Table of Contents

• State Establishment
  – State Establishment at SPINAT Node
  – State Establishment at End-Hosts

• Packet Processing
  – Control Signaling packet handling
  – ESP packet processing
    • IP Address and SPI Translation at SPINAT Nodes
    • SPI Translation at End-hosts

• Packet formats
NAPT vs. SPINAT

• In NAPT the port values are not protected,
  – in SPINAT SPI values in ESP headers are integrity protected

• SPINAT is not completely transparent

• SPINAT requires a separate key-exchange protocol to setup state
  – ESP header contains only destination SPI value not source
State and Translation

• The state is indexed by the SPI
• SPI is translated if two clients choose same value
  – SPI translation is done outside of the ESP HMAC protection
  – SPI translation is done both in end-host and SPINAT node
• The source IP address is replaced with the SPINAT’s address
SPINAT state establishment

MN

Private address space

I1
R1
I2
R2
ESP(SPI_mn)
ESP(SPI_cn)

Source IP replaced

Internet

I1
R1
I2 + ESP_INFO(SPI_spinat)
R2
ESP(SPI_spinat)
ESP(SPI_cn)
Table of Contents

• Background: Alternative Moving Network Approaches
• Basic concept
  – Pre-Movement Phase
  – Node Movement Phase
  – Delegation Phase
  – Network Movement Phase
• Protocol Description
  – Mobile Router Discovery
  – HIP base/update exchange between the MN and its peers
  – Mobile Node Authorizes a Mobile Router
  – MR runs update exchange with the peer nodes
  – Leaving a Moving Network; Revoking tickets
  – Kerberos vs. Ticket based Delegation of Signaling Rights
  – Using the keying material
• Packet processing
  – End-to-end Base Exchange
  – End-to-end update exchange
• Payload Format
Alternative Moving Network Approaches

1. Each of the mobile nodes takes care of mobility signaling separately.

2. A tunneling approach all traffic is tunneled through some home router in the fixed network side.

3. Mobile node to delegates the right to do mobility signaling to the mobility router, which under certain conditions may delegate this right further into some node in the fixed network side.
Concepts

• HIP Mobile router acts as signalling proxy
  – Signaling rights are delegated to MR to minimize the signalling
  – Signaling rights may be further delegated to a proxy in fixed network

• Tickets used instead of X.509/SPKI certificate
  – Not Kerberos: Kerberos doesn’t work for nested MRs as nested MR would be the KDC and client at the same time
  – Not SPKI: Tickets use symmetric crypto instead public key certificates
  – Tickets are created from the session key generated during BEX
Concepts (cont.)

- Service discovery used to find the nearest/on path MR
- HIP Registration protocol extended
- Mobile Network is not renumbered
  - MR acts as either as an NAT (SPINAT) or it does 1-to-1 mapping (IPv6)
HIP MR - state establishment

MN

HIP Mobile Router

CN

Private address space

Internet

I1 / UPD (SEQ)

R1’ ( + REG_INFO)

I2’ ( + REG_REQ + ticket)

R2’ ( + REG_RESP)

R1 / UPD (SEQ ACK)

I2 / UPD (ACK)

R2

UPD(SEQ, ticket)

UPD(ACK)

IN PARALLELL
HIP MR - location update

MN

HIP Mobile Router

Private address space

NOTIFY (LOCATOR)

MN IP: C

ESP packets

UPD (SEQ + HMAC(ticket))

MR IP: A

Handoff

UPD (SEQ ACK)

UPD (ACK)

ESP packets

MR IP: B

CN

Internet
So what now???

- Lots and lots of details missing from the drafts
  - Closing of HIP connections
  - Multihoming
- More details needed for the data packet processing
- Revocation of tickets needs more work
- Packet formats needs to specified for both drafts