Replay Attacks

One Time Passwords

Lamport's One-time Password Scheme

Using Time in One-time Passwords
Problem with Improved Scheme 3

- Scheme 3 is susceptible to replay attacks
  - Attacker eavesdrops on the communication channel and intercepts a legitimate authentication exchange
  - Attacker later replays the authentication exchange
Replay on a Different Verifier

Replay Attacks

One Time Passwords

Lamport’s One-time Password Scheme

Using Time in One-time Passwords

To counter, ensure that an identifier of the intended verifier is included in the (protected) authentication message
Reflection Attack

**Replay Attacks**

**One Time Passwords**

**Lamport’s One-time Password Scheme**

**Using Time in One-time Passwords**

---

**Authentication schemes based on symmetric key cryptography can be vulnerable to these types of attacks**

I am Charlie and here is the shared secret as password

I am Bob and here is the shared secret as password
Man-in-the-Middle Attack

To protect against such attack combine the authentication process with a key establishment process.
Replay on the Same Verifier

Replay Attacks

One Time Passwords

Lamport’s One-time Password Scheme

Using Time in One-time Passwords

Dr. Indrajit Ray, Computer Science Department
**Improved Scheme 4**

**Replay Attacks**

**One Time Passwords**

**Lamport’s One-time Password Scheme**

**Using Time in One-time Passwords**

---

**Claimant Terminal**

- \( p' \)
- \( f \)
- \( q' \)
- \( g \)
- \( id \)
- \( nrv \)

**Message**

**Verifier**

- \( id \)
- \( q \)
- \( g \)
- \( r \)
- \( compare \)

**Authentication**

OK or not

Dr. Indrajit Ray, Computer Science Department

CS 556 - Computer Security - © 2012 Colorado State University – 8 / 28
### Replay Attacks

**One Time Passwords**

**Lamport’s One-time Password Scheme**

**Using Time in One-time Passwords**

---

**One Time Passwords**
One Time Passwords

- Use a password exactly once
- Such schemes are safe from passive adversaries who eavesdrop and later attempt impersonation.
- Variations include
  - Shared lists of one time passwords
  - Sequentially updated one time passwords
  - One time password sequences based on one-way functions
Shared Lists of One Time Passwords

- User and system use a sequence of \( n \) secret passwords – each valid for a single authentication
- Drawback – maintenance of shared list
  - Have to use passwords in exact sequence – otherwise system has to check password against all remaining unused passwords
  - Not widely used
Sequentially Updated One Time Passwords

- Initially only a single secret is shared
- During authentication, user creates and transmits a new password using the current password
  - New password typically encrypted under a key derived from current password
- New password transmitted in current session, forms the password for the next session
- Method becomes difficult if communication failure occurs
One Time Password Sequences

- User does not send new password everytime; instead user and system computes next passwords locally
- Use one-way functions to compute passwords
- Improvement on Sequentially Updated One Time Passwords Scheme
  ✦ More efficient with respect to bandwidth
Lamport’s One-time Password Scheme

Replay Attacks
One Time Passwords
Lamport’s One-time Password Scheme
Using Time in One-time Passwords
Lamport’s One-Time Password Scheme

- Uses one-way hash function
- Relies on the fact that it is easier to compute the hash of a particular value than to compute the original value from the hashed value
  - That is, $H(x)$ is easy to compute given $x$
  - $H^{-1}(x)$ is difficult to compute given $H(x)$
Lamport’s Scheme (continued)

- Notation $H^t(x) = H(H^{t-1}(x))$
- User A begins with a secret $w$ and a one-way function $H$
- A constant $t$ is fixed – for example $t = 100$ or $1000$
  - $t$ defines the number of identifications allowed
  - The system has to be restarted thereafter with a new $w$
- A transfers (the initial shared secret) $w_0 = H^t(w)$ to the system; system initializes its counter for $A$ to $i_A = 1$
Lamport’s Scheme (continued)

- System stores (User name \(A\), \(H^t(w)\))
- The \(i^{th}\) identification message, \(1 \leq i \leq t\), is as follows:

\[
A \rightarrow \text{system}: \ A, \ i, \ w_i \ (= H^{t-i}(w))
\]

\[H^{t-i}(w) = H(H^{t-i-1}(w))\]

- \(A\) computes \(H^{t-1}(w)\) the first time
- If authentication is correct, system replaces \(H^t(w)\) by \(H^{t-1}(w)\) and sets \(i_A \leftarrow i_A + 1\)
Lamport’s Scheme (continued)

Replay Attacks

One Time Passwords

Lamport’s One-time Password Scheme

Using Time in One-time Passwords

\[ W = E0UDE**O2jR>fx, \quad t = 6 \]
Lamport’s Scheme (continued)

- A typically calculates $H^t(w)$ using a hand-held calculator, a trusted workstation or a portable computer
  - In Bellcore’s implementation of this scheme – S/Key – user calculates the sequence on a secure machine and encodes it as a sequence of short words
- Scheme is vulnerable to pre-play attacks where an attacker intercepts and traps an as-yet unused password
USING TIME IN ONE-TIME PASSWORDS
Time Synchronized Schemes

Replay Attacks

One Time Passwords

Lamport’s One-time Password Scheme

Using Time in One-time Passwords

Hand Held Authenticator

Secret Key

\[ f(S, t) \]

One Time Password
Time Synchronized Scheme

- A hand-held authenticator is used
  - It contains an internal clock, a secret key and a display
  - Display outputs a function (DES / one-way function) of the current time and the key
  - Current time is in minutes, rather than seconds, so the value changes about once per minute
Time Synchronized Scheme (continued)

- User supplies the user-id and the display value
- System uses the secret key, the one-way function and its clock to calculate the expected output – login is valid if values match
- Clocks need to be synchronized
A non-repeating challenge from the system is used instead of the clock.
Non Repeating Values

- Ensures that an attempt to replay an earlier authentication exchange will be detected
- Potential sources:
  - Sequence numbers – claimant and verifier agree upon policy to generate sequence numbers
  - Time stamps – clocks need to be synchronized to at least within a window
Non Repeating Values (continued)

- Time stamps
  - To guarantee uniqueness, verifier needs to buffer copies of all messages received within window
- Random value (or nonce) sent previously from the verifier
Password – Improved Scheme 5

**Replay Attacks**

**One Time Passwords**

**Lamport’s One-time Password Scheme**

**Using Time in One-time Passwords**

---

**Claimant Terminal**

- `p'`
- `q'`
- `f`
- `g`
- `id`

**Verifier**

- `id`
- `q`
- `nrv`
- `g`
- `r`
- `r'`
- `id`

**Response Message**

Authentication OK or not
**Hand Held Password Generator**

### Replay Attacks

#### One Time Passwords

#### Lamport’s One-time Password Scheme

#### Using Time in One-time Passwords

**User PIN from Token entered**

**Password Generator**

- **Secret Key**
  - $f(PIN, S, e)$

**System**

- **A (user)**
  - $f(PIN, S, e)$
  - $e$
  - (challenge)
  - $f(PIN, S, e)$
  - $e$
  - (response)

- **A**
  - PIN
  - S

**Login Request**

- **Password Generator**
  - $f(PIN, S, e)$
  - $e$
  - (challenge)
  - $f(PIN, S, e)$
  - $e$
  - (response)

**Accept**

- yes

**Reject**

- no