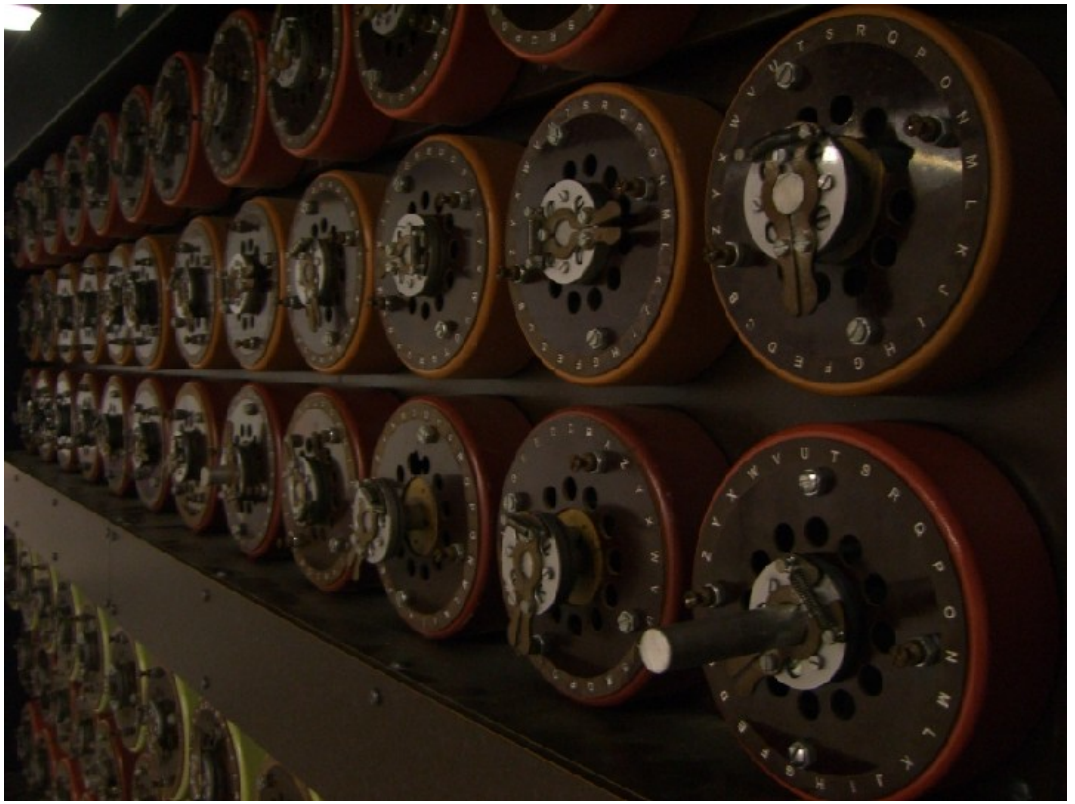


Sichere Kommunikation

Hamburg, 06.06.07

hinnerk@hamburg.ccc.de

»ab 2008 sollen alle Verbindungsdaten über Website-Besuche und E-Mail-Verkehr gespeichert werden«

Berliner Zeitung, 25.04.2007

Vorab

- Die Folien liegen im Wiki des CCC Hamburg.
- Fragen und Ergänzungen bitte an hinnerk@hamburg.ccc.de.

Totale Sicherheit ist ausgeschlossen.

Sicherheit ist ein Prozess,
kein Zustand

Eine Geschichte

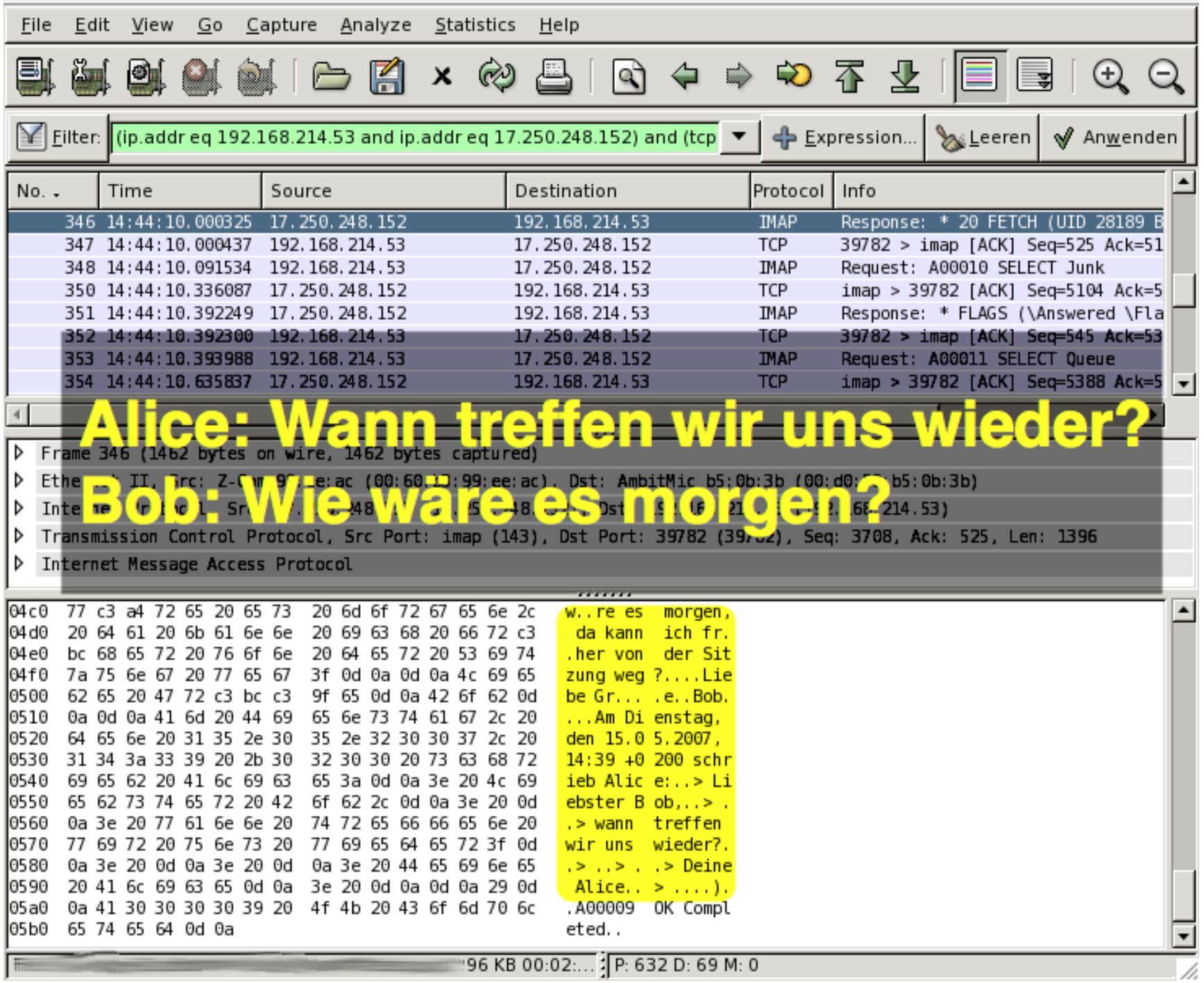
Alice liebt Bob

Bob hat bereits eine Frau.

Eve

Alice schickt Bob eine E-Mail

Eve lauscht am Netzwerk.


File Edit View Go Capture Analyze Statistics Help
Filter: (ip.addr eq 192.168.214.53 and ip.addr eq 17.250.248.152) and (tcp
Expression... Leeren Anwenden
No. Time Source Destination Protocol Info
346 14:44:10.000325 17.250.248.152 192.168.214.53 IMAP Response: * 20 FETCH (UID 28189 B
347 14:44:10.000437 192.168.214.53 17.250.248.152 TCP 39782 > imap [ACK] Seq=525 Ack=51
348 14:44:10.091534 192.168.214.53 17.250.248.152 IMAP Request: A00010 SELECT Junk
350 14:44:10.336087 17.250.248.152 192.168.214.53 TCP imap > 39782 [ACK] Seq=5104 Ack=5
351 14:44:10.392249 17.250.248.152 192.168.214.53 IMAP Response: * FLAGS (\Answered \Fla
352 14:44:10.392300 192.168.214.53 17.250.248.152 TCP 39782 > imap [ACK] Seq=545 Ack=53
353 14:44:10.393988 192.168.214.53 17.250.248.152 IMAP Request: A00011 SELECT Queue
354 14:44:10.635837 17.250.248.152 192.168.214.53 TCP imap > 39782 [ACK] Seq=5388 Ack=5
Alice: Wann treffen wir uns wieder?
Bob: Wie wäre es morgen?
Frame 346 (1462 bytes on wire, 1462 bytes captured)
Transmission Control Protocol, Src Port: imap (143), Dst Port: 39782 (39782), Seq: 3708, Ack: 525, Len: 1396
Internet Message Access Protocol
04c0 77 c3 a4 72 65 20 65 73 20 6d 6f 72 67 65 6e 2c w..re es morgen,
04d0 20 64 61 20 6b 61 6e 6e 20 69 63 68 20 66 72 c3 da kann ich fr.
04e0 bc 68 65 72 20 76 6f 6e 20 64 65 72 20 53 69 74 .her von der Sit
04f0 7a 75 6e 67 20 77 65 67 3f 0d 0a 0d 0a 4c 69 65 zung weg ?....Lie
0500 62 65 20 47 72 c3 bc c3 9f 65 0d 0a 42 6f 62 0d be Gr... .e..Bob.
0510 0a 0d 0a 41 6d 20 44 69 65 6e 73 74 61 67 2c 20 ...Am Di enstag,
0520 64 65 6e 20 31 35 2e 30 35 2e 32 30 30 37 2c 20 den 15.0 5.2007,
0530 31 34 3a 33 39 20 2b 30 32 30 30 20 73 63 68 72 14:39 +0 200 schr
0540 69 65 62 20 41 6c 69 63 65 3a 0d 0a 3e 20 4c 69 ieb Alic e:..> Li
0550 65 62 73 74 65 72 20 42 6f 62 2c 0d 0a 3e 20 0d ebster B ob,..> .
0560 0a 3e 20 77 61 6e 6e 20 74 72 65 66 66 65 6e 20 .> wann treffen
0570 77 69 72 20 75 6e 73 20 77 69 65 64 65 72 3f 0d wir uns wieder?.
0580 0a 3e 20 0d 0a 3e 20 0d 0a 3e 20 44 65 69 6e 65 .> ..> . .> Deine
0590 20 41 6c 69 63 65 0d 0a 3e 20 0d 0a 0d 0a 29 0d Alice.. > ....).
05a0 0a 41 30 30 30 30 39 20 4f 4b 20 43 6f 6d 70 6c .A00009 OK Compl
05b0 65 74 65 64 0d 0a eted..
96 KB 00:02:...
P: 632 D: 69 M: 0

Eve: »Wer ist eigentlich Alice?«

Bob: »Eine Bekannte.

Eve: »So so.«

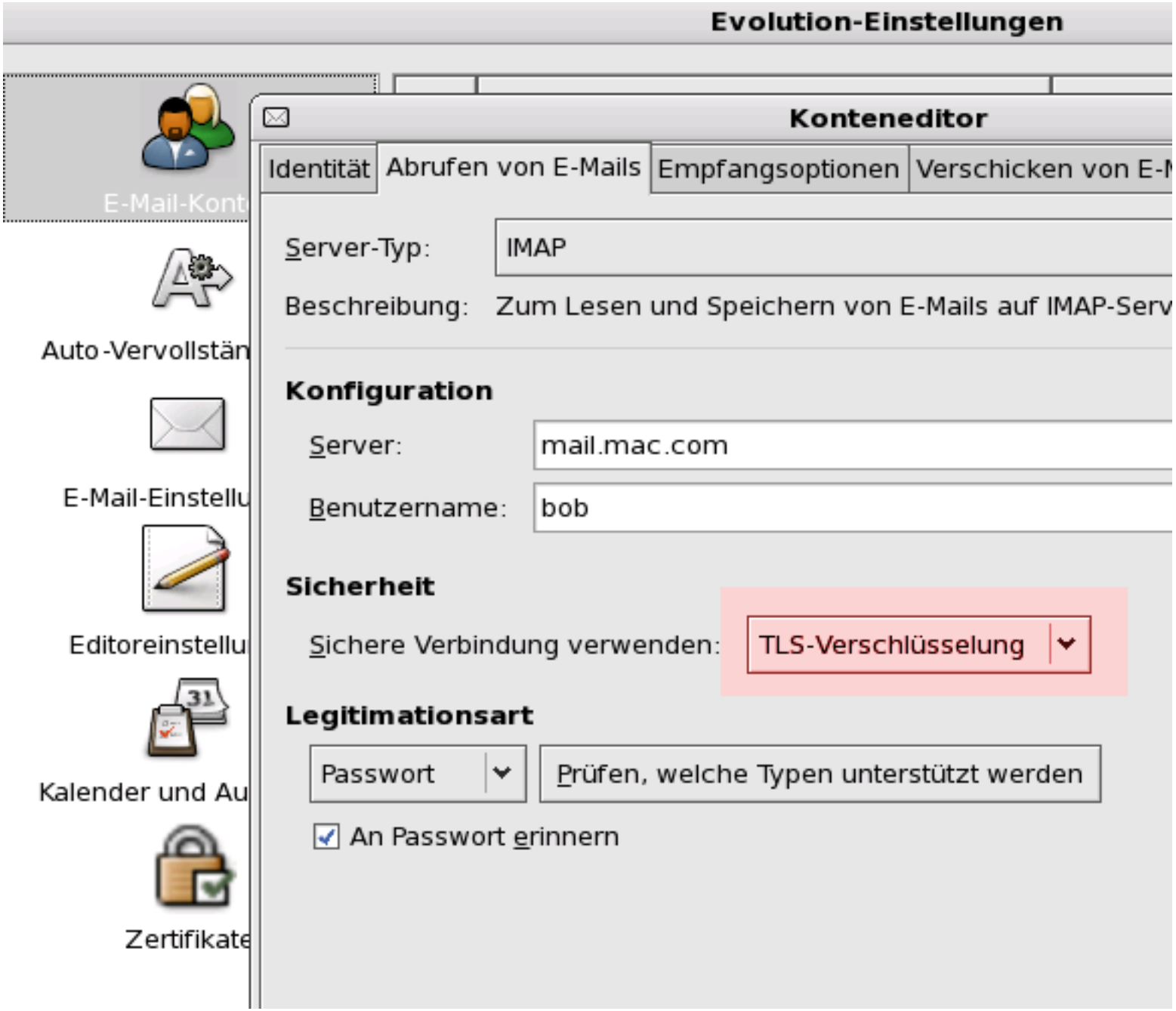
Bob: »Woher kennst Du sie denn?«

Eve: »Uhhh...«

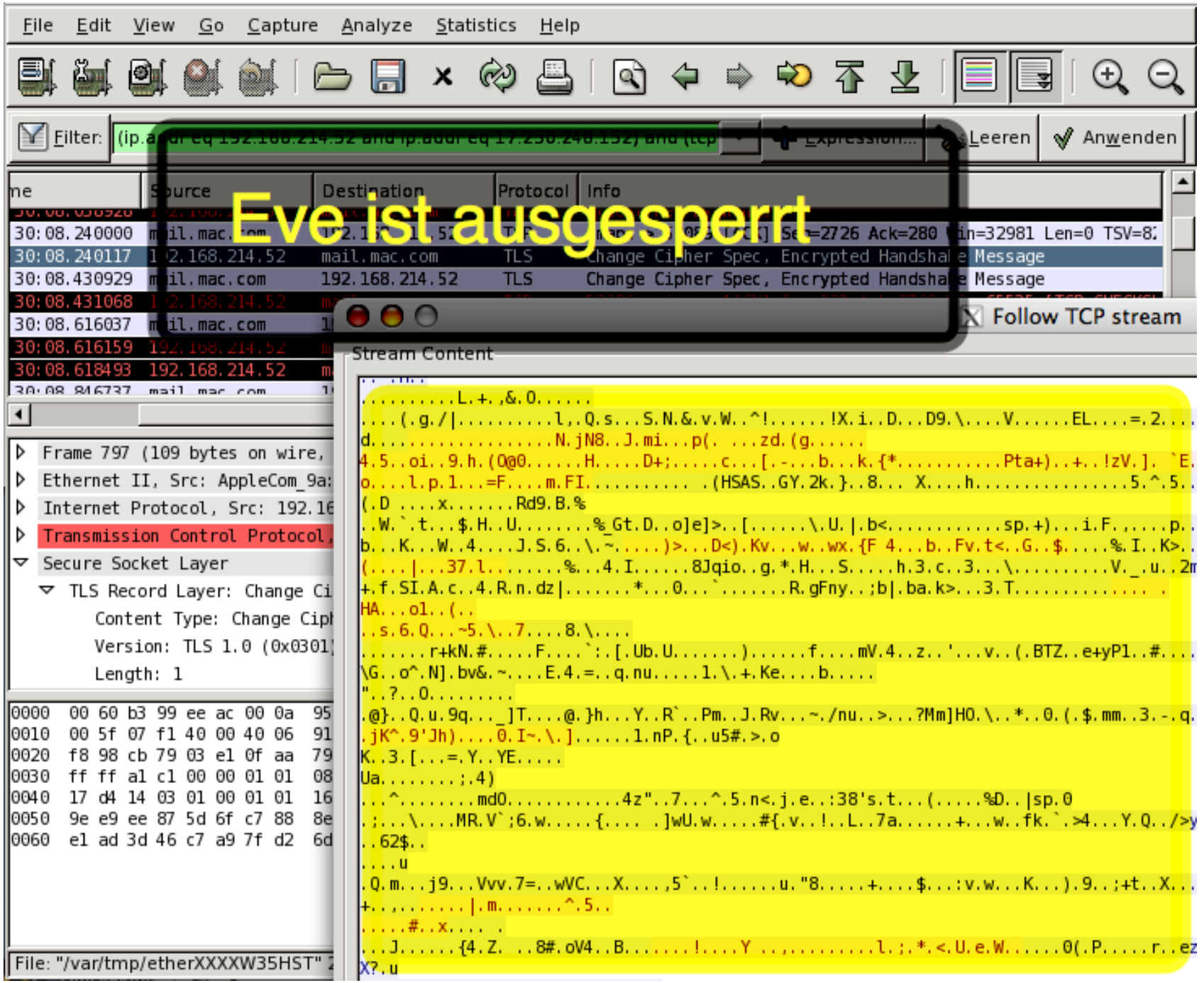
Merke

- Unverschlüsselte Netzwerke sind leicht abzuhören.
- Am Netzwerk zu lauschen ist automatisierbar, es erfordert keine Sachkenntnis.
- Abhörprofis nutzen ihre Informationen indirekt.

Bob trifft Gegenmaßnahmen


Evolution-Einstellungen
E-Mail-Kont
Auto-Vervollstän
E-Mail-Einstellu
Editoreinstellu
Kalender und Au
Zertifikate
Konteneditor
Identität
Abrufen von E-Mails
Empfangsoptionen
Verschicken von E-M
Server-Typ:
IMAP
Beschreibung:
Zum Lesen und Speichern von E-Mails auf IMAP-Serv
Konfiguration
Server:
mail.mac.com
Benutzername:
bob
Sicherheit
Sichere Verbindung verwenden:
TLS-Verschlüsselung
Legitimationsart
Passwort
Prüfen, welche Typen unterstützt werden
An Passwort erinnern

Eve lauscht wieder am Netzwerk...


File Edit View Go Capture Analyze Statistics Help
Filter:
Expression...
Leeren
Anwenden
Source
Destination
Protocol
Info
30:08.240000 mail.mac.com
30:08.240117 192.168.214.52 mail.mac.com TLS Change Cipher Spec, Encrypted Handshake Message
30:08.430929 mail.mac.com 192.168.214.52 TLS Change Cipher Spec, Encrypted Handshake Message
30:08.431068
30:08.616037 mail.mac.com
30:08.616159 192.168.214.52
30:08.618493 192.168.214.52
Eve ist ausgesperrt
Follow TCP stream
Stream Content
Frame 797 (109 bytes on wire,
Ethernet II, Src: AppleCom_9a:
Internet Protocol, Src: 192.16
Transmission Control Protocol,
Secure Socket Layer
TLS Record Layer: Change Ci
Content Type: Change Cip
Version: TLS 1.0 (0x0301)
Length: 1
0000 00 60 b3 99 ee ac 00 0a
0010 00 5f 07 f1 40 00 40 06
0020 f8 98 cb 79 03 e1 0f aa
0030 ff ff a1 c1 00 00 01 01
0040 17 d4 14 03 01 00 01 01
0050 9e e9 ee 87 5d 6f c7 88
0060 e1 ad 3d 46 c7 a9 7f d2
File: "/var/tmp/etherXXXXW35HST"

Aus ihrem ersten Lauschangriff hat Eve das Passwort von Bob.

Bob hat sein Passwort geändert, als er die Verschlüsselung eingeschaltet hat.

Umfrage

Hat hier jemand ein Passwort, das seit mehr als einem Jahr in Gebrauch ist?

Benutzt jemand ein Passwort für mehr als einen Account?

Benutzt jemand ein Passwort aus einem natürlichen Wort, oder eines mit weniger als 12 Zeichen?

Zurück zu Bob, Eve und Alice

Alice und Bob treffen sich in einem Café.

Zufällig treffen sie auf den Chef von Alice.

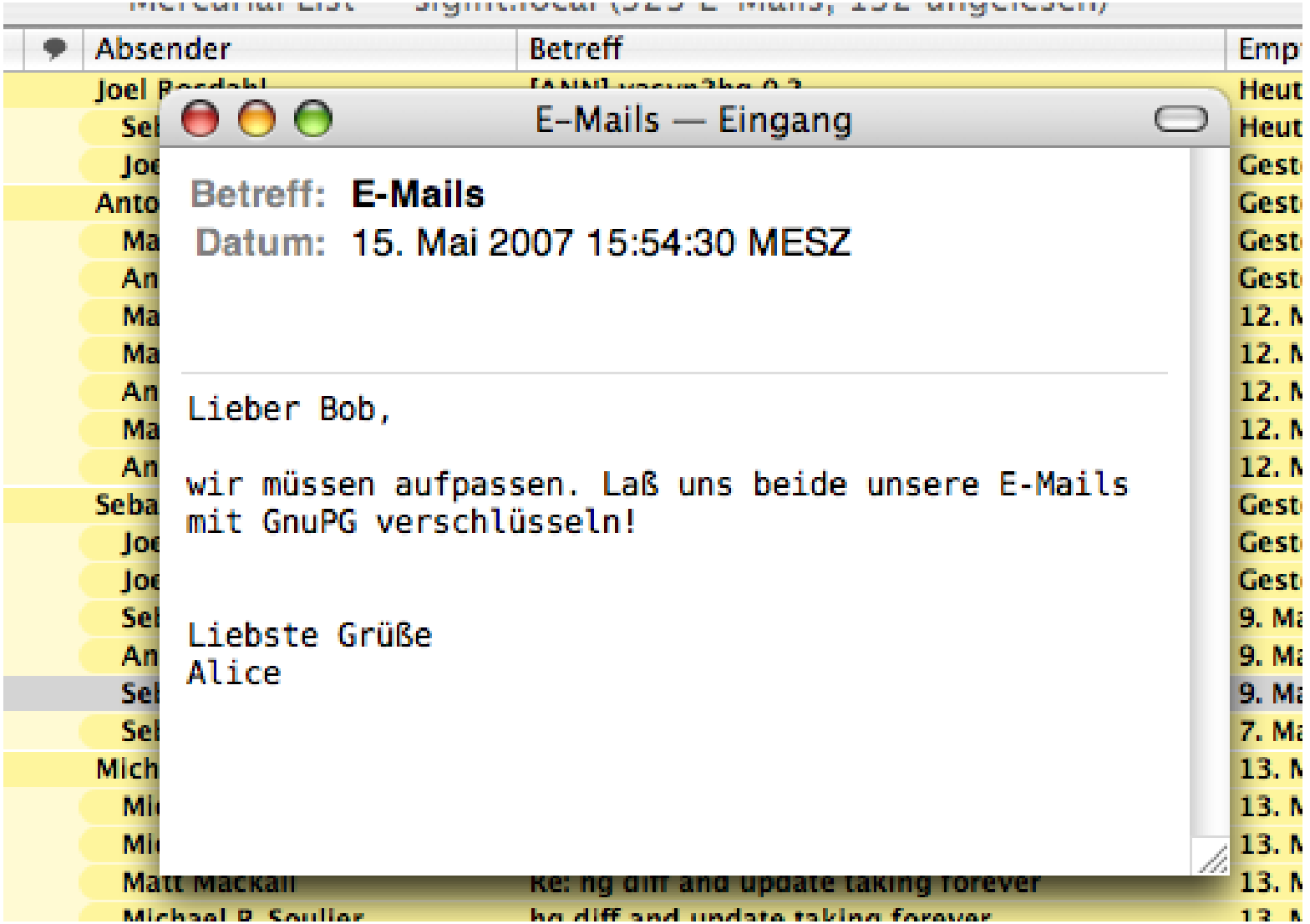
Der Chef mag Alice gern.

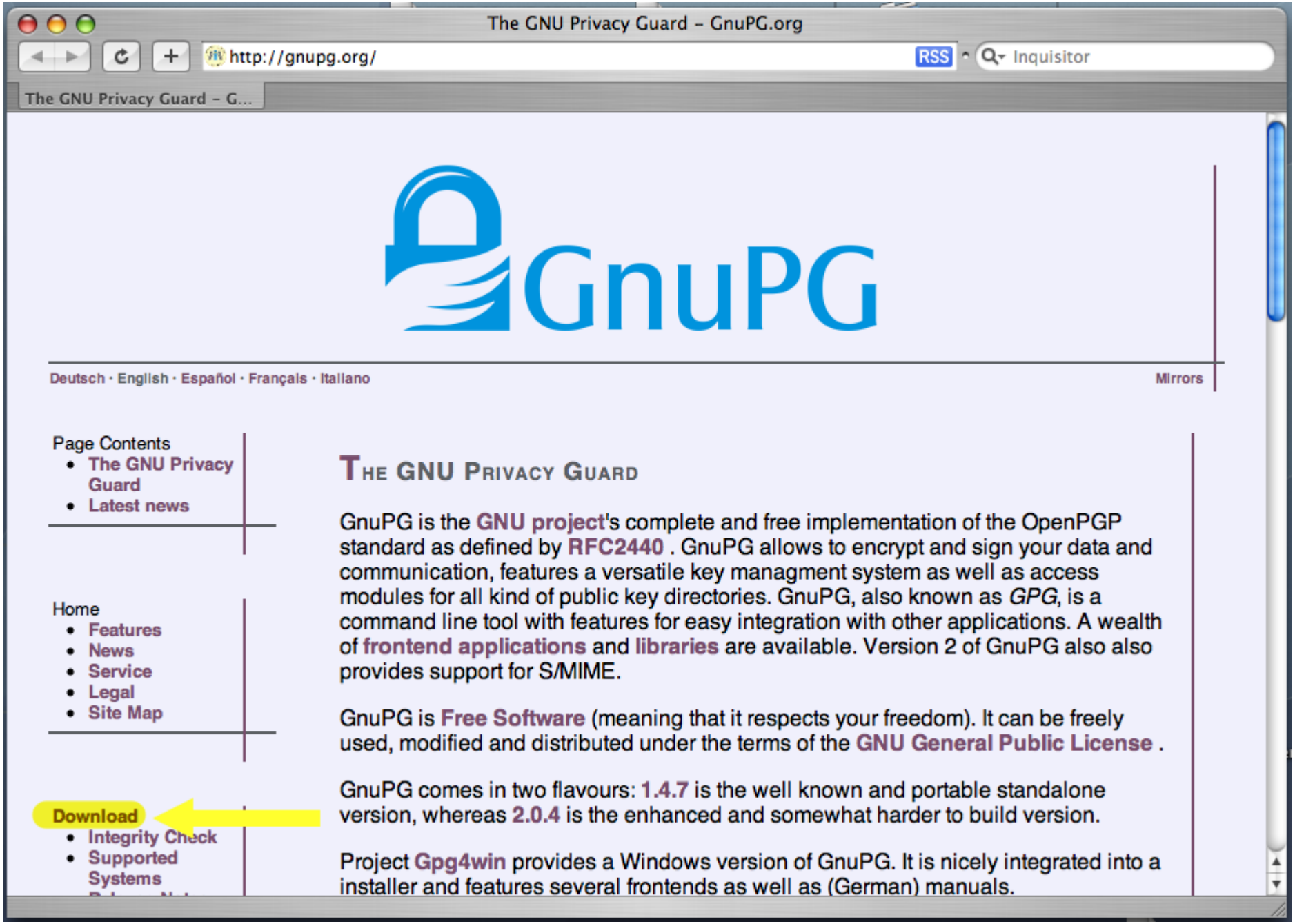
Bob wird auf ihren Chef eifersüchtig.

Alice ist mißtrauisch.

War das Zusammentreffen ein Zufall?

Liest ihr Chef ihre E-Mail?


Absender
Betreff
E-Mails — Eingang
Betreff: E-Mails
Datum: 15. Mai 2007 15:54:30 MESZ
Lieber Bob,
wir müssen aufpassen. Laß uns beide unsere E-Mails mit GnuPG verschlüsseln!
Liebste Grüße
Alice

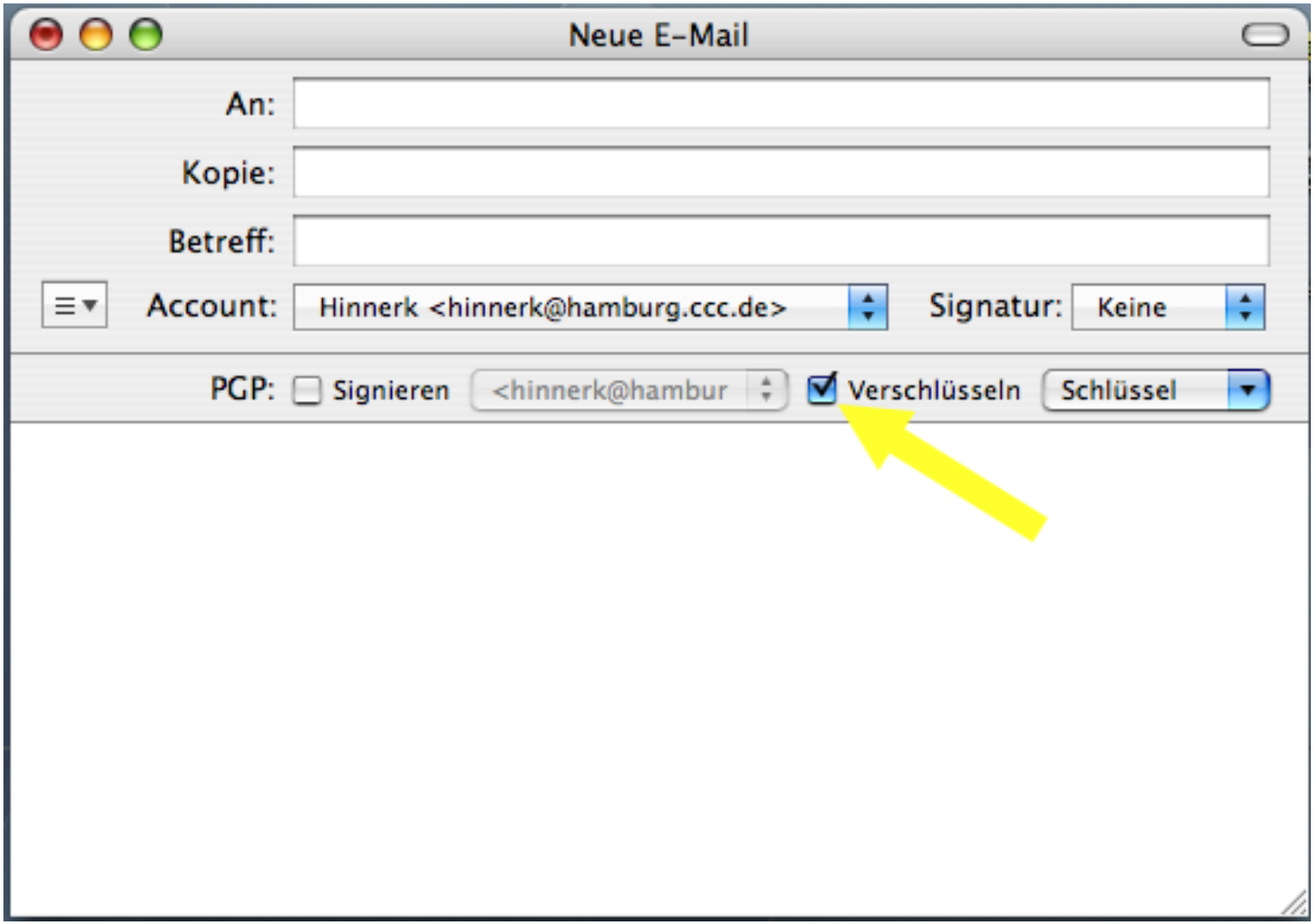


GnuPG - GNU Privacy Guard

Bob: »Ist installiert. Was nun?«

Alice lädt ihren Schlüssel auf einen öffentlichen Server.

Bob lädt den Schüssel von Alice vom Server.

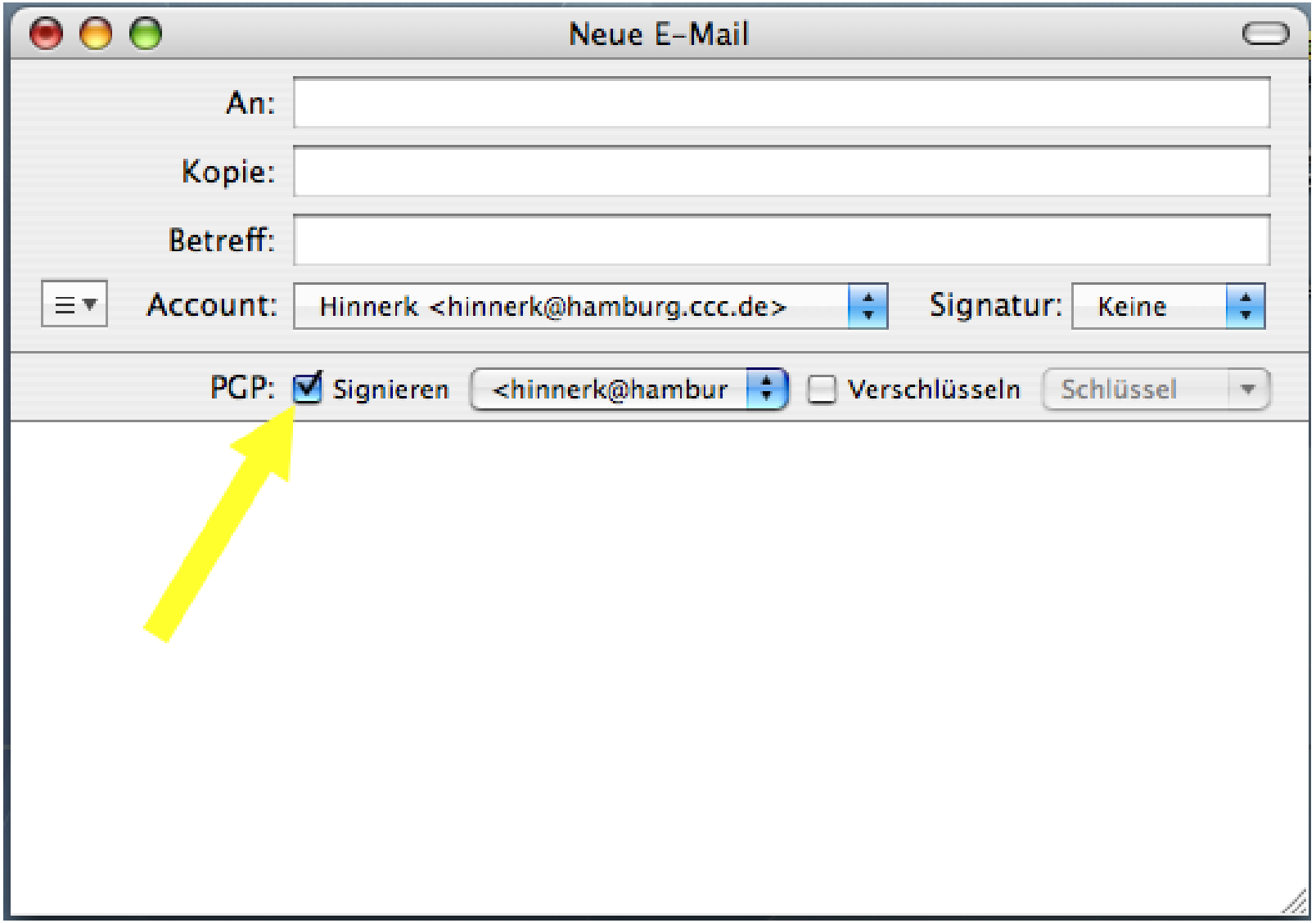

Neue E-Mail
An:
Kopie:
Betreff:
Account:
Hinnerk <hinnerk@hamburg.ccc.de>
Signatur:
Keine
PGP:
Signieren
<hinnerk@hambur
Verschlüsseln
Schlüssel

Der Chef von Alice lädt ihren Schlüssel vom Server.

Alice bekommt eine verschlüsselte E-Mail von Bob, in der er sie um ein Treffen bittet.

Statt Bob taucht ihr Chef zum Treffen auf.

Wie kann Alice feststellen, ob eine E-Mail tatsächlich von Bob kam?


Neue E-Mail
An:
Kopie:
Betreff:
Account:
Hinnerk <hinnerk@hamburg.ccc.de>
Signatur:
Keine
PGP:
Signieren
<hinnerk@hambur
Verschlüsseln
Schlüssel

Woher weiß Alice, daß der Schlüssel tatsächlich Bob gehört?

```
$ gpg --fingerprint bob
pub   1024D/9892D76B 2007-05-15 [expires: 2008-05-14]
  Schl.-Fingerabdruck =  28D8 E963 BA41 A71F D0AC  61C8
                         8EEA 6FA9 9892 D76B
uid                  Bob Meier (Der Gutmensch)
<bob@spamcatcher.local>
sub   4096g/59EBC95F 2007-05-15 [expires: 2008-05-14]
```

Per Telefon vergleichen Bob und Alice die Fingerabdrücke ihrer Schlüssel.

Bob und Alice senden nur noch verschlüsselte und unterschriebene E-Mails.

Der Chef von Alice kann trotzdem:

- Empfänger und Absender lesen und ändern.
- Den Betreff der Nachrichten lesen und ändern.

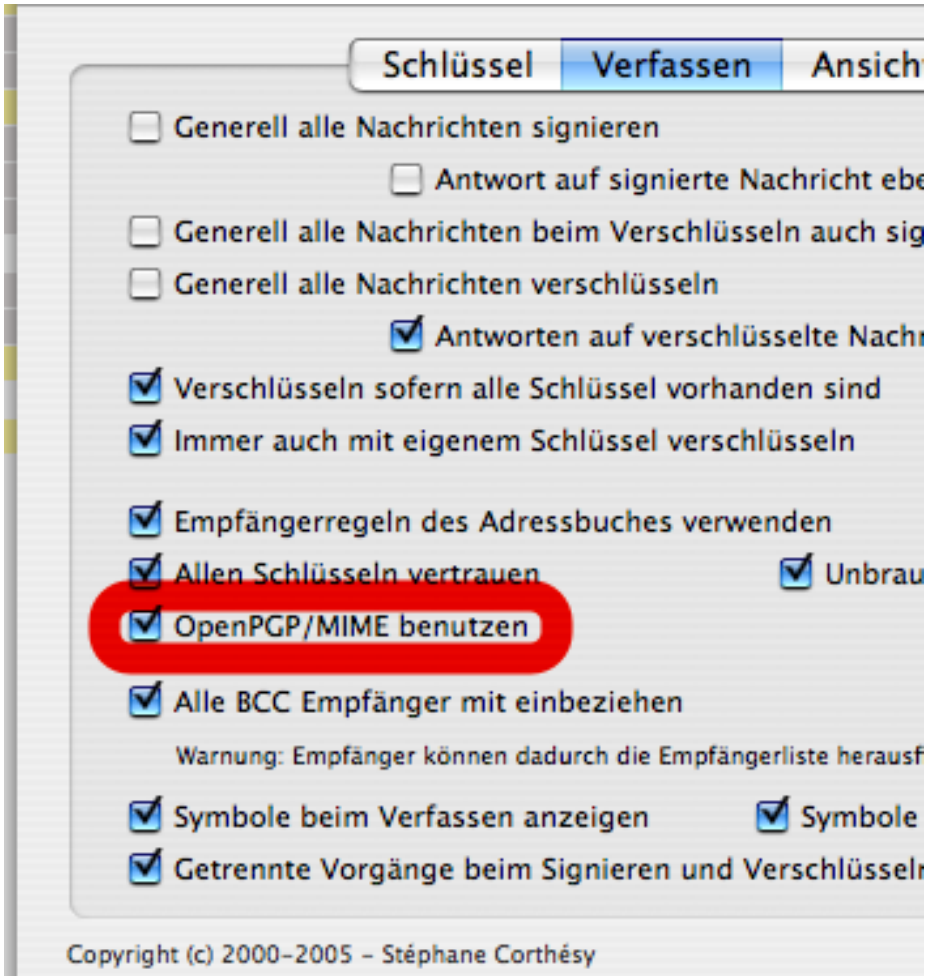
Eve könnte das nicht, weil Bob zusätzlich den Übertragungskanal sichert.

Merke

- Ein **sicherer Kanal** schützt nur die unmittelbare Übertragung, nicht die gespeicherte oder weitergeleitete Nachricht.
- Eine **sichere Nachricht** schützt nicht zusätzlich übertragene Daten (Empfänger, Sender, Passwort, ggf. Betreff).

GnuPG: Technische Details

- Verschlüsselte Nachrichten und Webmailer sind problematisch.
- Nur mit PGP/MIME werden auch angehängte Dateien verschlüsselt.



Zurück zu Eve.

Eve will wissen was los ist und fragt einen Privatdetektiv.

Angebot 1:

- Die Installation einer Wanze in der Tastatur von Bobs Rechner. Damit werden alle Tastendrücke (Passwörter, geschriebene E-Mails, etc.) aufgezeichnet.
- Hardwarewanzen sind per Software nicht zu entdecken, setzen aber für Einbau und zur Abfrage der Daten Zugriff auf das Gerät voraus.

Angebot 2: Abhörsoftware

- Installation einer Software, die alle anfallenden Daten sammelt (Passwörter, empfangene E-Mails, ...)
- Ist vielleicht durch Software zu entdecken.
- Kann meist ohne Zugriff auf den Rechner eingespielt werden.

Bob wundert sich über hohe Netzwerklast.

Ein Computerspezialist findet auf Bobs Computer eine Abhörsoftware.

Nach einer heftigen Aussprache mit Eve zieht Bob zu Alice.

Eve hat alle alten Daten von Bob.

Bob muß alle Schlüssel zurückziehen, neue Schlüssel erstellen, alle Passwörter auswechseln und das ganze System auf seinem Computer neu aufsetzen.

Seine Daten kann er nicht zurückziehen.

Mit den von Bob und Alice unterschriebenen E-Mails als Beweis reicht Eve die Scheidung ein.

Merke

- Wenn das System kompromittiert ist, gibt es keinen Schutz.
- Veröffentlichte Daten können nicht zurückgezogen werden.

Technischer Lösungsansatz

- Ein Rechner mit Verschlüsselungssoftware ohne Netzwerk für vertrauliche Daten.
- Ein Rechner für Netzwerkzugriff für Versand und Empfang von Daten.
- Verschlüsselte Daten per Medium (z.B. USB-Stick) übertragen.

Technologieüberblick

GnuPG und PGP

- GnuPG und PGP sind halbwegs kompatibel.
- GnuPG ist kostenlos. PGP ein kommerzielles Produkt.
- Der Quellcode von GnuPG liegt offen und kann nach Fehlern und Schadcode durchsucht werden.

S/MIME

- Technisch und von der Sicherheit her mit GnuPG und PGP vergleichbar.
- Nicht mit GnuPG und PGP kompatibel.
- Wird eher in Behörden und Unternehmen verwendet.
- Qualifizierte digitale Signaturen nach S/MIME-Standard sind der handschriftlichen Unterschrift gleichgestellt (SigG, SigV, BGB, ...).


98580 © DSV 05/06 EPC/GD
Bankleitzahl 200 505 50
electronic cash
GeldKarte
TRUST

Pause?

Instant Messaging
(IM)

AIM, ICQ, MSN, Yahoo Messenger,
web.de, gmx, Google, ...

Kommunikation über den Server des Anbieters.

Meist kein sicherer Kanal möglich.

Verträge sehen oft das Abhören durch Anbieter und das Übernehmen von übertragenen Inhalten(!) durch den Anbieter vor.

Alternative: Eigener Jabberserver

Nachrichtensicherheit ist vom Server unabhängig.

IM: Software

- Adium, Gaim/Pidgin mit OTR
- OTR Proxy für AIM
- Trillian SecureIM: Keine Signaturen
- Gaim-encryption: GnuPG/PGP
- SILC: Kein IM

Off The Record (OTR)

- Relativ neues Protokoll.
- Abgefangene Kommunikation kann nicht nachträglich entschlüsselt werden, auch wenn die Schlüssel der Beteiligten bekannt werden (»perfect forward secrecy«).
- Während der Kommunikation ist der Kommunikationspartner feststellbar, später nicht mehr (»deniability«).

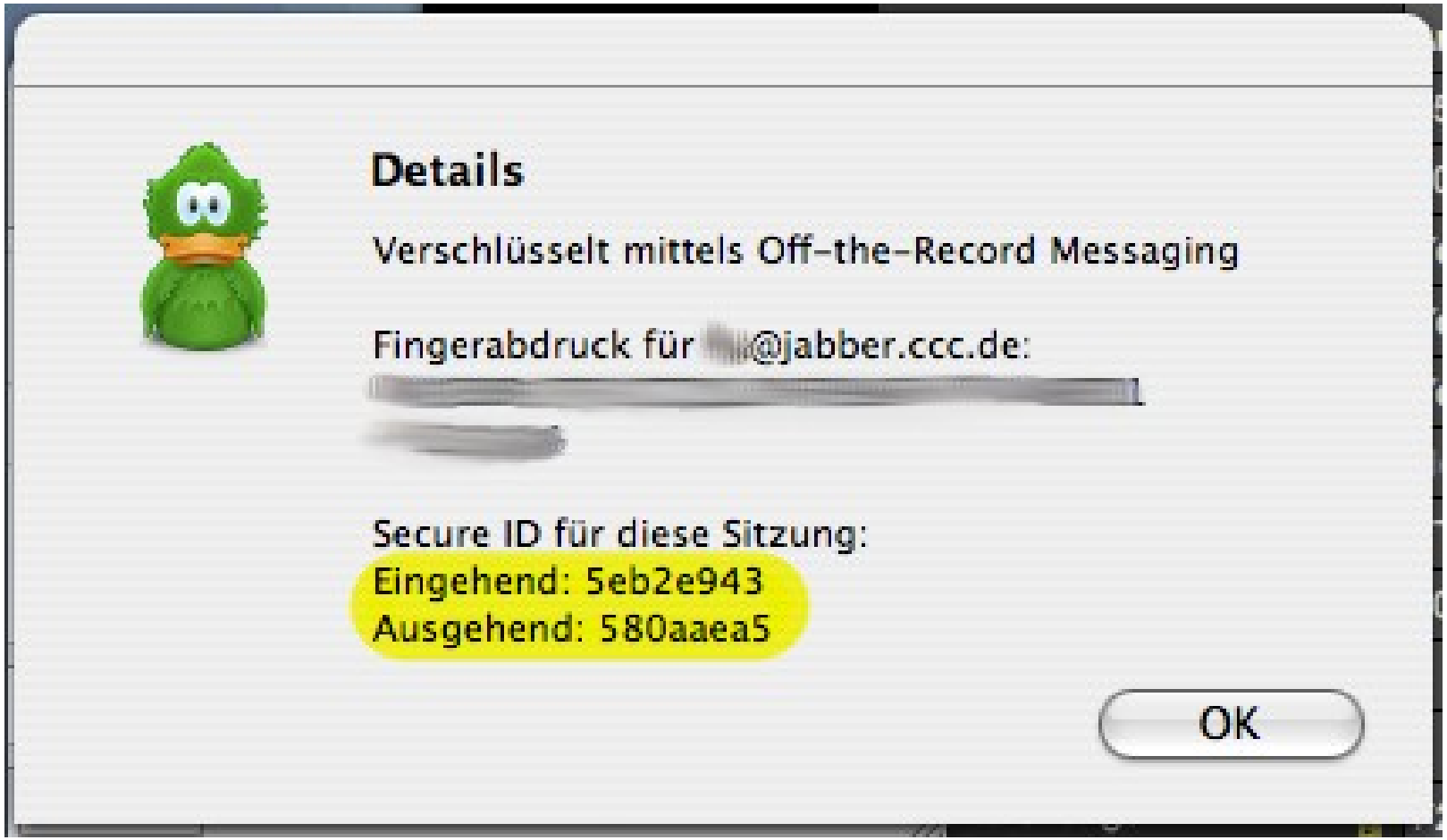

Katrin
Hinnerk
13:47
Hi
Verschlüsselter OTR Chat eingeleitet.
13:47
Katrin
13:47
Die folgende Nachricht war nicht verschlüsselt:Huhu!
Katrin

OTR verwendet Fingerabdrücke ähnlich wie GnuPG und PGP.


OTR Fingerabdrucküberprüfung
Ihr Fingerabdruck @jabber.ccc.de): 580aaea5
Angegebener Fingerabdruck für
@jabber.ccc.de: 5eb2e943
Ist dies der bestätigte korrekte Fingerabdruck
für @jabber.ccc.de?
Hilfe
Nein
Ja

OTR: »Secure ID«

- Festzustellen, ob ein Chat abgehört wird.
- Auch bei kompromittierten Schlüsseln sicher.
- Muß während des Gespräches verglichen werden.
- Nur die eigene Hälfte vorlesen, die andere vorlesen lassen.


Details
Verschlüsselt mittels Off-the-Record Messaging
Fingerabdruck für [redacted]@jabber.ccc.de:
[redacted]
Secure ID für diese Sitzung:
Eingehend: 5eb2e943
Ausgehend: 580aaea5
OK

Telefonie

Analoges Telefon und ISDN

- Abhören ist einfach und billig.
- Propritäre Sicherheitsprodukte vorhanden.
  - Teuer, die Sicherheit ist fragwürdig.
- Offene Produkte basieren auf Rechner + Modem.

Secure Telefon Unit (STU-III)

Secure Terminal Equipment (STE)

Mobiltelefonie

- Abhören ist für Privatmenschen illegal, für staatliche Stellen Routine.
- Gegenmittel: Cryptophone
- Teuer, aber mit Quellcode.
- Exportrestriktionen.

Pager

- Analoge Pager lassen sich mit einfachsten Mitteln abhören.
- Digitale Pager lassen sich auch abhören, es wird nur teurer.
- Solitaire ist ein Stift-und-Papier-Verschlüsselungsalgorithmus.

Internettelefonie

Skype

- Widersetzt sich der Analyse.
- Skype Inc. kann Kommunikation entschlüsseln.
- Mehr hier: Paper "Silver Needle in the Skype"

Voice over IP (VoIP)

- Praktisch alle Protokolle sind unverschlüsselt.
- Hardware (WLAN-Telefone, ...) unterstützt noch keine Verschlüsselung.
- Für rechnerbasierte Kommunikation: ZRTP

ZRTP

- Eingeführt mit Zfone (Phill Zimmermann)
- ZRTP verschlüsselt den Mediendatenstrom von SIP, Jabber, H.323 etc.
- Windows, Linux, Mac OS X
- Offene Lizenz, Offener Quellcode, kostenlose Software

Was fehlt noch?

- Festplattenverschlüsselung
- Sicherheit gegen Verkehrsanalyse (Tor, JAP, Freenet, IIP)

Anhang

Quellen

- Titelbild: Rotoren einer Bombe, Photographie von James Morris
- Alice & Bob nach Wikipedia: Alice und Bob
- STU-III und STE aus der Wikipedia

Alice & Bob

- Alice und Bob sind gewöhnliche Beteiligte
- Carol und Dave sind die dritte und vierte Partei
- Eve ist ein passiver Angreifer
- Mallory, Marvin, Mallet, Oscar oder Oskar sind aktive Angreifer
- Trudy ist ein Eindringling
- Trent ist ein vertrauenswürdiger Dritter

Nach: Wikipedia: Alice und Bob

Schlüsselerzeugung mit GnuPG

```
$ gpg --gen-key
```

```
gpg (GnuPG) 1.4.7; Copyright (C) 2006
[...]

Bitte wählen Sie, welche Art von Schlüssel
Sie möchten:
   (1) DSA and Elgamal (default)
   (2) DSA (nur signieren/beglaubigen)
   (5) RSA (nur signieren/beglaubigen)
Ihre Auswahl? 1
```

```
DSA keypair will have 1024 bits.
ELG-E keys may be between 1024 and 4096
bits long.
What keysize do you want? (2048) 4096
```

```
Requested keysize is 4096 bits
Please specify how long the key should be
valid.
         0 = key does not expire
       <n>  = key expires in n days
       <n>w = key expires in n weeks
       <n>m = key expires in n months
       <n>y = key expires in n years
Key is valid for? (0) 1y
```

```
Key expires at Wed May 14 16:36:14 2008
CEST
Is this correct? (y/N) y
```

```
You need a user ID to identify your key;
the software constructs the user ID
from the Real Name, Comment and Email
Address in this form:
    "Heinrich Heine (Der Dichter)
<heinrichh@duesseldorf.de>"

Real name: Bob Meier
Email address: bob@spamcatcher.local
Comment: Der Gutmensch
```

```
You selected this USER-ID:

Bob Meier (Der Gutmensch) <bob@spamcatcher.local>"

Change (N)ame, (C)omment, (E)mail or
(O)kay/(Q)uit? O
```

```
You need a Passphrase to protect your
secret key.

Enter passphrase:
Repeat passphrase:
```

We need to generate a lot of random bytes. It is a good idea to perform some other action (type on the keyboard, move the mouse, utilize the disks) during the prime generation; this gives the random number generator a better chance to gain enough entropy.

```
.++++++++++++++++.++++++++++++++++++++++++
+++++.+++++..+++++++++++++++++++..+++++++
++++++++++++++++++++++++++++++++++++++++++
+.++++++++++>++++++++++..>+++++<+++++....>
+++++.................+++++
```

```
gpg: key 9892D76B marked as ultimately trusted
public and secret key created and signed.

gpg: checking the trustdb
gpg: 3 marginal(s) needed, 1 complete(s) needed, PGP trust
model
gpg: depth: 0  valid:   1  signed:   0  trust: 0-, 0q, 0n,
0m, 0f, 1u
gpg: next trustdb check due at 2008-05-14
pub   1024D/9892D76B 2007-05-15 [expires: 2008-05-14]
      Key fingerprint = 28D8 E963 BA41 A71F D0AC  61C8
                        8EEA 6FA9 9892 D76B
uid   Bob Meier (Der Gutmensch) <bob@spamcatcher.local>
sub   4096g/59EBC95F 2007-05-15 [expires: 2008-05-14]
```