Mật mã & Ứng dụng

Trần Đức Khánh
Bộ môn HTTT – Viện CNTT&TT
ĐH BKHN

Chủ đề

- Hệ Mật mã không Khóa
- Hệ Mật mã khóa bí mật (đối xứng)
- Hệ Mật mã khóa công khai (bất đối xứng)
- Hàm băm, chữ ký số
- Quản lý khóa, giao thức mật mã,…

Giao thức mật mã

- Giao thức mật mã
- Thống nhất khóa
  - Diffie-Hellman
- Xác thực
  - Needham-Schroeder

Giao thức

- Giao thức
  - Một chuỗi các bước thực hiện
  - Các bước thực hiện phải tường minh
  - Tất cả các tình huống phải được dự tính và có các bước thực hiện trước
  - Có ít nhất 2 bên tham dự
  - Các bên tham dự phải hiểu biết và tuân thủ các bước thực hiện

Giao thức mật mã

- Giao thức truyền thông = Giao thức trong đó các bước thực hiện là trao đổi thông tin
- Giao thức mật mã = Giao thức truyền thông + Mật mã học
- Thông thường một giao thức mật mã kết hợp các khía cạnh sau
  - Thống nhất khóa
  - Xác thực
  - Mã hóa
  - Chống phủ nhận

Mô tả giao thức mật mã

- Các thực thể tham gia giao thức
- Các bước thực hiện của giao thức
  1. Bước 1
  2. Bước 2
  3. …
- Một bước thực hiện
  - Alice gửi cho Bob thông tin M
    - Aice -> Bob: M

Giao thức mật mã SSL/TLS

- SSL/TLS
  - Giao thức mật mã để trao đổi thông tin trên Internet
  - SSL được phát triển bởi Netscape
  - TLS kế thừa từ SSL phiên bản 3.0
  - Ứng dụng
    - Duyệt Web, Email, IM, VoIP,…
    - Thương mại điện tử: Visa, MasterCard, American Express,…

Khởi tạo phiên SSL/TLS

- Các pha khởi tạo SSL/TSL
  1. Bắt tay
  2. Thương lượng lựa chọn giải thuật
     - Thống nhất khóa: RSA, Diffie-Hellman,…
     - Mã hóa khóa đối xứng: 3DES, AES,…
     - Chữ ký số: RSA, DSA,…
     - Hàm băm: SHA, MD5,…
  3. Xác thực
  4. Thống nhất khóa

Khởi tạo phiên SSL/TLS

1. Client chào Server
   - C -> S: Hi, I'm Client
2. Server chào Client
   - S -> C: Hi, I'm Server
3. Server xác thực với Client
   - S -> C: PK, sig(PK)
4. Client kiểm định chữ ký sig(PK)
5. Client tạo ra một số ngẫu nhiên bí mật
   - MS
6. Client gửi Server MS mã hóa
   - C - > S: y=E(PK,MS)
7. Server giải mã y
   - MS = D(K,y)
8. Client và Server tạo 2 khóa bí mật
   - K1, K2 = h(MS)

Giao thức mật mã

- Giao thức mật mã
- Thống nhất khóa
  - Diffie-Hellman
- Xác thực
  - Needham-Schroeder

Thống nhất khóa

- Trao đổi thông tin bí mật với tốc độ nhanh
  - Mật mã khóa đối xứng
- Thiết lập và trao đổi khóa
  - Các thực thể tham gia phải thống nhất khóa đối xứng
  - Quá trình thống nhất khóa phải đảm bảo
    - Tính bí mật
    - Tính toàn vẹn

Giao thức Diffie-Hellman

- 1976, Diffie và Hellman phát minh giao thức thống nhất khóa
  - Hình thành và trao đổi khóa chung bí mật trên một kênh truyền tin không an toàn
- Sử dụng các kết quả trong lý thuyết nhóm số nguyên nhân tính đồng dư
- Dựa trên độ phức tạp của bài toán
  - Logarit rời rạc

Diffie-Hellman

1. Alice (A) chọn và gửi cho Bob (B) số nguyên tố p và một phần tử nguyên thủy g thuộc nhóm nhân tính mod p
   - A -> B: p,g
2. Alice chọn một số tự nhiên ngẫu nhiên a và gửi g^a mod p cho Bob
   - A -> B: g^a mod p
3. Bob chọn một số tự nhiên ngẫu nhiên b và gửi g^b mod p cho Alice
   - B -> A: g^b mod p
4. Alice tính (g^b mod p)^a mod p
5. Bob tính (g^a mod p)^b mod p
6. Khóa chung bí mật g^(a*b) mod p

Diffie-Hellman

- Ví dụ: p = 23, g = 5, a = 6, b = 15
  1. Alice gửi Bob p=23, g=5
     - A -> B: 23,5
  2. Alice chọn a=6, và gửi Bob g^a mod p = 5^6 mod 23 = 8
     - A -> B: 8
  3. Bob chọn b=15, và gửi Alice g^b mod p = 5^15 mod 23 = 19
     - B -> A: 19
  4. Alice tính
     - 19^6 mod 23 = 2
  5. Bob tính
     - 8^15 mod 23 = 2
  6. Khóa K = 2

Độ an toàn của Diffie-Hellman

- Khóa bí mật
  - Bài toán Diffie-Hellman
    - Biết g, g^a, g^b. Tìm g^(a*b)?
  - Bài toàn Logarit rời rạc
    - Biết g^a. Tìm a?
- Tính xác thực
  - Tấn công dạng “Man-in-the-middle”
    - Alice và Bob muốn thống nhất khóa bí mật
    - Eve là kẻ ở giữa
    - Alice và Eve thống nhất g^(a*e)
    - Bob và Eve thống nhất g^(b*e)

Giao thức mật mã

- Giao thức mật mã
- Thống nhất khóa
  - Diffie-Hellman
- Xác thực
  - Needham-Schroeder

Xác thực

- Rất nhiều ứng dụng đòi hỏi các thực thể tham gia phải chứng minh danh tính
  - Mô hình Client-Server an toàn
- Quá trình xác nhận danh tính của các thực thể phải đảm bảo
  - Tính toàn vẹn
    - Chống mạo danh

Giao thức Needham-Schroeder

- 1978, Needham và Schroeder phát minh giao thức xác thực trên mạng máy tính không an toàn
  - Chứng minh nhận dạng của các thực thể trao đổi thông tin
  - Ngăn chặn nghe lén, thay đổi thông tin
- Ứng dụng
  - Xác thực trong mô hình Client-Server: Kerberos
- 2 loại giao thức
  - Khóa đối xứng
  - Khóa công khai

Needham-Schroeder khóa đối xứng

- Alice (A) muốn trao đổi thông tin với Bob (B)
- Alice và Bob cùng tin tưởng một Server (S) trung gian
  - Kas khóa đối xứng giữa A va S
  - Kbs khóa đối xứng giữa B va S
  - Na và Nb là các “nonce”
  - Kab là khóa đối xứng giữa A và B

Needham-Schroeder khóa đối xứng

1. A gửi thông tin của mình và B cho S
   - A -> S: A,B,Na
2. S gửi khóa Kab cho A, thông tin được mã hóa
   - S -> A: {Na,Kab,B,{Kab,A}_Kbs}_Kas
3. A gửi khóa Kab cho Bob, thông tin được mã hóa
   - A -> B: {Kab,A}_Kbs
4. B trả lời A đã nhận được khóa Kab, thông tin được mã hóa
   - B -> A: {Nb}_Kab
5. A báo B rằng A sẵn sàng và đang giữ khóa Kab, thông tin được mã hóa
   - A -> B: {Nb-1}_Kab

Tấn công Needham-Schroeder khóa đối xứng

- Tấn công “Replay”
  - Charlie lấy được {Kab,A}_Kbs và sử dụng Kab ở một phiên trao đổi thông tin khác với Bob mà Bob không phát hiện được

Ngăn chặn tấn công “Replay”

- Giải pháp dùng trong Kerberos
  - Tem thời gian (Timestamp)
  - Nonce

Needham-Schroeder khóa công khai

- Alice (A) muốn trao đổi thông tin với Bob (B)
- Alice và Bob cùng tin tưởng một Server (S) trung gian
  - Ka và ka khóa riêng và công khai của A
  - Kb và kb khóa riêng và công khai của B
  - Ks và ks khóa riêng và công khai của S
  - Na và Nb là các “nonce”

Needham-Schroeder khóa công khai

1. A yêu cầu S khóa công khai của B
   - A -> S: A,B
2. S gửi khóa công khai của B cho A
   - S -> A: {kb,B}_Ks
3. A gửi nonce của mình cho B
   - A -> B: {Na,A}_kb
4. B yêu cầu S khóa công khai của A
   - B -> S: B,A
5. S gửi khóa công khai của A cho B
   - S -> B: {ka,A}_Ks
6. B gửi nonce của mình và của A cho A
   - B -> A: {Na,Nb}_ka
7. A khẳng định đã nhận được nonce của B
   - A ->B: {Nb}_kb

Tấn công Needham-Schroeder khóa công khai

- Tấn công "Man-in-the-middle"
  1. A -> I: {Na,A}_ki
  2. I -> B: {Na,A}_kb
  3. B -> I: {Na,Nb}_ka
  4. I -> A: {Na,Nb}_ka
  5. A -> I: {Nb}_ki
  6. I -> B: {Nb}_kb

Ngăn chặn tấn công "Man-in-the-middle"

- Thay
  - B -> A: {Na,Nb}_ka
- Bởi
  - B -> A: {Na,Nb,B}_ka