

Digitale Selbstverteidigung

eine Einführung

Jens-Wolfhard Schicke-Uffmann

6. September 2013

Grundsätzliches

-  Selbst durch gesetzliche Änderungen in Deutschland werden ausländische Geheimdienste ihre Arbeit nicht einstellen
-  Digitale Selbstverteidigung ist *ein* Baustein des freien demokratischen Meinungsaustauschs
-  Politische Lösungen sind zusätzlich nötig, um die geheimdienstliche Überwachung der Bevölkerung abzustellen

Die eigenen Grenzen kennen

Heutiger Inhalt:

- ✚ Tempora (UK), Technikaufwuchsprogramm (DE), SORM-II (RU), u.ä.
- ✚ PRISM (US)
- ✚ Trojaner, Viren, Würmer
- ✚ gezielte Ermittlungsarbeit
- ✚ Telefonie, Mobiltelefone

Bei Unsicherheit:

- 🗨 Die ganz geheimen Dinge bespricht man am besten ohne Handys irgendwo auf einem Feldweg

Das Ziel für heute: Eine Mail schreiben können, ohne dass die Geheimdienste der Welt mitlesen.

Nur weil du verschlüsselst...

... heißt das nicht, dass SIE dich nicht abhören können (aber dass es teurer für SIE ist).

-  Absichtlich eingebaute Hintertüren
-  Trojaner und Rootkits
-  Wanzen, Keylogger
-  Elektromagnetische Abstrahlung
-  Human Intelligence

Webdiensteanbieter

-  Daten bei Dritten sind nie sicher
-  PRISM: **Microsoft**, Yahoo, Google, Facebook, PalTalk, YouTube, Skype, AOL, **Apple**

Softwareauswahl

OpenSource:

-  Jeder kann die Quellen lesen
-  Es gibt unabhängige Sicherheitsforscher, die das auch tun
-  Trotzdem jede Menge Lücken
-  ... die zeitnah behoben werden.

Die Alternative:

-  <https://en.wikipedia.org/wiki/NSAKEY>
-  https://en.wikipedia.org/wiki/IBM_Notes#Security

Mailverschlüsselung

Ungefähre Analogien:

-  Unverschlüsselte Mail: Postkarten mit Bleistift beschreiben
-  Signierte Mail: Kugelschreiber und Unterschrift
-  Verschlüsselte Mail: Brief

Webmail

-  Webbasierte Verschlüsselungssoftware ist nicht vertrauenswürdig
-  Admins können mitlesen
-  Geheimdienste können mitlesen
-  Ermittlungsbehörden können mitlesen

Das Problem mit den Metadaten

Mailverschlüsselung bezieht sich **nur** auf den Inhalt, nicht auf

-  Absender
-  ... inklusive IPs zwischengeschalteter Server
-  Betreff
-  Mailclient und andere identifizierende Merkmale
-  Zeitpunkt der Kommunikation

Public-Key Kryptographie

Jeder Teilnehmer hat:



Privaten Schlüssel



Öffentlichen Schlüssel

Verschlüsselt wird mit dem öffentlichen Schlüssel.

Entschlüsselt wird mit dem privaten Schlüssel.

Signiert wird mit dem privaten Schlüssel.

Public-Key Kryptographie

Jeder Teilnehmer hat:



Privaten Schlüssel



Öffentlichen Schlüssel

Verschlüsselt wird mit **dem** öffentlichen Schlüssel.

Entschlüsselt wird mit dem privaten Schlüssel.

Signiert wird mit dem privaten Schlüssel.

Schlüsselsignaturen (und Netzwerkanalyse)

Um sicher zu stellen, dass man den richtigen Schlüssel hat

 Fingerprints vergleichen

 Signaturen anderer auf dem Schlüssel überprüfen

Problem bei Schlüsselsignaturen: Das soziale Netzwerk wird sichtbar.

PGP & Enigmail

“Pretty Good Privacy”

 <http://openpgp.org/>

 GnuPG als OpenSource-Implementation

 Konkrete Ausgestaltung eines Public-Key Verfahrens

Enigmail

 PGP-Plugin für Thunderbird und SeaMonkey

 Benötigt eine GnuPG-Installation

 <http://www.enigmail.net>

GunPG installieren

-  Linux Debian: `apt-get install gnupg`
-  Windows: <http://www.gpg4win.org/>
-  Mac OS X: <https://gpgtools.org/>

Enigmail installieren

-  Runterladen: <http://www.enigmail.net/download/>
-  Plugin installieren: "Tools", "Add-ons", "Install"
-  Schlüssel erzeugen: "OpenPGP", "Key Management", "Generate", "New Key Pair"
-  Passwort setzen
-  Revocation Certificate generieren
-  Eigenen Schlüssel signieren
-  Schlüssel veröffentlichen: Eigene Adresse suchen, "Keyserver", "Upload public keys"

Andere Systeme

Sehr deutlich nicht empfohlen!

Outlook:

 <https://www.symantec.com/desktop-email-encryption/>
(Kein Open Source)

 <https://code.google.com/p/outlook-privacy-plugin/>
(Outlook 2010 und 2013)

 <http://www.gpg4win.org/> und GpgOL
(Outlook 2003 und 2007)

Mac:

 <https://gpgtools.org/gpgmail/index.html>

Anonymisiertes Browsing

Anwendungsfälle:

-  Anonyme Mails schreiben
-  Anonyme Veröffentlichungen (z.B. via pastebin)
-  Regimekritische Webseiten besuchen

Offensichtliches:

-  Cookies, HTML5 Local Storage, Flash Local Storage verhindern
-  Nirgends einloggen (außer mit gesonderten Accounts)
-  Nicht den eigenen Namen unter Beiträge schreiben
-  Keine unnötige private Korrespondenz
-  Längere Texte in ungewöhnlichem Stil verfassen

Browser Identification

-  <https://panopticklick.eff.org/>
-  Browserversion, Plugin-Versionen, Installierte Fonts, Bildschirmgröße, etc.

IP Adresse

-  Bei der Einwahl ins Internet wird technisch notwendig eine IP zugewiesen
-  Die Zuordnung IP \leftrightarrow Anschluss kann gespeichert werden (“Vorratsdatenspeicherung”, “Mindestspeicherfrist”)
-  Die IP einer Anfrage wird routinemäßig bei fast allen Webanbietern abgespeichert

Onion Routing

Anstatt direkt zum Ziel zu verbinden

 Verbindung zu einem ersten Proxy

 ... von dort zu einem zweiten ...

 ... und zu einem dritten, der zum Ziel verbindet.

 Der 1. Proxy: Sieht, wer zum Netzwerk verbunden ist, aber nicht was dort passiert.

 Der 2. Proxy: Sieht, dass überhaupt Netzwerkverkehr vorhanden ist.

 Der 3. Proxy: Sieht, was das Netzwerk im Internet tut, aber nicht wer die Anfrage stellt. (“Exit Nodes”)

Tor Browser Bundle

-  <https://www.torproject.org/projects/torbrowser.html.en>
-  Onion Routing Software TOR + Browser + Voreinstellungen
-  Trotzdem(!) kaum Schutz gegen Browser-Version Tracking
-  TOR nicht für Aktionen benutzen, die dich identifizieren können
-  Genug Exit Nodes werden von Sicherheitsforschern oder Geheimdiensten und anderen Kriminellen betrieben
-  ... auch deshalb: Niemals irgendwo (mit relevanten Daten) einloggen.

Fragen???

Jetzt.

Wer es sicherer braucht

 Selber informieren!

 <https://stratum0.org/--HackerspaceBraunschweig>

 <http://crunchbang.org/forums/viewtopic.php?id=24722>

 <https://gnunet.org/>

 <http://wiki.qubes-os.org/trac>

Wir üben Mails verschlüsseln

Links unter: <http://drahflow.name/cryptoparty.html>

-  Installieren
-  Schlüssel erzeugen
-  Schlüssel veröffentlichen
-  Verschlüsselte und signierte Mail als Test an drahflow@gmx.de
-  Verschlüsselte und signierte Antwort erhalten

Schlüssel erzeugen

The screenshot shows a dialog box titled "Generate OpenPGP Key". At the top, there is a window title bar with standard minimize, maximize, and close buttons. Below the title bar, the "Account / User ID" is set to "Patrick Brunschwig <patrick@mozilla-enigmail.org> - Private Mail". A checked checkbox indicates "Use generated key for the selected identity". There are two options for a passphrase: "No passphrase" (unchecked) and "Passphrase" (checked). The "Passphrase" section has two input fields, both containing masked characters. A "Comment" field is empty. The "Key expiry" is set to "Advanced". Below this, the key expires in "5" years, with an unchecked option for "Key does not expire". At the bottom left are "Generate key" and "Cancel" buttons. A "Key Generation Console" section contains a note: "NOTE: Key generation may take up to several minutes to complete. Do not exit the application while key generation is in progress. Actively browsing or performing disk-intensive operations during key generation will replenish the 'randomness pool' and speed-up the process. You will be alerted when key generation is completed." Below the note is an empty progress bar.

Account / User ID: Patrick Brunschwig <patrick@mozilla-enigmail.org> - Private Mail

Use generated key for the selected identity

No passphrase

Passphrase: [masked] Passphrase (repeat): [masked]

Comment: [empty]

Key expiry: **Advanced**

Key expires in: 5 years Key does not expire

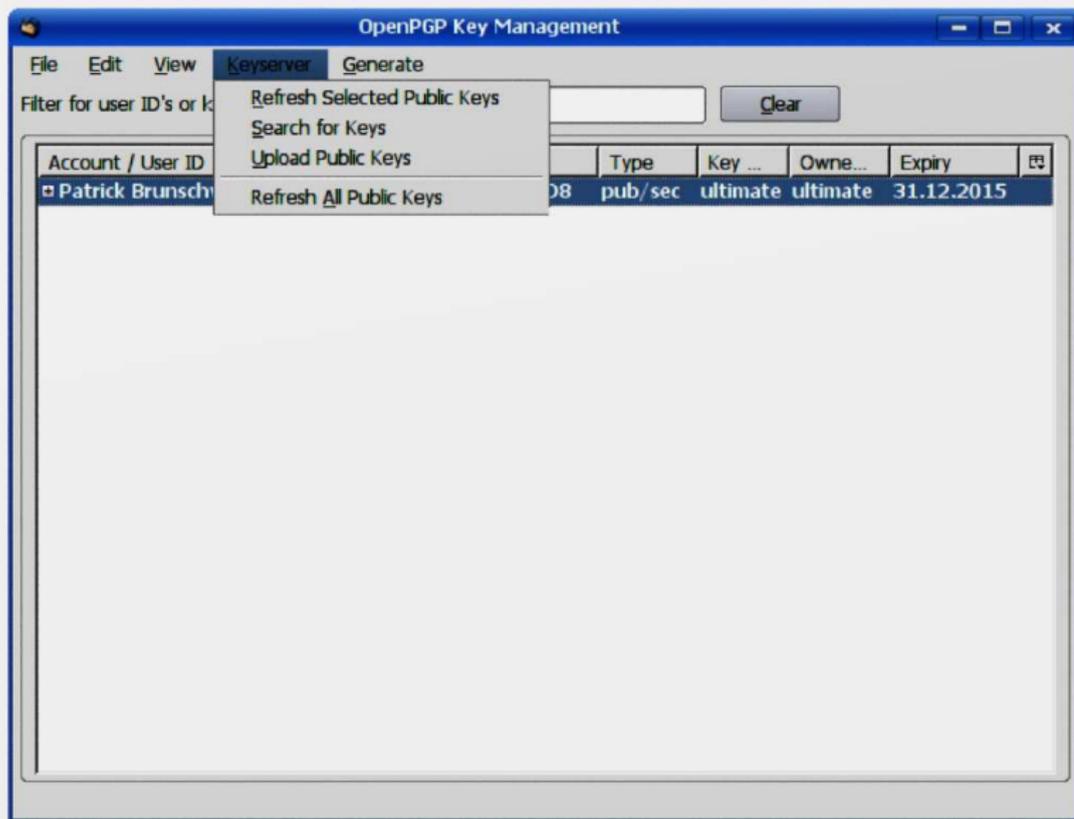
Generate key Cancel

Key Generation Console

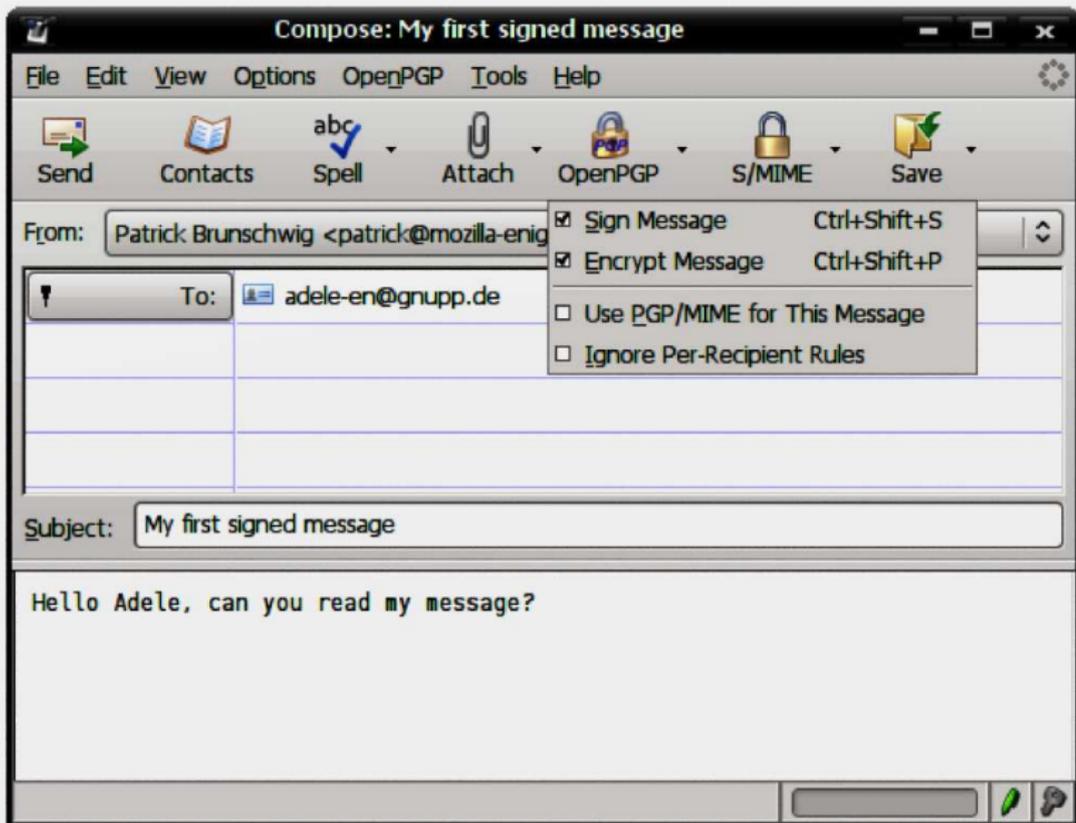
NOTE: Key generation may take up to several minutes to complete. Do not exit the application while key generation is in progress. Actively browsing or performing disk-intensive operations during key generation will replenish the 'randomness pool' and speed-up the process. You will be alerted when key generation is completed.

[Progress bar]

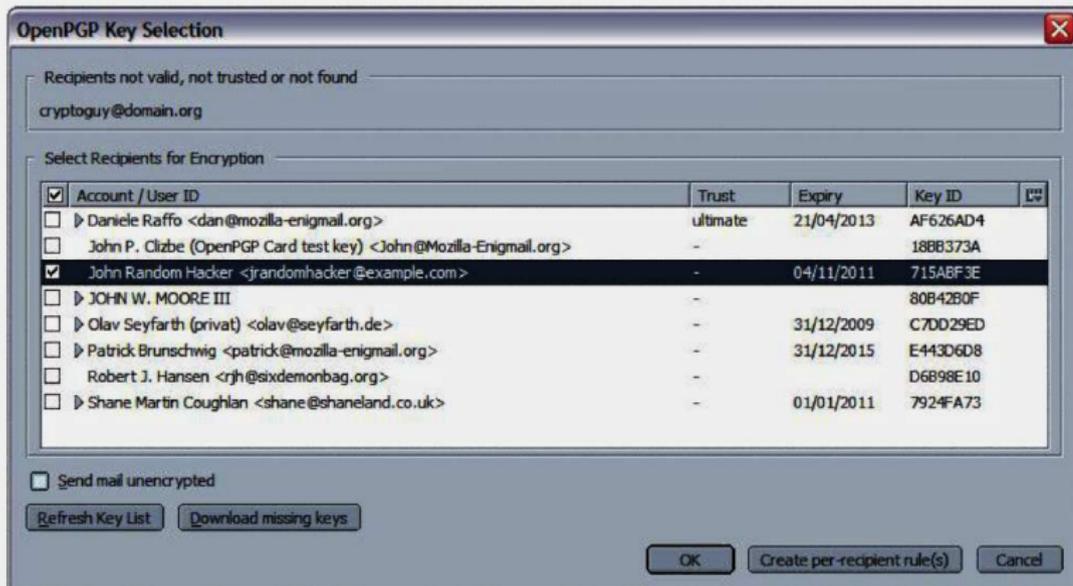
Schlüssel veröffentlichen



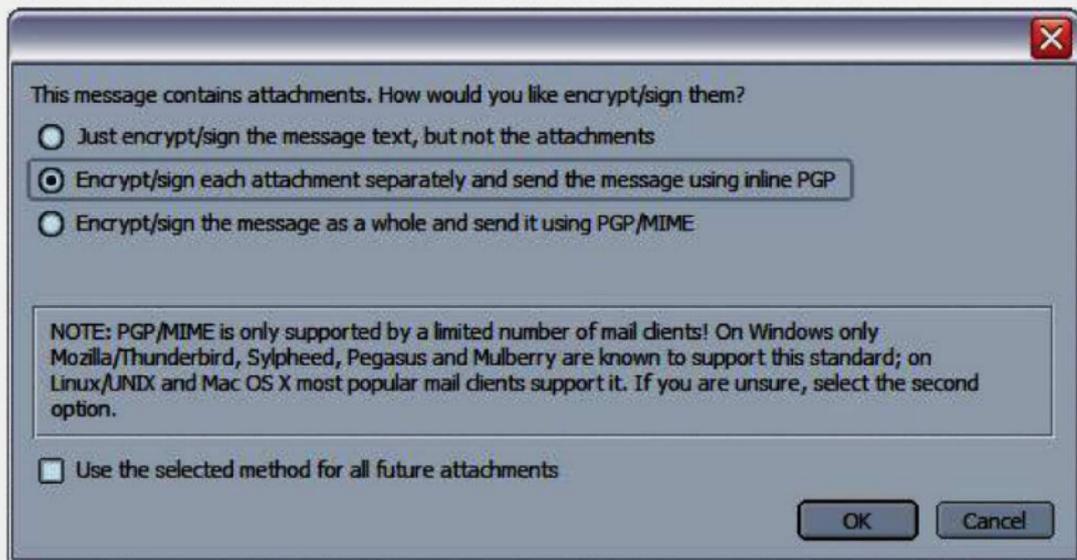
Mail signieren und verschlüsseln



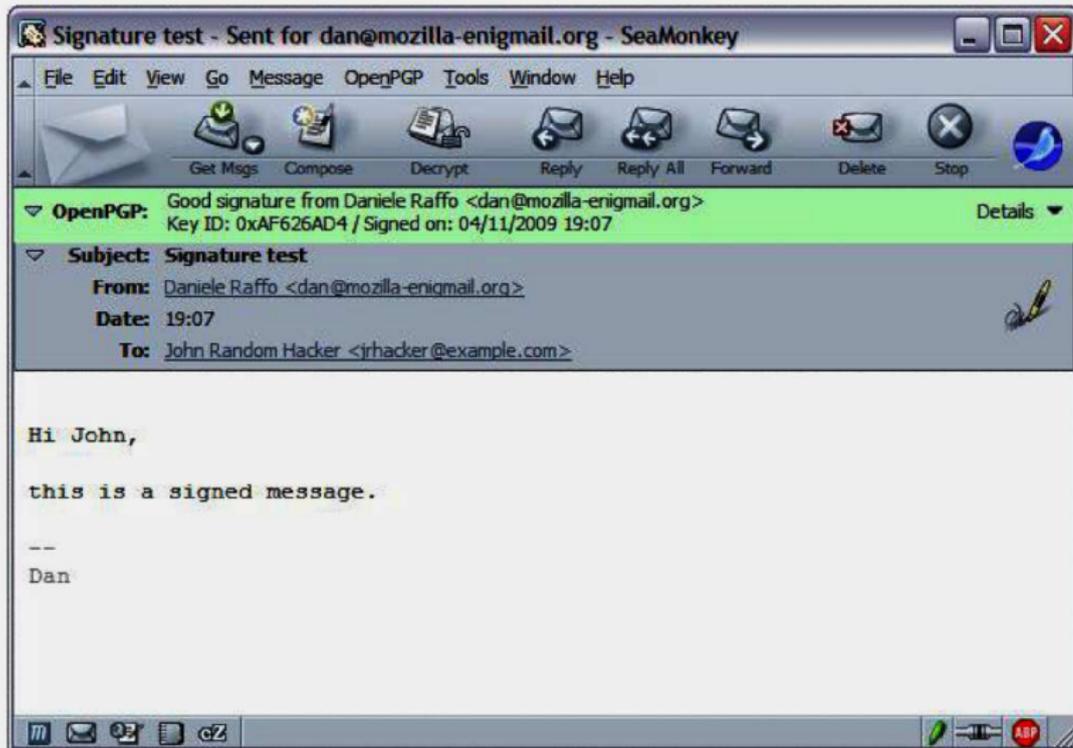
Schlüsselauswahl beim Versand



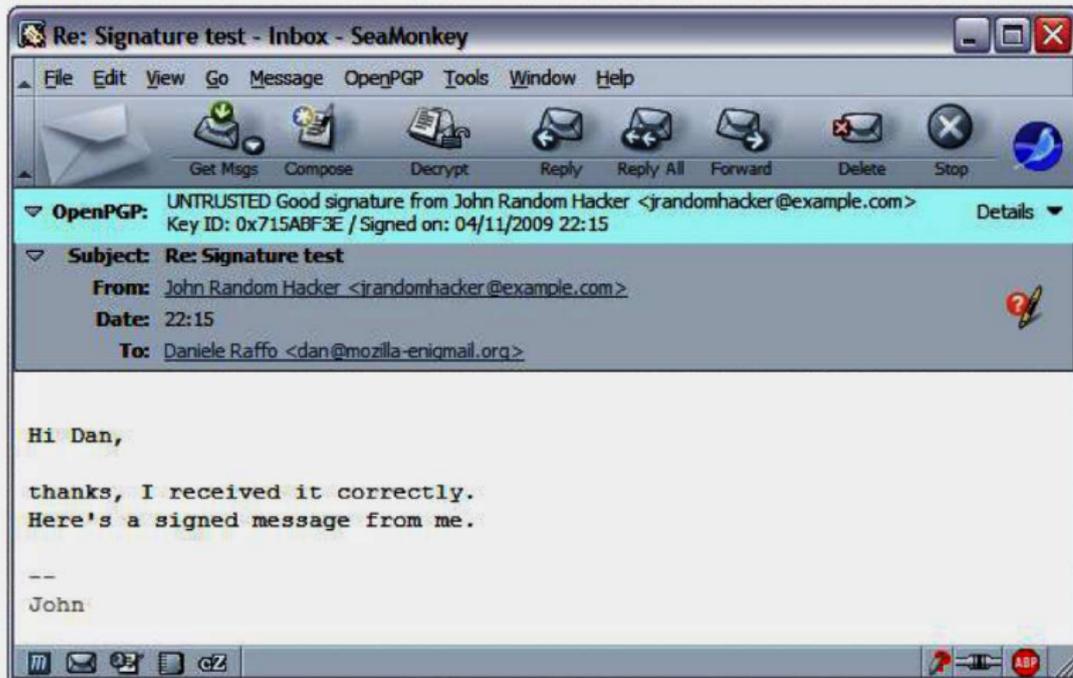
Attachments



Korrekt signierte Mail



Unvertrauenswürdig signierte Mail



Unbekannt signierte Mail

The screenshot shows a SeaMonkey email client window titled "Re: Signature test - Inbox - SeaMonkey". The interface includes a menu bar (File, Edit, View, Go, Message, OpenPGP, Tools, Window, Help) and a toolbar with icons for Get Msgs, Compose, Decrypt, Reply, Reply All, Forward, Delete, Stop, and a search icon. A yellow status bar at the top of the message pane reads: "OpenPGP: Unverified signature; click on 'Details' button for more information". Below this, the message header shows: "Subject: Re: Signature test", "From: John Random Hacker <jrandomhacker@example.com>", "Date: 22:15", and "To: Daniele Raffo <dan@mozilla-enigmail.org>". The main body of the email contains a PGP signed message:

```
-----BEGIN PGP SIGNED MESSAGE-----
Hash: SHA1

Hi Dan,

thanks, I received it correctly.
Here's a signed message from me.

-- --
John
-----BEGIN PGP SIGNATURE-----
Version: GnuPG v1.4.9 (MingW32)

iEYEARECAAYFAkrx7wYACgkQt9EF/3Favz55kQCfVID3Ab1j44t518BcpAXG9V0V
ayYAn18KP1yioT+JwnMS2hZeAu714SCw
=Rypo
-----END PGP SIGNATURE-----
```

The bottom of the window shows a standard Windows taskbar with icons for Mozilla, SeaMonkey, and other applications.

Fehlerhaft signierte Mail

The screenshot shows the SeaMonkey email client interface. The window title is "Re: Signature test - Inbox - SeaMonkey". The menu bar includes File, Edit, View, Go, Message, OpenPGP, Tools, Window, and Help. The toolbar contains icons for Get Msgs, Compose, Decrypt, Reply, Reply All, Forward, Delete, Stop, and a globe icon. A pink error banner at the top reads: "OpenPGP: Error - signature verification failed; click on 'Details' button for more information". Below the banner, the email header shows: "Subject: Re: Signature test", "From: John Random Hacker <irandomhacker@example.com>", "Date: 22:15", and "To: Daniele Raffo <dan@mozilla-enigmail.org>". The main content area displays a PGP signed message with the following text:

```
-----BEGIN PGP SIGNED MESSAGE-----  
Hash: SHA1  
  
You have been pwned!  
  
-- --  
John  
-----BEGIN PGP SIGNATURE-----  
Version: GnuPG v1.4.9 (MingW32)  
  
iEYEARECAAYFAkrx7wYACgkQt9EF/3Favz55kQCfVID3Ab1j44t518BcpAXG9V0V  
ayYAn18KP1yioT+JwnMS2hZeAu7145Cw  
=Rypo  
-----END PGP SIGNATURE-----  
  
From - Wed Nov 04 22:42:26 2009  
X-Mozilla-Status: 0011
```

The status bar at the bottom shows various system icons and a red "ABP" icon.

Wir üben anonym Surfen

 Tor Browser Bundle installieren

 Tor starten

 `http://duckduckgo.com/`

 bzw. `http://3g2upl4pq6kufc4m.onion/`