Chương III

RADIUS

I. GIỚI THIỆU

7Mỗi khi một modem được nối vào một máy tính hoặc một máy chủ liên lạc (communications server) trên một mạng máy tính đoàn thể (corporate network) thì lập tức mạng này trở nên dễ bị thương tổn bởi những sự xâm phạm về an toàn bảo mật (security). Những nhà quản trị mạng (network administrators) chỉ có một số rất ít các công cụ phòng chống các cuộc tấn công này. Thêm vào đó, các hệ thống kỹ thuật an toàn của các quốc gia thường đòi hỏi những phần cứng đặc biệt và chỉ tương thích với một số ít các sản phẩm. Vấn đề này sẽ tăng lên nhiều lần trên những mạng lớn vời nhiều điểm truy xuất.

Tổ chức thương mại về những kỹ thuật truy xuất từ xa Lucent (Lucent Technologies Remote Access Business Unit) đã phát triển một giải pháp an toàn phân tán (distributed security) được gọi là dịch vụ xác nhận quyền hạn của người sử dụng truy cập từ xa (Remote Authentication Dial-In User Service hay viết tắt là RADIUS) nhằm giải quyết các vấn đề liên quan đến những yêu cầu về an toàn của việc tính toán từ xa. Giải pháp này sẽ loại bỏ đòi hỏi những phần cứng đặc biệt và cung cấp sự truy xuất vào các hệ thống kỹ thuật an toàn khác nhau. An toàn phân tán sẽ tách biệt sự xác nhận quyền hạn của người sử dụng (user authentication) và sự phân quyền (authorization) khỏi quá trình giao tiếp (communication process) và tạo ra dữ liệu xác nhận quyền của người sử dụng (user authentication data) duy nhất và tập trung.

Dựa vào mô hình đã được định nghĩa trước đó của Tổ chức các nhiệm vụ về kỹ

thuật Internet (Internet Engineering Task Force - IETF), RADIUS cung cấp một hệ thống an toàn kiểu client/server mở và có thể cải tiến (scalable). RADIUS server có thể dễ dàng sửa đổi thích ứng với những sản phẩm an toàn của các công ty thứ ba (third-party) hoặc là những hệ thống an toàn độc quyền (proprietary). Bất cứ một máy chủ giao tiếp hoặc một phần cứng mạng nào được trang bị giao thức RADIUS client đều có thể giao tiếp với một RADIUS server.

II. Kiến trúc client/server của RADIUS (RADIUS Client/Server architecture)

RADIUS là một hệ thống an toàn phân tán có chức năng đảm bảo an toàn cho việc truy cập từ xa tới một mạng và các dịch vụ mạng khỏi các truy cập bất hợp pháp. RADIUS bao gồm hai phần : trình chủ xác nhận quyền (authentication server) và các giao thức khách (client protocols). Trình chủ được cài đặt trên máy tính trung tâm khu vực của khách hàng (customer's site). RADIUS được thiết kế sao cho đơn giản hoá quá trình xử lý an toàn bằng cách tách rời kỹ thuật xử lý an toàn (sercurity technology) và kỹ thuật giao tiếp (communications techonology).

Thông tin tất cả quyền hạn của user và khả năng truy xuất các dịch vụ mạng được chứa trên máy chủ xác nhận quyền (hay RADIUS). Những thông tin này được lưu ở những dạng phù hợp với yêu cầu của khách hàng. RADIUS sẽ xác nhận quyền của các user đối với tập tin mật mã (UNIX password file), NIS (Network Information Service) và cả một cơ sở dữ liệu của RADIUS được quản lý một cách riêng biệt. Các máy chủ giao tiếp (Communications servers) làm việc với các modems như là những RADIUS clients. RADIUS client gởi các yêu cầu xác nhận quyền cho RADIUS server và thực thi dựa trên các kết quả trả lời gởi về từ server.

III. RADIUS hoạt động như thế nào: sự xác nhận quyền của user với RADIUS.

RADIUS xác nhận quyền các user thông qua một chuỗi các giao tiếp giữa client và

server. Mỗi khi một user đã được xác nhận quyền, client sẽ cho phép user đó truy cập các dịch vụ mạng tương ứng. Sau đây là sự mô tả quá trình xác nhận quyền sử dụng máy chủ giao tiếp (communications server) và RADIUS.

User sẽ gọi modem để nối vào máy chủ giao tiếp. Khi mối nối modem được thực hiện xong, máy chủ giao tiếp sẽ yêu cầu user nhập tên và mật mã vào từ dòng lệnh nhắc.

Máy chủ giao tiếp (communications server) sẽ tạo ra một gói dữ liệu từ những thông tin này được gọi là một yêu cầu xác nhận quyền (authentication request). Gói dữ liệu này chứa thông tin nhận dạng máy chủ giao tiếp gởi yêu cầu xác nhận này, cổng (port) được sử dụng cho mối nối modem, tên user (username) và mật khẩu (password). Để tránh khỏi bị nghe trộm (eavesdropping), máy chủ giao tiếp, như là một RADIUS client, sẽ mã hoá (encrypting) mật khẩu trước khi nó được gởi đi trên đường truyền đến RADIUS server.

Yêu cầu xác nhận quyền (authentication request) được gởi đi trên mạng từ RADIUS client đến RADIUS server. Sự giao tiếp này có thể được thực hiện trên mạng cục bộ (local area network - LAN) hay trên mạng diện rộng (wide area network - WAN), cho phép các quản trị viên mạng (network managers) định vị từ xa các RADIUS clients từ RADIUS server. Nếu RADIUS server không thể được nhận ra, do hỏng hóc chẳng hạn, thì RADIUS client sẽ định lại hướng đi cho yêu cầu xác nhận quyền đến một server dự phòng (alternate server).

Sau khi nhận được yêu cầu xác nhận quyền, máy chủ kiểm tra quyền (authentication server) sẽ kiểm tra tính hợp lệ (validating) yêu cầu và giải mã (decrypting) gói dữ liệu để lấy thông tin về tên người sử dụng và mật khẩu. Thông tin này sẽ được gởi đến cho hệ thống an toàn (security system) tương ứng, như những tập tin mật khẩu của UNIX (UNIX password files), Kerberos, một hệ thống an toàn thương mại (commercial) hoặc

thậm chí do khách hàng phát triển (custom developed).

Nếu tên người dùng và mật khẩu là đúng thì server sẽ gởi một phản hồi nhận biết xác nhận quyền (authentication acknowledgment) chứa thông tin về hệ thống mạng và các yêu cầu dịch vụ của người dùng. Ví dụ như, RADIUS server sẽ báo cho máy chủ giao tiếp biết rằng người dùng cần TCP/IP và/hoặc NetWare sử dụng PPP (Point to Point Protocol) hoặc SLIP (Serial Line Internet Protocol) để nối với mạng. Phản hồi nhận biết (acknowledgment) thậm chí có thể chứa thông tin sàng lọc (filtering infomation) giới hạn sự truy cập của người dùng tới những tài nguyên (resources) cụ thể trên mạng.

Nếu tại bất cứ lúc nào trong quá trình đăng ký vào mạng (log-in process) các điều kiện không được thỏa, thì RADIUS server sẽ gởi một thông báo từ chối xác nhận quyền (authentication reject) đến máy chủ giao tiếp và user bị từ chối truy cập vào mạng.

Để đảm bảo các yêu cầu sẽ không dược trả lời đối với những người không được phép (unauthorized hackers), RADIUS server sẽ gởi khóa xác nhận quyền (authentication key) hoặc chữ ký (signature) để tự xác minh với RADIUS client. Mỗi lần thông tin này được nhận bởi máy chủ giao tiếp, nó sẽ cho phép cấu hình cần thiết để phân phát những dịch vụ mạng hợp lệ cho người dùng.

IV. Những lợi ích của an toàn phân tán (Benefits of Distributed Security)

Giải pháp phân bố cho an toàn mạng (network security) đưa đến nhiều lợi ích.

- ***An toàn hơn (Greater security)***

Kiến trúc chủ/khách của RADIUS cho phép tất cả thông tin an toàn được nằm trong một cơ sở dữ liệu tập trung đơn lẻ thay vì được phân phát ở các thiết bị khác nhau trên mạng. Giải pháp này sẽ tăng độ an toàn. Một hệ thống UNIX đơn lẻ sẽ dễ dàng hơn nhiều khi chạy RADIUS so với nhiều máy chủ giao tiếp rải rác khắp toàn mạng.

- ***Dễ nâng cấp (Scalable architecture)***

RADIUS tạo ra một cơ sở dữ liệu đơn lẻ, được định vị tập trung của các user và các dịch vụ cho phép. Đây là một tính chất đặc biệt quan trọng đối với những mạng có ngân hàng modem lớn và có nhiều hơn một máy chủ giao tiếp. Với RADIUS, thông tin của user được lưu ở một nơi duy nhất là RADIUS server cho phép quản lý sự xác nhận quyền của user và sự trup cập các dịch vụ từ một vị trí duy nhất. Bởi vì bất cứ một thiết bị nào có trang bị RADIUS đều có thể là RADIUS client, cho nên một user từ xa sẽ có thể truy cập vào cùng dịch vụ từ bất cứ máy chủ giao tiếp nào kết nối với RADIUS server.

- ***Giao thức mở (Open protocols)***

RADIUS mở hoàn toàn, được phân phối ở dạng mã nguồn và có thể dễ dàng chỉnh sửa để làm việc được với các hệ thống và giao thức đã tồn tại. Đặc tính này tiết kiệm rất nhiều thời gian bằng cách cho phép user thay đổi RADIUS server so cho phù hợp với mạng của họ hơn là phải sửa đổi lại mạng sao cho phù hợp máy chủ giao tiếp. RADIUS có thể được thay đổi để sử dụng được với bất cứ một hệ thống an toàn nào có trên thị trường và làm việc được với bất cứ thiết bị giao tiếp nào có trang bị giao thức RADIUS client. RADIUS server có những phần có thể thay đổi (modifiable stubs) mà khách hàng có thể chỉnh sửa phù hợp để có thể chạy được với bất kỳ kỹ thuật an toàn (security technology) nào.

- ***Sự nâng cao trong tương lai (future enhancement)***

Khách hàng có thể lợi dụng các kỹ thuật an toàn mới mà không cần phải đợi Lucent cung cấp thêm kỹ thuật này vào máy chủ giao tiếp. Kỹ thuật an toàn mới chỉ cần được trực tiếp thêm vào RADIUS server bởi khách hàng hoặc ngoài tài nguyên cũng được. RADIUS cũng sử dụng một kiến trúc mở rộng ở chổ khi mà kiểu và độ phức tạp của dịch vụ mà máy chủ giao tiếp phải cung cấp tăng lên, thì RADIUS có thể được mở rộng dễ dàng để cung cấp các dịch vụ này.

I. Ai đang sử dụng RADIUS (Current users of RADIUS)

Bất kỳ công ty nào có một phòng quản lý hệ thống thông tin tập trung (centralized MIS department) quản lý một mạng máy tính cộng đồng "đông dân cư" đều liên quan đến vấn đề an toàn. Nhiều khách hàng này đã cài đặt RADIUS hoặc đang dự định. Họ đã chỉnh sửa RADIUS sao cho làm việc được với mạng hiện tại. Ví dụ, một hãng sản xuất máy tính đã chỉnh sửa RADIUS server sao cho làm việc được với mạch an toàn (security card) của Enigma. Trong mạng này RADIUS server quản lý sự giao tiếp với kỹ thuật an toàn của Enigma để xác nhận tính hợp lệ của user và cho phép truy cập vào mạng. Theo cách này, họ có thể cài đặt máy chủ giao tiếp mà vẫn bảo toàn được sự đầu tư của họ vào kỹ thuật an toàn của Enigma.

RADIUS cũng được dùng cho các mạng của trường đại học mà có cung cấp kết nối kiểu gọi IP (Dial-In IP Connectivity) cho các sinh viên hoặc các khoa. Để cung cấp an toàn phân tán (distributed security), RADIUS server phải được chỉnh sửa sao cho làm việc được với hệ thống an toàn Kerberos để xác nhận tên người dùng và mật khẩu.

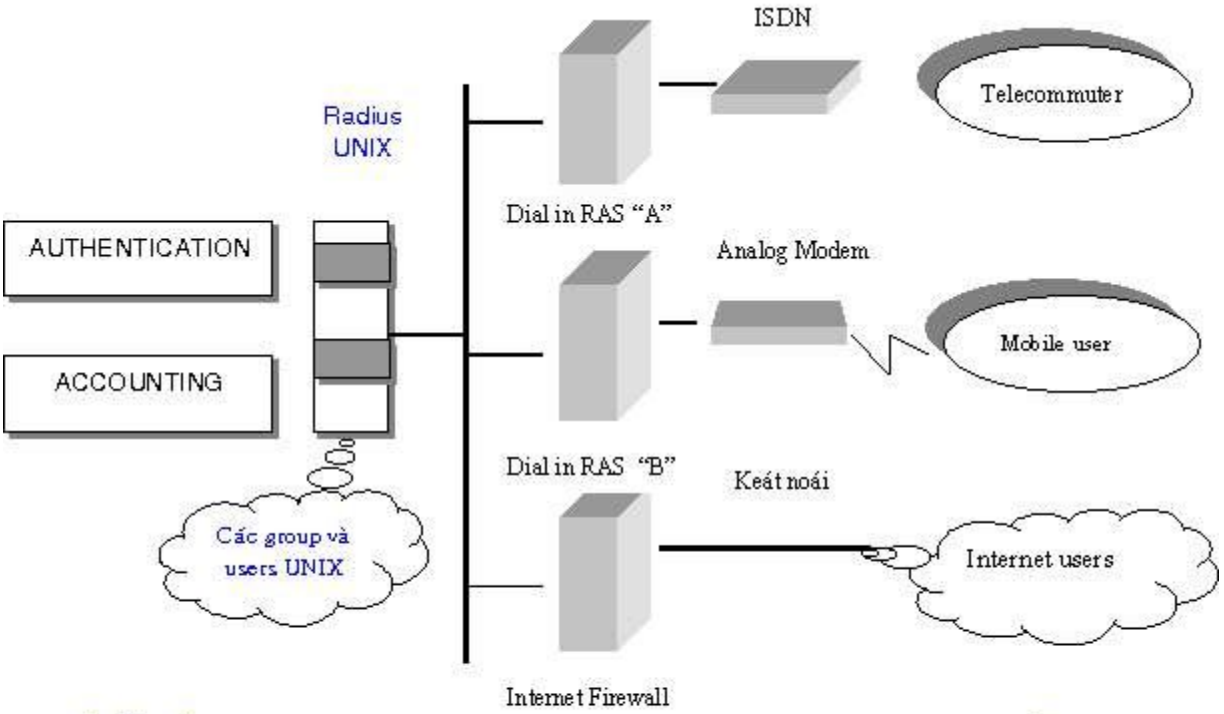
Nhiều ISP (Internet Service Provider) cũng sử dụng RADIUS để cung cấp chế độ bảo vệ an toàn cho các khách hàng truy cập vào mạng của họ từ nhiều POP (Point Of Presence) - điểm truy cập - khác nhau. Các hệ thống an toàn của UNIX được đặc trưng sử dụng cho các môi trường như vậy.

Ngoài ra các công ty phục vụ công cộng (utility company) đã sửa RADIUS theo cùng một kiểu, đó là lưu trữ tên và mật khẩu ở trên hơn 1000 bảng mật khẩu của UNIX (Unix password table).

II. RADIUS là một chuẩn (RADIUS as a standard)

Nhóm nghiên cứu về RADIUS của IETF (Internet Engineering Task Force) đã công bố vào

tháng giêng 1996 xác nhận giao thức RADIUS là một chuẩn về giải pháp an toàn gọi từ xa của IETF (RFC #2058).



Mô hình Radius