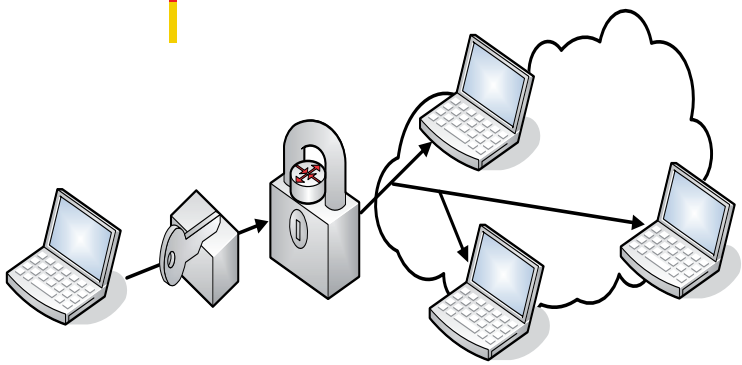
Hochschule für Angewandte Wissenschaften Hamburg
Hamburg University of Applied Sciences

Prof. Dr. Thomas Schmidt
HAW Hamburg, Dept. Informatik
Berliner Tor 7, D-20099 Hamburg
schmidt@informatik.haw-hamburg.de

GEFÖRDERT VOM
Bundesministerium
für Bildung
und Forschung



AuthoCast - Autonome Zertifizierung mobiler Multicast-Sender

Angetrieben durch die wachsende Marktdurchdringung von Infotainment-Angeboten wie IPTV gewinnen Gruppenkommunikationsdienste stark an praktischer Bedeutung. Multicast bietet hierfür eine effiziente Möglichkeit der Datenverteilung. Komplementär dazu entsteht ein ubiquitäres, mobilitätstransparentes Internet der nächsten Generation.

Ziel von AuthoCast ist die skalierbare und kryptographisch starke Authentifizierung von mobilen Multicast-Quellen auf der Basis bestehender Standards mit Blick auf ein realistisches Deployment. AuthoCast schützt auf einfache Weise, Multicast-Anwender und Infrastrukturen vor Mißbrauch und Angriffen.

Diverse Protokollvorschläge zur Mobilitätsunterstützung von Multicast-Quellen existieren derzeit. Bisher weist aber keines der Routing-Verfahren eine Sicherung gegen die missbräuchliche Nutzung etablierter Verteilbäume, etwa für DDoS-Attacken, auf.

AuthoCast authentifiziert unaufwändig Multicast-Sender gegenüber Empfängern und Routern mithilfe von standardisierten CGAs. Das entwickelte Protokoll benötigt keinen Rückkanal und minimiert den Nachrichtenaustausch für echtzeitfähige Anwendungsszenarien. AuthoCast wurde für IP- und Overlay-Multicast einschließlich ASM und SSM entworfen.

Weitere Informationen: http://moviecast.realmv6.org/authocast.html

- **Mobile IPv6:** Die Bewegung eines Computers im Internet führt zur Veränderung seiner Adresse. Ähnlich einem Nachsendeantrag regelt Mobile IPv6 die transparente Zustellung.
- **Multicast:** Multicast ist ein Verteilungsmechanismus, der ein *einmal* versandtes Paket im Netz dupliziert und bei *vielen* Gruppenteilnehmern ankommen lässt.
- **SSM:** Source Specific Multicast
- **ASM:** Any Source Multicast
- **DDoS:** Distributed Denial of Service Attacken versuchen Rechner verteilt anzugreifen. Im Kontext von Multicast ist dies einfacher, da mit dem Senden eines Datenpakets mehrere Empfänger parallel erreicht werden können.
- **CGA:** Kryptographisch generierte Adressen (CGAs) erlauben erstmalig, dass sich IPv6-Pakete selbstkonsistent authentifizieren. Sie lösen das *Proof-of-Ownership*-Problem ohne dedizierte Infrastruktur (PKI). Ein Knoten beweist den Besitz einer IP-Adresse, indem er sie aus seinem Public Key ableitet und das Datenpaket mit dem zughörigen Private Key signiert. Der Empfänger verifiziert eine CGA über die mitgeschickte Signatur und den Public Key.

Hochschule für Angewandte Wissenschaften Hamburg
Hamburg University of Applied Sciences

REALMv6 - Real-Time und Multicast Mobilität in IPv6

Noch eine Vision - aber überall in der Implementierung ist IPv6 als allgegenwärtiges, vorherrschendes Protokoll, welches mobile und drahtlose Geräte genauso in einem transparenten, globalen Netz vereint, wie heutige Desktops. Die kooperative Forschungsinitiative REALMv6 hat zum Ziel, gemeinsam mit ihren internationalen Partnern Algorithmen und Protokolle zur echtzeitfähigen mobilen Unicast- und Multicastkommunikation zu entwicken, in Simulationen und Testbeds zu analysieren und optimieren und ihre offene Standardisierung und Verbreitung zu befördern.

Das Internet der nächsten Generation basiert auf dem Protokoll IPv6. IPv6 verfügt über eine umfassende Mobilitätsunterstützung. Darüber hinaus bietet das Protokollumfeld weitreichende Leistungspotentiale zur Echtzeitfähigkeit, Sicherheit und der Entwicklung neuer Kommunikationsfunktionen. Eine besondere Herausforderung besteht in der Gestaltung und Verbreitung mobiler Multicast-Dienste.

REALMv6 ist eine offene Plattform für Forschungsgruppen und Hersteller, gerichtet auf den Wissens- und Erfahrungsaustausch, die Kooperation in Entwicklung und Tests sowie die Vorbereitung auf gemeinsame Projekte.

Weitere Informationen: http://www.realmv6.org

link-lab

NAPIER UNIVERSITY
EDINBURGH SCOTLAND

fhtw
Fachhochschule für Technik
und Wirtschaft Berlin
University of Applied Sciences

daviko