PGP und authentisierte Kommunikation mit Nutzern des URZ

1. Was ist PGP?
   - Funktionsprinzipien und Fähigkeiten
   - verwendete Verfahren
   - Einbindung in Mail User Agents und andere Tools
   - Alternativen
2. Verwendung im URZ
   - wofür?
   - Technologie
   - offene Probleme und Lösungsvorschläge

Was ist PGP?

- Pretty Good Privacy (Philip Zimmermann)
- internationale Version 2.6.i (Ståle Schumacher) für Unix und DOS
  (`http://www.ifi.uio.no/~staalesc/PGP/versions.html`)
- electronic privacy program
- Verschlüsselungsverfahren
  - symmetrisch (Secret Key, Bulk Encryption): IDEA
  - asymmetrisch (Public Key): RSA Cryptosystem
- kryptografisches Hash-Verfahren (Message Digest): RSA MD5
- Key-Managementverfahren (key signing, web of trust)
- Komprimierungsverfahren: PKZIP

Was ist PGP?

fälschungssichere und authentische Kommunikation zwischen Nutzern

- Verschlüsseln von Nachrichten (ggf. für mehrere Empfänger)
  erforderlich: public key des Empfängers (der Empfänger)
- Unterschreiben von Nachrichten
  erforderlich: secret key des Absenders
- Unterschreiben und Verschlüsseln von Nachrichten
  erforderlich: secret key des Absenders und public key des Empfängers
- konventionelle Ver- und Entschlüsselung (ähnlich `crypt(1)`)
  frei wählbarer Schlüssel

Was ist PGP?

fälschungssichere und authentische Kommunikation zwischen Nutzern

- Entschlüsseln
  erforderlich: secret key des Empfängers
- Prüfen der Unterschrift
  erforderlich: public key des Absenders
- Entschlüsseln und Prüfen der Unterschrift
  erforderlich: secret key des Empfängers und public key des Absenders

Was ist PGP?

Key-Management

- Schlüsselpaar generieren
- öffentlichen Schlüsselbund (`$HOME/.pgp/pubring.pgp`) verwalten
  - öffentliche Schlüssel unterschreiben
  - Vertrauensgrade definieren
- geheimen Schlüssel (`$HOME/.pgp/secring.pgp`) schützen
- Schlüssel zurückziehen

Was ist PGP?

Key-Management: Key-Server

- 12 Key-Server halten weltweit signed public keys
- Deutschland:
  `pgp-public-keys@fbihh.informatik.uni-hamburg.de`
- Mail-Schnittstelle zum Eintragen, Abfragen und Zurückziehen von public keys

Was ist PGP?

Mail User Agents und PGP

- elm

  elm - Options (`$HOME/.elm/elmrc`)

  ```
  pager = /uni/global/bin/morepgp
  editor = /uni/global/bin/mailpgp
  ```

- pine

  pine - Setup (`$HOME/.pinerc`)

  ```
  editor=/uni/global/bin/mailpgp
  feature-list=enable-alternate-editor-implicitly, ...
  ```

- privtool

Einbau in andere Tools prinzipiell möglich (`pgp -f` Unix-like Filter)

Was ist PGP?

Alternativen

- wie bisher
  - vertrauliche Nachrichten im Klartext
  - Autor von Nachrichten nicht zuverlässig zu ermitteln
- Formulare mit Unterschriften
  - hoher Aufwand, nutzerunfreundlich
  - Autor nicht zuverlässig zu ermitteln
- PEM (SecuDE)
  - sehr komplex, noch zu unhandlich, wenig verbreitet
  - Schlüsselverteilung über X.509

Verwendung im URZ

wofür?

- Ersatz einiger Formulare durch entsprechende WWW-Forms mit digitaler Unterschrift
- sichere Übermittlung von Daten zum Türzugangskontrollsystem mit digitaler Unterschrift
- Übermittlung vertraulicher Informationen zwischen Mitarbeitern und von Nutzern an Mitarbeiter (verschlüsselt und mit digitaler Unterschrift)

Verwendung im URZ

digitale Unterschriften in WWW-Forms

Client **Server**

WWW-Form (ausgefüllt)

http://www.tu-chemnitz.de/cgi-bin/nph-pgp&text=...

cgi-bin/nph-pgp&text=...

application/pgp + Text

mailcap:

application/pgp ; signmail %s

xterm -e pgp -sta $1

mail service <$1.asc

oder

wwwget http://www.tu-chemnitz.de/cgi-bin/mail&text=signed_text

cgi-bin/mail&text=signed_text

mail service <signed_text

Verwendung im URZ

Datenübermittlung zum Türzugangssystem

- übermittelte Daten werden nur akzeptiert, wenn sie von einer bestimmten Person (Türverwalter) erstellt wurden
- Einsatz von PGP
  - Schlüsselaustauch (public keys) mit Türverwalter
  - Prüfung der digitalen Unterschrift bei Übernahme der Daten
- Einsatz von AFS
  - Verzeichnis im AFS nur schreibbar für den Türverwalter

Verwendung im URZ

offene Probleme

- Schlüsselverteilung
  - Zuordnung Schlüssel/Person muß 100%-ig stimmen
  - jeder Nutzer muß seinen öffentlich Schlüssel persönlich im URZ/Nutzerservice abliefern
  - Dispatcher unterschreibt diesen Schlüssel (und bürgt damit für die Korrektheit)
  - von Admins in Fakultäten unterschriebene Schlüssel werden ebenfalls akzeptiert
  - Nutzer sind für Sicherheit ihres geheimen Schlüssels selbst verantwortlich

Verwendung im URZ

offene Probleme

- technische Probleme/Aufgaben
  - Entwickeln/Testen entsprechender Werkzeuge
  - langfristiges Aufbewahren unterschriebener Nachrichten
  - Datenformat festlegen (Datum muß in Nachricht enthalten sein)