CS 556 – Computer Security
Spring 2018

Dr. Indrajit Ray
Email: indrajit@cs.colostate.edu

Department of Computer Science
Colorado State University
Fort Collins, CO 80523, USA

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

Replay Attacks

Problem with Improved Scheme 3

REPLAY ATTACKS
ONE TIME PASSWORDS
LAMPORT'S ONE-TIME PASSWORD SCHEME
USING TIME IN ONE-TIME PASSWORDS

- 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

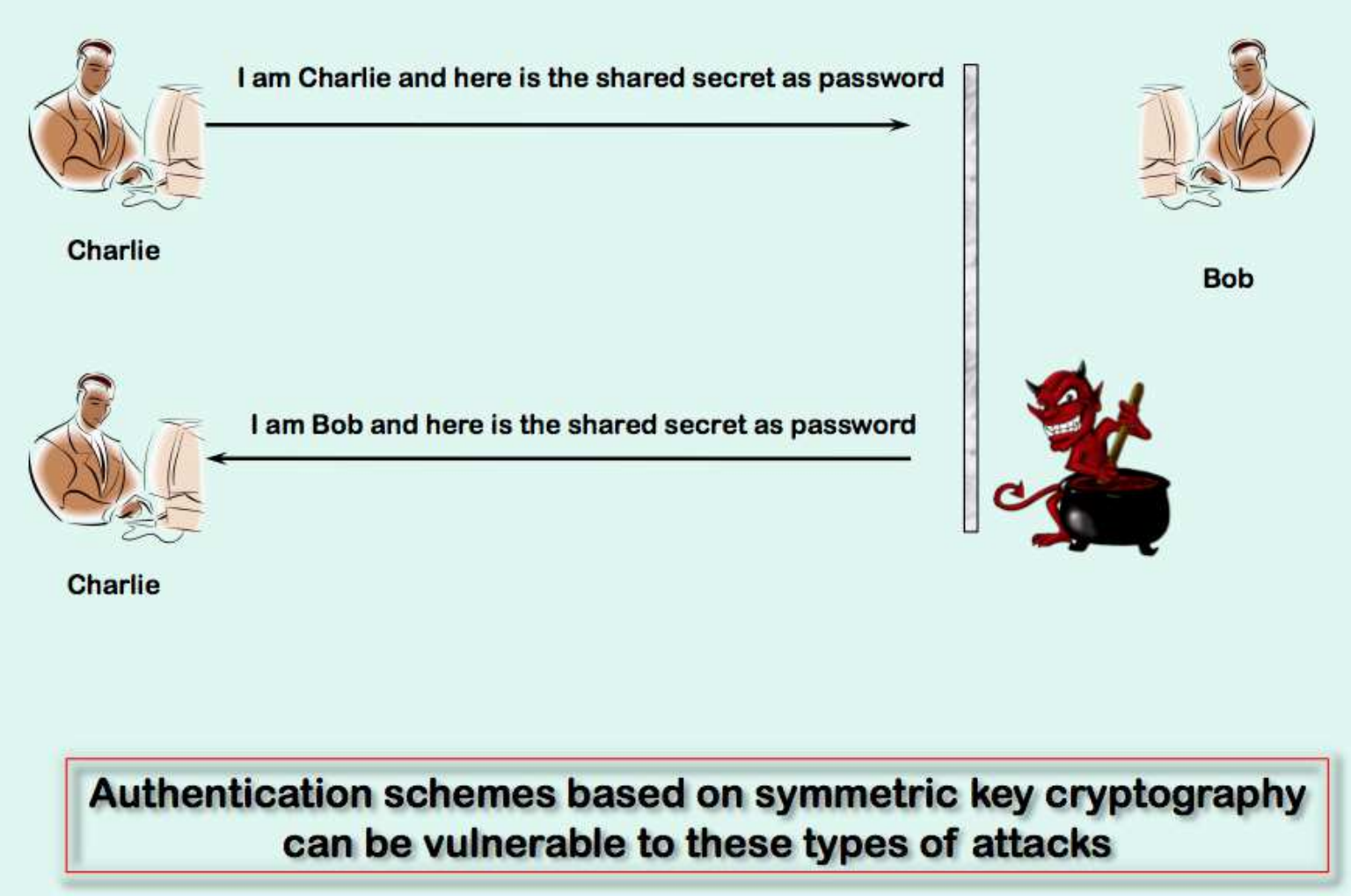
Reflection Attack

Replay Attacks

One Time Passwords

Lamport's One-time Password Scheme

Using Time in One-time Passwords



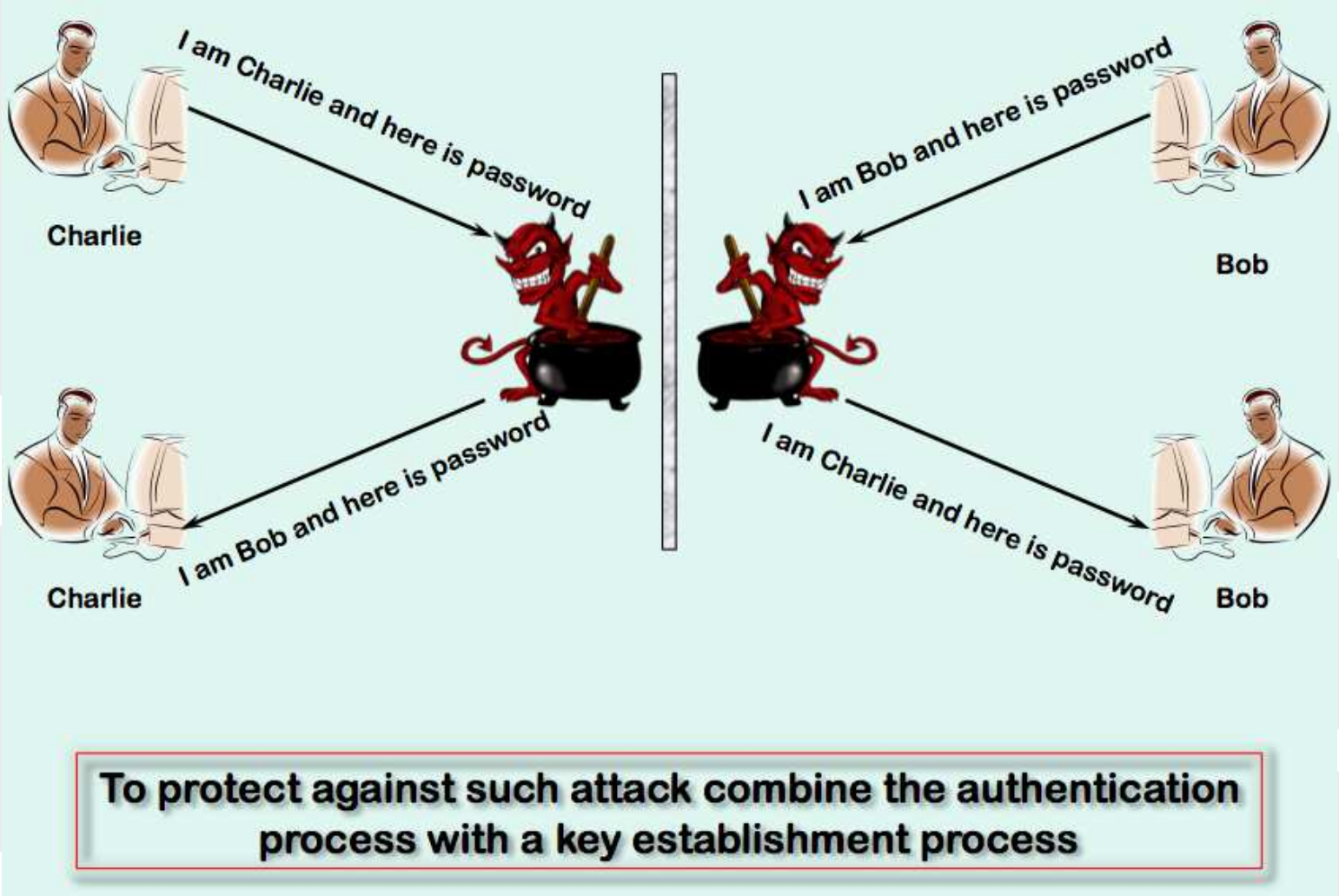
Man-in-the-Middle Attack

Replay Attacks

One Time Passwords

Lamport's One-time Password Scheme

Using Time in One-time Passwords



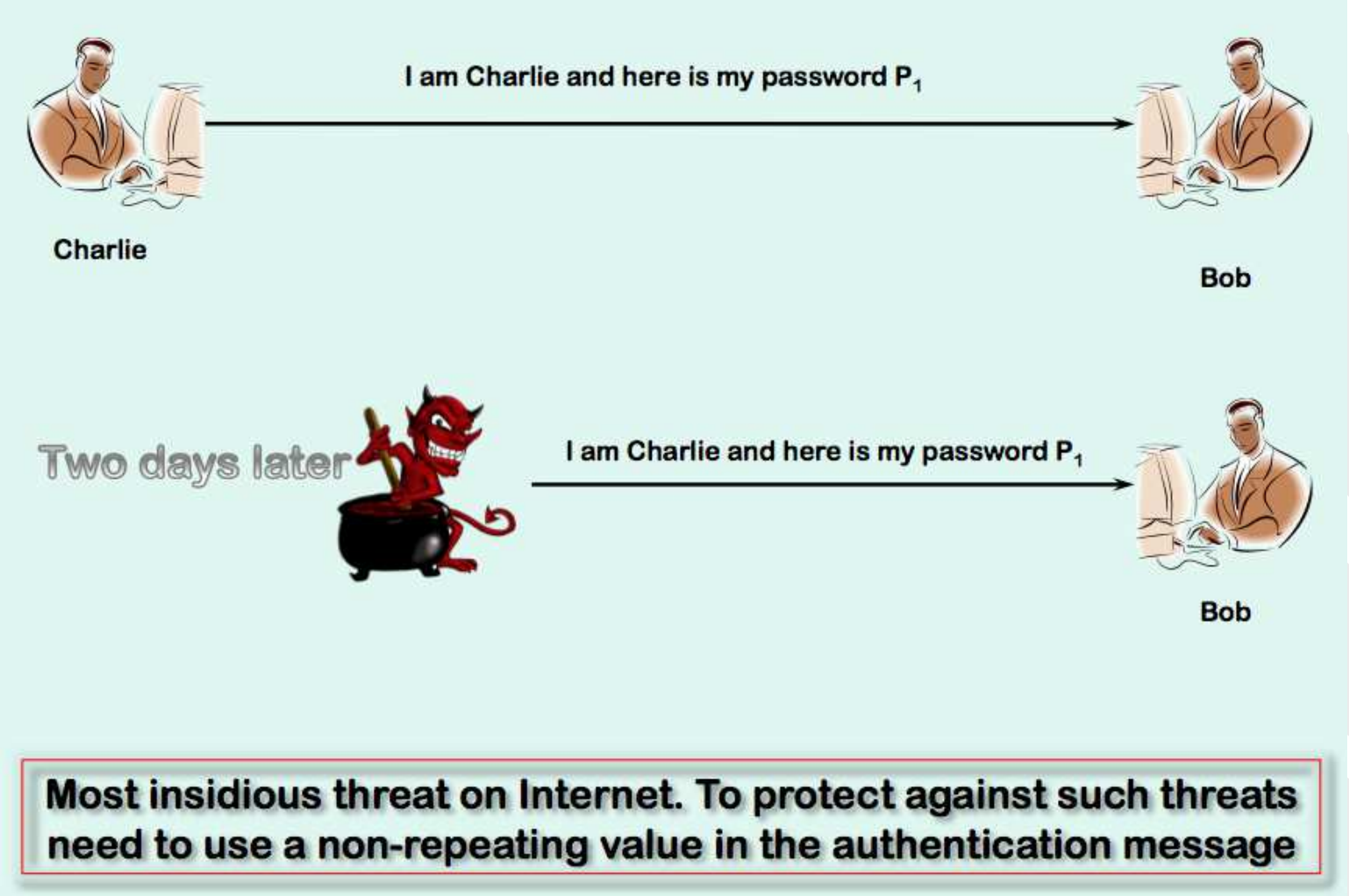
Replay on the Same Verifier

REPLAY ATTACKS

ONE TIME PASSWORDS

LAMPORT'S ONE-TIME PASSWORD SCHEME

USING TIME IN ONE-TIME PASSWORDS



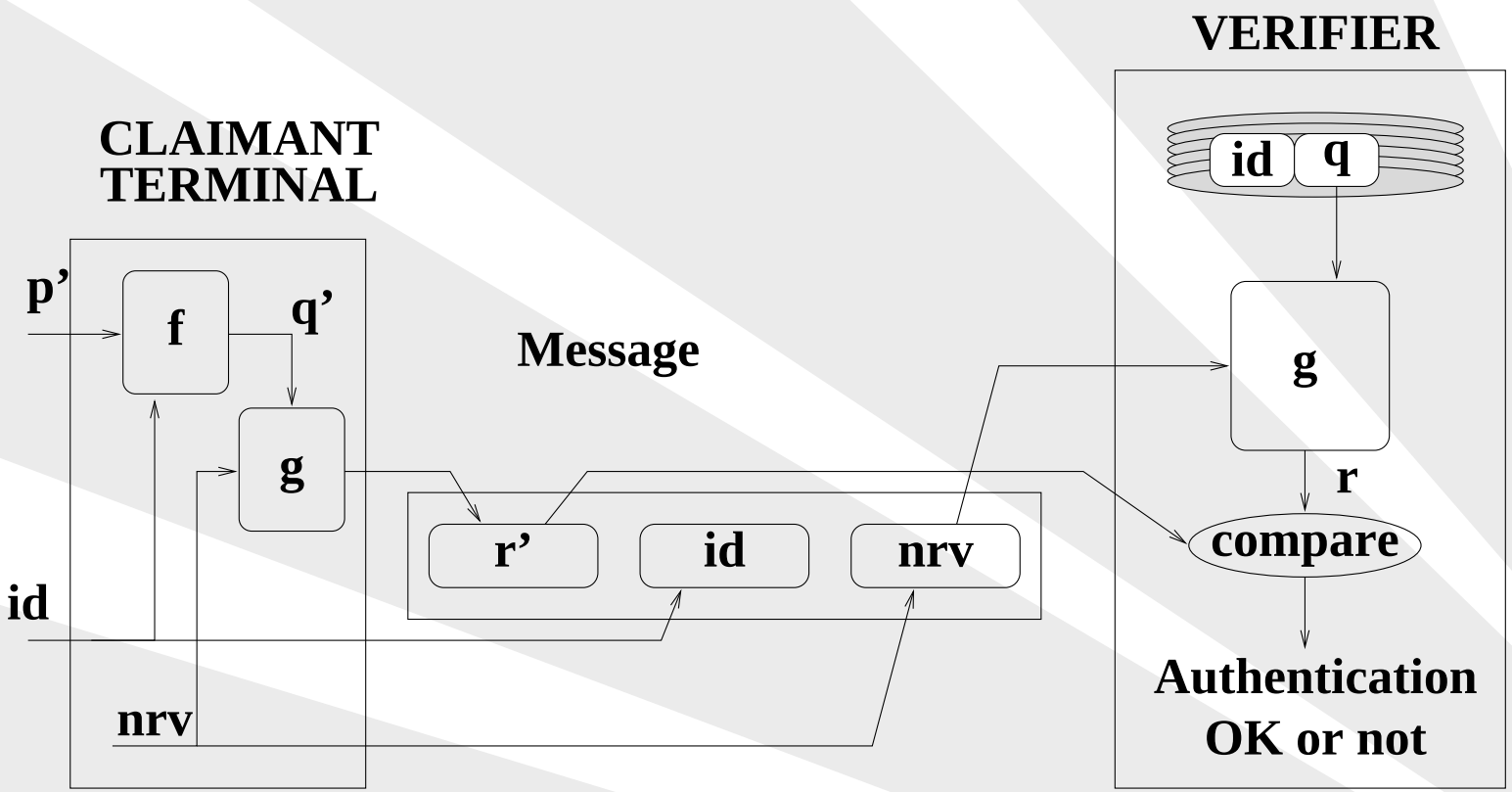
Improved Scheme 4

REPLAY ATTACKS

ONE TIME PASSWORDS

LAMPORT'S ONE-TIME PASSWORD SCHEME

USING TIME IN ONE-TIME PASSWORDS



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

One Time Passwords

One Time Passwords

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

Replay Attacks
One Time Passwords
Lamport's One-time Password Scheme
Using Time in 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 passswords
  - Not widely used

Sequentially Updated One Time Passwords

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

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

- 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

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

Lamport's One-time Password Scheme

Lamport's One-Time Password Scheme

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

- 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, $\mathrm{H}(x)$ is easy to compute given x
  - $\mathrm{H}^{-1}(x)$ is difficult to compute given $\mathrm{H}(x)$

Lamport's Scheme (continued)

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

- Notation $\mathrm{H}^t(x) = \mathrm{H}(\mathrm{H}^{t-1}(x))$
- 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)

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

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

$$A \rightarrow system: \; A, \; i, \; w_i \; (= H^{t-i}(w))$$

  - $H^{t-i}(w) = H(H^{t-i-1}(w))$

- 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 $i_A \leftarrow i_A + 1$

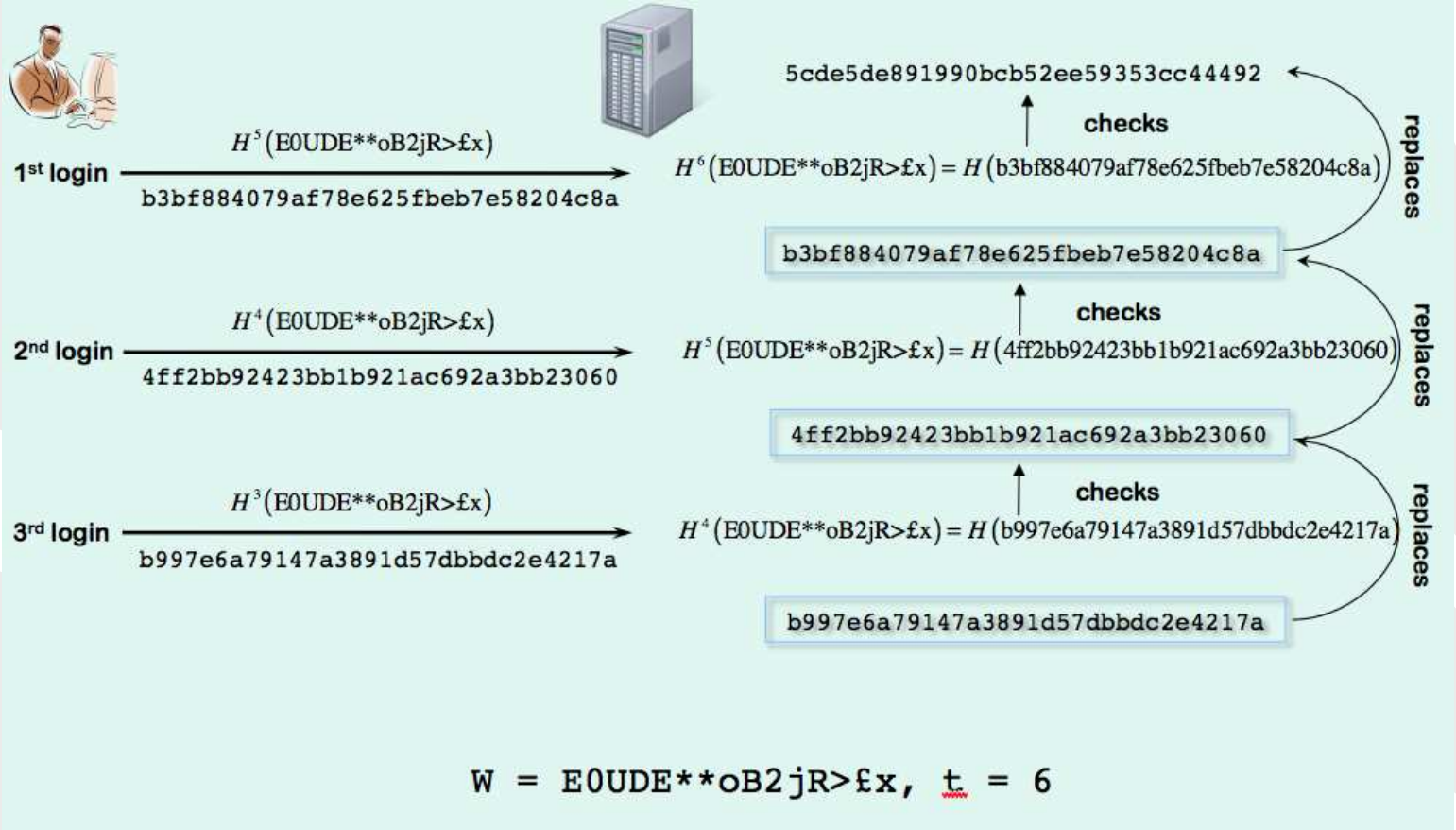
Lamport's Scheme (continued)

Replay Attacks

One Time Passwords

Lamport's One-time Password Scheme

Using Time in One-time Passwords



Lamport's Scheme (continued)

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

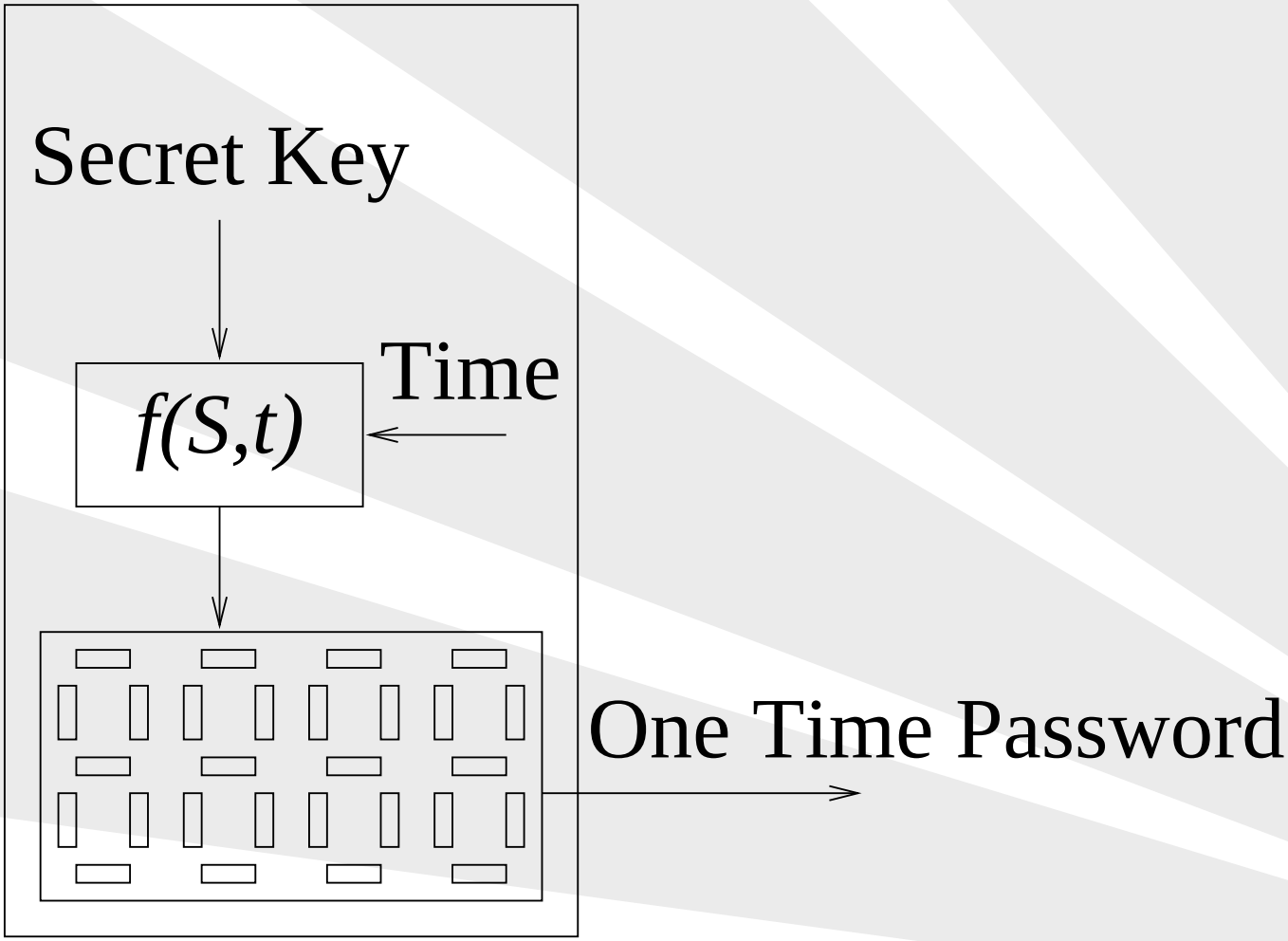
- *A* typically calculates $H^t(w)$ using a hand-held calculator, a trusted workstation or a portable computer
  - In Bellcore's implementation of this scheme – S/Key – user calculates the sequence on a secure machine and encodes it as a sequence of short words
- Scheme is vulnerable to *pre-play* attacks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

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

Using Time in One-time Passwords

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

Hand Held Authenticator



Time Synchronized Scheme

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

- 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)

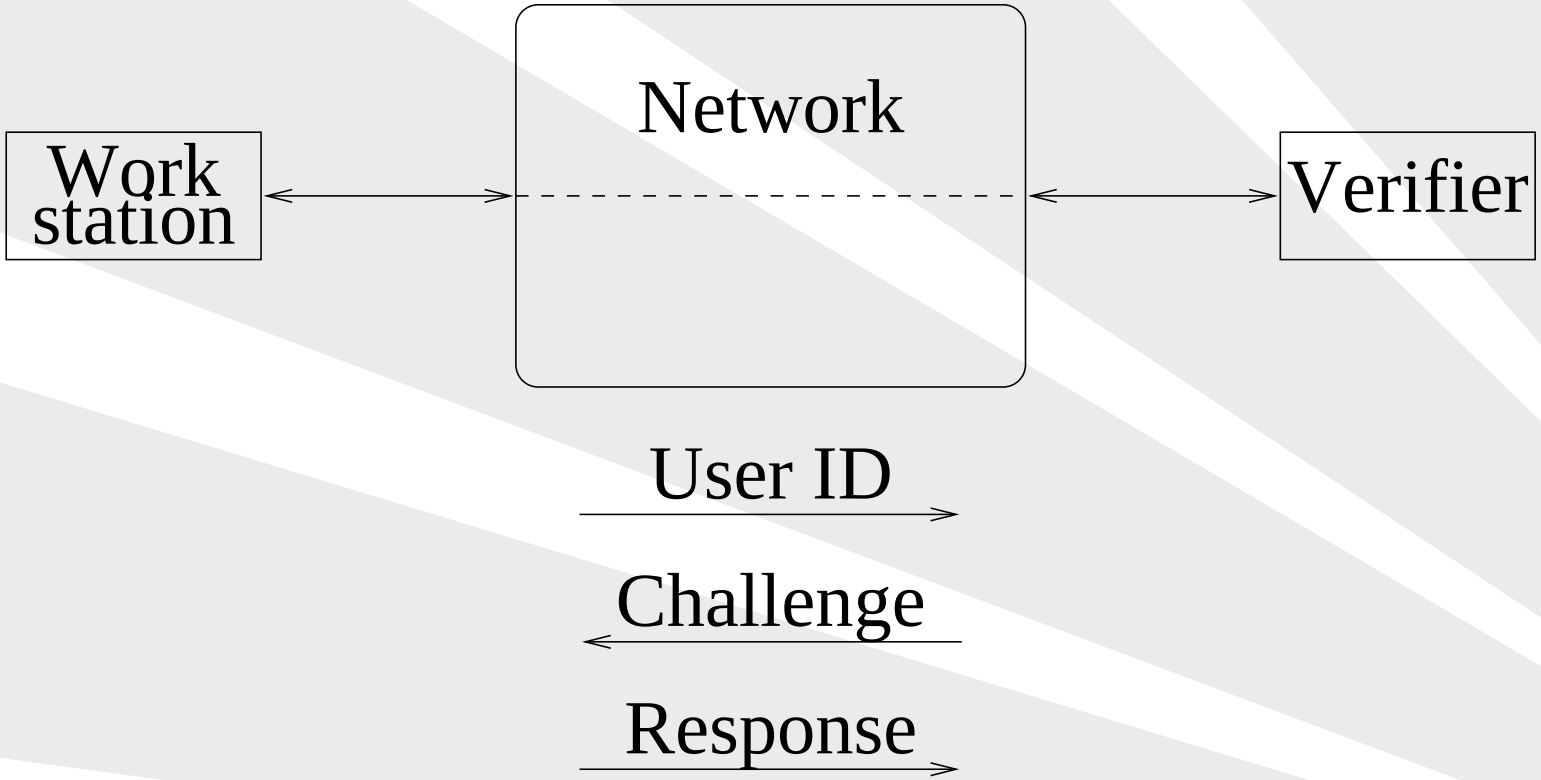
Replay Attacks
One Time Passwords
Lamport's One-time Password Scheme
Using Time in One-time Passwords

- 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

Challenge Response Schemes

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

- A non-repeating challenge from the system is used instead of the clock



Non Repeating Values

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

- 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

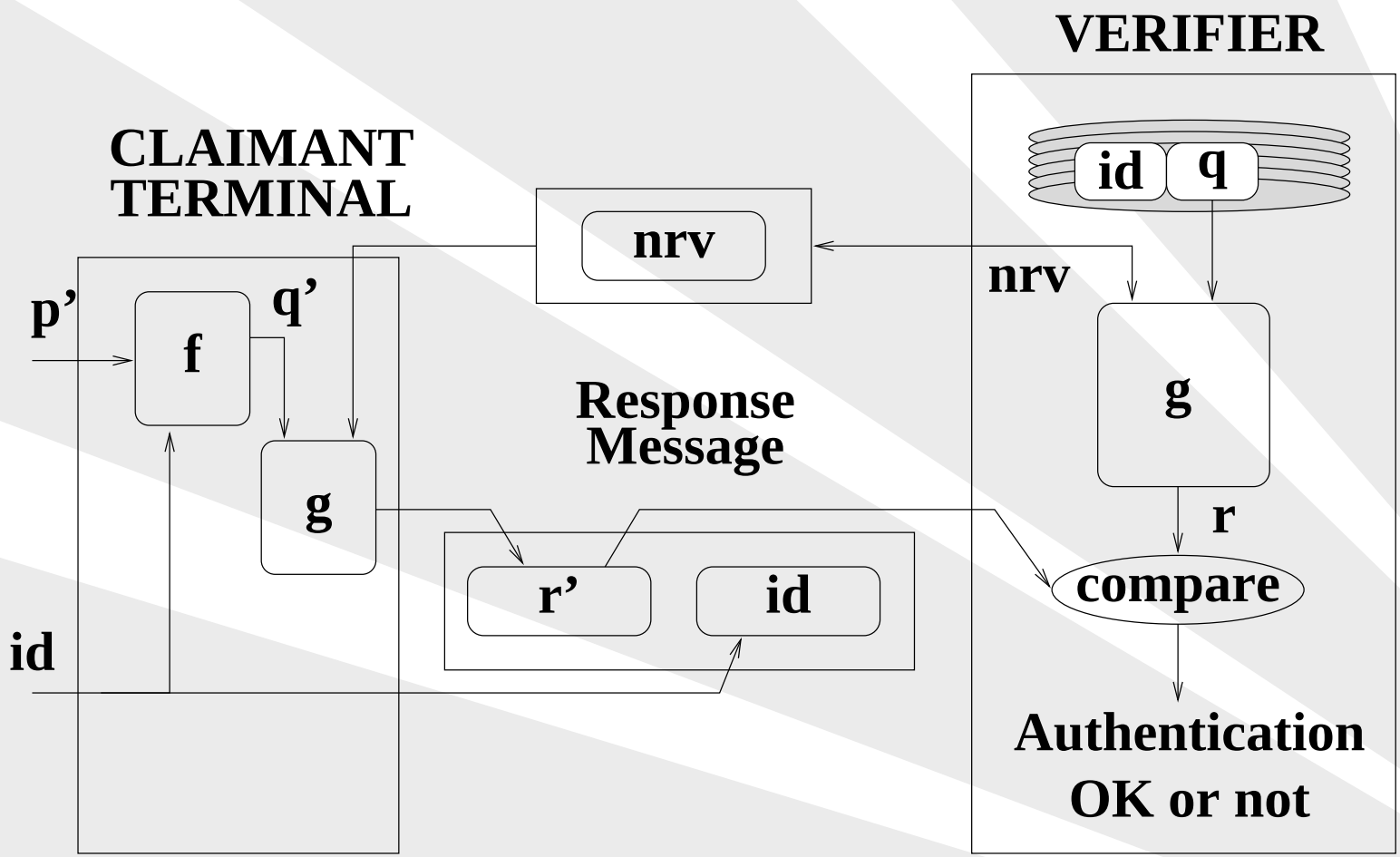
Non Repeating Values (continued)

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

- 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



Hand Held Password Generator

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