Email-Verschlüsselung mit GPG

Vortrag bei YaLUG Friedrichshafen
von Sebastian Scheible
am 14.9.2005

Überblick

- Warum überhaupt verschlüsseln?
- Public Key-Verschlüsselung
  - Hashing und Verschlüsselung
  - Web of Trust
  - Certificate Authorities
- PGP (Pretty Good Privacy)
- GPG (Gnu Privacy Guard)

Überblick

- Schwachstellen
  - Schwachstellen in MD5/SHA1
- Standards für die Email-Verschlüsselung
  - PGP/inline
  - PGP/MIME
  - S/MIME
- Unterstützung in Emailprogrammen
  - Plugins
- Unterstützung in Instant Messengern

Warum überhaupt verschlüsseln?

- “Ich habe doch nichts zu verbergen!”
- Wirklich nicht?
  - Liebesbriefe
  - Jobsuche aus ungekündigter Position
- Kompromitierter Übertragungsweg
- Das Recht auf Privatsphäre

Public Key-Verschlüsselung

- Geheimer (Private) Key
- Öffentlicher (Public) Key
- Hashing und Verschlüsselung
  - Hashes: Falltürfunktionen
  - Signaturen: Verschlüsselte Hashes

Public Key-Verschlüsselung

- Web of Trust
  - Schlüsselaustausch zwischen Unbekannten
  - Eine Kette aus gemeinsamen Bekannten
    - Alice signiert den öffentlichen Schlüssel von Bob
    - Charly will Bob eine vertrauliche Email schicken, er kennt jedoch nur Alice
    - Durch die Signatur erfährt Charly, dass Alice dem Schlüssel von Bob vertraut
    - Charly verschlüsselt die Email mit dem öffentlichen Schlüssel von Bob

Public Key-Verschlüsselung

- Certificate Authorities
  - Zentrale Signierstellen, denen viele Vertrauen
    - Identitätsprüfung
    - Cross-Zertifizierungen
    - Beispiel:
      - Zertifizierungsstelle von Heise (auf Messen)
        - http://www.heise.de/security/dienste/pgp/
- Keyserver

PGP (Pretty Good Privacy)

- 1991 von Phil Zimmermann veröffentlicht
- Exportbeschränkungen und ein Buch
- Patente, Vertrauen und Quellcode
  - OpenPGP (RFC2440) und GnuPG
- Jetzt kommerziell
- Frontend inbegriffen
- http://einklich.net/anleitung/pgp2.htm

GPG (Gnu Privacy Guard)

- Freie Software
- Frontends:
  - Linux: kgpg, gpgp, gpgkeys, ...
  - Windows: WinPT
    - http://winpt.sourceforge.net
- http://www.gnupg.org
- http://www.gnupg.org/howtos/de

Schwachstellen

- Schwachstellen vor dem Bildschirm
  - Ähnliche Fingerprints
    - Schlüssel aus Keyservern müssen sorgfältig verifiziert werden
- Schwachstellen in Hashverfahren
  - Kollisionsangriffe auf MD5 und SHA1

Standards für Email-Verschlüsselung

- PGP/inline
  - Keine Dateianhänge oder Umlaute
- PGP/MIME
- S/MIME
  - inkompatibel zu PGP/GPG

Unterstützung in Email-Programmen

- Unterschiedliche Unterstützung
  - Eingebaut
  - Plugins
  - Relays
- Übersicht:
  - http://www.bretschneidernet.de/tips/secmua.html
- Plugin für Outlook:
  - http://www3.gdata.de/gpg

Unterstützung in Instant Messengern

- Unterschiedlich
  - Kopete, Gaim, Psi, Miranda, Licq, ...
  - Plugins
  - Kompatibilität im Zweifelsfall testen

Und wenn wir gerade dabei sind...

- Fingerprint des Vortragenden:
  - sebastian.scheible@gmx.net: C7C8 A2BA 053B 2150 BD21 251B A357 F727 F080 FDA0
- Schlüssel erhältlich bei wwwkeys.de.pgp.net