Patrick
Maurer

Marc
Müller

Soxy – VoIP Security Proxy Server

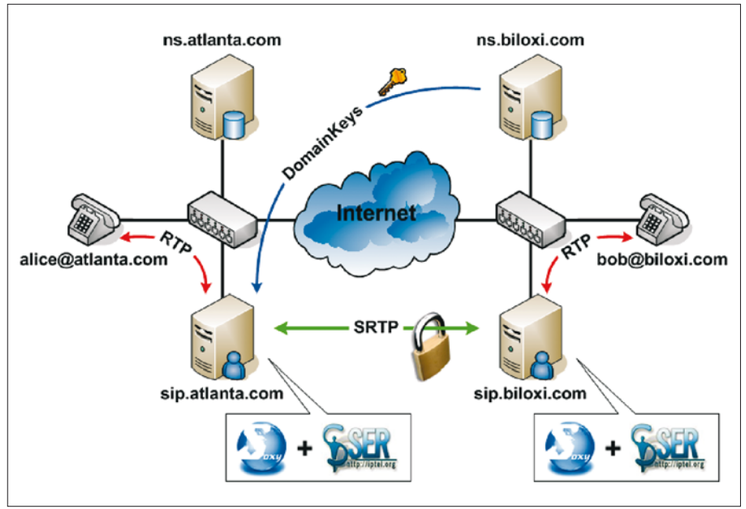
Sicher telefonieren über das Internet

Diplomanden	Patrick Maurer, Marc Müller
Examinator	Prof. Dr. Andreas Steffen
Experte	Dr. Ralf Hauser, PrivaSphere, Zürich
Themengebiet	Internet-Technologien und -Anwendungen

Aufgabenstellung: Viele Voice over IP (VoIP) Hardware-Telefone oder Softphones unterstützen entweder überhaupt keine Sicherheitsmechanismen oder die von den verschiedenen Herstellern implementierten Sicherheitsprotokolle sind nicht kompatibel zueinander. Ohne Authentifizierung und Verschlüsselung kann jedoch die Identität des Kommunikationspartners nicht festgestellt werden und es besteht das Risiko, dass die Gespräche abgehört werden können.

Ziel der Arbeit: Im Rahmen dieser Diplomarbeit soll ein VoIP Security Proxy Server konzipiert und realisiert werden, der als «Bump-in-the-Line» automatisch die Verschlüsselung der RTP-Multimediapakete mittels des Secure RTP Verfahrens vornimmt. Der Schlüsselaustausch sowie die Authentisierung der Kommunikationspartner sollen im Rahmen des SIP Verbindungsaufbaus ebenfalls automatisch auf der Basis des Multimedia Internet Keying Protokolls (MIKEY) geschehen. Es soll für jede VoIP Domäne jeweils ein Security Proxy Server zuständig sein.

Lösung: Damit alle Nachrichten den Security Proxy Server durchlaufen, wird dieser zwischen den Client und den SIP Proxy Server geschaltet. Die Nachrichten, die einen Gesprächsaufbau zur Folge haben, werden so manipuliert, dass die Sprachdaten über den Security Proxy Server umgeleitet werden. In den SDP Payload dieser Pakete werden zusätzlich MIKEY Schlüsselinformationen eingebettet. Diese werden für die Authentifizierung und das Aushandeln eines gemeinsamen Session-Schlüssels verwendet. Für die Authentisierung werden DomainKeys und X.509 Zertifikate unterstützt. DomainKeys sind öffentliche RSA Schlüssel, die im Domain Name System (DNS) hinterlegt sind. Bei erfolgreichem Gesprächsaufbau werden sämtliche Gesprächsdaten über einen Secure RTP Tunnel übertragen. Ein grosser Vorteil dieser Lösung ist, dass keine Anpassung der Clients erforderlich ist.



Interaktion der beteiligten Komponenten