

Mobile Ad Hoc Networks and Secure Routing

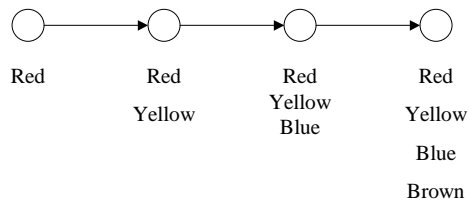
John Marshall
marshall@cs.fsu.edu

19 February 2003

1

Route Accumulation

Route request
issued by Red
to Brown



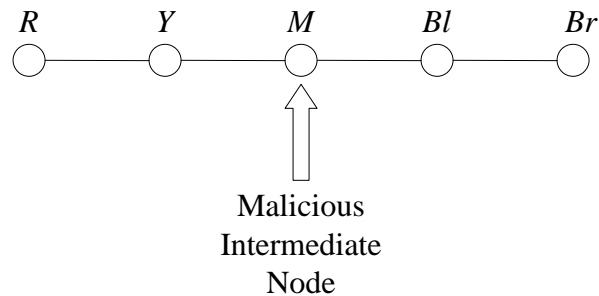
2

“Leap-frogging” Vulnerabilities

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

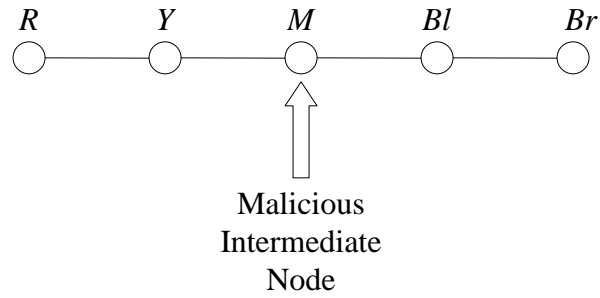
3

Attack on SRP



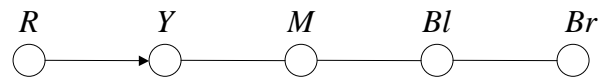
4

Attack on SRP



5

Attack on SRP

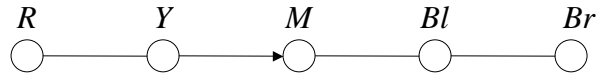


route

Source: R
Target: Br
Q_{seq}
Q_{ID}
MAC
<i>R</i>

6

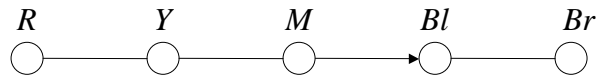
Attack on SRP



Source: R
Target: Br
Q_{seq}
Q_{ID}
<i>MAC</i>
<i>R, Y</i>

7

Attack on SRP

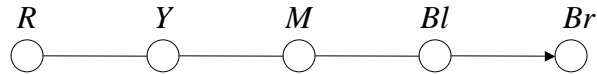


M does not append
IP-address

Source: R
Target: Br
Q_{seq}
Q_{ID}
<i>MAC</i>
<i>R, Y</i>

8

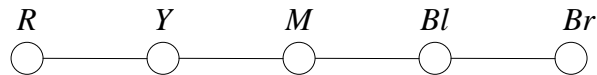
Attack on SRP



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

9

Attack on SRP

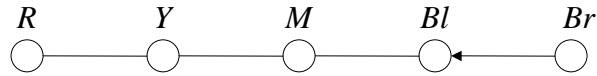


- **target** validates Q_{seq} and MAC
- accepts route request packet
- issues route reply packet

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

10

Attack on SRP



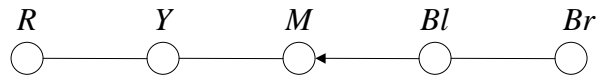
- route {R, Y, Bl, Br} part of MAC

route

Source: R
Target: Br
Q_{seq}
Q_{ID}
MAC
Br

11

Attack on SRP



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

12

Attack on SRP

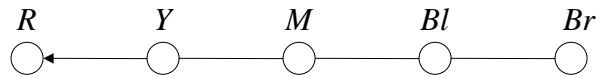


Again, *M* does not append IP-address

Source: R
Target: Br
Q_{seq}
Q_{ID}
<i>MAC</i>
<i>Br, Bl</i>

13

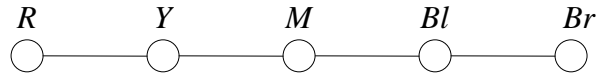
Attack on SRP



Source: R
Target: Br
Q_{seq}
Q_{ID}
<i>MAC</i>
<i>Br, Bl, Y</i>

14

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

15

Solution Detecting the Attack

- Detects and mitigates node misbehavior
- *bloodhound*

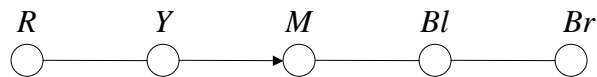
16

bloodhound

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

17

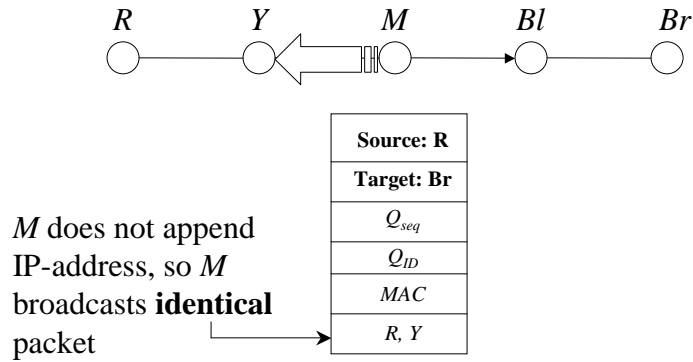
Illustration of *bloodhound*



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

18

Illustration of *bloodhound*



19

More Questions

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

20

Formal Methods

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

21

Weakest Precondition

- Hoare logic
 - Precondition
 - Statement
 - Postcondition

22

WP Example

Precondition: $x = ?$

Statement: $y = x + 7$

Postcondition: $y = 10$

23

CPAL-ES

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

24

CPAL-ES Example

Precondition: ?

S: $\Rightarrow T(\text{S.route})$

T: $\leftarrow (\text{T.route}')$

T: $\text{T.route} := \langle \text{T.route}', \text{T} \rangle$

Postcondition:

T: $\text{assert}(\text{T.route} == \langle \text{S}, \text{T} \rangle)$