Biện pháp tăng cường bảo mật cho mạng WiMAX

■ TS. Nguyễn Chấn Hùng
■ TS. Lê Nhật Thăng

Trong các mạng vô tuyến, bảo mật luôn là vấn đề làm đau đầu các nhà cung cấp. Mạng WiMAX tuy đã khá hoàn thiện song vẫn còn đó những điểm yếu trong vấn đề bảo mật. Bài viết chỉ ra những điểm yếu đó và một số biện pháp để tăng cường bảo mật cho mạng WiMAX.

I. CÁC ĐIỂM YẾU TRONG BẢO MẬT CỦA WIMAX

1. Lớp vật lý và phân lớp riêng (Physical Layer & Privacy Sublayer)

Trong chuẩn IEEE 802.16, Privacy Sublayer nằm trên đầu của lớp vật lý. Do đó các mạng 802.16 có thể bị tổn hại từ những tấn công ở lớp vật lý, ví dụ như các kiểu tấn công Jamming và Scrambling (sự trộn âm). Jamming được thực hiện bằng cách đẩy mạnh một nguồn nhiễu mạnh nào đó để giảm khả năng của kênh, từ đó dẫn đến từ chối tất cả các dịch vụ khác. Tuy nhiên Jamming có thể được tìm ra nhờ các thiết bị phân tích radio. Scrambling là một dạng tấn công khác của Jamming nhưng nó chiếm những vị trí trong khoảng thời gian ngắn giữa các thời điểm hướng đến các khung cụ thể. Điều khiển và quản lý bản tin có thể ngăn cản tấn công kiểu này song lại không cản được với trễ bản tin hỏng... Sự xáo trộn âm các khe đường lên là khá khó bởi vì kẻ tấn công phải hiểu được thông tin điều khiển và gửi nhiễu trong một khoảng thời gian riêng biệt.

Mục tiêu chính của phân lớp Privacy Sublayer là bảo vệ các nhà cung cấp dịch vụ chống lại các hành vi ăn cắp dịch vụ chứ không phải là đảm bảo cho mạng người sử dụng. Dễ thấy rằng lớp riêng chỉ bảo vệ dữ liệu tại lớp 2 trong mô hình OSI (data link),

nơi mà nó không đảm bảo mã hóa từ đầu cuối tới đầu cuối dữ liệu của người sử dụng. Hơn nữa nó không bảo vệ lớp vật lý từ bản chất của tấn công. Do đó nó cần phải có các công nghệ bảo mật cho lớp vật lý và các lớp cao hơn.

Ăn cắp nhận dạng lại là một vấn đề khác, nó là việc tái lập trình một thiết bị với địa chỉ phần cứng của một thiết bị khác. Địa chỉ có thể được lấy cắp trên phần vô tuyến bằng chắc chắn các bản tin quản lý. Một BS (Base Station) giả mạo là một trạm tấn công hoạt động giống như một BS hợp lệ. Nó làm đảo lộn một cài đặt của SSs/MSs (Subcriber Stations/ Mobile Subcribers) khi cố gắng có được sự thông quan dịch vụ, cái mà họ tin rằng sẽ mang lại một BS hợp lệ. Nó là một điểm khó trong mạng 802.16 bởi vì chế độ TDMA. Trong trường hợp này kẻ tấn công phải truyền tải trong khi BS thật sự đang truyền, với nhiều tín hiệu mạnh và ở nơi mà tín hiệu của BS thực là yếu hơn (tín hiệu ở mức nền tảng), hơn thế nữa kẻ tấn công phải bắt được sự nhận dạng và chờ đến khi một khe thời gian của BS thực được bắt đầu.

Trong thế giới vô tuyến có một số vấn đề chung và IEEE 802.16 cũng không phải là ngoại lệ. Một kiểu tấn công kinh điển đã xuất hiện từ kiểu tấn công được gọi là Water Torture Attack, theo đó một kẻ tấn công gửi một chuỗi các khung để làm tiêu tốn hết pin của người nhận. Thêm vào đó, kẻ tấn công với một bộ thu RF được bố trí hợp lý có thể ngăn chặn các bản tin gửi qua mạng vô tuyến, và do đó một cơ chế bảo mật trong thiết kế được yêu cầu. Các cơ chế bảo mật hiện nay không đánh địa chỉ tốt như trong mạng mesh 802.11a, một mạng dẫn đầu trong các cơ chế bảo mật. Việc giới thiệu tính di động trong chuẩn IEEE 802.16e sẽ làm cho kẻ tấn công càng dễ dàng hơn trong công việc của mình. Cụ thể là trong chuẩn này thì vị trí vật lý của kẻ tấn công đã không còn là vấn đề đáng ngại, các bản tin quản lý thì trở nên dễ bị tấn công hơn so với trong 802.11. Do đó nó cần được duy trì một kết nối bảo mật trong khi một SS di động dịch chuyển giữa các BS. (Johnston & Walker, 2004)

Với một máy phát RF được cấu hình hợp lý, một kẻ tấn công có thể viết lên một kênh RF, giả mạo khung mới và bắt giữ, thay đổi và truyền lại các khung từ một khía cạnh được cho phép. Thiết kế này phải đảm bảo chắc chắn một công nghệ nhận thực dữ liệu. Nó cũng có thể gửi lại một khung không bị thay đổi một cách hợp lệ. Trong trường hợp khoảng cách truyền tải là lớn, giao diện vô tuyến và khoảng cách có thể cho phép một kẻ tấn công sắp xếp lại và lựa chọn cẩn thận các khung chuyển tiếp. Do đó thiết kế phải tìm được các khung được dùng lại. (Johnston & Walker, 2004)

2. Vấn đề nhận thực lẫn nhau

Hai loại chứng nhận đã được phân loại bởi chuẩn IEEE 802.16: một là các chứng nhận cho các nhà sản xuất và loại thứ hai là cho các chứng nhận SS. Không có chứng nhận cho BS. Một chứng nhận nhà sản xuất xác nhận nhà sản xuất của một thiết bị IEEE 802.16. Nó có thể tự chứng nhận hoặc được xác nhận bởi bên thứ 3. Một chứng nhận SS xác nhận một SS riêng biệt và tính đến cả địa chỉ MAC của nó. Các nhà sản xuất tạo và xác nhận những chứng nhận SS. Nhìn chung BS sử dụng khóa công khai của chứng nhận nhà sản xuất để xác minh chứng nhận SS và từ đây việc nhận dạng thiết bị là được công nhận. Thiết kế này thừa nhận rằng SS duy trì khóa riêng tương ứng tới khóa công khai của nó trong một kho lưu trữ kín, chống lại kẻ tấn công từ thỏa hiệp dễ dàng nó. Khe hở lớn của thiết kế bảo mật IEEE 802.16 là thiết kế một chứng nhận BS. Nó chỉ bảo vệ các máy trạm client chống lại tấn công lặp lại hay tấn công giả mạo nhờ cung cấp một kế hoạch cho

nhận thực lẫn nhau. Điều này được hỗ trợ bởi Wongthavarawat (2005) "không có nhận thực lẫn nhau nào được cung cấp, chúng có thể làm tổn hại bằng các tấn công lặp lại và xen giữa và chứng nhận SS là một phương pháp nhận thực giới hạn". Trong 802.16e, EAP có thể thực hiện những phương pháp nhận thực đặc biệt giống như EAPTLS (chứng nhận dựa trên X.509).

3. Các định nghĩa không rõ ràng

Thiết kế IEEE 802.16 thất bại trong việc định nghĩa một cách rõ ràng các hỗ trợ bảo mật SA (Security Association) được cấp phép. Ví dụ, trạng thái của SA không bao giờ phân biệt một SA được cấp phép từ một cái khác, và do đó có thể bị tổn hại từ kiểu tấn công lặp lại. Điều này sẽ trở thành vấn đề đặc biệt khi IEEE 802.16e thực sự di động và chuyển vùng. Ngoài ra SS không thể xác nhận sử dụng lại dữ liệu các SA. Do đó kế hoạch mã hóa có thể bị tổn hại bởi các kiểu tấn công sử dụng lại khóa mã hóa. Thêm vào đó các BS không được cấp phép không chứa sự nhận dạng BS, từ đây SS không thể phân biệt trao quyền từ các BS không được trao quyền. Đến đây chúng ta có thể thừa nhận rằng sự lẩn tránh nó từ SS chống lại việc quản lý khóa và mã hóa, từ sự bảo vệ SS trước các tấn công lặp lại và giả mạo. Một giải pháp chống lại những tổn hại từ tấn công lặp lại là sử dụng bộ tạo giá trị ngẫu nhiên từ BS và SS tới các SA trao quyền. Theo đó thì cặp khóa riêng và công khai được sử dụng để xác nhận các địa chỉ MAC giống nhau với điều kiện là phải định nghĩa một cách rõ ràng tất cả các xác nhận địa chỉ MAC để đảm bảo địa chỉ MAC là duy nhất nhằm tránh vấn đề giả mạo.

4. Dữ liệu riêng

Trong IEEE 802.16, sử dụng mã hóa DES trong chế độ CBC cho dữ liệu cá nhân. DES trong chế độ CBC sử dụng 56 bit khóa DES (TEK) và Véc tơ khối tạo CBC (CBCIV) (Initialization Vector). Chế độ CBC yêu cầu một vector khởi tại IV ngẫu nhiên để đảm bảo kế hoạch (RSA, 2004). Quay trở lại thảo luận trước của Wongthavarawat (2005) thì CBCIV là có thể đoán trước được, VD: CBCIV = [IV Parameter from TEK exchange] XOR [PHY Synchronization field] và 56 bit khóa là không đảm bảo an toàn với khả năng tính toán ngày nay, từ đó nó có thể bị tổn hại trước các tấn công để có được văn bản ban đầu. Thêm vào đó không cung cấp việc tìm kiếm tính toàn vẹn của bản tin sẽ làm tăng khả năng của các tấn công chủ động. Ngoài ra thì theo Johnston and Walker,(2004) bởi vì vector khởi tạo SA là không đổi và là công khai cho TEK của nó và trường đồng bộ PHY (synchronization field) là lặp lại và có thể đoán trước nên vector khởi tạo MPDU là có thể đoán trước.

IEEE 802.16e chọn AES CCM sử dụng khóa 128 bít giống như một phương pháp mật mã dữ liệu mới để đảm bảo kiểm tra tính toàn vẹn của bản tin và bảo vệ trước tấn công lặp lại bằng cách sử dụng số gói (PN-Packet Number). Lần này bộ phát được xây dựng duy nhất giống như bộ mã hóa ngẫu nhiên trên gói, để đảm bảo tính duy nhất và thêm vào cơ chế nhận thực.

5. Quản lý khóa

Trong IEEE 802.16 có vấn đề giao thức quản lý khóa, trong chuẩn này sử dụng khoảng trống chuỗi TEK, nó sử dụng chuỗi số để phân biệt các bản tin. Giao thức nhận ra mỗi TEK với một chuỗi số 2 bit, nó sử dụng chuỗi số từ 0-4 trên tất cả khóa sử dụng lại lần thứ 4 để giúp SS có thể phân biệt ra các khóa sử dụng lại trong tấn công lặp lại.

6. Các điểm yếu khác

Trong dữ liệu định nghĩa SA, một AK

có thể kéo dài tới 70 ngày, trong khi đó thì thời gian sống của TEK chỉ có 30 phút, điều này cho phép một kẻ tấn công xen vào sử dụng lại các TEK. Một SA dữ liệu có thể tiêu thụ tới 3.360 TEK trong khoảng thời gian sống của AK đang đòi hỏi không gian SAID phải mở rộng từ 2 lên mức tối thiểu là 12 bits. IEEE 802.11 có nghĩa là SS phải tin tưởng rằng BS luôn luôn tạo ra AK mới, và vì vậy cần một bộ tạo số ngẫu nhiên của BS phải hoàn hảo nếu không AK và TEK sẽ dễ bị tổn hại.

Trong IEEE 802.16, không đề cập đến vấn đề nhận thực BS tới SS điều này tạo điều kiện cho kiểu tấn công giả mạo có thể làm tổn hại đến giao thức PKM. Một ví dụ, SS không thể xác minh bất cứ quyền hạn bản tin nào đến từ BS được phép. BS phản hồi lại SS sử dụng thông tin công khai vì vậy bất cứ BS giả mạo nào có thể tạo ra một phản hồi như vậy.

II. BIỆN PHÁP TĂNG CƯỜNG BẢO MẬT CHO WIMAX

1. Nhận thực lẫn nhau

Hầu hết mọi điểm yếu về bảo mật của WiMAX đều tập trung vào vấn đề thiếu chứng nhận cho BS. Chỉ có một cách để SS chống lại sự giả mạo là thay thế kế hoạch nhận thực bằng một kế hoạch khác hỗ trợ khả năng nhận thực lẫn nhau.

2. Các lỗi bảo vệ dữ liệu

Chuẩn 802.16 sử dụng DES-CBC cho mã hóa dữ liệu. DES-CBC yêu cầu một IV để bảo mật v n đề này. Tuy nhiên điều đáng ngại ở đây là 802.16 lại sử dụng một IV có thể đoán trước được. Để giải quyết vấn đề này, một đề xuất mới là có thể tạo ra ngẫu nhiên một IV trên mỗi khung, và sau đó nó có thể được chèn vào trong phần tải trọng. Với cách làm như vậy một kẻ tấn công sẽ không thể biết được IV để giải mã dữ liệu đi qua mạng.

3. Cải thiện bảo mật tích hợp trong 802.16e

Nhiều cải tiến trong suốt quá trình nghiên cứu và hầu hết trong số đó sẽ được tích hợp trong phiên bản tiếp theo của giao thức IEEE 802.16e đã được phê chuẩn trong tháng 1/2006.

Có thể kể đến một số cải tiến như:

- PKMv2 sẽ được sử dụng thay thế cho PKM.
- PKMv2 định nghĩa một cách sử dụng giao thức nhận thực mở rộng EAP (Extensible Authentication Protocol).

Hơn thế nữa PKMv2 chỉ rõ một phương thức "bắt tay ba bước" để thiết lập một khóa nhận thực AK giữa BS và SS. Đây là cách để truyền AK giữa BS và SS an toàn hơn. Hai phương pháp nhận thực lẫn nhau dựa trên RSA và EAP sẽ được cung cấp. Cả hai hoặc một trong hai phương pháp có thể được sử dụng riêng rẽ. Chúng sẽ cùng tạo ra khóa rồi sau đó được xử lý bởi hệ thống phân cấp khóa. Trong nhận thực lẫn nhau dựa trên RSA, chứng nhận X.509 được sử dụng cả bởi BS và SS và đã giải quyết rất nhiều vấn thiếu sót bảo mật liên quan đến giả mạo. Trong nhận thực EAP thì dựa trên mô hình ba bên (three-party) để nhận thực.

Chuẩn 2001 định nghĩa các loại mã nhận thực dựa trên hàm băm HMAC (Hash Function based Message Authorication Code) cho các bản tin quản lý. Trong PKMv2, vấn đề này có thể được thương lượng giữa HMAC hoặc CMAC. CMAC là một AES dựa trên MAC được định nghĩa bởi NIST như một tiêu chuẩn của chính phủ Mỹ. Chỉ chuỗi các bản tin có thể được bảo vệ với một mã HMAC/CMAC đã được mở rộng. Các mã luôn kết thúc TLV trong một bản tin gồm nhiều TLV. Bằng cách này nó đảm bảo bản tin được truyền qua mạng mà không bị tấn

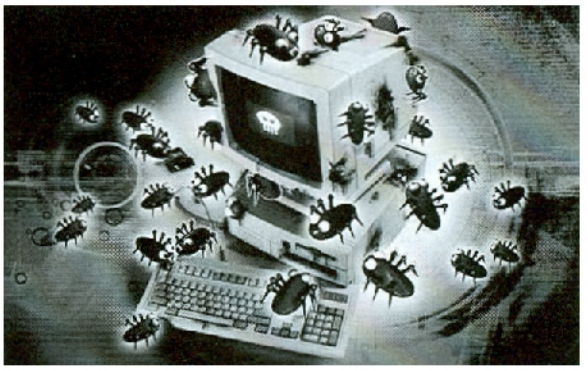
công. Nếu một ai đó cố gắng chèn một bản tin vào lưu lượng thì gần như chắc chắn phía thu sẽ nhận ra rằng bản tin đó không gửi bởi người gửi hợp lệ bởi vì chuỗi mã (digest) chứa trong mỗi bản tin sẽ không khớp với digest đã được xây dựng bởi bên thu.

Một số phương pháp mật mã sẽ được tích hợp lại với nhau. Đầu tiên là AES-CCM (trong 802.16-2004) đã được nhập vào thành 802.11i và 802.16e với việc thêm AES-CTR và AES-CBC. AES-CCM được sử dụng để kiểm tra tính toàn vẹn, nhận thực và bảo vệ lưu lượng dữ liệu. AES-CMC thì lại hữu dụng trong trường hợp cần đảm bảo lưu lượng thấp với mức bảo mật không cao trong cùng một thời điểm. AES-CTR là một phương pháp đặc biệt sẽ được sử dụng để mật mã hóa lưu lượng MBS.

Cuối cùng thì với mỗi nhóm khác nhau có thể sẽ có các mô hình bảo mật khác nhau. Việc kết hợp các phương pháp bảo mật cần tính đến sự cân bằng giữa các phương pháp thành phần để đảm bảo phù hợp nhất với mục đích bảo mật dữ liệu đó.

VI. KẾT LUẬN:

Chuẩn IEEE 802.16e đã có một số thay đổi trong cơ chế bảo mật, nó tạo ra trên mỗi khung một IV ngẫu nhiên, chống tấn công lặp lại bằng cách sử dụng PN (packet number). Nó sẽ sử dụng AES như một phương pháp mã hóa chính và giới thiệu một phương pháp nhận thực dựa trên giao thức nhận thực mở rộng như EAPTLS, EAPTTLS, PEAP, EAPSIM, mở rộng nhận thực tới server AAA. Chế độ AESCCM là một mật mã liên kết dữ liệu mới cho cơ chế nhận thực dữ liệu, được định nghĩa bởi NIST. Chuẩn này cũng thay thế khóa TripleDES đang thử nghiệm trong giao thức PKM bằng chế độ AESECB và linh động hạ thấp giá thành nhận thực lại trong quá trình chuyển vùng (roaming).



Cơ chế bảo mật là một quá trình xử lí phức tạp, nó yêu cầu những nghiên cứu chuyên sâu cũng như sự ước lượng thông số và các kết quả thực hiện. IEEE 802.16e sẽ mở cửa cho di động không dây tuy nhiên nó cũng có thể bị tổn hại bởi vì chưa có một ràng buộc nào đối với kẻ tấn công. Sẽ còn nhiều vấn đề phải tăng cường nghiên cứu như vấn đề quản lý khóa từ BS đến SS, nhận thực người sử dụng chuyển vùng và nâng cấp thoại. IEEE 802.16 (WiMAX) có thể sẽ giành được thành công trong lĩnh vực truyền thông vô tuyến. Các nhà cung cấp thiết bị đã sẵn sàng cung cấp thiết bị WiMAX của họ. Tuy nhiên công nghệ này vẫn đang trong giai đoạn phát triển và cần nhiều hơn nữa những nghiên cứu trong thời gian tới.

** Nghiên cứu này nằm trong khuôn khổ đề tài trọng điểm cấp Nhà nước KC.01.10/06-10: "Nghiên cứu phát triển một số sản phẩm tính toán khắp nơi và di động"*

TÀI LIỆU THAM KHẢO:

[1]. Jamshed Hasan School of Computer and Information Science, Edith Cowan University, *Australia Security Issues of IEEE 802.16 (WiMAX)*

[2]. Derrick D. Boom: *Denial Of Service Vulnerabilities In Ieee 802.16 Wireless Networks*, Thesis at Naval Postgraduate School Monterey, California

[3]. Arkoudi-Vafea Aikaterini *"SECURITY OF IEEE 802.16"*