BIDV NGÂN HÀNG ĐẦU TƯ VÀ PHÁT TRIỂN VIỆT NAM

Ứng dụng xác thực đa yếu tố trong giao dịch ngân hàng điện tử

Trình bày: ThS. Đặng Mạnh Phổ
Giám đốc Ban Công nghệ BIDV

Khái niệm xác thực

- Xác thực (tiếng Anh: Authentication - xuất phát từ Authentic có nghĩa là “thật”, “thực”,“đích thực” hoặc “chính cống”) là một hành động nhằm xác lập hoặc chứng thực một người nào đó (hay một cái gì đó) đáng tin cậy, có nghĩa là những lời khai báo do người đó đưa ra hoặc về cái đó là sự thật.
- Xác thực một đối tượng còn có nghĩa là công nhận nguồn gốc của đối tượng, trong khi, xác thực một người thường bao gồm việc thẩm tra nhận dạng của họ.

Khái niệm xác thực

- Trong an toàn thông tin máy tính nói chung và giao dịch ngân hàng điện tử nói riêng xác thực là một quy trình nhằm xác minh nhận dạng số (*digital identity*) của bên gửi thông tin (*sender*) trong liên lạc trao đổi xử lý thông tin chẳng hạn như một yêu cầu đăng nhập. Bên gửi cần phải xác thực có thể là một người sử dụng máy tính, bản thân một máy tính hoặc một phần mềm.
- Việc xác thực thường phụ thuộc vào một hoặc nhiều yếu tố xác thực (*authentication factor*) để minh chứng cụ thể.

Ý nghĩa của xác thực

- Xác thực là khâu đặc biệt quan trọng để bảo đảm an toàn cho hoạt động của hệ thống thông tin dạng như hệ thống ngân hàng điện tử.
- Hệ thống luôn luôn trước tiên xác thực một thực thể khi nó cố thử thiết lập liên lạc. Khi đó nét nhận dạng của thực thể được dùng để xác định sự truy nhập của nó như một đặc quyền hoặc để đạt được sự sẵn sàng phục vụ.
- Đối với các giao dịch ngân hàng điện tử điển hình như giao dịch qua ATM / POS, giao dịch Online/Internet Banking, giao dịch Mobile Banking... thì xác thực là bắt buộc trong quản lý truy cập.

Các yếu tố xác thực

Những yếu tố xác thực dành cho con người (người sử dụng) nói chung có thể được phân loại như sau:

- ***Những cái mà người sử dụng sở hữu bẩm sinh,*** **chẳng hạn như dấu vân tay hoặc mẫu dạng võng mạc mắt, chuỗi ADN, mẫu dạng giọng nói, chữ ký, tín hiệu sinh điện đặc thù do cơ thể sống tạo ra, hoặc những định danh sinh trắc học (*biometric* identifier)...**
- ***Những cái người sử dụng có*****, chẳng hạn như chứng minh thư, chứng chỉ an ninh (*security token*), chứng chỉ phần mềm (*software token*) hoặc điện thoại di động...**
- ***Những gì người sử dụng biết*****, chẳng hạn như mật khẩu (password), mật ngữ (*pass phrase*) hoặc mã số định danh cá nhân (*personal identification number - PIN*)…**

Xác thực đa yếu tố

- Trong thực tế, nhiều khi một tổ hợp của những yếu tố trên được sử dụng, lúc đó người ta nói đến xác thực đa yếu tố *(Multi-factor authentication)*
- Chẳng hạn trong giao dịch ATM, thẻ ngân hàng và mã số định danh cá nhân (PIN) được sử dụng - trong trường hợp này đó là một trong các dạng xác thực 2 yếu tố (*two-factor authentication – 2FA*).
- Cũng trong ví dụ trên nếu sử dụng thêm một yếu tố nữa như dấu vân tay chẳng hạn thì ta sẽ có xác thực ba yếu tố (*three-factor authentication- 3FA).*
- Tương tự như vậy cho xác thực n yếu tố (n ≥ 2): *n-factor authentication- nFA*

Một số phương pháp xác thực (1)

-Xác thực dựa trên User Name (định danh người sử dụng) và Password (mật khẩu): **Sự kết hợp của một cặp username và password có thể nói là cách xác thực cơ bản nhất (và cũng phổ biến nhất). Với phương thức xác thực này, thông tin cặp username và password nhập vào được đối chiếu với dữ liệu lưu trữ trên hệ thống, nếu trùng khớp username và password, thì người sử dụng (User) được xác thực còn nếu không người sử dụng bị từ chối hoặc cấm truy cập.**

-Nói chung phương thức xác thực này có tính bảo mật không cao lắm vì những lý do như thường thì thông tin cặp username và password nhập vào được gửi đi xác thực trong tình trạng *plain text (ký tự văn bản thuần)*, tức không được mã hóa và có thể bị chặn bắt trên đường truyền, thậm chí ngay trong quá trình nhập vào; lộ password do đặt quá đơn giản (dạng '123456', 'abc123' v.v.) hoặc dễ đoán (tên / ngày sinh của người thân...).

Một số phương pháp xác thực (2)

-Giao thức xác thực bắt tay có thử thách - Challenge Handshake Authentication Protocol (CHAP): **Challenge Handshake Authentication Protocol (CHAP) cũng là mô hình xác thực dựa trên username/password. Khi User cố gắng đăng nhập (log on), máy chủ (server) đảm nhiệm vai trò xác thực sẽ gửi một thông điệp thử thách (challenge message) trở lại máy tính User. Lúc này máy tính User sẽ phản hồi lại username và password được mã hóa. Server xác thực sẽ so sánh phiên bản xác thực User được lưu giữ với phiên bản mã hóa vừa nhận, nếu trùng khớp thì User sẽ được xác thực. Bản thân password không bao giờ được gửi qua mạng.**

- Phương thức CHAP thường được sử dụng khi User đăng nhập vào các máy chủ ở xa (remote server) của hệ thống, chẳng hạn như RAS server. Dữ liệu chứa password được mã hóa đôi khi được gọi là hash password (mật khẩu băm) theo tên của phương pháp mã hoá dùng các hàm băm.

Một số phương pháp xác thực (3)

-***Xác thực Kerberos***: Kerberos là nền tảng xác thực chính của nhiều hệ điều hành như UNIX, Windows... Xác thực Kerberos dùng một server trung tâm để kiểm tra việc xác thực user và cấp phát thẻ thông hành (service ticket) để User có thể truy cập vào tài nguyên hệ thống.

-Xác thực Kerberos là một phương thức có tính an toàn khá cao nhờ việc dùng cấp độ mã hóa rất mạnh.

-Kerberos cũng dựa trên độ chính xác của thời gian xác thực giữa Server và Client, do đó cần phải đảm bảo kết nối đồng bộ thời gian giữa các thành phần này của hệ thống.

Một số phương pháp xác thực (4)

-Xác thực sử dụng token (biểu trưng kỹ thuật số): **Token là phương tiện vật lý như các thẻ thông minh (smart card), thẻ đeo của nhân viên (ID badge) chứa thông tin xác thực hoặc bộ tạo OTP (*One Time Password - mật khẩu dùng một lần*).**

-Tokens có thể lưu trữ mã số nhận dạng cá nhân (PIN), thông tin về user, lưu giữ hoặc tạo ra password.

-Các thông tin trên token chỉ có thể được đọc / xử lý bởi các thiết bị / hệ thống đặc dụng. Chẳng hạn như thẻ thông minh được đọc bởi đầu đọc thẻ smart card chuyên dụng, OTP được xử lý bởi hệ thống xác thực sử dụng yếu tố xác thực thứ hai là mật khẩu dùng một lần.

Một số phương pháp xác thực (5)

***-Xác thực áp dụng các phương pháp nhận dạng sinh trắc học (Biometrics)*: Đây là mô hình xác thực có tính bảo mật cao dựa trên đặc điểm sinh học của từng cá nhân, trong đó sử dụng các thủ tục như quét dấu vân tay (fingerprint scanner), quét võng mạc mắt (retinal scanner), nhận dạng giọng nói (voice-recognition), nhận dạng khuôn mặt (facerecognition) v.v.**

-Nhờ các tiến bộ vượt bậc của công nghệ sinh học phương thức xác thực dựa trên nhận dạng sinh trắc học ngày càng trở nên phổ biến và được chấp nhận rộng rãi. Ví dụ xác thực quét dấu vân tay hiện đã khá phổ biến trên các máy tính xách tay, thậm chí trên điện thoại di động.

Một số phương pháp xác thực (6)

-Xác thực đa yếu tố (Multi-Factor Authentication): **Đây là phương thức xác thực dựa trên nhiều yếu tố xác thực kết hợp, là mô hình xác thực yêu cầu kiểm chứng ít nhất là hai yếu tố xác thực. Trong phương thức này có thể có sự kết hợp của bất cứ yếu tố nào, ví dụ như đặc tính bẩm sinh, những cái bạn có để chứng minh hoặc những gì bạn biết để chứng minh.**

-Một ví dụ về xác thực đa yếu tố liên quan đến giao dịch ngân hàng điện tử là xác thực chủ thẻ trong giao dịch ATM (Yếu tố xác thực đầu tiên của bạn là thẻ ATM (cái bạn có), sau khi đưa thẻ vào máy đọc bạn sẽ phải đưa tiếp yếu tố xác thực thứ hai là PIN (cái bạn biết).

-Một ví dụ khác là xác thực người sử dụng dịch vụ giao dịch Internet Banking: Bạn đăng nhập với username + password sau đó còn phải đưa tiếp OTP (mật khẩu dùng một lần) được sinh ra trên token của riêng bạn.

Một số phương pháp xác thực (7)

-Phương thức xác thực lẫn nhau (Mutual Authentication):
Đây là phương thức bảo mật trong đó các thành phần tham gia giao tiếp với nhau kiểm tra xác thực lẫn nhau.
- Chẳng hạn trong một hệ thống mạng Client/Server, trước hết Server chứa tài nguyên kiểm tra "giấy phép truy cập" của Client và sau đó Client lại kiểm tra "giấy phép cấp tài nguyên" của Server.
-Cũng tương tự như vậy khi bạn thực hiện giao dịch với hệ thống e-Banking của một Ngân hàng bạn cần phải kiểm tra xem hệ thống đó có đúng là của Ngân hàng của bạn không và ngược lại hệ thống e-Banking của Ngân hàng cũng sẽ kiểm tra bạn.

Xác thực đa yếu tố - Bảo mật vs Tiện dụng

- An toàn bảo mật trong giao dịch ngân hàng điện tử là hết sức quan trọng, trong đó xác thực người sử dụng là một trong những khâu cốt tử.
- Với xác thực đa yếu tố ta có thể tăng mức độ an toàn bảo mật lên rất cao nhờ việc kiểm chứng nhiều yếu tố xác thực. Hiển nhiên là mức độ an toàn bảo mật sẽ càng cao khi số yếu tố xác thực càng nhiều.
- Tuy nhiên, khi số yếu tố xác thực lớn thì hệ thống càng phức tạp kéo theo chi phí đầu tư và duy trì vận hành tốn kém, đồng thời lại bất tiện cho người sử dụng. Do vậy, trên thực tế để cân bằng giữa an toàn bảo mật và tính tiện dụng người ta thường áp dụng xác thực hai yếu tố và xác thực ba yếu tố.
- Nên lưu ý rằng xác thực đa yếu tố dù có mang lại mức độ an toàn bảo mật cao hơn, nhưng về lý thuyết cũng không thể là tuyệt đối an toàn nên chúng ta không bao giờ được chủ quan trong lĩnh vực an toàn thông tin.