zentraler informatik dienst

universität wien

EHLO

End2End ist nicht genug!
SMTP TLS an der Uni Wien

November 2015

Wolfgang Breyha

Vorstellung

Wolfgang Breyha

Beruflicher Werdegang

- 1997: Netway Communications
- 2001: UTA
- 2004: Tele2
- 2005: ZID Universität Wien

root am ZID der Universität Wien

Verantwortlich für Entwicklung und Betrieb des Linux Mailsystems

Mailsystem der Universität Wien

- auf Open Source basierende Eigenentwicklung abgestimmt auf die Bedürfnisse der Uni Wien
- ~ 120.000 IMAP Mailboxen
  - ~ 35 TB
  - ~ 205 Mio. E-Mails
- Spamfilter für Institutsmailserver
- ~ 400.000 - 600.000 Connections/Tag
- ~ 125.000 (extern) + 250.000 (intern) Mails/Tag
- 25 virtuelle Maschinen
- IPv6 seit 2006

Agenda

- warum TLS?
- Umsetung an der Uni Wien
- TLS in Zahlen

Grundsätzliches

- Unterscheidung POP3/IMAP/MSA und MTA
  - MUAs sind mit Browser gleichzusetzen
  - MTA → MX … ganz andere Baustelle

warum TLS? - Authentizierung

$ telnet imap.univie.ac.at 110
Connected to imap.univie.ac.at.
+OK jarvis.univie.ac.at Cyrus POP3 Murder v2.4.17-univie-6.5 server ready
user testuser
-ERR [AUTH] STARTTLS or SSL/TLS needed.
pass testpass
-ERR [AUTH] Must give USER command

$ telnet imap.univie.ac.at 143
Connected to imap.univie.ac.at.
* OK [CAPABILITY IMAP4rev1 …. STARTTLS LOGINDISABLED] ...
. login testuser testpass
. NO Login only available with active encryption (SSL/STARTTLS)

warum TLS? - Authentizierung

```
# ngrep -i '(user|pass)' port 110
interface: eth0 ...
filter: ( port 110 ) and (ip or ip6)
match: (user|pass)
#######
T 2001:62a:4:xxxxxxx:54201 -> 2001:62a:4:25::143:112:110 [AP]
  user testuser..
#####
T 2001:62a:4:xxxxxxx:54201 -> 2001:62a:4:25::143:112:110 [AP]
  pass testpass..
```

warum TLS? - Authentizierung

```
# ngrep -i 'login' port 143
interface: eth0 (.....)
filter: ( port 143 ) and (ip or ip6)
match: login
####
T 2001:62a:4:25::143:110:143 -> 2001:62a:4::xxxxx:42973 [AP]
  * OK [CAPABILITY IMAP4rev1 .... STARTTLS LOGINDISABLE ....
##
T 2001:62a:4:xxxxxxx:42973 -> 2001:62a:4:25::143:110:143 [AP]
  . login testuser testpass..
##
T 2001:62a:4:25::143:110:143 -> 2001:62a:4:xxxxxx:42973 [AP]
  . NO Login only available with active encryption (SSL/STARTTLS)..
```

warum TLS? - Authentizierung

- plaintext, SASL-PLAIN, SASL-LOGIN offen mitlesbar
  - base64 ist nicht einmal “obscurity”
- Problem explizites TLS via STARTTLS
  - Fehler in Clientimplementierungen schicken Passwort trotz Serverablehnung
  - IMAP: LOGINDISABLED ignoriert
  - POP3: USER Errorcode ignoriert
  - SMTP AUTH eher unkritisch weil optional. Client muß in EHLO Antwort suchen.
- nur implizites TLS auf ports 993/995 garantiert verschlüsselten Passworttransport

warum TLS? - E-Mail Transport

This is an OpenPGP/MIME encrypted message (RFC 4880 and 3156)
--EWEEhPhKwVoQVnE5q7W31HXWUUHsh3hb9
Content-Type: application/pgp-encrypted
Content-Description: PGP/MIME version identification

Version: 1

--EWEEhPhKwVoQVnE5q7W31HXWUUHsh3hb9
Content-Type: application/octet-stream; name="encrypted.asc"
Content-Description: OpenPGP encrypted message
Content-Disposition: inline; filename="encrypted.asc"

-----BEGIN PGP MESSAGE-----
Version: GnuPG v2

hQIOA2pGr3zlEFqpEAf/dQl1Lbg+urv8PKrHRNw566bFwunN5B5UKpbPUJY4ODlN
KwcHyAFJtkTy+z4yUEtgJQaaUnQSO5SZ8ltqU0Dkqrk/FRyYgyvAD9VivRIx+pTj
KFULzWhs+iCCPbwO……

warum TLS? - E-Mail Transport

PGP ist gut und richtig, aber da war noch was…

Received: from … by ...
Received: from … by ...
To: nicht recht geheimer Empfaenger <…@...>
From: Wolfgang Breyha <…@…..>
Subject: Jehova!

und

MAIL FROM: <…@…..>
250 2.5.0 Ok
RCPT TO: <…@...>
250 2.5.0 Ok

… wird dabei gerne übersehen.
→ TLS ist ebenso wichtig um die Header
und insbesonder das Envelope zu schützen.

warum TLS?

- PGP und S/MIME: jeder User ist sich selbst überlassen
- TLS: ein verantwortungsvoller und motivierter Admin, viele glückliche User. Unabhängig davon ob diese “nichts zu verbergen haben”.
- verschlüsseltes Grundrauschen erhöhen um end2end verschlüsselte E-Mails schlechter erkennbar zu machen

Umsetzung Uni Wien

- 19xx bis 2013
  - OpenSSL aus Standardpaketen
  - Default (Ciphers und Options)
  - SSL/TLS für SMTP AUTH Pflicht
  - POP3/IMAP SSL/TLS optional
  - STARTTLS auf MTAs
  - opportunistic SSL/TLS ausgehend

Kurz: alles was sich offensichtlich anbietet

Umsetzung Uni Wien

- post Snowden, heartbleed, …
  - aktive Mitarbeit bei bettercrypto.org
  - selbst kompilierte OpenSSL Pakete für EL6 (derzeit 1.0.2 zwecks EC autoselect)
  - TLSv1.2 im Mailcluster
  - SSLv2/v3 deaktiviert
  - Optimierte Ciphers und Optionen
  - POP3/IMAP TLS verpflichtend … Einführung unter Schmerzen ;-)
  - DANE-SMTP ausgehend
  - DNSSEC …. .ac.at noch nicht signiert

Erfahrungen - Ciphers und Optionen

- SSLv2/3 off … keine nennenswerten Probleme
- compression off … keine Probleme
- Preferenz auf AES 256 und 128 … keine Probleme
    - Vorteil Intel AES-NI Hardwaresupport
- ECDHE … keine Probleme
- prefer server ciphers … keine unmittelbaren Probleme
- DHE … Probleme mit alten Clients (key size)
    - bestimmte TLSv1:DHE...AES-Kombinationen entfernt
    - durch prefer server ciphers verstärkt

Zahlen, Zahlen und noch mehr Zahlen

- Entwicklung...
  - **eingehend:**
    - Mai 2013: 33% mit TLS, Rest ohne
    - Mai 2014: 43% mit TLS, ….
    - Okt. 2015: 57% mit TLS, ….
  - **ausgehend:**
    - Mai 2013: 40% mit TLS
    - Mai 2014: 70% mit TLS (unet → GMX)
    - Okt. 2015: 91% mit TLS (hotmail, .at)

Zahlen, Zahlen und noch mehr Zahlen

- Beispiel 21.10.2015:
  - 244853 verschlüsselte ausgehende E-Mails
    - 212873 ... PFS (DHE/ECDHE)
    - 198146 ... TLSv1.2

    - 53500 ... GMX
    - 48200 ... gmail
    - 38500 ... hotmail
    - 12500 ... yahoo
    - 5000 ... .at ISP (kein PFS, CV=no)
    - 4100 ... outlook.com
    - 3600 ... .at ISP
  - 21956 ... unverschlüsselt

Zahlen, Zahlen und noch mehr Zahlen

- Beispiel 21.10.2015: ausgehende Verbindungen
  - 3547 Cipher-Zertifikat Paare
    - PFS?
      - » 1258 ... ECDHE
      - » 1758 ... DHE
      - » 533 ... ohne PFS
    - Cert verifzierbar?
      - » 2021 ... CV=no, 456 davon "/OU=Domain Control Validated"
      - » 1498 ... CV=yes (eigentlich irrelevant)
      - » 28 ... CV=dane

Zahlen, Zahlen und noch mehr Zahlen

- Beispiel 21.10.2015: ausgehende Verbindungen
  - 1861 ... hosts unverschlüsselt
    - 495 ... .at
      (darunter Steuerberater, Anwaltskanzleien, Notare, Ärzte, Presse (klein wie ganz groß), Frauenhäuser, Schulen, Hilfsorganisationen, Sportverbände, Diazösen und ISPs)
  - 35 ... .ac.at (exkl. .at Anteil)
  - 10 ... .gv.at (exkl. .at Anteil)

Zahlen, Zahlen und noch mehr Zahlen

- Beispiel 21.10.2015:
  - 87414 verschlüsselte eingehende E-Mails
    - 87302 ... PFS (DHE/ECDHE)
    - 59403 ... TLSv1.2
    - 40130 … GCM
  - 66329 ... unverschlüsselt
  - 1400 client certificates
    - 691 … CV=no
      54 "/OU=Domain Control Validated"
  - 11 hosts scheitern an SSLv3

Resümee

- Danke Edward Snowden!
- Es bewegt sich was, aber es ist noch genug zu tun
- Admins sind aufgefordert
    - vorhandene Möglichkeiten auszuschöpfen
    - mehr Sorgfalt und Tests der eigenen Server
    - unverschlüsselten Client-Traffic verhindern
    - Mut zur Optimierung zu haben (bettercrypto.org)
- let's do DANE

zentraler informatik dienst

universität wien

Fragen?