# EHLO

# 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

# ARC – Authenticated Received Chain

## Themenüberblick

- kurz SPF, DKIM und DMARC
- Authentication-Results Header
- ARC - Authenticated Received Chain

# SPF - RFC 7208 (ehem. 4408)

- DNS TXT Records definieren legitimierte Mailrelays für fragliche Domain
  - $ host -t txt blafasel.at
    blafasel.at descriptive text "v=spf1 include:_spf.blafasel.at mx -all"
  - $ host -t txt utanet.at
    utanet.at descriptive text "v=spf1 ip4:213.90.36.0/25 ... ?all"

- Nutzen von SPF alleine leider gering
- Aufwand durch SRS erheblich erhöht
- RFC 7208 streicht SPF RR. Nur noch TXT RR

# DKIM
# DomainKeys Identified Mail

- http://www.dkim.org/
- Erweiterte Kombination aus
    - Yahoo! DomainKeys
    - CISCO Identified Mail
- Erster Baustein im Mai 2007 => RFC 4871
- Author Domain Signing Practices (ADSP)
  seit August 2009 => RFC 5617 => deprecated
- neueste Version RFC 6376

# DKIM - technisches

- signiert Teile des Headers und den Body
- Signatur im Mailheader

```
DKIM-Signature: v=1; a=rsa-sha256; c=relaxed/relaxed;
        d=univie.ac.at; s=rev1; h=Message-ID:Date:From:MIME-Version:To:
        Subject:Content-Type:Content-Transfer-Encoding; bh=CHKp57xvG+TkL
        tX7hfa7jYenETIpLWpRR7c1cM4GJ3E=; b=bxs//cYqDJTBuZ93e2rmpZyyVmpHP
        ....
```

- PublicKey als DNS TXT

```
# host -t txt rev1._domainkey.univie.ac.at
rev1._domainkey.univie.ac.at descriptive text "v=DKIM1\; k=rsa\; g=*\; s=email\; t=y\; p=MIGfMA....."
```

- signiert bzw. verifiziert wird durch border MTAs.

# DKIM vs. SPF

- bezieht sich auf From: Header anstatt auf envelope from
- keine TXT Records für die Domain selbst
    - <selector>._domainkey.<domain>
- keine Verifikation des Pfades
    - keine Probleme mit Forwards (SRS)
    - leichtere Sender Delegation

# DMARC

- https://dmarc.org/
- Im Grunde eine Kombination von DKIM und SPF
- Wird von Google, Facebook, Yahoo & Co getrieben
- RFC 7489
- policy in TXT RR _dmarc.domain.tld

```
$ dig +short _dmarc.univie.ac.at TXT
"v=DMARC1\; p=none\; rua=mailto:dmarc-rua@univie.ac.at"
```

- automatische XML reports an in der policy definierte Adressen

# DMARC - Verifzierungsschritte

- RFC 5322 From: Domain
- DMARC TXT RR? nein => no policy, sonst...
- DKIM-Signaturen werden geprüft
- SPF check
- Wenn eine verifizierte DKIM-Signatur (d=) zu DMARC Domain passt => pass
- Wenn die SPF Domain (envelope from) zu DMARC passt und der SPF check “pass” ergeben hat => pass
- Domaincheck policy (adkim, aspf; default relaxed)
    - relaxed: organisational domain match
    - strict: FQDN match

# Authentication-Results – RFC 7001

Authentication-Results: blafasel.at;
iprev=pass (mail-wr0-x229.google.com) smtp.client-ip=2a00:1450:400c:c0c::229;
spf=pass smtp.mailfrom=gmail.com;
dkim=pass header.d=gmail.com header.s=20161025 header.a=rsa-sha256;
dmarc=pass header.from=gmail.com;
arc=none

Authentication-Results: mx.google.com;
dkim=pass header.i=@googlegroups.com header.s=20161025 header.b=nrsMFpch;
spf=pass (google.com: ... permitted sender) smtp.mailfrom=...@googlegroups.com;
dmarc=pass (p=NONE sp=NONE dis=NONE) header.from=googlegroups.com

# ARC – Authenticated Received Chain

- http://arc-spec.org/
    - draft-ietf-dmarc-arc-protocol
    - draft-ietf-dmarc-arc-usage
- ADMD - Administrative Management Domain
- ARC-Set bestehend aus
    - ARC-Message-Signature
    - ARC-Authentication-Results
    - ARC-Seal
- Mehrere ARC-Sets werden zur Chain

# ARC – Header

- Alle Header haben einen i= Tag mit einer laufenden Nr.
- ARC-Authentication-Results
  - selber Inhalt wie Authentication-Results + i= Tag
- ARC-Message-Signature
  - ähnlich wie DKIM-Signatur
  - signiert Message-Body und selektiv Header jedoch nie ARC-Header und Authentication-Results
    - Notiz: Google signiert derzeit mit Draft-06 und exkludiert nur ARC-Seal-Header.
- ARC-Seal
  - weitere Signatur, die alle ARC-Header signiert

# ARC – Verifikation

- Informationen von allen ARC-Sets sammeln
  - wenn keine vorhanden: state=none
- alle ARC-Sets müssen komplett sein
- die Chain muss beginnend bei 1 durchgehend nummeriert sein und darf keine doppelten Einträge haben.
- Der cv= Tag in den ARC-Seals muss für i=1 none und i>1 pass sein
- ARC-Message-Signaturen von N → 1 verifizieren
- ARC-Seal-Signaturen von N → 1 verifizieren
- Nur wenn alles ok state=pass, sonst state=fail

# ARC – signieren

- j++
- ARC-Authentication-Results erzeugen
- ARC-Message-Signature erzeigen
- ARC-Seal erzeugen

# Links

- Main site
  http://arc-spec.org/
- Authenticated Received Chain (ARC) Protocol Draft
  https://datatracker.ietf.org/doc/draft-ietf-dmarc-arc-protocol
- ARC Usage Draft
  https://datatracker.ietf.org/doc/draft-ietf-dmarc-arc-usage

# Fragen?