
Sun
microsystems
Connectathon 2001

Cthon 2001

Connectathon 2001

Summary of Mobile IPv6 Security Issues

Revision 1.0 03/07/2001

Mohan Parthasarathy, Alper E. Yegin, Carl Williams
Sun Microsystems, Inc.

Overview of issues?

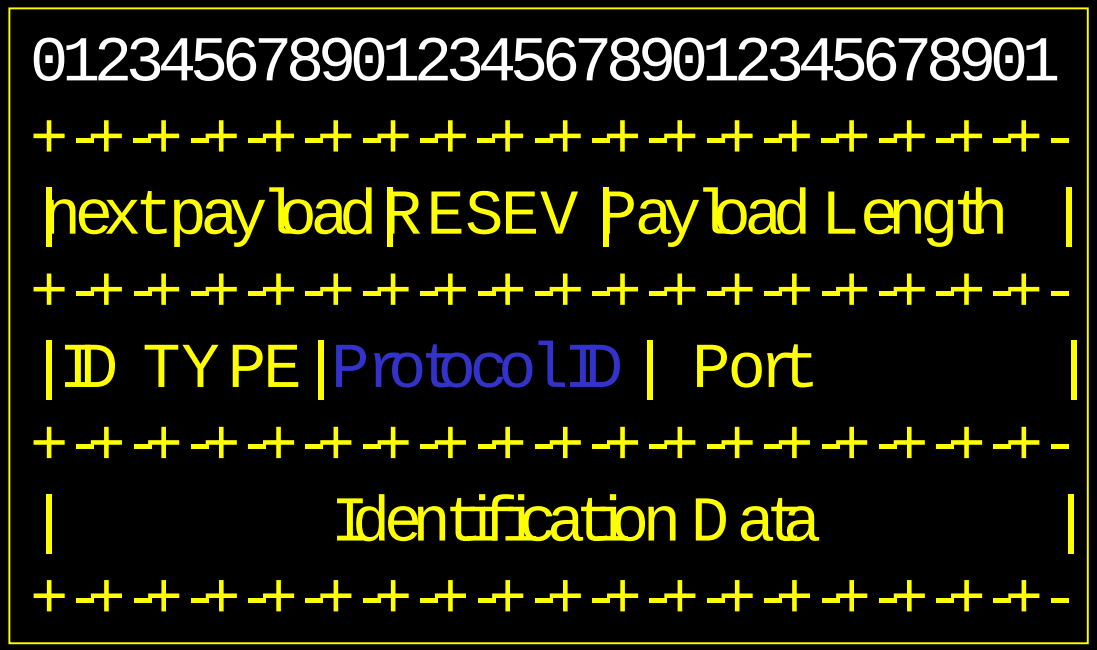
- IKE doesn't have a way to negotiate IPsec SAs for a particular destination option
- Policy Selector – should we define one for specific destination options?
- ESP with Auth – (MN-CN) – should we use that instead of negotiating a new SA?
- ICMP errors could blow away the binding cache entry.
- Authorization issue – How does one verify whether the MN is authorized to use the home address or "care-of address".

Policy Selector – Specific Destination Option?

- IP Traffic is mapped to IPsec policy by *"selectors"*
- Current Selectors as specified in RFC 2401
  - Destination IP address
  - Source IP address
  - Name
  - Transport layer protocol (ipv4 protocol or ipv6 nexthdr fields)
  - Ports
- Want a specific destination option defined as a selector?
  - Binding updates
  - Binding ack
  - Binding request

IKE – ID payload

- We don't have a way to negotiate IPsec Sas for particular destination option.
  - ProtocolID can be set to 60 which means all destination options.



  - How do we do it for binding update, request, and ack only?

ESP with auth

- Currently, binding update must be protected using AH.
- If ESP with auth SA is available between MN and CN, should we use this instead of negotiating a new SA with AH?
- Would need to use alternate "care-of" address option in binding update.

Authorization issue

- Binding updates are protected with IPsec. But IPsec itself does not tell you how to do the authorization part... .
- Establishment of IPsec SA between MN and CN
  - Phase 1: (authentication phase)
    - Identity could be FQDN, certificate, etc...
  - Phase 2: (negotiating IPsec SA)
    - Use home address as the identity (per Mobile IPv6 spec) – so that the SAs can be bound to the home address.
- Problem: What prevents MN from using home address of some other mobile node in phase 2.

Authorization issue (cont)

- After issue raised on IPsec mailing list so following solution was proposed:
  - Have a certificate for every mobile node that has the home address and the identity.
  - Policy that verifies the phase I identity against the home address used in phase II.
- This is possible between MN and HA – but how do we do this with Random CN?
- Requires global PKI

Authorization issue (cont)

Possible Solutions using DNSSEC

- Punt Ipsec
  - Send signed message using the private key associated with the home address... .
  - Receiver can obtain the public key from the DNS corresponding to the home address to verify the signature.
- DNSSEC plus Ipsec Alternative 1:
  - In phase 1 lookup the public key using the identity sent in phase 1 (FQDN) and verify the signature.
  - In phase 2 reverse lookup the home address (identity sent) and match it with what we got in phase 1.

Authorization issue (cont)

- DNSSEC plus IPsec Alternative 2:
  - In phase 1 use the home address itself as the identity and get the public key for verification of signature.
  - In phase 2 match the identity – home address (one that was sent in phase 1).
  - ISSUE: some IKE implementations check whether the phase 1 identity matches the source address of the packet if the identity is an address.
  - Possible solution : Invent a new ID type.

Authorization issue (cont)

- Bradner et al Solution:
  - Doesn't need global PKI
  - MN Generates public-private key pair.
  - MN computes hash of public key – EID and send to CN at the beginning of the session.
  - MN needs to send public key, signed BU using the private key.
  - CN receives the public key & verifies with EID and then verifies the signature of the binding update.

Problems: What prevents someone from spoofing the MN and sending a bogus EID.


Sun
microsystems