Network Security: Security of Internet Mobility

Tuomas Aura, Microsoft Research, UK

Outline

- Mobile IPv6
- Threats and protection mechanisms
- Spoofed bindings, bombing attack
- Return routability test

Mobile IPv6

Mobile IPv6

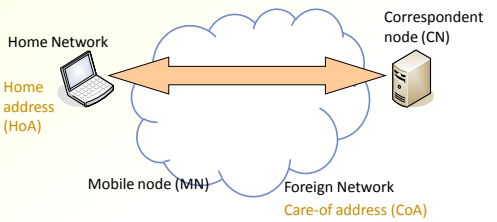
- Network-layer mobility protocol
- Developed since 1991; now standardized by the Internet Engineering Task Force (IETF)
- Mobile IP(v4) [RFC 3344], IPv6 [RFC 3775]
- History:
  - Mobile IPv6 standardization halted in 2000 because of security concerns
  - Security protocol proposed by us in 2001 became a part of the standard. Major security problems fixed
- Next, we'll go through the threat analysis and security protocol design step by step

Mobile IPv6 and addresses

- The mobile node (MN) has two IPv6 addresses
- Home address (HoA):
  - Subnet prefix of the home network
  - Used as address when MN is at home. Used as node identifier when MN is roaming in a foreign network
  - Home network may be virtual – MN never at home.
- Care-of address (CoA):
  - MN's current point of attachment to the Internet
  - Subnet prefix of the foreign network
- Correspondent node (CN) can be any Internet host

(Note: MN and CN are hosts, not routers.)

Mobility



- How to communicate after MN leaves its home network and is roaming in a foreign network?

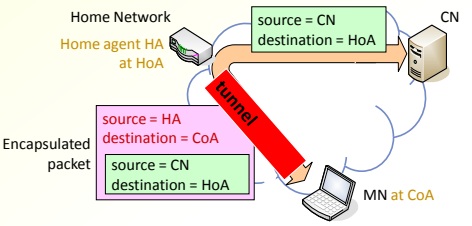
(HoA, CN and CoA are IPv6 addresses)

Mobile IPv6 goals

- Mobility goals:
  - MN is always reachable at HoA as long as it is connected to the Internet at some CoA
  - Connections don't break when CoA changes
- Performance goals (different levels):
  - Roaming (transparent access to VPN, email and web while away from home) has low QoS requirements
  - Mobile multimedia (real-time voice and sound while constantly moving) requires delays < 200 ms
- Security goals:
  - As secure as the current Internet without mobility

7

Mobile IPv6 tunnelling



- Home agent (HA) is a router at the home network that forwards packets to and from the mobile
- MN always reachable at HoA

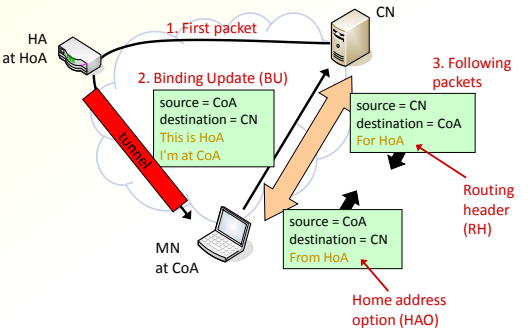
8

Tunneled packets on the wire

- IPsec ESP tunnel between HA and MN
  - HA uses its own IPv6 address as the tunnel endpoint
  - MN uses the CoA as the tunnel endpoint → both SPD and SAD must be updated at HA when the mobile moves
- Packet from CN to HoA:
  IP[CN,HoA] | Payload (intercepted by HA)
  Forward tunnel from HA to CoA:
  IP[HA,CoA] | ESP | IP[CN,HoA] | Payload
- Reverse tunnel from MN to HA:
  IP[CoA,HA] | ESP | IP[HoA,CN] | Payload
  Packet forwarded from HA to CN:
  IP[HoA,CN] | Payload
- Note: no problems with ingress filtering because all source addresses are topologically correct

9

Route optimization (RO)



10

Route-optimized packets on the wire

- Packet from CN to MN:
  IP[CN,CoA] | RH[HoA] | Payload
  (RH = Routing header Type 1, "for HoA")
- Packet from MN to CN:
  IP[CoA,CN] | HAO[HoA] | Payload
  (HAO = Home address option, "from HoA")
- Again, all source addresses are topologically correct

11

Route optimization

- Important optimization:
  - Normally, only the first packet sent via home agent (HA). Binding udpate (BU) triggered when MN receives a tunneled packet. All following packets optimized
  - But, if CN does not support BU or decides to ignore them, then all packets are tunneled via HA
- MN may send the BU at any time
  - In principle, IP layer is stateless and does not know whether there was previous communication

12

Binding update

- Originally, a 2-message protocol:
  - Binding update (BU) from CoA to CN
  - Binding acknowledgement (BA) from CN to MN

  Now a much more complex protocol, for security reasons that we'll soon explain
- CN caches the HoA–CoA binding in its binding cache for a few minutes
  - MN may send a new BU to refresh the cache or to update its location
  - CN may send a binding request (BR) to MN to ask for a cache refresh

13

Who are MN, CN?

- Any IPv6 host may be the correspondent
- Any IPv6 address can become mobile, even though most never do
- By looking at the address, CN cannot know whether home address (HoA) belongs to a mobile node

→ Security flaws in Mobile IPv6 may be used to attack any Internet node

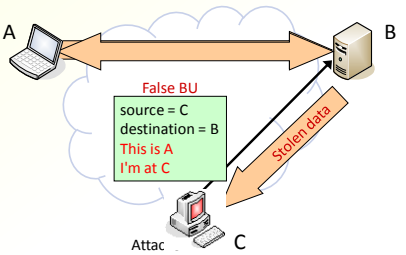
14

Threats and protection mechanisms

All weaknesses shown here have been addresses in the RFC

15

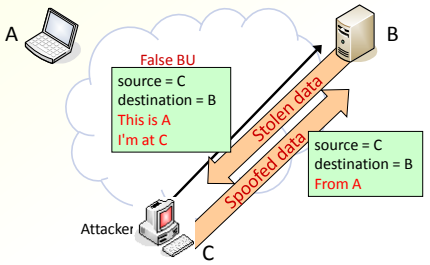
Attack 1: false binding updates



- A, B and C can be any IPv6 nodes (i.e. addresses) on the Internet

16

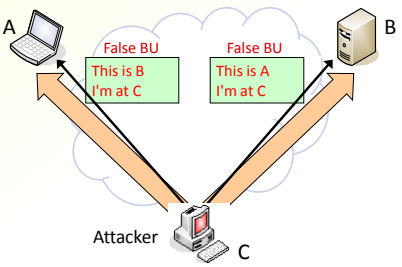
Connection hijacking



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

17

Man-in-the-middle attack



18

If no security measures added

- Attacker anywhere on the Internet can hijack connection between any two Internet nodes, or spoof such a connection
- Attacker must know the IPv6 addresses of the target nodes, though

19

BU authentication

- MN and HA trust each other and can have a secure tunnel between them. Authenticating BUs to CN is the problem
- The obvious solution is strong cryptographic authentication of BUs
- Problem: there is no global system for authenticating any Internet node

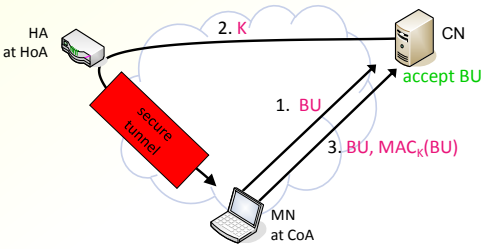
20

Authentication without infrastructure?

- How authenticate messages between any two IPv6 nodes, without introducing new security infrastructure?
- Set requirements to the right level: Internet with Mobile IPv6 deployed must be as secure as before it → no general-purpose strong authentication needed
- Some IP-layer infrastructure *is* available:
  - IPv6 addresses
  - Routing infrastructure
- Surprisingly, both can be used for BU authentication:
  - Cryptographically generated addresses (CGA)
  - Routing-based "weak" authentication, called return routability

21

BU Authentication – v.1



- CN send a key in plaintext to HoA

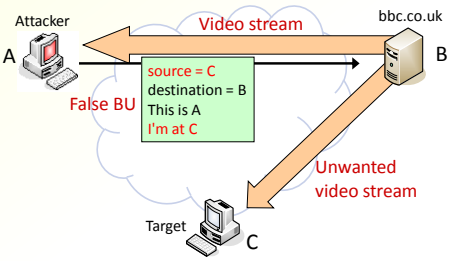
22

Is that good enough?

- "Weak", routing-based authentication, but it meets the stated requirement
- Attacker has to be on the path between CN and HA to break the authentication and hijack connections
  - This is true even if the MN never leaves home, so mobility does not make the Internet less secure
  - Not possible for any Internet node to hijack any connection → significantly reduced risk
- K is not a general-purpose session key! Only for authenticating BUs from MN to CN
- Anything else?
  - The weak authentication, CAM, and other protocols discourage lying about who you are
  - Still possible to lie about where you are!

23

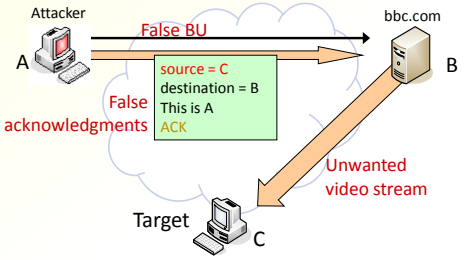
Attack 2: bombing attack



- Attacker can flood the target by redirecting data streams

24

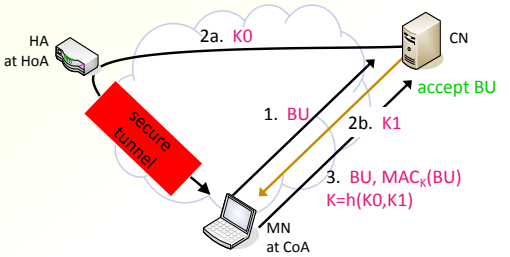
Bombing attack - ACKs



- Attacker participated in the transport-layer handshake → can spoof TCP ACKs or similar acknowledgements
- Attacker only needs to spoof one ACK per sender window to keep the stream going
- Target will not even send a TCP Reset!

25

BU Authentication – v.2



- CN sends a message to CoA to ask whether someone there wants the packets
- Common misconception: the purpose is not to send K0 and K1 along two independent paths!

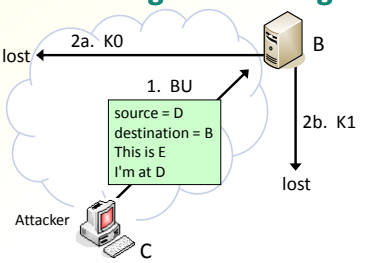
26

Is that good enough?

- Not possible to lie about identity or location; all information in BUs is true
- Almost ready, but we still need to consider standard denial of service attacks against the BU protocol

27

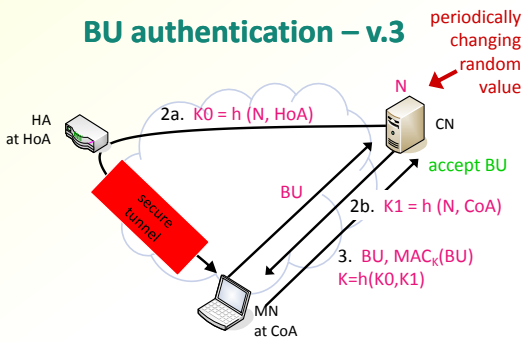
Attack 3: Exhausting state storage



- Correspondent will generate and store K0, K1
- Attacker can flood CN with false BUs → CN has to remember thousands of K0s and K1s

28

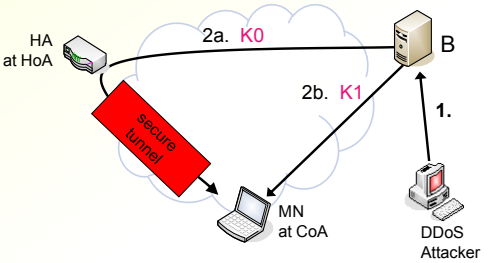
BU authentication – v.3



- We can make the correspondent stateless

29

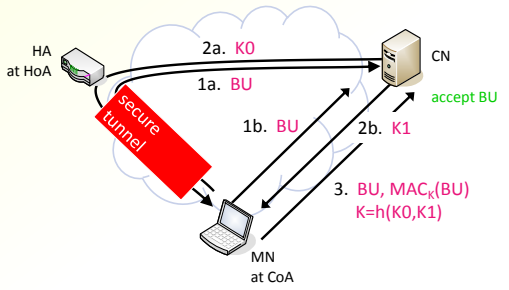
Attack 4: reflection and amplification



- Two DDoS packets become one — minor issue
- IP trace-back cannot find the attacker

30

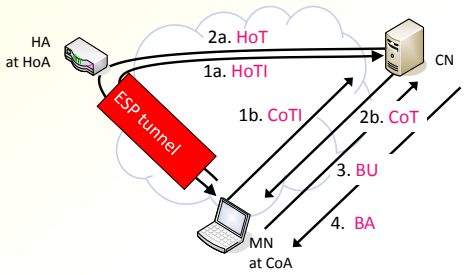
BU Authentication – v.4



- Balanced message flows prevent amplification

31

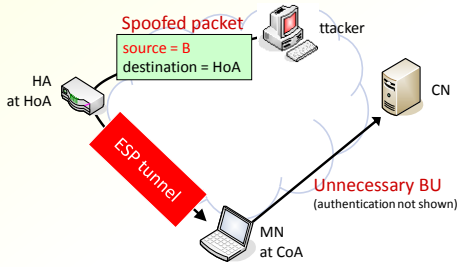
The Mobile IPv6 Standard Protocol



- Return routability (RR) test for HoA and CoA
- Similar mechanisms, completely different purpose

32

Attack 5: Unnecessary BUs

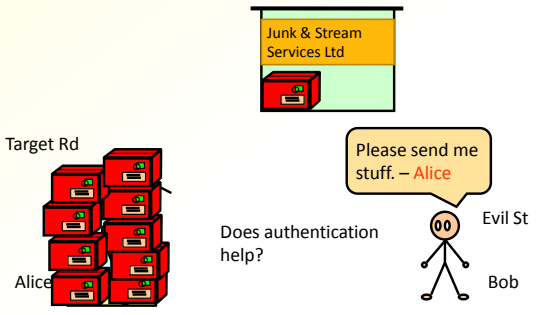


- Tunneled packets trigger BUs → spoofed packets to home address trigger true but unnecessary BUs → DoS Attack against MN or a correspondent
- Defense: limit the amount of resources used for BU authentication; revert to non-optimized routing

33

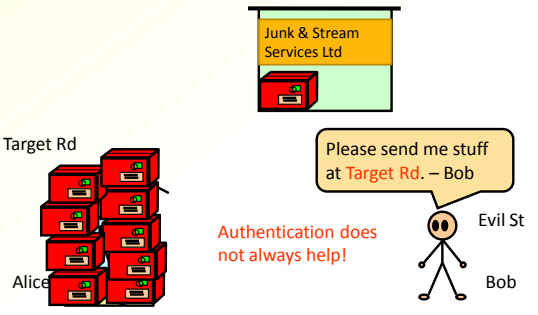
More about bombing attacks

Packet-bombing attack



35

Packet-bombing attack



36

SIP/RTP

- Session initialization protocol (SIP): application-layer signaling protocol for establishing multimedia sessions
- Session description protocol (SDP)
- Real-time transport protocol (RTP)

37

SIP INVITE Method

SIP headers

```
INVITE sip:carol@streamer.com SIP/2.0
Via: SIP/2.0/UDP pc12.evil.org;branch=z9hG4bK796afe9
Max-Forwards: 100
To: Carol <sip:carol@streamer.com>
From: Bob <sip:bob@evil.org>;tag=7482728239
Call-ID: b4jw7q8weiop9e@pc12.evil.com
CSeq: 1 INVITE
Contact: <sip:bob@pc12.evil.org>
Content-Type: application/sdp
Content-Length: 142

v=0
o=bob 5567283244 5567283112 IN IP4 pc12.evil.org
s=Evil attack
i=An audio stream to Bob
c=IN IP4 11.22.33.44
t=2875561965 3554545292
r=1h 1h 0
a=sendonly
m=audio 49170 RTP/AVP 0
```

Bob requests an RTP stream

SDP body

Bob's IP address = stream destination

38

SIP Bombing Attack

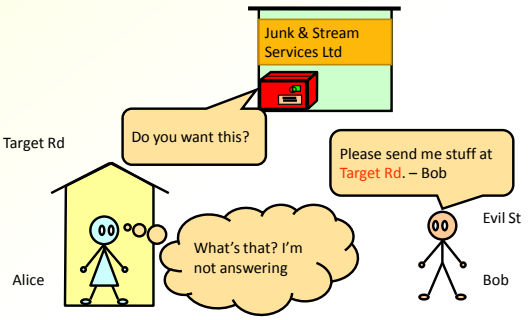
```
INVITE sip:carol@streamer.com SIP/2.0
Via: SIP/2.0/UDP pc12.evil.org;branch=z9hG4bK796afe9
Max-Forwards: 100
To: Carol <sip:carol@streamer.com>
From: Bob <sip:bob@evil.org>;tag=7482728239
Call-ID: b4jw7q8weiop9e@pc12.evil.com
CSeq: 1 INVITE
Contact: <sip:bob@pc12.evil.org>
Content-Type: application/sdp
Content-Length: 142

v=0
o=bob 5567283244 5567283112 IN IP4 pc12.evil.org
s=Evil attack
i=An audio stream to Bob
c=IN IP4 12.34.56.78
t=2875561965 3554545292
r=1h 1h 0
a=sendonly
m=audio 49170 RTP/AVP 0
```

alices-pc.target.com

39

Ask Permission to Send (1)



40

Protocol layering issues

- Mobility is usually implemented in a lower protocol layer than data transport (e.g., IP vs. TCP).
  → Mobility is transparent to the data-sending layer
  → Sender does not know about changes of the peer address
- ➔ Solutions typically lead to layer violations i.e. require network and transport layer to know about each other's state

42

Exercises

- Based on the historical flaws in Mobile IPv6, are there any potential security problems in dynamic DNS? Does Secure DNS solve these problems?
- Design a more efficient binding-update protocol for Mobile IPv6 assuming a global PKI is available
- How could the return-routability test for the care-of address (CoA RR) be optimized if the mobile is opening a TCP connection? What are the advantages and disadvantages?
- What problems arise if mobile node can automatically pick a home agent in any network

43