Towards Efficient Route Optimization: Applying Cryptographically Generated Addresses and Credit-Based Authorization

Christian Vogt, Jari Arkko, Wassim Haddad
chvogt@tm.uka.de, jari.arkko@ericsson.com, wassim.haddad@ericsson.com

Overview and discussion on draft-arkko-mipshop-cga-cba-01.txt

63th Meeting of the Internet Engineering Task Force
Mipshop Working Group Session, August 2, 2005

Goals for Improving RO

Authentication

- Make it more secure and faster, but still infrastructure-less

CoA tests

- Avoid their delays by doing them concurrently

Mailing-list discussions and reviews

- Incorporate lessons learned

Improved RO Protocol

"Ingredients"

- CGAs for secure, fast, and infrastructure-less authentication

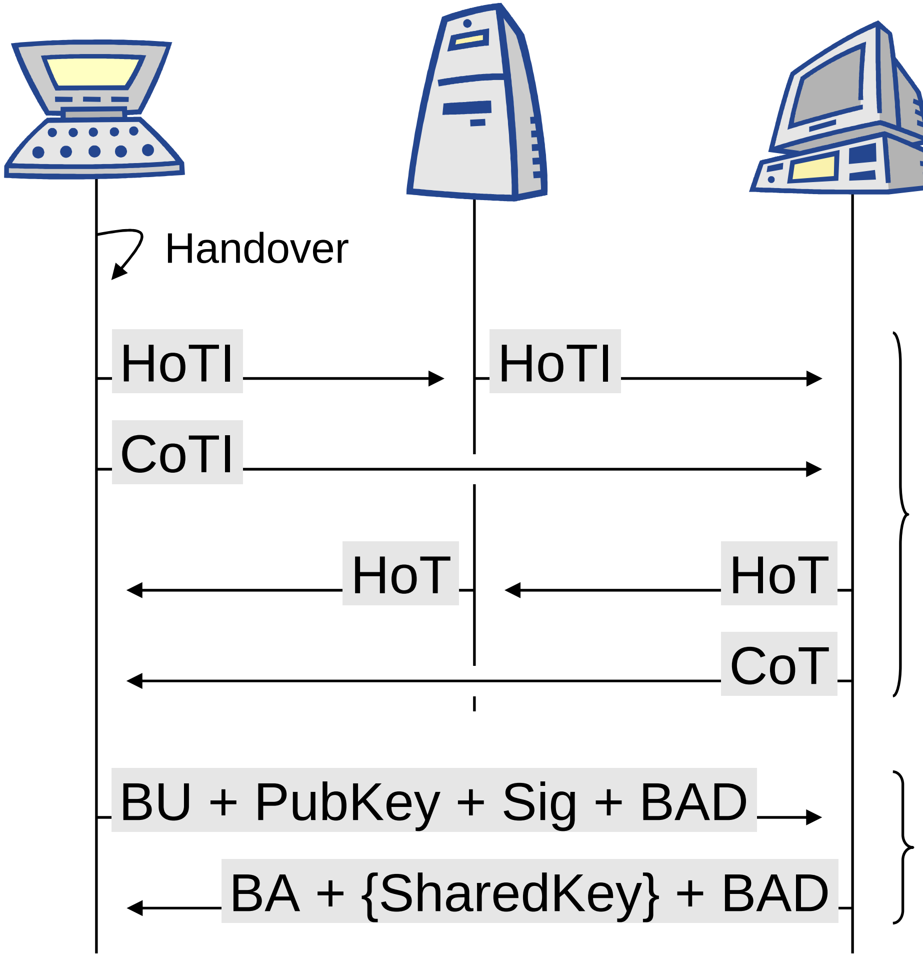
  Originally applied to MIPv6 in draft-haddad-mip6-cga-omipv6-04.txt

- Credit-Based Authorization for concurrent CoA tests

  Originally proposed in draft-vogt-mobopts-credit-based-authorization-00.txt

How the Protocol Bootstraps

The Initial Exchange



Handover

HoTI

HoTI

CoTI

HoT

HoT

CoT

BU + PubKey + Sig + BAD

BA + {SharedKey} + BAD

Standard Return Routability
Standard KBM

Standard BAD
Verify HoA (CGA)
Establish shared key

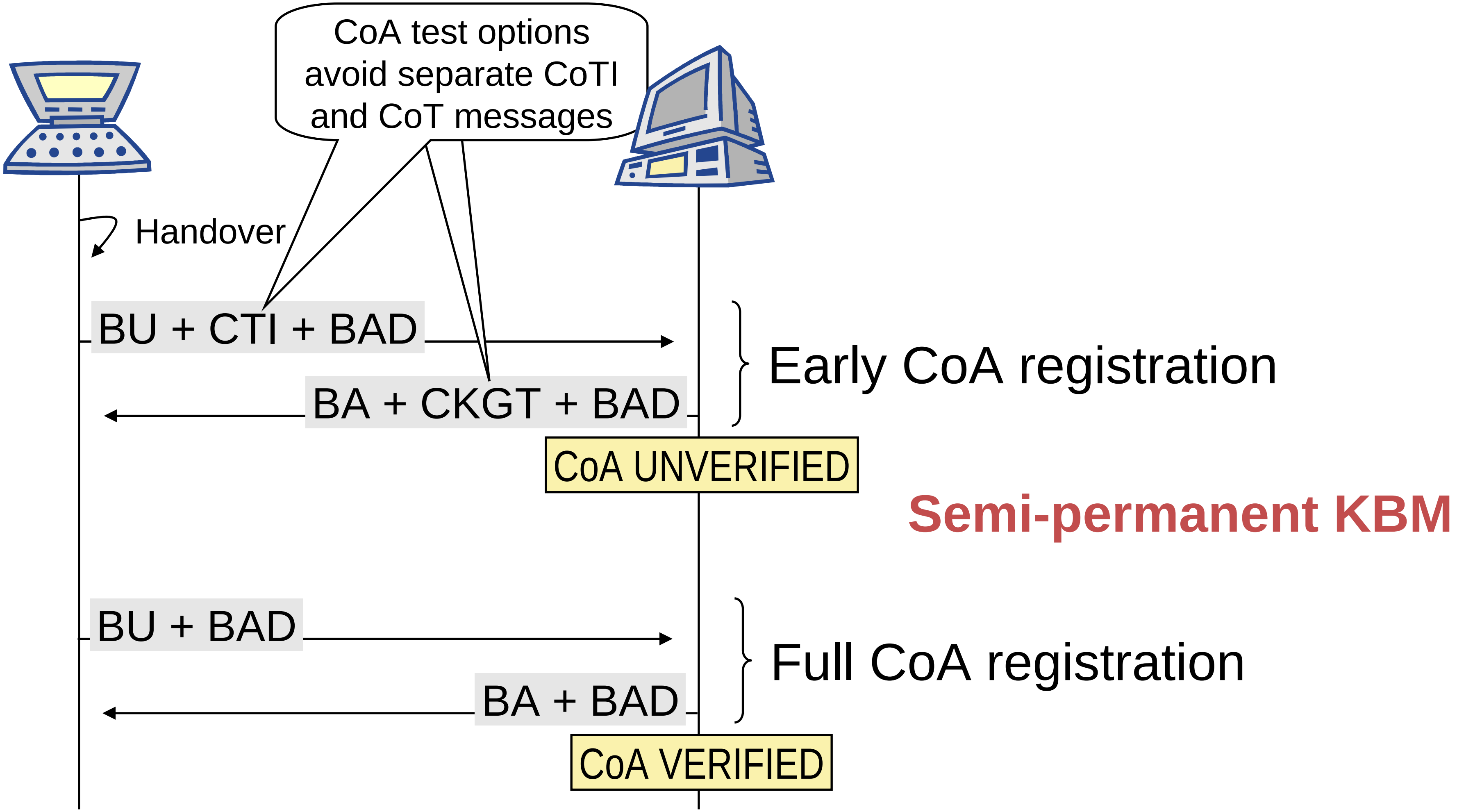
Not shown: extended sequence numbers

After the initial exchange…

…the peers have established...

- Standard binding-cache entry with extended lifetime (up to 24 hours)
- Extended sequence number (good for a period of 24 hours)
- Semi-permanent security association (valid for up to 24 hours)

How Subsequent Exchanges Look Like



CoA test options avoid separate CoTI and CoT messages

Handover

BU + CTI + BAD

BA + CKGT + BAD

Early CoA registration

CoA UNVERIFIED

Semi-permanent KBM

BU + BAD

BA + BAD

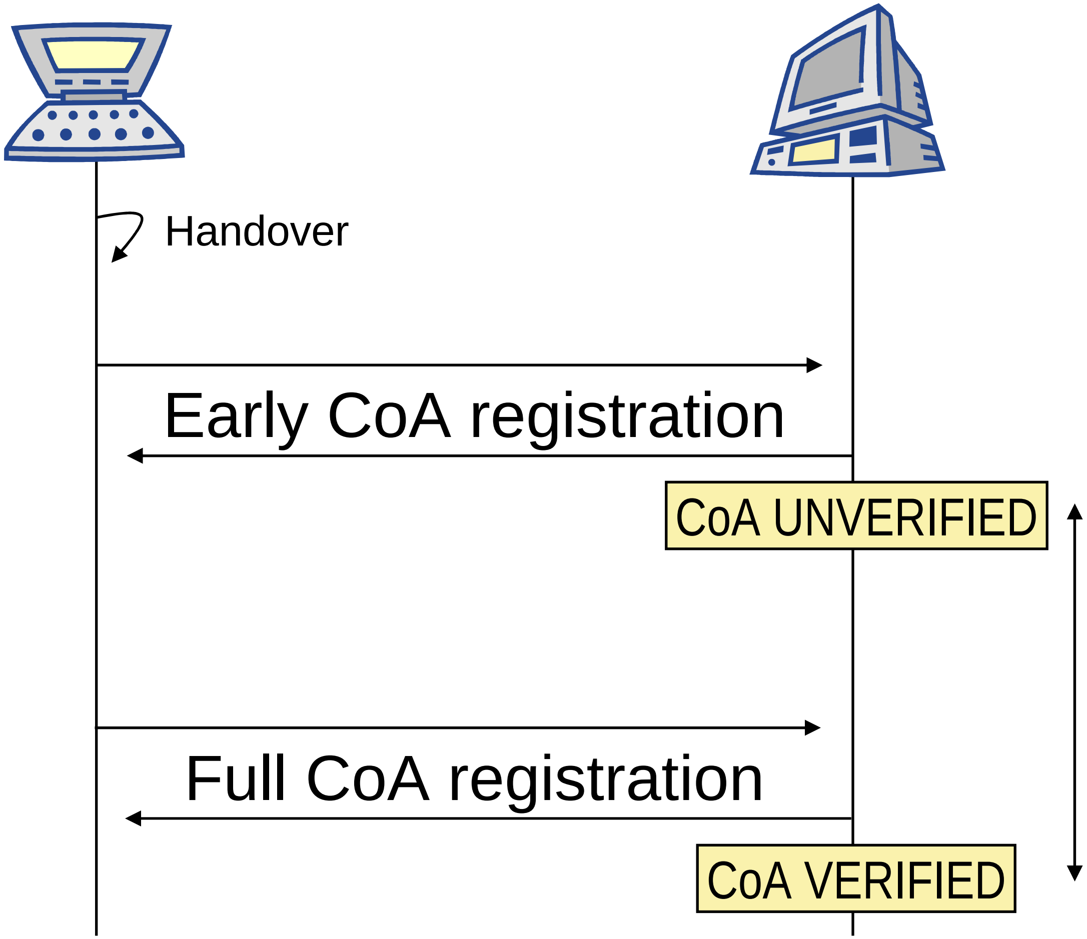
Full CoA registration

CoA VERIFIED

Not shown: extended sequence numbers

Handling Payload Packets

Where Credit-Based Auth. Comes Into Play



Use new CoA,
but limit traffic
from CN to new CoA
during this period

Lessons Learned From ML and Reviews

- Replaced temporary tunneling of packets through HA during handover by sending them directly to CoA or dropping them, depending on credit
- Some folks not convinced of CBA because description was confusion
    - Rewrite according to draft-iab-model-03.txt
- Independence from HA eliminates single point of failure
- Integrated CoA test into registration messages, using CTI and CKGT options, to reduce signaling overhead
    - Useful for other RO protocols, too, once IANA numbers assigned?
- Moved from initial three-message handshake to four-message one: one message more, but no longer vulnerable to reflection and amplification

Comments, questions, concerns?

What is good, where did we go too far?