ỨNG DỤNG FRAMEWORK X.805 CỦA ITU_T TRONG ĐẢM BẢO AN NINH HỆ THỐNG TRUYỀN THÔNG

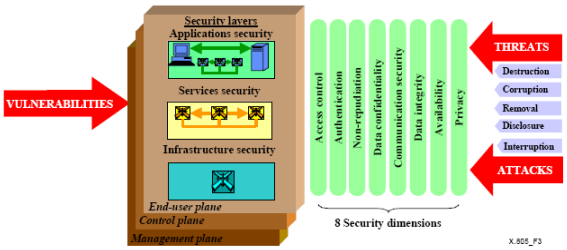
ThS. Cao Minh Thắng

Viện công nghệ Thông tin và Truyền thông CDIT

***Tóm tắt**: X.805 là khuyến nghị về kiến trúc an ninh toàn trình (end-to-end) cho một hệ thống truyền thông (HTTT) do ITU-T đề xuất. Kiến trúc này cung cấp một Framework rất hữu ích cho người làm công tác an toàn bảo mật các HTTT. Trong những năm vừa qua Phòng NCPT An toàn thông tin của Viện công nghệ Thông tin và Truyền thông CDIT đã nghiên cứu sử dụng công cụ này để phân tích và đề xuất nhiều giải pháp an ninh hữu ích cho mạng NGN và dịch vụ của VNPT. Trong khuôn khổ bài báo này, tác giả sẽ tập trung phân tích tính ưu việt và khả năng ứng dụng rộng rãi của bộ công cụ tư duy an toàn bảo mật này.*

1. TỔNG QUAN VỀ X.805

Kiến trúc an ninh mà X.805 đề xuất cho ta thấy quan điểm về an ninh HTTT một cách toàn diện, từ trên xuống, từ đầu cuối đến đầu cuối và có thể được áp dụng cho các phần tử mạng, các dịch vụ, và các ứng dụng để phát hiện, dự đoán và hiệu chỉnh các lỗ hổng an ninh.



Hình 1. Kiến trúc an ninh X.805

Kiến trúc an ninh hướng đến giải quyết các vấn đề quan trọng khi xây dựng an ninh HTTT từ đầu cuối đến đầu cuối, đó là:

- Các thành phần nào của HTTT cần được bảo đảm an ninh?
- Cần hoạt động nào của HTTT cần được đảm bảo an ninh?
- Có những loại nguy cơ an ninh nào có thể tác động đến HTTT?
- Cần phải thực hiện những biện pháp an ninh gì để đối phó với các nguy cơ an ninh?

Những vấn đề này được giải quyết bởi các thành phần kiến trúc tương ứng đó là: các lớp an ninh, các mặt phẳng an ninh, các nguy cơ an ninh và các biện pháp an ninh.

2. CÁC LỚP VÀ MẶT PHẲNG AN NINH

Các lớp an ninh

Ở góc nhìn thứ nhất X.805 phân tích HTTT thành 3 lớp theo thứ tự từ thấp đến cao bao gồm lớp hạ tầng (Infrustructure Layer), dịch vụ (Service Layer) và ứng dụng (Application Layer), trong đó:

- Lớp an ninh cơ sở hạ tầng: Lớp an ninh hạ cơ sở hạ tầng bao gồm tập hợp các phương tiện truyền dẫn cũng như các phần tử mạng được bảo vệ bằng các biện pháp an ninh. Lớp cơ sở hạ tầng là các thành phần cơ bản xây dựng nên mạng, các dịch vụ mạng và các ứng dụng trên đó. Các thành phần thường thấy trong lớp cơ sở hạ tầng mạng đó là: router, switch và các server cũng như các tuyến truyền thông nối giữa các router, các switch và các server đó.
- Lớp an ninh các dịch vụ: Lớp an ninh dịch vụ giải quyết các vấn đề an ninh của các dịch vụ mà các nhà cung cấp đưa tới khách hàng. Những dịch vụ này bao gồm các dịch vụ truyền tải truyền tải cơ bản cũng như các dịch vụ hỗ trợ dùng để hỗ trợ các dịch vụ khác (người sử dụng sử dụng trực tiếp dịch vụ này). Một số dịch vụ hỗ trợ mà chúng ta thường thấy đó là: dịch vụ hỗ trợ người dùng truy cập Internet (các dịch vụ AAA, dịch vụ DHCP, dịch vụ DNS…); một số dịch vụ hỗ trợ giá trị gia tăng như là dịch vụ freephone, QoS, VPN, dịch vụ thông tin vị trí, dịch vụ chat…Lớp an ninh dịch vụ

được sử dụng để bảo vệ các nhà cung cấp dịch vụ và khách hàng của họ, cả 2 đối tượng này là mục tiêu của các nguy cơ. Chẳng hạn, kẻ tấn công có thể nhằm vào nhà cung cấp dịch vụ để hạn chế khả năng cung cấp dịch vụ của họ hay là làm gián đoán dịch vụ cho một khách hàng nào đó (có thể là một tổng công ty) của nhà cung cấp dịch vụ.

- Lớp an ninh các ứng dụng: Lớp an ninh ứng dụng tập trung vào an ninh cho các ứng dụng chạy trên mạng được truy nhập bởi khách hàng. Những ứng dụng này được thực thi nhờ sự hỗ trợ của các dịch vụ mạng và bao gồm một số ứng dụng điển hình như ứng dụng truyền file (chẳng hạn FTP) và các ứng dụng duyệt Web; một số ứng dụng cơ bản như là ứng dụng tra số điện thoại, ứng dụng thư điện tử và thư thoại, cũng như các ứng dụng phức tạp hơn như là: ứng dụng quản lý quan hệ khách hàng, ứng dụng thương mại điện tử, đào tạo từ xa…Các ứng dụng có thể được cung cấp bởi nhà cung cấp dịch vụ ứng dụng (ASP) thứ 3, bởi nhà cung cấp dịch vụ đóng vai trò như là các ASP, hay bởi các doanh nghiệp tự tổ chức trung tâm dữ liệu trong chính mạng của họ. Tại lớp an ninh ứng dụng này, có 4 mục tiêu tiềm năng có thể bị tấn công đó là: người sử dụng ứng dụng, nhà cung cấp ứng dụng, middleware được cung cấp bởi thành phần thứ 3 (chẳng hạn các dịch vụ web-hosting) và nhà cung cấp dịch vụ.

Các mặt phẳng an ninh

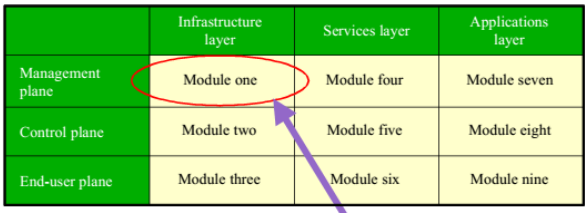
Đứng ở góc độ các hoạt động với các đối tượng có liên quan, X.805 phân chia các đối tượng tác động vào HTTT thành ba loại chính là đối tượng quản lý, đối tượng điều khiển và đối tượng người sử dụng. Tương ứng với ba đối tượng đó, X.805 phân tích an ninh một HTTT theo ba mặt phẳng:

- Mặt phẳng an ninh quản lý: Mặt phẳng an ninh quản lý liên quan đến việc bảo vệ các chức năng OAM&P của các phần tử mạng, các phương tiện truyền dẫn, các hệ thống hỗ trợ (các hệ thống hỗ trợ vận hành, hệ thống hỗ trợ kinh doanh, hệ thống hỗ trợ khách hàng…) và các trung tâm dữ liệu. Mặt phẳng an ninh quản lý hỗ trợ các chức năng liên quan đến lỗi hệ thống, dung lượng hệ thống, quản trị hệ thống, độ khả dụng và an ninh hệ thống. Cần chú ý rằng lưu lượng quản lý có thể chạy cùng hay được tách riêng khỏi lưu lượng người sử dụng.
- Mặt phẳng an ninh điều khiển: Mặt phẳng an ninh điều khiển liên quan đến việc bảo vệ các hoạt động nhằm cho phép phân bổ thông tin, các dịch vụ và ứng dụng một cách hiệu quả trên mạng. Hoạt động trong mặt phẳng điều khiển thường bao gồm các dòng thông tin giữa các thiết bị trong mạng (chẳng hạn các switch hay router) để xác định đường đi tốt nhất trong mạng. Kiểu thông tin này thường được gọi là thông tin điều khiển hay báo hiệu. Thành phần mạng dùng để vận chuyển những kiểu gói tin này có thể dùng chung hay tách rời khỏi lưu lượng người sử dụng của nhà cung cấp dịch vụ. Chẳng hạn, các mạng IP mang thông tin điều khiển chung với lưu lượng trong khi mạng PSTN mang thông tin điều khiển của nó trong một mạng báo hiệu riêng biệt (mạng SS7). Loại lưu lượng điều khiển mà chúng ta vẫn thường thấy đó là thông tin trao đổi của các giao thức định tuyến, DNS, SIP, SS7, Megaco/H.248…
- Mặt phẳng an ninh người sử dụng: Mặt phẳng an ninh người sử dụng đề cập đến các vấn đề an ninh của việc truy nhập và sử dụng mạng của nhà cung cấp dịch vụ từ phía khách hàng.Mặt phẳng này liên quan đến dòng lưu lượng của người sử dụng. Người sử dụng có thể chỉ sử mang trong việc cung cấp kết nối, cũng có thể sử dụng mạng với các dịch vụ giá trị gia tăng như là VPN, hay cũng có thể sử dụng mạng để truy cập tới các ứng dụng mạng.

Các mạng nên được thiết kế theo cách để làm sao các sự kiện xảy ra đối với mặt phẳng an ninh này được cách ly hoàn toàn với các mặt phẳng an ninh khác. Chẳng hạn, khi xảy ra việc quá tải hệ thống DNS trên mặt phẳng người sử dụng được tạo ra bởi có quá nhiều yêu cầu từ phía người sử dụng, thì hệ thống cũng không nên bị khoá ở giao diện OAM&P trong mặt phẳng quản lý, để nhà quản trị có thể truy nhập qua giao diện này vào để khắc phục.

Phân tích HTTT theo lớp và mặt phẳng an ninh

Có thể thấy với kiến trúc an ninh X.805, một HTTT bất kỳ sẽ được phân chia thành 9 module (Hình 2). Mỗi module này là một điểm giao nhau giữa một lớp và một mặt phẳng an ninh. Việc phân rã HTTT thành các module sẽ giúp cho việc phân tích các nguy cơ và tìm giải pháp đảm bảo an ninh sẽ đơn giản và chặt chẽ hơn.



Hình 2. Phân chia các module an ninh của HTTT bằng ma trận lớp – mặt phẳng

3. CÁC NGUY CƠ VÀ GIẢI PHÁP AN NINH

Các nguy cơ an ninh

Các nguy cơ được nêu ra ở đây được mô tả trong ITU-T Rec. X.800 (1991) bao gồm 5 loại:

- Phá huỷ thông tin hay các tài nguyên khác (Destruction of information & # resource)
- Sửa đổi thông tin (information corruption and modification)
- Đánh cắp thông tin hay các tài nguyên khác (theft of information)
- Làm lộ thông tin (disclosure of information)
- Làm gián đoạn dịch vụ (interuption of service)

Các giải pháp an ninh

Đứng trước các nguy cơ an ninh hiện có, các giải pháp an ninh cần thiết phải được thực hiện một cách chặt chẽ cho hệ thống. Xem xét một cách có hệ thống, có thể thấy nhìn chung các biện pháp an ninh được phân chia thành một số các giải pháp như sau:

- Điều khiển truy nhập (Access Control): Phương pháp này nhằm hạn chế và điều khiển việc truy nhập vào các phần tử mạng, các dịch vụ và các ứng dụng. Một số cơ chế phổ biến để thực hiện biện pháp này đó là: Sử dụng mật khẩu, sử dụng danh sách điều khiển truy nhập (ACL), sử dụng Firewall.
- Nhận thực người sử dụng (Authentication): Phương pháp này sử dụng nhận dạng người sử dụng để kiểm tra tính đúng đắn của người sử dụng. Một số cơ chế phổ biến để thực hiện biện pháp này mà chúng ta thường thấy đó là: sử dụng khoá chia sẻ, sử dụng hạ tầng khoá công cộng – PKI, sử dụng chữ ký số, sử dụng chứng chỉ số.
- Chứng minh tránh phủ nhận (Non-Repudation): Phương pháp này nhằn ngăn chặn khả năng người sử dụng nào đó từ chối hành động mà họ đã thực hiện vào mạng. Một số cơ chế phổ biến để thực hiện biện pháp này mà chúng ta thường thấy đó là: sử dụng cơ chế ghi lại sự kiện hệ thống, sử dụng chữ ký số.
- Bảo mật dữ liệu (Confidentiality of Data): Phương pháp này nhằm đảm bảo tính bí mật cho dữ liệu của người sử dụng tránh không được biết bởi người không mong muốn. Cơ chế phổ biến để thực hiện biện pháp này đó là: mật mã.
- Đảm bảo an toàn trong quá trình truyền dữ liệu (Communication): Phương pháp này nhằm đảm bảo dòng thông tin chỉ đi từ nguồn đến đích mong muốn, các điểm trung gian không mong muốn được biết thông tin không thể truy nhập vào dòng thông tin. Một số cơ chế phổ biến để thực hiện biện pháp này đó là: sử dụng VPN thông qua MPLS hay một số giao thức như là L2TP,…
- Đảm bảo tính toàn vẹn dữ liệu (Data Integrity): Phương pháp này nhằm đảm bảo rằng dữ liệu nhận được và được phục hồi là giống với dữ liệu đã được gửi đi từ nguồn. Một số cơ chế phổ biến để thực hiện biện pháp này mà chúng ta thường thấy đó là: sử dụng thuật toán băm MD5, sử dụng chữ ký số, hay phần mềm chống virus.
- Đảm bảo tính khả dụng (Avaiability): Phương pháp này nhằm đảm bảo cho

người sử dụng hợp lệ luôn có thể sử dụng các phần tử mạng, các dịch vụ và các ứng dụng. Một số cơ chế phổ biến để thực hiện biện pháp này mà chúng ta thường thấy đó là: sử dụng hệ thống phát hiện/ngăn ngừa truy nhập trái phép (IDS/IPS), sử dụng cơ chế dự phòng, sử dụng BC/DR (Business Continuity/Disaster Recovery).

- Đảm bảo tính riêng tư cho người sử dụng (Privacy): Phương pháp này nhằm đảm bảo tính riêng tư cho nhận dạng và việc sử dụng mạng của người sử dụng. Một số cơ chế phổ biến để thực hiện biện pháp này mà chúng ta thường thấy đó là: sử dụng NAT, sử dụng mật mã.

Quan hệ giữa các nguy cơ và giải pháp an ninh

Điểm rất độc đáo trong kiến trúc an ninh X.805 là mối quan hệ giữa các nguy cơ và giải pháp an ninh cho HTTT (Hình 3).

Security dimension	Security threat				
	Destruction of information or other resources	Corruption or modification of information	Theft, removal or loss of information and other resources	Disclosure of information	Interruption of services
Access control	Y	Y	Y	Y	
Authentication			Y	Y	
Non-repudiation	Y	Y	Y	Y	Y
Data confidentiality			Y	Y	
Communication security			Y	Y	
Data integrity	Y	Y			
Availability	Y				Y
Privacy				Y	

Hình 3. Mối quan hệ giữa các nguy cơ và giải pháp an ninh

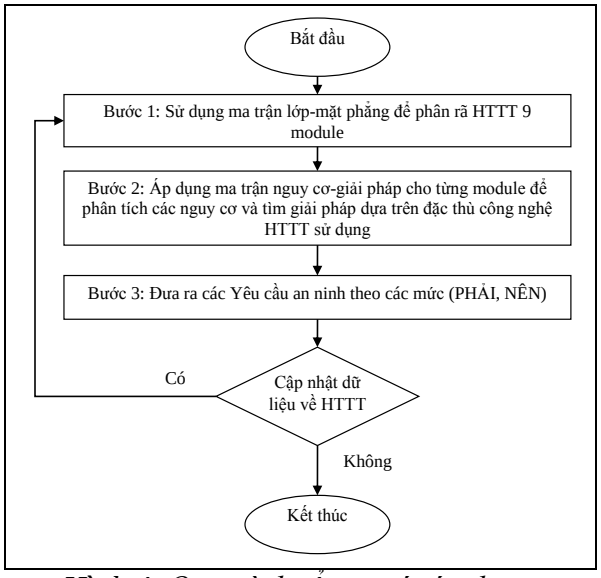
Các mối quan hệ này giúp tra cứu rất tiện lợi loại giải pháp nào có thể áp dụng (ký hiệu Y) cho mỗi loại nguy cơ an ninh mà HTTT có thể gặp phải.

Nhìn vào bảng này ta có thể thấy một số điểm đặc biệt:

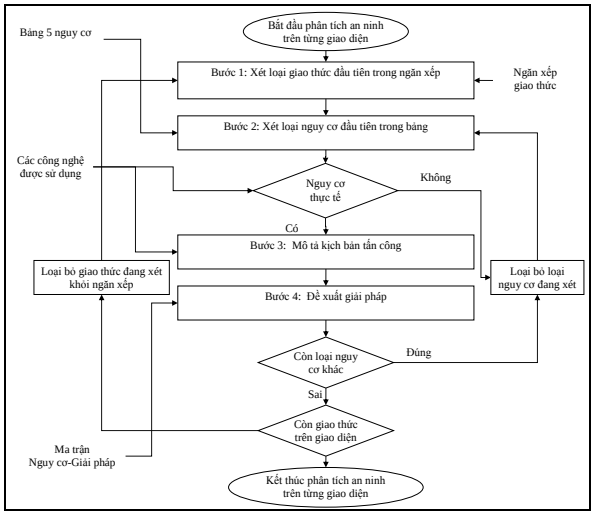
- Giải pháp *Tránh phủ nhận (Non-repudation)*: Được áp dụng cho tất cả các loại nguy cơ có thể xảy ra đối với HTTT. Đây chính là lý do các HTTT cần đảm bảo an toàn cần có cơ chế ghi log tất cả các hoạt động để truy vết khi xảy ra các sự cố an ninh thì kẻ tấn công không thể phủ nhận trách nhiệm.
- Giải pháp *Điều khiển truy nhập (Access Control)*: được sử dụng với hầu hết các nguy cơ trừ nguy cơ Gián đoạn dịch vụ mà để giải quyết nguy cơ này cần sử dụng *Avaiability*. Điểm này cần lưu ý là mục đích của *Access Control* là chặn không truy cập còn mục đích của *Avaibility* là đảm bảo không gián đoạn dịch vụ khi *Access Control* không kiểm soát.

4. ỨNG DỤNG X.805

Dựa trên Framework X.805, tác giả đã đề xuất một quy trình đơn giản áp dụng Framework này trong việc xây dựng các giải pháp an ninh cho HTTT tổng quát như trên Hình 4.



Hình 4. Quy trình tổng quát áp dụng Framework X.805 để phân tích và đề xuất giải pháp an ninh cho HTTT



Hình 5. Ví dụ chi tiết bước 2 của quy trình tổng quát áp dụng trên mạng IP/NGN

Trên thực tế kinh nghiệm áp dụng X.805, CDIT nhận thấy mỗi HTTT cụ thể có thể cần chi tiết hóa quy bước 2 thành quy trình con cho phù hợp. Ví dụ, với các mạng viễn thông đặc biệt là mạng IP/NGN thì việc phân tích an ninh chủ yếu tập trung phân tích lỗ hổng gây ra bởi các giao thức trên nền IP trên các giao diện giữa các thực thể trong mạng (*Hình 5*).

5. KẾT LUẬN

Giá trị của X.805 nằm ở tính hệ thống mà kiến trúc đã chỉ ra giúp cho công tác an ninh đặc biệt là an ninh HTTT được xử lý một cách có bài bản và toàn diện. Để dễ triển khai, CDIT đã xây dựng một số quy trình áp dụng rất cụ thể và thực tế đã chứng minh là hoạt động có hiệu quả. Từ năm 2009 đến nay, với Framework này CDiT đã xử lý hiệu quả nhiều vấn đề về an ninh trên mạng IP/NGN cũng như các hệ thống hỗ trợ điều hành sản xuất kinh doanh của Tập đoàn VNPT. Trong thời gian tới, CDIT sẽ tiếp tục đề xuất đưa vào giảng dạy nội dung này để góp phần nâng cao chất lượng ngành đào tạo An toàn thông tin của Học viện công nghệ Bưu chính Viễn thông.

6. TÀI LIỆU THAM KHẢO

1. *X.805 ITU-T Recommendation*
2. *X.509 ITU-T Recommendation*

Thông tin tác giả:

Cao Minh Thắng

Sinh năm: 1981

Lý lịch khoa học:

- Tốt nghiệp đại học ngành Điện tử Viễn thông vào các năm 2003 tại Học viện Công nghệ Bưu chính Viễn thông;
- Tốt nghiệp cao học ngành Kỹ thuật Điện tử năm 2010 tại Học viện Công nghệ Bưu chính Viễn thông;
- Hiện đang là nghiên cứu sinh ngành Kỹ thuật Điện tử tại Học viện Công nghệ Bưu chính Viễn thông;
- Hiện đang công tác tại Viện công nghệ Thông tin và Truyền thông CDIT, Học viện Công nghệ Bưu chính Viễn thông.

Lĩnh vực nghiên cứu hiện nay: Mật mã, An toàn thông tin.

Email: thangcm@ptit.edu.vn; thangcm@cdit.com.vn