Christian Höhn
Silvan Geser

Advanced Voice-over-IP Security

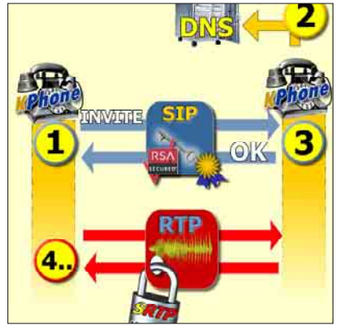
MIKEY-Protokoll für KPhone

Diplomanden	Christian Höhn, Silvan Geser
Examinator	Prof. Dr. Andreas Steffen
Themengebiet	VoIP Verschlüsselung

Aufgabenstellung: Voice-over-IP Telefonie über das Internet mittels des HTTP-basierten Session Initiation Protokolls (SIP) erfreut sich zunehmender Beliebtheit. Meist geschieht dabei aber weder eine Authentisierung der Gesprächspartner, noch eine Verschlüsselung des eigentlichen Gesprächs. Dies obwohl entsprechende sichere Standards wie SIPv2 und Secure RTP zur Verschlüsselung der Multimediaströme vorhanden wären. Die Voice-over-IP Gemeinschaft wird sich in naher Zukunft zudem vermehrt mit dem Problem von lästigen SPIT Anrufen (Spam-Over-Internet-Telephony) konfrontiert sehen.

Um diesen unbefriedigenden Zustand zu verbessern, wurde in einer vorangegangenen Studienarbeit bereits erfolgreich die Secure RTP Funktionalität für den verbreiteten Linux Client Kphone realisiert. So kann das eigentliche Gespräch nun sicher übertragen werden. Der zur Verschlüsselung nötige Master Key muss dabei aber bei beiden Partnern vorgängig manuell eingetragen werden. Diese Variante ist aufwändig, skaliert schlecht und ist bei zu kurz gewählten Schlüsseln potentiell unsicher.

Ziel der Arbeit: Im Rahmen dieser Diplomarbeit soll nun ein automatischer Schlüsselaustausch implementiert werden. Dafür sollen bewährte Protokolle und bewiesenermassen sichere kryptographische Code-Bibliotheken zum Einsatz kommen. Die bereits eingebaute SRTP Gesprächsverschlüsselung soll ohne grosse Anpassungen übernommen werden können. Kphone sollte in der Lage sein, SPIT Anrufe zu erkennen und gegebenenfalls zu ignorieren.
Diese Ziele sollen ohne den Einsatz von X.509 Zertifikaten erreicht werden, da diese immer noch wenig verbreitet sind und es fraglich ist, ob sie sich im grösseren Stil durchsetzen werden.
Unsere Kphone-Erweiterung soll in zukünftige Versionen des Open Source Clients einfliessen und für jedermann verfügbar sein.



VoIP Gespräch mit Verschlüsselung

Lösung: Der automatische Schlüsselaustausch wird mittels des Multimedia-Internet-Keying Protokolls (MIKEY) implementiert. Die Schlüsselinformationen werden mit Hilfe von MIKEY in die für den Gesprächsaufbau zuständigen SIP Pakete eingebettet. Der bewährte RSA-Algorithmus garantiert dabei hohe Übertragungssicherheit für den Austausch der Schlüssel.
Zur Vorbeugung gegen SPIT Attacken soll das für die SPAM Bekämpfung entwickelte Domainkeys Verfahren (DKIM) eingesetzt werden. Beide Gesprächsteilnehmer müssen dazu auf dem eigenen Domain Name Server (DNS) ihre öffentlichen Schlüsselinformationen hinterlegen. Die SIP Anfrage wird vom Anrufer mit Hilfe eines geheimen privaten Schlüssels signiert. Die Überprüfung mit den auf dem DNS Server hinterlegten öffentlichen Schlüssel zeigt dem Angerufenen, ob das Gespräch auch tatsächlich vom Besitzer der im Anruf angegebenen Absenderadresse kommt.
Der öffentliche RSA Schüssel des Angerufenen wird für die Übertragung des geheimen Session Keys verwendet.