Technische Universität München
Lehrstuhl für Netzarchitekturen und Netzdienste
Prof. Dr. Georg Carle

3.11.2008

Diplomarbeit Feb 2009

Blaz Primc

Authentisierende Adressierung in Netzen

Motivation

Im häuslichen Kontext finden sich zunehmend Geräte, deren Nutzwert durch geeignete Vernetzung beträchtlich gesteigert werden kann (Rolladensteuerung, Heizung, Kühlschrank, …).

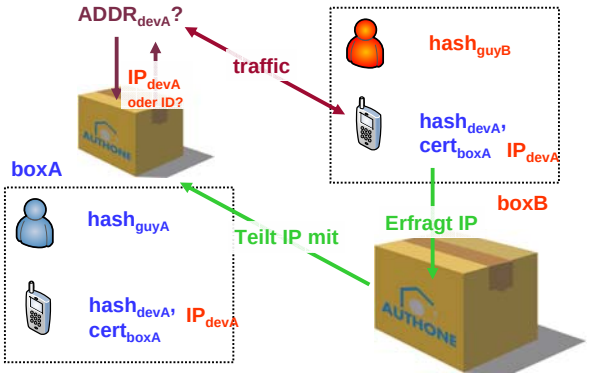
In (Heim-)netzen gibt es verschiedene Entitäten, die logisch angesprochen werden sollen (toaster1@meinZuhause). Gleichzeitig sollen diese Entitäten aufgrund ihrer authentisierten Identität Rechte eingeräumt bekommen können. Dies soll in der (Heim-)umgebung sowie in befreundeten Umgebungen erfolgen können („ich besuche einen Freund und darf seinen Drucker verwenden“).

Aufgabenstellung

In dieser Arbeit soll eine lauffähige Umgebung geschaffen werden, die eine Adressierung anhand von hierarchisch geordneten öffentlichen Schlüsseln (Public Keys) erlaubt. Die Implementierung eines geeigneten Adressierungsschemas auf Basis der kryptografischen Schlüssel ermöglicht dabei eine eindeutige Identifikation (Authentisierung).

Die Arbeit gliedert sich zunächst in die folgenden drei Teile:

1. Herstellen von Vertrauensbeziehungen durch ein geeignetes Schlüsselaustauschverfahren („Home-Zertifikate austauschen“)
2. Realisierung eines Addresslookup innerhalb eines Heimkontextes („me ist innerhalb myHome erreichbar unter 2001:4ca0:2001::1“)
3. Realisierung einer funktionierenden Adressierung über den Heimkontext hinaus (bspw. Haus eines Freundes) („me@myHome ist erreichbar unter 2001:4ca7:1042::23“)



Dabei sollen geeignete Standardalgorithmen und Verfahren zum Einsatz kommen, die ebenfalls bezüglich ihrer Eignung untersucht werden sollen.

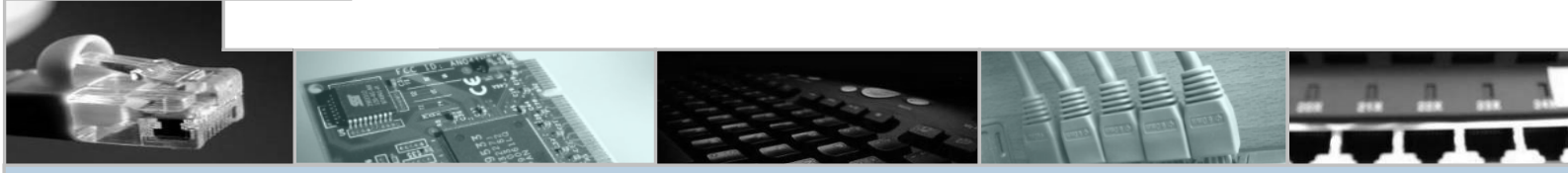
Wichtige Ziel der Arbeit ist eine lauffähige Demo am Ende, bei der sowohl Geräte angesprochen werden können als auch deren Mobilität unterstützt wird („mit PDA zu Freund“). Im Bereich der Mobilität ist eine Erweiterung der Arbeit in Richtung „seamless handover“ denkbar.
Weitere Vertiefungen sind möglich.

Voraussetzungen

Erfahrung in Java.
Spaß an kryptografischen Verfahren und der Implementierung von Protokollen.

Stichworte

Adressierungsschema, address lookup, Protokollentwicklung, Kryptographie



Marc-Oliver Pahl, Andreas Müller, Heiko Niedermayer, Holger Kinkelin
{pahl, mueller, niedermayer, kinkelin}@net.in.tum.de