Credit-Based Authorization

⟨draft-vogt-mipv6-credit-based-authorization⟩

Christian Vogt, chvogt@tm.uka.de

Jari Arkko, jari.arkko@nomadiclab.com

Roland Bless, bless@tm.uka.de

Mark Doll, doll@tm.uka.de

Tobias Küfner, kuefner@tm.uka.de

MIP6 Meeting, 60th IETF Meeting, San Diego

August 3, 2004

This document contains annotations for each presentation slide.

Motivation

Base Mobile IPv6 Correspondent Registration

- 2 RTT global signaling

Optimizations include…

- HMIPv6: Manage mobility locally
- FMIPv6: Move global signaling off critical path (through packet forwarding)
- CGA-OMIPv6: Replace HoA test by CGA authentication
- Early Binding Updates: Proactive HoA test, **concurrent CoA test**

Motivation, Annotations

A correspondent registration in standard Mobile IPv6 takes two round-trip times of global signaling. This can be an issue for applications with rigid delay requirements.

There are several optimizations that seek to minimize the delay of a correspondent registration. Amongst those are the following.

HMIPv6 and FMIPv6 are local optimizations. They require support in the access network. HMIPv6 handles mobility locally, thereby eliminating most of the global signaling. FMIPv6 moves global signaling to a time period where it does not delay communications by using local tunnels.

CGA-OMIPv6 and Early Binding Updates [1] are end-to-end approaches. They do not require support in the access network. CGA-OMIPv6 replaces the potentially long home-address test with fast and secure CGA authentication. Early Binding Updates eliminate the latency of the return-routability procedure. They do a proactive home-address test before the handover and a concurrent care-of-address test in parallel with data transfer to and from the probed care-of address.

[1] Christian Vogt, Roland Bless, Mark Doll, Tobias Küfner: "Early Binding Updates for Mobile IPv6", draft-vogt-mip6-early-binding-updates

Motivation (2)

Concurrent CoA test: **CoA** is **used though unconfirmed** for a while

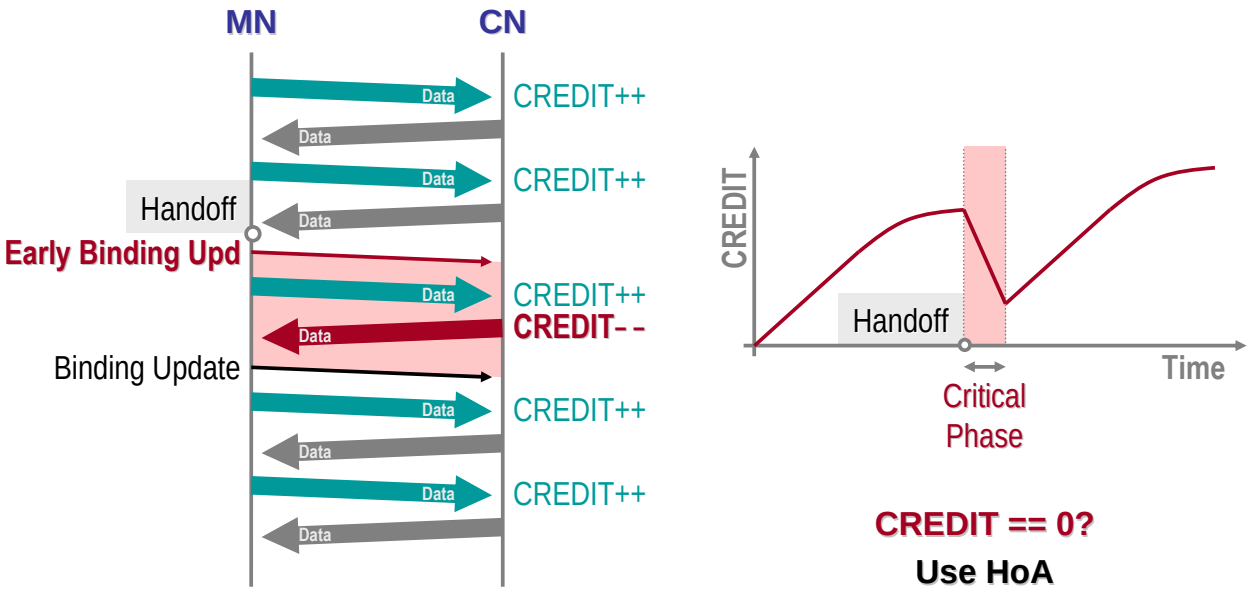
- Discussion on the ML
- **Amplified flooding** attacks are possible threat
- **Prevent misuse** of unconfirmed CoAs
- Credit-Based Authorization as **protection**

Motivation (2), Annotations

There was a long discussion on the mailing list whether the concurrent care-of-address test introduces new security threats. Indeed, we have a new phase of uncertainty, during which the correspondent node doesn't yet know whether or not the mobile node is actually present at the new care-of address. Let's call the new care-of address *unconfirmed* during this phase, and let's call it *confirmed* thereafter.

Some people, including us, feel that using an unconfirmed care-of address can introduce the threat of amplified flooding attacks. We took this as a motivation to develop Credit-Based Authorization, a mechanism that proactively prevents misuse of unconfirmed care-of addresses.

Credit-Based Authorization



Amplified flooding impossible.
Non-amplified flooding discouraged.

Credit-Based Authorization, Annotations

Credit-Based Authorization [2] weighs up the data volume that the correspondent node sends to a mobile node's unconfirmed care-of address and the data volume that this mobile node has previously sent to the correspondent node. Thereby, the correspondent node will never send more data to an unconfirmed care-of address than it has previously received from the mobile node. This eliminates the threat of amplified flooding attacks.

More specifically, the correspondent node maintains a *credit account* for each mobile node it communicates with. When the correspondent node receives a packet from a particular mobile node, the correspondent node gives the mobile node a credit amount equal to the size of the received packet.

When the correspondent node sends a packet to the mobile node, if the mobile node's care-of address is unconfirmed, the correspondent node charges a credit amount proportional to the size of the to-be-sent packet. The amount of charged credit equals the packet size multiplied by some factor X > 1.0. This factor X ensures that the mobile node's credit shrinks faster than it grows.

What happens when the mobile node's care-of address is unconfirmed and no credit is left? In this case, the correspondent node sends packets to the mobile node's home address instead of sending them to the care-of address. Recall that, with Early Binding Updates, the home address is authenticated at all times. Sending packets to the home address is therefore legitimate, regardless of whether the care-of address is unconfirmed or confirmed. The correspondent node will continue to accept packets that the mobile node sends from its care-of address during this time.

When the mobile node's care-of address becomes confirmed, packets for the mobile node will again be sent to the care-of address.

[2] Christian Vogt, Jari Arkko, Roland Bless, Mark Doll, Tobias Küfner: "Credit-Based Authorization for Mobile IPv6 Early Binding Updates", draft-vogt-mipv6-credit-based-authorization

Analysis & Summary

- Make **concurrent CoA test** feasible
  - Reduce registration latency by **50%**
- **End-to-end** optimization
  - No access-network support required
  - Support for inter-domain handovers
- **Transparent** to MN
- Increased **complexity** at CN: **Implementation** will show results
- Applicable to **other** RR **optimizations** (e.g., OMIPv6, Pre-conf. KBMs w/ CoA test)
- Draft investigates **more adaptive** CBA variant
  - More feedback required
  - draft-vogt-mipv6-credit-based-authorization

Analysis & Summary, Annotations

What benefits in terms of efficiency do we get from Credit-Based Authorization? Credit-Based Authorization prevents misuse of unconfirmed care-of addresses. This can reduce the latency of a Mobile IPv6 correspondent registration from two round-trip times to one round-trip time.

Early Binding Updates, combined with Credit-Based Authorization, is an end-to-end optimization. There are two advantages of end-to-end optimizations over local approaches like HMIPv6 and FMIPv6: First, end-to-end optimizations do not require infrastructure in the access network. Second, they are not restricted to intra-domain handovers, but also work for cross-domain handovers.

Credit-Based Authorization is transparent to the mobile node. However, it entails an increased complexity at the correspondent node. There is the related question of how complex Credit-Based Authorization is to implement. To gain practical experience, we are currently in the process of implementing Credit-Based Authorization. A very basic implementation of Early Binding Updates, without Credit-Based Authorization, is already finished.

Credit-Based Authorization not only applies to Early Binding Updates. It can be useful for any return-routability optimization that does not omit the care-of-address test. CGA-OMIPv6, or a combination of pre-configured binding-management keys with care-of-address tests, are two examples where Credit-Based Authorization could yield further performance gains.

Draft-vogt-mipv6-credit-based-authorization discusses a variant of Credit-Based Authorization which is more adaptive to applications with asymmetric traffic patterns. This variant has different security properties. More feedback from the research community is required to settle on the level of security that is actually desired.