

CCC BREMEN

R.M.ALBRECHT

Mailverschlüsselung mit GnuPG

Robert M. Albrecht

Vorgehensweise

- Grundlagen 80% Effekt
- Praxis 20% Aufwand

- Vertiefung Theorie 20% Effekt
- Vertiefung Praxis 80% Aufwand

Agenda

- Was bringt es ?
- Welche Techniken gibt es ?
- Wie funktioniert es ?
- Wie benutze ich es ?
- Fortgeschrittenes: Smartcards, ...
- Was kann ich noch alles verschlüsseln ?

Löst eMail-Verschlüsselung mein Problem ?

Fangen Sie nicht am falschen Ende mit Sicherheit an:

- Betriebssystem und Anwendungen aktuell halten
- Nur vertrauenswürdige Software installieren
- Aktuellen Virens Scanner benutzen
- Mails nur über SSL abholen und verschicken
- Nur vertrauenswürdigen Rechner benutzen (Internet-Cafes ? Hotels, ?)
- Datenträger (Festplatten, USB-Sticks) verschlüsseln
- Benutzerverwaltung aktivieren, Kennwörter setzen

Was wird verschlüsselt und was nicht ?

- Email Verschlüsselung verschlüsselt den Inhalt.
- Die äußeren Verbindungsdaten (Absender, Empfänger, Betreff, Datum, Uhrzeit) sind immer noch im Klartext zu sehen und werden von der Vorratsdatenspeicherung erfasst.

Zwei Welten der Email-Verschlüsselung

PGP

- Dezentrales Modell
- Vorherrschend im freien Internet
- Von den üblichen Mailprogrammen nicht unterstützt
- Üblicherweise für Mailverschlüsselung genutzt, kann aber auch Dateien, ...

X.509

- Zentrales Modell
- Wird viel in Firmen genutzt
- Eingebaut in Thunderbird und Outlook
- Bekanntester Anwendungsfall: SSL (https, OpenVPN, ...)

Symmetrische & Asymmetrische Schlüsselsysteme

- Symmetrische Systeme benutzen zum Ver- und Entschlüsseln den gleichen Schlüssel
- Asymmetrische Systeme benutzen zum Ver- und Entschlüsseln unterschiedliche Schlüssel
- Verschlüsseln: Öffentlicher Schlüssel (public)
- Entschlüsseln: Privater Schlüssel (private)

Öffentlicher & Privater Schlüssel

- Der öffentliche Schlüssel wird verteilt:
Homepage, Visitenkarte, Schlüsselservers, ...
- Der private Schlüssel muss geheim bleiben.
- Ohne den privaten Schlüssel kann nichts entschlüsselt werden:
Kopie machen und sicher aufbewahren

Wie benutze ich die Schlüssel ?

Bob will Alice eine verschlüsselte eMail schicken

Bob

Öffentlicher Schlüssel

Privater Schlüssel

Alice

Öffentlicher Schlüssel

Privater Schlüssel

Bob benutzt Alice öffentlichen Schlüssel zum Verschlüsseln.

Alice benutzt ihren privaten Schlüssel zum Entschlüsseln.

Das Web of Trust

- Bob veröffentlicht seinen öffentlichen Schlüssel auf seiner Homepage.
- Aber woher weiß ich, ob der Schlüssel auch wirklich Bob gehört ?
 - Kein Problem beim direkten persönlichen Kontakt mit direkter Schlüsselübergabe
 - Ansonsten kann man sich die Identität und Korrektheit des Schlüssels von Dritten bestätigen lassen
 - Dadurch entsteht das Web of Trust.

Das Web of Trust

- Beim X509 gibt es nur eine zentrale Bestätigungsstelle, die Certificate Authority, zum Beispiel:
- Verisign: USA, kommerziell
- Teletrust: D, konform zum dt. Signaturgesetz
- CaCert: Community-Projekt zum Aufbau eines X509 Web of Trust

Was bringen Smartcards ?

- Wo hebe ich den privaten Schlüssel auf ?
- PGP-Smartcards ca 20 Euro
- Kartenleser ca. 20 Euro

- Schlüssel direkt auf der Karte oder dem Rechner erzeugen ?

Was ist los mit Mailinglisten ?

- Email-Verschlüsselung verträgt sich mit Mailinglisten nicht gut

GNU PG in der Praxis

- Reihenfolge:
 - GnuPG installieren
 - Schlüssel erzeugen
 - Mailclient anpassen
 - Ausprobieren

GNU PG installieren

- Ansprechpartner:
 - Linux: Jali
 - MacOS X: Crest
 - Windows: Viele
- Download unter
 - www.gnupg.org oder macgpg.sourceforge.net

Den Mailclient anpassen

- Thunderbird
 - Extras – Addons – Herunterladen
 - Enigmail suchen
 - Bei 64 Bit Linux klappt die automatische Installation nicht
- Outlook 2003: www.gpg4win.de
- Apple Mail: www.sente.ch/software/GPGMail/

Genug gesabbelt: Viel Spaß am Gerät !

Episode 2-7

- Festplattenverschlüsselung
- Lokale Browser
- OpenVPN auf Miet-Server
- Remailer
- Onion Routing
- Telefonieren

CCC BREMEN

ROMAL@GMX.DE