Universität Tübingen
Rechnernetze und Internet
Prof. Dr. Georg Carle

Studienarbeit

PGPfone – vertrauliche Gespräche über das Netz

Beschreibung:

Pretty Good Privacy (kurz PGP) steht heute in erster Linie für vertrauliche Kommunikation via Email. Mit Hilfe eines Web-of-Trust-Ansatzes werden die Schlüssel ohne zentralen Server verwaltet. Auf die Methoden von PGP können aber auch andere Dienste aufbauen. Im Falle von PGPfone soll Voice-over-IP (VoIP) auf diese Weise abgesichert werden. PGPfone ist eine Open-Source-Anwendung unter Windows. Sie ermöglicht VoIP direkt zwischen den beteiligten Rechner über das Internet. Sicherheit soll durch die Verwendung von PGP gewährleistet werden.

Aufgabenstellung:

Mit Hilfe des Source-Codes und der Dokumentation von PGPfone sollen die Funktionsweise, die Benutzbarkeit und die Protokolle untersucht werden. Wichtig ist auch das Erfassen von technischen Beschränkungen, die sich durch die Verwendung der Software hinter Firewalls oder durch Network Address Translation (NAT) ergeben können. Desweiteren ist die Überprüfung der Verbindungsqualität durch entsprechende Performance-Parameter von Bedeutung. Dies ist zu untersuchen und ggf. in PGPfone selbst zu implementieren. Mit Hilfe von Tools wie NIST Net ist es möglich, das Verhalten längerer Verbindungen im Labor nachzubilden. Hierbei können Verkehrsmitschnitte (Traces) gewonnen werden. Bei einer Sicherheitslösung stellt sich natürlich auch immer die Frage, welche Sicherheitsziele erreicht werden und welche nicht. Vielleicht können durch kleine Änderungen oder bestimmte Nutzung mehr Sicherheitsziele erreicht werden. Dies ist zu bewerten. Wichtig erscheint uns hierbei, dass nicht ausgespäht werden kann, wer mit wem gerade telefoniert. Dieses Problem wird von PGP selbst aber nicht angegangen.

Vorraussetzungen:

Kenntnisse in C++- und Windows-Programmierung sind hilfreich.

Stichworte:

VoIP, PGP (Pretty Good Privacy), Applikation, C++, Windows, Sicherheit.

Dr. Falko Dressler – Lehrstuhl für Rechnernetze und Internet – Morgenstelle 10 C9
eMail: dressler@informatik.uni-tuebingen.de – Tel.: 29-70507 – Web: net.informatik.uni-tuebingen.de
Heiko Niedermayer – Lehrstuhl für Rechnernetze und Internet – Morgenstelle 10 C9
eMail: niederma@informatik.uni-tuebingen.de – Tel.: 29-70509 – Web: net.informatik.uni-tuebingen.de