TÍCH HỢP CƠ SỞ HẠ TẦNG KHÓA CÔNG KHAI - Giải pháp hiệu quả trong việc tăng cường bảo mật giao dịch thư điện tử

Đào Ngọc Chiến, Ngô Văn Thành, Tống Việt Hùng
Trung tâm Nghiên cứu và Phát triển quốc gia về công nghệ mở
Bộ KH&CN

Thư điện tử đóng vai trò quan trọng trong trao đổi thông tin hàng ngày nhưng lại ẩn chứa nhiều nguy cơ mất an toàn. Với mong muốn xây dựng hệ thống thư điện tử tin cậy, giúp dễ dàng chủ động trong triển khai, bảo dưỡng, nâng cấp và phát triển, Trung tâm Nghiên cứu và Phát triển quốc gia về công nghệ mở (RDOT) đã nghiên cứu, chỉnh sửa và tối ưu hóa trên nền tảng công nghệ nguồn mở để tích hợp cơ sở hạ tầng khóa công khai (PKI) vào hệ thống thư điện tử máy chủ và máy trạm. Giải pháp này hứa hẹn sẽ đem đến hệ thống thư điện tử tin cậy, tiết kiệm chi phí bản quyền, đồng thời giúp các đơn vị chủ động trọng việc tùy biến, bảo dưỡng, nghiên cứu, phát triển hệ thống cho các yêu cầu cao hơn, góp phần tăng cường tính bảo mật trong giao dịch thư điện tử ở Việt Nam hiện nay.

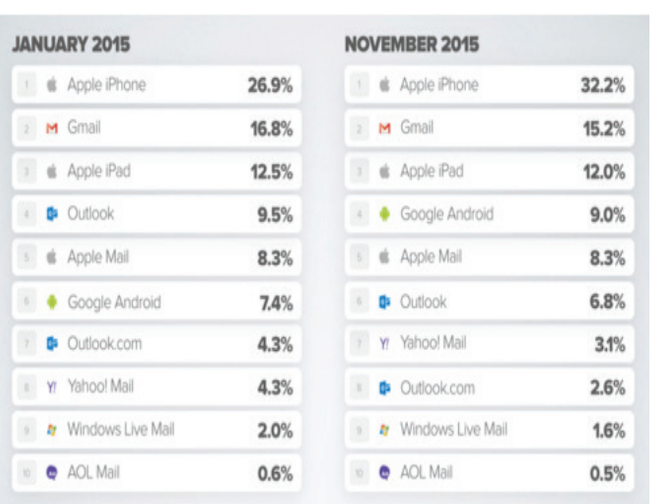
Thực trạng sử dụng các hệ thống thư điện tử

Các dịch vụ trên public cloud

Ngày nay các hệ thống webmail đang bùng nổ về số lượng người dùng với khả năng lưu trữ từ xa vượt trội và đặc biệt là hoàn toàn miễn phí. So sánh các số liệu thống kê của trang limus.com ở tháng 1 và tháng 11/2015 ta sẽ nhận ra sự thay đổi lớn với các hệ thống thư điện tử lớn như Apple iPhone, Gmail, Android (hình 1). Theo đó, Apple iPhone tiếp tục được phổ biến, tăng trưởng 5,3% trong cả năm, trong khi Outlook có sự sụt giảm về số lượng người dùng, giảm 1,7%.

Mặc dù được người dùng phổ thông rất ưa chuộng nhưng đối với những doanh nghiệp hay cơ quan thì các hệ thống webmail lại không phải là một giải pháp hay. Các hệ thống webmail yêu cầu người dùng luôn phải online trong quá trình làm việc, nghĩa là hoàn toàn phụ thuộc vào băng thông quốc tế. Nếu băng thông bị ngưng trệ do bảo trì hoặc trục trặc, người dùng sẽ gặp rất nhiều khó khăn trong việc sử dụng hệ thống thư của mình, làm ảnh hưởng tới tiến độ công việc. Webmail thường bị giới hạn về tốc độ và tính năng so với những hệ thống email khác, một phần do sự hạn chế của HTML (trang web).

Sẽ là rất khó nếu muốn sử dụng các hệ thống webmail trong các cơ quan nhà nước vì nhiều vấn đề liên quan đến bảo mật. Những nhà cung cấp dịch vụ webmail sẽ kiểm soát toàn bộ hệ thống, điều này đồng nghĩa với việc người sử dụng hoàn toàn bị phụ thuộc vào nhà cung cấp dịch vụ. Đây là vấn đề rất nguy hiểm với những cơ quan cần đảm bảo an toàn cho thông tin khi mà các hệ thống webmail luôn bị đánh giá là không an toàn và là mục tiêu của spam. Đa phần các hệ thống webmail không cho phép người sử dụng tự cài đặt thêm các phần mềm bảo mật, diệt virus, chặn thư rác khác.



Hình 1. Tỷ lệ sử dụng các hệ thống thư điện tử năm 2015.

Các hệ thống thư điện tử dùng riêng

Các hệ thống thư điện tử được dùng riêng cho các doanh nghiệp, cơ quan nhà nước gồm rất nhiều loại, tuy nhiên có thể chia làm 2 loại chính sau:

Các hệ thống thư điện tử thương mại nguồn đóng: Được các doanh nghiệp ưa chuộng vì khả năng bảo mật cao và thường được sử dụng thêm nhiều tính năng từ các phần mềm cộng tác của nhà sản xuất, trong đó 2 hệ thống được ưa chuộng nhất là Microsoft Exchange và MDaemon. Đây là 2 hệ thống email có nhiều tính năng vượt trội như: Duy trì kiểm soát, các tính năng làm việc nhóm, các tính năng chống virus, thư rác, tấn công lừa đảo… Trong khi Exchange được rất nhiều doanh nghiệp lớn như ADVA Optical Networking SE, Dar Al-Handasah, Đại học King Saud, Midroc Europe, MedcoEnergi Internasional… sử dụng thì MDaemon lại phù hợp hơn với những doanh nghiệp vừa và nhỏ (dưới 500 nhân viên). Tuy nhiên, các hệ thống kiểu này có nhược điểm là chi phí đầu tư lớn. Chi phí cho một hệ thống Mail Exchange không dưới 10.000 USD và còn tăng tùy thuộc vào số lượng email account mà doanh nghiệp muốn tạo cho các nhân viên, còn với MDaemon mặc dù giá thành thấp hơn nhưng chi phí triển khai cho khoảng 100 users cũng tiêu tốn khoảng 3.000-5.000 USD. Mặc dù tính bảo mật cao, nhưng những hệ thống này không có kiến trúc mở, gây khó khăn cho người dùng khi muốn chỉnh sửa, mở rộng các tính năng bảo mật.

Các hệ thống thư điện tử nguồn mở: Được xây dựng xung quanh một MTA (Mail Transfer Agent) mã nguồn mở. Các hệ thống thư điện tử mã nguồn mở được xây dựng, đóng gói sẵn, có đầy đủ các tính năng, hoàn toàn miễn phí, và quan trọng hơn là người sử dụng có thể tùy ý chỉnh sửa hệ thống, mở rộng chức năng bảo mật. Ngoài ra, những hệ thống mã nguồn mở nổi tiếng còn nhận được sự hỗ trợ toàn diện của cộng đồng người sử dụng trên toàn thế giới. Có rất nhiều hệ thống thư điện tử mã nguồn mở đang được sử dụng trên thế giới, tiêu biểu như: Zimbra (được xây dựng bởi cộng đồng phần mềm tự do nguồn mở và Công ty VMWare, hiện có trên 500 triệu người sử dụng). Zimbra đơn giản hóa việc liên lạc, tăng cường khả năng quản trị trên đám mây công cộng cũng như đám mây riêng, tiện dụng hơn cho người dùng thư điện tử, sổ địa chỉ và lịch. Rất nhiều các cơ quan, tổ chức không chỉ tư nhân mà cả chính phủ đã sử dụng Zimbra làm hệ thống thư điện tử. Một ứng dụng khác là RoundCube được một số trường đại học sử dụng để cung cấp dịch vụ thư điện tử cho sinh viên và nhân viên. Mặc dù những hệ thống này có tính bảo mật kém hơn so với những hệ thống thư điện tử thương mại, nhưng với kiến trúc mở, người dùng hoàn toàn có thể tích hợp thêm những phần mềm bảo mật từ những nhà cung cấp khác. Ngoài ra, những hệ thống này là hoàn toàn miễn phí và cũng không đòi hỏi cấu hình máy tính mạnh.

Giải pháp tích hợp hạ tầng khóa công khai trong bảo mật thư điện tử

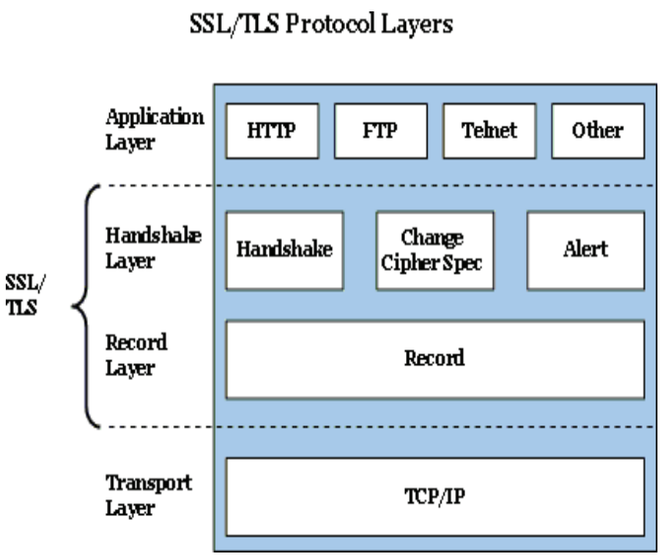
Khi việc sử dụng thư điện tử (email) ngày càng được coi trọng, phổ biến trong các hoạt động kinh tế, xã hội đồng nghĩa với việc bùng nổ các nguy cơ lừa đảo, can thiệp, tấn công, phá hoại hoặc vô tình tiết lộ các thông tin của doanh nghiệp, người sử dụng. Việc đưa ra cấu trúc hạ tầng PKI (Public Key Infrastructure) cùng các tiêu chuẩn và công nghệ ứng dụng của nó có thể được coi là một giải pháp tổng hợp và độc lập giải quyết vấn đề này.

Khái niệm PKI thường được dùng để chỉ toàn bộ hệ thống bao gồm nhà cung cấp chứng thực số (Certificate Authority) cùng các cơ chế liên quan đồng thời với toàn bộ việc sử dụng các thuật toán mã hóa khóa công khai trong trao đổi thông tin. PKI bản chất là một hệ thống công nghệ vừa mang tính tiêu chuẩn, vừa mang tính ứng dụng được sử dụng để khởi tạo, lưu trữ và quản lý các chứng thực điện tử (digital certificate) cũng như các mã khoá công cộng và cá nhân.

Tích hợp hạ tầng PKI vào các hệ thống thư điện tử để đảm bảo an toàn cho các giao dịch điện tử không mới tại Việt Nam và trên thế giới. Nhưng với mong muốn xây dựng hệ thống thư điện tử tin cậy, giúp dễ dàng chủ động trong triển khai, bảo dưỡng, nâng cấp và phát triển, RDOT đã nghiên cứu, chỉnh sửa và tối ưu hóa trên nền tảng công nghệ nguồn mở để tích hợp vào hệ thống thư điện tử máy chủ và máy trạm. Giải pháp này hứa hẹn sẽ đem đến hệ thống thư điện tử tin cậy, tiết kiệm chi phí bản quyền, đồng thời giúp các đơn vị chủ động trong việc tùy biến, bảo dưỡng, nghiên cứu, phát triển hệ thống cho các yêu cầu cao hơn. Có thể kể đến một số tính năng nổi bật của hệ thống như:

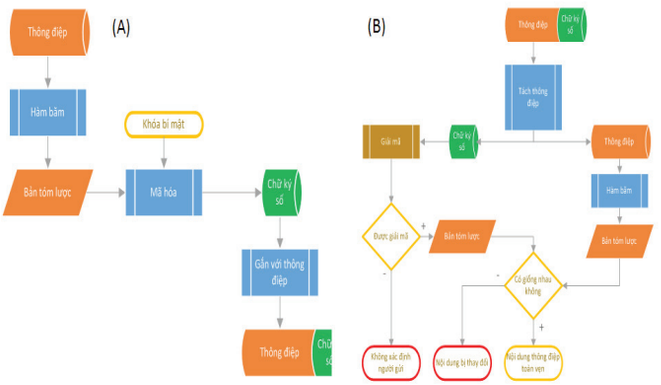
Sử dụng giao thức truyền thông có bảo mật (HTTPS): Là tổ hợp giao thức truyền thông siêu văn bản (HTTP) và SSL/TLS để cung cấp dịch vụ truyền thông được mã hóa và xác thực an toàn cho máy chủ web thư điện tử. Sự đảm bảo an toàn, bảo mật được

thiết lập trên cơ sở các cơ quan chứng thực điện tử được cài đặt trước trên trình duyệt. SSL/TLS hoạt động ở tầng phụ thấp hơn tầng ứng dụng trong mô hình OSI, tất cả nội dung trong thông điệp đều được mã hóa (kể cả tiêu đề) nên đảm bảo độ tin cậy rất cao. Để máy chủ tiếp nhận liên kết HTTPS cần tạo một khóa công khai cho máy chủ web. Chứng thư cấp cho khóa ngày được ký xác nhận bởi một công nghệ chữ ký số (CA - Certification Authorities) đáng tin cậy. CA chứng nhận rằng máy chủ được cấp chứng thư là thực thể đúng với thông tin đăng ký. Các trình duyệt có thể thẩm định được các chứng thư do những CA ký xác nhận.



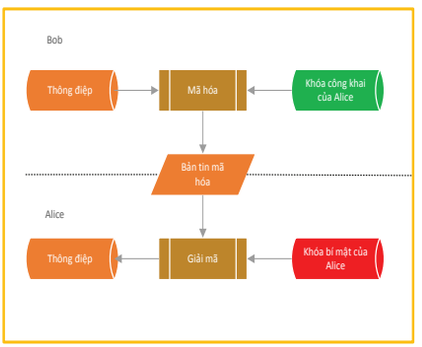
Hình 2. Hoạt động của giao thức SSL/TLS.

Ký, mã hóa xác thực thư điện tử: Bằng việc sử dụng chứng thực cá nhân, người sử dụng sẽ ngăn ngừa được các nguy cơ mất an toàn mà không ảnh hưởng đến những ưu điểm của thư điện tử. Với chứng chỉ số cá nhân, người sử dụng có thể tạo thêm một chữ ký điện tử vào email như một bằng chứng xác nhận của mình. Chữ ký điện tử là đoạn dữ liệu, đính kèm với thông điệp để chứng minh danh tính của người gửi thông điệp và giúp người nhận kiểm tra tính toàn vẹn của nội dung thông điệp gốc. Một trong những cách phổ biến nhất hiện nay để tạo ra một chữ ký số là sử dụng mật mã khóa công khai. Quá trình sử dụng chữ ký số bao gồm 2 quá trình: Tạo chữ ký và kiểm tra chữ ký.



Hình 3. Quy trình tạo (A) và kiểm tra (B) chữ ký số.

Mã hóa và giải mã thư điện tử: Khi không mã hóa, email có nguy cơ bị xâm nhập và đọc trộm bất cứ lúc nào, hoặc có thể bị mất tài khoản. Bên cạnh việc "chặn bắt" nội dung email và các tập tin đính kèm, những kẻ lừa đảo còn có thể chiếm toàn bộ tài khoản email khi không có cách bảo mật hợp lý. Để bảo mật email hiệu quả, giải pháp của RDOT đã mã hóa: (i) Kết nối từ nhà cung cấp dịch vụ email; (ii) Nội dung email gửi đi; (iii) Nội dung email được lưu trữ.



Hình 4. Hình minh họa mã hóa và giải mã thư điện tử.

Tích hợp PKI trên hệ thống thư điện tử Zimbra nguồn mở: Hệ thống thư điện tử Zimbra với tính ưu việt về bảo mật cao, chất lượng phần mềm tốt, tính linh hoạt, tính tùy biến cao được RDOT nghiên cứu tích hợp với hạ tầng khóa công khai để sử dụng chứng thư số và các dịch vụ chứng thực chữ ký số bảo mật và xác thực cho nội dung thư điện tử. Hệ thống PKI này sẽ cấp phát chứng thư số cho các người dùng trong hệ thống thư điện tử, các chứng thư số này sẽ được sử dụng để xác thực và bảo mật thư điện tử. Hệ thống được RDOT thử nghiệm thành công và phát hành miễn phí, bổ sung thêm lựa chọn cho hệ thống thư điện tử an toàn cho lĩnh vực hành chính công ✍