

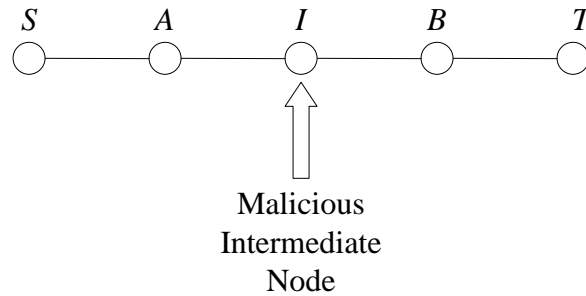
Visualization for CPAL-ES Encoding

John Marshall

17 March 2003

1

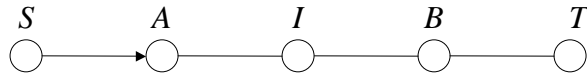
Attack on SRP



17 March 2003

2

Attack on SRP



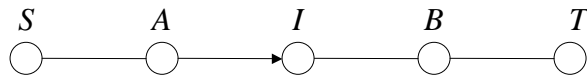
route

Source: S
Target: T
Q_{seq}
Q_{ID}
MAC
S

17 March 2003

3

Attack on SRP

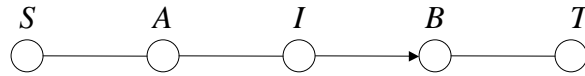


Source: S
Target: T
Q_{seq}
Q_{ID}
MAC
S,A

17 March 2003

4

Attack on SRP



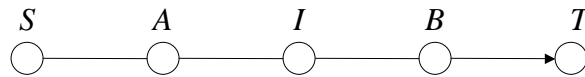
I does not append IP-address

Source: S
Target: T
Q_{seq}
Q_{ID}
MAC
S,A

17 March 2003

5

Attack on SRP

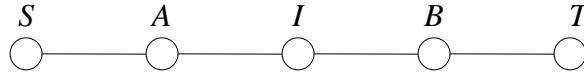


Source: S
Target: T
Q_{seq}
Q_{ID}
MAC
S,A,B

17 March 2003

6

Attack on SRP



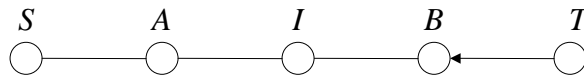
- **target** validates Q_{seq} and MAC
- accepts route request packet
- issues route reply packet

Source: S
Target: T
Q_{seq}
Q_{ID}
MAC
S,A,B,T

17 March 2003

7

Attack on SRP



- *route* {S,A,B,T} part of MAC

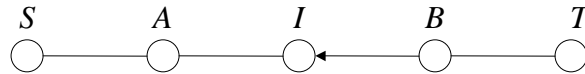
route

Source: S
Target: T
Q_{seq}
Q_{ID}
MAC
T

17 March 2003

8

Attack on SRP

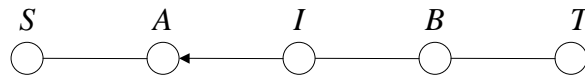


Source: S
Target: T
Q_{seq}
Q_{ID}
MAC
T,B

17 March 2003

9

Attack on SRP



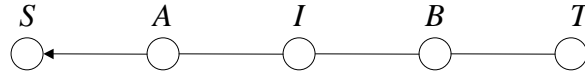
Again, *I* does not
append IP-address

Source: S
Target: T
Q_{seq}
Q_{ID}
MAC
T,B

17 March 2003

10

Attack on SRP

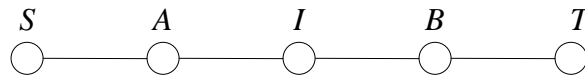


Source: S
Target: T
Q_{seq}
Q_{ID}
MAC
T,B,A

17 March 2003

11

Attack on SRP



Source: S
Target: T
Q_{seq}
Q_{ID}
MAC
T,B,A,S

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

17 March 2003

12

Solution Detecting the Attack

- Detects and mitigates node misbehavior
- *bloodhound*

17 March 2003

13

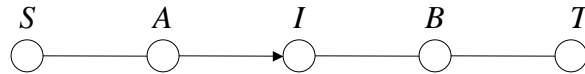
bloodhound

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

17 March 2003

14

Illustration of *bloodhound*

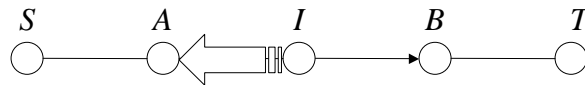


Source: S
Target: T
Q_{seq}
Q_{ID}
MAC
S,A

17 March 2003

15

Illustration of *bloodhound*



I does not append IP-address, so *I* broadcasts **identical** packet

Source: S
Target: T
Q_{seq}
Q_{ID}
MAC
S,A

17 March 2003

16