End-to-End Mobility Support:
Combining Security and Efficiency

Christian Vogt, chvogt@tm.uka.de

NEC Europe, Network Laboratories, Heidelberg
September 16, 2004
Outline

- **Mobility** scenarios, **security** threats
- **Flooding** attacks *(will be our focus)*
- **Protection** in Mobile IPv6 *(induces latency…)*
- **Latency**-oriented optimization *(has three parts…)*
  - Early Binding Updates
  - Credit-Based Authorization
  - IP-Address Spot Checks
- Open **issues**, future work
- Summary
Mobility Scenario

- Mobile Node (MN) **moves** through IP sub-networks
- MN **configures** new IP addresses
- MN **registers** new IP addresses with Correspondent Node (CN)
- CN and MN **switch** to new IP address
- Mobility-management protocol **screens** IP-address changes
Security Threats: Impersonation

- If a MN can change its own IP address…
- …then an attacker might be able to redirect packets on behalf of a victim
- The attacker could be a connection high-jacker…

Before the attack...

Connection high-jacking
Security Threats: Impersonation (2)

- ...an eavesdropper or MiTM...
- ...or it could simply cause havoc
- ⇒ Authentication before redirection
Security Threats: Resource Exhaustion

- If it takes the CN a lot of resources to process an IP-address registration...
- ...then an attacker might massively register spoofed IP-addresses
- CN can no longer have meaningful communications
- \( \Rightarrow \) Commit resources only after MN’s authentication

Before the attack...

Blocking meaningful communications
Security Threats: Flooding

- If a MN can redirect its packets to a new IP address...
- ...then an attacker might redirect a high load of traffic to a victim
- Victim can be any IP node
Security Threats: Flooding (2)

- **Attacker**
  - TCP SYN + ISN
  - TCP ACK
  - **Attacker knows ISN**
  - **IP-Address Update**
  - TCP ACK
  - TCP ACK
  - TCP ACK

- **TCP Server (CN)**
  - TCP SYN-ACK + ISN
  - TCP ACK
  - TCP ACK
  - TCP ACK
  - TCP ACK

- **Victim**
  - Segment
  - Segment
  - Segment
  - Segment

- **Authentication** is what matters

- **Check** a new **IP address** before using it
Focus on Flooding Attacks

Consider Mobile IPv6 as an example…
Mobile IPv6: An Overview

- MN has two IP addresses
  - **Care-of address** (CoA) from visited network
  - **Home address** (HoA) from Home Agent’s (HA) network
- **Home Agent** proxies MN (MN reachable at HoA)
- Mobile IPv6 swaps HoA, CoA (binding)
  - HoA for **upper layers**, signaling **authentication** (long-term significance)
  - CoA for **packet transportation** (topologically correct)
- **Correspondent registration** (binding update)
  - HoA test for signaling authentication
  - New-CoA test for flooding-attack prevention
Correspondent Registration

Mobile IPv6 (RFC 3775)

Christian Vogt, Research Institute of Telematics, University of Karlsruhe, Germany
Correspondent Registration (2)

Mobile IPv6 (RFC 3775)

- Bidirectional comm.
- No communications
- Unidirectional comm.

- Home Test Init
- Care-of Test Init
- Care
- Home Test (T1)
- Care-of Test (T2)
- CN sends packets misrouted
- CN learns new CoA
- CN’s packets misrouted
- Binding Ack

- MN not sending
- Last packet successfully delivered at old CoA
- MN resumes sending
- First packet delivered at new CoA

Goal: Reduce registration latency

Handover

Mobile IPv6 (RFC 3775)
Early Binding Updates

- Home Test Init
- Early Bndg. Upd. (T1)
- Early Binding Ack
- Bndg. Upd. (T1,T2)
- Binding Ack
- Proactive HoA test

Concurrent CoA test

Handover

Christian Vogt, Research Institute of Telematics, University of Karlsruhe, Germany
Early Binding Updates (2)

- **Home Test Init**:
  - Last packet successfully delivered at old CoA

- **Early Bndg. Upd. (T1)**
  - Care-of Test Init

- **Bndg. Upd. (T1,T2)**
  - First packet delivered at new CoA through HA

- **Bidirectional comm.**
  - First packet directly delivered at new CoA

- **Handover**
  - CN learns new CoA
  - CN has packets misrouted

- **Unidirectional comm.**
  - New CoA becomes verified

- **Bidirectional ▲ comm.**
  - CN learns new CoA

- **Unidirectional comm.**
  - Proactive HoA test

- **Bidirectional comm.**
  - Goal: Reduce registration latency

**Goal**: Reduce registration latency
Temporarily routing through the HA is sub-optimal.

Can we enable direct bidirectional communications even while the new CoA is unverified?

Yes, we can…
Credit-Based Authorization

- CN does **send** packets **to an unverified CoA**, but…
- **Not more than** recently **received** from MN
- ⇒ **No amplification**
- **Redirection** possible, but **little attractive** (direct flooding is easier)

Goal

Direct bidirectional comm. while new CoA unverified
Credit-Based Authorization: An Example

**MN**

**Handoff**

**Early Binding Update**

**Binding Update**

**CN**

CREDIT++
CoA verified
CREDIT++
CoA verified
CREDIT++
CREDIT- - (CoA unverified)
CREDIT++
CoA verified
CREDIT++
CoA verified
Credit-Based Authorization: An Example (2)

Aging prevents time-shifting

CN learns new CoA

New CoA becomes verified

New CoA unverified
- MN usually sends less than CN
- MN may not get enough credit

While CoA is verified... While CoA is unverified...

Support applications with asymmetric traffic, too

Goal

This throughput is missing
If we can give a MN credit for packets that it sends…

…then we could also give the MN credit for packet reception

The MN spends comparable resources on receiving packets as on sending packets
Supporting Asymmetric Traffic (3)

Handoff

Early Binding Update

Binding Update

MN

CN

CREDIT++ (CoA verified)

CREDIT++ (CoA verified)

CREDIT++ (CoA verified)

CREDIT++ (CoA verified)

CREDIT-- (CoA unverified)
Supporting Asymmetric Traffic (4)

While CoA is verified... While CoA is unverified...

Support applications with asymmetric traffic, too

Throughput as usual

Goal
Supporting Asymmetric Traffic, more…

- CN knows what it sends…
- …but not what the MN receives
- An attacker may locate behind bottleneck

Goal
Credit received packets, not sent packets
Preventing the attack
(Packets are dropped somewhere)

Under attack
Preparing the attack
(Collecting credit)
Care-of Address Spot Checks

CREDIT ~
\[
\frac{\text{# Cookies returned}}{\text{# Cookies sent}}
\]

Goal
Credit received packets, not sent packets
The Big Picture

Early Binding Early Binding AckAck
CareCare--of Test (T2)

Home Test Init

Bidirectional comm.

Early Bndg. Upd. (T1)
Care-of Test Init

Last packet successfully delivered at old CoA

Concurrent CoA test

Bidirectional comm.

First packet directly delivered at new CoA

Bndg. Upd. (T1,T2)

Unidirectional comm.

Handover

Bidirectional comm.

MN HA CN

Home Test (T1) Proactive HoA test

Early Binding Ack Care-of Test (T2)

CN learns new CoA

CN's packets misrouted

New CoA unverified

Bidirectional comm.

Goal

Direct bidirectional comm. while new CoA unverified

(draft-vogt-mip6-early-binding-updates)
(draft-vogt-mipv6-credit-based-authorization)
Early Binding Updates are specific to Mobile IPv6, but…

- Concurrent IP-address tests
- Credit-Based Authorization
- IP-Address Spot Checks

…are also **applicable to other MM protocols** (e.g., HIP, Mobike, SCTP)

- Credit-Based Authorization (w/o Spot Checks) is **transparent** to MN

- **End-to-end** vs. local
  - Fast and Hierarchical Mobile IPv6 are faster…
  - …but do not work across administrative domains
Open Issues, Future Work

Open Issues

- How do these optimizations perform in a real scenario?
- What are the impacts on applications?
- Credit sent or received packets?
- What protocol parameters are best? (Aging, tentative binding lifetime)
- How complex is an implementation?

Future work

- MN may anticipate movement and proactively configure new IP address

⇒ Credit-Based Authorization allows for anticipated IP-address registration
Mobility causes security threats

- Impersonation
- Resource exhaustion
- Flooding

Solution: HoA/CoA-address test (in Mobile IPv6)

- Trade security for latency

Optimization: Early Binding Updates

- Proactive HoA test
- Concurrent CoA test

CN still cannot send to unverified CoA ⇒ Credit-Based Authorization

- Credit packets received from MN
- …or packets sent to MN
- …or packets received by MN (Spot Checks)