Security Issues in a CDPD Wireless Network

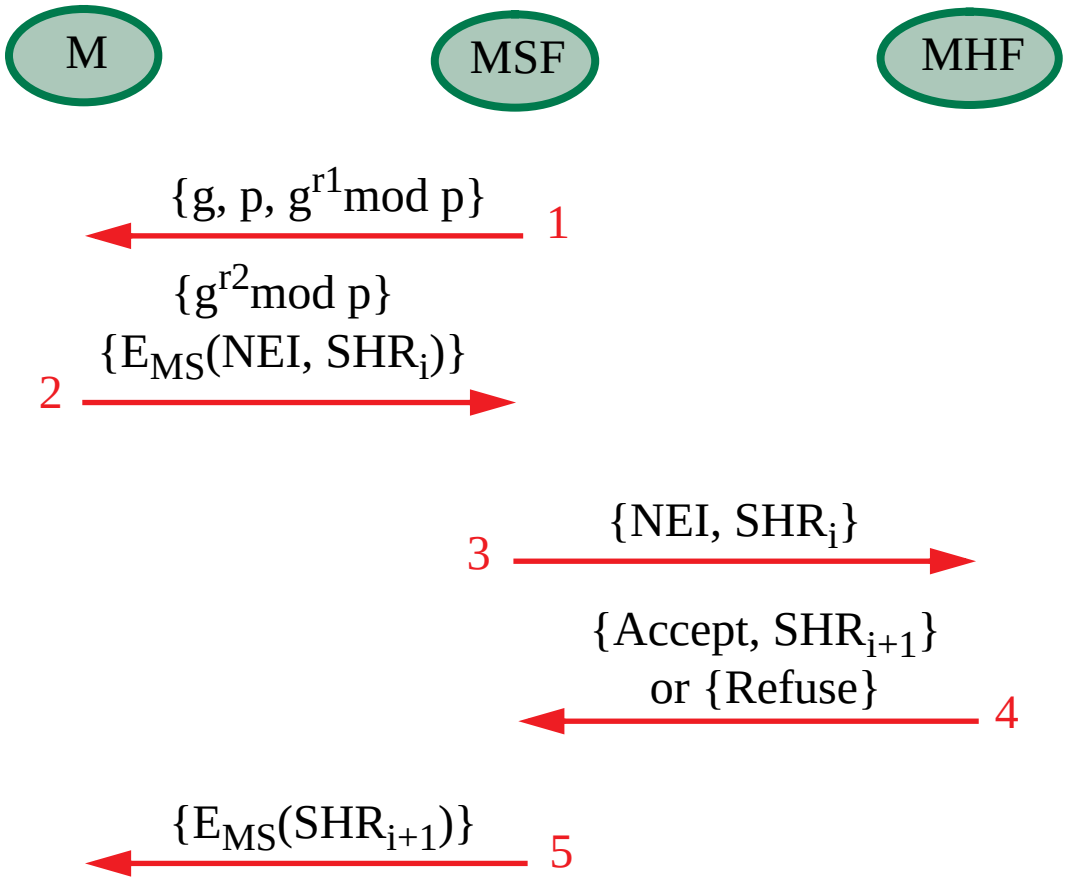
by

Yair Frankel, et. al.

Summarized by Johnathan M. Reason
CS294-7 Lecture
Department of Electrical Engineering and Computer Science
University of California at Berkeley
April 12, 1996

Current CDPD Authentication Protocol

Step	Action
1	Generate r2 Compute K_{MS}
2	M sends its cred. S decrypts M's cred.
3	S relays M's cred. H verifies M's cred.
4	H sends response and updates SHR
5	S encrypts new SHR and sends it to M



Pros and Cons of Current Protocol

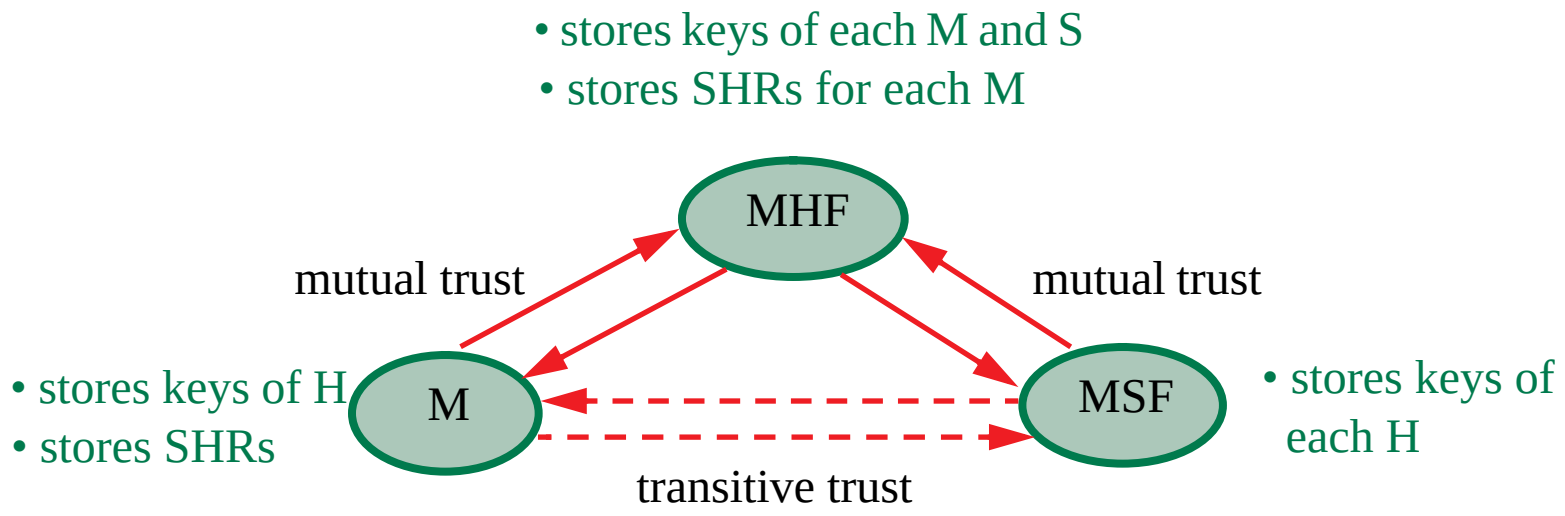
Pros

- Simple to implement and maintain.

Cons

- Mutual trust is not established (only assumed) between M, S, and H.
- Vulnerable to man-in-the-middle attacks.
  - A bogus S can spoof air link to obtain M's credentials.
- Vulnerable to intrusion attempts by a fraudulent M.
  - A bogus M with valid credentials can gain access to the network.
- Messages sent over the backbone network are not authenticated.
  - Any adversary can obtain M's credentials by listening on the backbone.
- Diffe-Hellman key-exchange is computationally intensive.
  - Public-key algorithms are approximately three orders of magnitude slower than secret-key algorithms.

Authenticated Trust Model for Proposed Protocol



Trust established directly through authenticated messages.

Trust established indirectly through authenticated messages.

Proposed Authentication Protocol

Step	Action
1	M sends its cred.
2	S relays M's cred. S sends challenge to H H authenticates M & S
3	H sends resp. to S H sends new chal. to M S authenticates H & M
4	S relays response M authenticates H & S

$$T_{MH} = \begin{cases} R_{MH} \\ T'_{MH} = A_{MH}(S_{HM}, R_{MH}, NEI_S, \text{“response”}) \end{cases}$$

1 →

$$T_{SH} = \begin{cases} T_{MH} \\ R_{SH} \\ T'_{SH} = A_{SH}(T'_{MH}, R_{SH}, NEI_M, \text{“relay”}) \end{cases}$$

2 →

$$T_{HS} = \begin{cases} T_{HM} \\ \text{“accept” or “deny” (“a” or “d”)} \\ T'_{HS} = A_{HS}(T'_{HM}, R_{SH}, NEI_M, \text{“a” or “d”}) \end{cases}$$

← 3

$$T_{HM} = \begin{cases} S'_{HM} \\ \text{“refresh”} \\ T'_{HM} = A_{HM}(R_{MH}, S'_{HM}, NEI_S, \text{“refresh”}) \end{cases}$$

← 4

Pros and Cons of Proposed Protocol

Pros

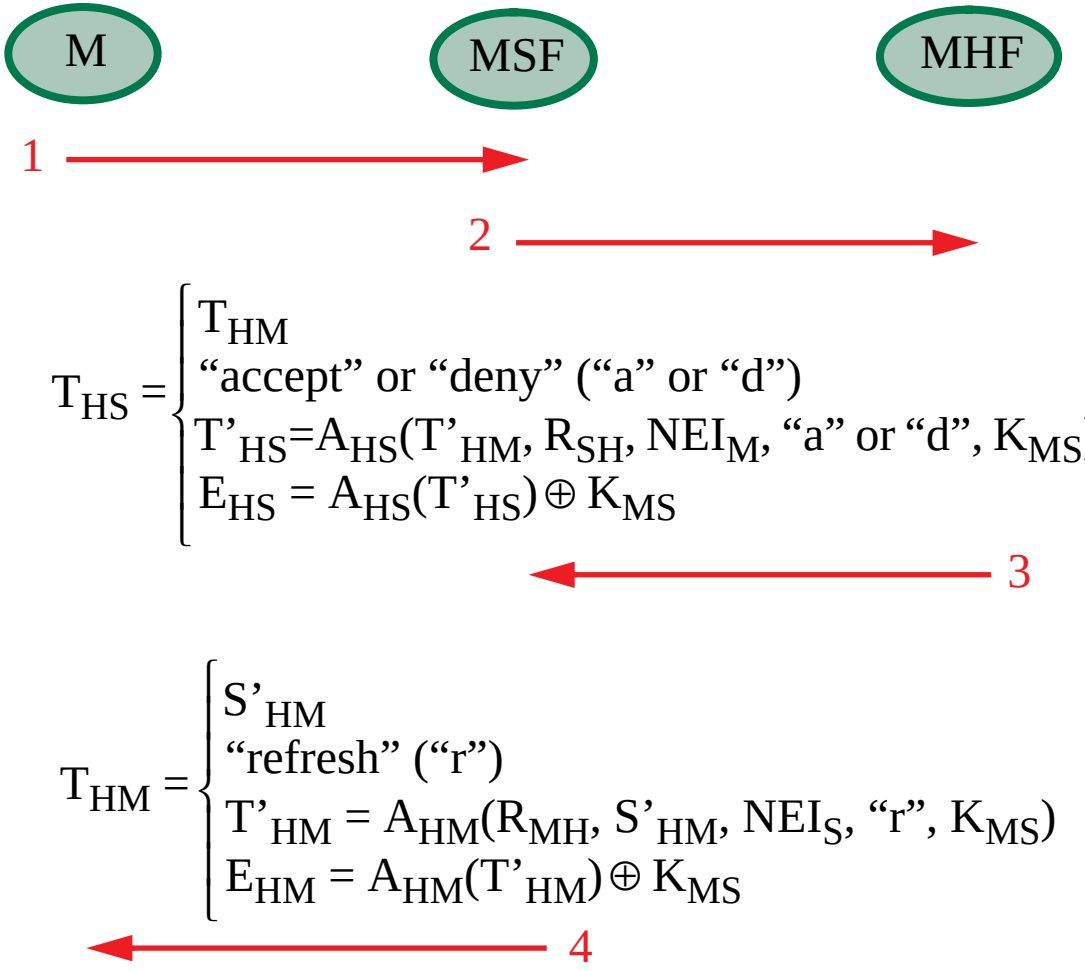
- Mutual trust is established between M, S, and H.
- Supports anonymity and privacy of data.
- Requires fewer transmissions than current protocol.

Cons

- Key management
  - H must maintain secret keys for each M and S.
  - Likewise, each S must maintain keys for each H.
  - Probably will not scale well in public network (Internet) scenario.
  - How will the keys be updated if compromised, especially for mobiles?
  - How are keys maintained across carriers?
- K_{MH} is vulnerable to known-plain-text attacks.
  - T_{MH} and T_{HM} are know to an adversary listening on the air link.
- Intrusion attempts by a bogus M can not be detected definitively.
- Possible intrusion attempts by M are not detected until step 2 of protocol.
  - Backbone network bandwidth is wasted.

Key Exchange in Proposed Protocol

Step	Action
1	Same as before
2	Same as before
3	H sends resp. to S H sends new chal. to M H sends key to M & S S authenticates H & M
4	S relays new chal. S relays key M authenticates H & S



$$T_{HS} = \begin{cases} T_{HM} \\ \text{“accept” or “deny” (“a” or “d”)} \\ T'_{HS} = A_{HS}(T'_{HM}, R_{SH}, NEI_M, \text{“a” or “d”}, K_{MS}) \\ E_{HS} = A_{HS}(T'_{HS}) \oplus K_{MS} \end{cases}$$

$$T_{HM} = \begin{cases} S'_{HM} \\ \text{“refresh” (“r”)} \\ T'_{HM} = A_{HM}(R_{MH}, S'_{HM}, NEI_S, \text{“r”}, K_{MS}) \\ E_{HM} = A_{HM}(T'_{HM}) \oplus K_{MS} \end{cases}$$

- $A_{HS}()$ and $A_{HM}()$ are pseudorandom functions based on MD-5.

Anonymity in Proposed Protocol

Context

Define:

- $P_M \equiv \{A_H(f(S_{HM})) \oplus NEI_M, S_{HM}\}$ and $P'_M \equiv \{A_H(f(S'_{HM})) \oplus NEI_M, S'_{HM}\}$
- $P_H \equiv \{A_G(g(S_{HM})) \oplus NEI_H, S_{HM}\}$ and $P'_H \equiv \{A_G(g(S'_{HM})) \oplus NEI_H, S'_{HM}\}$

where

A_H is authentication function using key K_H (key known only by H).
A_G is authentication function using key K_G (global key).
g and f are globally known functions.
P_M and P_H are pseudonyms for the identity of M and H, respectively.

Modifications to the New Protocol

Transmission 1: Replace NEI_M and NEI_H in T_{MH} with P_M and P_H.

Transmission 3: Add P'_M and P'_H to E_{HM} using appropriate one-time pad.
Add P'_M and P'_H to T'_{HM}.

Note: In transmission one of the proposed protocol, transmission of NEI_M and NEI_H is implied, not explicitly shown.