MẬT MÃ ỨNG DỤNG TRONG AN TOÀN THÔNG TIN

Bài 07. Giao thức mật mã

1. Một số khái niệm
2. Xác thực bằng mật khẩu
3. Xác thực bằng thách đố - giải đố
4. Một số giao thức khác

Tài liệu tham khảo

1. Nguyễn Ngọc Cương, Trần Thị Lượng, **Mật mã ứng dụng trong ATTT**
2. Trần Văn Trường, **Mật mã học nâng cao**, Hv KTMM, 2007
3. Behrouz A. Forouzan, **Cryptography and Network security** (Chapter 14), McGraw Hill, 2007
4. Mihir Bellare and Phillip Rogaway, **Introduction to Modern Cryptography** (Chapter 7)

3

1. Một số khái niệm
2. Xác thực bằng mật khẩu
3. Xác thực bằng thách đố - giải đố
4. Một số giao thức khác

Một số khái niệm trong xác thực

- **Xác thực** là một thủ tục mà qua đó, một thực thể thiết lập một tính chất được yêu cầu cho một thực thể khác
- **Thực thể**: người dùng, tiến trình, client, server
- **Tính chất được yêu cầu**: có mật khẩu đúng...

5

Một số khái niệm trong xác thực

- **Tính sống của thực thể**: Tính sống của thực thể A đối với một thực thể B là tính chất cho biết rằng thực thể A đang tham gia vào phiên liên lạc với thực thể B
- Thông điệp M mà B nhận được có thể **được tạo bởi A** nhưng chưa chắc đã **được gửi bởi A**!

➔ Tính sống: các thông điệp mà B nhận được là do A gửi chứ không phải ai khác!

6

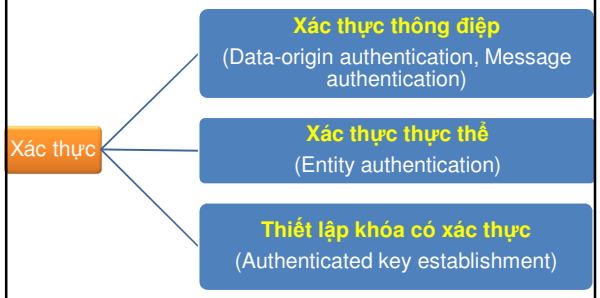
Một số khái niệm trong xác thực

❑**Tính tươi của thông điệp**: là khi thực thể nhận thông điệp cho rằng khoảng thời gian giữa thời điểm gửi và thời điểm nhận thông điệp là đủ nhỏ.

- Giao thức thời gian thực: vài giây;
- Hệ thống liên lạc mật mã: khóa ngày, khóa giờ,...
- Ngân hàng: thời hạn séc

7

Dạng xác thực



8

Một số khái niệm trong xác thực

❑**Xác thực thực thể** là việc một thực thể thiết lập một giao tiếp sống với một thực thể thứ hai mà định danh của thực thể này đúng là định danh mà thực thể thứ nhất yêu cầu [2].

❑**Entity authentication** is a technique designed to let one party prove the identity of another party [3]

9

Một số khái niệm trong xác thực

❑**Xác thực thông điệp** là một cơ chế cho phép khẳng định rằng thông điệp không bị thay đổi trong quá trình truyền và bên nhận có thể kiểm tra được nguồn gốc của thông điệp

10

Xác thực thông điệp vs. Toàn vẹn dữ liệu

Xác thực thông điệp	Toàn vẹn dữ liệu
Trong liên lạc	Có thể trong liên lạc hay trong lưu trữ
Xác định nguồn gốc	Không yêu cầu
Xác định tính tươi	Không yêu cầu

11

1. Một số khái niệm
2. Xác thực bằng mật khẩu
3. Xác thực bằng thách đố - giải đố
4. Một số giao thức khác

Xác thực bằng mật khẩu

❑**Xác thực bằng mật khẩu:**

- xác thực thực thể
- xác thực dựa vào «cái gì đó mà người dùng biết»

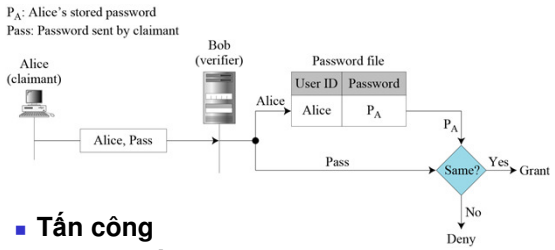
❑**Loại mật khẩu**

- mật khẩu cố định
- mật khẩu một lần

13

Xác thực bằng mật khẩu

1. Lưu mật khẩu dạng rõ

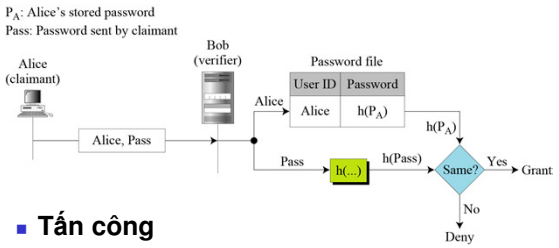


- **Tấn công**
  - **Chặn bắt mật khẩu**
  - **Chiếm file chứa mật khẩu**

14

Xác thực bằng mật khẩu

2. Lưu mật khẩu dạng băm

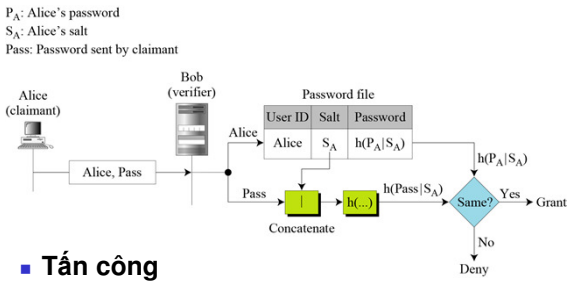


- **Tấn công**
  - **Tấn công từ điển 1 mật khẩu**
  - **Tấn công từ điển cả file**

15

Xác thực bằng mật khẩu

3. Lưu mật khẩu dạng băm có salt

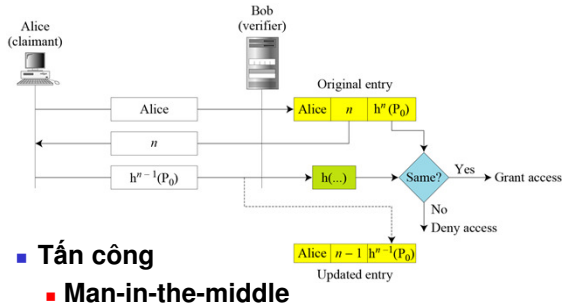


- **Tấn công**
  - **Tấn công từ điển 1 mật khẩu**

16

Xác thực bằng mật khẩu

4. Mật khẩu một lần Lamport



- **Tấn công**
  - **Man-in-the-middle**
  - **Tấn công từ điển!?**

17

Xác thực bằng mật khẩu

❑**Nhận xét:**

- claimant chứng minh bản thân bằng cách cung cấp yếu tố bí mật
- yếu tố bí mật được truyền trực tiếp qua kênh không an toàn

18

1. Một số khái niệm
2. Xác thực bằng mật khẩu
3. Xác thực bằng thách đố - giải đố
4. Một số giao thức khác

Xác thực bằng thách đố - giải đố

- Claimant có thể chứng minh rằng mình biết yếu tố bí mật mà không cần gửi trực tiếp yếu tố bí mật đó
- Thách đố (challenge) là một giá trị thay đổi theo thời gian không phụ thuộc ý muốn của claimant (được sinh ngẫu nhiên bởi verifier; hoặc giá trị bộ đếm)
- Giải đố (response) là kết quả biến đổi challenge và yếu tố bí mật bằng một hàm nào đó

20

Xác thực bằng thách đố - giải đố

❑**Ký hiệu quy ước (1/2)**

- **Alice (A), Bob (B), Trent (T), Malice (M)**... là tên của thực thể;
- **Alice → Bob: M**: Alice gửi M đến Bob;
- **{M}K**: mã hóa M bởi khóa K;

21

Xác thực bằng thách đố - giải đố

❑**Ký hiệu quy ước (1/2)**

- **K_A**: khóa công khai của A;
- **K_{AB}**: khóa bí mật chia sẻ giữa A và B;
- **T_X**: tem thời gian tạo bởi thực thể X;
- **N_X**: số ngẫu nhiên tạo bởi thực thể X;
- **$sig_A(M)$**: chữ ký số tạo bởi thực thể A trên thông báo M;

22

Xác thực bằng thách đố - giải đố

I. Mật mã đối xứng + nounce

❑ **Điều kiện**

Alice và Bob chia sẻ khóa bí mật K_{AB}

❑ **Yêu cầu**

Bob xác thực được Alice

23

Xác thực bằng thách đố - giải đố

❑ **Thực hiện**

1. Alice → Bob: "Alice" — **Initialization**
2. Bob → Alice: N_B; — **Challenge**
3. Alice → Bob: $\{M, N_B\}K_{AB}$ — **Response**
4. Bob giải mã lời giải đố — **Decision**

Giải thích quyết định của Bob!

24

Xác thực bằng thách đố - giải đố

II. Hàm một chiều + nounce

❑ **Điều kiện**

Alice và Bob chia sẻ khóa bí mật K_{AB}

❑ **Yêu cầu**

Bob xác thực được Alice

25

Xác thực bằng thách đố - giải đố

❑ **Thực hiện**

1. Alice → Bob: "Alice"
2. Bob → Alice: N_B;
3. Alice → Bob: M, MDC(K_{AB}, M, N_B);
4. Bob tính lại MDC(K_{AB}, M, N_B)
   - Chấp nhận M nếu hai MDC trùng nhau;
   - Từ chối M nếu hai MDC không trùng nhau

MCD = Manipulation Detection Code

26

Xác thực bằng thách đố - giải đố

III. Chữ ký số + nounce

❑ **Điều kiện**

Alice có cặp khóa bí mật, công khai

❑ **Yêu cầu**

Bob xác thực được Alice

27

Xác thực bằng thách đố - giải đố

❑ **Thực hiện**

1. Alice → Bob: "Alice"
2. Bob → Alice: N_B
3. Alice → Bob: M, sig_A(M, N_B)
4. Bob sử dụng K_A để kiểm tra chữ ký
   - Chấp nhận M nếu chữ ký hợp lệ;
   - Từ chối M nếu chữ ký không hợp lệ;

28

Xác thực bằng thách đố - giải đố

IV. Mật mã đối xứng + timestamp

❑ **Điều kiện**

- Alice và Bob thống nhất cơ chế nhãn thời gian
- Alice và Bob chia sẻ khóa bí mật K_{AB}

❑ **Yêu cầu**

Bob xác thực được Alice

29

Xác thực bằng thách đố - giải đố

❑ **Thực hiện**

1. Alice → Bob: "Alice", $\{M, T_A\}K_{AB}$
2. Bob giải mã thông điệp
   - Chấp nhận M nếu T_A hợp lệ
   - Từ chối M nếu T_A không hợp lệ

30

Xác thực bằng thách đố - giải đố

V. Hàm một chiều + timestamp

❑ **Điều kiện**

– Alice và Bob thống nhất cơ chế nhãn thời gian

– Alice và Bob chia sẻ khóa bí mật K_{AB}

❑ **Yêu cầu**

Bob xác thực được Alice

31

Xác thực bằng thách đố - giải đố

❑ **Thực hiện**

1. Alice → Bob: M, T_A, MDC(K_{AB}, M, T_A);
2. Bob kiểm tra T_A, tính lại MDC(K_{AB}, M, T_A)
   – Chấp nhận M nếu hai MDC trùng nhau;
   – Từ chối M nếu hai MDC không trùng nhau

32

Xác thực bằng thách đố - giải đố

VI. Chữ ký số + timestamp

❑ **Điều kiện**

– Alice và Bob thống nhất cơ chế nhãn thời gian

– Alice có cặp khóa bí mật, công khai

❑ **Yêu cầu**

Bob xác thực được Alice

33

Xác thực bằng thách đố - giải đố

❑ **Thực hiện**

1. Alice → Bob: M, T_A, sig_A(M, T_A)
2. Bob sử dụng K_A để kiểm tra chữ ký
   – Chấp nhận M nếu chữ ký hợp lệ;
   – Từ chối M nếu chữ ký không hợp lệ;

34

Xác thực bằng thách đố - giải đố

❑ **Challenge là nhãn thời gian**

- Tránh được sự tương tác nên thích hợp cho những ứng dụng không tương tác (ví dụ như thư điện tử)
- Khó khăn trong việc đồng bộ đồng hồ

35

Xác thực bằng thách đố - giải đố

Các bên tham gia hoặc đã có khóa bí mật chung (K_{AB}), hoặc đã biết khóa công khai của nhau (K_A hay K_B). Vậy tại sao cần xác thực? Liệu có thể đơn giản là truyền thông báo và mã hóa (hoặc ký) nó?

A → B: $\{M\}K_{AB}$;
hoặc
A → B: M, sig_A(M).

36

1. Một số khái niệm
2. Xác thực bằng mật khẩu
3. Xác thực bằng thách đố - giải đố
4. Một số giao thức khác

Một số giao thức khác

❑**Các giao thức đã xem xét**

- Xác thực một chiều
- Xác thực trực tiếp giữa hai bên với nhau

❑**Một số giao thức khác**

- Xác thực lẫn nhau ba bước ISO
- Xác thực qua bên thứ ba tin cậy Woo-Lam
- Thêm phụ gia để chống tấn công từ điển
- Thỏa thuận khóa có xác thực

38

Xác thực lẫn nhau ba bước ISO (1/2)

Xác thực lẫn nhau ba bước ISO

❑ **Giả thiết**:

- A có chứng thư số khóa công khai CertA,
- B có chứng thư số khóa công khai CertB

❑ **Yêu cầu**:

- A và B đạt được sự xác thực lẫn nhau

39

Xác thực lẫn nhau ba bước ISO (2/2)

Cách thức:

1. B → A: N_B;
2. A → B: CertA, TokenAB
3. B → A: CertB, TokenBA

Trong đó:

TokenAB = N_A || N_B || B || $sig_A(N_A$ || N_B || B)

TokenBA = N_B || N_A || A || $sig_B(N_B$ || N_A || A)

40

Giao thức Woo-Lam (1/2)

Giao thức Woo-Lam

❑ **Giả thiết**:

- A và B cùng tin cậy bên thứ ba T
- A và T chia sẻ khóa K_{AT},
- B và T chia sẻ khóa K_{BT}

❑ **Yêu cầu**:

- B xác thực được A

41

Giao thức Woo-Lam (2/2)

1. A → B: "Alice"
2. B → A: N_B
3. A → B: $\{N_B\}K_{AT}$
4. B → T: {"Alice", $\{N_B\}K_{AT}\}K_{BT}$
5. T → B: $\{N_B\}K_{BT}$
6. B giải mã thông điệp của T
   - Thu được N_B thì A được xác thực;
   - Ngược lại, A bị từ chối.

42

Thêm phụ gia vào giao thức (1/2)

❑**Giả thiết**
- U và H đã thỏa thuận mật khẩu P_U

❑**Yêu cầu**
- H và U xác thực lẫn nhau
- H và U thỏa thuận được khóa K bí mật
- Không truyền P_U và $H(P_U)$ qua kênh không an toàn

43

Thêm phụ gia vào giao thức (2/2)

1. U → H: ID_U, $\{\varepsilon_U\}P_U$ //ε_U = ngẫu nhiên
2. H → U: $\{\{K\}\varepsilon_U\}P_U$ //K = ngẫu nhiên
3. U → H: $\{N_U\}K$
4. H → U: $\{N_U, N_H\}K$
5. U → H: $\{N_H\}K$ //kiểm tra N_U trước
6. H giải mã và kiểm tra N_H

44

Thỏa thuận khóa có xác thực

❑**Giả thiết**
- Tham số hệ thống:
  - Nhóm hữu hạn với phần tử sinh **a**
  - Thuật toán mật mã đối xứng E
- Alice, Bob có chứng thư số CertA, CertB

❑**Yêu cầu**
- Alice, Bob xác thực lẫn nhau
- Alice, Bob trao đổi khóa bí mật K

45

Thỏa thuận khóa có xác thực

❑**Thực hiện**

1. Alice → Bob: a^x
2. Bob → Alice: a^y, CertB, $E_K(sig_B(a^x, a^y))$
3. Alice → Bob: CertA, $E_K(sig_A(a^x, a^y))$

($K = a^{xy} = a^{yx}$)

46