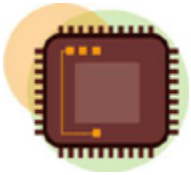
Technische Universität München
Lehrstuhl für Netzarchitekturen und Netzdienste
Prof. Dr. Georg Carle

SEP / Hiwi

Preventing Theft of Cryptographic Identifiers using Trusted Computing Technology

Hintergrund

Kryptographische Identfikatoren (CryptoIDs) werden von RSA-Schlüsseln abgeleitet und finden in Kommunikationsprotokollen bei der authentisierten Identifikation von Entitäten Einsatz. Wird der private Teil des RSA Schlüsselpaars gestolen, ist der Angreifer in der Lage die fremde Identität anzunehmen. Das *Trusted Platform Module* (TPM) ist ein kryptographischer Chip, der unter anderem RSA Schlüssel generieren, speichern und für die Signatur von Daten verwenden kann. All diese Aktionen finden in einer von Software-Angriffen abgeschirmten Umgebung statt. Ein TPM kann somit als Speicher des zu einer CryptoID gehörigen privaten Schlüssels dienen und verhindert wirkungsvoll Identitätsdiebstahl durch Malware.



Aufgaben-beschreibung

Im Projekt **AutHoNe** (Autonomic Home Networking, www.authone.de/) werden moderne Heimnetzwerke untersucht. Ein solches Heimnetz ist wiederum Teil eines Netzes aus anderen Heimnetzwerken.
Die zentrale Komponente eines Heimnetzes ist das *Home Gateway*, das durch eine CryptoID von außen adressiert und authentisiert werden kann. Das Home Gateway ist unter anderem dafür verantwortlich die Identitäten anderer Geräte im Heimnetz zu beglaubigen. Der Schutz des Schlüsselmaterials des Home Gateways ist somit essentiell für das gesamte Heimnetz.

AUTHONE

Ziel

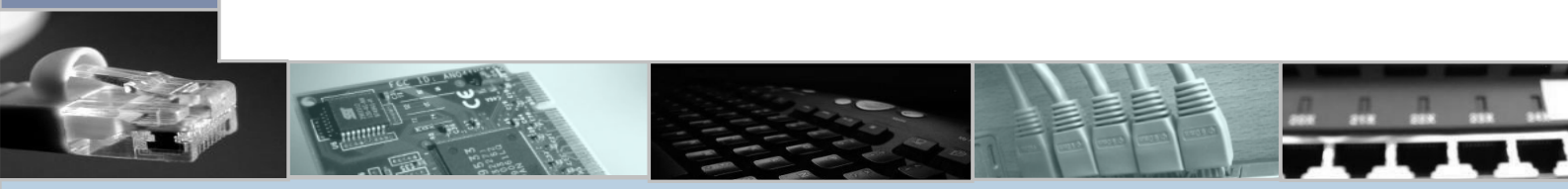
Ziel dieser Arbeit ist die Entwicklung eines Verfahrens zum Schutz der Identität des Home Gateways und der Beweis dieser Sicherheit gegenüber anderen Home Gateways basierend auf Trusted Computing Technologie. Zusätzlich soll ein Protoyp des Verfahrens implementiert werden.

Voraus-setzungen

Programmierkenntnisse in Java, Interesse am Ausprobieren neuer Technologien und an der Arbeit in einem größeren Projektkontext.

Stichworte

Trusted Computing, Trusted Platform Module, Identity Theft, Cryptograpic Identifier



Mehr Infos am Lehrstuhl I8: Netzarchitekturen und Netzdienste
Holger Kinkelin: hk@net.in.tum.de