Early Binding Updates and Credit-Based Authorization – A Status Update

Christian Vogt, chvogt@tm.uka.de
Why Do We Need Enhancement?

- Mobile IPv6 Route Optimization uses return-routability procedure to authorize binding between…
  - Home address == Who I am
  - C/o address == Where I am
- Idea: Verify MN's reachability at
  - home address for authentication
  - c/o address for binding authorization
- Handoff delays btw. 3 and 4 RTT
  - depends on degree of parallelism that implementation use
- Reduce this!
Enhancement Approaches

Early Binding Updates

- Modification to Mobile IPv6 binding-update procedure
  - Proactivity
  - Concurrency
  - Higher degree of parallelism
- Reduces handoff latency
  - to 1 RTT for reactive handoffs
  - to 0~1 RTT for proactive handoffs

Credit-Based Authorization

- Strategy followed by CN
- Determines data that CN can securely send to MN before MN's reachability at new c/o address verified
Standard Mobile IPv6

Mobile Node

- Binding Update
- Home Test

Home Agent

- Binding Ack
- Home Test Init
- Home Test

Correspondent Node

- Correspondent registration
- Care-of Test Init
- Care-of Test
- Binding Update
- Binding Ack

Authenticated w/both tokens

Include tokens

Link-layer handoff

Return-routability procedure
Standard Mobile IPv6

Institute of Telematics
Universität Karlsruhe (TH)
www.tm.uka.de

Christian Vogt, chvogt@tm.uka.de
65th IETF/IRTF, Dallas, TX, Mobopts Research Group, March 21, 2006

Switch to new c/o address

In parallel

Optimistic approach

Home Test
Care-of Test

Binding Update
Binding Ack

Link-layer handoff

Home Test Init
Care-of Test Init

Home Test Init

Binding Update

Correspondent registration

Mobile Node

Home Agent

Correspondent Node

3 RTT

4 RTT

Switch to new c/o address

Return-to-reliability procedure
Mobile IPv6 + Early Binding Updates

- **Home Test (Init) exchange** prior to handoff
- **Home and correspondent registration** simultaneously
- **Tentative registration of new c/o address** without c/o test
- **Deferred full registration of new c/o address**
- **Care-of Test (Init) exchange** in parallel with data
Mobile IPv6 + Early Binding Updates

Mobile Node -> Home Agent -> Correspondent Node

1 RTT
switch to new c/o address

proactive home-address test
Home Test Init
Home Test

link-layer handoff
Care-of Test Init
Binding Ack
Early Binding Ack
Care-of Test
Binding Ack

concurrent care-of-address test
Binding Update
Early Binding Update
Binding Update
However...

CN sends packets to unverified location
period of vulnerability
requires additional protection

care-of address
unverified

Mobile Node

proactive home-address test
Home Test Init
Home Test
link-layer handoff

Home Agent

Binding Update
Early Binding Update
Care-of Test Init
Home Test Init
Home Test

Correspondent Node

Binding Ack
Early Binding Ack
Care-of Test
Binding Ack

concurrent care-of-address test

Christian Vogt, chvogt@tm.uka.de
65th IETF/IRTF, Dallas, TX, Mobopts Research Group, March 21, 2006
Why This Is An Issue

Attacker could…

- establish a higher-layer connection (e.g., download)
- redirect packets to victim
- spoof TCP acknowledgments

Amplification!

- CN generates large data packets
- Attacker sends small ACKs

Without amplification…

- Flooding no more effective than direct flooding
- Direct flooding always possible
...and How It Can Be Solved

Idea
- Limit packets sent to unverified c/o address so as to not cause amplification

Solution
- Count the bytes received from MN/attacker
- Send no more bytes to unverified c/o address

Credit-Based Authorization
- Byte counter == "Credit account"
Credit-Based Authorization

Mobile Node

- Acquires credit by sending pkts.
- Consumes credit for being sent pkts. to unverified addr.

Correspondent Node

- Maintains credit account
Credit-Based Authorization

Mobile Node

Correspondent Node
Credit-Based Authorization

Mobile Node

Correspondent Node
Credit-Based Authorization

Mobile Node

Correspondent Node
Credit-Based Authorization

Mobile Node

Correspondent Node

Credit-Based Authorization
Credit-Based Authorization

Mobile Node

Correspondent Node

15

Christian Vogt, chvogt@tm.uka.de
65th IETF/IRTF, Dallas, TX, Mobopts Research Group, March 21, 2006
Credit-Based Authorization

Mobile Node

Correspondent Node

[Diagram showing communication between a Mobile Node and a Correspondent Node with arrows indicating data flow]
Credit-Based Authorization
Credit-Based Authorization

Mobile Node

Correspondent Node

c/o address
unverified

Christian Vogt, chvogt@tm.uka.de
65th IETF/IRTF, Dallas, TX, Mobopts Research Group, March 21, 2006
Credit-Based Authorization

Mobile Node

c/o address
unverified

Correspondent Node
Credit-Based Authorization

Mobile Node

c/o address unverified

Correspondent Node

Node

65th IETF/IRTF, Dallas, TX, Mobopts Research Group, March 21, 2006
Credit-Based Authorization

Mobile Node

Correspondent Node

c/o address unverified
Credit-Based Authorization

Mobile Node

Correspondent Node

c/o address unverified

X

Christian Vogt, chvogt@tm.uka.de
65th IETF/IRTF, Dallas, TX, Mobopts Research Group, March 21, 2006
Credit-Based Authorization

Mobile Node

c/o address
unverified

Correspondent Node
Credit-Based Authorization
However…

Credit account allows an attacker to…

- accumulate credit over a long time
- at a slow rate, and
- use this credit all at once

Facilitates large burst of packets from attackers with low-bandwidth Internet access

Credit aging prevents this
Credit Aging

exponential aging

CN learns new c/o address

new c/o address becomes verified

new c/o address

unverified

time

credit
Experimental Evaluation

- Handoff delays w/IP telephony
- Handoff delays w/TCP file transfers
- Throughput of TCP file transfers
- Analysis of TCP benefits
IP Telephony: Parameters

Application
- 64 kbps payload
- 10ms chunks
- 164B per packet (IPv6, extensions, UDP, RTP)
- bidirectional

Network
- 200ms round-trip time

Mobility protocols
- standard (conservative) Mobile IPv6
- optimistic Mobile IPv6
- w/Early Binding Updates and Credit-Based Authorization

Confidence
- 500 handoffs per mobility protocol
Institute of Telematics
Universität Karlsruhe (TH)

29
Christian Vogt, chvogt@tm.uka.de
65th IETF/IRTF, Dallas, TX, Mobopts Research Group, March 21, 2006

Handoff Delay w/IP Telephony

RTT == 200 ms

occurrence fraction

0.25
0.2
0.15
0.1
0.05
0

0 0.2 0.4 0.6 0.8 1
handoff latency (s)

1 RTT + ε
3 RTT + ε
4 RTT + ε

ebu/cba
optim
conserv
TCP File Downloads: Parameters

Application
- 60s download (chargen-generated data)
- 1024 kbps bandwidth
- unidirektional
- TCP Reno

Network
- 40ms to 200ms round-trip time

Mobility protocols
- standard (conservative) Mobile IPv6
- optimistic Mobile IPv6
- w/Early Binding Updates and Credit-Based Authorization

Confidence
- 20 experiments per mobility protocol per round-trip time
- 5 handoffs per experiment
Handoff Delay w/TCP File Transfers

- conserv
- optim
- ebu/cba

handoff latency (s) vs. round-trip time (ms)

40 80 120 160 200
Throughput w/TCP File Transfers

Why does TCP benefit so much?
Why TCP Benefits So Much

1st timeout → new c/o address

1st timeout → old c/o address
2nd timeout → new c/o address
TCP behavior after 1st timeout
- set cwnd = 1
- set ssthresh = flightsize
- do Slow Start until cwnd > ssthresh

TCP behavior after 2nd timeout
- set cwnd = 1
- set ssthresh = 2 (minimum)
- effectively skip Slow Start
New Drafts

draft-vogt-mobopts-simple-ebu-00.txt
- includes diff's to RFC 3775
- specifies support for proactive handoffs
- no IANA requirements

draft-vogt-mobopts-simple-cba-00.txt
- transparent to MN
- no signaling
- no IANA requirements
Early BU == BU where
  - Kbm == SHA1(home keygen token)
  - Care-of Nonce Index == 0

Early BA accordingly

CN w/EBA support
  - checks Nonce Indices option
    - Care-of Nonce Index == 0 ? ⇒ early Binding Update
    - Care-of Nonce Index != 0 ? ⇒ standard Binding Update

CN w/o EBU support
  - sends BA w/status 137, "Expired care-of nonce index" or
  - sends no BA due to Authentication failure

MN sets Acknowledge flag in early BU
Conclusion

Advantages of EBU/CBA
- Reduce handoff delays to 0~1 RTT (L3 only)
- Better accommodate TCP's retransmission algorithm
- No special network support required
- Applicable to inter-domain handovers

Drawbacks of EBU
- Additional signaling, especially for proactive home-address tests if done periodically
- Still 1 RTT latency for reactive handoffs
- Still 0~1 RTT latency for proactive handoffs
Acknowledgment

Many thanks to my students for their eager and reliable co-operation:

- Ralf Beck
- Daniel Jungbluth
- Max Laier