Analysis of 4-way handshake protocol in IEEE 802.11i

Changhua He
Stanford University
Mar. 04, 2004

History of Security Concerns

- **802.11b (WEP)**
  - Wired Equivalent Protocol
  - Many attacks found
- **WPA: Wi-Fi Protected Access**
  - Proposed by Wi-Fi Alliance
  - Short-term solution based on 802.1x
- **802.11i**
  - Standards approved Oct. 2003
  - Long-term solution, may need hardware upgrades
  - This project focus on part of the authentication protocol in the standard

Terms

- **Authenticator**: Entities implemented in AP
- **Supplicant**: Entities implemented in Laptop
- **Authentication Server**
- **PMK**: Pair-wise Master Key
- **PTK**: Pair-wise Transient Key
- **MIC**: Message Integrity Code
- **ANonce**: nonce generated by authenticator
- **SNonce**: nonce generated by supplicant
- **AA**: Authenticator Address (MAC)
- **SPA**: Supplicant Address (MAC)

802.11i Authentication

Idealized 4-way Handshake
Prior to 4-way handshake, we assume:

- PMK only known to Supplicant and Authenticator, never transmitted over network

Objectives:

- Generate PTK and confirm the procession and freshness of PTK

Methodology:

- Use Mure to model the protocol from simplest version, find out attacks, add fields step by step to defend the attacks, get complete one.
- Can make clear the function of each fields, and find out attacks for the complete protocol.

Objectives:

- Generate PTK and confirm the procession and freshness of PTK

Methodology:

- Use Mure to model the protocol from simplest version, find out attacks, add fields step by step to defend the attacks, get complete one.
- Can make clear the function of each fields, and find out attacks for the complete protocol.

In each run:

- Turn on/off fields: nonce, sequence, mtype, address

Invariant

\begin{align*}
& \text{Invariant "PTKs are consistent and fresh"} \\
& \text{forall } i: \text{AuthenticatorId do} \\
& \text{forall } j: \text{SupplicantId do} \\
& \text{aut}[i].associations[j].session.state = A\_DONE \\
& \to \\
& (\text{sup}[j].associations[i].session.state = S\_DONE & \text{ptkEqual(aut}[i].associations[j].session.ptk, sup[j].associations[i].session.ptk) & aut[i].associations[j].sid = sup[j].associations[i].sid }) | \\
& (\text{sup}[j].associations[i].session.state = S\_PTKSA & aut[i].associations[j].sid = sup[j].associations[i].sid )
\end{align*}

Summary of fields

- Nonces is necessary for fresh PTK
- Mtype
  - Necessary, otherwise can fool supplicant to calculate msg 3, or vice versa
- Sequence
  - Not necessary here
  - Defense msg 3 replay, but it is harmless
- AA, SPA
  - Bind PTK to the physical device, not necessary here, but need to be considered with PMK
Implementation error

DoS attack

The standard adopts TPTK & PTK: not work

Conclusions

Murphi Modelling

802.11i 4-way handshake protocol

Implementation error (corresponding to DoS attack)