

# CS355: Cryptography

## Lecture 33: Entity Authentication (Identification).

# Authentication

---

- **Entity authentication (identification)**: the process whereby one party is assured of the identity of a second party involved in a protocol and that the second has actually participated.
- **Data source authentication**: represents an indication about the source of the data.



# Requirements of Identification Protocols

---

- Requirements of identification protocols
  - for honest prover A and verifier B, A is able to convince B
  - no other party can convince B
  - in particular, B cannot convince C that it is A
- Kinds of attackers
  - passive and replay
  - active, man in the middle
  - the verifier

# Properties of Identification Protocols

---

- Reciprocity of identification (one -way or mutual)
- Computational efficiency (encryption, signing)
- Communication efficiency (communication rounds, messages)
- Involvement of a third party
- Nature of trust in the third party
- Storage of secrets

# Authentication Using Fixed Passwords

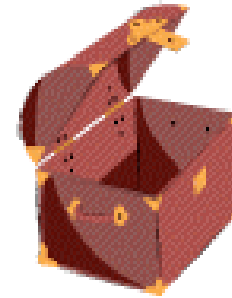
---

- Client authenticates to a server using a password.
- Passwords must be kept in encrypted password files or as digests
- Strengthen passwords by “salting”
- Passphrases, more complex passwords
- Attacks:
  - Replay of fixed passwords
  - Exhaustive password search
  - Password-guessing and dictionary attacks

# Unix crypt Algorithm

---

- Used to store Unix passwords
- Information stored in `/etc/passwd` is:
  - Iterated DES encryption of 0 (64 bits), using the first 8 characters of the password as key
  - 12 bit random salt taken from the system clock time at the password creation
- Why use the salt: to alter the expansion function  $E$  of DES, to defend against attacks on DES using off-the-shelf hardware that can crack DES



# Lamport's One-Time Password

---

Stronger authentication than password-based

- One-time setup:
  - A selects a value  $w$ , a hash function  $H()$ , and an integer  $t$ , computes  $w_0 = H^t(w)$  and sends  $w_0$  to B
  - B stores  $w_0$
- Protocol: to identify to B for the  $i^{\text{th}}$  time,  $1 \leq i \leq t$ 
  - A sends to B:  $A, i, w_i = H^{t-i}(w)$
  - B checks  $i = i_A, H(w_i) = w_{i-1}$
  - if both holds,  $i_A = i_A + 1$

# Challenge-Response Protocols

---

- Goal: one entity authenticates to other entity proving the knowledge of a secret, 'challenge'
- Time-variant parameters used to prevent replay, interleaving attacks, provide uniqueness and timeliness : nonce (used only once)
- Three types:
  - Random numbers
  - Sequences
  - Timestamp

# Challenge-Response Protocols

---

- **Random numbers:**
  - pseudo-random numbers that are unpredictable to an adversary;
  - vulnerable to birthday attacks, use larger sample;
  - must maintain state;
  - do not prevent interleaving attacks (parallel sessions)
- **Sequences:**
  - serial number or counters;
  - long-term state information must be maintained by both parties+ synchronization
- **Timestamp:**
  - provides timeliness and detects forced delays;
  - requires synchronized clocks

# Challenge-Response Protocols Using Digital Signatures

---

- unilateral authentication with timestamp  
A → B: cert<sub>A</sub>, t<sub>A</sub>, B, S<sub>A</sub>(t<sub>A</sub>, B)
- unilateral authentication with random numbers  
A ← B: r<sub>B</sub>  
A → B: cert<sub>A</sub>, r<sub>A</sub>, B, S<sub>A</sub>(r<sub>A</sub>, r<sub>B</sub>, B)
- mutual authentication with random numbers  
A ← B: r<sub>B</sub>  
A → B: cert<sub>A</sub>, r<sub>A</sub>, B, S<sub>A</sub>(r<sub>A</sub>, r<sub>B</sub>, B)  
A ← B: cert<sub>B</sub>, A, S<sub>B</sub>(r<sub>B</sub>, r<sub>A</sub>, A)

# Attacks: Examples

---

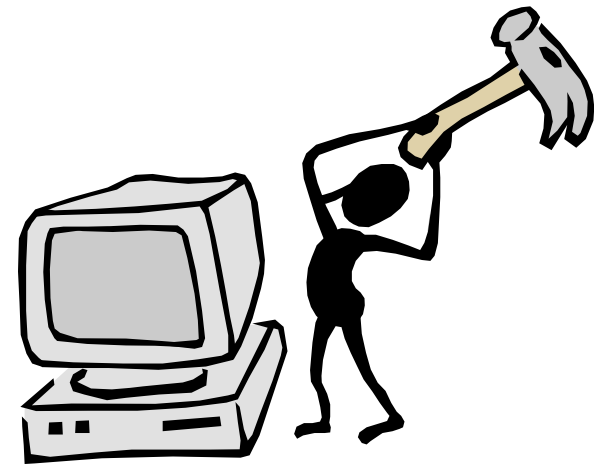
- E1: “Man-in-the-middle” attack on unauthenticated DH
- E2: Reflection attack

Protocol: A and B authenticate to each other

- (1)  $A \rightarrow B : r_A$
- (2)  $B \rightarrow A : E_k(r_A, r_B)$
- (3)  $A \rightarrow B : r_B$

Attack: E wants to trick A to accept him as B

- (1)  $A \rightarrow E : r_A$
- (2)  $E \rightarrow A : r_A$  : Starting a new session
- (3)  $A \rightarrow E : E_k(r_A, r_A')$  : Reply of (2)
- (4)  $E \rightarrow A : E_k(r_A, r_A')$  : Reply of (1)
- (5)  $A \rightarrow E : r_A'$ ; this concludes session started with (1)



**AUTHENTICATION RELIES ON THE SECRECY OF KEY K**

# Attacks: Examples (cont.)

---

- E3: Interleaving attacks

## Protocol

- (1)  $A \rightarrow B : r_A$
- (2)  $B \rightarrow A : r_B, S_B(r_B, r_A, A)$
- (3)  $A \rightarrow B : r_A', S_A(r_A', r_B, B)$

Attack: E wants to pass as A to B

- (1)  $E \rightarrow B : r_A$
- (2)  $B \rightarrow E : r_B, S_B(r_B, r_A, A)$
- (3)  $E \rightarrow A : r_B$
- (4)  $A \rightarrow E : r_A', S_A(r_A', r_B, B)$
- (5)  $E \rightarrow B : r_A', S_A(r_A', r_B, B)$

