

Security of Internet Location Management

Tuomas Aura (Microsoft Research, UK)
Michael Roe (Microsoft Research, UK)
Jari Arkko (Ericsson Research, Finland)

11 Dec 2002 Tuomas Aura, Microsoft Research 1

Outline

1. Mobile IPv6 and route optimization
2. Attacks: false Binding Updates (BU)
3. Routing-based authentication
4. More attacks, protocol improvements

11 Dec 2002 Tuomas Aura, Microsoft Research 2

Internet Protocol (IPv6)

source = B
destination = A
...

- Data sent in IP packets, routed through the Internet
- Source spoofing possible

11 Dec 2002 Tuomas Aura, Microsoft Research 3

Mobility

Home A Correspondent B
Current location C

- How to communicate after mobile leaves home?

11 Dec 2002 Tuomas Aura, Microsoft Research 4

Mobile IPv6

source = B
destination = A

source = A
destination = C
original:
source = B
destination = A

- Mobile always uses the same address A
- Home agent forwards packets

11 Dec 2002 Tuomas Aura, Microsoft Research 5

Route Optimization

1. first packet

2. Binding Update (BU)
source = C
destination = B
This is A
I'm at C

3. following packets

11 Dec 2002 Tuomas Aura, Microsoft Research 6

Route Optimization

- Important optimization
- Any IPv6 node can be a correspondent, any address can be mobile
- Binding Update (BU) usually triggered when mobile receives a tunneled packet, but it **may be sent at any time**

11 Dec 2002 Tuomas Aura, Microsoft Research 7

False Binding Updates

- Hijack old connections or open new
- A, B and C can be any Internet nodes

11 Dec 2002 Tuomas Aura, Microsoft Research 8

BU Authentication

- The obvious answer: cryptographic BU authentication, PKI + IPSec
- No global PKI; IPSec too expensive
- New ideas needed!
- Requirements:
 - ➔ as secure as the non-mobile IPv4
 - ➔ zero user and admin interaction

11 Dec 2002 Tuomas Aura, Microsoft Research 9

Creating trust from nothing?

- How authenticate between any two IPv6 nodes, without adding infrastructure?
- Some IP-layer infrastructure available:
 - IPv6 addresses
 - Routing infrastructure
- Address-based CAM [O'Shea,Roe2001]
- Routing-based "weak" authentication

11 Dec 2002 Tuomas Aura, Microsoft Research 10

BU Authentication – v.1

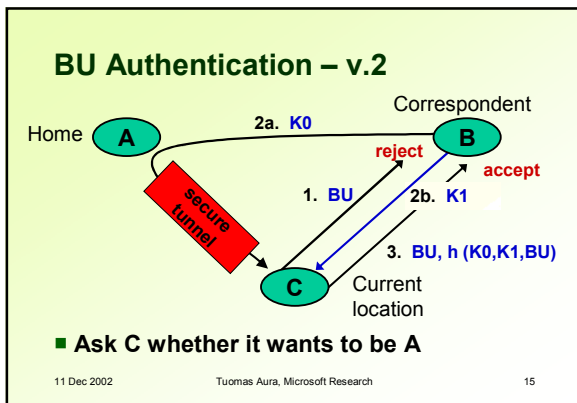
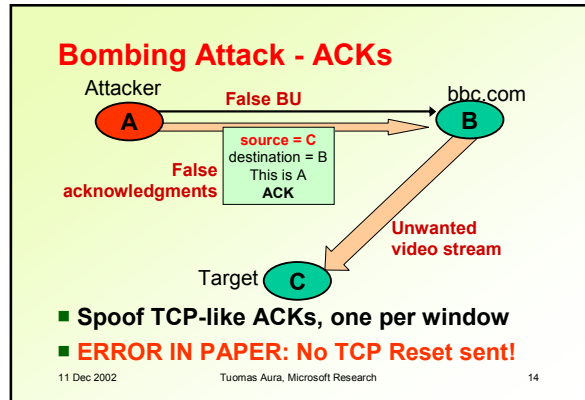
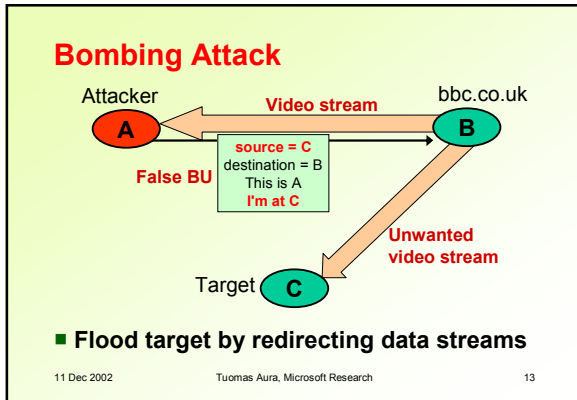
- Send a key in plaintext

11 Dec 2002 Tuomas Aura, Microsoft Research 11

Is that good enough?

- Our protocol, CAM, and other protocols discourage lying about **who you are**
- Still possible to lie about **where you are!**

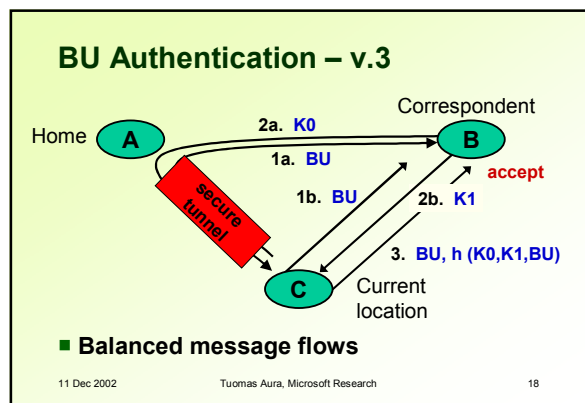
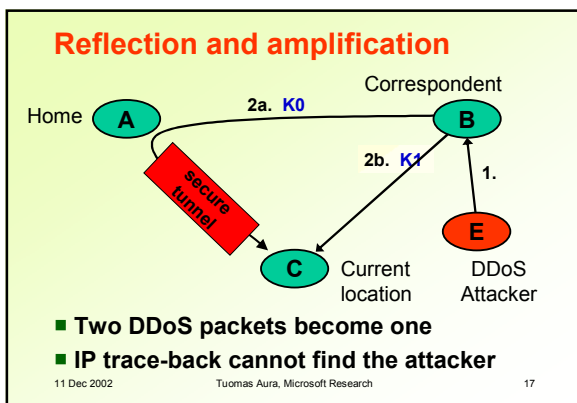
11 Dec 2002 Tuomas Aura, Microsoft Research 12



Is that good enough?

- All information in BUs is true
- Next: Denial of service attacks against the authentication protocol

11 Dec 2002 Tuomas Aura, Microsoft Research 16



Exhausting State Storage

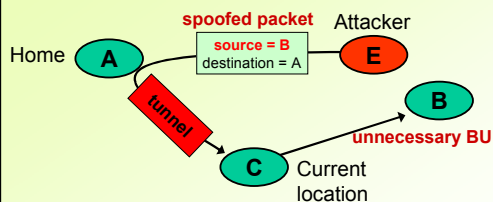
- Correspondent stores K0, K1
 - DoS attack similar to SYN flooding
- Solution: **stateless correspondent**
 - $K0 = h(N, A)$, $K1 = h(N, C)$
 - $N = B$'s periodically changing secret

11 Dec 2002

Tuomas Aura, Microsoft Research

19

Unnecessary BUs



- Spoofed packets to home address trigger **true but unnecessary BUs**

11 Dec 2002

Tuomas Aura, Microsoft Research

20

Summary

- Security the blocking Mobile IPv6 standardization in IETF – not any more
- The difficult part: understanding threats and security requirements
- A “weak” protocol but it does the job: as secure as Internet without mobility
- Solving new problems created by new technology (mobility) before it is deployed

11 Dec 2002

Tuomas Aura, Microsoft Research

21