



NETWORK INFORMATION SECURITY VIETNAM

Các quy tắc cơ bản về mã hóa -Cryptography Fundamentals

Chúng ta đã nhận dạng ra một số các mục tiêu chính của Security như tính bí mật (confidentiality), tính tích hợp (integrity), và tính sẵn sàng (availability). Mã hóa-Encryption là một trong những công cụ bảo mật đa năng và chúng ta có thể sử dụng nó để đạt được mục tiêu đề ra. Trong chủ đề này, chúng ta xác định các thành phần cơ bản trong mã hóa, các khái niệm, và các công cụ. Có thể xem mã hóa là một vũ khí cực mạnh, và phức tạp trong cuộc chiến bảo vệ an toàn cho máy tính. Có nhiều hệ thống mật mã, và cách thiết lập cũng khác nhau. Tuy nhiên có sự tương đồng giữa tất cả các hệ thống mã hóa, điều mà các security professionals nên nắm vững. Các thuật ngữ cơ bản về mã hóa và những ý tưởng bạn tiếp thu trong chủ đề này sẽ giúp bạn kiểm tra, hiểu và quản lý được bất cứ loại hệ thống mã hóa nào sau này bạn dự định triển khai.

Encryption

Encryption, mã hóa là một kỹ thuật bảo mật làm biến đổi (converts) dữ liệu từ hình thức đơn giản, rõ ràng (plain hoặc cleartext form) sang hình thức dữ liệu biến thành mật mã (coded, hoặc ciphertext form. Chỉ những ai có được thông tin giải mã cần thiết mới có thể decode và đọc nội dung dữ liệu. Encryption có thể là một chiều, có nghĩa là mã hóa được thiết kế để ẩn cleartext đi và không bao giờ có thể giải mã được. Hoặc có thể 2 chiều chuỗi kí tự được mã hóa (ciphertext) có thể chuyển trở lại thành cleartext và đọc được.

Encryption



http://it-ebooks.com

100/14

Figure 1-10: Encryption.

Encryption và các mục tiêu bảo mật

Encryption được dùng để như một kỹ thuật nhằm nâng vấn đề security lên một cấp độ quan trọng. Encryption hỗ trợ sự cần mật bởi vì nó bảo vệ dữ liệu chống các truy cập bất hợp pháp. Nó hỗ trợ tính tích hợp bởi vì rất khó để làm xáo trộn hay thay đổi dữ liệu đã mã hóa mà không bị phát hiện. Nó hỗ trợ việc không thể thoái thác trách nhiệm, không thể chối từ (non-repudiation), bởi vì chỉ có các đối tượng tiến hành mã hóa mới có thể giải mã dữ liệu. Thêm vào đó, một vài hình thức mã hóa được áp dụng trong những xác thực nhằm bảo vệ tối đa passwords khi giao dịch. Qua đây các bạn cũng thấy rằng mã hóa là phương tiện rất tốt nhằm hỗ trợ việc xác thực diễn ra an toàn



NETWORK INFORMATION SECURITY VIETNAM

Giải thích thêm về **non-repudiation** (trách nhiệm không thể thoái thác, thay đổi) Trong thương mại điện tử (e-Commerce) và các giao dịch điện tử khác bao gồm cả ATMs (cash machines: máy rút tiền mặt), thì tất cả các thành phần tham gia giao dịch phải tuyệt đối tin tưởng rằng: giao dịch luôn đảm bảo an toàn; Những đối tượng tham gia giao dịch đã nói rằng họ là ai (authentication), và giao dịch đã được kiểm tra lần cuối cùng trước khi thực hiện. Các hệ thống phải đảm bảo rằng các thành phần tham gia không thể thoái thác (chối bỏ) phiên giao dịch sau đó. Để bảo vệ an toàn trong giao dịch số thì các thành phần tham gia cần áp dụng xác nhận số hay còn gọi chữ ký số (Digital Signatures), đây không chỉ là xác nhận số kiểm tra người gửi mà còn gắn lên giao dịch tem thời gian 'time stamp' xác định rõ phiên giao dịch đã xảy ra tại thời điểm nào và vì thế khó có thể chối bỏ trách nhiệm giao dịch hay không công nhận rằng giao dịch đã diễn ra hợp lệ. Các bạn có thể tham khảo thêm trong thực tế như các vụ khách hàng kiện ra tòa vì tiền trong tài khoản ATM không cánh mà bay, phía ngân hàng có thể dựa vào luật Non- repudiation để chứng minh trước tòa rằng tại thời điểm đó, giao dịch rút tiền đã diễn ra hợp lệ..

Các thuật toán mã hóa

Một thuật toán mã hóa là một quy tắc (rule), một hệ thống (system), hoặc là một cơ chế (mechanism) được sử dụng để mã hóa data. Các thuật toán có thể là nh74ng sự thay thế mang tính máy móc khá đơn giản, nhưng trong mã hóa thông tin điện tử, nhìn chung sử dụng các hàm toán học cực kỳ phức tạp. Thuật toán càng mạnh, càng phức tạp thì càng khó để giải mã.

Encryption Algorithms



http://it-ebooks.com/.../Encryption/

001-10

Figure 1-11: Encryption algorithms.

Một ví dụ đơn giản về áp dụng thuật toán vào mã hóa. Một lá thư với các ký tự alphabe, sau khi sử dụng thuật toán mã hóa đã trở thành các ký tự khác, và bạn dường như không thể hiểu nội dung này (giải mã).

Khóa –Keys



NETWORK INFORMATION SECURITY VIETNAM

Một khóa mã hóa là một mẫu (phần) thông tin đặc biệt được kết hợp với một thuật toán để thi hành mã hóa và giải mã. Mỗi khóa khác nhau có thể "chế tạo" ra các văn bản mã hóa khác nhau, và nếu bạn không chọn đúng khóa thì không tài nào mở được dữ liệu đã mã hóa trên, cho dù biết được mã hóa văn bản trên dùng thuật toán gì. Sử dụng khóa càng phức tạp, mã hóa càng mạnh.

Keys

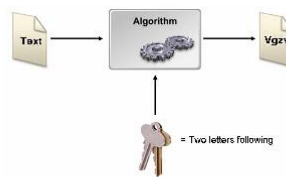


Figure 1-12: Keys.

Ví dụ về một khóa mã hóa đơn giản

Dùng khóa sau để mã hóa nội dung bức thư, khóa như sau: "thay thế mỗi ký tự xuất hiện trong bức thư bằng ký tự thứ 3 đứng sau nó." Cùng thuật toán dạng trên nhưng lần này sử dụng một khóa khác như sau "thay thế mỗi ký tự xuất hiện trong bức thư bằng ký tự đứng trước nó 2 ký tự" và như vậy kết quả của hai bức thư cùng nội dung sau khi sử dụng 2 keys khác nhau sẽ là khác nhau..

Mã hóa hàm băm -Hashing Encryption

Hãy hình dung một củ hành đã được băm nhuyễn ra có thể tái tạo lại củ hành như ban đầu, hay chú Bò đã tiêu hóa một nhúm cỏ khô, liệu có thể tái tạo lại nhúm cỏ khô này, vậy hãy xem mã hóa hàm băm là gì..

Là cách thức mã hóa một chiều tiến hành biến đổi văn bản nhận dạng (cleartext) trở thành hình thái mã hóa mà không bao giờ có thể giải mã. Kết quả của tiến trình hashing còn được gọi là một hash (xử lý băm), giá trị hash (hash value), hay thông điệp đã được tiêu hóa (message digest) và tất nhiên không thể tái tạo lại dạng ban đầu. Trong xử lý hàm băm dữ liệu đầu vào có thể khác nhau về độ dài, thế nhưng độ dài của xử lý Hash lại là cố định. Hashing được sử dụng trong một số mô hình xác thực password . Một giá trị hash có thể được gắn với một thông điệp điện tử (electronic message) nhằm hỗ trợ tính tích hợp của dữ liệu hoặc hỗ trợ xác định trách nhiệm không thể chối từ (non-repudiation).



NETWORK INFORMATION SECURITY VIETNAM

Hashing Encryption



Figure 1-13: Hashing is one-way encryption.

Một ví dụ về dùng Hashing trong CHAP (CHAP là phương thức xác thực truy cập quay số từ xa Remote Access Service, RAS client truy cập vào RAS Server) Hashing được sử dụng để mã hóa passwords trong xác thực CHAP. RAS client sẽ gửi một hash password (passw băm) tới RAS server. RAS server chứa hashe password client đã tạo trước đó. Nếu hashes trùng khớp, passwords được chấp thuận và clients sẽ được server xác thực. Việc gửi một hash thay vì gửi chính password có nghĩa là passwords đó không cần truyền qua mạng trong suốt quy trình server xác thực clients.

Các thuật toán mã hóa Hashing

Một vài thuật toán mã hóa được dùng cho mã hóa hashing.

Thuật toán hashing	Mô tả
Message Digest 5 (MD5)	Thuật toán MD5 tạo thành một dạng thông điệp được mã hóa với 128-bit, được tạo ra bởi Ronald Rivest và hiện là công nghệ mã hóa mang tính phổ biến rộng rãi - public.
Secure Hash Algorithm (SHA) versions 1, 256, 384, và 512 bit.	SHA dựa trên mô hình MD5 nhưng mạnh hơn gấp 2 lần. SHA-1 tạo giá trị hash với 160-bit Trong khi đó SHA-256, SHA-384, và SHA-512 tạo giá trị hash tương ứng với 256-bit, 384-bit, và 512-bit.

Mã hóa đối xứng -Symmetric Encryption

Mã hóa đối xứng hay mã hóa chia sẻ khóa (shared-key encryption) là mô hình mã hóa 2 chiều có nghĩa là tiến trình mã hóa và giải mã đều dùng chung một khóa. Khóa này phải được chuyển giao bí mật giữa hai đối tượng tham gia giao tiếp. Khóa này có



NETWORK INFORMATION SECURITY VIETNAM

thể được cấu hình trong software hoặc được mã hóa trong hardware. Mã hóa đối xứng thực hiện nhanh nhưng có thể gặp rủi ro nếu khóa bị đánh cắp.

Symmetric Encryption

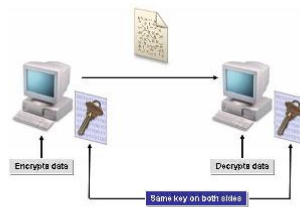


Figure 1-14: Symmetric encryption.

Mã hóa bất đối xứng -Asymmetric Encryption

Mã hóa bất đối xứng, hay mã hóa khóa công khai(public-key encryption), là mô hình mã hóa 2 chiều sử dụng một cặp khóa là khóa riêng (private key) và khóa công (public keys). Thông thường, một thông điệp được mã hóa với private key, và chắc chắn rằng key này là của người gửi thông điệp (message sender). Nó sẽ được giải mã với public key, bất cứ người nhận nào cũng có thể truy cập nếu họ có key này. Chú ý, chỉ có public key trong cùng một cặp khóa mới có thể giải mã dữ liệu đã mã hóa với private key tương ứng. Và private key thì không bao giờ được chia sẻ với bất kỳ ai và do đó nó giữ được tính bảo mật.

Asymmetric Encryption

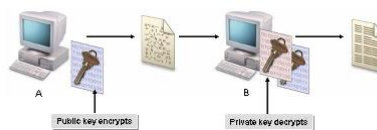


Figure 1-15: Asymmetric encryption.



NETWORK INFORMATION SECURITY VIETNAM

Các cách thức viết mật mã

Có 2 loại viết mật mã chính: viết mật mã theo luồng (stream cipher) và viết mật mã theo khối (block cipher).

Cách thức viết mật mã –cipher types	Mô tả
Stream	là kiểu tiến hành mã hóa mỗi bit dữ liệu tại một thời điểm. Mỗi ký tự dữ liệu thông thường sẽ được viết thành mật mã. Những thuật toán này thực thi khá nhanh. Dữ liệu sau khi được mã hóa có kích cỡ như ban đầu. Phương pháp này tạo ra ít lỗi hơn so với các phương pháp khác và nếu có lỗi xảy ra cũng chỉ ảnh hưởng trên một bit.
Block	Tiến hành mã hóa một khối dữ liệu tại một thời điểm, thường kích cỡ một block mã hóa là 64-bit. An toàn hơn so với stream nhưng đồng thời cũng chậm hơn. Có vài chế độ mã hóa theo block như: <i>Mã hóa ECB (Electronic Code Block)</i> , mỗi block sẽ được mã hóa bởi chính mình. <i>Mã hóa CBC (Cipher Block Chaining)</i> trước khi một block được mã hóa, thông tin từ block trước đó sẽ được thêm vào block. Theo cách này, bạn có thể chắc chắn rằng dữ liệu được lặp lại tại mỗi thời điểm trong tiến trình mã hóa sẽ khác nhau. <i>Mã hóa CFB (Cipher FeedBack mode)</i> có lược đồ mã hóa từng phần của block hơn là toàn bộ blocks .

Các thuật toán mã hóa đối xứng

Một vài thuật toán được sử dụng cho mã hóa đối xứng

Thuật toán mã hóa đối xứng	Mô tả
Data Encryption Standard (DES)	DES là một thuật toán mã hóa đối xứng dạng block-cipher, mã hóa dữ liệu trong từng blocks 64-bit sử dụng một khóa 56-bit với 8 bits chẵn lẻ. Chính độ dài của khóa ngắn cho nên DES là một thuật toán mã hóa hơi yếu.



NETWORK INFORMATION SECURITY VIETNAM

Triple DES (3DES)	3DES là một thuật toán mã hóa đối xứng tiến hành mã hóa dữ liệu thông qua việc xử lý mỗi block 3 lần và mỗi lần dùng một khóa khác nhau. Trước hết nó sẽ mã hóa plain text thành ciphertext dùng một khóa, sau đó lại tiếp tục mã hóa ciphertext với khóa, và tiếp tục mã hóa ciphertext thứ 2 này với một khóa khác nữa
Advanced Encryption Standard (AES) algorithm	AES là thuật toán mã hóa đối xứng block cipher 128-bit được phát triển bởi Vincent Rijmen và được sự hỗ trợ của chính phủ Mỹ xem như một thuật toán thay thế DES. AES cũng được gọi là Rijndael "Rhine-dale" phát âm theo tên người tạo ra. Rijndael là một trong năm thuật toán được sự hậu thuẫn của AES.
Rivest Cipher (RC) 4, 5, and 6	Thuật toán RC bao gồm một series được phát triển bởi Ronald Rivest. Tất cả có chiều dài khóa khác nhau. RC4 là một stream cipher. RC5 và RC6 là các block ciphers với các kích cỡ khác nhau
Skipjack	Skipjack là một thuật toán block cipher được thiết kế bởi Cơ quan bảo mật quốc gia Hoa kỳ - US National Security Agency (NSA) được sử dụng trong chip Clipper Fortezza PC card
Blowfish	Blowfish là một thuật toán mã hóa miễn phí dùng block 64-bit sử dụng khóa có độ dài khác nhau. Được phát triển bởi Bruce Schneier.
CAST-128	CAST-128, được đặt theo tên người phát triển là Carlisle Adams và Stafford Tavares, là một thuật toán mã hóa đối xứng có chiều dài khóa 128-bit. Là một trong những đối thủ cạnh tranh chính của AES.

Thuật toán mã hóa bất đối xứng	Mô tả
Rivest Shamir Adelman (RSA)	RSA, được đặt tên theo người thiết kế là Ronald Rivest, Adi Shamir, và Len



NETWORK INFORMATION SECURITY VIETNAM

	Adelman, là thuật toán thành công đầu tiên sử dụng cho mã hóa khóa công (public-key encryption). Nó có độ dài khóa khác nhau và các kích cỡ block khác nhau. RSA vẫn được xem là rất an toàn nếu được triển khai đúng với các khóa có chiều dài cao.
Diffie-Hellman	Diffie-Hellman là một giao thức mã hóa cung cấp khóa chuyển đổi an toàn. Được mô tả vào năm 1976, được hình thành trên nền tảng của các kỹ thuật mã hóa public-key phổ biến bao gồm cả RSA.
Elgamal	Elgamal là một thuật toán mã hóa public-key được phát triển bởi Taher Elgamal. Nó cũng dựa trên nền tảng của Diffie-Hellman.
Paillier Cryptosystem	Paillier cryptosystem là một thuật toán mã hóa bất đối xứng được phát triển bởi Pascal Paillier.

Chữ ký số -Digital Signatures

Một chữ ký số là một giá trị hash được mã hóa gắn vào thông điệp nhằm xác định người gửi là ai (sender). Digital signatures nhằm đảm bảo tính tích hợp trọn vẹn của thông điệp khi gửi (integrity), nếu vì lý do nào đó khiến signature bị thay đổi trong quá trình truyền giá trị hash của người nhận (receiver) không trùng khớp giá trị hash ban đầu tính tích hợp không còn, không đảm bảo sự an toàn. Signatures còn hỗ trợ *non-repudiation* bởi vì giá trị hash được mã hóa chỉ duy nhất và xuất phát từ người gửi.

Digital Signatures

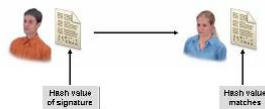


Figure 1-16: Digital signatures.



NETWORK INFORMATION SECURITY VIETNAM

Digital Signatures và mã hóa bất đối xứng

Các thuật toán mã hóa bất đối xứng, có thể kết hợp với các thuật toán hash để tạo ra các digital signatures. Trong tình huống này, người gửi sẽ tạo ra một phiên bản hashed của thông điệp gửi đi, sau đó mã hóa chính hash này với private key của anh ta. Hash sau khi được mã hóa sẽ được gắn vào message như một digital signature. Như vậy người gửi (sender) sẽ cung cấp Digital Signatures và người nhận (receiver) nhận thông điệp đã "xác nhận số" ấy phải sử dụng public key tương ứng để open. Khi người nhận dùng public key để giải mã signature sẽ phát hiện được phiên bản của hash. Điều này sẽ xác minh chính xác người gửi, vì nếu public và private keys không gặp nhau, người nhận sẽ không thể nào giải mã được signature. Người nhận sau đó tạo một phiên bản hash của tài liệu với public key và so sánh 2 giá trị hash này. Nếu chúng gặp nhau, điều đó chứng tỏ dữ liệu không bị thay đổi. Quy trình này hơi ngược với quy trình mã hóa dữ liệu dùng public-key có nghĩa là người gửi sẽ dùng public key để mã hóa dữ liệu và người nhận sẽ dùng private key để giải mã.

Ví dụ: Có thể mượn tượng đơn giản là: A cần gửi cho B thông điệp bí mật. Trước khi gửi A hỏi B " Anh B, anh có ổ khóa (public-key) nào không hãy gửi cho tôi. B reply: Ok tôi có một ổ khóa chắc chắn đây, anh dùng nó để khóa thông điệp sẽ gửi cho tôi nhé. A trả lời, vâng anh đưa ổ khóa cho tôi để tôi khóa thông điệp lại và sẽ chuyển nó đến cho anh.. Sau đó A chuyển thông điệp dùng ổ khóa của B đến cho B, B dùng chìa khóa riêng của mình (private-key) để tra vào ổ khóa và open..các bạn thấy đơn giản không nào.