Autonome Zertifizierung mobiler Multicast-Sender — AuthoCast —

Hochschule für Angewandte Wissenschaften Hamburg
Hamburg University of Applied Sciences

Thomas C. Schmidt, Olaf Christ und Matthias Wählisch

Department Informatik, HAW Hamburg & link-lab, Berlin

link-lab

Einleitung

Diverse Protokollvorschläge zur Unterstützung von mobilen Multicast Quellen existieren heute [1]. Bisher weist keines der verschiedenen adaptiven Verfahren eine Sicherung gegen die missbräuchliche Nutzung etablierter Verteilbäume, etwa für DDoS–Attacken, auf. AuthoCast authentifiziert Multicast Sender in ASM wie SSM Szenarien kryptographisch stark und leichtgewichtig an der Routing-Infrastruktur und den Empfängern.

Hintergrund: CGAs

Kryptographisch generierte Adressen (CGAs) [2] erlauben erstmalig, dass sich IPv6-Pakete selbstkonsistent authentifizieren. Sie lösen das *Proof-of-Ownership*-Problem ohne Sicherheitsinfrastruktur, z.B. PKI:

- IP-Adresse entsteht aus Public Key
- Sender signiert Paket mit Private Key
- Public Key und Signatur werden mit Datenpaket verschickt

Die Komplexität zum Erzeugen einer CGA ist parametrisierbar und steigt exponentiell.

AuthoCast-Protokollübersicht

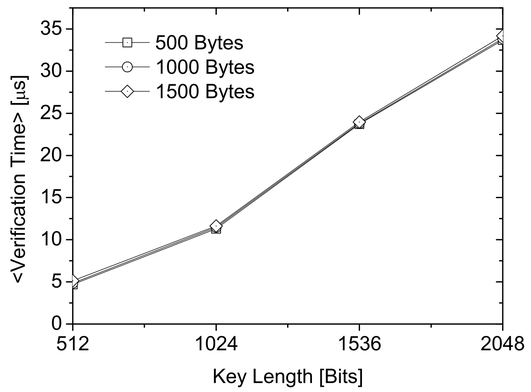
Konzept

AuthoCast [3] erzielt eine Authentifizierung mittels CGAs. Die Router-Verteilzustände werden um (CoA, HoA, G) erweitert. Das Protokoll folgt den Prinzipien:

- Verwendung bestehender Informationen
- Nutzung existierender Paketköpfe

IPv6 Header	Hop-by-Hop Options Header	Dest. Options Header	Mobility Header			Upper Layer Header + Data
Src: CoA Dst: G	Router Alert Option	Home Address Option	Binding Update Message	CGA Param. Option	CGA Signature Option	Data

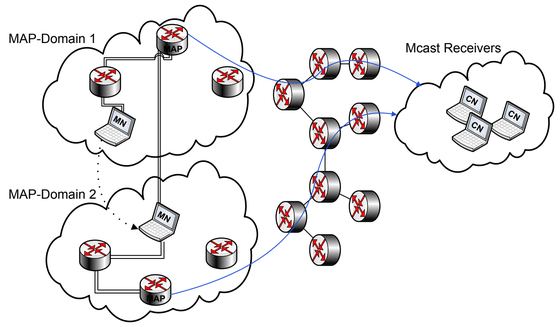
Evaluation



Prozessierungszeit für die CGA-Signaturverifikation auf 2.4 GHz AMD Athlon

Ablauf

- Home Adresse wird als CGA erzeugt
- Mobile SSM-Quelle sendet Nutzdaten und State Update nach Adresswechsel an vorherige Baumwurzel
- Mobility Agents analysieren State Update basierend auf Router Alert Option
- Durchführung der CGA-Verifikation
- Negative Überprüfung verwirft das Paket und baut kein Multicast-State auf
- Positive Überprüfung leitet das Paket bis zum Empfänger für das BU weiter



Marktchancen

Durch seine standardkonforme und skalierbare Architektur hat AuthoCast realistische und gute Marktchancen:

- Software-Router: vertretbarer zusätzlicher Prozessierungsaufwand
- Hardware-Router: Kryptoprozessoren *direkt* auf Linecards implementierbar
- Kombinierbare Algorithmik mit SEND
- Nahtlose Integration in bestehendes IPv6-Mobilitätsmanagement

Literatur

[1] T. C. Schmidt, M. Wählisch, and G. Fairhurst, "Multicast Mobility in MIPv6: Problem Statement and Brief Survey," MobOpts, IRTF Internet Draft 04, July 2008.

[2] T. Aura, "Cryptographically Generated Addresses (CGA)," IETF, RFC 3972, March 2005.

[3] T. C. Schmidt, M. Wählisch, and O. Christ, "AuthoCast – A Protocol for Mobile Multicast Sender Authentication," in *Proc. of MoMM 2008*. ACM, November 2008.

Kontakt: Thomas C. Schmidt, Matthias Wählisch, HAW Hamburg, Dept. Informatik, Berliner Tor 7, D-20099 Hamburg – Email: {*t.schmidt, waehlisch*}*@ieee.org*
Die vorgestellte Arbeit wurde durch das Bundesministerium für Bildung unf Forschung im Projekt *Moviecast* (http://moviecast.realmv6.org) gefördert.