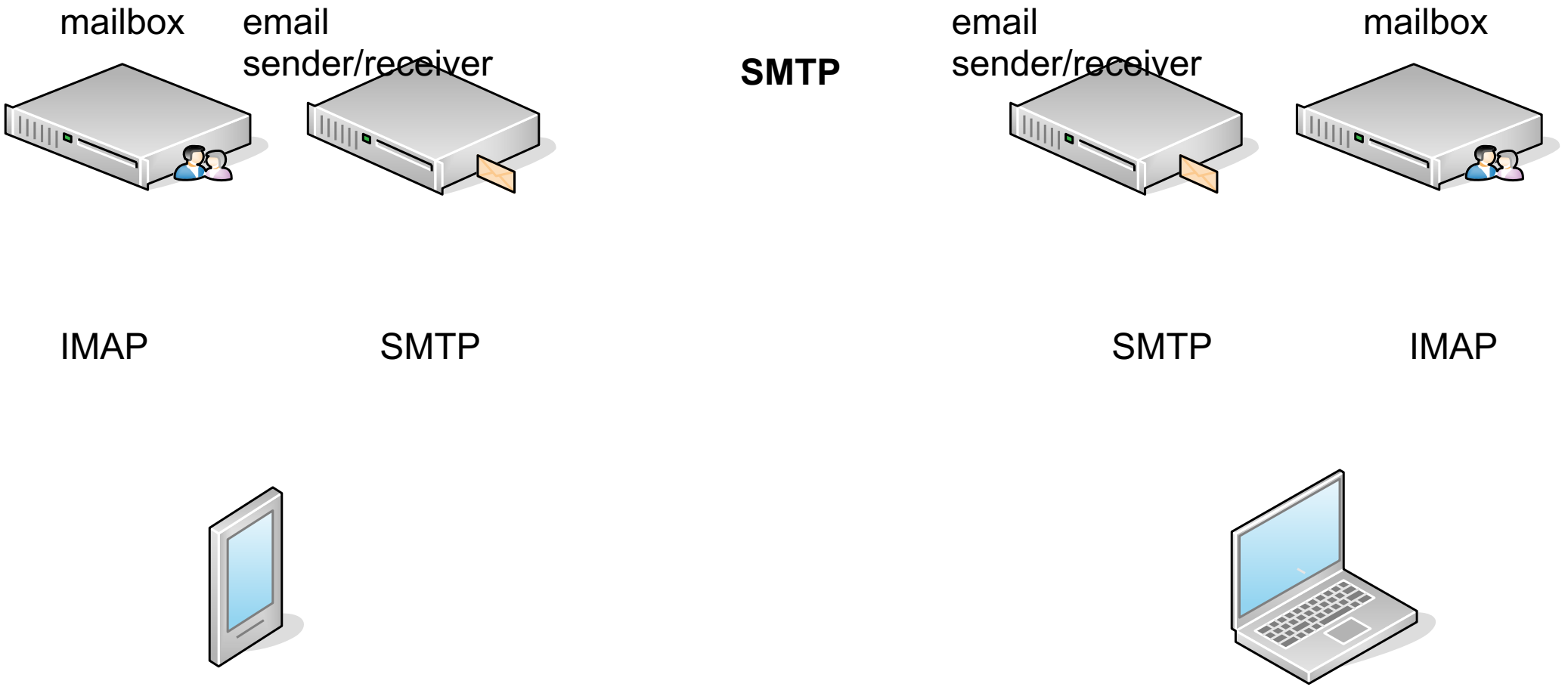
Email and DKIM/DMARC in theory and practice

József Kadlecsik
Wigner Research Centre for Physics
kadlecsik.jozsef@wigner.hu

Content

- Email and SMTP
- DKIM
- DMARC
- Practical issues

Email communication

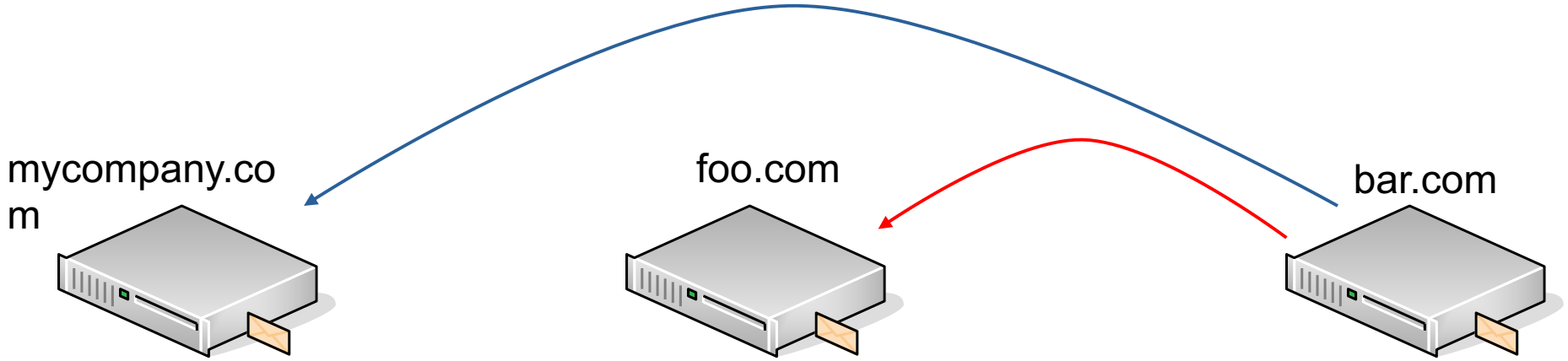


Simple Mail Transport Protocol

- Store and forward
  - Mail queue
- Email cannot be lost (without trace)
  - Logging
  - Bounce email
- Cleartext
  - Auditor :-)
- DNS: MX, A, AAAA, TXT, NS, PTR

SMTP forward

Forward: somebody@foo.com → otheraddress@bar.com



MAIL FROM: <boss@mycompany.com>
RCPT TO: <somebody@foo.com>

MAIL FROM: <somebody@foo.com>
RCPT TO: <otheraddress@bar.com>

MAIL FROM: <boss@mycompany.com>
RCPT TO: <otheraddress@bar.com>

Envelope – header - body

MAIL FROM: <far@away.galaxy>	Bounce email address
RCPT TO: <victim@your.place>	Mailbox email address
From: "XY Bank" <admin@another.galaxy>	What we „see” as sender
To: "Alice" <victim@your.place>	Intended recipient
Subject: Invoice	Subject
Urgent!	Email body
Click here: https://got.you/	

What you see as user

From: XY Bank
Subject: Invoice

Urgent!
Click here!

DKIM

- DKIM: DomainKeys Identified Mail
  - DKIM-Signature added to the header:
    - Hash of signed headers
    - Hash of message body
  - RSA keypair, easy to rotate:
    - private: signing
    - public: verification
  - DNS TXT record: public key

DNS TXT record

- `20151130._domainkey.wigner.hu. 14400 IN TXT "v=DKIM1; k=rsa; t=s; p=...`
- Selector
  - Arbitrary
- t=y:s
  - y: testing
  - s: key valid for subdomains as well

DKIM-Signature header example

```
DKIM-Signature: v=1; a=rsa-sha256; c=relaxed/relaxed;
d=wigner.hu; h=mime-version:user-agent:references:message-
id:in-reply-to:from:from:date:date:subject; s=20151130;
t=1457883089; x=1459697490;
bh=j2e9uzF+s/6GFmD7tMPBt+euSO00ED90w1DtcZV4qzM=;
b=lVfBi+HWrvtH+ttd70HFeK6tswYzrER4DAes/Mi
```

Are we ready?

- External site receives an email from our namespace without DKIM-Signature:
  - How does it know we use DKIM?
  - Selector

DMARC

- Domain-based Message Authentication, Reporting and Conformance
- We tell the world we use DKIM (and SPF)
  - Announce policy to the receivers
    - none
    - quarantine
    - reject
  - DNS TXT record

DMARC DNS record

```
_dmarc.wigner.hu.  1800    IN  TXT
    "v=DMARC1; p=none; adkim=s;
pct=100; rua=mailto:dmarc-
report@wigner.hu; ruf=mailto:dmarc-
report@wigner.hu"
```

DKIM problems in practice

- Software configuration mistakes
  - Proxy firewall
- External portals
- Attacks in the name part of email address
  - From: „XY Bank” <random@email.address>
- Mailing lists

Mailing lists can break DKIM

- Modified header
  - Subject is modified
- Modified email body
  - Mailing list textual header or footer added

Solutions

- DKIM compatible mailing list settings
  - Mailing list address goes into From:
  - Original poster into Reply-To:
  - Generare own DKIM signature
- ARC

Summary

- DKIM and DMARC are good and necessary
- Adopt it