Fraunhofer
SIT

FRAUNHOFER-INSTITUT FÜR
SICHERE INFORMATIONSTECHNOLOGIE

SECURE VoIP

VERSCHLÜSSELTE INTERNET-TELEFONIE FÜR HANDELSÜBLICHE MOBILTELEFONE

Fraunhofer-Institut für Sichere Informationstechnologie SIT

Kontakt:
Matthias Ritscher
Rheinstraße 75
64295 Darmstadt

Telefon 06151 869-313
Fax 06151 869-224
matthias.ritscher@sit.fraunhofer.de
www.sit.fraunhofer.de

Mit IP-Telefonie können Unternehmen ihre Telefonkosten erheblich reduzieren. Viele am Markt erhältliche VoIP-Lösungen lassen sich jedoch relativ leicht manipulieren oder belauschen, weil die Sprachinformationen in der Regel nicht verschlüsselt werden. Für drahtgebundene VoIP-Telefonie gibt es deshalb bereits erste Produkte, die eine Verschlüsselung anbieten. Da in Zukunft auch Mobiltelefone VoIP-Telefonie unterstützen sollen, hat das Fraunhofer-Institut SIT eine Software-Lösung entwickelt, die eine verschlüsselte Verbindung zwischen zwei handelsüblichen Mobiltelefonen ermöglicht. Secure VoIP garantiert Ende-zu-Ende-Sicherheit für VoIP-basierte Sprachübertragungen.

Schutz in unsicheren Kontexten

Secure VoIP bietet Ende-zu-Ende-Sicherheit von Sprachkommunikation und benötigt keine spezielle Hardware. Unternehmen können mit der Software sicherheitssensitive Telefongespräche vor unberechtigtem Abhören schützen. Dies ist vor allem notwendig, wenn Datenverbindungen nicht ausreichend gesichert werden, zum Beispiel bei der Nutzung öffentlicher Hot-Spots.

Funktioniert mit fast allen Geräten

Der Prototyp verwendet einen AES-Algorithmus zur Verschlüsselung des Sprachkanals und basiert auf J2ME, einer Programmierplattform, die von zahlreichen Mobiltelefon-Herstellern unterstützt wird. Beim Aufbau einer Sprachverbindung wird zunächst auf sichere Weise ein kryptografischer Schlüssel zwischen den Endgeräten ausgehandelt (Diffie-Hellman-Verfahren). Mit Hilfe dieses geheimen Sitzungsschlüssels sichert die Software anschließend die Sprachübertragung. Die AES-Verschlüsselung mit Hilfe von Secure VoIP funktioniert mit nahezu allen J2ME-fähigen Mobiltelefonen – unabhängig vom Hersteller oder der verwendeten Datenverbindung (WLAN, UMTS oder GPRS).

Sprachqualität

Die Verschlüsselung hat keinerlei Auswirkungen auf die akustische Qualität der Übertragung – Rauschen, Knacken und andere Störgeräusche treten nicht auf. Bei handelsüblichen Mobiltelefonen treten jedoch noch Verzögerungen auf, die eine Echtzeitkommunikation verhindern. Zur ersten Realisierung wurde deshalb eine Push-to-talk-Lösung gewählt. Gleichzeitig arbeitet das Projektteam an einer Portierung auf andere Mobilfunkplattformen wie etwa Symbian, um die Leistungsfähigkeit zukünftiger Endgeräte optimal ausschöpfen zu können. Um die Entwicklungsarbeiten zu beschleunigen, wurde im Rahmen von Secure VoIP ein Werkzeug erstellt, mit dem sich die Leistungsfähigkeit von Mobiltelefonen und deren Eignung für VoIP-Sprachdienste überprüfen lässt.

Wie geht's weiter?

Das Fraunhofer-Institut SIT bietet Herstellern und Anbietern von VoIP-Lösungen Unterstützung bei der Absicherung und Weiterentwicklung bestehender Systeme.

03/2008