Grundlagen der Verschlüsselung
Von Sebastian Andres <sebastian@sebastianandres.de>
14. März 2009
Linuxtage Chemnitz

Übersicht

- Allgemeines
- Algorithmen
- Public-Key-Verfahren
- Digitale Signatur / Zertifikate
- Fragen / Diskussion

Allgemeines

- Warum überhaupt Verschlüsselung?
- Wenn Verschlüsselung dann wie? (Welche Algorithmen sind überhaupt sicher?)
- Schwachstelle Mensch: Der beste Schlüssel nützt nichts, wenn die Benutzer das Passwort unsicher aufbewahren, oder das Passwort vergessen.

Algorithmen

- DES (data encryption standard): Von der US-Regierung entwickelt und daher relativ schwach.
- Triple-DES (Erweiterung von DES)
- AES: Advanced Encryption Standard (Rijndael): Von dem NIST als Standard festgelegt (Es gab eine Ausschreibung dafür).
- cast5 (Gilt als sehr sicher)

Public-Key-Verfahren

- Wie kann man Schlüssel sicher austauschen?
- Der Schlüssel wird geteilt (Vorhängeschloss wird öffentlich ausgelegt, die Zahlenkombination bleibt geheim).
- der Öffentliche Teil des Schlüssels wird im Internet oder auf Key-Servern verteilt.

Digitale Signatur / Zertifikate

- Ist der Absender wirklich derjenige den ich erwartet habe? Bzw. Ist der Server der, für den er sich ausgibt?
- Wurde an dem Inhalt der Nachricht etwas verändert? (Interessant bei Paketen der Distributionen, hat jemand an dem Paket etwas verfuscht?)

Fragen & Links

Fragen?

Links:

GnuPG: http://www.gnupg.org
OpenSSL: http://www.openssl.org
Mein GPG-Key: http://www.sebastianandres.de/key.txt (300DB2D2)