eMail-Verschlüsselung für Einsteiger

Kai 'zeus' Kostian ⟨zeus@ctdo.de⟩
Stefan Kinzel ⟨stefan@ctdo.de⟩
Markus Lindenberg ⟨markus@lindenberg.io⟩

Chaostreff Dortmund

Cryptoparty im Langen August
04.10.2015

Index

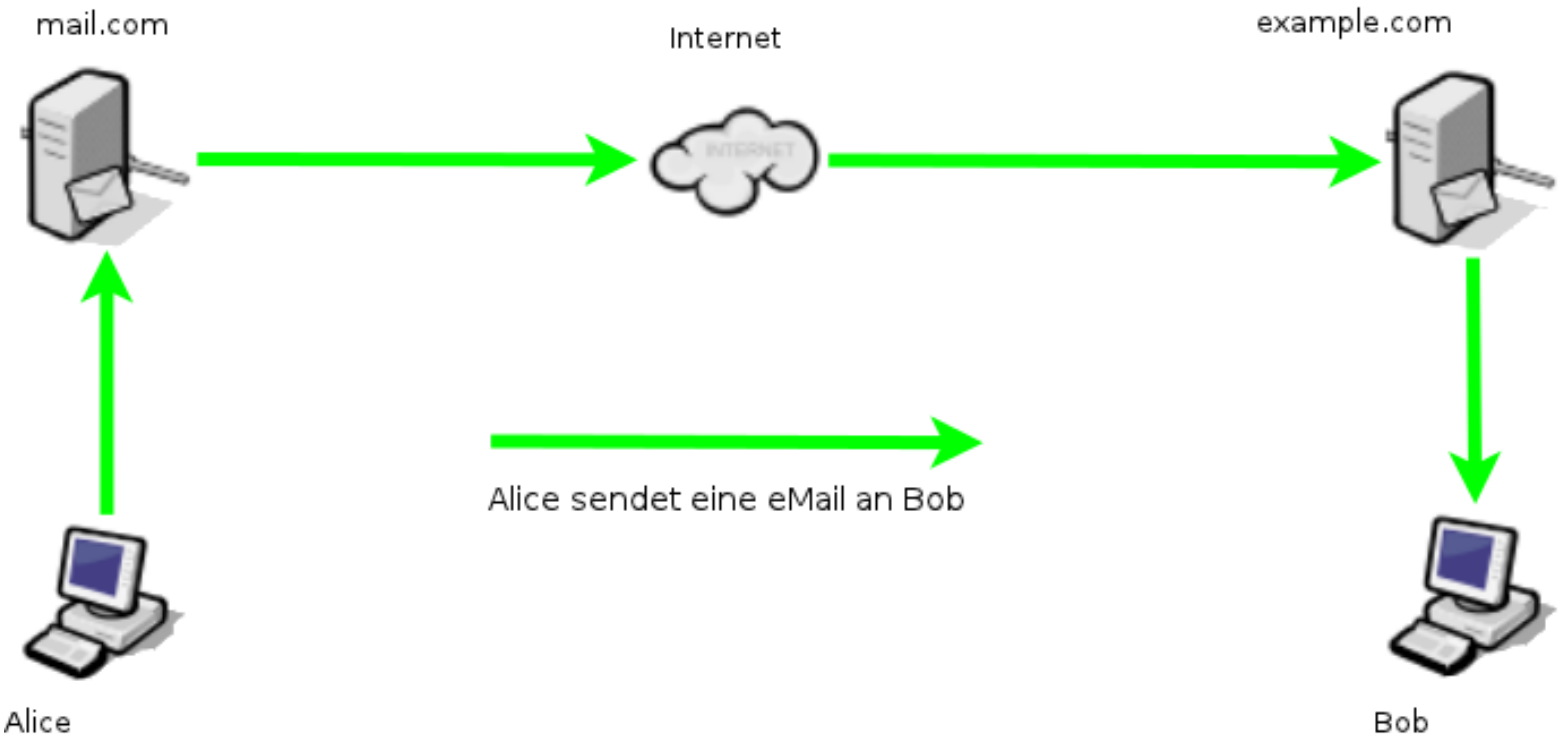
Kryptographie kurz erklärt

- Wird seit dem Römischen Reich zur Übermittlung von geheimen Informationen genutzt (z.B. Schlachtpläne)
- Die Anfänge: Caesar-Chiffre (Schlüssel "C"):
  - DiesisteinKlartext
  - GLHVLVWHLQNODUWHAW
- Durchbruch der Verschlüsselung seit der Enigma(1918): DES(1975), RSA(1977), AES(1998), ...
- Verschiedene Verfahren: Symmetrische und asymmetrische Schlüsselverfahren

eMail-Grundlagen

- Elektronische Post seit 1984
- Getrennte Server für Empfang (POP3 - veraltet, und IMAP) und Versand (SMTP) einer eMail
- eMails bestehen aus Header- und Body-Teil
  - Wichtig: Betreff gehört zum Envelope (Header!)
- Verschlüsselte Kommunikation nur bis zum Provider ohne Zusatzsoftware möglich
- eMails passieren im "Klartext" meist einige bis einige dutzend Server

eMail mit Alice und Bob



Wie eMail-Verschlüsselung funktioniert - Ein Überblick

- PGP - Pretty Good Privacy (1991) - Programm zur Beschreibung des Schlüsselmodells
  - Bis Ende der 90er unter Kriegswaffengesetz in USA - mittlerweile von McAfee aufgekauft
- OpenPGP (1998) - Offener Standard und Beschreibung des Verfahrens basierend auf PGP v.5
- GnuPG (1998) - Freies Programm auf Basis des Standards von OpenPGP
- Web of Trust (Keine zentrale Zertifizierungsinstanz)

Bedarf an Vertrauenswürdigkeit

- Je peinlicher oder persönlicher eine Information, desto mehr Bedarf an Schutzwürdigkeit
- Je brisanter die Informationen, desto mehr Bedarf an Schutzwürdigkeit
- Je teurer es ist, wenn Informationen in die falschen Hände gelangen, desto mehr Bedarf an Schutzwürdigkeit

⇒ Alles verschlüsseln, was verschlüsselbar ist

Unterschied zwischen Transport und Inhaltsverschlüsselung

- Transport-Crypto **IST NICHT GLEICH** Inhalts-Crypto!
- Transportverschlüsselung **KANN** vor Account- und Identitätsdiebstahl schützen
- Inhaltserschlüsselung schützt vor Manipulation, vor Mitlesern und ermöglicht Authentifizierung des Kommunikationspartners
- beides sind **ERGÄNZENDE** Verfahren
  - SSL und TLS (https) sind Transportverschlüsselungen
  - GPG, PGP, AES u.Ä. sind Inhaltsverschlüsselungen

GPG, PGP, GnuPG... und andere P und G's...

- Asymmetrisches Schlüsselverfahren mit Passwörtern **UND** Schlüsseldateien
- Private- und Public-Keys
- Signatur mit **Private**-Key des Senders
- Verschlüsselung mit **Public**-Key des Empfängers
- Entschlüsselung durch **Private**-Key des Empfängers

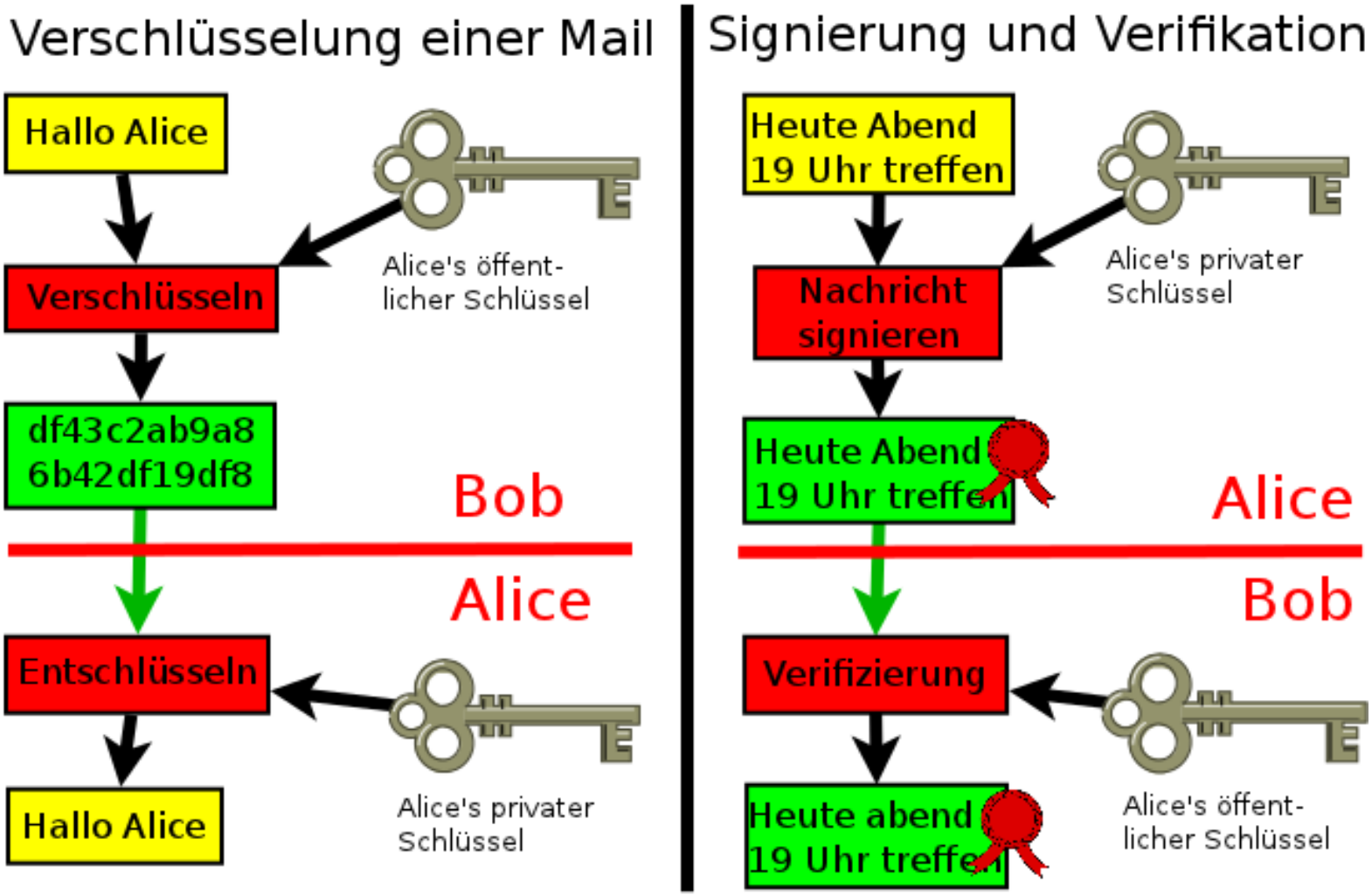
Vorteile:

- Überprüfbarkeit der Authentizität von Schlüsseln durch Fingerprints
- Überprüfbarkeit einer Nachricht auf Manipulation durch Signaturen
- Erweiterung von "Vertrauen" durch Keysigning (gegenseitiges Unterschreiben von Schlüsseln)
  - Verschiedene Vertrauensebenen - Ein wesentlicher Bestandteil der Chain of Trust / des Web of Trust

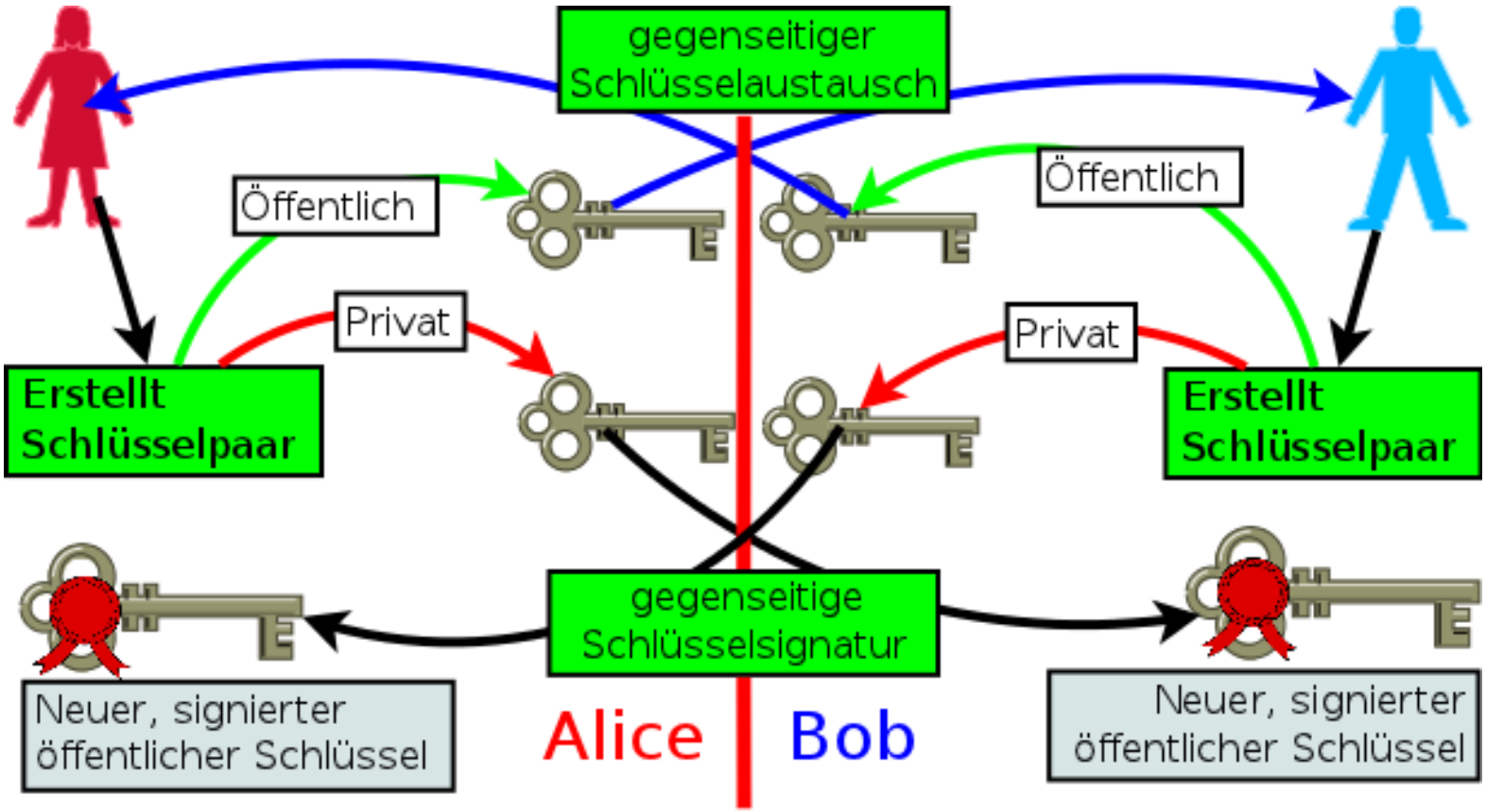
Vorraussetzungen

- Schlüsselerzeugung mit OpenPGP bei ausreichender Schlüssellänge (z.B. 4096 bit) und sicherem Passwort
  - 2 Schlüssel werden erzeugt; 1 privater und 1 öffentlicher
  - Der öffentliche Schlüssel muss an alle künftigen Kommunikationspartner weitergegeben werden
  - Der private Schlüssel sowie das Passwort **DARF NIEMALS** weitergegeben werden
- Schlüsselaustausch am besten persönlich vornehmen
  - Praktische Alternative für den Schlüsseltausch: Keyserver
  - Schlüsselserver dienen zum Austausch von Public-Keys mit automatischer Synchronisation untereinander
  - **Achtung: Verifikation von Schlüsseln ist bei Nutzung von Keyservern wichtiger denn je !!**
- Verifizierung von Schlüsseln entweder persönlich oder über alternative Kanäle (z.B. Fingerprint am Telefon vorlesen)

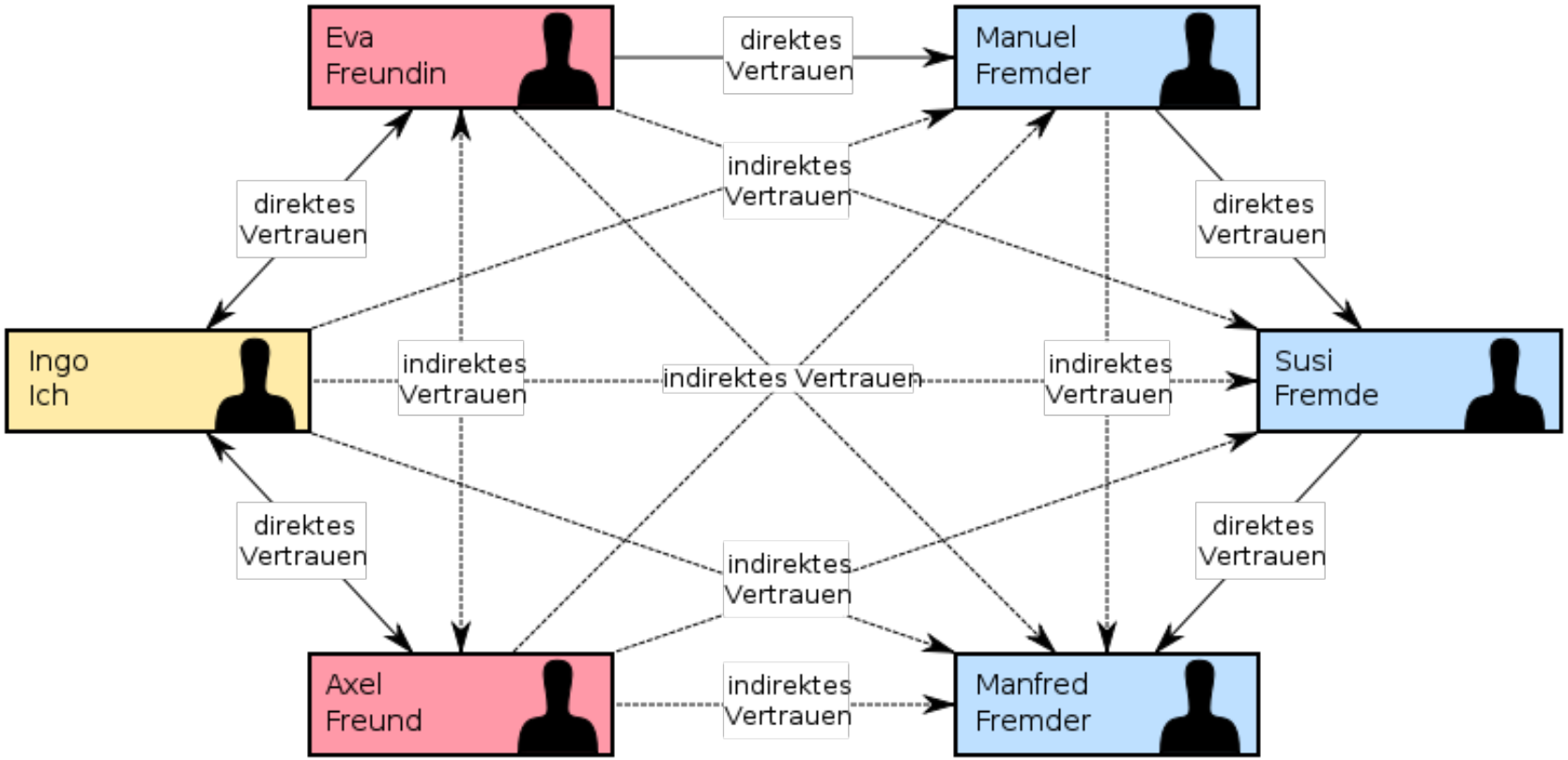
eMail-Verschlüsselung mit Alice und Bob



Keysigning mit Alice und Bob



Web of Trust - Vertrauensketten



- Schaffung von Vertrauensketten durch direktes und indirektes Vertrauen
- Kurz gesagt: Ich vertraue Jedem, dem von Jemandem vertraut wird, dem ich vertraue

Fingerprints im Detail

- Für Penible: Der Fingerprint ist ein 160-bit SHA-1-Hash des Octets 0x99 über den Public-Key (RFC4880 Kapitel 12.2)
- Key-ID: Die unsignifikantesten (letzten) 64 Bits des Fingerprints
- Hex-Dezimale Notation von Fingerprints und Key-ID's
- Beispiel: Immo Wehrenberg - immo@bundessicherheitsministerium.de

	Fingerprint-Aufbau
Print:	8BFC 303C 1574 5912 23B5 CFDD 5A59 5F09 **9B40 9979**
ID:	0x **9B40 9979**

Chain of Trust - Teil I : Die Theorie

In der Theorie ist Theorie und Praxis Ein- und Dasselbe

In der Theorie ...

- ...gibt man niemals den Private-Key oder das Passwort weiter (oder vergisst eines von beiden irgendwo...)
- ...nimmt man für jeden Zweck ein anderes Passwort
- ...benutzt man nur "sichere" Passwörter mit >20 Zeichen, mit Sonderzeichen, Groß- und Kleinbuchstaben und Zahlen
- ...benutzt man nur vertrauenswürdige Hard-& Software und zwar nur in Umgebungen, die man vollständig kontrollieren kann

Chain of Trust - Teil II : Die Praxis

Wenn man sagt, dass man einer Sache grundsätzlich zustimmt, so bedeutet es, dass man nicht die geringste Absicht hat, sie in der Praxis durchzuführen. -Otto von Bismarck

In der Praxis...

- ...passieren Fehler eher selten durch schlechte Konzepte oder Technik, sondern durch dessen mangelhafte Umsetztung
- ...ist der Mensch nach wie vor der "Single Point of Failure" in diesem Trustmodell
- ...passieren die meisten GAUs immernoch durch:
  - Dummheit
  - Naivität
  - Faulheit
  - oder (vor allem!) Schusseligkeit
- Das ist nun mal die Realität...

Backups

- Backups von privaten Schlüsseln bzw. Widerrufszertifikaten anzufertigen ist **UNERLÄSSLICH**
- Der goldene Weg: Auf Papier und/oder USB-Stick im Schliessfach/Tresor lagern, am besten redundant
  - Problem: bei Verlust/Verlegen des Keys ist das abtippen mühselig (etwa 1 Din-A4 Seite voller kryptischer Zeichen)
- Fazit: Jedes Konzept hat seine Schwächen

Ist nur mit Vorsicht zu genießen

Verschlüsselung mobil, tragbar und bequem auf dem USB-Stick / Smartphone ist zwar möglich, aber nicht ratsam, denn man bricht die Chain of Trust:

- man hat das "Zielsystem" seltenst auch nur halbwegs unter Kontrolle (z.B. Keylogger)
- man kann nicht abschätzen, wo Private-Key oder Passwort vielleicht landen
- gestohlene Identitäten sind besonders tragisch, wenn sich der "Dieb" auch noch authentifizieren kann
- halbwegs sicherer weg für alle, die alle Warnungen ignorieren wollen:
  - verschlüsselter USB-Stick (oder CD) mit Keys drauf
  - am besten als bootbares Live-System
  - **DAS ALLES HILFT TROTZDEM NICHTS GEGEN MANIPULIERTE TASTATUREN ODER FIES AUSGERICHTETE KAMERAS!!**

Es gibt da noch mehr, womit man Verschlüsseln kann

Es gibt da noch ein wenig Hardware, mit der man die ganze Sache sicherer gestalten kann, und sogar das mit der Mobilität geht irgendwie...

- **@markus: add your stuff here...**

Praxisbeispiel: Thunderbird mit Enigmail-Addon unter Linux

AB HIER KOMMT
EINE GANZ TOLLE
SUPER-LIVE-DEMO

Bullshit made in Germany [1]

E-Mail made in Germany

Aktivierung von SSL/TLS zwischen den Mail-Servern der beteiligten (deutschen) Provider

DE-Mail, E-Postbrief, ...

Marketingkampagne zur Einführung der Briefmarke für E-Mail

Schlandnet

Die Telekom ist schuld!

[1] http://media.ccc.de/browse/congress/2013/30C3_-_5210_-_de_-_s
-_201312282030_-_bullshit_made_in_germany_-_linus_neumann.html

Was Ihr sonst noch so wissen wollt...

Hier ist jetzt Platz für Fragen und Antworten zum Thema

- - -

Diese Vortragsfolien gibt es (ungekürzt) auch zum Download unter

`https://wiki.ctdo.de/vortraege/gnupg`

- - -

- - -

Links zum selber Nachlesen

Bild auf Seite 13:
http://de.wikipedia.org/wiki/Datei:Web_of_Trust.svg

Links zum Thema:

- http://www.chaostreff-dortmund.de
- http://de.wikipedia.org/wiki/E-Mail-Verschl%C3%BCsselung
- http://de.wikipedia.org/wiki/Pretty_Good_Privacy
- http://de.wikipedia.org/wiki/OpenPGP
- http://de.wikipedia.org/wiki/Gnupg
- http://de.wikipedia.org/wiki/Alice_und_Bob
- http://de.wikipedia.org/wiki/Web_of_trust
- http://de.wikipedia.org/wiki/Schl%C3%BCsselserver
- http://de.wikipedia.org/wiki/Hexadezimalsystem
- http://de.wikipedia.org/wiki/SHA-1
- http://tools.ietf.org/html/rfc4880

Ende des Vortragsteils

Danke das ihr solange durchgehalten habt!

Nachwort

Nachwort: https://xkcd.com/538/