BẢO MẬT
trong mạng truy nhập băng rộng
Cable Modem

ThS. Dương Thị Thanh Tú

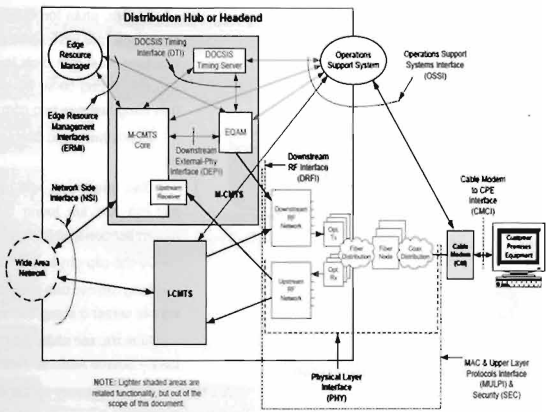
Nội dung bài báo chỉ ra những lỗ hổng bảo mật trong hệ thống DOCSIS 2.0 cũng như một số hình thức tấn công vào mạng truy nhập băng rộng Cable Modem (CM) qua đó giới thiệu những tính năng mới trong DOCSIS 3.0 để đảm bảo an toàn thông tin trong mạng CM.

CÁC HÌNH THỨC TẤN CÔNG TRONG MẠNG CM

Ngày nay, khi các công nghệ truy nhập mạng đang ngày càng phát triển thì vấn đề bảo mật cũng ngày càng trở nên cấp bách. Các nguy cơ tấn công với nhiều hình thức khác nhau đang xuất hiện ngày càng nhiều với nhiều hình thức khác nhau theo các mục đích khác nhau, từ đơn giản đến phức tạp như truy nhập và chiếm quyền điều khiển thiết bị của khách hàng, sử dụng dịch vụ trái phép, đánh cắp thông tin, v.v....Các hình thức tấn công này có thể để lại nhiều hậu quả không lường thấm chí là nặng nề như mất khả năng cung cấp dịch vụ trong thời gian dài. Nhiều hacker lợi dụng những lỗ hổng về bảo mật của các hệ thống mạng truy nhập để đạt được mục đích của mình. Chính vì thế bảo mật trở thành một vấn đề rất cần được chú trọng trong quá trình vận hành và khai thác bất cứ một công nghệ truy nhập nào.

Công nghệ truy nhập băng rộng Cable Modem (CM) là công nghệ truyền số liệu trên mạng truyền hình cáp (CATV) vốn là mạng lai ghép giữa cáp quang và cáp đồng trục (HFC- Hybrid Fiber Coaxial). Công nghệ này cho phép cung cấp cho khách hàng hai dịch vụ chính là truyền hình cáp và truy nhập băng rộng, ngoài ra còn có những dịch vụ mở rộng như VoIP, VoD, truyền hình tương tác, game online, hội nghị truyền hình,... Các chuẩn chủ yếu của CM bao gồm: DOCSIS phát triển bởi CableLabs, DAVIC của châu Âu và IEEE 802.14.

Tính đến tháng 2 năm 2010, trên thế giới đã có khoảng 497.77 triệu thuê bao băng rộng, trong đó thuê bao CM chiếm khoảng 20% số thuê bao băng rộng tại thời điểm này. Đến thời điểm hiện nay, số lượng thuê bao CM ngày càng tăng lên và CM vẫn được xếp vào một trong những công nghệ băng rộng có độ phổ biến trên thế giới.



Kiến trúc tham khảo của việc truyền dữ liệu IP qua Modem cáp

Cùng như bất cứ một công nghệ mang truy nhập nào, công nghệ CM cũng phải đối mặt với rất nhiều cách tấn công khác nhau như sử dụng trộm dịch vụ, đánh cắp thông tin của thuê bao, thậm chí đánh sập các server (ví dụ như server DHCP) dẫn đến ngừng cung cấp dịch vụ, v.v.. Các hình thức tấn công này phần lớn nằm ở phần truy nhập từ CM đến Hệ thống kết cuối Modem cáp (CMTS-Cable Modem Termination System)- Hệ thống kết nối nhà điều hành mạng và hệ thống mạng cáp HFC. Một số phương thức tấn công tiêu biểu có thể kể ra như sau:

- Phương thức tấn công vật lí: sử dụng các thiết bị kết nối với CM để có thể hack firmware hoặc thay thế firmware trong CM

- Sử dụng các chương trình quét SNMP, tìm kiếm xem các cổng SNMP của CM có để mở không, thông qua đó hacker có thể tấn công vào thiết bị CM

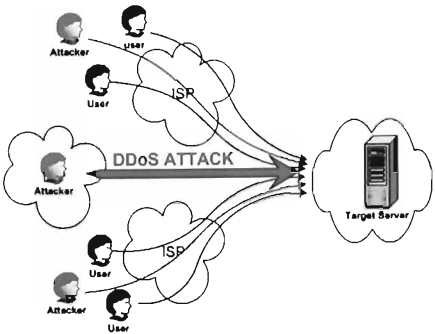
- Chạy các chương trình giả TFTP server, kết nối với CM để tải file cấu hình đã được hack hoặc viết bởi hacker về CM nhằm sử dụng trộm dịch vụ hoặc dùng ở tốc độ cao hơn cho phép

- Các gói tin truyền trên mạng đặc biệt là các gói tin broadcast và multicast do không được mã hóa nên có thể bị bắt và phân tích bởi các phần mềm như WireShark, qua đó hacker có thể thu được những thông tin của thuê bao cũng như của nhà cung cấp

- Các server ở mạng đường trục như DHCP, TFTP, ToD có thể bị tấn công khá dễ dàng theo kiểu từ chối dịch vụ phân tán (DDoS) hoặc chiếm quyền truy nhập

Để hacker có thể thực hiện các thâm nhập trái phép như trên là do các chuẩn công nghệ Modem cáp trước đây có khá nhiều lỗ hổng về bảo mật, có thể liệt kê ra như:

- Firmware của các thiết bị CM phiên bản cũ



Tấn công DDoS

không được cập nhật hoặc bản cập nhật không được mã hóa.

- File cấu hình không được mã hóa và có thể bị sửa đổi.

- Lưu lượng từ CMTS đến CM không được mã hóa hoặc mã hóa không đủ mạnh.

- Chưa có xác thực giữa CM và các server;

- Chưa có quá trình kiểm tra tính toàn vẹn của các bản tin kể cả file cấu hình;

- Chưa có quá trình xác nhận địa chỉ IP nguồn;

- Các server DHCP, TFTP và ToD chưa được bảo vệ triệt để (ví dụ: địa chỉ IP và địa chỉ MAC của server có thể bị phát hiện).

- Chưa có quá trình xác nhận địa chỉ MAC hợp lệ của các CM.

CÁC TÍNH NĂNG BẢO MẬT MỚI TRONG CÔNG NGHỆ CM

Để khắc phục những lỗ hổng về bảo mật như đã liệt kê trong phần trên, DOCSIS đã đưa ra tiêu chuẩn mới DOCSIS 3.0 với những tính năng mới về bảo mật, phần lớn được định nghĩa trong kiến trúc BPI+ (Base Line Privacy Interface Plus) tạm dịch là tiêu chuẩn bảo mật đường cơ sở bổ xung. Những tính năng mới này bao gồm:

- Mã hóa lưu lượng dùng mã AES 128 bit.

- Xác thực sớm đối với CM và mật mã hóa lưu lượng (EAE - Early Authentication and Encryption).

- Cơ chế cấp quyền truy nhập.

- Nâng cao các tính năng bảo mật đối với các server ở mạng đường trục.

- Kiểm tra, xác nhận địa chỉ IP nguồn (SAV - Source Address Verification).

- Quá trình học về TFTP proxy và file cấu hình.

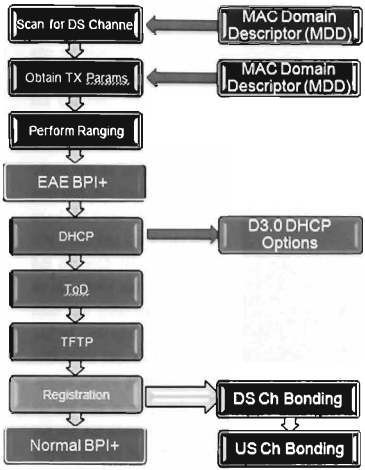
- Thuật toán MMH sử dụng cho quá trình kiểm tra tính toàn vẹn của bản tin (MIC) ở CMTS.

- Thu hồi chứng chỉ.

- Cập nhật các hỗ trợ của các chứng nhận cho việc bảo vệ tải phần mềm trong tương lai.

- Hỗ trợ mã hóa theo cách thức mới cho bản tin multicast.

Như vậy, trong DOCSIS 3.0 ngoài việc bao gồm các quá trình xác thực đối với CM, trao đổi khóa và tạo lập các phiên lưu lượng đã được mã hóa giữa CM và CMTS (được định nghĩa trong BPI+), nó còn bổ sung thêm khả năng bảo mật cho các server mạng đường trục của công nghệ Cable Modem và bảo mật quá trình tải phần mềm (ở đây là firmware phiên bản mới) về các CM. Những tính năng mới này cung cấp cho người sử dụng Modem cáp sự bảo mật dữ liệu qua mạng cáp đồng thời ngăn chặn sự truy nhập của những người dùng không được phép qua các dịch vụ mạng RF MAC.



Quá trình đăng ký cáp các modem DOCSIS 3.0

KIẾN TRÚC BPI+

BPI+ được tạm dịch là tiêu chuẩn bảo mật đường cơ sở bổ sung, được cải tiến dựa trên tiêu chuẩn BPI của các phiên bản trước, bao gồm 2 thành phần giao thức:

- Một giao thức đóng gói cho các dữ liệu gói qua mạng mạng cáp. Giao thức này định nghĩa:

1. Định dạng của khung cho việc truyền các gói dữ liệu đã được mã hóa trong khung MAC của DOCSIS;

2. Cài đặt cho phép việc mã hóa phù hợp, ví dụ : việc ghép đôi các thuật toán mã hóa dữ liệu và xác nhận;

3. Các qui tắc để áp dụng các thuật toán đo cho gói dữ liệu của khung MAC trong DOCSIS.

- Giao thức quản lí khóa (Quá trình bảo mật cơ bản để quản lí khóa, BPKM - Baseline Privacy Key Management) cung cấp sự bảo mật cho việc phân phối dữ liệu khóa từ CMTS đến CM. Thông qua BPKM, CM và CMTS đồng bộ dữ liệu khóa. Ngoài ra, CMTS còn sử dụng giao thức để cài đặt truy nhập có điều kiện đối với các dịch vụ mạng.

Mã hóa gói dữ liệu

Sự cải tiến về mã hóa gói dữ liệu trong DOCSIS 3.0 được thực hiện trong phần lớp MAC của DOCSIS. Trong đó, thông tin đặc thù về bảo mật ở header của gói tin được đặt trong header mở rộng theo tiêu chuẩn bảo mật cơ bản [DOCSIS MILPIv3.0].

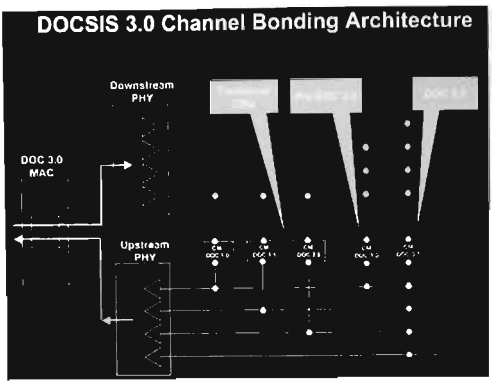
DOCSIS chỉ mã hóa các gói dữ liệu khung MAC, không mã hóa header. Các tin nhắn quản lí MAC DOCSIS, ngoại trừ bản tin REG-REG-MP cũng không được mã hóa. Bản tin REG-REG-MP chỉ được mã hóa khi tính năng EAE hoạt động.

Giao thức quản lý khóa

CM sử dụng giao thức quản lí khóa bảo mật cơ bản (BPKM) để được nhận, lấy các thành phần khóa mã hóa lưu lượng từ CMTS, hỗ trợ việc xác nhận lại theo định kì và lấy khóa mới. Giao thức BPKM sử dụng các tiêu chuẩn số, một thuật toán mã hóa khóa công khai và 2 khóa 3DES để bảo mật sự trao đổi khóa giữa CM và CMTS.

Giao thức BPKM dựa trên mô hình client/server. Trong đó, CM là BPKM client, yêu cầu các thành phần của khóa còn CMTS là BPKM server, phản hồi lại những yêu cầu này. Để bảo đảm rằng mỗi CM client riêng biệt chỉ nhận được các thành phần mã khóa đã được cho phép, giao thức BPKM được truyền trên các bản tin quản lí MAC của DOCSIS.

Đầu tiên, DOCSIS sử dụng mật mã hóa công khai để trao đổi giữa CM và CMTS của nó. Sau đó, dữ liệu trao đổi này sẽ tạo ra khóa thứ hai BPKM, thường được dùng để mã hóa lưu lượng. Cơ chế 2 tầng trong việc phân phối khóa này cho phép các mã khóa lưu lượng



Kênh liên kết DOCSIS 3.0

được cập nhật không phải gánh chịu mào đầu của hoạt động tính toán chuyên sâu của mã hóa công khai.

Mỗi một CM đều có một chứng nhận số duy nhất được cung cấp bởi nhà cung cấp dịch vụ Modem Cáp. Chứng nhận số bao gồm:

- Khóa công khai của CM
- Địa chỉ MAC của CM
- Nhận dạng của nhà cung cấp
- Số sen của CM

Khi đề nghị một mã khóa cho phép, thiết bị CM sẽ "trình" chứng nhận số cho CMTS. CMTS kiểm tra chứng nhận số đó, nếu đúng, nó sẽ dùng mã khóa công khai của CM để mã hóa các dữ liệu CMTS phản hồi lại các yêu cầu của CM.

Liên kết bảo mật trong DOCSIS

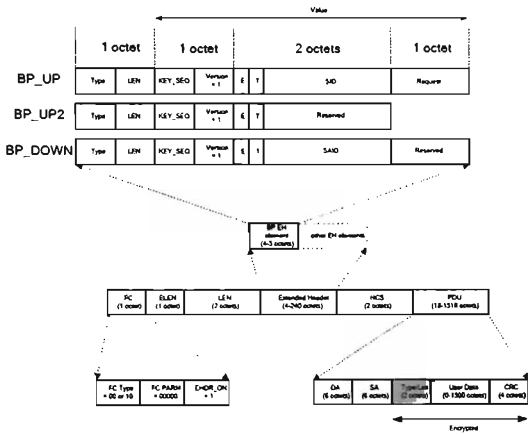
Một liên kết bảo mật trong DOCSIS được gọi là một SA (Security Association). SA là một tập các thông tin bảo mật mà một CMTS chia sẻ với một hoặc nhiều CM để cung cấp kết nối an toàn qua mạng cáp.

Có 3 loại liên kết bảo mật DOCSIS: sơ cấp, tĩnh, và động. Một kết nối bảo mật sơ cấp được ràng buộc với một CM đơn lẻ và được thiết lập khi CM hoàn thành quá trình xác thực. Liên kết bảo mật tĩnh có thể được chia sẻ cho nhiều CM và được thiết lập, dựa trên cấu hình CMTS, khi 1 CM hoàn thành quá trình xác thực. Một kết nối bảo mật động có thể được chia sẻ bởi nhiều CM và được thiết lập động một cách bình thường, đáp ứng lại các lời yêu cầu về quá trình khởi tạo về lưu lượng đường xuống.

Các thông tin về một kết nối bảo mật bao gồm dãy mã hóa, các khóa mã hóa lưu lượng và các vectơ khởi tạo CBC và sự tồn tại của thông tin khóa. Mỗi liên kết bảo mật được xác định với 14 bit điều khiển, được gọi là kí hiệu nhận dạng liên kết bảo mật.

Mỗi CM mà trên đó tính năng bảo mật được kích hoạt thiết lập một liên kết bảo mật sơ cấp với CMTS của nó. Khi CM mã hóa lưu lượng lưu lượng lên, bao gồm cả các bản tin quản lí MAC REG-REQ-MP, nó cần phải sử dụng liên kết bảo mật sơ cấp của CM. Giá trị nhận dạng liên kết bảo mật (SAID) sơ cấp được thiết lập trong khi trao đổi xác nhận khởi tạo.

Dòng lưu lượng xuống có thể được mã hóa dưới bất cứ dạng liên kết bảo mật nào. Một gói tin IP multicast lưu lượng xuống (thường có đích là nhiều CM), do đó, thường được mã hóa bởi liên kết bảo mật tĩnh hoặc động. Lưu lượng unicast đường xuống được định hướng ở các thiết bị CPE phía sau thiết bị CM thường được mã hóa bởi liên kết bảo mật sơ cấp của CM.



Khuôn dạng PDU với thành phần EH

Một CM cần phải hỗ trợ:

- Một kết nối bảo mật sơ cấp;
- Ít nhất 15 SA mà mỗi kết nối có thể sử dụng như là kết nối tĩnh hay động .

- Một CMTS cần phải hỗ trợ:
- Một kết nối bảo mật sơ cấp cho mỗi CM;
- Ít nhất một SA động (cho một CMTS).

Sử dụng giao thức BPKM, một CM yêu cầu từ CMTS của nó thành phần khóa của một kết nối bảo mật. CMTS sẽ bảo đảm rằng mỗi client CM chỉ truy nhập các kết nối bảo mật được phép.

Các thành phần của khóa của một kết nối bảo mật (ví dụ, khóa và véctơ khởi tạo CBC) có thời gian sử dụng giới hạn. Khi CMTS cung cấp các thành phần khóa SA cho CM, nó cũng cung cấp luôn cho CM thời gian sử dụng còn lại của các thành phần đó. CM có trách nhiệm phải yêu cầu những thành phần khóa mới trước khi thành phần khóa hiện thời hết hạn. Giao thức BPKM tập trung vào cách thức CM và CMTS duy trì đồng bộ mã khóa.

QoS của các nhận dạng dịch vụ và nhận dạng kết hợp bảo mật trong DOCSIS

Nhận dạng kết hợp bảo mật (SAID - Security Association Identifier) trong DOCSIS được mã hóa và đặt vào phần mào đầu lớp MAC trong khung luồng xuống. Nếu khung luồng xuống là gói unicast được đánh địa chỉ đến một thiết bị CPE phía sau một CM riêng biệt thì các khung sẽ được mã hóa riêng biệt với một kết nối bảo mật sơ cấp của CM. Trong trường hợp khung luồng xuống là gói multicast thì SAID đóng hoặc tĩnh sẽ chứa phần sắp xếp nhóm multicast và đặt trong phần mào đầu mở rộng. Sau đó, kí hiệu nhận dạng kết nối bảo mật SAID (sơ cấp, tĩnh hoặc động), sẽ tổ hợp với các trường dữ liệu khác trong thành phần mào đầu mở rộng luồng xuống, xác định modem nhận và tập riêng biệt các thành phần khóa cần thiết để giải mã trường dữ liệu gói của khung MAC đã được mã

hóa của DOCSIS.

Bởi vì tất cả các lưu lượng luồng lên đều được mã hóa bởi SA sơ cấp của CM nên các khung MAC luồng lên của DOCSIS sẽ không mang theo một kí hiệu nhận dạng kết nối bảo mật SAID trong phần mào đầu mở rộng. Thay vào đó, thành phần EH của tiêu chuẩn bảo mật cơ sở chứa một nhận dạng dịch vụ (SID - Service Identifier) với đảm bảo QoS được gán cho CM.

Phần mào đầu mở rộng của chuẩn bảo mật đường cơ sở phục vụ nhiều mục đích khác nhau cho PDU trong các khung MAC DOCSIS luồng lên. Như là sự thay thế cho tập các thành phần của khóa sử dụng để mã hóa các khung dữ liệu gói, phần mào đầu mở rộng trong tiêu chuẩn bảo mật cơ sở cung cấp một cơ chế để các cấp phát các yêu cầu băng thông. Trong một số trường hợp, nó có thể mang theo dữ liệu phần mềm điều khiển.

Có hai chức năng được liên kết trong một SID QoS nếng biết. Vì lí do này, các thành phần mào đầu mở rộng bảo mật cơ sở trong các đường lên thích hợp chứa một SID QoS hơn là một SAID cơ sở. SAID có thể được CMTS suy ra từ SID của QoS luồng lên logic mà trên đó nhận được địa chỉ MAC.

KẾT LUẬN

Với việc đưa ra các cơ chế bảo mật mới, DOCSIS 3.0 đã hạn chế tối đa các khả năng tấn công vào mạng Modem Cáp. Cơ chế nhận thực trước và mã hóa (EAE), cùng với cơ chế cấp phép đã tạo ra một mạng lưới kiểm soát chặt chẽ các thiết bị đầu vào CM và các thiết bị phía server CMTS. Chỉ những thiết bị CM đã được nhận dạng và cấp phép thì mới được truy nhập vào mạng. Do đó đã hạn chế được tới mức thấp nhất khả năng các Hacker có thể sử dụng các thiết bị làm giả TFTP Server để đánh cắp thông tin hay sử dụng biện pháp hack Firmware của các thiết bị CM. Thêm vào đó là cơ chế mã khóa lưu lượng (TEK) đã cung cấp một giải pháp nâng cao tính an toàn cho quá trình truyền thông giữa các thiết bị CM và CMTS

Tài liệu tham khảo

[1]. *"Data-Over-Cable Service Interface Specifications, DOCSIS 3.0, Security Specification"*. Cable Television Laboratories, Inc, June 11th 2010

[2]. DER ENGEL, *"Hacking the Cable Modem"*, No Starch Press, 2006

[3]. SAMUEL KOO AND JIHONG YOON, *"Hacking the Cable Modem"*, Presentation, Free Anonymous Internet World, August 2008