HSR
HOCHSCHULE FÜR TECHNIK
RAPPERSWIL

Kurzfassung der Studienarbeit

Abteilung	**Informatik**
Name der Teammitglieder	**Marc Müller** **Patrick Maurer**
Titel der Studienarbeit	**VoIP Security mit Minisip**
Examinatorin / Examinator	**Prof. Dr. Andreas Steffen**

Kurzfassung der Studienarbeit

Angetrieben durch die steigende Bandbreite der Netzwerke, insbesondere dem Internet und deren freien Kapazitäten, hat in der letzten Zeit Voice over IP (VoIP) stark an Bedeutung gewonnen. Für Privatpersonen ist VoIP eine interessante Technik, um kostengünstige Gespräche über grosse Distanzen zu führen. Für Firmen ist hauptsächlich die zusätzliche Flexibilität ein Grund, um
von einer klassischen Telefonanlage auf VoIP umzusteigen. Ein Endgerät kann an einen beliebigen Netzwerkanschluss angeschlossen werden und erhält immer die gleiche Anschlusskennung.

Durch den Wechsel von der klassischen drahtgebundenen Telefonie zu VoIP fällt ein Teil der bestehenden Sicherheit weg. Es wird kein physischer Zugriff auf die Telefonleitung mehr benötigt, um Gespräche abzuhören. Ein potentieller Angreifer kann das Gespräch an einem beliebigen Punkt zwischen den beiden Gesprächspartnern mithören. Zudem kann einfach eine falsche Identität vorgegeben werden. Dies ist unter anderem ein grosses Hindernis für die effektive Bekämpfung von Spam over Internet Telephony (SPIT).

Als etablierter Standard wird heute in den meisten Fällen das Session Initiation Protocol (SIP) verwendet. SIP ist zusammen mit dem Session Description Protocol (SDP) verantwortlich für den Aufbau der Verbindung und das Aushandeln der nötigen Parameter. SIP und SDP arbeiten beide als textbasierte Protokolle im Klartext und können daher ebenfalls frei eingesehen werden.

Den meisten Anwendern ist diese Problematik nicht bewusst. Deshalb ist es im Interesse aller, dass einfache und effiziente Lösungen für diese Probleme gefunden werden.

Ziel dieser Arbeit ist ein Demonstrator basierend auf dem Minisip-Client. Eine Authentisierung auf der Basis von Zertifikaten war bereits implementiert. Der Einsatz von Zertifikaten bedingt jedoch eine vorhandene Public Key Infrastructure (PKI). Neu ist die Authentisierung mit DomainKeys realisiert. Der Public-Key jedes Benutzers ist in einem TXT-Record auf seinem DNS-Server abgelegt. Somit kann ein Client den Public-Key des Gegenübers per DNS-Abfrage beziehen und es ist keine zusätzliche PKI mehr nötig. Die Signatur der Pakete für den Diffie-Hellman Schlüsseltausch wird dann mit diesem Public-Key verifiziert. Die Sprachdaten werden mit dem ausgehandelten Schlüssel symmetrisch verschlüsselt.