



NETWORK INFORMATION SECURITY VIETNAM

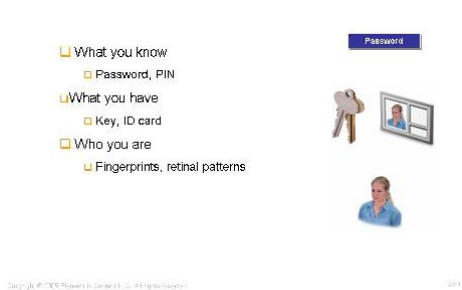
Các phương thức xác thực -Authentication Methods

Bạn đã được học về xác thực (authentication), đây là một trong 4 nhân tố chính trong bảo mật computer. Mặc dù authentication luôn có cùng một mục tiêu, nhưng có nhiều cách tiếp cận khác nhau để hoàn thành.. Trong chủ đề này, chúng ta sẽ thảo luận vài phương thức xác thực chính phổ biến hiện nay.

Một số nhân tố được sử dụng chính trong xác thực chẳng hạn:

- password (mật mã)
- key (khóa)
- fingerprints (vân tay)

Authentication Factors



Xác thực dựa trên User Name và Password

Sự kết hợp của một user name và password là cách xác thực cơ bản nhất. Với kiểu xác thực này, chứng từ ủy nhiệm User được đối chiếu với chứng từ được lưu trữ trên database hệ thống, nếu trùng khớp username và password, thì user được xác thực và nếu không User bị cấm truy cập. Phương thức này không bảo mật lắm vì chứng từ xác nhận User được gửi đi xác thực trong tình trạng *plain text*, tức không được mã hóa và có thể bị tóm trên đường truyền.

User Name/Password Authentication

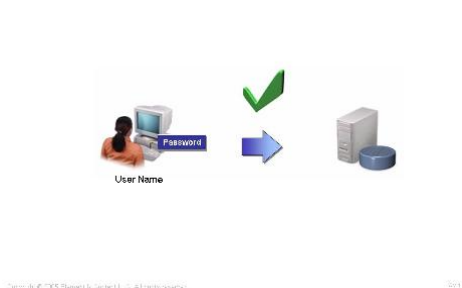


Figure 1-3: User name/password authentication



NETWORK INFORMATION SECURITY VIETNAM

Challenge Handshake Authentication Protocol (CHAP)

Challenge Handshake Authentication Protocol (CHAP) cũng là mô hình xác thực dựa trên user name/password. Khi user cố gắng log on, 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 user name 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, user sẽ được authenticated. Bản thân Password không bao giờ được gửi qua network. Phương thức CHAP thường được sử dụng khi User logon vào các remote servers của cty chẳng hạn như RAS server. Dữ liệu chứa password được mã hóa gọi là password băm (hash password). Một gói băm là một loại mã hóa không có phương cách giải mã.

CHAP

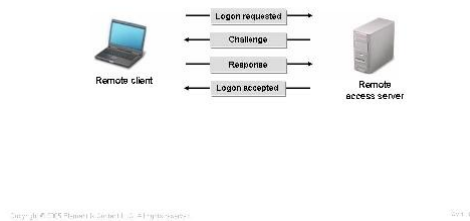


Figure 1-4: CHAP.

Kerberos

Kerberos authentication dùng một Server trung tâm để kiểm tra việc xác thực user và cấp phát thẻ thông hành (service tickets) để User có thể truy cập vào tài nguyên. Kerberos là một phương thức rất an toàn trong authentication bởi vì dùng cấp độ mã hóa rất mạnh. Kerberos cũng dựa trên độ chính xác của thời gian xác thực giữa Server và Client Computer, do đó cần đảm bảo có một time server hoặc authenticating servers được đồng bộ time từ các Internet time server. Kerberos là nền tảng xác thực chính của nhiều OS như Unix, Windows



NETWORK INFORMATION SECURITY VIETNAM

Kerberos



Copyright © 2005 Pearson Education, Inc. All Rights Reserved.

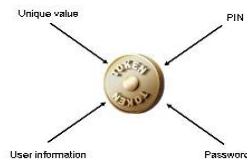
10/11/14

Figure 1-5: Kerberos.

Tokens

Tokens là phương tiện vật lý như các thẻ thông minh (smart cards) hoặc thẻ đeo của nhân viên (ID badges) chứa thông tin xác thực. Tokens có thể lưu trữ số nhận dạng cá nhân-personal identification numbers (PINs), thông tin về user, hoặc passwords. Các thông tin trên token chỉ có thể được đọc và xử lý bởi các thiết bị đặc dụng, ví dụ như thẻ smart card được đọc bởi đầu đọc smart card gắn trên Computer, sau đó thông tin này được gửi đến authenticating server. Tokens chứa chuỗi text hoặc giá trị số duy nhất thông thường mỗi giá trị này chỉ sử dụng một lần.

A Token



Copyright © 2005 Pearson Education, Inc. All Rights Reserved.

10/11/14

Ví dụ về Smart Cards

Smart cards là ví dụ điển hình về xác thực tokens- token-based authentication. Một smart card là một thẻ nhựa có gắn một chip máy tính lưu trữ các loại thông tin điện tử khác nhau. Nội dung thông tin của card được đọc với một thiết bị đặc biệt.

Biometrics

Biometrics (phương pháp nhận dạng sinh trắc học) mô hình xác thực dựa trên đặc điểm sinh học của từng cá nhân. Quét dấu vân tay (fingerprint scanner), quét võng mạc mắt (retinal scanner), nhận dạng giọng nói(voice-recognition), nhận dạng khuôn mặt(facerecognition). Vì nhận dạng sinh trắc học hiện rất tốn kém chi phí khi triển khai nên không được chấp nhận rộng rãi như các phương thức xác thực khác.



NETWORK INFORMATION SECURITY VIETNAM

Biometrics

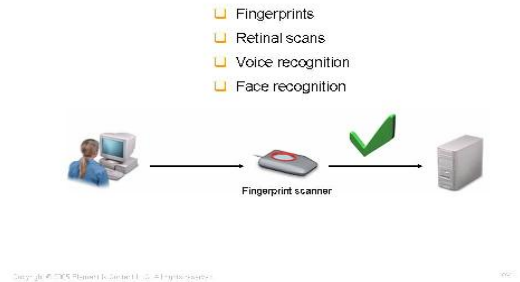


Figure 1-7: Biometrics.

Multi-Factor Authentication

Multi-factor authentication, xác thực dựa trên nhiều nhân tố kết hợp, là mô hình xác thực yêu cầu kiểm ít nhất 2 nhân tố xác thực. Có thể đó là sự kết hợp của bất cứ nhân tố nào ví dụ như: bạn là ai, bạn có gì chứng minh, và bạn biết gì?.

Ví dụ: về một Multi-Factor Implementation:

Cần phải đưa thẻ nhận dạng vào đầu đọc và cho biết tiếp password là gì

Multi-factor Authentication

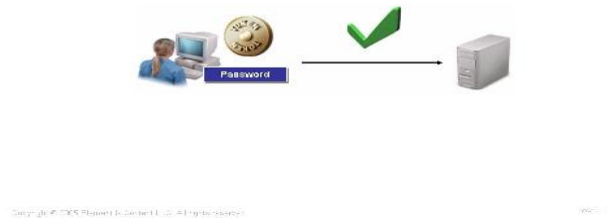


Figure 1-8: Multi-factor authentication

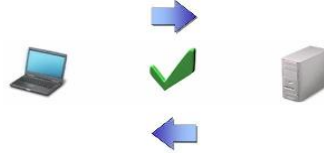
Mutual Authentication

Mutual authentication, xác thực lẫn nhau là kỹ thuật bảo mật mà mỗi thành phần tham gia giao tiếp với nhau kiểm tra lẫn nhau. 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. Điều này giống như khi bạn giao dịch với một Server của bank, bạn cần kiểm tra Server xem có đúng của bank không hay là một cái bẫy của hacker giăng ra, à ngược lại Server bank sẽ kiểm tra bạn...



NETWORK INFORMATION SECURITY VIETNAM

Mutual Authentication



Copyright © 2008 NIS.com.vn. All rights reserved.

18/01/08

Figure 1-9: *Mutual authentication.*