“Childproof” Authentication for Mobile IPv6 (CAM)

Michael E. Locasto

<locasto@cs.columbia.edu>
COMS 6998.1 Adv. Topics in Security

Overview

- Why the effort to deploy Mobile IPv6 without IPsec? (and quantify CP)
- brief sketch of traditional Mobile IP
- The paper:
  - observations & system
  - conclusions
- Tie-in to other papers & Discussion

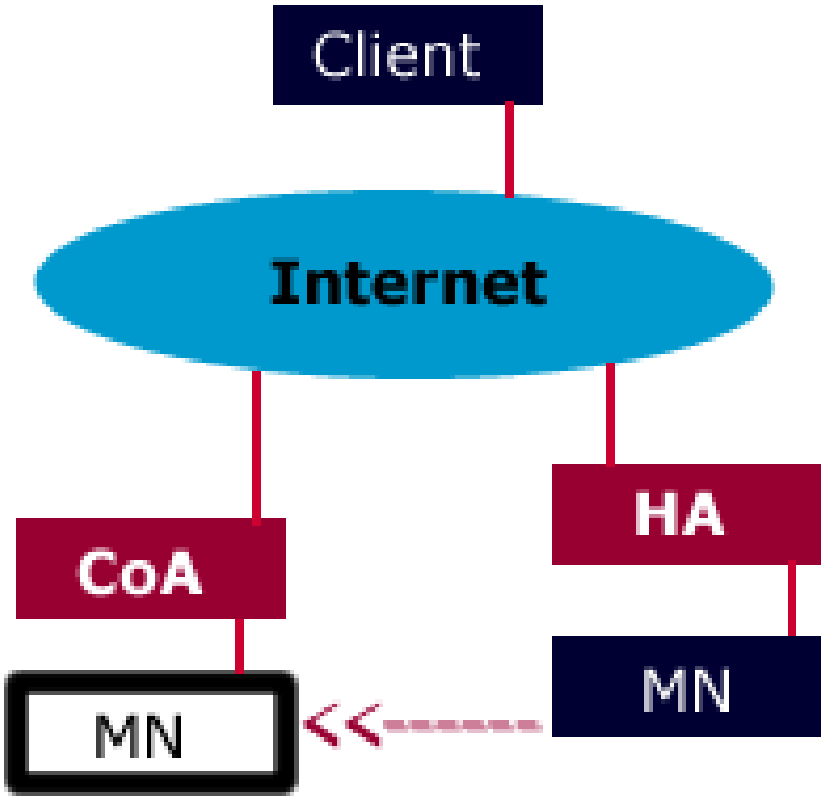
Why CAM?

- Motivation for MIP (address tied to net)
- Motivation for IPv6 (+IPsec)
- Motivation for CAM ("reduce risk of deploying MIPv6 without AH support")
  - claim: IPsec has problems too
- "Childproof" == basic, limited, "usuable" functionality

Traditional MobileIP

- The problem: mobile nodes
  - cannot ‘flatten’ routing
  - network layer is good target
  - split ‘identifier’ and ‘location’
  - tunnel IP in IP to reach remote node
- Clearly, many opportunities to subvert
  - IPv6 mandates AH for MIP ‘binding update’
  - home addr option field not auth’d

How MobileIP works



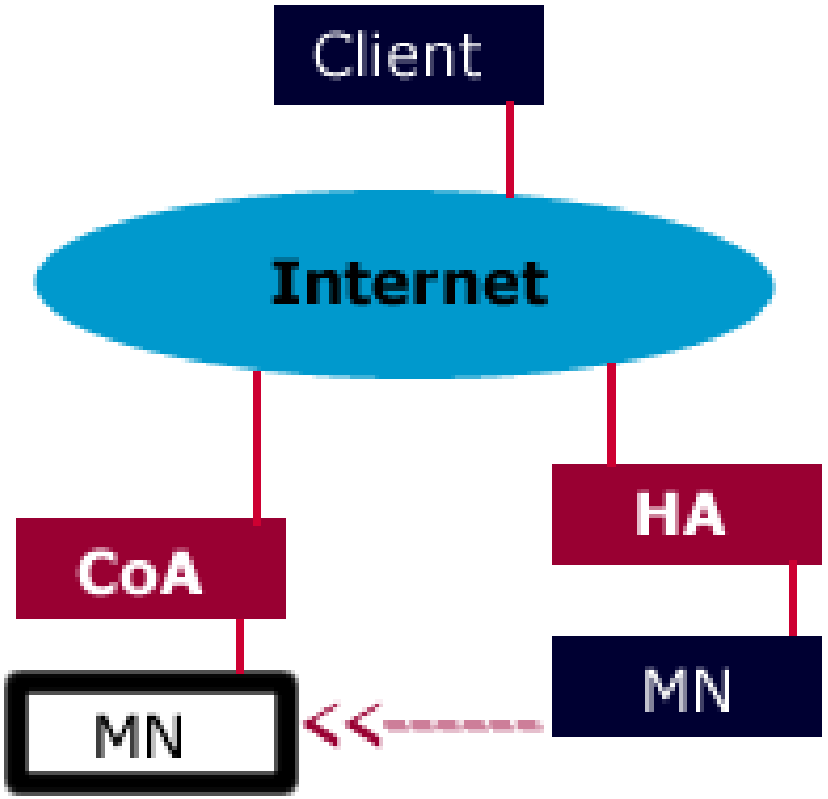
- M leaves net
- M tells HA
- C seeks M (HA)
- HA tunnels to M/CoA
- M may update C (bypass HA)
- Why not DHCP?

What is CAM?

- 1-way auth of “Binding Update”
- embedded in MIPv6 message exchange
- home addr = [net][SHA-1(pubkey)]
- send correspondent everything it needs to know to validate mobile node
- “Believe that my CoA is X because I can prove I am Y.”

How does CAM work?

- Message =
  {
  $A'_m, A_c, A_m, PK_m, i, T_m,$
  {
  $H(A'_m, A_c, A_m, T_m)$
  }SK_m
  }
- add "destination sub-option"



CAM Limitations

- Ignores IPsec
- One way (mobile --> correspondent only)
- change home addr with new key every few days (mobile server?)
- What about transition?
  - IP->CAM->IPSec
  - IP->IPSec

Themes & Tie-ins

- Design problems && patterns
  - difficult to come up with a “secure” protocol (including auth, integrity, PFS, non-repudiation, etc)
  - If 2 guys from M$ can’t do it, what does that say for us poor slobs?
  - careful definitions, state limits, reduction to a known proof methodology

Further Reading

- http://w.c.c.e/~locasto/projects/cam/
  - RFC 3344, 3024, 2002
  - JI '91 SIGCOMM paper (~ji/F02/)
  - JI presentation on Mobile IP
  - survey paper on Mobile IP
  - Greg O'Shea presentations...