REGIONALES RECHENZENTRUM ERLANGEN [RRZE]

E-Mail-Grundlagen

Netzwerkausbildung – Praxis der Datenkommunikation, 07.02.2018

Reiner Fischer, RRZE

Dieser Vortrag wird aufgezeichnet.

Die ersten beiden Sitzreihen befinden sich im Kameraradius.

Überblick (1)

1. Allgemeines
   - Unterschiedliche Mail-Welten
   - Internet-Mail: Beteiligte Systeme
   - Briefpost vs. Internet-Mail

2. Mail-Transport
   - SMTP: Historie/Charakteristika
   - SMTP-Dialog
   - Mail-Routing
   - SMTP mit Authentifizierung
   - MIME-Kodierung

Überblick (2)

3. Postfach-Zugriff
   - POP3
   - IMAP
   - Webmail

4. „Gruppen-Mail“
   - Funktionsverteiler/-postfach
   - Mailingliste

5. E-Mail-Dienste am RRZE
   - Relay- und Postfachdienste
   - List Services

6. Nachrichtenfilter
   - Server-/Clientseitig
   - Abwesenheitsnotiz

Überblick (3)

7. E-Mail-Sicherheit
   - Ende-zu-Ende-Verschlüsselung
     - OpenPGP und S/MIME
       - Kryptographische Signatur
       - Inhaltsverschlüsselung
   - Transportverschlüsselung
     - SSL/TLS
   - Schwachpunkte bei OpenPGP, S/MIME, TLS
   - Ausblick: DANE
     - DANE/TLSA
     - DANE/OPENPGPKEY
     - DANE/SMIMEA

Unterschiedliche „Mail-Welten“

Historisch: unterschiedliche Mail-Standards

- Firmenstandards, z.B.
  - Novell
  - Microsoft
- Internetstandard SMTP (Simple Mail Transfer Protocol)
- ISO-/CCITT-Standard MHS/X400
  - im Industriebereich verbreitet
  - im Hochschulbereich ohne Bedeutung
- Übergang durch Gateways

Internet-Mail: Beteiligte Systeme (1)

- Benutzeroberflächen / Mail-Clients
  - vernetzter PC — Mail-Client (Thunderbird, Outlook, ...)
  - vernetzte Unix-WS — Mail-Client (Thunderbird, mutt, …)
  - Internet-Cafe — Web-Browser (Firefox, Chrome, …)
- Server für den Mail-Transport
  - Kommunikation (Client-Server und Server-Server) via SMTP (Simple Mail Transfer Protocol)

Internet-Mail: Beteiligte Systeme (2)

- Server für den Postfach-Zugriff
  - Schnittstellen (Zugriffsprotokolle)
    - POP3 (Post Office Protocol Version 3)
      - Einfaches Protokoll mit eingeschränkten Fähigkeiten
    - IMAP (Internet Message Access Protocol)
      - Wesentlich vielseitiger und leistungsfähiger
    - Webmail
      - Unabhängig von lokalem Rechnerzugang

Analogie: Briefpost vs. Internet-Mail

- Postkarte ↔ E-Mail
- Brief ↔ Verschlüsselte E-Mail
- Briefumschlag ↔ Envelope
- Briefbogen ↔ Content
  - Briefkopf ↔ Header
  - Brieftext ↔ Body
- Anschrift ↔ E-Mail-Adresse
- Poststempel ↔ Received-Header
- Briefkasten ↔ Mail-Server
- Postamt ↔ Mail-Server
- Verteilerpostamt ↔ Mail-Relay-Server

WIE GELANGT EINE E-MAIL VOM ABSENDER ZUM EMPFÄNGER?

Übertragungsprotokoll SMTP

SMTP: Charakteristika (1)

- „der“ E-Mail-Standard im Internet (RFC 5321), TCP/IP-basiert
- nur für ASCII-Texte (7 Bit) konzipiert
- verwendet MIME (Multipurpose Internet Mail Extensions) als Internet-Standard zur Kodierung/Dekodierung von 8-Bit-Daten
  - RFC 2045 bis RFC 2049 (1996)
- nutzt Domain Name System (DNS) für Mail-Routing
- Adressformat gem. RFC 5322
  - Beispiel: Reiner.Fischer@rrze.fau.de

SMTP: Charakteristika (2)

- Server wartet standardmäßig auf Verbindunganfragen
  - von Servern auf TCP-Port 25 (SMTP-Port)
  - von Clients auf TCP-Port 587 (Submission Port)
- Sendender Server/Client eröffnet SMTP-Dialog
  - Manuelle Überprüfung der Erreichbarkeit des Ziel-Servers:

    „telnet <Ziel-Server> <Ziel-Port>“

SMTP: Mail-Routing (1)

- Ausgangsrechner: Mailserver, bei dem Einlieferung erfolgt
  - Postausgangsserver für Mail-Clients
- Dieser bestimmt nächsten Rechner, an den die Mail übermittelt wird
  - Dies kann sein:
    - ein spezieller Rechner, der alle Mails von diesem System annimmt (Relay Host, Smart Relay)
    - ein weiterer Zwischenrechner (Hop)
    - der Zielrechner, auf dem das Postfach des Empfängers liegt
- In der X400-Terminologie heißen diese Rechner Message Transfer Agents (MTA)
- Im Internet heißen solche Rechner Mail eXchanger (MX)

SMTP: Mail-Routing (2)

- Zieladresse: `empfaenger@maildom.ain`
- Adressteil hinter dem @ wird als IP-Domain interpretiert und als Mail-Domain bezeichnet.
- Sender-Host sucht Ziel-Host für die Mail-Domain über einen MX-Record im DNS:
  - DNS-Request mit `type = mx` für Mail eXchanger (`=Ziel-Host`)
  - Antwort: Satz von Rechneradressen inkl. Präferenz
  - Antwort: „`non-existent domain`“, falls kein Eintrag gefunden wird.
- Mail wird direkt an den so ermittelten Mail eXchanger abgeschickt.

SMTP: Mail-Routing (3)

Beispiele: MX-Einträge für Mail-Domains der FAU

- Mail-Domain rrze.uni-erlangen.de:

```
rrze.uni-erlangen.de   preference 10   mx-rz-1.rrze...
rrze.uni-erlangen.de   preference 10   mx-rz-2.rrze...
rrze.uni-erlangen.de   preference 10   mx-rz-3.rrze...
```

- Mail-Domain leb.e-technik.uni-erlangen.de:

```
leb.e-technik.uni-erlangen.de preference 10  lebds003.e-technik...
leb.e-technik.uni-erlangen.de preference 30  mx-rz-1.rrze...
leb.e-technik.uni-erlangen.de preference 30  mx-rz-2.rrze...
leb.e-technik.uni-erlangen.de preference 30  mx-rz-3.rrze...
```

- Bedeutung: Niedrige Präferenz = Hohe Priorität

SMTP: Mail-Routing (4)

- Anmerkung für Subnetz-/Mailadministratoren:
  DNS-Einträge für FAU werden vom RRZE zentral verwaltet
  (Beantragung von MX-Einträgen durch Subnetzbetreuer an dns-admin@fau.de mit Kopie an postmaster@fau.de)
- MX-Einträge nachschlagen im RRZE-Unix-Verbund mit /usr/sbin/nslookup

  `set type=mx`

  Adressteil hinter dem @ eingeben (z.B. `rrze.uni-erlangen.de`)

  für weitere Hilfe `?`

  zum Verlassen: `exit`
- nslookup-Kommando auch unter Windows vorhanden
- Neuere Alternative: `dig`

Beispiel für SMTP-Dialog (1)

Dialogpartner:

<<: Sender-Host (Mailserver oder einliefernder Mailclient)
>>: Empfänger-Host (Mailserver)

Dialog:

```
>> 220 smtp.uni-erlangen.de eMail Sentinel 2003 ESMTP Service ready
<< EHLO rabea.rrze.uni-erlangen.de
>> 250-smtp.uni-erlangen.de

<< MAIL FROM: <Reiner.Fischer@rrze.uni-erlangen.de>
>> 250 sender <Reiner.Fischer@rrze.uni-erlangen.de> OK

<< RCPT TO: <Hans.Muster@rrze.uni-erlangen.de>
>> 250 recipient <Hans.Muster@rrze.uni-erlangen.de> OK
```

Beispiel für SMTP-Dialog (2)

```
<< DATA
>> 354 Enter mail, end with “.” on a line by itself

<< From: Reiner.Fischer@rrze.uni-erlangen.de
<< To: Hans.Muster@rrze.uni-erlangen.de
<< Subject: Testmail
<<
<< Dies ist eine Testnachricht.
<< .

>> 250 Message received and queued
```

Bedeutung der Codes:

45x Sende-Host soll Übermittlung erneut versuchen (temp. Ablehnung)
55x Sende-Host muss Unzustellbarkeitsreport generieren (perm. Ablehnung)
250 nach DATA-Phase: Abnahme-Quittung

SMTP: Adressierung (1)

- Unterscheidung von E-Mail-Adressen
  - auf dem Briefumschlag (Envelope)
    - › für Adressierung maßgeblich, für Adressaten unsichtbar
  - auf dem Briefkopf (Header)
    - › für Adressierung unerheblich, für Adressaten sichtbar
- Adressumsetzungen auf Transportweg möglich
  - Domainspezifisches Absender-Rewriting

user@host.doma.in → user@doma.in

SMTP: Adressierung (2)

- Benutzerspezifisches Absender-Rewriting

user@host.doma.in → vorname.nachname@doma.in

- Empfängerspezifisches Rewriting der Zieladresse

vorname.nachname@doma.in → user@zieldoma.in

z.B. Alias-Auflösung oder Auto-Forward

SMTP: Vermeidung von Adressierungsfehlern (1)

- Gültige Adressierungen gem. RFC 5322
  - Hans.Muster@beispiel.de
  - “Hans Muster“@beispiel.de
  - “Muster, Hans“ <Hans.Muster@beispiel.de>
  - “Prof. Dr. Hans Muster“ Hans.Muster@beispiel.de
  - “Prof. Dr. Hans Muster“ <Hans.Muster@beispiel.de> (Institut A)
  - hans@beispiel.de, john@example.us

SMTP: Vermeidung von Adressierungsfehlern (2)

- Unzulässige Adressierungen gem. RFC 5322
  - Prof. Dr. Hans Muster Hans.Muster@beispiel.de
  - Hans Muster@beispiel.de
  - Muster, Hans <hans.muster@beispiel.de>
  - <Hans.Muster@beispiel.de> (Prof. Dr. Hans Muster)
  - hans@beispiel.de; john@example.us
- Vorsicht bei Cut & Paste!
- Trennzeichen für E-Mail-Adressen ist das Komma
  - Strichpunkt als Trennzeichen laut Standard nicht erlaubt!

SMTP: Historische Entwicklung (1)

- RFC 821: Simple Mail Transfer Protocol (1982)
- RFC 822: Standard for the format of ARPA Internet text messages (1982)
- RFC 974: Mail routing and the domain system (1986)
- RFC 1869: SMTP Service Extensions (1995) (ESMTP)
- RFC 2554: SMTP Service Extensions for Authentication (1999)
- RFC 2821: Simple Mail Transfer Protocol (2001)
  - ersetzt RFC 821, 974 u.a.
- RFC 2822: Internet Message Format (2001)
  - ersetzt RFC 822

SMTP: Historische Entwicklung (2)

- RFC 3461: SMTP Service Extension for Delivery Status Notifications (DSNs) (2003)
- RFC 4954: SMTP Service Extensions for Authentication (2007)
  - ersetzt RFC 2554
- RFC 5321: Simple Mail Transfer Protocol (2008)
  - ersetzt RFC 2821, 1869
- RFC 5322: Internet Message Format (2008)
  - ersetzt RFC 2822

SMTP/AUTH: Hintergrund

- Problem: Nutzung eines SMTP-Servers i.d.R. nur möglich, wenn sich der Host des Senders im gleichen Netz befindet wie der Server (Spam-Relay-Schutz)
- Abhilfe: SMTP/AUTH als Erweiterung des ESMTP-Protokolls um Authentifizierungsmechanismen mit Benutzername und Passwort (RFC 4954)
- Bei Mechanismen mit Klartextübertragung von Benutzername und Passwort nur zusammen mit Verbindungsverschlüsselung (TLS/SSL) sinnvoll
- Verbindungsverschlüsselung i.A. nur bis zum Einlieferungsserver, nicht auf dem gesamten Transportweg!

SMTP/AUTH: Gängige Mechanismen (1)

- In Mail-Clients findet man häufig nachfolgend genannte Authentifizierungsmechanismen

- SASL-Mechanismen (Simple Authentication and Security Layer)
  - PLAIN (RFCs 2595, 4616)
    - › Klartext-Übertragung von Benutzername/Passwort (nur base64-kodiert, nicht verschlüsselt)

SMTP/AUTH: Gängige Mechanismen (2)

- LOGIN
  - Wie PLAIN, aber Übertragung von Benutzername/Passwort in zwei Schritten
- CRAM-MD5 (RFC 2195)
  - Challenge-Response-Prinzip auf Basis des MD5-HMAC-Algorithmus
  - Keine Klartext-Übertragung von Benutzername/Passwort
  - „Sichere“ Authentifizierung auch über unverschlüsselte Kanäle
- SPA (Secure Password Authentication)
  - basiert auf Microsofteigenem Authentifizierungsprotokoll NTLM

WIE KÖNNEN BELIEBIGE DATEN PER E-MAIL ÜBERTRAGEN WERDEN?

Kodierstandard MIME

MIME-Kodierung (1)

- Kodierstandard für Nicht-ASCII-Zeichen
  - RFCs 2045 Multipurpose Internet Mail Extensions (MIME) (1996)
    - ergänzt durch RFCs 2046 – 2049 bzw. 4288 - 4289
- Verwendet die Standard-Mail-Header
  - Content-Type
  - Content-Transfer-Encoding
- Kodiermethoden
  - quoted-printable (für Nicht-7bit-ASCII-Zeichen)
  - base64 (bei Windows/Unix für Binärdaten)
    - erhöht Platzbedarf um etwa 33%
    - binhex (bei Apple Macintosh für Binärdaten)

MIME-Kodierung (2)

- Multipart-Message mit mehreren Bodyparts, abgegrenzt durch Grenzlinie (boundary)
  - Content-Type: multipart/…
- Erweiterter Standard für kryptographische Signatur und Inhaltsverschlüsselung
  - PGP/MIME (OpenPGP , RFC 4880)
    - › Content-Type: multipart/signed und multipart/encrypted
  - S/MIME (Secure MIME, RFC 3851)
    - › Content-Type: multipart/signed und application/pkcs7-mime
  - In gängigen Mailprogrammen implementiert oder als Plugin verfügbar

MIME-Kodierung: Textnachricht

Rohansicht einer einfachen Textnachricht

```
Return-Path: <Reiner.Fischer@rrze.uni-erlangen.de>
Received: from [131.188.78.38] by max6.rrze.uni-erlangen.de with ESMTP for
          Hans.Muster@rrze.uni-erlangen.de; Mon, 24 Nov 2003 15:11:19 +0100
From: Reiner Fischer <Reiner.Fischer@rrze.uni-erlangen.de>
Date: Mon, 24 Nov 2003 15:11:06 +0100
To:  Hans Muster <Hans.Muster@rrze.uni-erlangen.de>
Subject: Test
Message-ID: <3FC2117A.5080809@rrze.uni-erlangen.de>
User-Agent: Mozilla/5.0 (Windows; U; Windows NT 5.0; en-US; rv:1.4)
            Gecko/20030624 MIME-Version: 1.0
Content-Type: text/plain; charset=us-ascii
Content-Transfer-Encoding: 7bit
Content-Disposition: inline

This is a test message.
```

MIME-Kodierung: Mehrteilige Nachricht

Rohansicht einer Textnachricht mit Umlauten und Anhang

```
From: absender@example.com
To: empfaenger@example.com
Subject: der Betreff der Nachricht
MIME-Version: 1.0
Content-Type: multipart/mixed; boundary="example-1"

--example-1
Content-Type: text/plain; charset="iso-8859-1"
Content-Transfer-Encoding: quoted-printable
Content-Disposition: inline

Beispiel f=FCr einen sch=F6nen Nachrichtentext mit Umlauten

--example-1
Content-Type: image/gif; name="bild.gif"(Art der Nachricht, z.B. Klartext, Bilder...)
Content-Transfer-Encoding: base64 (Kodierverfahren)
Content-Disposition: attachment; filename ="bild.gif "

R0lGODlhIgFGAOYAAABmmYCruf///zCIpa/S3QCZzECZtgCNvN/p7CB3lKDDzmCZrACGsxB2$(B!D(B

--example-1--
```

MIME-Kodierung: Delivery Status Notification (1)

- Positive DSN: Delivery Confirmation
- Negative DSN: Non-Delivery Report (NDR)

- NDR als Beispiel für eine MIME-kodierte Nachricht

- NDR besteht aus drei Teilen
  - 1. Informativer Text mit Ablehnungsgrund
  - 2. Detailangaben zur Ablehnung
  - 3. Kopfzeilen der ursprünglichen Nachricht

MIME-Kodierung: Delivery Status Notification (2)

```
Return-Path: <>
To: Alice@Example.ORG
From: Postmaster@Boondoggle.GOV
Subject: Delivery failure for Sam@Boondoggle.GOV
Content-Type: multipart/report; report-type=delivery-status; boundary=defgh
MIME-Version: 1.0

--defgh
Your message, originally addressed to George@Tax-ME.GOV,
 and forwarded from there to Sam@Boondoggle.GOV could not be
 delivered, for the following reason:

write error to mailbox, disk quota exceeded

--defgh
Content-Type: message/delivery-status
```

MIME-Kodierung: Delivery Status Notification (3)

```
Reporting-MTA: Boondoggle.GOV
Original-Envelope-ID: QQ314159
Original-Recipient: rfc822;George@Tax-ME.GOV
Final-Recipient: rfc822;Sam@Boondoggle.GOV
Action: failed
Status: 4.2.2 (disk quota exceeded)

 --defgh
Content-Type: message/rfc822-headers

(headers of returned message go here)

 --defgh--
```

WIE KANN ICH AUF MEIN E-MAIL-POSTFACH ZUGREIFEN?

Zugriffsprotokolle POP3 und IMAP

Postfach-Zugriff per POP3 (1)

- Aktueller Standard: POP3 (RFC 1939)
  - ergänzt durch RFCs 1957, 2449, 5034
- Download der Mails vom Server auf den lokalen Rechner
- Authentifizierung mit Benutzername und Passwort
- Eingeschränkter Zugriff auf die Mails auf dem Server
  - Zugriff nur auf serverseitigen Posteingang (keine weiteren Ordner)
  - evtl. Zugriff auf einzelne Mails (bei manchen Mail-Clients)
- Wahlweise Löschen der Mails auf dem Server nach erfolgreichem Download oder Belassen einer Kopie auf dem Server

Postfach-Zugriff per POP3 (2)

Vorteile:

- einfaches Protokoll, wenige Befehle, leicht konfigurierbar
- Offline-Betrieb nach Download
- von praktisch allen Mail-Clients und Providern unterstützt

Nachteile:

- nur Zugriff auf serverseitigen Posteingangsordner
- unhandlich bei wechselnden Arbeitsplätzen

Postfach-Zugriff per IMAP (1)

- „Proposed Standard“: RFC 3501 (IMAP4rev1, 2003)
  - Updates: RFCs 4314 (IMAP ACL Extension), 4466, 4469, 4551, 5550, 7162
- Kein Download der Mails vom Server auf lokalen Rechner notwendig, aber möglich
- Verwaltung von Mail-Ordnern auf dem Server (Erstellen, Umbenennen, Löschen; Setzen/Löschen von Flags; Suchen von Mails); Einrichtung von Ordnerfreigaben an andere Nutzer

Postfach-Zugriff per IMAP (2)

- Zugriff auf Server-Ordner wie auf lokale Ordner
- Offline-Betrieb und Resynchronisation mit dem Server

Vorteile:

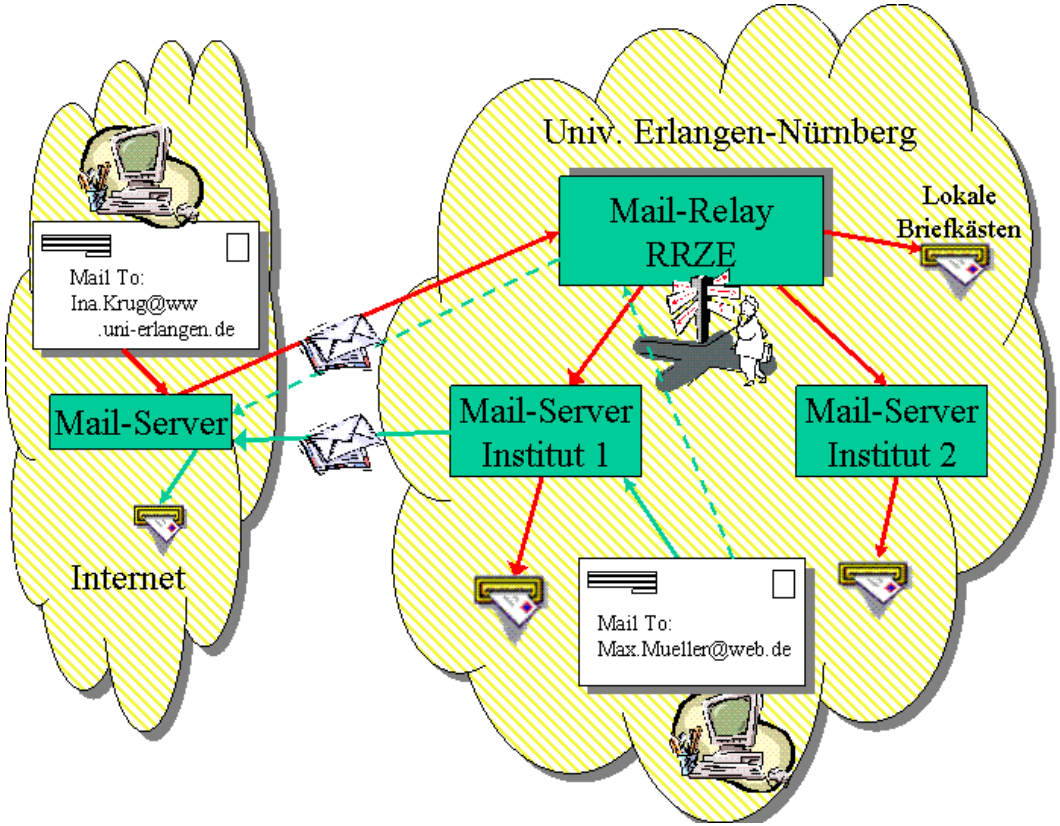
- Zugriff auf zentrales Postfach von verschiedenen Arbeitsplätzen aus (gleiche Sicht unabhängig vom Standort)
- wird von allen gängigen Mail-Clients und den meisten Mailprovidern unterstützt

WELCHE DIENSTE BIETET DAS RRZE IM BEREICH E-MAIL AN?

Relay-, Postfach-, Groupware-Dienste

List Services

E-Mail-Struktur der FAU



E-Mail-Dienste des RRZE: Übersicht (1)

- FAU-Mailrelay (Postfix+AMaViS+SpamAssassin)
  - Blockierung der Einlieferung durch Hosts, die sich nicht protokollkonform verhalten oder keinen PTR-Record haben oder auf globalen Blacklists (Spamhaus) stehen
  - Greylisting, Viren-/Phishingfilter, Spamanalyse/–markierung
  - Recipient Address Validation

E-Mail-Dienste des RRZE: Übersicht (2)

- List Server (Mailman) lists.fau.de (Stand: 09.01.2018)
  - IdM-provisionierte Studierendenlisten (studienfach-/abschluss-/semesterspezifisch) und Mitarbeiterlisten
    - 1.218 Listen in Betrieb
  - Manuell zu pflegende Listen für Forschung und Lehre
    - 1.728 Listen in Betrieb

E-Mail-Dienste des RRZE: Übersicht (3)

- Postfach-Dienst FAUMail (Dovecot)
  - Angebot für Studierende sowie für Beschäftigte von Einrichtungen der FAU mit Bedarf an reiner E-Mail-Funktionalität
  - POP3-/IMAP-/Webmail-Zugang
  - Speicherplatz: 2 GB (Beschäftigte), 1 GB (Studierende)
  - Backend-Server: Dovecot, Web-Frontend: Roundcube
- Groupware-Dienst (MS Exchange)
  - Angebot für Beschäftigte von Einrichtungen der FAU mit Bedarf an Kalenderfunktionalität, Terminverwaltung etc.

E-Mail-Dienste des RRZE: FAU-Mail-Relay (1)

- Hintergrunddienste (für Nutzer weitgehend unsichtbar)
- Zentraler Eintrittspunkt für E-Mail aus dem Internet in die FAU
- „Schutzwall“ für die Mailsysteme innerhalb der FAU und externer Kunden (blockiert ca. 70% aller Einlieferungsversuche von extern)
- Verhältnis angenommener zu abgelehnter E-Mails pro Tag
  - ca. 90 Tsd. / 217 Tsd. (Jahresmittel 2017)

E-Mail-Dienste des RRZE: FAU-Mail-Relay (2)

„Smart-Relays“:

- für Mail-Server innerhalb FAU-Netz: mailhub.rrze.uni-erlangen.de
- für Mail-Clients
  - innerhalb FAU-Netz: smtp.fau.de
  - weltweit: smtp-auth.fau.de (nur mit Authentifizierung und Verbindungsverschlüsselung TLS/SSL)
- Systeme, die nur ohne Authentifizierung versenden können, müssen bei postmaster@fau.de registriert werden (z.B. Scanner, Kopierer, Faxgeräte etc.) und können dann über smtp.fau.de versenden

E-Mail-Dienste am RRZE: SMTP/AUTH

- FAU-Mail-Relay kann mit SMTP/AUTH von FAU-Mitgliedern auch bei Internetanbindung über beliebige Provider zum Einliefern von E-Mails genutzt werden
- Konfigurationsdaten für Mailprogramm:
  - Postausgangsserver: smtp-auth.fau.de
  - Port 587, TLS bzw. STARTTLS aktiviert (bevorzugt)
  - Port 465, SSL aktiviert (alternativ)
  - Benutzername: IdM-Benutzerkennung oder E-Mail-Adresse
  - Passwort: IdM-Passwort

E-Mail-Dienste des RRZE: POP3-/IMAP-Server

FAUMail-Postfächer

- Posteingangsserver: faumail.fau.de
- Zugangsdaten: E-Mail-Adresse, E-Mail-Passwort
- Port 110 (POP3) bzw. 143 (IMAP) mit TLS/STARTTLS (bevorzugt)
- Port 995 (POP3) bzw. 993 (IMAP) mit SSL

Exchange-Postfächer

- Posteingangsserver: groupware.fau.de
- Zugangsdaten: Exchange-Benutzerkennung/-Passwort
- Port 110 (POP3) bzw. 143 (IMAP) mit TLS/STARTTLS (bevorzugt)
- Port 995 (POP3) bzw. 993 (IMAP) mit SSL

Empfohlene Variante für FAUMail: IMAP

E-Mail-Dienste des RRZE: Webmail-Server

FAUMail

- Webmail-Portal https://faumail.fau.de
- Zugangsdaten: E-Mail-Adresse, E-Mail-Passwort

Exchange

- Outlook Web App https://groupware.fau.de
- Zugangsdaten: Exchange-Benutzerkennung/-Passwort

„Gruppen-Mail“ (1)

Oberbegriff für die Adressierung mehrerer Empfänger über eine einzige E-Mail-Adresse

Vom RRZE angebotene Varianten

- Funktionsverteiler am FAU-Mailrelay / Distribution List unter MS Exchange
  - Verteilung an Einzeladressen -> ggf. Mehrfachspeicherung

„Gruppen-Mail“ (2)

- Funktionspostfach unter FAUMail/Shared Mailbox unter MS Exchange
  - Speichernde Stelle mit verantwortlicher Person
  - Freigabemöglichkeit an weitere Personen
  - Funktionalität wie persönliches Postfach
  - Vermeidung von „Password Sharing“
- Mailingliste
  - Listenverwaltungssystem Mailman (Open Source)
  - Mail- und Webinterface für Administratoren und Nutzer
  - Umfangreiche Zugriffsschutzmechanismen
  - Archiv (öffentlich oder nur für Mitglieder zugänglich)

Nachrichtenfilter: Übersicht (1)

- Ausführen bestimmter Aktionen mit E-Mails, die vorgegebene Kriterien bzgl. bestimmter Kopfzeilen und/oder Inhalte erfüllen
- Anwendungen
  - Spam-Filter, siehe http://www.rrze.fau.de/internet-e-mail/e-mail/anti-spam/spam-analyse/
  - Sortierfilter
    - › Ordnen der Mail nach Funktionsbereich des Adressaten anhand klassifizierender Zeichenfolgen in Betreffzeile und/oder weiterer Kopfzeilen etc.
  - Abwesenheitsnotiz

Nachrichtenfilter: Übersicht (2)

- Serverseitige Filter (Delivery Filters)
  - werden vor der Ablage im Serverpostfach ausgeführt
  - FAUMail (Dovecot) unterstützt die Filtersprache ‘Sieve’ (RFC 5228)
    - erlaubt komplexe serverseitige Filterung, nutzbar über
      - FAUMail-Webinterface (Einstellungen -> Filter)
      - Sieve-Plugin für Thunderbird (Extras -> Sieve-Filter)
- Clientseitige Filter
  - werden vom Mailprogramm beim Zugriff auf das Serverpostfach ausgeführt
  - Beispiel: Mozilla Thunderbird (Extras -> Filter)

Nachrichtenfilter: Abwesenheitsnotiz

Beispiel: FAUMail (Dovecot)

- Webinterface https://faumail.fau.de
  - Menü „Einstellungen“ -> „Filter“ -> Filtervorlage „Urlaub“
    - Betreff und Text der Autoantwort eingeben
    - Datum und Uhrzeit für Beginn und Ende der Autoantwort angeben
    - Reiter „Erweiterte Einstellungen“
      - Eigene E-Mail-Adressen, für die der Autoresponder ansprechen soll, mit Komma getrennt eintragen
      - Antwortintervall in Tagen angeben

E-Mail-Einstellungen im IdM-Self-Service (1)

Beantragung / Verwaltung von Dienstleistungen
für FAU-Mitglieder

- IdM-Portal https://www.idm.fau.de
  - Persönliche @fau.de-Adresse beantragen / ändern
    - Menü „Anfragen / Aufgaben“ -> „Dienstleistung“
  - Postfach beantragen

E-Mail-Einstellungen im IdM-Self-Service (2)

- Zustelloptionen (Postfachzustellung / Weiterleitung) ändern
  - Menü „Einstellungen“ -> „E-Mail“ -> Rubrik „E-Mail-Adressen“
    - Schaltfläche „…“ links neben der E-Mail-Adresse anklicken
    - „Anzeigen“
    - Gewünschtes Postfach auswählen und/oder E-Mail-Adresse im Feld „Weiterleitung an eine andere E-Mail-Adresse“ eintragen
- Abonnieren von E-Mail-Themengebieten (Newsletter)
  - https://www.idm.fau.de/go/optInOut/emailOptions

E-Mail-Funktionen im IdM-Admin-Portal

- Verwaltung von Zugriffsberechtigungen bei gemeinsam genutzten Postfächern unter Exchange und FAUMail durch Postfach-Verantwortliche
- Mitgliederverwaltung von Mailinglisten durch List Owner
  - bei IdM-prov. Listen: für statisch verwaltete Mitglieder

E-MAIL-SICHERHEIT

- Inhaltsverschlüsselung (E2E-Verschlüsselung)
- Kryptographische Signatur
- Transportverschlüsselung
- Ausblick: DANE

E-Mail-Sicherheit: Inhaltsverschlüsselung / Kryptograph. Signatur (1)

- Inhaltsverschlüsselung (Ende-zu-Ende-Verschlüsselung)
  - Gewährleistet Vertraulichkeit (nur Adressat kann Inhalt lesen)
  - Einschränkung: Kopfzeilen der E-Mail bleiben unverschlüsselt!
    - Absender, Empfänger, Betreff, … liegen im Klartext vor
- Kryptographische Signatur
  - Gewährleistet Authentizität und Integrität der E-Mail
  - Wird erreicht durch Bildung eines Hash-Wertes über den Inhalt und dessen Verschlüsselung mit geheimem Schlüssel des Senders

E-Mail-Sicherheit: Inhaltsverschlüsselung / Kryptograph. Signatur (2)

- Beide Maßnahmen liegen in der Hand des Nutzers bzw. seines E-Mail-Programms
- Heutige Standardverfahren: OpenPGP und S/MIME
  - Basieren beide auf Public-Key-Kryptographie, sind zueinander inkompatibel

E-Mail-Sicherheit: Transportverschlüsselung (1)

- Secure Sockets Layer (SSL) / Transport Layer Security (TLS)
  - Hybridverschlüsselung
    - Identifikation/Authentifikation der Kommunikationspartner sowie Aushandlung eines Sitzungsschlüssels erfolgt mittels Public-Key-Kryptographie (asymmetrische Verschlüsselung)
    - Ver- und Entschlüsselung der Nutzdaten erfolgt jeweils mit dem Sitzungsschlüssel (symmetrische Verschlüsselung)
  - Sicherer Datenkanal zwischen potenziell unsicheren Transportknoten

E-Mail-Sicherheit: Transportverschlüsselung (2)

- I.d.R. nur Einlieferungsweg für E-Mails zwingend verschlüsselt, die Kommunikation der MTAs untereinander nur optional und vom Nutzer nicht beeinflussbar
- Optimal: Kombination aus Transport- und Inhaltsverschlüsselung

E-Mail-Sicherheit: OpenPGP vs. S/MIME (1)

- OpenPGP („Pretty Good Privacy“)
  - Für Daten aller Art geeignet
  - Basiert auf mit lokaler Software generierbaren Schlüsselpaaren (Public/Private Key)
  - Teilnehmer können sich gegenseitig Vertrauen aussprechen und ihre Public Keys signieren (Web of Trust)
  - In vielen Programmen per Plugin integrierbar
    - Thunderbird: via Plugin „Enigmail“
    - Outlook: via Plugin „GpgOL“ (Teil von Gpg4win)

E-Mail-Sicherheit: OpenPGP vs. S/MIME (2)

- S/MIME
  - Nur für E-Mails geeignet
  - Basiert auf von offiziellen Zertifizierungsstellen (CAs) ausgestellten Zertifikaten im X.509-Format
  - Hierarchische Zertifizierungskette, deren Zertifikate allesamt im Mailprogramm installiert sein müssen
  - In vielen Programmen integriert
  - Thunderbird: einfach nutzbar
  - Outlook: gut integriert

E-Mail-Sicherheit: OpenPGP

- Standardisiertes Datenformat für verschlüsselte und kryptographisch signierte Daten (RFC 4880, Nov. 2007)
- Hauptanwendung: Signierung und Verschlüsselung von E-Mails
  - Prinzipiell zur Verschlüsselung beliebiger Daten geeignet
- Formate bei E-Mail-Verschlüsselung:
  - PGP/INLINE
    - E-Mail wird als Text-Mail erzeugt, welche die Signatur bzw. den verschlüsselten Inhalt in Radix64-kodierter Form (=Base64+Prüfsumme) enthält
  - PGP/MIME
    - Digitale Signatur bzw. verschlüsselter Inhalt wird als eigener MIME-Part in die E-Mail integriert

E-Mail-Sicherheit: S/MIME

- Secure/MIME (RFC 3851, Juli 2004)
- Zweck: Kryptographische Signierung und Inhaltsverschlüsselung von E-Mails
- Basiert auf Zertifizierungshierarchie (Wurzelzertifikat -> Zwischenzertifikate -> Nutzerzertifikat)
  - Beispiel: FAU: Telekom Root-CA -> DFN-CA -> FAU-CA
- Beantragung eines Nutzerzertifikats für dienstliche Belange an der FAU: http://www.rrze.fau.de/internet-e-mail/zertifikate/

E-Mail-Sicherheit: OpenPGP mit Thunderbird (1)

- OpenPGP für Thunderbird: Plugin „Enigmail“
  - Stellt Menü „Enigmail“ zur Verfügung
    - Einrichtung über „Einrichtungsassistent“ oder manuell über „Einstellungen“
- Freie OpenPGP-Implementierung GnuPG (Gnu Privacy Guard)
  - In Linux-Distributionen bereits enthalten
  - Für Windows über http://www.gpg4win.de erhältlich
    - vom Bundesamt für Sicherheit in der Informationstechnik (BSI) beauftragt

E-Mail-Sicherheit: OpenPGP mit Thunderbird (2)

- Zunächst Schlüsselpaar erzeugen und geheimen Schlüssel mit Passphrase sichern oder bereits vorhandenes Schlüsselpaar importieren
  - Menü „Enigmail“ -> „Schlüssel verwalten“

- OpenPGP für E-Mail-Konto aktivieren
  - Kontextmenü „Einstellungen“ -> „OpenPGP-Sicherheit“
  - Schlüssel auswählen
    - via E-Mail-Adresse oder Empfängerregeln

E-Mail-Sicherheit: S/MIME mit Thunderbird

- Zertifikat in Thunderbird importieren
  - Einstellungen -> Erweitert -> Zertifikate
- S/MIME für E-Mail-Konto aktivieren
  - Konto markieren -> Kontextmenü „Einstellungen“ -> S/MIME-Sicherheit
    - Digitale Unterschrift
      - Zertifikat auswählen (falls mehrere vorhanden)
      - Nachrichten digital unterschreiben (als Standard)
    - Verschlüsselung
      - Zertifikat auswählen (falls mehrere vorhanden)
      - Standard-Verschlüsselung: Nie

Schwachpunkte bei TLS / OpenPGP / S/MIME (1)

- Schwachpunkte bei TLS
  - Aushebeln der Verschlüsselung durch Man-in-the-Middle-Angriff möglich (Herausfiltern des STARTTLS-Kommandos)
  - Zertifikatsausstellung/-prüfung
    - Jede Zertifizierungsstelle (CA) darf Zertifikate für jeden Hostnamen ausstellen
      - Gefährdung der einwandfreien Identifikation des Kommunikationspartners, sobald eine CA nachlässig arbeitet / prüft
  - DNS-Cache-Poisoning (Einschleusen falscher Informationen)

Schwachpunkte bei TLS / OpenPGP / S/MIME (2)

- Schwachpunkte bei OpenPGP
  - Schlüsselverteilung
    - Jeder kann Schlüssel für jede E-Mail-Adresse auf Schlüsselserver hochladen
    - Manuelle Schlüsselüberprüfung (Fingerprint) ratsam, aber nicht zwingend

Fazit: Vermeintlich gesichert übertragene Daten können in unbefugte Hände gelangen

Lösung: DANE (1)

DNS-based **A**uthentication of **N**amed **E**ntities

- Protokollfamilie, die DNSSEC-Infrastruktur zur Authentisierung verwendet (RFCs 6698 (2012); Updates: 7218 (2014), 7671 (2015))
  - DANE/TLSA (RFC 6698, Aug. 2012)
    - for SMTP (RFC 7672, Oktober 2015)
  - DANE/OPENPGPKEY (RFC 7929, Aug. 2016)
  - DANE/SMIMEA (RFC 8162, Mai 2017)

Lösung: DANE (2)

- Prinzip: DNS als sichere Schlüssel- bzw. Zertifikatsablage
  - Schlüssel / Zertifikate nur aus einer einzigen Quelle, auf die nur der legitime Verwalter schreibenden Zugriff hat

- Voraussetzung: DNSSEC (RFC 4033ff)
  - Manipulationssichere Auslieferung von DNS-Informationen durch kryptografische Signatur aller Resource Records (RR)
    - › Zusätzlich Auslieferung eines RRSIG-Records zu jedem RR

DANE: Aktivitäten / Perspektiven (1)

- Aktivitäten
  - „Kleine“ Provider als Vorreiter
    - Posteo (Mai 2014): Erstmals Mailtransport mit DANE abgesichert
  - Empfehlung durch Bundesamt für Sicherheit in der Informationstechnik (BSI) im August 2015
  - Provider des „E-Mail made in Germany“-Verbunds (GMX, WEB.DE) schwenken auf DANE um
  - Bayerische Hochschulen kooperieren zur Einführung von DNSSEC und DANE (FAU: DNSSEC und DANE/TLSA für Mailtransport seit 09/2016)

DANE: Aktivitäten / Perspektiven (2)

- Entwicklung eines SMIMEA-Plugins für Thunderbird durch Verisign
- SMILLA (SMIMEA-Milter für Mailserver, Open Source, sys4/Posteo)
- Openpgpkey-Milter (Proof of Concept, Paul Wouters, 2013/14)

- Perspektiven
  - Zweifelsfreie Identifizierung der Kommunikationspartner
  - Nutzung selbstsignierter Zertifikate möglich
  - Automatisierung der Mailverschlüsselung

Dokumentation / Literatur

- E-Mail-Dienste am RRZE
  http://www.rrze.fau.de/internet-e-mail/e-mail/
- RRZE-Starthilfe
  http://www.starthilfe.rrze.fau.de/internet-und-email/
- Antworten auf die häufigsten Fragen
  http://www.faq.rrze.fau.de
- Anleitung: PGP und S/MIME mit Thunderbird und Outlook
  http://www.blafusel.de/files/quis_custodiet_custodes.pdf
- DANE: Automatische Mailverschlüsselung mit S/MIME
  http://www.heise.de/netze/meldung/DANE-Automatische-Mail-Verschluesselung-mit-S-MIME-3041530.html

ORGANISATORISCHES

- Die Vorträge im Überblick
- Andere Vortragsreihen des RRZE
- Ablageorte Vortragsfolien
- RRZE-Veranstaltungskalender / Mailingliste abonnieren
- Themenvorschläge & Anregungen

Weitere Vorträge im Rahmen der „Netzwerkausbildung“

- immer mittwochs (ab 14 c.t.) in Raum 2.049 am RRZE

18.10.2017 – Modelle, Begriffe, Mechanismen
25.10.2017 – Lokale Netze: Switching, Routing, Strukturierung
08.11.2017 – Troubleshooting von WLAN- und VPN-Problemen
15.11.2017 – TCP-/IP-Troubleshooting
29.11.2017 – Handeln mit Adressen – ARP, DHCP, DNS
06.12.2017 – IP-FAU-6 (Teil 1)
13.12.2017 – IP-FAU-6 (Teil 2)
10.01.2018 – Elementare Sicherheitsmaßnahmen: Firewall und Netzzugriff
17.01.2018 – Anschluss von Wohnheimnetzen
24.01.2018 – Traffic Engineering: Proxy, NAT
31.01.2018 – Routingprotokolle
07.02.2018 – E-Mail-Grundlagen

Andere Vortragsreihen des RRZE

Campustreffen

- immer donnerstags ab 15 Uhr c.t.
- vermittelt Informationen zu den Dienstleistungen des RRZE
- befasst sich mit neuer Hard- & Software, Update-Verfahren sowie Lizenzfragen
- ermöglicht den Erfahrungsaustausch mit Spezialisten

Systemausbildung „Grundlagen und Aspekte von Betriebssystemen und System-nahen Diensten”

- immer mittwochs ab 14 Uhr c.t. (in den Sommersemestern)
- Ergänzung zur Netzwerkausbildung “Praxis der Datenkommunikation”
- führt in den grundsätzlichen Aufbau eines Systems sowie eingesetzte Techniken und Komponenten ein
- richtet sich primär an alle Interessierten (Studierende & Beschäftigte)

Vortragsfolien & Vortragsaufzeichnung

Die Vortragsfolien werden nach der Veranstaltung auf der Webseite des RRZE abgelegt:
http://www.rrze.fau.de/ausbildung-schulung/veranstaltungsreihen/netzwerkausbildung/

Die meisten Vorträge des RRZE werden aufgezeichnet und können nach der Veranstaltung vom Videoportal der FAU heruntergeladen werden:
www.fau.tv

RRZE-Veranstaltungskalender & Mailinglisten

- Kalender abonnieren oder bookmarken
  - Alle Infos hierzu stehen auf der Webseite des RRZE unter: http://www.rrze.fau.de/news/kalender.shtml

- Mailingliste abonnieren
  - Wöchentliche Terminhinweise werden zusätzlich an die Mailingliste RRZE-Aktuelles gesendet, abonnierbar für FAU-Mitglieder unter: https://www.idm.fau.de/go/optInOut/emailOptions

Themenvorschläge & Anregungen

Themenvorschläge und Anregungen nehmen wir gerne entgegen!

Bitte schreiben Sie uns einfach eine E-Mail an:
rrze-zentrale@fau.de (Betreff: Netzwerkausbildung)

Vielen Dank für Ihre Aufmerksamkeit!

Regionales RechenZentrum Erlangen [RRZE]
Martensstraße 1, 91058 Erlangen
http://www.rrze.fau.de