XÁC THỰC VÀ ĐỊNH DANH AN TOÀN - CÔNG NGHỆ U2F

SECURE AUTHENTICATION AND IDENTIFICATION - UNIVERSAL SECOND FACTOR (U2F) TECHNOLOGIES

TỐNG HÙNG ANH(*)

TÓM TẮT: *Tên người dùng/mật khẩu là cơ chế xác thực cho các dịch vụ dựa trên Internet - nhưng không an toàn! Chúng tôi chỉ ra cơ chế xác thực và định danh mới tập trung vào khả năng sử dụng và bảo mật nhờ công nghệ xác thực hai yếu tố có thể sử dụng ở mọi nơi, công nghệ U2F của Hiệp hội Công nghiệp xác thực mở được gọi là Liên minh FIDO (Fast IDentity Online Alliance).*

Từ khóa: *xác thực và định danh an toàn.*

ABSTRACT*: Username/password is still the authentication mechanism for Internet based services - but it is not secure enough! The study identified a new authentication and identification mechanism that focuses on usability and security with two-factor authentication technology that can be used anywhere, the FIDO Alliance (Fast IDentity Online Alliance) U2F technology.*

Key words: *secure authentication and identification.*

1. ĐẶT VẤN ĐỀ

Làm thế nào để cải thiện việc xác thực người dùng trên các dịch vụ trực tuyến mà không ảnh hưởng đến khả năng sử dụng của người dùng và ở mọi dịch vụ trực tuyến của họ? Một cách lý tưởng, xác thực và định danh an toàn phải đáp ứng cùng lúc tất cả yêu cầu từ người dùng (cá nhân, công ty, doanh nghiệp) và các nhà cung cấp dịch vụ trực tuyến: phương pháp chứng thực mạnh, tính riêng tư, tính khả dụng, kể cả khả năng sử dụng và khả năng tương tác giữa các thiết bị xác thực khác nhau. Giải quyết những vấn đề này Liên minh FIDO được hình thành tháng 7 năm 2012.

Bài báo này chúng tôi muốn giới thiệu bạn đọc công nghệ U2F là một chuẩn xác thực mở cho phép người sử dụng Internet ngay lập tức truy cập an toàn bất kỳ dịch vụ trực tuyến nào, với một thiết bị duy nhất và không có trình điều khiển, hoặc phải cài phần mềm hỗ trợ nào trên mày tính của người dùng ở đầu cuối.

2. NỘI DUNG

2.1. Xác thực người dùng mạnh trên các dịch vụ trực tuyến

Xác thực chia sẻ nâng cao (Enhanced Shared-Secret Authentication) được hiểu là các phần mở rộng của chứng thực dựa trên kiến thức thông thường (Single-Factor Authentication). Ví dụ: mật khẩu bổ sung, khóa trang web, các biểu tượng đồ họa chúng phải được kiểm tra trước khi hỗ trợ

(*)ThS. Trường Đại Học Văn Lang, *Email: tonghunganh@vanlanguni.edu.vn*

xác thực lẫn nhau, các lựa chọn mã ngẫu nhiên dựa trên các mẫu đầu vào,...

Xác thực nhiều yếu tố (Multifactor Authentication) đề cập đến việc thực hiện hợp nhất của hai hoặc nhiều lớp nhân tố xác thực con người:

Một cái gì đó chỉ được biết đến với người dùng dựa trên kiến thức (ví dụ: mật khẩu, cụm từ, bí mật chia sẻ,...).

Một cái gì đó chỉ được giữ bởi người dùng dựa trên sở hữu (ví dụ: mã thông báo bảo mật, thẻ thông minh, thiết bị di động,...).

Một cái gì đó chỉ có cho người sử dụng các đặc điểm sinh học hoặc hành vi sinh trắc học (ví dụ: như nhận dạng khuôn mặt, dấu vân tay, nhận dạng giọng nói, chữ ký,...).

2.2. Giới thiệu về Liên minh FIDO

Công nghệ U2F được tạo ra bởi Google và Yubico, sau đó giao lại cho tổ chức Hiệp hội Công nghiệp xác thực mở được gọi là Liên minh FIDO (FIDO Alliance).

2.2.1. Nhiệm vụ của Liên minh FIDO

Nhiệm vụ của Liên minh FIDO là thay đổi bản chất của chứng thực trực tuyến bằng cách:

Xây dựng các đặc tả kỹ thuật theo cơ chế mở, có khả năng mở rộng tương tác, giảm sự phụ thuộc vào mật khẩu xác thực của người dùng.

Đảm bảo thành công trên toàn thế giới thông qua các thông số kỹ thuật chứng thực trực tuyến.

Phát triển tiêu chuẩn được công nhận để chuẩn hóa chính thức chứng thực trực tuyến.

2.2.2. Mục tiêu của Liên minh FIDO

Mục tiêu của Liên minh FIDO là cách mạng hóa xác thực trực tuyến với sự hỗ trợ công nghệ, không chỉ mang lại cho người dùng nhiều tính bảo mật mạnh mẽ hơn mà còn dễ dàng và tiện lợi để sử dụng. Những lý tưởng cơ bản thúc đẩy nỗ lực của Liên minh FIDO: Xác thực mạnh mẽ và dễ sử dụng; Bảo vệ sự riêng tư của người dùng; Giảm chi phí đối với các nhà cung cấp dịch vụ trực tuyến; Giảm chi phí cơ sở hạ tầng và sự phức tạp cho doanh nghiệp.

2.2.3. Giải pháp của Liên minh FIDO đã có ứng dụng trên thị trường

Hiện nay, công nghệ xác thực U2F của Liên minh FIDO được triển khai trong hàng trăm triệu thiết bị, tổng tiềm năng hơn 1,5 tỷ tài khoản người dùng. Công nghệ xác thực U2F của Liên minh FIDO được kích hoạt thông qua các triển khai ban đầu từ PayPal, Samsung, Google, và nhiều thành viên khác [2]. Bất kỳ người dùng có thiết bị tích hợp công nghệ xác thực U2F của Liên minh FIDO hoặc thiết bị được chứng nhận bởi FIDO® đều có thể bắt đầu xác thực bất cứ khi nào xác thực Liên minh FIDO hỗ trợ, chẳng hạn như trình duyệt Chrome và tài khoản Google được công bố vào tháng 10 năm 2014.

2.2.4. Tại sao công ty và doanh nghiệp của bạn nên cân nhắc tham gia Liên minh FIDO?

Phát triển và triển khai các giải pháp xác thực của Liên minh FIDO mang lại một số lợi ích cho các tổ chức thành viên dựa trên việc liệu họ có muốn triển khai xác thực của Liên minh FIDO hay sản xuất phần mềm hoặc phần cứng tương thích xác thực của Liên minh FIDO, để

tăng cường xác thực cho khách hàng của họ, bao gồm [3]:

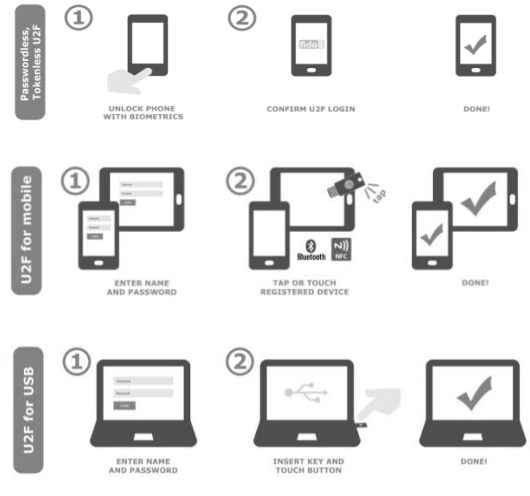
Bảo mật tài khoản/giao dịch mạnh hơn

Cải thiện trải nghiệm người dùng - Giải pháp của Liên minh FIDO cho phép các công ty và doanh nghiệp cải thiện sự thuận tiện cho cả khách hàng và nhân viên không cần phải nhớ mật khẩu phức tạp.

Cải thiện lợi tức đầu tư cho việc xác thực - Chi phí liên quan đến việc triển khai và hỗ trợ các giải pháp mới sẽ giảm đáng kể so với các phương pháp độc quyền hiện tại, kết nối một loại thiết bị với một ứng dụng duy nhất. Chức năng quản lý hệ thống sẽ được cung cấp bởi cơ sở hạ tầng của Liên minh FIDO chứ không phải do mỗi nhà phát triển phải xây dựng.

Giảm rủi ro gian lận - Người dùng các trang web và điện thoại di động có hỗ trợ của Liên minh FIDO sẽ giảm được nguy cơ bị gian lận danh tính, với sự tiện lợi của việc hạn chế dựa vào mật khẩu.

2.2.5. Công nghệ U2F



Hình 1. (nguồn Yubico)

Công nghệ U2F được triển khai thành công bởi các dịch vụ trực tuyến có quy mô lớn, bao gồm Gmail, Dropbox, GitHub, Salesforce.com, Chính phủ Anh và nhiều thành viên trong Liên minh FIDO.

Công nghệ U2F cung cấp khả năng xác thực mạnh mẽ qua các giao thức, kết nối USB, NFC, Bluetooth và trong các ứng dụng không có mật khẩu/không có mã, minh họa xem hình 1.

Bạn cần có một thiết bị khóa công nghệ U2F [4].

Hình 2. (nguồn Amazon)

Hình 2 là sản phẩm (thiết bị) có chứng chỉ của Liên minh FIDO (fido CERTIFIED, U2F) và tổ chức Google có trình duyệt Chrome là thành viên của Liên minh FIDO.

Bạn sẽ phải làm theo các hướng dẫn bởi nhà cung cấp dịch vụ trực tuyến của bạn (ví dụ: Google Chrome là dịch vụ trực tuyến bạn đang sử dụng), sau đây chúng tôi trình bày tóm tắt hướng dẫn của Yubico.

Hình 3. (nguồn Yubico)

Yubico thay đổi các vai trò để chứng thực mạnh mẽ, cung cấp bảo mật cao cấp với sự dễ dàng sử dụng chưa từng có.

Sáng chế cốt lõi của họ là Yubikey, một thiết bị USB nhỏ, hỗ trợ giao thức xác thực và mã hóa. Với một xác thực đơn giản, nó bảo vệ truy cập vào máy tính, mạng, và các dịch vụ trực tuyến cho các tổ chức lớn nhất thế giới.

Yubico là nhà đóng góp hàng đầu cho tiêu chuẩn chứng thực mở - công nghệ U2F. Công nghệ của họ được triển khai tại 9/10 công ty Internet hàng đầu và được hàng triệu người sử dụng ở hơn 160 quốc gia yêu thích.

Khóa bảo mật FIDO-U2F của Yubico [5] là một YubiKey được thiết kế đặc biệt, dựa vào mật mã bảo mật cao, mật mã khóa công khai.

Tính năng cốt lõi

Hoạt động trên Microsoft Windows, Apple Mac OS X và Linux.

Chạm vào nút để kích hoạt bảo mật dựa trên mã khóa công khai: hoạt động ngay lập tức, không cần phải nhập lại mật mã từ thiết bị - thay thế văn bản SMS.

Xác định như một thiết bị USB chuẩn trên tất cả các máy tính.

Không có phần mềm hoặc trình điều khiển khách hàng nào cần được cài đặt.

Thiết bị được chống thấm, khó bị phá hủy trong quá trình sử dụng thông thường.

Trọng lượng 3gram, và kết nối qua cổng USB trên máy tính.

Sản xuất tại Mỹ và Thụy Điển với độ an toàn và chất lượng cao [6].

Hình 4. *Cách hoàn thành - hai bước xác thực* (nguồn Yubico)

1) Nhập tên người dùng và mật khẩu thông thường của bạn vào trường đăng nhập của bất kỳ ứng dụng nào hỗ trợ FIDO U2F (xem hình 4).

2) Lắp khóa bảo mật vào cổng USB với mặt màu vàng hướng lên (xem hình 3).

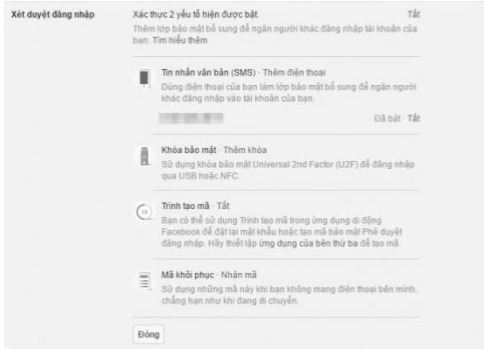
Chỉ cần chạm vào nút vàng trên khóa bảo mật để tạo ủy nhiệm đăng nhập an toàn của bạn (xem hình 3).

Ứng dụng công nghệ U2F cho trình duyệt Chrome

Hướng dẫn sử dụng một khóa bảo mật FIDO U2F xác thực trong trình duyệt Google Chrome [7].

Ứng dụng công nghệ U2F cho facebook

Mới đây, facebook đã bổ sung một tính năng bảo mật tài khoản mới cho người dùng khi đăng nhập. Bạn có thể sử dụng những chiếc USB bảo mật sử dụng chuẩn công nghệ U2F làm lớp bảo mật thứ hai cho tài khoản Facebook của mình sau lớp bảo mật thứ nhất là mật khẩu [8].



Hình 5. (nguồn facebook)

USB bảo mật sử dụng công nghệ U2F là một thiết bị phần cứng sử dụng chuẩn USB để kết nối với máy tính, khi đã có trong tay thiết bị này, chúng ta hoàn toàn có thể thiết lập và sử dụng nó để đăng nhập vào Facebook (xem hình 5).

Sử dụng USB bảo mật có thể giúp bạn tránh khỏi Phishing (một phương thức lừa đảo bằng cách bắt bạn nhập mật khẩu Facebook) hay các cuộc tấn công đánh cắp mật khẩu có thể gây nguy hiểm cho những thông tin của bạn. Khi được thiết lập với USB bảo mật sử dụng công nghệ U2F, tin tặc sẽ phải cần đến mật khẩu và cả chiếc USB mà bạn đang nắm giữ mới có thể xâm nhập vào tài khoản của bạn được.

Cách sử dụng USB bảo mật cũng khá đơn giản (tương tự như phần *Ứng dụng cho trình duyệt Chrome*). Khi được yêu cầu xác thực sẽ có các thông báo hướng dẫn của Facebook, bạn chỉ cần cắm USB vào máy tính rồi nhấn nút xác nhận trên USB là xong (xem hình 6).

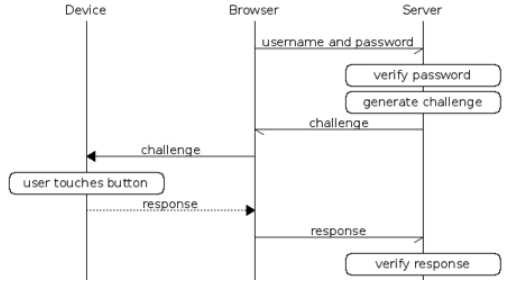
Hình 6. (nguồn facebook)

2.2.6. Ưu điểm và khuyết điểm của công nghệ U2F

Ưu điểm của công nghệ U2F

Mạnh về an ninh - Xác thực hai yếu tố mạnh mẽ, sử dụng mật mã khóa công khai [9] bảo vệ chống lại tấn công giả mạo [10] (Phishing) bất kỳ giải pháp nào yêu cầu người sử dụng chép mã OTP [11] đều không thể chống lại tấn công giả mạo (Phishing), phiên tặc (Man-In-The-Middle) [12], và các cuộc tấn công bằng phần mềm độc hại.

Dễ dàng sử dụng - Hoạt động với sự trợ giúp trình duyệt (bắt đầu từ Chrome và Opera với Mozilla đến năm 2017) cho phép xác thực ngay cho bất kỳ dịch vụ trực tuyến nào. Không có mã để gõ, hoặc trình điều khiển để cài đặt. Người dùng chỉ cần sờ hoặc nhấn vào một nút duy nhất trên thiết bị đã có chứng chỉ của Liên minh FIDO hoặc thiết bị cá nhân đã có chứng chỉ của Liên minh FIDO để xác thực. Các giải pháp khác đều yêu cầu người dùng phải chép một mã số (thường được gọi là OTP) từ thiết bị sinh mã. Bảo mật cao - Cho phép người dùng lựa chọn, sở hữu và kiểm soát danh tính trực tuyến của họ. Mỗi người dùng cũng có thể chọn để có nhiều danh tính, bao gồm cả ẩn danh (không có thông tin cá nhân liên quan đến nhận dạng). Một thiết bị U2F tạo ra một cặp khóa mới cho mỗi dịch vụ trực tuyến, và chỉ có dịch vụ trực tuyến lưu trữ khóa công khai. Với cách tiếp cận này, không có bí mật được chia sẻ giữa các nhà cung cấp dịch vụ trực tuyến, và thậm chí các thiết bị U2F với chi phí thấp có thể hỗ trợ bất kỳ dịch vụ trực tuyến nào. Sau đây, chúng tôi trình bày tóm tắt ba ý chính về bảo mật cao của công nghệ U2F: sơ đồ giải thích dòng chảy quy trình cơ bản của U2F, xác thực U2F và sơ đồ tổng quát biểu diễn sản sinh các khóa: khóa riêng (Private key), khóa công khai (Public key) của thiết bị Yubikey.



Hình 7. Sơ đồ giải thích quy trình cơ bản của giao thức U2F [13]. (Nguồn Yubico)

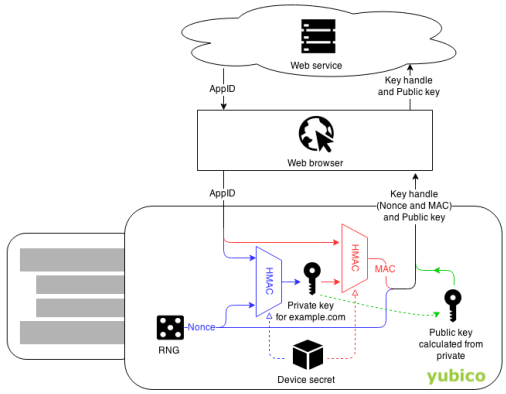
Xác thực U2F

Mục đích của công nghệ U2F chỉ đơn giản cung cấp một cơ chế để bên một trang web hoặc dịch vụ trực tuyến có thể xác minh tính xác thực của người được xác thực bởi công nghệ U2F. Bên dịch vụ trực tuyến yêu cầu chứng chỉ chứng nhận để tìm hiểu thông tin về người xác thực, chẳng hạn như YubiKey. Thông tin được truy vấn có thể bao gồm nhà cung cấp, loại thiết bị và tính năng đảm bảo - bảo mật của thiết bị xác thực. Tính xác thực của thông tin chứng nhận được đảm bảo bằng một chứng nhận số có thời hạn hiệu lực cụ thể [14].

Ngoài chứng thực đối với tính xác thực của thiết bị, chứng nhận số cũng được sử dụng để xác định thiết bị nào có thể được sử dụng bởi bên tham gia chứng thực. Ví dụ: trang web ngân hàng muốn người dùng có thể cung cấp thiết bị U2F của riêng mình để xác thực hai yếu tố, nhưng sẽ chỉ cho phép người dùng sử dụng thiết bị từ các nhà cung cấp được chấp thuận nhất định.

Tuy nhiên, không có yêu cầu nào để chỉ ra loại thiết bị hoặc phần mềm phía máy khách đang sử dụng thiết bị U2F hoặc bên nhà cung cấp dịch vụ trực tuyến có thể quyết định chấp nhận bất kỳ loại chứng nhận số hoặc một loại cụ thể nào. Sơ đồ tổng quát biểu diễn sản sinh các khóa riêng, khóa công khai (Private key, Public key) của thiết bị Yubikey.

Khi người dùng đăng ký một thiết bị U2F với một dịch vụ trực tuyến mới, dịch vụ trực tuyến cung cấp một AppID [15] (điều này gắn với URL của trang web và ngăn ngừa các trang web lừa đảo). Thiết bị U2F tạo ra một tham số **Nonce, N** [16] là một số tùy ý mà chỉ có thể sử dụng một lần.



Hình 8. Sơ đồ tổng quát biểu diễn sản sinh các khóa riêng, khóa công khai (Private key, Public key [17]) của thiết bị Yubikey (nguồn Yubico)

Chú chích: Tham số AppID (The Application ID) [15]; Tham số None, N [16]; HMAC-SHA256 và MAC (Message Authentication Code)[18]

Sau đó, thiết bị U2F lấy AppID và Nonce (Crytographic Nonce), xử lý thông qua HMAC-SHA256 [18] (chức năng khóa một chiều), sử dụng bí mật thiết bị cụ thể làm khóa bảo mật. Khóa cụ thể cho thiết bị này được tạo ra trên chip tại thời điểm sản xuất.

Đầu ra của hàm băm trở thành khóa riêng và Nonce cùng với một MAC (Message Authentication Code), trở thành các khóa xử lý (khóa riêng, khóa công khai (Private key, Public key) của việc xác thực. Trong quá trình xác thực, MAC giúp đảm bảo rằng, một xử lý quan trọng (key handle) chỉ có giá trị cho sự kết hợp cụ thể của thiết bị và AppID được tạo ra trong quá trình đăng ký. Để xác thực, xử lý quan trọng (Key Handle) được chuyển đến Yubikey một lần nữa và sẽ được xác minh. MAC đảm bảo xử lý không bị sửa đổi và chứng chỉ thuộc về ứng dụng đã cho. Cùng với bí mật gốc được lưu trữ trên Yubikey, đây là tất cả mọi thứ cần thiết để lấy được khoá riêng cụ thể được sử dụng

cho chứng chỉ truy cập toàn cầu và tăng lên khi xác thực mỗi lần, đây là trạng thái duy nhất của Yubikey được sửa đổi trong bước này. Bộ đếm này được chia sẻ giữa các chứng chỉ.

Vì không có dữ liệu xác thực cụ thể được lưu trữ trên YubiKey nên không thể liệt kê số lượng xử lý quan trọng (key handle) "được lưu trữ" (vì chúng không được lưu trữ trên thiết bị). Cũng không có cách nào để thiết lập lại thiết bị.

Nhiều lựa chọn - Các tiêu chuẩn mở cung cấp tính linh hoạt và cho phép có sự lựa chọn sản phẩm. Được thiết kế cho điện thoại và máy tính, cho nhiều phương thức xác thực (cổng USB hoặc tích hợp trực tiếp vào thiết bị,...) và với các phương thức truyền thông khác nhau (USB, NFC, Bluetooth,...). Công nghệ U2F là một chuẩn mở, do đó các doanh nghiệp cần độ bảo mật cao có thể tự đánh giá và triển khai giải pháp này mà không cần nhờ vào bên thứ ba. Các giải pháp như thẻ xác thực giao dịch trực tuyến RSA SecurID [19] hoàn toàn đóng, không ai biết bên trong chúng hoạt động như thế nào.

Chi phí và hiệu quả - Các nhà cung cấp dịch vụ trực tuyến không phải chịu chi phí và hỗ trợ phân phối các thiết bị U2F an toàn. Người dùng có thể chọn từ một thiết bị giá rẻ từ nhiều nhà cung cấp, có sẵn tại Amazon và các cửa hàng bán lẻ khác trên toàn thế giới. Yubico cung cấp phần mềm máy chủ miễn phí và mã nguồn mở cho tích hợp đầu cuối (Back-End).

Nhận dạng điện tử - Đối với các tổ chức yêu cầu mức độ bảo mật cao hơn, có các dịch vụ trực tuyến buộc thiết bị U2F của bạn vào xác thực cả trực tuyến (Online) và ngoại tuyến (Offline).

Khuyết điểm của công nghệ U2F

Sự tiện lợi là yếu tố cần tính đến để triển khai rộng rãi một giải pháp bảo mật. Hiện nay, chưa có nhiều dịch vụ trực tuyến hỗ trợ công nghệ U2F, chỉ có một số hãng lớn bao gồm Microsoft, Qualcomm, Google, Dropbox, Bank of America, Github, trong đó Google Chrome cũng là trình duyệt duy nhất tích hợp phương thức xác thực này, Firefox và Edge đang được tích hợp nhưng chưa hoàn thiện, đồng thời việc người dùng phải mua thiết bị phần cứng (đầu thẻ U2F với giá từ vài đô la đến vài chục đô la Mỹ) chuyên dụng cũng ngăn cản người dùng sử dụng phương thức xác thực này.

3. KẾT LUẬN

Trong tương lai, với sự nỗ lực dựa trên nhiệm vụ và mục tiêu xem phần 2.2.1 và 2.2.2 của Liên minh FIDO, đây sẽ là một giải pháp hứa hẹn mang đến môi trường Internet an toàn hơn và giảm chi phí khi triển khai. Bảo mật trong hệ thống máy tính là cả một quy trình chứ không phải là một sản phẩm công nghệ thông tin (phần mềm, phần cứng) riêng lẻ. Các tin tặc lại thường nhắm vào những điểm yếu với đối tượng có nhiều sơ hở nhất, đó chính là người dùng. Việc đảm bảo an toàn cho người dùng máy tính ở đầu cuối sẽ gia tăng đáng kể cho sự an toàn của cả quy trình bảo mật hệ thống máy tính.

Bài báo chúng tôi trình bày kiến thức cơ bản về xác thực trực tuyến trở nên đơn giản và mạnh mẽ hơn, theo Microsoft cần xác thực nhiều yếu tố (Multifactor Authentication) và giới thiệu công nghệ xác

thực U2F (hai yếu tố) của Hiệp hội Công nghiệp xác thực mở được gọi là Liên minh FIDO cũng như ưu và khuyết điểm của giải pháp FIDO; phù hợp cho các độc giả là người dùng (cá nhân, công ty, doanh nghiệp) muốn tìm hiểu, chọn lựa và sử dụng các sản phẩm công nghệ thông tin (phần cứng, phần mềm) và dịch vụ trực tuyến hiện có của họ với việc xác thực trực tuyến trở nên đơn giản và mạnh mẽ hơn; cũng như bất kỳ nhà sản xuất thiết bị nào, nhà phát triển phần mềm hoặc nhà cung cấp dịch vụ trực tuyến có thể xây dựng hỗ trợ các giao thức của U2F vào các sản phẩm và dịch vụ trực tuyến hiện có của họ nhằm giúp việc xác thực trực tuyến trở nên đơn giản và mạnh mẽ hơn cho người dùng của họ.

TÀI LIỆU THAM KHẢO

1. Xác thực nhiều yếu tố, *Strong User Authentication*, http://msdn. microsoft.com
2. *Thành viên Liên minh FIDO*, https://fidoalliance.org/participate/members/.
3. *Lợi ích của thành viên Liên minh FIDO*, https://fidoalliance.org/participate/.
4. *Thiết bị Yubikey*, https://www.amazon.com/Yubico.
5. *Khóa bảo mật FIDO-U2F của Yubico*, Yubikey, https://www.yubico.com.
6. *Thiết bị Yubikey sản xuất tại Mỹ và Thụy Điển,* https://www.yubico.com.
7. *Hướng dẫn sử dụng một khóa bảo mật FIDO U2F xác thực trong trình duyệt Google Chrome*, https://support.google.com.
8. *Bảo mật sử dụng chuẩn công nghệ U2F làm lớp bảo mật thứ hai cho tài khoản Facebook*, https://www.facebook.com/help/132694786861712?helpref=related.
9. *Mật mã hóa khóa công khai,* https://vi.wikipedia.org.
10. *Tấn công giả mạo*, https://vi.wikipedia.org/wiki/Tấn_công_giả_mạo.
11. *Mã xác thực OTP, One-time password,* https://en.wikipedia.org.
12. *Tấn công giả mạo, Man in the middle attack*, https://en.wikipedia.org.
13. *Giao thức của U2F,* https://developers.yubico.com/U2F/Protocol_details/.
14. *Chứng nhận số Liên minh FIDO*, https://fidoalliance.org/certification/.
15. *Thuật ngữ tham số App ID*, https://developers.yubico.com/U2F/App_ID.html.
16. *Thuật ngữ tham số Nonce, N*, https://en.wikipedia.org/wiki/Cryptographic_nonce.
17. *Các khóa riêng, khóa công khai* , https://en.wikipedia.org.
18. *Hàm băm mật mã học, HMAC-SHA256,* https://en.wikipedia.org.
19. *Xác thực giao dịch trực tuyến RSA SecurID*, https://en.wikipedia.org

Ngày nhận bài: 30/5/2017. Ngày biên tập xong: 25/6/2017. Duyệt đăng: 18/10/2017