Sicheres E-Mailen

- PING e.V.

- Sicherheit
- E-Mail-Angriffspunkte
- Was kann ich tun?

Sicherheit

- Was ist Sicherheit?
- Sicherheit – Wie funktioniert das?
- Was muß ich tun, um (mehr) Sicherheit zu erlangen?

Was ist Sicherheit?

- Das Wissen, daß nur Dinge passieren, die man auch wirklich will.
- Dinge geschehen auf gewohnte Art.
- Vertrauen
  - In die installierte Software
  - In andere Personen
  - In die Übermittlung meiner Daten

- Sicherheit ist kein Zustand, sondern ein Prozeß!

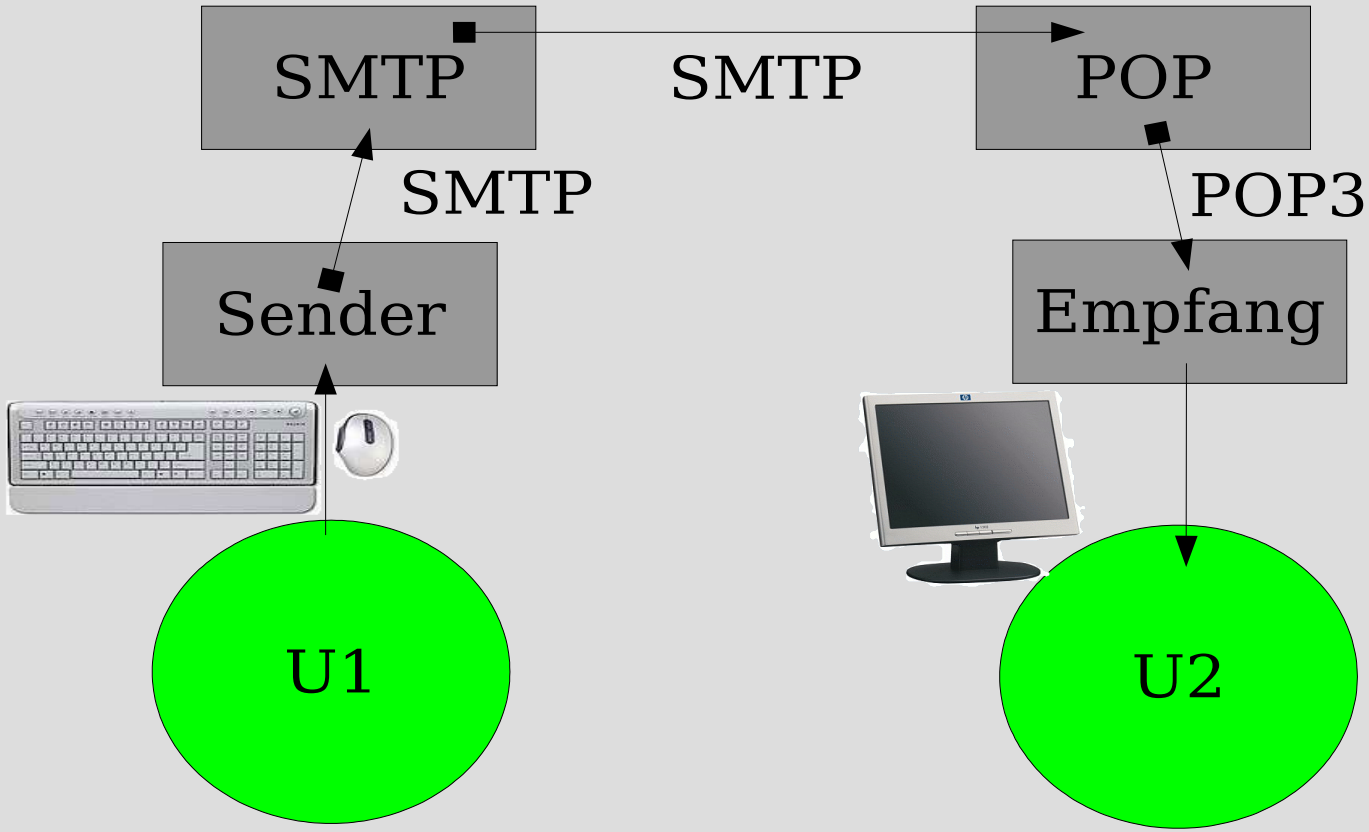
Sicherheitsaspekte

- Identifikation
  - Wer bist Du?
- Authentifikation
  - Bist Du es wirklich?
- Autorisation
  - Was darfst Du?

E-Mailen

- Was geschieht? Wie ist der Ablauf?
- Wo sind die möglichen Unsicherheiten?
- Wie kann ich die beheben?

E-Mail: Ablauf



Mail: Identifikation

- Absender
  - Mailadresse?
  - sonst wenig Methoden.

- „Wer bist Du?“ ist hier nicht so wichtig wie „Bist Du es wirklich?“

Mail: Authentifikation

- Schwache Methoden:
  - Header der Mail: Übliches Routing?
    - Technische Analyse
  - Ungewöhnliche Inhalte?
    - „Hallo, ich bin Peter Schmittmann, ein Neffe des jüngst verstorbenen Dr. Heiner Müller-Lüdenscheid, und ich trete hiermit mit einer vertraulichen Bitte an sie heran...“
    - „gesunder Menschenverstand“
- Starke Methoden:
  - „Elektronische Signatur“

Mail: Autorisation

- Was darf eine Mail überhaupt?
  - Mich zur Bekanntgabe von vertraulichen Daten auffordern?
  - Programme auf meinem System ausführen?
  - Daten ohne mein Zutun versenden?
- NEIN!
- HTML-Mails sind in der Hinsicht bedenklich: Es werden automatisch Daten geladen und Programme ausgeführt.

Leseautorisation Mail

- Wer darf eine E-Mail lesen?
  - Absender
  - Empfänger
- Wer kann sie zusätzlich lesen?
  - „Lauscher“ an der Leitung
  - Systemverwalter
  - Leute, die anderweitig Zugriff auf die Daten bekommen.

Sicherheitslücken

- Im E-Mail-Konzept kann:
  - Jemand vorgeben, jemand anders zu sein
  - Jemand die Mail lesen, der nicht dazu berechtigt ist.

- Abhilfen:
  - Mailunterschrift
  - Mailverschlüsselung

Kryptographie

- Zwei Arten Verschlüsselung:
  - Symmetrisch
    - Einfach
    - Schnell
    - Relativ unsicher
  - Asymmetrisch
    - Mathematisch aufwendig
    - Sehr sicher!

Verschlüsselung

- Symmetrisch:
  - ROT13 ;-)
  - DES (Data Encryption Standard)
  - AES (Advanced Encryption Standard)
  - Blowfish,Twofish...
- Asymmetrisch
  - RSA (Rivest, Shamir, Adleman)
  - Diffie-Hellman
  - ElGamal
  - Elliptische Kurven

  -> Öffentlicher und privater Schlüssel

Sicherheit

- RSA-Algorithmus: Große Primzahlen.
- Zwei große (mehr(!) als 100stellige Primzahlen) werden miteinander multipliziert.
- Das Verfahren ist dann zu brechen, wenn man die resultierende Zahl in Primfaktoren zerlegen kann.
- -> sehr, sehr viel Rechenzeit.
- Andere Verfahren: Ähnliche Komplexität.

Anwendung

- Mailtext
- Aus Mailtext und privatem Schlüssel eine Signatur generieren.
- Signatur wird an Mailtext angehängt.

- Zwei Verfahren:
  - OpenPGP
  - S/MIME

S/MIME

- „X.509“-Zertifikat (wie im Webbrowser)
- Historisch auf X.500 basierend
- X.500: die „Kommittee“-Version von E-Mail, hat sich aber nicht durchgesetzt, da Internet E-Mail einfacher.
- Hierarchische Struktur.
- Kauf eines Zertifikates notwendig.

OpenPGP

- „PGP-Signatur“, Schlüsselring und Keyserver
- Basiert auf PGP („Pretty Good Privacy“)
- Standardisierung, als PGP wegkommerzialisiert zu werden drohte.
- „Web Of Trust“
- Gegenseitiges Unterschreiben des Schlüssels

Anwendung

- Erweiterungen/Plugins (Enigmail...)
- Format auswählen:
  - S/MIME V2
  - S/MIME V3
  - OpenPGP
  - PGP/MIME

Schlüsseltausch (PGP)

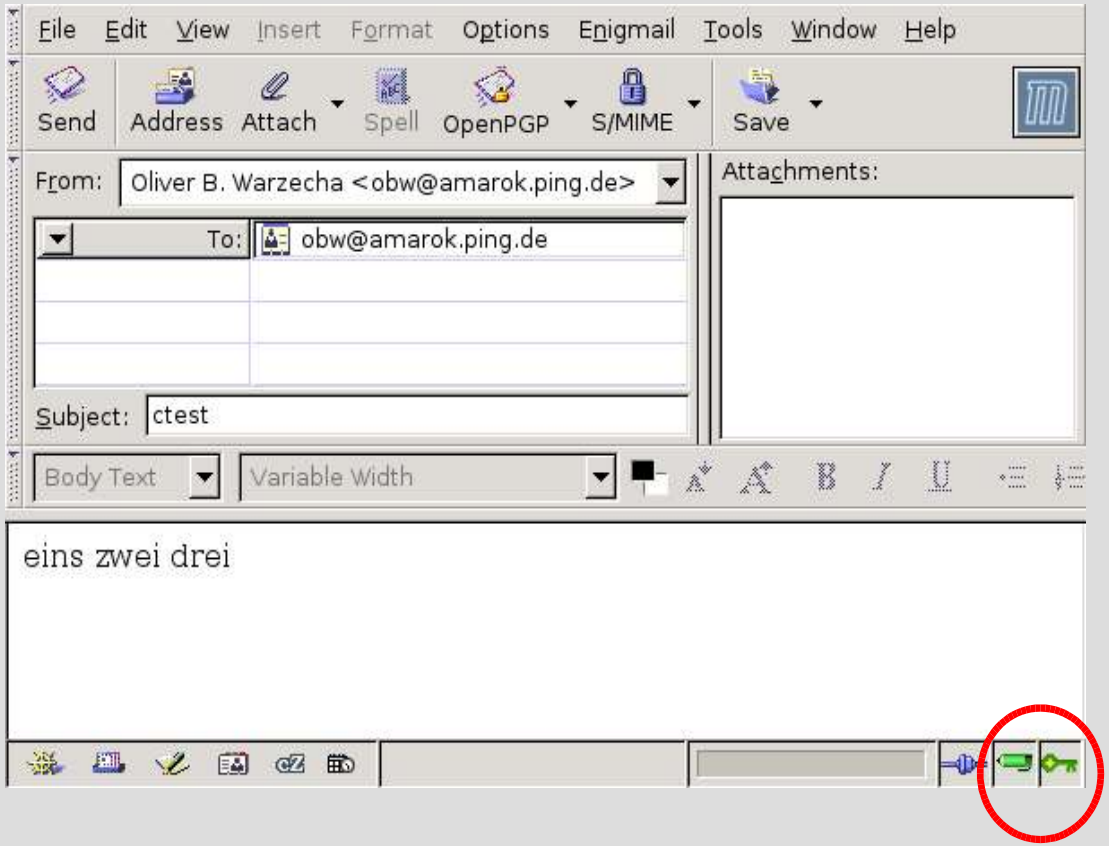
- Öffentliche Keyserver
- Gegenseitiges Unterschreiben der Schlüssel zur Identitätsbestätigung

Anwendung:

- Unterschreiben:
  - Ich signiere mit meinem privaten Schlüssel
  - Jeder kann mit meinem öffentlichen Schlüssel überprüfen, daß diese Nachricht von mir stammt
- Verschlüsseln:
  - Ich verschlüssele mit dem öffentlichen Schlüssel des beabsichtigten Empfängers.
  - Nur der Empfänger kann die Nachricht entschlüsseln, da nur er den passenden privaten Schlüssel besitzt.

Beispiel

- Mail schreiben
- Verschlüsselung wählen
- Gegebenenfalls Schlüssel des Empfängers wählen
- Gegebenenfalls Paßphrase für eigenen Schlüssel eingeben



Beispiel(2)

- Verschlüsselte Mail:

-----BEGIN PGP MESSAGE-----
Charset: ISO-8859-1
Version: GnuPG v1.4.1 (GNU/Linux)
Comment: Using GnuPG with Mozilla - http://enigmail.mozdev.org

hQEMAzQNFeN7XpWRAQgAkL3L3f81OkCvq5TNqijIKdkewi9a72u0uI0/FBljWtRw
gyPunppIXSbSCr6RQc935SZ4z6P6L1GJamX5cq7b3sCzF/7UgUYWTcM4wafBfGJm
wXkdD38alVxsIz80A+58OLmC6QwImZz8osJpvYQ1G23fHvYIehnKozopJOolXrn6
skCMtz+4f2MK12Djhliq3djUHGe/XOrL6XwA4NxWgfM2lDQCxLHsFDtUJ5vL/0Ww
4j0xfe8IfJyJde9gOrpbP4qyPTATCJjvLbOHu7Ek542DQP8ptOl3jNwn59iYYx8/
62yI3SKwtMgMSuWYqV82zBeIBSNT1iTm8mr/c9S+ZMlEc3sgSo4Rt1HC+v4YNBb0
Os/LX8yML9l6rs5OGLNunlPPBFYZU7IUhlk34Y9WsqlzoaCCa5OfQYZEWFxKp5wD
1IFzX5A=
=1ORb
-----END PGP MESSAGE-----

Beispiel(3)

- Entschlüsselte Mail:

From: "Oliver B. Warzecha" <obw@amarok.ping.de>
Subject: Crypttest
Date: Mon, 05 Sep 2005 17:16:10 +0200
User-Agent: Mozilla/5.0 (X11; U; Linux i686; en-US; rv:1.7.11)
Gecko/20050818
To: obw@amarok.ping.de

[-- PGP output follows (current time: Mon Sep 5 18:54:16 2005) --]
gpg: WARNING: using insecure memory!
gpg: please see http://www.gnupg.org/faq.html for more information
gpg: encrypted with 2048-bit RSA key, ID 7B5E9591, created 2000-10-25
      "Oliver B. Warzecha <obw@kleinbus.org>"
gpg: WARNING: message was not integrity protected

[-- End of PGP output --]

[-- BEGIN PGP MESSAGE --]

Einz, zwei, drei, das kann keiner lesen, eieiei...^M

[-- END PGP MESSAGE --]

PGP-Keyserver

- z.B. http://www.dfn-pca.de/pgpkserv/
- Abfrage ist in Programmen integriert, man braucht sich also im Normalfall nicht darum zu kümmern.

Sicherheit ist keine Konstante

- Nichts ersetzt den Gebrauch des Verstandes.