Mobile Ad Hoc Networks and Secure Routing

John Marshall
marshall@cs.fsu.edu

13 February 2003

Introduction

- Ad hoc networks
- Routing
- Secure Routing Protocol (SRP)
- Attack on SRP
- Solution
- Theoretical basis for attacks
Mobile Ad Hoc NETworks

- MANET – “infrastructure-less”
- Transmission range
- Group coordination – routing

Ad Hoc Routing Protocol

- Route discovery
- Source-driven
- Intermediate nodes forward & accumulate path
Routing Example

Route request issued by Red to Brown

Security for MANETs

- Secure Routing Protocol (SRP)
- Goal – **guarantee** route to destination non-corrupted
SRP Assumptions

- Bi-directional communication
- Security Association (SA) between source and target, includes $K_{S,T}$
- Non-colluding nodes

SRP – Route request

- Issued by source
- Includes
  - Sequence number ($Q_{seq}$)
  - Unique identifier ($Q_{ID}$)
  - Message Authentication Code (MAC) using $K_{S,T}$
  - Route field
An Example of SRP

1. Route request

   - Route request
   - Compute MAC from Source, Target, Q_seq and Q_ID

2. Query propagation

   - Query propagation
   - Check Q_ID
   - Append IP-address
An Example of SRP

2. Query propagation

Route request receipt

- validate $Q_{seq}$ and $MAC$
An Example of SRP

3. Route reply

- compute new MAC with route
- send response packet

Source: R
Target: Br
Q_{req}
Q_{ID}
MAC
Br,Bl
An Example of SRP

4. Reply validation

- check $Q_{seq}$ and $Q_{ID}$ for legitimacy
- compute and compare MAC using reverse of accumulated route
Result of SRP

- Authors claim the route is **guaranteed** to be successfully established and legitimate
- Weaknesses
  1. Intermediate nodes not forced to append address
  2. Destination cannot authenticate *route*

---

Attack on SRP

![Diagram of SRP attack](image)

- Malicious Intermediate Node
Attack on SRP

Source: R
Target: Br
\( Q_{req} \)
\( Q_{id} \)
MAC
R

Route

R \( \rightarrow \) Y \( \rightarrow \) M \( \rightarrow \) Bl \( \rightarrow \) Br
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

\(Q_{req}\)
\(Q_{ID}\)
MAC
\(R, Y, BI\)
**Attack on SRP**

```
R   Y   M   Bl   Br
```

- **target** validates $Q_{seq}$ and $MAC$
- accepts route request packet
- issues route reply packet

---

**Attack on SRP**

```
R   Y   M   Bl   Br
```

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

---

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

---

**Source:** R  
**Target:** Br  
$Q_{seq}$  
$Q_{ID}$  
$MAC$  
$Br$
Again, $M$ does not append IP-address
Attack on SRP

Source: R
Target: Br
\[ Q_{seq} \]
\[ Q_{ID} \]
\[ MAC \]
\[ Br, Bl, Y \]

- check \( Q_{seq} \) and \( Q_{ID} \) for legitimacy
- compute and compare \( MAC \) using reverse of accumulated route
- route reply packet accepted
Implications of Attack

- Source has erroneous route
- route depends on malicious node $M$
- $M$ bears some level of control over route

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

Source: R
Target: Br
Q_{eq}
Q_{ip}
MAC
R, Y
Illustration of *bloodhound*

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

Source: R

Target: Br

$Q_{req}$

$Q_{ID}$

$MAC$

$R, Y$

Finding Attacks

- Intuitive attacks
- BAN logic analysis
- Formal methods (CPAL-ES)