Liest Big-Brother meine Email?

Arno Wagner

Computer Engineering and Networking Laboratory, ETH Zürich

Dies ist das geheime Rezept:

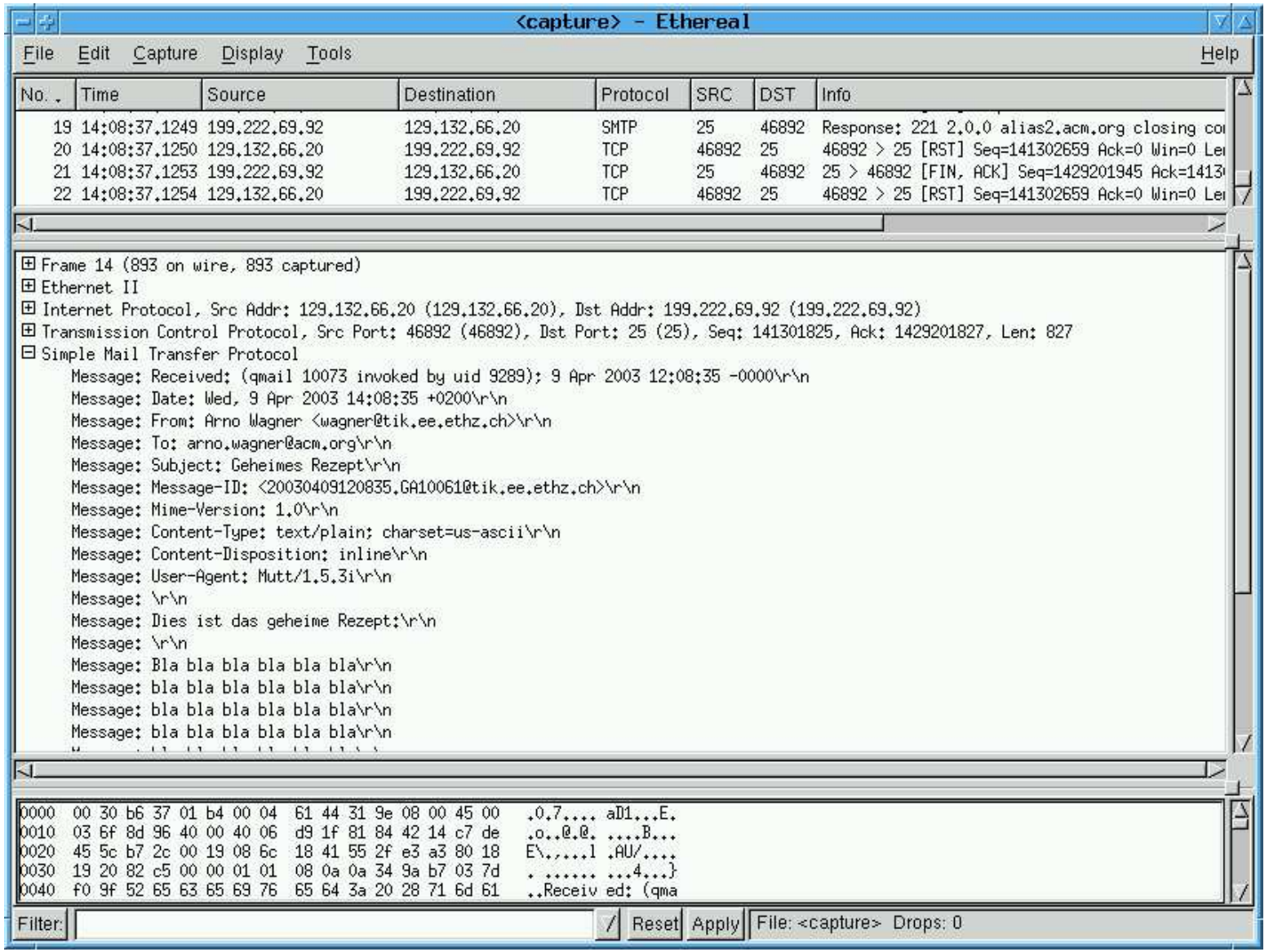
Bla bla bla bla bla bla
bla bla bla bla bla bla
bla bla bla bla bla bla
bla bla bla bla bla bla
bla bla bla bla bla bla
bla bla bla bla bla bla

Arno Wagner

ETH Zuerich

Gloriastr. 35

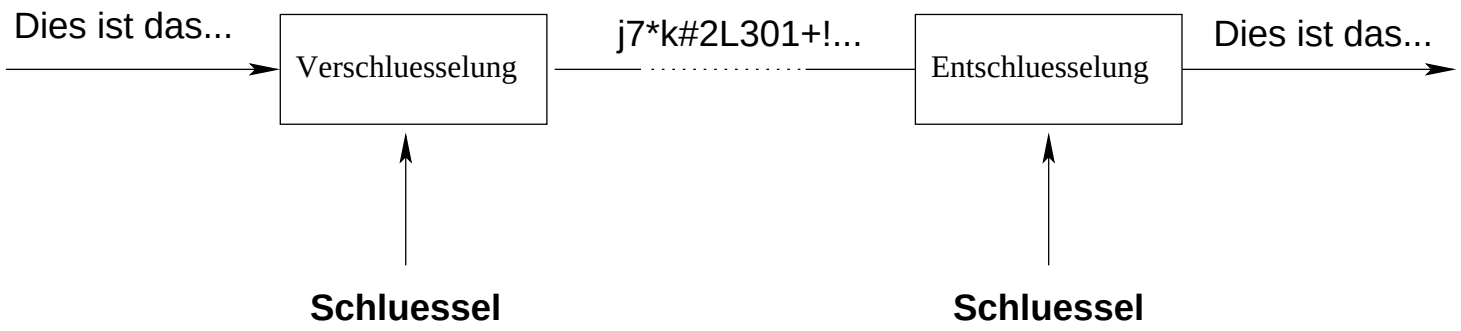
CH−8092 Zuerich


<capture> - Ethereal
File Edit Capture Display Tools Help
No. Time Source Destination Protocol SRC DST Info
19 14:08:37.1249 199.222.69.92 129.132.66.20 SMTP 25 46892 Response: 221 2.0.0 alias2.acm.org closing co
20 14:08:37.1250 129.132.66.20 199.222.69.92 TCP 46892 25 46892 > 25 [RST] Seq=141302659 Ack=0 Win=0 Le
21 14:08:37.1253 199.222.69.92 129.132.66.20 TCP 25 46892 25 > 46892 [FIN, ACK] Seq=1429201945 Ack=1413
22 14:08:37.1254 129.132.66.20 199.222.69.92 TCP 46892 25 46892 > 25 [RST] Seq=141302659 Ack=0 Win=0 Le
Frame 14 (893 on wire, 893 captured)
Ethernet II
Internet Protocol, Src Addr: 129.132.66.20 (129.132.66.20), Dst Addr: 199.222.69.92 (199.222.69.92)
Transmission Control Protocol, Src Port: 46892 (46892), Dst Port: 25 (25), Seq: 141301825, Ack: 1429201827, Len: 827
Simple Mail Transfer Protocol
Message: Received: (qmail 10073 invoked by uid 9289); 9 Apr 2003 12:08:35 -0000\r\n
Message: Date: Wed, 9 Apr 2003 14:08:35 +0200\r\n
Message: From: Arno Wagner <wagner@tik.ee.ethz.ch>\r\n
Message: To: arno.wagner@acm.org\r\n
Message: Subject: Geheimes Rezept\r\n
Message: Message-ID: <20030409120835.GA10061@tik.ee.ethz.ch>\r\n
Message: Mime-Version: 1.0\r\n
Message: Content-Type: text/plain; charset=us-ascii\r\n
Message: Content-Disposition: inline\r\n
Message: User-Agent: Mutt/1.5.3i\r\n
Message: \r\n
Message: Dies ist das geheime Rezept:\r\n
Message: \r\n
Message: Bla bla bla bla bla bla\r\n
Message: bla bla bla bla bla bla\r\n
Message: bla bla bla bla bla bla\r\n
Message: bla bla bla bla bla bla\r\n
0000 00 30 b6 37 01 b4 00 04 61 44 31 9e 08 00 45 00 .0.7.... aD1...E.
0010 03 6f 8d 96 40 00 40 06 d9 1f 81 84 42 14 c7 de .o..@.@. ....B...
0020 45 5c b7 2c 00 19 08 6c 18 41 55 2f e3 a3 80 18 E\.,...l .AU/....
0030 19 20 82 c5 00 00 01 01 08 0a 0a 34 9a b7 03 7d . ...4...}
0040 f0 9f 52 65 63 65 69 76 65 64 3a 20 28 71 6d 61 ..Receiv ed: (qma
Filter: Reset Apply File: <capture> Drops: 0

Wer Kann Email Mitlesen?

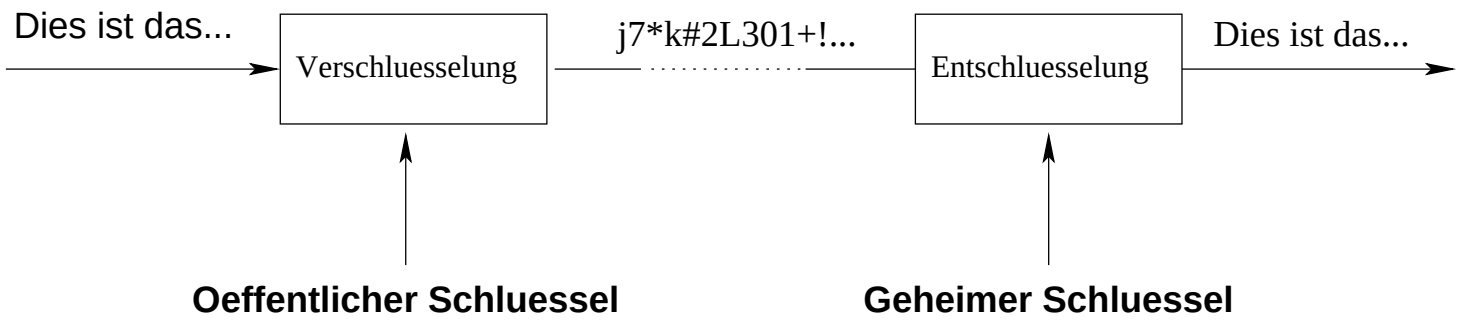
- Insider die z.B. das (W)LAN abhören
- Insider die Zugriff auf Mailserver haben
- Staatliche Stellen
- Geheimdienste (auch Industriespionage)

Verschlüsselung



- Macht Nachricht für Dritte unlesbar
- Benötigt einen gemeinsamen Schlüssel pro Beziehung

Verschlüsselung mit ”Public Key”



- Paare von Schlüsseln
- Verschlüsselung veröffentlichtem ”Public Key”.
- Entschlüsselung **nur** mit dem geheimen Schlüssel.

Zusätzlich: Elektronische Signatur möglich

Wann ist das Sicher?

- Öffentlicher Schlüssel ist korrekt zu Absender zugeordnet
- Geheimer Schlüssel ist geheim (Passphrase)

Für Signatur entsprechend.

Beschaffung Öffentlicher Schlüssel

- Direkte Übergabe
- Unzuverlässige Quellen (Keyserver, Email,...)
  - Erfordert Prüfung der Zuordnung
  - Direkt mit dem Besitzer: Fingerprint
  - Indirekt: Durch vertrauenswürdige Signatur
  - Indirekt: Durch eigene Signatur

Sicherheitsniveau

Sicherheit ist Abhängig vom Angreifer!

- Einzelpersonen?
- Kleinere Organisationen/Firmen?
- Grössere Organisationen?
- Gut ausgestattete Geheimdienste von Staaten?

Werkzeuge

- PGP (Pretty Good Privacy):
  `http://www.pgp.com/`
  `http://www.pgpi.org`
- GnuPG (Gnu Privacy Guard):
  `http://www.gnupg.org/`