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

12.09.2008

Diplom-/Masterarbeit
aufteilbar für Bachelor/SEP

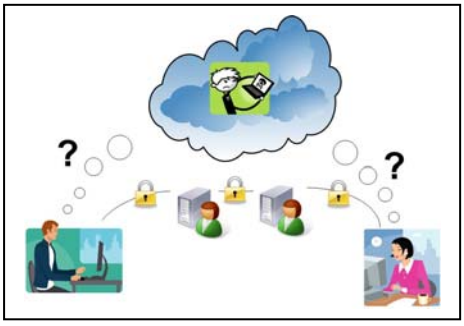
Analyse und Visualisierung der Vertrauensbeziehungen in Web of Trust-Netzwerken

Motivation

Standards wie GPG/PGP oder S/MIME liegt asymmetrische Kryptographie zugrunde. Dies vereinfacht die Schlüsselverteilung, aber es bleibt ein wichtiges Problem: Wie kann sichergestellt werden, dass ein Public Key wirklich zu einem bestimmten Teilnehmer gehört? Public Key Infrastructures (PKIs) sollen eine solche Zuordnung ermöglichen. Die Meinungen bezüglich der besten Variante gehen jedoch weit auseinander. Während die einen zentralisierte Ansätze um eine Certification Authority herum bevorzugen, sprechen sich andere für Vertrauensketten zwischen einzelnen Nutzern aus. Obwohl es viele Analysen zur Struktur solcher Webs of Trust gibt, fehlt bisher jedoch eine qualitative Bewertung. Dies macht es schwierig, die jeweiligen Ansätze zu vergleichen.

Aufgabenstellung

Diese Arbeit soll einen ersten Schritt in Richtung einer qualitativen Aussage zu Vertrauensbeziehungen in PKIs machen. Verwendet werden hierfür Daten aus dem GPG-Web of Trust. Diese werden mittels einer entsprechenden Software analysiert und visualisiert. Daraus soll ein verallgemeinertes Modell abgeleitet werden. Dieses Modell dient dann als Grundlage für die folgende Analyse von Vertrauensbeziehungen mit Hilfe eines Simulators. Es wird ein Szenarienraum untersucht, der über Parameter wie Zahl der Angreifer, Vertrauenswürdigkeit der Signaturen etc. bestimmt ist. Ziel der Arbeit ist es, bessere qualitative Angaben zur Sicherheit von PKIs zu machen.



Wird die Arbeit als BSc-Arbeit durchgeführt, entfällt der letzte Teil. Für ein SEP würde man den Programmierteil zu Lasten der Theorie erweitern.

Geboten wird

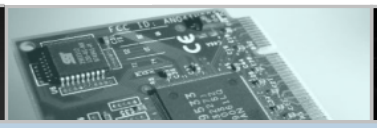
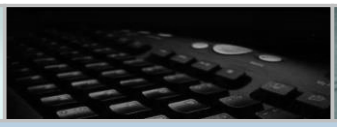
Mitarbeit an spannender Forschung in einem ausgesprochen netten Team. ☺

Voraussetzungen

Engagement und Freude an der Arbeit; Grundkenntnisse in Netzsicherheit; Grundkenntnisse in C++ und/oder Java

Stichworte

Web of Trust, PKI, Zertifikate, Visualisierung

Mehr Informationen am Lehrstuhl für Netzarchitekturen und Netzdienste bei folgenden Personen:

Ralph Holz: holz@net.in.tum.de oder Corinna Schmitt: schmitt@net.in.tum.de