Mobile Ad Hoc Networks and Secure Routing

John Marshall
marshall@cs.fsu.edu

19 February 2003

Route Accumulation

Route request issued by Red to Brown

Red Red Yellow Blue Red Yellow Blue Brown
“Leap-frogging” Vulnerabilities

- Weaknesses
  1. Intermediate nodes not forced to append address
  2. Destination cannot authenticate route

Attack on SRP
Attack on SRP

Source: R
Target: Br
Q_{req}
Q_{id}
MAC
route
R
Attack on SRP

Source: R
Target: Br
Q_{req}
Q_{ID}
MAC
R, Y

M does not append IP-address
Attack on SRP

Source: R
Target: Br
\(Q_{\text{req}}\)
\(Q_{\text{id}}\)
MAC
\(R, Y, Bl, Br\)

\[ R \rightarrow Y \rightarrow M \rightarrow Bl \rightarrow Br \]

- target validates \(Q_{\text{seq}}\) and \(MAC\)
- accepts route request packet
- issues route reply packet
Attack on SRP

- route \{R, Y, Bl, Br\} part of MAC

Source: R
Target: Br
- $Q_{req}$
- $Q_{id}$
- $MAC$
- $Br$
Attack on SRP

Again, $M$ does not append IP-address

Source: R
Target: Br
- $Q_{req}$
- $Q_{ID}$
- MAC
- Br, Bl

Attack on SRP

Source: R
Target: Br
- $Q_{req}$
- $Q_{ID}$
- MAC
- Br, Bl, Y
Attack on SRP

- Source: R
- Target: Br
- $Q_{seq}$
- $Q_{ID}$
- MAC
- Br, Bl, Y, R

- check $Q_{seq}$ and $Q_{ID}$ for legitimacy
- compute and compare MAC using reverse of accumulated route
- route reply packet accepted

Solution Detecting the Attack

- Detects and mitigates node misbehavior
- *bloodhound*
**bloodhound**

- Node should never receive packet identical to one it sent
- *bloodhound* listens in to overhear identical packets

Illustration of *bloodhound*
Illustration of *bloodhound*

$R \quad Y \quad M \quad Bl \quad Br$

$M$ does not append IP-address, so $M$ broadcasts **identical** packet.

Source: $R$
- $Q_{req}$
- $Q_{ID}$
- $MAC$
- $R, Y$

More Questions

- What happens when there is collusion?
- Are other attacks possible?
- If so, how can they be found?
Formal Methods

- Means of verifying protocol
- What is being verified?
  - Goals attained
  - Conditions to satisfy these goals

Weakest Precondition

- Hoare logic
  - Precondition
  - Statement
  - Postcondition
WP Example

Precondition: \( x = ? \)
Statement: \( y = x + 7 \)
Postcondition: \( y = 10 \)

CPAL-ES

- Cryptographic Protocol Analysis Language Evaluation System
- Extends WP reasoning to protocol analysis
- Encode protocols in CPAL and make assertions
CPAL-ES Example

Precondition: ?
S: => T(S.route)
T: <-(T.route’)
T: T.route := <T.route’, T>
Postcondition:
T: assert(T.route == <S,T>)