**Authentication protocol**

**Authentication** - process of determining if an entity is who they claim to be. Provide evidence.

**Protocols** - define the series of messages exchanged between two or more entities and their meaning.

**Authenticated key exchange**
- Confidentiality
- Timeliness
- Fresh
- Goal - send session key in encrypted form.

**Threat**
- Replay attack

**Solution**
1. Send sequence number

   ![](image)

   - Suggested for RF10
   - Does not scale

2. Timestamps
   - Host A accepts message only if its timestamp is "close" to its time
   - Synchronized clocks

3. Challenge / Response

   ![](image)

   nonce = N

   nonce = N
THREAT

Authentication

Replay Attack

REQUEST

READER

INTERROGATE

ID

TAG

OPEN/CLOSES

DOOR

Cavesdropper records tag response

- Opens door if correct ID is provided.

- If an attacker eavesdrops and records tag response, he can replay it to get access to the door.

WHAT MITIGATION TECHNIQUE(S) CAN HELP PREVENT THE REPLAY ATTACK AGAINST THE READER?

IN ORDER WORDS, WHAT CAN PREVENT REPLAYING THE TAG'S RESPONSE?

Solutions

(STALLINGS, 2006, pp.382)

1. Timestamp

R \xrightarrow{Reg} T

\xrightarrow{ID\|t}

Do you think we can have an accurate clock on a tag?

- No, synchronizing time is tough.

2.1 Challenge-Response

R \xrightarrow{Reg\|N} T

\xrightarrow{ID\|N}

N = nonce on challenge, reader changes nonce each time.

Can we do better?

2.2 Challenge-Response

R \xrightarrow{Reg\|N} T

\xrightarrow{ID\|f(N)}

f(k,N) many variations
2.3 Challenge-Response: Symmetric Key, $K$ = shared key

\[ R \xrightarrow{Reg} \| E(k, N) \rightarrow T \]
\[ \xrightarrow{T0\|E(k, f(N))} \]

*Note: $k$ = shared key is shared before this authentication occurs.*

- Who authenticates who?
- Who provides evidence?

$T$
- Reader authenticates tag
- Tag does *not* authenticate reader
- Tag is authenticated

How could tag authenticate the reader?

2.4 Challenge-Response: Symmetric Key, Mutual authentication

\[ R \xrightarrow{Reg} \| E(k, N) \rightarrow T \]
\[ \xrightarrow{T0\|E(k, f(N))} \]

2.5 Challenge-Response: Asymmetric Key

\[ R \xrightarrow{Reg} \rightarrow T \]
\[ \xrightarrow{K_{pu-T}} \| E_{D_T} \]
\[ \xrightarrow{E(K_{pu-T}, K_s)} \]

*Assume R+T know each other's public key.*

Assuming $K_{pu-T}$ received correctly, tag (T) provided some evidence because it cannot correctly decrypt $K_s$.

- The reader (R) provided no evidence
- The tag does not have evidence from the reader