QUẢN LÝ KHÓA

Giáo viên: Phạm Nguyên Khang
pnkhang@cit.ctu.edu.vn

Nội dung

- Tổng quan
- Phân phối khóa công khai
- Phân phối khóa bí mật
- Trao đổi khóa với Diffie-Hellman

Tổng quan

Việc phân phối khóa sử dụng mã hóa khóa công khai trong 2 ngữ cảnh:

- Phân phối khóa công khai
  - Thông báo rộng rãi (public announcement)
  - Thư mục công cộng (publicly avalable directory)
  - Thẩm quyền phân phối khóa (public-key authority)
  - Chứng chỉ khóa công cộng (public-key certificates)
- Phân phối khóa bí mật
  - Phân phối đơn giản (simple secret key distribution)
  - Phân phối với tin cậy và chứng thực (secret key distribution with confidentiality and authentication)

Phân phối khóa công cộng

Thông báo rộng rãi

- Người tham gia vào hệ thống (đã thống nhất một giải thuật mã hóa, ví dụ RSA) gởi khóa công khai đến tất cả mọi người.
- Khuyết điểm
  - Người giả dạng có thể mạo danh một ai đó trong hệ thống
  - Phải mất một thời gian để có thể phát hiện có kẻ mạo danh → mất khá nhiều thông tin

Thư mục công cộng

- Việc quản lý và bảo trì khóa được đảm nhiệm bởi một tổ chức tin cậy.
- Quy trình hoạt động
  1. Nhà thẩm quyền (authority) duy trì một thư mục gồm các mục có dạng {<định danh>, <khóa công cộng>}
  2. Người tham gia đăng ký một khóa công khai. Việc đăng ký phải được bảo mật.
  3. Người tham gia có thể thay thế khóa cũ vào bất kỳ lúc nào (khóa công khai đã sử dụng lâu hoặc bị lộ khóa bí mật)
  4. Theo định kỳ, nhà thẩm quyền công khai hoặc cập nhật toàn bộ thư mục.
  5. Người tham gia có thể truy cập thư mục trực tuyến →thông tin liên lạc cần được chứng thực (**?**).

Thư mục công cộng

- Khuyết điểm:
  - Nếu kẻ tấn công có được khóa bí mật của nhà thẩm quyền → có thể giả mạo khóa bí mật của các người tham gia.

Thẩm quyền phân phối khóa

- Phân phối khóa sẽ an toàn hơn bằng cách áp dụng chặt chẽ việc điều khiển lấy khóa từ thư mục.
- Trước tiên, nhà thẩm quyền công khai khóa công cộng của mình. Tiếp theo, quy trình phân phối khóa như sau:
  1. A gởi một thông điệp gồm nhãn thời gian (timestamp) và yêu cầu (request) đến nhà thẩm quyền, yêu cầu gởi khóa công cộng của B.
  2. Nhà thẩm quyền trả lời bằng một thông điệp được mã hóa bằng khóa cá nhân K_{sAuth}. A cần được đảm bảo rằng thông điệp đến từ nhà thẩm quyền. Thông điệp gồm có:
     - Khóa công cộng K_{pB}, A dùng để mã hóa thông điệp gởi cho B.
     - Request ban đầu, A dùng đối sánh với request trước đó và kiểm tra xem request có bị thay đổi không.
     - Nhãn thời gian ban đầu, A có thể xác định đây không phải là thông điệp cũ và chứa khóa hiện thời của B.

Thẩm quyền phân phối khóa

3. A lưu khóa K_{pB}, dùng mã hóa thông điệp bao gồm một định danh của A (ID_A) và một giá trị N_1 (nonce) sử dụng duy nhất trong lần giao dịch này.
4. B lấy khóa công khai của A (giống B1 và B2)
5. B gởi một thông điệp đến A, được mã hóa bằng K_{pA}, bao gồm giá trị N_1 của A và giá trị N_2 được B tạo ra. Vì chỉ B có thể giải mã thông điệp ở B3 và sự hiện diện của N_1 đảm bảo A rằng người liên lạc chính là B.
6. A gởi lại N_2, mã hóa bằng K_{pB}, đảm bảo B rằng người liên lạc là A.

Hai bước 5 và 6 được yêu cầu để đảm bảo tính bảo mật.

Thẩm quyền phân phối khóa

- 4 bước đầu có thể chỉ thực hiện 1 lần. Các khóa sẽ được lưu trữ lại cho việc sử dụng về sau. Kỹ thuật này được gọi là caching.
- Người dùng cần làm tươi (refresh) các khóa để cập nhật các khóa hiện thời.
- Khuyết điểm: bottleneck

Chứng chỉ khóa công cộng

- Chứng chỉ được sử dụng để trao đổi khóa giữa các người dùng, không cần liên lạc với nhà thẩm quyền.
- Mỗi chứng chỉ chứa một khóa công cộng và các thông tin khác được tạo ra bởi một nhà thẩm quyền cung cấp chứng chỉ (certificate authority). Các yêu cầu cần đạt:
  - Bất cứ ai cũng có thể đọc chứng chỉ để xác định tên và khóa công khai của người sở hữu.
  - Bất cứ ai cũng có thể kiểm tra nguồn gốc của chứng chỉ.
  - Chỉ có nhà thẩm quyền có thể tạo và cập nhật chứng chỉ.
  - Bất cứ ai cũng có thể kiểm tra thời gian lưu hành của chứng chỉ.

Chứng chỉ khóa công cộng

- Quy trình thực hiện:
  1. A cung cấp khóa công khai cho nhà thẩm quyền để yêu cầu một chứng chỉ. Công việc này phải được bảo mật.
  2. Nhà thẩm quyền cung cấp chứng chỉ dưới dạng $C_A = E_{KsAuth}[T, ID_A, K_{pA}]$ (K_{sAuth} là khóa bí mật của nhà thẩm quyền)
  3. A gởi chứng chỉ này đến B (nơi cần giao tiếp).
  4. B tính lại $(T, ID_A, K_{pA}) = D_{KpAuth}[C_A]$. Vì chứng chỉ có thể đọc được chỉ với khóa công khai của nhà thẩm quyền → xác định được nguồn gốc. T dùng để xác thực tính hiện thời của khóa.

Chứng chỉ khóa công cộng

- Nhãn thời gian T là cần thiết trong trường hợp khóa bí mật của A bị lộ. A cần tạo khóa mới và cập nhật lại chứng chỉ.
- T thường được dùng để xác định ngày hết hạn của chứng chỉ.

Phân phối khóa bí mật

Phân phối đơn giản

- Quy trình thực hiện:
  1. A tạo cặp khóa K_{pA}/K_{sA}, gởi một thông điệp đến B bao gồm K_{pA} và định danh ID_A
  2. B tạo khóa bí mật K_s, mã hóa bằng K_{pA} và gởi đến A
  3. A tính $D_{KsA}[E_{KpA}[K_s]]$ để phục hồi khóa bí mật.
  4. Sau khi sử dụng xong cặp khóa K_{pA}/K_{sA} được hủy bỏ ở cả 2 phía.

Phân phối đơn giản

- Phương pháp này vẫn có lỗ hổng:
  1. A tạo cặp khóa K_{pA}/K_{sA}, gởi một thông điệp đến B bao gồm K_{pA} và định danh ID_A
  2. E can thiệp vào thông điệp, tạo cặp khóa K_{pE}/K_{sE} và gởi $K_{pE} || ID_A$
  3. B tạo khóa bí mật K_s, mã hóa bằng K_{pE} và gởi đến A
  4. E lại can thiệp vào thông điệp, biết được K_s
  5. E gởi $E_{KpA}[K_s]$ đến A.

  Cả A và B đều không biết E có được K_s.

Phân phối với tin cậy và chứng thực

- Giả sử A và B đều biết được khóa công cộng của nhau thông qua một giao thức trao đổi khóa nào đó
- Quy trình thực hiện
  1. A dùng K_{pB} để mã hóa thông điệp bao gồm ID_A và giá trị N_1 (nonce), chỉ sử dụng duy nhất trong giao dịch này.
  2. B gởi thông điệp được mã hóa bằng K_{pA} bao gồm N_1 và N_2 do B tạo ra. Vì chỉ có B mã hóa được thông điệp ở B1 và sự có mặt của N_1 đảm bảo A rằng người đang giao tiếp là B.
  3. A gởi lại N_2, mã hóa với K_{pB}.
  4. A tạo khóa K_S và gởi $M = E_{KpB}[E_{KsA}[K_S]]$ cho B. Mã hóa với K_{pB} đảm bảo chỉ có B đọc được. Mã hóa với K_{sA} đảm bảo chỉ có A gởi thông điệp này.
  5. B tính lại $K_S=D_{KpA}[K_{sB}[M]]$.

Trao đổi khóa Diffie-Hellman

Diffie-Hellman

- DH không phải là giải thuật mã hóa. DH áp dụng kỹ thuật khóa công khai để tạo khóa bí mật cho giải thuật mã hóa đối xứng.
- Giải thuật
  - a, q nguyên tố cho trước.
  - A và B chọn 2 số bí mật X_A và $X_B < q$
  - $Y_A = a^{XA} \bmod q$
  - $Y_B = a^{XB} \bmod q$
  - $K = (Y_B)^{XA} \bmod q = (Y_A)^{XB} \bmod q$
- Các giá trị X thường có độ dài 160 bits để đảm bảo tính an toàn.
- Khuyết điểm: replay attack
  - Cho ví dụ