PHƯƠNG PHÁP MỚI NHẰM BẢO VỆ DỮ LIỆU CÁ NHÂN.

Các công ty và tổ chức giữ những thông tin nhạy cảm của hàng triệu người Mỹ đã và đang trở thành những mục tiêu hấp dẫn cho các tin tặc trong những năm gần đây, gây ra việc hàng triệu đôla trong kinh doanh bị mất đi và gây khốn đốn cho vô

Các công ty và tổ chức giữ những thông tin nhạy cảm của hàng triệu người Mỹ đã và đang trở thành những mục tiêu hấp dẫn cho các tin tặc trong những năm gần đây, gây ra việc hàng triệu đôla trong kinh doanh bị mất đi và gây khốn đốn cho vô số khách hàng. Nhưng hiện nay Amit Sahai, một phó giáo sư về tin học tại UCLA Henry Samueli School of Engineering and Applied Science cùng với đồng nghiệp của ông đang phát minh ra một phương pháp bảo vệ dữ liệu mới mà họ hy vọng sẽ khiến cho các tin tặc phải bó tay.

Cùng với các tác giả Brent Waters, một sinh viên tin học và Jonathan Katz của đại học Maryland, Sahai đã nghĩ ra một hệ thống toán học được biết đến như là mã hóa chức năng mà sẽ không chỉ giúp đơn giản hoá việc mã hoá dữ liệu trong các máy chủ mà cũng sẽ cho phép truy cập dữ liệu theo trực giác và điều này khiến cho các hacker khó khăn hơn trong việc thâm nhập vào thông tin nhạy cảm nhưng lại dễ dàng hơn cho các nhà lập trình trong việc bảo mật thông tin.

Dù phương pháp này chưa có mặt trên thị trường nhưng nó đã nhận được sự quan tâm lớn từ cộng đồng bảo mật dữ liệu. Nghiên cứu đã được giới thiệu tại hội nghị ở Istanbul.

Trong hội nghị đó Sahai và các đồng nghiệp cho rằng vấn đề lớn nhất trong bảo mật thông tin ngày nay đó là thế giới trông cậy vào các máy chủ đáng tin cậy để lưu trữ và bảo mật dữ liệu.

Sahai cho biết “Máy chủ đáng tin cậy này là một mô hình đơn giản và dễ thực hiện. Thông tin được lưu trong máy chủ và máy chủ có nhiệm vụ quyết định ai sẽ có dữ liệu đó. Bởi vì sự đơn giản trong lập trình, những máy chủ này trở nên phổ biến và là những mục tiêu chủ yếu”.

(Ảnh: freewebs.com)

Theo các tác giả ,một vấn đề nữa với các máy chủ đó là khuynh hướng tái tạo dữ liệu với quy mô lớn.

Waters cho biết "Để tạo ra sức mạnh và tính sẵn sàng thì dữ liệu được lưu trữ trên một vài máy chủ đáng tin cậy như các bản sao . Nếu một máy chủ hư thì máy khác có thể truy cập được. Có một thoả hiệp giữa tính sẵn sàng cũng như tính an toàn của giữ liệu. Máy chủ càng phức tạp thì càng có nhiều mục tiêu cho các tin tặc."

Theo một phân tích FBI 2007, tội phạm Internet đã làm cho việc kinh doanh của Mỹ mất mát đến 67 triệu đôla hàng năm, bao gồm chi phí trực tiếp cho việc sửa chữa những hệ thống bị thâmnhập. TJX, công ty mẹ của chuỗi cửa hàng quần áo giảm giá T.J. Maxx và Marshalls đã tiết lộ rằng trong suốt khoảng thời gian 18 tháng trở lại đây, các tin tặc đã lấy trộm đi 45,6 triệu số thẻ tín dụng và các thông tin khách hàng nhạy cảm khác. Trong hai người Mỹ thì có một hồ sơ cá nhân bị đánh cắp.

Sahai cho biết cách viết mật mã được xem như một nhánh của cả toán học và tin học và liên quan chặt chẽ với lý thuyết thông tin, an toàn máy tính và kỹ thuật. Trong khi kỹ thuật mã hoá lâu nay đã nổi bật thì mã hoá dữ liệu và việc quyết định việc cho phép truy cập thông tin như thế nào cho hàng trăm hay hàng ngàn người vẫn đang là một nan giải.

Ông nói "Nghĩ rằng xem việc mã hoá hiện nay như là khóa và thìa khoá.Dữ liệu đã bị khoá lại và để cho phép nhiều người truy cập thì cần phải làm nhiều bản sao của thìa khoá. Khoảng 10 ngàn người cần truy cập một tập tin thì vì thế bạn làm 10 ngàn bản sao thìa khoá. Với hàng triệu tập tin và hàng ngàn thìa khoá cho một tập tin thì bạn có thể tưởng tưởng nó phức tạp thế nào. Càng phức tạp để quản lý thông tin. Vì thế mặc dù chúng ta đang có được kỹ thuật mã hoá chắc chắn hàng thập kỷ nhưng nó đã không được dùng đúng"

Phương pháp mã hoá chức năng mới của các tác giả của cuộc nghiên cứu cho phép một lập trình viên cài đặc điểm của anh ta cho thông tin. Hệ thống toán học sẽ cho ra một tập tin đã được mã hoá mà chỉ người nào hợp với đặc điểm mới có thể giải mã. Hệ thống phức tạp quản lý nhiều khoá nay được đơn giản hoá và các máy chủ giữ những thông tin đã được mã hoá chính các máy chủ không thể đọc được. Thông tin giống như vô nghĩa đối với các tin tặc.
Ngoài ra, hệ thống toán học mới cho phép các chìa khoá được cá nhân hoá có nghĩa là chỉ cần một chìa khoá để mở tất cả thông tin có sẵn cho cá nhân đó.

Sahai cho biết đây là sáng kiến then chốt trong hệ thống. Chúng ta có phương pháp toán học này để ngẫu nhiên hoá các chìa khoá đã cá nhân hoá để sao cho chìa khoá cá nhân của bạn không phụ thuộc vào thuộc tính bạn có ví dụ như tên của bạn.
Hệ thống hạn chế tối đa những gì một tin tặc có thể làm được. Nếu anh ta là một thành viên, anh ta bì hạn chế với những truy cập anh ta có và vì các thìa khoá đã được cá nhân hoá, việc tìm ra ai đã truy cập và đưa thông tin ra ngoài đầu tiên trở nên dễ dàng hơn.

Sahai và Waters được coi như là những người sáng lập ra việc mã hoá chức năng. Sahai gần đây đã nhận giành được tài trợ nghiên cứu Okawa có uy tín.

Sahai cho biết "Một vài công việc cho công trình này đang được tiến hành và thật sự đang được hợp tác trở thành các hệ thống nghiên cứu. Nó đang chuẩn bị thành hiện thực. Brent và tôi có đã

có thể đăng ký bằng sáng chế ngay khi bắt đầu công việc và đã được một công ty mua. Chắc chắn quân đội và Cơ quan an ninh của Mỹ cũng quan tâm đến công trình này.”

Theo Waters “Mục đích của chúng tôi là cân nhắc lại mã hoá nào. Trong nhiều năm, con người có cái nhìn cứng nhắc về mã hoá. Những gì chúng tôi hy vọng làm là cho mọi người thấy được chúng tôi có thể làm ra những hệ thống mạnh và đơn giản hơn nhiều bằng cách thay đổi cách chúng ta nghĩ. Cuối cùng chúng tôi hy vọng bỏ đi những thành phần phức tạp và làm những cái đơn giản hơn mà an toàn hơn và mang lại lợi nhuận."

Ngoài vệc xuất hiện trong hội nghị Eurocrypt thì nghiên cứu sẽ xuất hiện trong số báo tới của Journal of Cryptography.