Verschlüsselte Kommunikation und Datensicherung

Andreas Herz

andi@geekosphere.org

11. Linux-Infotag 2012

24. März 2012

Über mich

Dipl.-Inf. Andreas Herz

- Informatik Studium an der Universität Augsburg
- Seit Mitte 2011 Entwickler bei Linogate GmbH in Augsburg

Überblick

Motivation

Verbreitete These

Aber ich hab doch nichts zu verbergen!

Wirklich?

Eigentlich jeder hat etwas zu verbergen.

Motivation

Verbreitete These

Aber ich hab doch nichts zu verbergen!

Wirklich?

Eigentlich jeder hat etwas zu verbergen.

Eigenschaften der Kryptographie

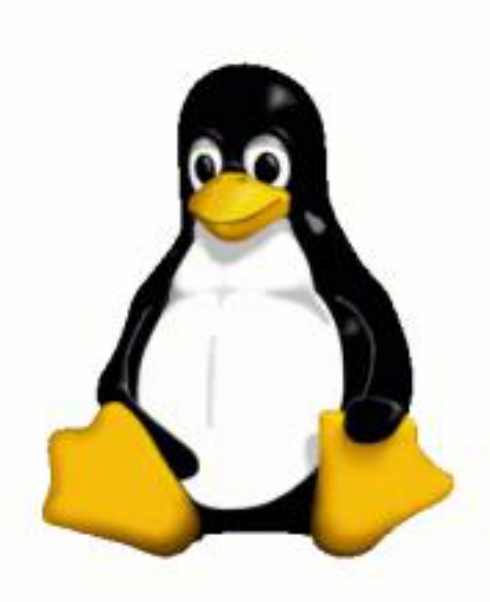
Geheimhaltung Inhalt für unbefugte unleserlich machen.

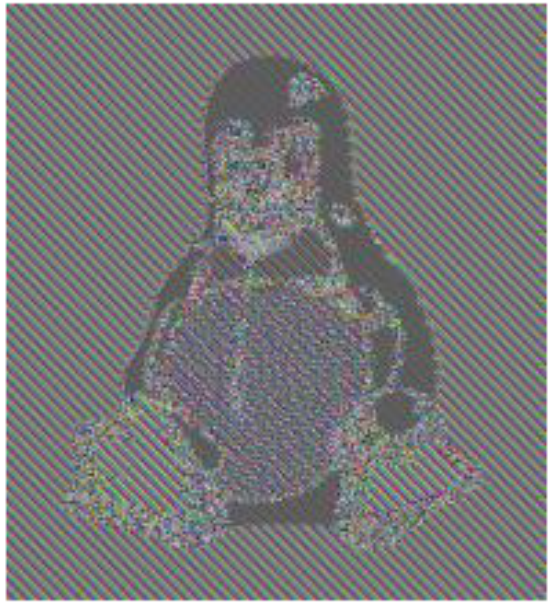
Authentifizerung Identitätsbeweis des Kommunikationspartners.

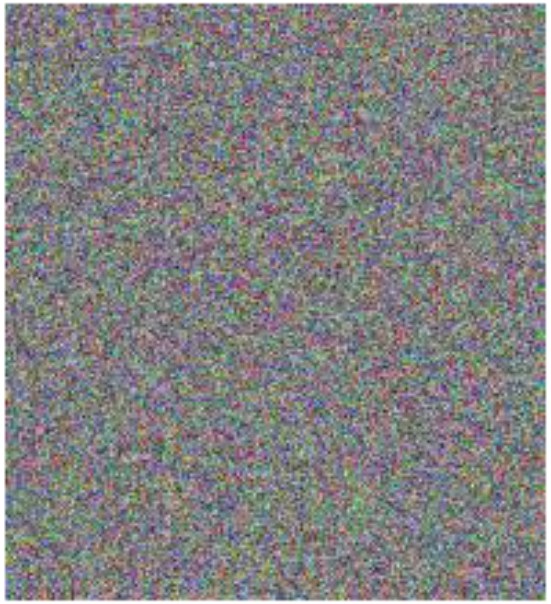
Integrität Die Daten bzw. der Inhalt wurde(n) nicht verändert.

Verbindlichkeit Die Übertragung kann nicht geleugnet werden.

Verschlüsselung != Verschlüsselung







Grundlagen

- Verschlüssung des Logins/Authentifizerung
- Authentifizierung der Gesprächspartner
- Gesicherte Übertragungswege
- Verschlüsselung des Inhalts

Sicher Chatten

Logindaten sicher übertragen

- Auf TLS/SSL achten
- Zertifikate beachten
- Fingerprints vergleichen

Inhalte verschlüsseln

- GPG (GNU Privacy Guard) mit Public-Key (bzw. PGP)
- Off-the-Record Messaging

Clients

Jabber/XMPP Clients mit Support für Verschlüsselung:

Client	GPG	OTR
mcabber	Ja	Ja
Gajim	Ja	Ja (Patch)
Pidgin	Nein	Ja (Plugin)
BitlBee	Nein	Ja (Patch)
Psi	Ja	Ja (Patch)

Pidgin kann OTR beispielsweise auch bei anderen Protokollen wie ICQ verwenden.

Mailverkehr absichern

Logindaten sicher übertragen

- Auf TLS/SSL achten
- Zertifikate beachten
- Ports 465, 585, 993, 995

Inhalte verschlüsseln (PKI basierend)

- OpenPGP/GnuPG
- S/MIME

Clients

Fast alle gängigen Mailclients können beide Verfahren:

- Thunderbird mit Enigmail Addon
- Mutt
- Claws-Mail
- Evolution

Problematik

- Bei der Einwahl ins Netz ist man meist mit einer eindeutigen (dynamischen) IPv4-Adresse identifizierbar.
- Wie es mit IPv6 konkret wird, muss sich erst noch zeigen.

Damit ergeben sich folgende Problemfelder:

- Abmahnwahn
- Vorratsdatenspeicherung
- Profilbildung
- Anonymität nicht gewährleistet

Gegenmassnahmen

Es gibt einige Möglichkeiten mit unterschiedlichen Ansätzen:

- TOR (The Onion Router) bzw. Vidalia als GUI
- I2P
- Freenet
- (VPN)

Virtuelle Private Netzwerke (VPN)

Nicht nur bei Firmen auch im privaten Bereich bieten VPNs einen sicheren und verschlüsselten Zugang in Netzwerke.

Einsatzzweck:

- Verbindung ins Firmennetzwerk von zu Hause
- Sicherer Zugang im mobilen Netz
- Verschlüsselter Datenaustausch
- „Anonymer“Zugang ins Internet

Tools:

- OpenVPN
- IPSec

Grundlagen

Um Daten zu verschlüsseln gibt es zwei grundlegende Verfahren, entweder die einzelnen Daten/Ordner verschlüsseln oder das Dateisystem bzw. die Festplatte.

Anwendungszweck:

- Geheime Daten vor unbefugtem Zugriff sichern
- Verlust der Hardware (Laptop/Fesplatte)
- Beschlagnahmung
- Privatsphäre schützen

Nachteile:

- Performance-Verlust (immer mehr vernachlässigbar)
- Wiederherstellung der Daten nahezu unmöglich bei Defekt oder Passwortverlust
- Erhöhter Konfigurationsaufwand

Datenverschlüsselung

Möglichkeiten der reinen Dateiverschlüsselung:

- GnuPG
- encFS

GnuPG bietet sich bei kleineren Dateien und Ordnern an, die man beispielsweise auch verschicken will.
encFS macht bei lokalen Ordnern mehr Sinn.

Systemverschlüsselung

Möglichkeiten der Festplatten- bzw. Systemverschlüsselung:

- DM-Crypt/LUKS
- Truecrypt

DM-Crypt/LUKS ist der Standard unter Linux, Truecrypt hingegen kann auch unter Windows/Mac OS X verwendet werden.
Empfehlung bei der Verschlüsselung mit DM-Crypt/LUKS ist **aes-xts-plain**.

Fragen

Fragen?

Ende

Vielen Dank für die Aufmerksamkeit!