** Cung cấp phương pháp cho phép ASF (Alert Standards Forum) chú ý chuyển tiếp qua cổng mà nó ở trạng thái không được phép truy cập.

4. Sự trao đổi thông điệp trong 802.1X

Chuẩn 802.1X gồm ba thực thể tham gia hoạt động trong hệ thống mạng: máy trạm (Client/Supplicant), Authenticator và máy chủ chứng thực (Authentication Server). Các thông điệp trao đổi với nhau trong số ba thực thể trên. Chuẩn 802.1X sử dụng EAP hoặc cụ thể hơn EAPOL trao đổi các thông điệp đó giữa Supplicant và Authenticator, giữa Authenticator và Authentication Server sử dụng giao thức RADIUS bởi định dạng EAP trong RADIUS. Có thể tham khảo thêm về tài liệu EAP over RADIUS.

Hình 6 mô tả đặc tính sự trao đổi thông điệp EAPOL/802.1X.



Hình 6. Trao đổi thông điệp EAPOL/802.1X

Mô tả quá trình hoạt động 802.1X như sau:

- **Bước 1:** Authenticator gửi thông điệp nhận dạng của EAP-Request đầu tiên đến Supplicant để hỏi sự nhận dạng của Supplicant. Supplicant cũng có thể bắt đầu quá trình này nếu nó được yêu cầu bằng cách gửi thông điệp EAPOL-Start.

- **Bước 2:** Nếu Supplicant gửi thông điệp EAP-Start, Authenticator yêu cầu sự nhận dạng của Supplicant bằng cách gửi thông điệp EAP-Request/ Identity.

- **Bước 3:** Trong sự hồi đáp lại, máy trạm gửi thông tin của nó trong khung EAP-Response/Identity. Authenticator giải mã thông tin từ khung EAPOL và chuyển thông tin EAP trong khung đến máy chủ chứng thực bằng giao thức RADIUS như RADIUS-Access- Request.

- **Bước 4:** Máy chủ RADIUS thương lượng với Supplicant bằng cách gửi RADIUS-Access-Challenge đến Authenticator, tại đây Authenticator đóng gói thông tin EAP trong khung EAPOL và chuyển nó đến Supplicant bằng EAP-Request.

- **Bước 5:** Sự hồi đáp EAP-Request, Supplicant gửi lại EAP-Response đến Authenticator, tại đây Authenticator giải mã thông tin EAP và gửi đến máy chủ chứng thực bằng RADIUS-Access-Resquest.

- **Bước 6:** Có vài sự trao đổi của EAP-Response/ RADIUS-Access-Request và RADIUS-Access-Challenge/ EAP-Request trước khi kết thúc máy chủ RADIUS gửi RADIUS-Access-Accept có nghĩa là người dùng đã được chứng thực. Khi sự hồi đáp được nhận bởi Authenticator, Authenticator giải mã thông tin EAP và gửi nó đến Supplicant bằng EAP-Success. Tại đây, cổng được phép truy cập và Supplicant đã được phép giao tiếp.

- **Bước 7:** Tại thời điểm này, Supplicant có thể bắt đầu trao đổi dữ liệu.

- **Bước 8:** Sau khi trao đổi dữ liệu kết thúc và Supplicant ngừng làm việc trên cổng truy cập, nó gửi EAP-Logoff đến Authenticator để thông báo rằng nó ngừng làm việc trên cổng và trả lại trạng thái cấm hoặc trạng thái không được phép truy cập.

5. Các loại EAP

Phần trước đã giải thích khung EAP-Resquest/ Response có một trường gọi là Type. Trường này có nhiều giá trị khác nhau, giúp trong việc quyết định phương pháp chứng thực EAP nào được sử dụng sau khi sự thương lượng giữa Supplicant và máy chủ chứng thực.

Có một số loại chứng thực EAP khác nhau đang được sử dụng như:

- **EAP- MD5:** Thách thức của EAP- MD5 (Message Digest) là một loại chứng thực EAP được định nghĩa trong RFC 3748. Nó đưa ra phương pháp bảo mật kém, do vậy không được khuyến khích sử dụng bởi vì có thể cho phép mật khẩu của người dùng dễ bị phát hiện, bởi vì MD5 dùng thuật toán băm (Hash) kém bảo mật nếu dùng phương pháp tấn công Dictionary attack. Trong loại chứng thực EAP này, chỉ có chứng thực một chiều; không có sự chứng thực lẫn nhau giữa EAP yêu cầu và EAP máy chủ. Bởi vì nó cung cấp sự chứng thực chỉ một bên EAP yêu cầu đến EAP máy chủ và không cung cấp sự chứng thực máy chủ EAP, phương pháp chứng thực EAP này cũng dễ bị tấn công theo phương pháp tấn công man-in-the-middle.

- **EAP:** LEAP (Lightweight Extensible Authentication Protocol) là loại chứng thực EAP được phát triển bởi Cisco System. LEAP sử dụng chính trong các mạng WLAN của Cisco. Giao thức này được phân phối qua Cisco Certified Extension (CCX) như một phần của thiết lập 802.1X và gia tăng sự bảo mật cho phương pháp bảo mật WEP (Wire Equivalent Privacy) trong mạng Wireless. LEAP mã hóa dữ liệu truyền đi dùng phương pháp phát sinh động các khóa bảo mật của WEP và cũng hỗ trợ sự chứng thực lẫn nhau. Mặc dù LEAP hỗ trợ sự chứng thực tương tác lẫn nhau, nhưng các thông tin của người dùng vẫn có thể dễ dàng bị lấy cắp. Do đó để gia tăng khả năng bảo mật cho LEAP, chúng ta thiết lập mật khẩu phức tạp cho người dùng.

- **PEAP:** PEAP (Protected Extensible Authentication Protocol) được tham gia phát triển bởi Cisco System, Microsoft, và RSA Security. Phương pháp chứng thực EAP này cho phép vận chuyển an toàn dữ liệu chứng thực, do đó phương pháp này cung cấp bảo mật rất tốt. Đây là phương pháp phức tạp bởi tạo ra một con đường riêng biệt giữa các máy trạm PEAP và một máy chủ chứng thực.Trong PEAP, chỉ một bên máy chủ tạo ra chứng nhận PKI (Public Key Infrastructure) được yêu cầu tạo ra một con đường bảo mật riêng TLS (Transport Layer Security) để bảo vệ sự chứng thực người dùng. Sự yêu cầu chỉ thực hiện một bên máy chủ tạo ra chứng nhận làm đơn giản hóa việc hoạt động và quản trị bảo mật mạng LAN/WLAN.

- **EAP-TLS:** EAP-TLS (Transport Layer Security) được định nghĩa trong RFC 5216. Trong đó, TLS là một giao thức mã hóa, nó cung cấp bảo mật tầng trên TCP và các giao thức của tầng cao hơn (HTTP, SMTP, NNTP) được vận chuyển trong kênh bảo mật. Bảo mật đưa ra giao thức TLS là một phương pháp mạnh bởi vì nó cung cấp dựa trên việc cấp chứng nhận và sự chứng thực tương tác lẫn nhau. Nó sử dụng PKI để bảo mật sự giao tiếp đến một máy chủ chứng thực. Trái ngược với PEAP, EAP-TLS có nhiều khó khăn trong việc quản trị bởi vì nó yêu cầu tạo chứng nhận bên máy trạm cùng với tạo chứng nhận bên máy chủ để thực hiện sự chứng thực. Lý do EAP-TLS được xem là một trong những loại bảo mật chứng thực EAP tốt nhất, mà thậm chí nếu một mật khẩu bị lấy cắp, nó không đủ phá vỡ cấu trúc EAP-TLS đang chạy trong hệ thống, bởi vì hacker vẫn cần có khóa riêng của máy trạm. Bảo mật được cung cấp bởi EAP-TLS có thể làm gia tăng việc bảo mật nếu chúng ta có thẻ thông minh bởi vì trong thẻ thông minh có các khóa bảo mật riêng biệt.

- **EAP-FAST:** EAP-FAST (Flexible Authentication via Security Tunneling) được định nghĩa trong RFC 4851 và đã được phát triển bởi Cisco System. Giao thức này đã được thiết kế cho sự bảo mật yếu kém của LEAP trong khi việc triển khai thực hiện ở mức độ an toàn thấp. Thay vì sử dụng một sự nhận dạng, sự chứng thực tương tác lẫn nhau được dùng phương pháp PAC (Protected Access Credential). Một tập tin PAC được phát sinh trên mỗi người dùng, mà có thể quản lý động bởi máy chủ chứng thực. EAP-FAST sử dụng PAC để thiết lập một kênh truyền TLS riêng, trong đó mỗi máy trạm kiểm tra độ tin cậy. PAC có thể cung cấp tập tin đến máy trạm bằng thao tác thủ công hay tự động. Sự cung cấp thủ công được phân phát đến máy trạm trên đĩa cứng hoặc một phương pháp phân phối bảo mật mạng. Sự cung cấp tự động một sự phân phối theo nhóm.

EAP-FAST có ba bước thực hiện:

- **Giai đoạn 0:** Giai đoạn này là tùy chọn trong đó PAC cung cấp thủ công hay tự động.

- **Giai đoạn 1:** Trong giai đoạn này, máy trạm và máy chủ chứng thực sử dụng PAC để thiết lập kết nối kênh truyền TLS riêng.

- **Giai đoạn 2:** Trong giai đoạn này, thông tin của máy trạm được trao đổi bên trong kênh truyền mã hóa.

EAP-FAST cũng có thể không sử dụng tập tin PAC mà sử dụng dựa trên sự nhận dạng chứng thực tương tác lẫn nhau trong TLS.

6. Kết luận

6.1. So sánh các loại chứng thực EAP

Bảng so sánh thể hiện các đặc điểm chính của các loại chứng thực EAP được trình bày trong bài viết.

Bảng so sánh các loại chứng thực EAP

	MD5	**LEAP**	**PEAP**	**FAST**	**TLS**
Các thuộc tính sự chứng thực	Chứng thực một chiều	Chứng thực lẫn nhau	Chứng thực lẫn nhau	Chứng thực lẫn nhau	Chứng thực lẫn nhau
Yêu cầu sự nhận dạng của máy trạm	Không	Không	Không	Không, chỉ có tập tin PAC	Có
Yêu cầu sự nhận dạng của máy chủ	Không	Không	Có	Không, chỉ có tập tin PAC	Có
Sự khó khăn trong việc triển khai	Dễ dàng	Mức độ vừa phải	Mức độ vừa phải	Mức độ vừa phải	Khó khăn (Cần yêu cầu việc triển khai nhận dạng của máy trạm)
Tính bảo mật	Kém	Tốt (nhưng đặt mật khẩu phải phức tạp)	Tốt	Tốt	Tốt nhất

6.2. Kết luận

Chuẩn 802.1.X thiết kế nguyên bản cho việc triển khai các mạng có dây hay các mạng LAN. Ngày nay, chuẩn 802.1.X trở nên thông dụng và quan trọng hơn không chỉ tăng cường bảo mật cho mạng LAN mà còn được sử dụng rộng rãi cho việc triển khai mạng Wireless (802.11) và yêu cầu bảo mật tốt hơn cho mạng Wireless. Bảo mật được yêu cầu trong suốt quá trình hoạt động của một hệ thống mạng, do đó nhiều nhà sản xuất thiết bị mạng đã bắt đầu sử dụng và hỗ trợ chuẩn 802.1X trong các sản phẩm của họ. Những người thiết kế và quản trị mạng cần biết tiêu chuẩn này đang được triển khai trong thực tế và đồng thời qua bài viết, tác giả mong muốn mang đến cho độc giả một sự hiểu biết cơ bản về hoạt động chuẩn 802.1X và các loại phương pháp chứng thực EAP khác nhau làm việc như thế nào để làm gia tăng mức độ bảo mật cho toàn hệ thống mạng.

Tài liệu tham khảo

Arunesh Mishra and William A. Arbaugh. 2002. *An Initial SecurityAnalysis of the IEEE 802.1X Standard.* http://www.cs.umd. edu/~waa/1x.pdf.

IEEE Standard 802.1x-2001 – *Standard for Port based Network Access Control.*

Vivek Santuka, Premdeep Banga, Brandon J. Carroll .2011. *AAA Identity Management Security.* Cisco Press.

Yusuf Bhaiji – CCIE. 2008. *CCIE Professional Development Series Network Security Technologies and Solutions.* Cisco Press.