Kryptografie-Schulung

für Anfänger ohne Vorkenntnisse

Inhalt der Schulung

- Chat: XMPP (Jabber) & OTR
- E-Mail: OpenPGP

Warum dies?

- XMPP und OTR
  - einfachere Handhabung ähnlicher Basisaktionen
  - Schulungserleichterung (Chatraum) und Onlinesupport
  - „E-Mail-Analogie“ für Chat: das wichtigste offene System
  - für Windows, Linux, Mac, Smartphones; Clients & Server
- OpenPGP
  - eins von zwei relevanten Systemen für E-Mail
  - mächtiges, flexibles System (auch für Dateien und Text)
  - dezentrale Ausrichtung, weniger Automatismen

Ablauf

- Softwareinstallation, ggf. Mailkonfiguration
- Registrierung & Einrichtung der XMPP-Accounts
- parallele Aktionen:
  - Präsentation
    - kurzer Einführungsvortrag („Pflichtteil“)
    - Vorführung der wichtigsten Aktionen
  - Konfiguration der Computer durch Dozenten / Helfer
- üben
- ggf. Restvortrag: Hintergrundwissen

Links

- Softwareinstallation
  - http://openpgp-schulungen.de/sw/
- Registrierung der XMPP-Accounts (Jabber)
  - z.B. auf https://jabber.de/

Wenn alle die gesamte Software installiert und einen Mail- und einen XMPP-Account funktionierend eingerichtet haben, beginnt der Vortrag.

Kurzeinführung Kryptografie - 1

Was man für den Einstieg wissen muss (Basisaktionen)

Was braucht man?

- ein Schlüsselpaar
  - öffentlicher Schlüssel (Zertifikat)
  - privater Schlüssel
  - kann man kostenlos selber (mehrfach) erzeugen
  - dasselbe Prinzip bei Chat, E-Mail, Webservern
  - wird über mehrere Nummern identifiziert
    - Fingerprint (sicher): CF51 CB88 7D9A B184 AD50 21F4 DA6B 2836 5A21 B2D0
    - bei E-Mail auch: key ID: 0x5A21B2D0

Wie funktioniert es?

- Man braucht den öffentlichen Schlüssel des anderen, um
  - Daten für ihn zu verschlüsseln
  - seine Unterschriften zu prüfen
- Man braucht den eigenen privaten Schlüssel
  - um erhaltene Daten zu entschlüsseln
  - um zu versendende Daten zu unterschreiben
- **Das muss man sich merken!** (siehe Zettel)

Kryptografie-Hauptregel

Wird der richtige Schlüssel verwendet?

1) suchen & importieren (bei Chat & Web automatisch)
2) Verifizieren: sichere Quelle (Datei oder Fingerprint)
3) dem System die Verifizierung (Gültigkeit) anzeigen
   - bei E-Mail / OpenPGP: (lokal) signieren
4) gültige und nichtgültige Schlüssel unterschiedlich handhaben

Passphrase

- Die privaten Schlüssel sollen nicht ungeschützt auf Computern herumliegen (v.a. nicht ohne Plattenverschlüsselung).
- Eine Passphrase ist ein Passwort, das Leerzeichen enthalten kann.
- Die Passphrase verschlüsselt den privaten Schlüssel, schützt aber im laufenden Betrieb nur begrenzt. Nützlich für Schlüsselbackups.
- Die Passphrase kann geändert werden.

Vorführung

- XMPP
  - Kontakte hinzufügen (direkt & aus dem Chatraum)
- OTR
  - Fingerprint anzeigen / als gültig markieren
- OpenPGP
  - Zertifikat verbreiten (Keyserver & Mailanhang)
  - Zertifikat suchen, importieren
  - verifizierte & unverifizierte Zertifikate benutzen

und jetzt

- Passphrase ändern
- Fingerprint aufschreiben (Merkzettel)
- öffentlichen Mail-Schlüssel in Datei speichern
  - 0x12345678__vorname_name.asc
  - Schlüssel (und FPR) per Mail an Veranstalter
- Chatkontakte aus dem Chatraum hinzufügen
- üben: Mails schicken, Kontakte hinzufügen
  - Zertifikat des Dozenten suchen & importieren

Kurzeinführung Kryptografie - 2

Was man für den Einstieg wissen sollte (Hintergründe)

Was ist Kryptografie?

1) Verschlüsselung / Entschlüsselung
2) Unterschreiben / Unterschriften prüfen (speziell: Beglaubigung & Authentifizierung)

Man möchte ein bestimmtes Maß an Sicherheit, im Extremfall die **Garantie** dafür, dass Daten nur vom gewünschten Empfänger gelesen werden können und/oder vom behaupteten Absender unterschrieben wurden.

Einiges zur Sicherheit und Risiken

- Schlüssel werden nicht geknackt, sondern gestohlen
- Die echten Risiken sind
  - Fehler in der Software (unsichere Computer)
  - Fehlverhalten der Nutzer
- Es gibt nicht die eine gute Lösung für alles. Es gibt unwichtige und hochsensible Daten.
- Es muss nicht immer alles sicher sein, aber man muss sich über das Schutzniveau klar sein

Relation der Sicherheitsaspekte

Die Gesamtsicherheit ergibt sich ca.

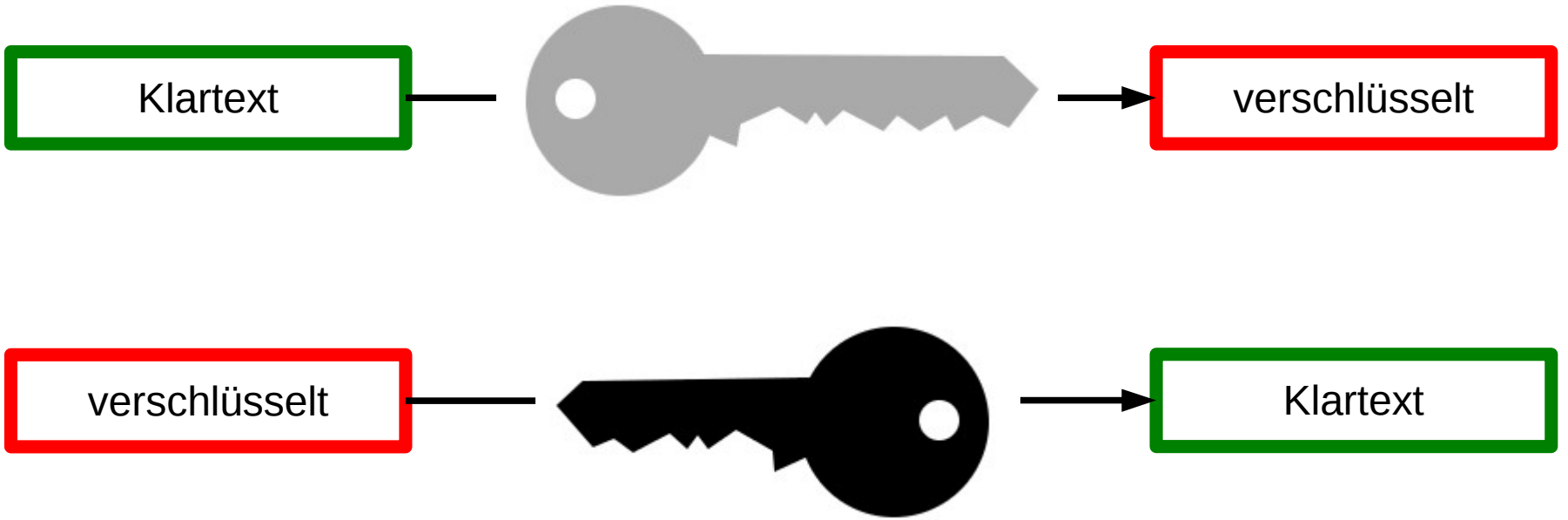
- zu 10% aus der Technik
- zu 60% daraus, dass man (immer!) weiß, was man tut
- zu 30% aus Disziplin: Es reicht nicht zu wissen, was getan werden müsste – man muss es auch tun...

symmetrisch vs. asymmetrisch

symmetrisch: Derselbe Schlüssel (Passwort) verschlüsselt und entschlüsselt.

symmetrisch vs. asymmetrisch

asymmetrisch: ein Schlüssel („öffentlich“) verschlüsselt, ein anderer („privat“ / „geheim“) entschlüsselt.



Kryptografie-Hauptregel

Wird der richtige Schlüssel verwendet?

1) suchen & importieren
2) verifizieren
3) gültig machen (lokal signieren)

Identitätsprüfung

- lästig, aber notwendig, weil meistens nicht ausreichend ist,
  - dass **IRGENDWER** die Daten oder den Schlüssel unterschrieben hat
  - dass **IRGENDWER** die Daten entschlüsseln kann, niemand sonst
- „Man in the Middle“-Angriff
- Verschlüsselung / Signierung alleine reicht nicht für eine gesicherte Kommunikation

Schlüsselverifikation

- Statt Vergleich des ganzen Schlüssels Vergleich einer fälschungssicheren Prüfsumme („Fingerprint“):
- `CF51 CB88 7D9A B184 AD50`
  `21F4 DA6B 2836 5A21 B2D0`
- Dasselbe Problem bei Chat, E-Mail und verschlüsselten Webseiten. Mal offensichtlich, mal vor dem Anwender versteckt.

Was noch?

- regelmäßig benutzen
- auf dem Laufenden bleiben
- neue Nutzer gewinnen
  - www.openpgp-schulungen.de/fuer/unterstuetzer/
- viel Spaß damit und – nicht verzweifeln, die Software wird allmählich besser...