CERT.LV

Informācijas tehnoloģiju drošības incidentu novēršanas institūcija

Email Authentication for Penetration Testers

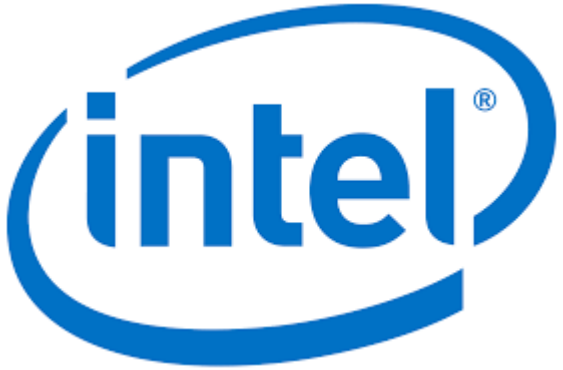
29.12.2019, 36c3

Andrew Konstantinov, andrejs@cert.lv

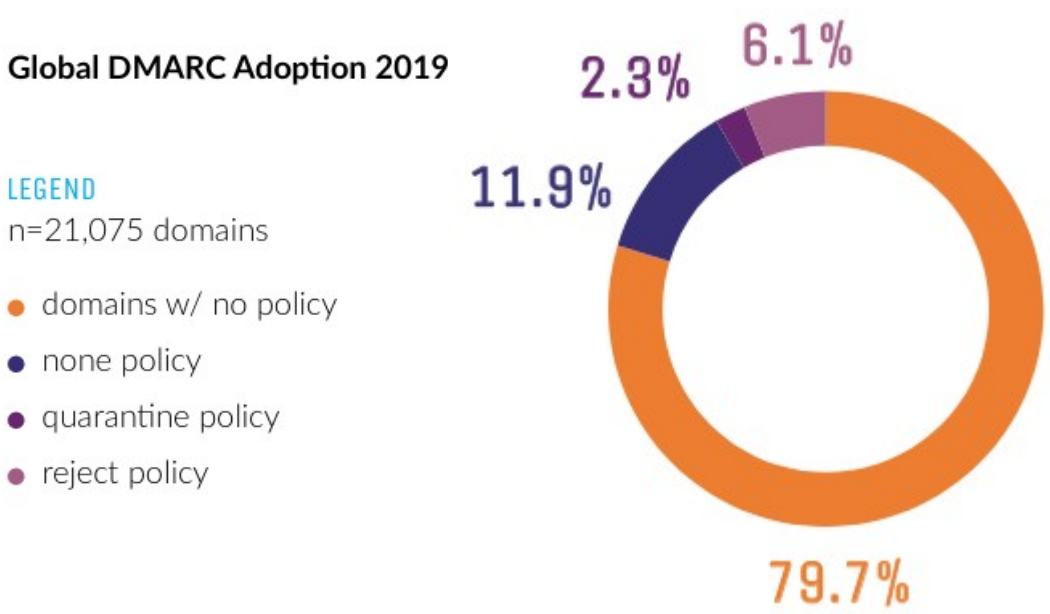
Who am I?

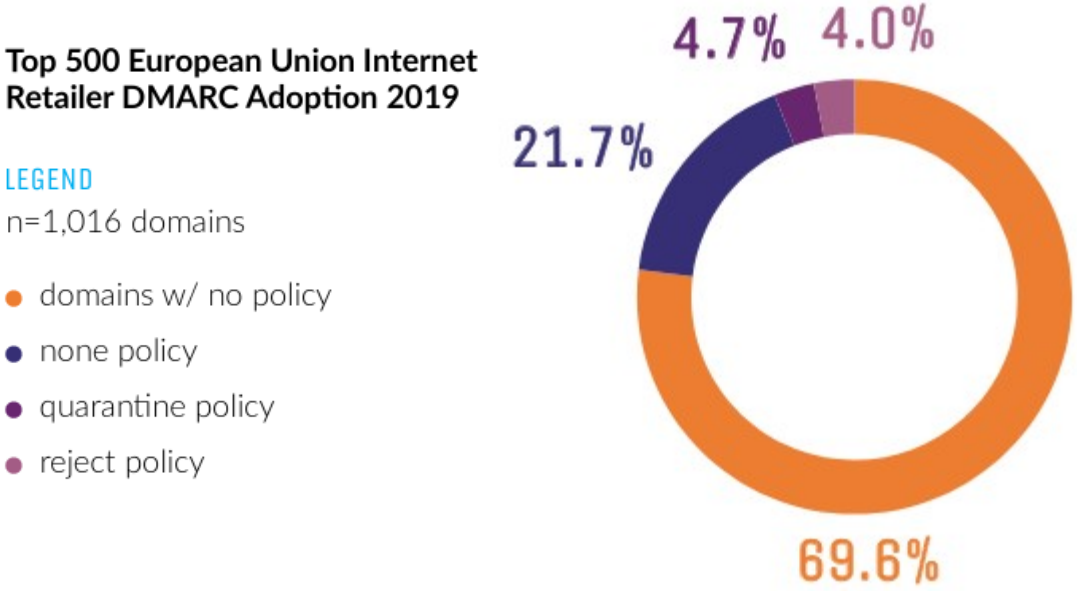
- Andrew, andrejs@cert.lv
  - 679A C8D4 A391 6736 D558 07C1 D3D9 0B7C 666A EDCD

- Currently work for: **cert.lv**
- Previously worked at:



Why pentesters should care?





Source: "Global DMARC Adoption 2019" by 250ok

Contents

Who is this talk for?

- Penetration testers / Red teamers
- Sysadmins / Mail admins
- Newbies willing to learn about email

Email threat landscape

- Insufficient account authentication (passwords & more)
- Webmail (usual web app risks)
- Phishing / Spearphishing / BEC
  - Attacks relying on user error
  - **Attacks w/o any user-visible signs of tampering**
- Vulnerability assessment (missed patches & configuration errors)
- DoS (incl. spam)

Topic of this talk

A little (poorly kept) secret

- (Availability && Reliability) >>> Security
- Support costs easier to quantify than risk
- Backwards compatibility >>> Innovation

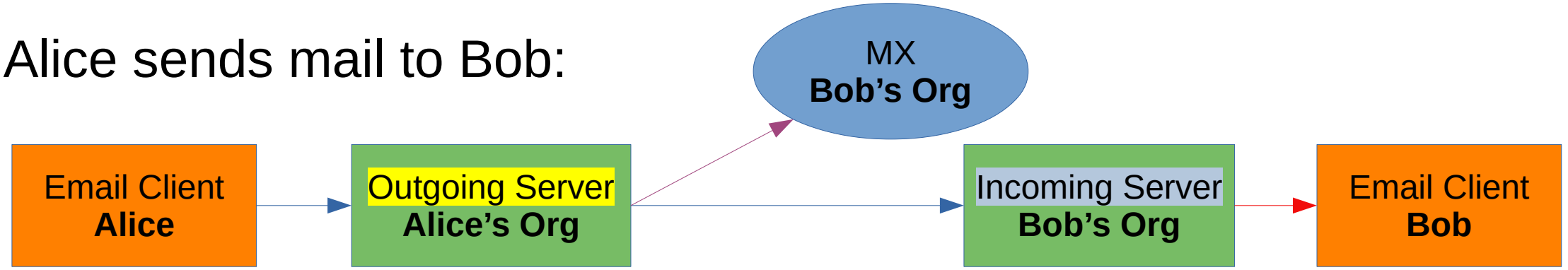
CERT.LV

Informācijas tehnoloģiju drošības incidentu novēršanas institūcija

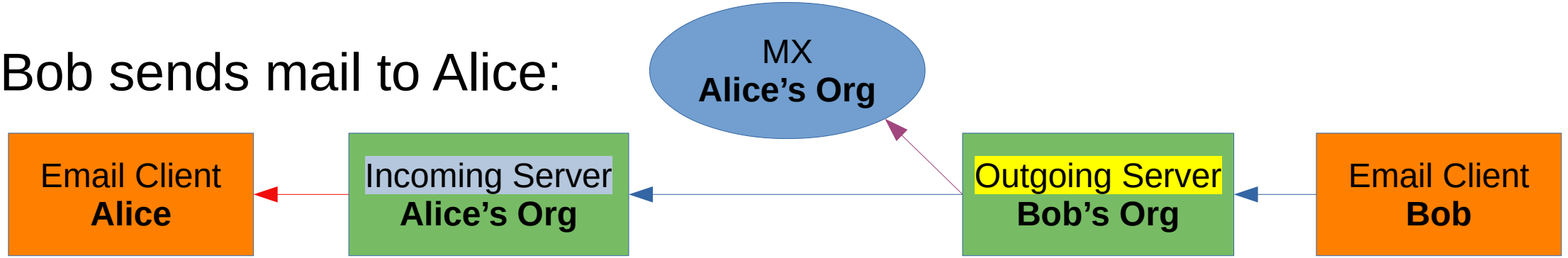
Intro to SMTP

Normal data flow

1) Alice sends mail to Bob:

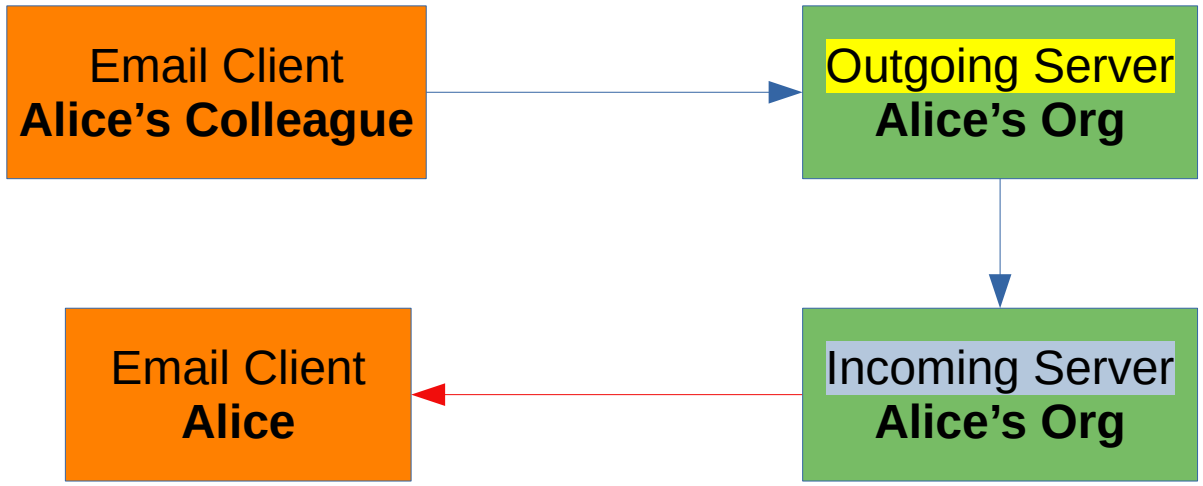


2) Bob sends mail to Alice:



Normal data flow

3) Alice receives mail from her colleague:



An example of SMTP conversation

SMTP Envelope
(RFC 5321)

HELO sendhost.a.org
MAIL FROM: <alice@a.org>
RCPT TO: <bob@b.org>
DATA

Content/Message
(RFC 5322)

From: “Alice” <alice@a.org>
To: “Bob” <bob@b.org>
Date: Sat, 29 Dec 2019 14:00:00 +0100
Subject: Test message

Hi Bob,

Long time no see. How are you?

Bye
.

QUIT

Headers

Body

Envelope-Sender vs From

Email as seen by me:

Email as seen by email admins:

From: relatives

RFC 5322 (3.6.2) defines following Originator headers:

- From:
  - Max 1 header, may contain multiple addresses
- Sender:
  - Max 1 header, may contain one address
- Reply-To:
  - Max 1 header, may contain multiple addresses

In practice:

- Messages with malformed headers still likely to be delivered (best effort)
- If more than 1 header present, typically the 1st one takes priority
- Resent-From: and Resent-Sender: have similar semantics
- Headers displayed to user are implementation-dependent
- None of the Originator headers are actually required

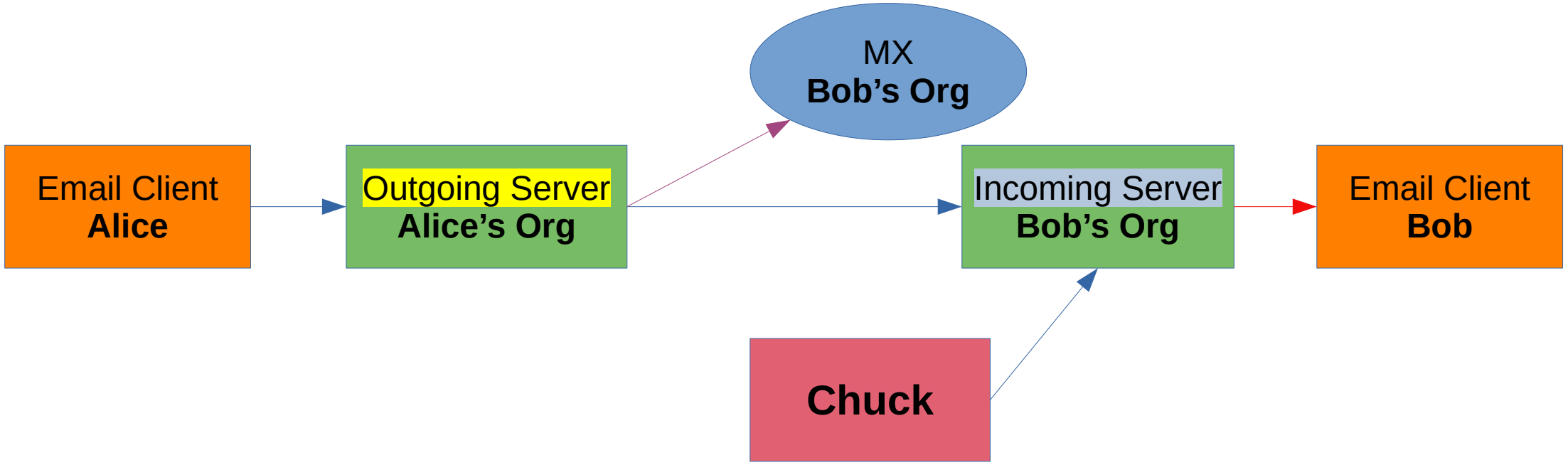
CERT.LV

Informācijas tehnoloģiju drošības incidentu novēršanas institūcija

Basic spoofing

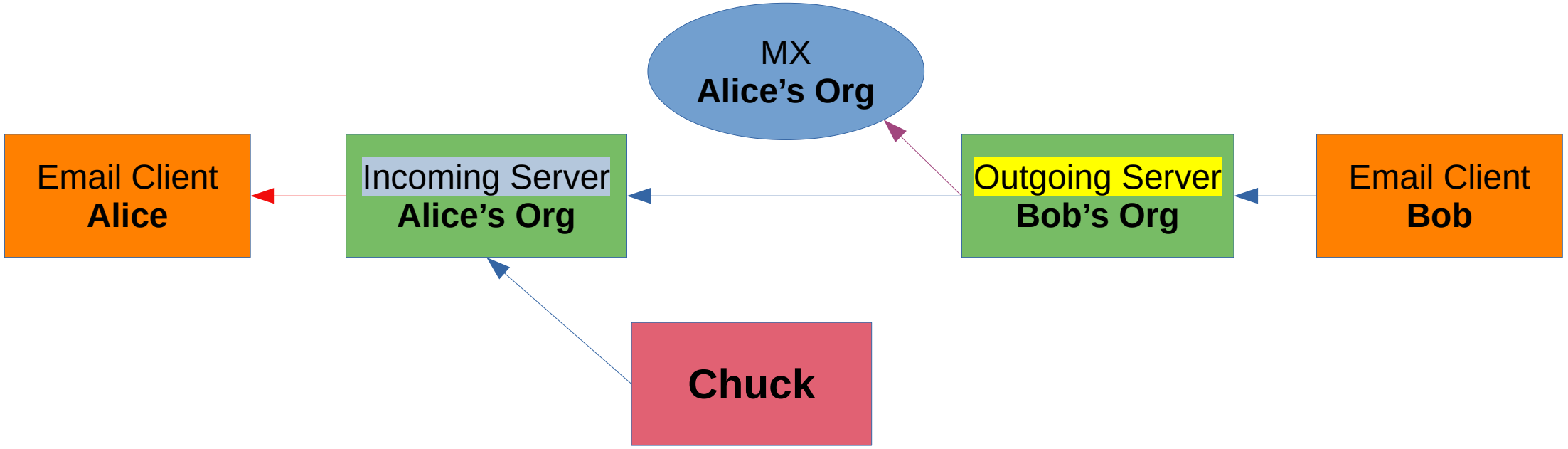
Data flow in spoofing attacks

1) Chuck sends mail to Bob, impersonating Alice



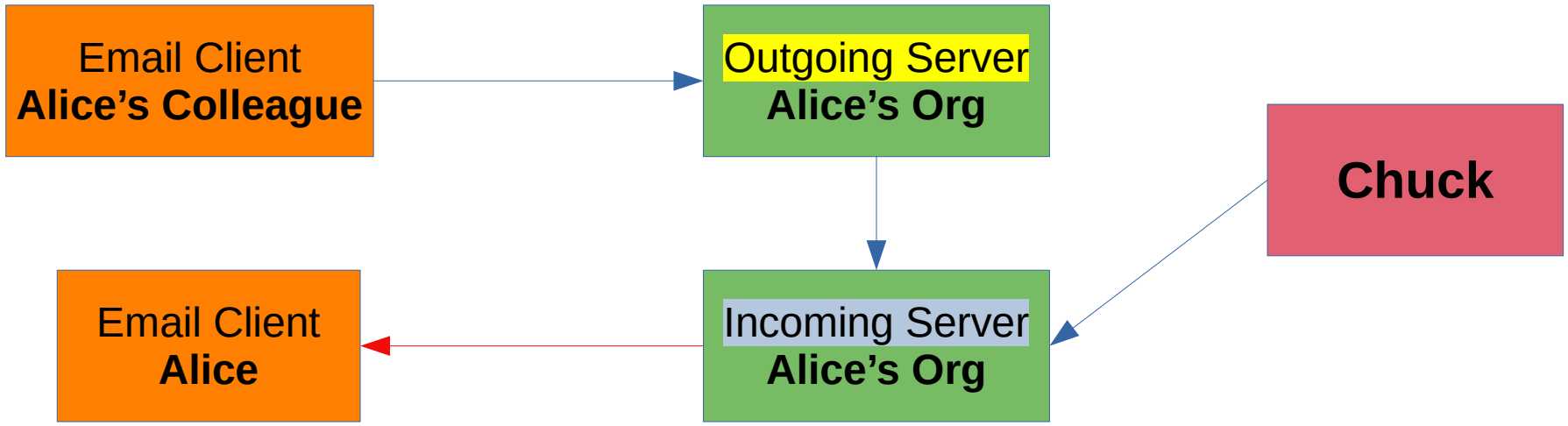
Data flow in spoofing attacks

2) Chuck sends mail to Alice, impersonating Bob



Data flow in spoofing attacks

3) Chuck sends mail to Alice, impersonating her coworker



You've been hacked! (or have you?)

From pimp@parkdalehookers.ca
Subject **pimp@parkdalehookers.ca is hacked**
To markmark <pimp@parkdalehookers.ca>

Hello!

My nickname in darknet is prasad90.
I hacked this mailbox more than six months ago,
through it I infected your operating system with a virus (trojan) created by me and have been monitoring you for a long time.

So, your password from pimp@parkdalehookers.ca is markmark

Even if you changed the password after that - it does not matter, my virus intercepted all the caching data on your computer
and automatically saved access for me.

I have access to all your accounts, social networks, email, browsing history.
Accordingly, I have the data of all your contacts, files from your computer, photos and videos.

I was most struck by the intimate content sites that you occasionally visit.
You have a very wild imagination, I tell you!

During your pastime and entertainment there, I took screenshot through the camera of your device, synchronizing with what you are watching.
Oh my god! You are so funny and excited!

I think that you do not want all your contacts to get these files, right?
If you are of the same opinion, then I think that $816 is quite a fair price to destroy the dirt I created.

Send the above amount on my BTC wallet (bitcoin): 1FHPbKHcSx9CaXJzDpLoXG733ipQ77UNx9
As soon as the above amount is received, I guarantee that the data will be deleted, I do not need it.

Otherwise, these files and history of visiting sites will get all your contacts from your device.
Also, I'll send to everyone your contact access to your email and access logs, I have carefully saved it!

Since reading this letter you have 48 hours!
After your reading this message, I'll receive an automatic notification that you have seen the letter.

I hope I taught you a good lesson.
Do not be so nonchalant, please visit only to proven resources, and don't enter your passwords anywhere!
Good luck!

1) Change password if still in use
2) Identify hacked service (HaveIBeenPwned, Firefox Monitor)
3) Stop reusing passwords & Start using password manager
4) Enable MFA
5) **Ask your email admin to implement anti-spoofing**

A spoofed SMTP conversation

SMTP Envelope
(RFC 5321)

HELO sendhost.a.org
MAIL FROM: <alice@a.org>
RCPT TO: <bob@b.org>
DATA

Content/Message
(RFC 5322)

From: “Alice” <alice@a.org>
To: “Bob” <bob@b.org>
Date: Sat, 29 Dec 2019 14:00:00 +0100
Subject: Test message

Hi Bob,

Long time no see. How are you?

Bye
.

QUIT

Headers

Body

Ad-hoc protection mechanisms

Limited efficacy against spoofing:

- Check sender's existence through SMTP callback
- Check that hostname in HELO/EHLO matches sender IP
  - Resolve hostname
  - Make reverse DNS lookup (PTR record) for sender IP

Not effective at all, but need to take in account

- Reputation of sender IP (DNS blacklists)
- Greylisting

CERT.LV

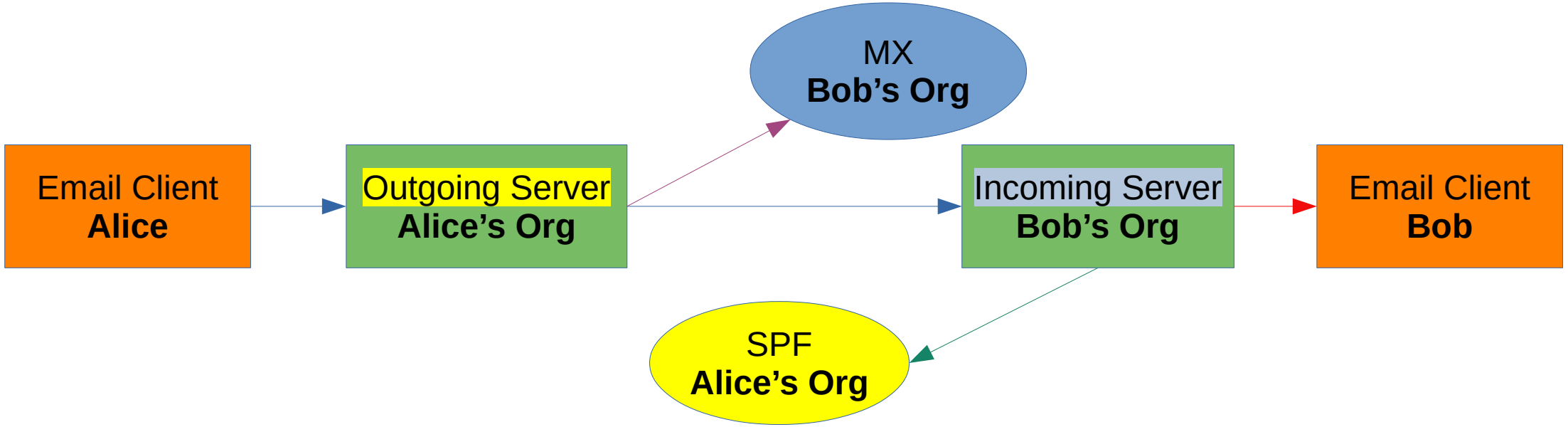
Informācijas tehnoloģiju drošības incidentu novēršanas institūcija

Intro to SPF

Sender Policy Framework (SPF)

Mirrors MX records

Envelope-Sender limits hosts that are allowed to send mail



SPF syntax

Example: v=spf1 ip4:234.123.61.237 -all

Common mechanisms:

- IP4 / IP6
- A
  - Resolve DNS entry (a:smtp.alice.tld)
  - Without listing a DNS entry, resolves domain part after @ (typically points to the web server)
- MX
  - Resolve **incoming** mail servers (mx:alice.tld)
- ALL
- INCLUDE

Qualifiers

- \+ (PASS)
  - The default one, rarely used explicitly
- \- (FAIL)
  - Usually used with “-ALL”
- ~ (SOFTFAIL)
  - Testing, mail should not rejected if matches here

Examples

- v=spf1 a a:smtp.alice.tld -all
- v=spf1 include:_spf.google.com -all

Usage of SPF globally

- ~75% of 100k
- ~55% of 1m
- Majority uses SOFTFAIL
- Source: https://trends.builtwith.com/mx/SPF
- Note:
  - Not all websites might have mails (those should have “v=spf1 -all”)
  - Impossible to calculate how many incoming servers check it

CERT.LV

Informācijas tehnoloģiju drošības incidentu novēršanas institūcija

Spoofing mails protected by SPF

~ALL

E.g. recommended record for G Suite:

- “v=spf1 include:_spf.google.com **~all**”

Why SOFTFAIL is popular:

- Bugs in configuration/implementation
- “**-ALL**” breaks naïve forwarding, mailing lists
- “**~ALL**” enough for delivery to major hosters (mass effect)

A tricky case of “include”

Example:

- “v=spf1 **include**:spf.protection.outlook.com -all”

Quote from RFC:

- In hindsight, the name "include" was poorly chosen. Only the evaluated result of the referenced SPF record is used, rather than literally including the mechanisms of the referenced record in the first. For example, evaluating a "-all" directive in the referenced record does not terminate the overall processing and does not necessarily result in an overall "fail". (Better names for this mechanism would have been "if-match", "on-match", etc.)

Wrong usage:

- No “-ALL” in the top record (default is “?ALL” which makes result NEUTRAL)
- “~ALL” in the top, “-ALL” in subrecord

Too many rules in SPF record

Example:

- v=spf1 ip4:1.2.3.4/24 a a:my-hosting.tld mx ptr -all

Causes:

- Admins not being sure how SPF works
- Truly messy architecture

There is generally no need to include MX

Including web server in designated senders – huge attack surface

SPF flaws: insufficient granularity

- IP indicated by SPF might contain multiple services
- Even if mail is the only service – multiple domains
- Exploiting any of them (SSRF will do) leads to SPF PASS
- Shared hosting:
  - Attackers can exploit the oldest website
  - Pentesters can simply purchase hosting on the same server

SPF flaws: checking wrong identifier

- **Fatal design flaw!**
- Only Envelope-Sender is protected
- End user typically does not see Envelope-Sender
- From: header (displayed by email client) not protected
- Behavior fixed by DMARC, but majority SPF installations do not have DMARC configured

CERT.LV

Informācijas tehnoloģiju drošības incidentu novēršanas institūcija

Intro to DKIM

DomainKeys Identified Mail (DMARC)

- More granular than SPF (protects individual domains)
- Uses cryptography:
  - Message body & some headers are **signed** using published key
  - Signed != encrypted
- Example:
  - DKIM-Signature: v=1; a=rsa-sha256; c=relaxed/relaxed; d=booking.com; s=bk; t=1577295829; bh=803ssAXjsAtCuH6Ci0pl5lCm7+FBSwSnY3aNmyPl8zw=; h=Content-Type:MIME-Version:Date:From:Sender:Subject:To:Reply-To:Message-Id:From; b=Rf9WnJrdSo8QIsjpZ1pam6Z/7ohUU4tIhzdoQA4cJPBsuHI/752SxtbTqbmOw4stxzJ1Q6twsiX3Kx997YPtaLLrDD5DYkkpjgyUQz1oXfcvegEIr6YN1vkLaxfjNflM4RjJuNHIvOGTDuAEmVEv1Hxuu9gEXXOHnP53aKdYLSg=
  - bk._domainkey.booking.com. 247 IN TXT "v=DKIM1; k=rsa; p=MIGfMA0GCSqGSIb3DQEBAQUAA4GNADCBiQKBgQDmNb2UJoFyoB6HkYMSwDZABbPNbefVDUzSFINodSkpv4kvHckpNM4OA+CpeAm0cFN8pyK65s1FVchYSjPJFrFcaHBIcmMMFrB0HFHP5mHWETagw062LplBE8gfNCfcZ3D3i35KOoetbEdD9lDVLIaF0iYGU7f+J0MK3DD1rAIwewIDAQAB"

DKIM usage

Sender:

1) Generate public / private key
2) Publishes public key in DNS
3) Uses private key to sign messages (at an outgoing server)

Recipient:

4) Queries public key from TXT record
5) Verifies signature

DKIM usage stats

- Unknown
- Custom selectors – impossible to enumerate passively
- DNS servers following RFC closely:
  - Check existance of _domainkeys.alice.tld subtree
  - Not all DNS servers conform to RFC
  - Existance of the subtree != correct usage of DKIM

CERT.LV

Informācijas tehnoloģiju drošības incidentu novēršanas institūcija

Spoofing mails protected by DKIM

Major flaw of DKIM

- Selectors unknown in advance
- Impossible to check whether there should have been signature if it has been stripped
- Modifying existing DKIM – hard/impossible, but removing the header altogether is trivial
- Behavior fixed by DMARC!

Untrusted domain selector

RFC does not require domain selector to match any part of Originator's address

```
DKIM-Signature: v=1; a=rsa-sha256; c=relaxed/relaxed;
   d=[redacted].20150623.gappssmtp.com; s=20150623;
   h=mime-version:from:date:message-id:subject:to;
   bh=qBfFnP07HvG2c6s6WOF3dYU5nody6LVEUAXxFVYUE1k=;
   b=nfEg28b98gZ2lYPALU8yR/gxWBpw6vRho349JSAGggBSw/
     lxZMEqh3G+y0ZA7PKNNdAZj6v7q9TthhW+EHICO2CA+YAc
    BT5OIW7MmcKgN82eqgxq7ad/TdEr3rYS9KLe7Mhy4UCS
    c5hSMPAN2aTL1urwKZaUMX8Ng4mnImmRTdsF/3njm2OKo
    FeDm9PAgzEzhL939D0kJcqx3fwF35KobS7DYLi5Pd+fp+
    5AoBdUjBTNvnYNHlWku1Prbo7uSoa/OcbbTDA80+vqCh
    aoXQr9RtcDrxme2/Yqplzqp2v09MeNW1R16851c7mio
    ZlrjplH29q3rHZXRJpSmrkQnlWoKQ==
```

Best practice:

Envelope-Sender == From: == DKIM domain selector

But attackers are not limited by best practices!

Modifying DKIM

- Modifying headers:
  - Adding new headers
  - Overwriting existing ones by adding additional copy to the top
    - Breaks RFC, but email clients typically will still parse message and display 1st from the top
    - DKIM validates listed headers from bottom
  - Protection mentioned in DKIM RFC – “oversigning”
- Modifying message body:
  - Existing body could be hidden through header modifications
  - Body could be replaced with a new one if DKIM header uses “body length” (“l=”) parameter
    - “body length” is meant for mailing lists that might add some text at the bottom
  - Add new MIME content through modifying Content-Type && append new MIME block to the body

  Source: “Breaking DKIM - on Purpose and by Chance”, by Steffen Ullrich

CERT.LV

Informācijas tehnoloģiju drošības incidentu novēršanas institūcija

Intro to DMARC

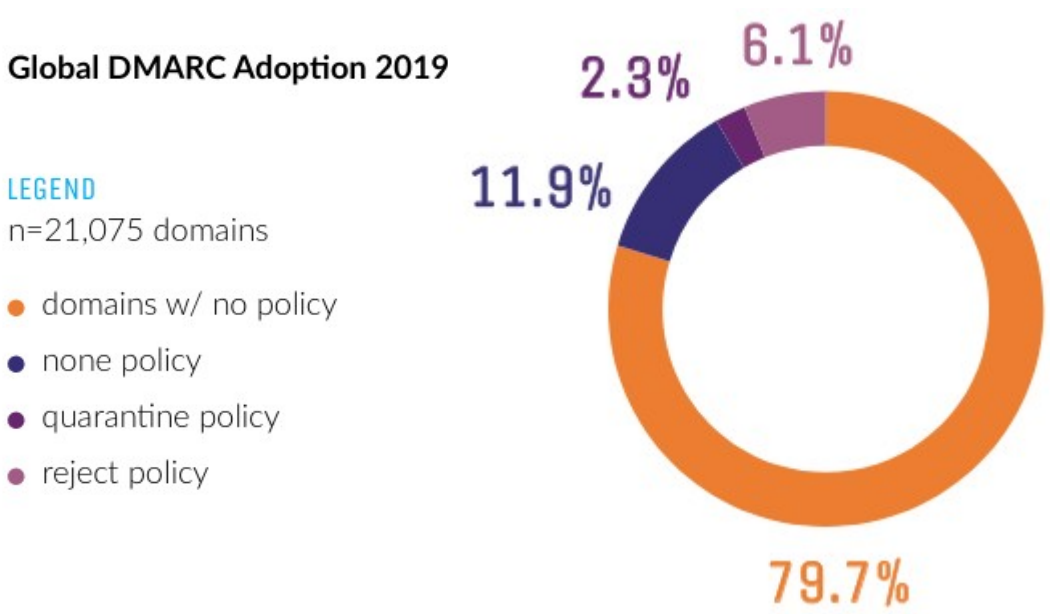
Domain Message Authentication Reporting & Conformance

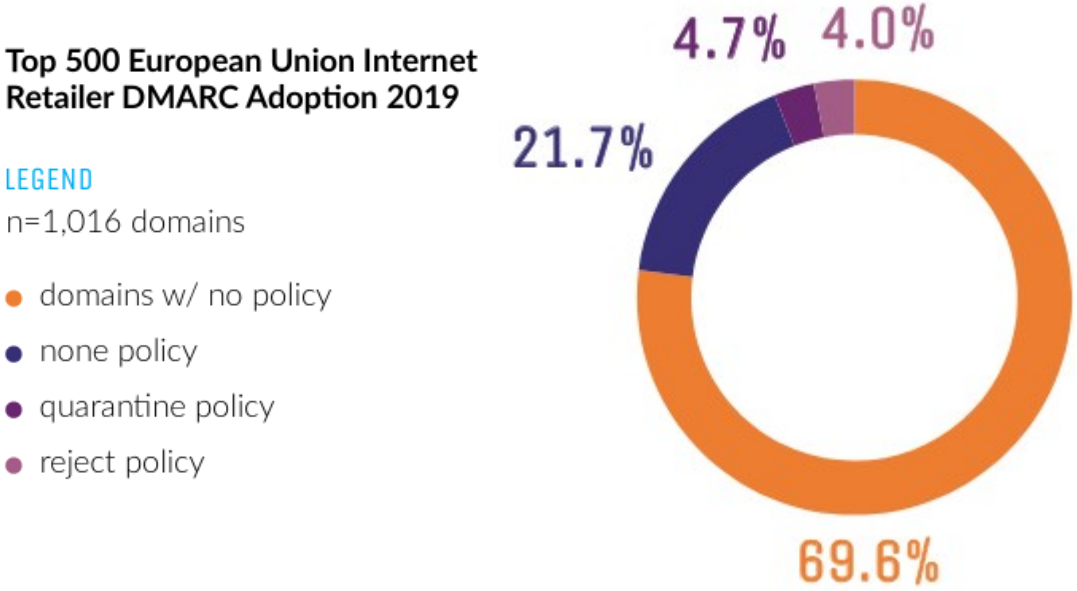
- Reporting:
  - Potentially could be used to understand remote configuration
  - Rarely implemented & enabled in the wild (currently)
- Conformance:
  - Requires either SPF or DKIM to be passed for delivery
  - Makes SPF check From: header

Examples

- Minimal example:
  - "v=DMARC1; p=reject"
- More tags are available that deal with:
  - Reporting
  - Alignment
- Possible policy values:
  - None
  - Quarantine
  - Reject

Usage statistics (should be 100%)





Source: “Global DMARC Adoption 2019” by 250ok

CERT.LV

Informācijas tehnoloģiju drošības incidentu novēršanas institūcija

Spoofing mails protected by DMARC

Critical look at modifications

- DKIM + DMARC (no SPF) – fixes the major DKIM problem
  - Header / Body modifications should still be addressed
  - In many cases leaving SPF out is not practical
- SPF + DMARC – fixes alignment, but does not protect from:
  - Misconfiguration (SOFTFAIL, too much granularity)
  - Not enough granularity
- SPF + DKIM + DMARC – as strong/weak as SPF + DMARC

CERT.LV

Informācijas tehnoloģiju drošības incidentu novēršanas institūcija

Recap SPF, DKIM, DMARC

Recap

	Significance	Ease of implementation Sender side	Ease of implementation Recipient side
SPF	Limit outgoing email to designated IPs	Easy (DNS only)	Moderate (software support)
DKIM	Sign each mail with per-domain key(s)	Hard (software support, key management)	Moderate (software support)
DMARC	Fixes major flaws in SPF & DKIM	Easy (DNS only)	Moderate (software support)

No support in MS Exchange

DKIM + DMARC (no SPF) – provides the best protection, but only if recipient supports both of them

Notes on testing

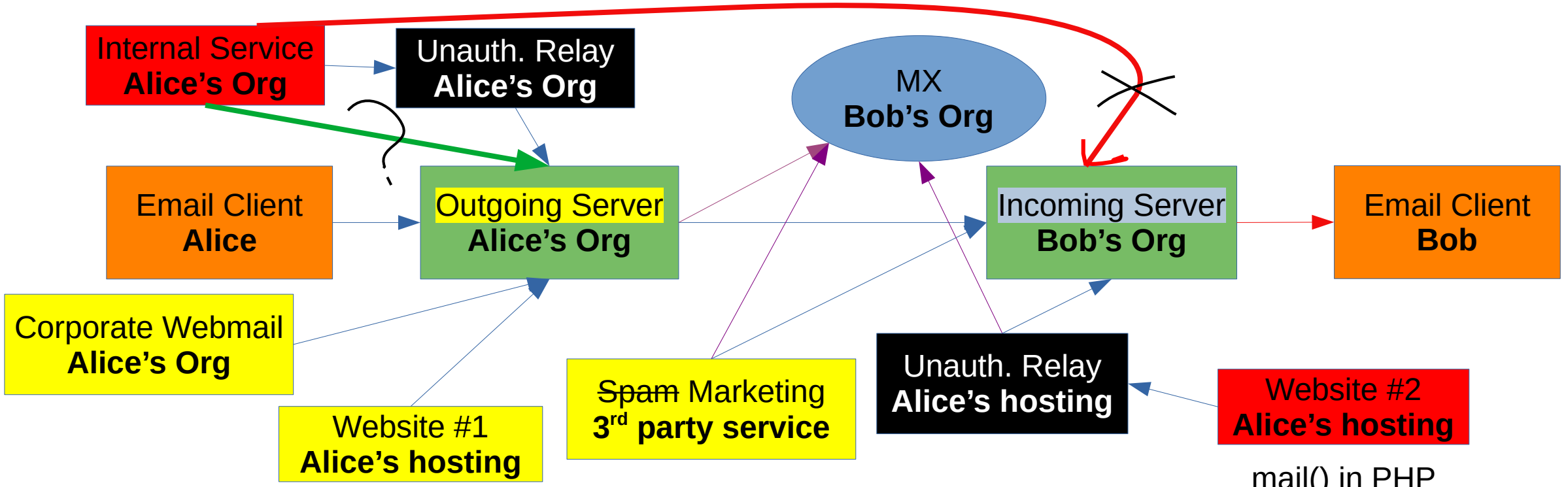
- All three scenarios should be tested:
  - Forging spoofed emails supposedly coming from Alice
  - Sending spoofed emails to Alice that impersonate Bob
    - Assume that Bob's org has the best possible SPF, DKIM and DMARC
  - Sending spoofed emails to Alice from her coworkers
- Possible additional hardening for incoming mails:
  - Centrally maintained addressbooks
  - Whitelists enforced on the server

CERT.LV

Informācijas tehnoloģiju drošības incidentu novēršanas institūcija

Unauthenticated relays

Realistic email architecture



- Unless open relay, exploiting requires chaining
- But maybe not

Identifying relays

- From SPF records
- From headers
- Typical sources:
  - Web forms (might be multiple)
  - Mass mails, ads, marketing
  - Outgoing servers
  - ISP

Exploiting relays

- Easy mode:
  - Open relays
  - ISP
  - Shared hosting
- Requires chaining:
  - Web
  - IP based ACL (e.g. accept any mail from LAN)

CERT.LV

Informācijas tehnoloģiju drošības incidentu novēršanas institūcija

Conclusion

Takeaways

- DMARC
  - should always be present
  - if absent – spoofing almost certainly possible
- DKIM – long-term best option
  - SPF + DKIM + DMARC – your best bet is bypassing SPF
  - DKIM + DMARC – look for header vulns or unauth relays
- SPF – most popular currently
  - Weakest link in SPF + DKIM + DMARC scenario
  - Best bet – insufficient granularity
- Check incoming configuration as well

Thank you!

https://www.cert.lv/

andrejs@cert.lv

679A C8D4 A391 6736 D558
07C1 D3D9 0B7C 666A EDCD