CISPA
HELMHOLTZ CENTER FOR INFORMATION SECURITY

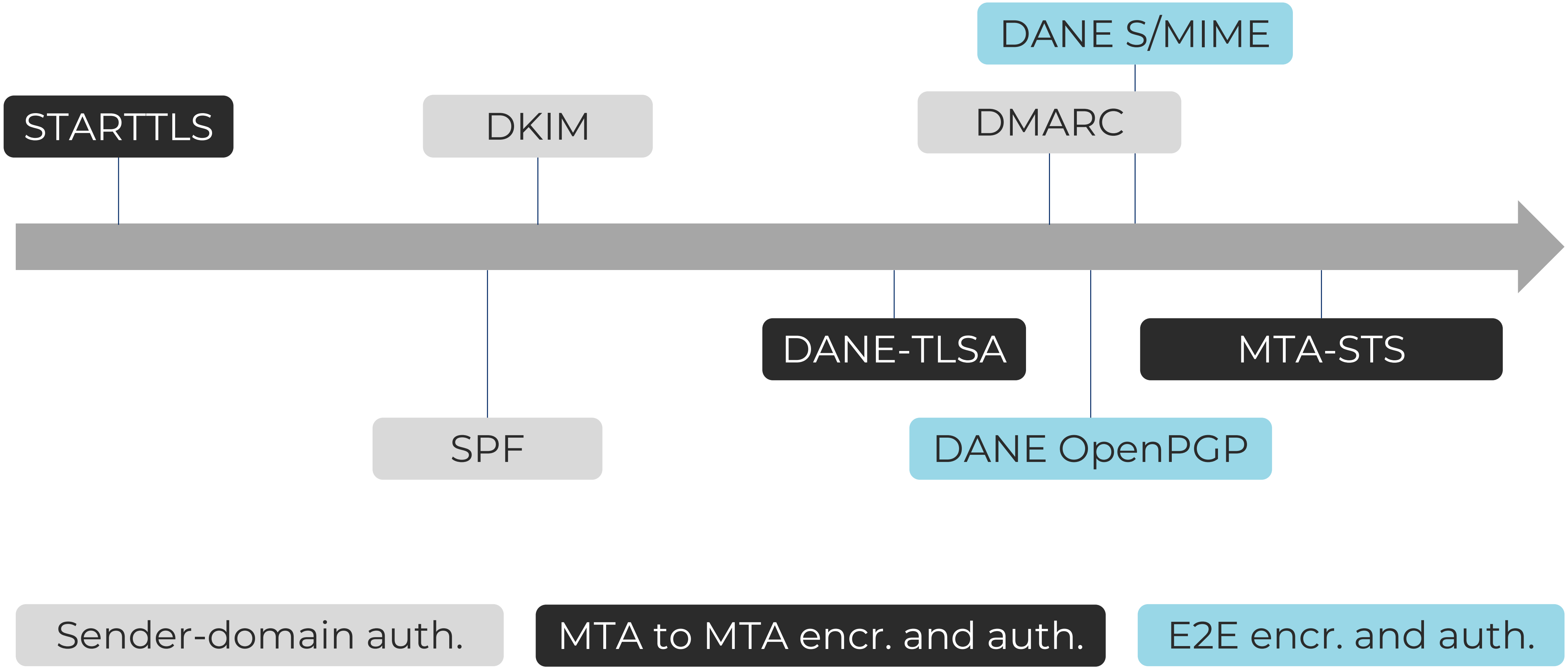
Extended Hell(o): A Comprehensive Large-Scale Study on Email Confidentiality and Integrity Mechanisms in the Wild

Birk Blechschmidt[+] and Ben Stock[*]

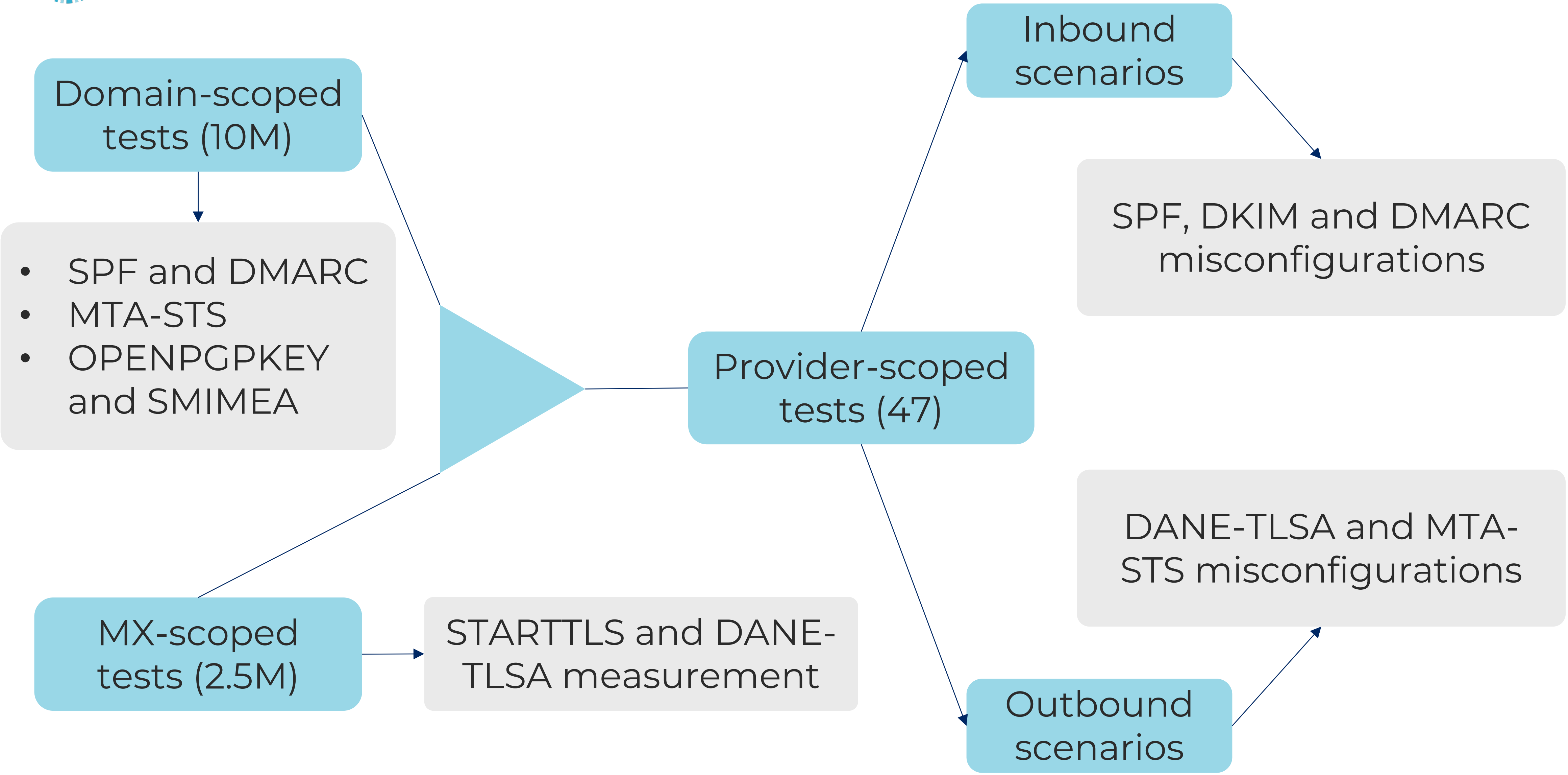
[+]*Saarland University* [*]*CISPA Helmholtz Center for Information Security*

32nd USENIX Security Symposium

Background: Email Security Mechanism Evolution



Measurement Methodology

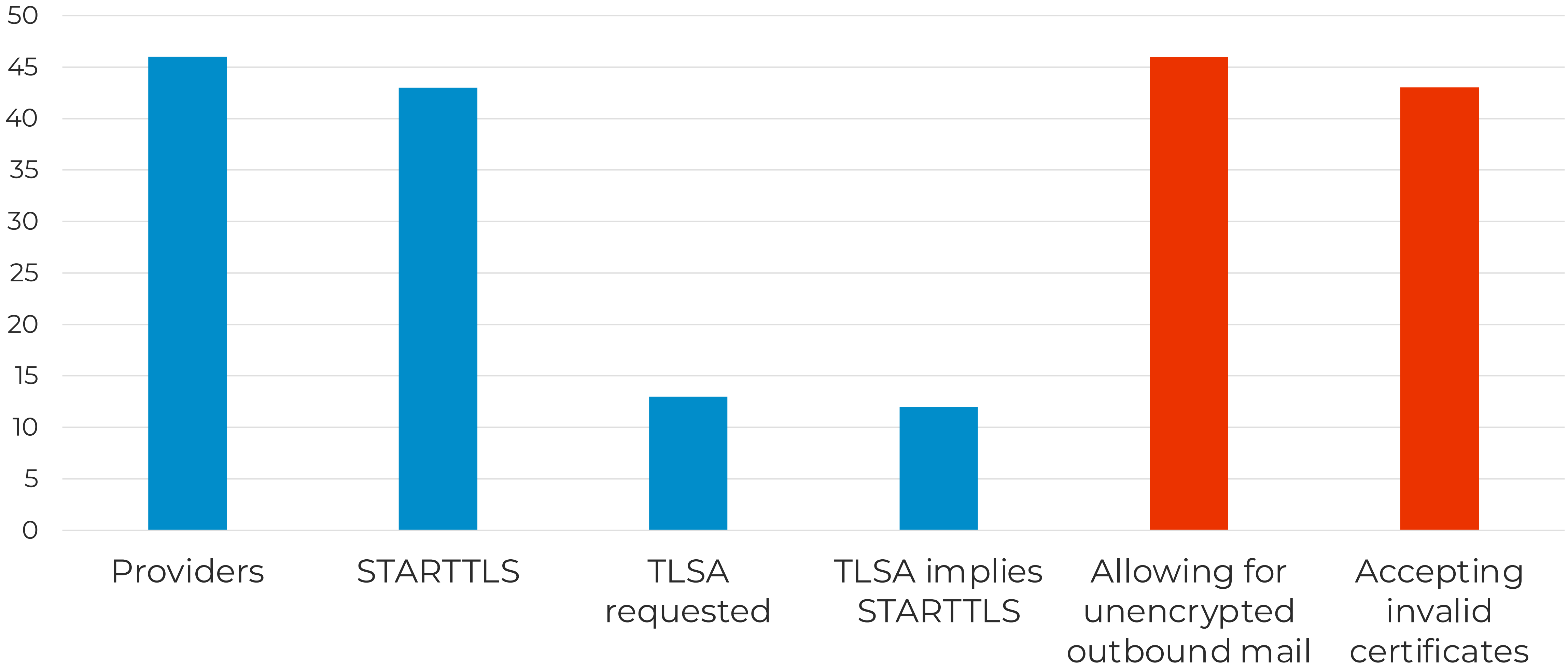


Provider-Scoped Results: SPF, DKIM and DMARC

Scenario	gmail.com	sapo.pt	zoho.com	tutanota.com	vodafone.de
No SPF, DMARC Reject, no DKIM	🟢	🔴	🟢	🟢	🔴
SPF fail, DMARC Reject, DKIM key unpublished	🟢	🟢	🟢	🟢	🔴
SPF fail, DMARC Quarantine, DKIM key unpublished	🟢	🟢	🟢	🟢	🔴
DMARC Parent Reject	🟢	🔴	🟢	🔴	🔴
Double From 1	🟢	🔴	🟢	🟢	🔴
Double From 2	🟢	🔴	🔴	🟢	🔴

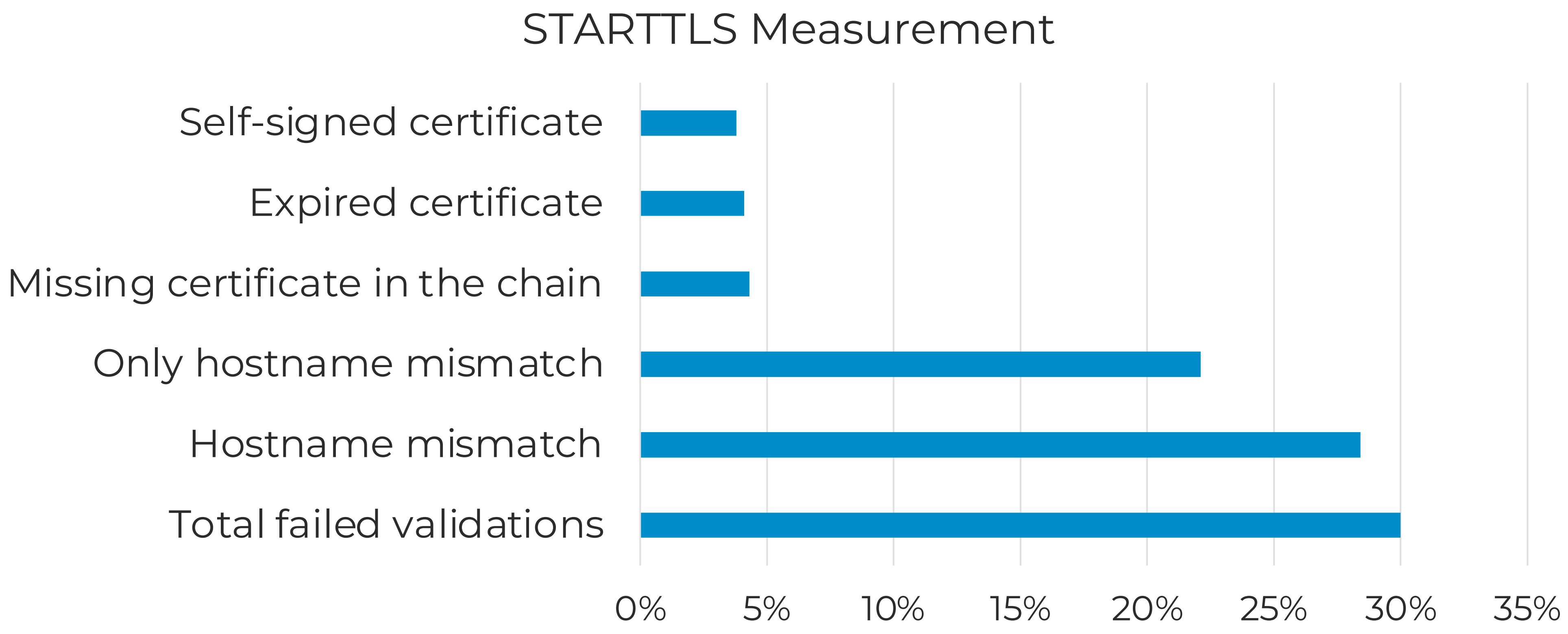
- Few providers provide satisfying security
- As a sender, implementing a single mechanism is not sufficient
- We can produce UI mismatches through double *From* headers in three providers supporting DMARC
- DMARC's parent reject policy is sometimes not implemented correctly
- Some providers with no filtering or proprietary mechanisms (e.g. IP address reputation)

Provider-Scoped Results: TLS & DANE-TLSA



MX-Scoped Results: TLS certificates

- 30% of certificates fail validation



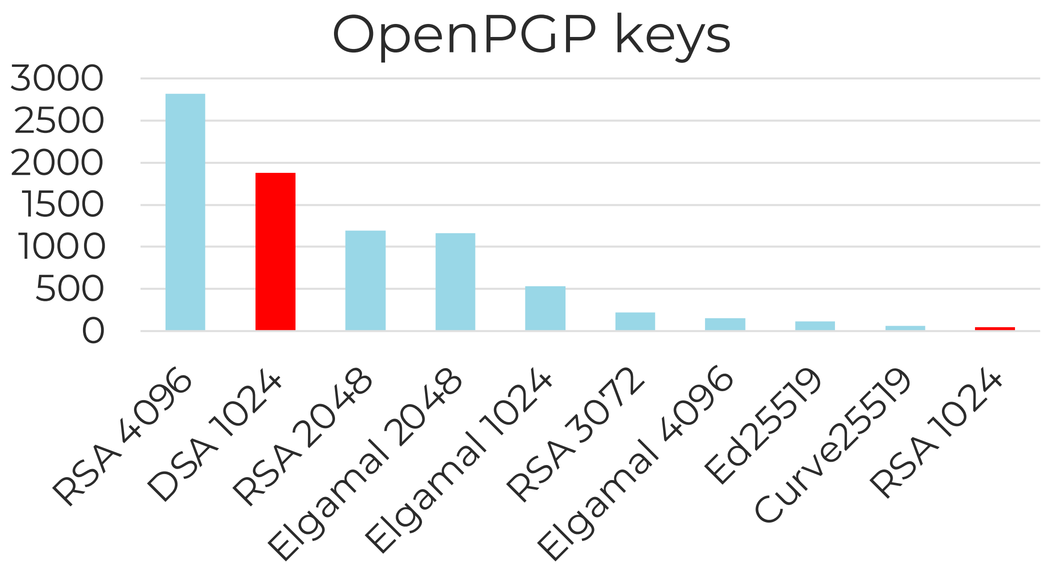
How to transmit emails securely between MTAs

- Each MX should have a TLSA record (**9,480** records of 2.5M MX records)
- TLSA must be DNSSEC-signed (**8,398** servers remaining)
  - **8,176** servers responsible for **117,126** domains have a matching TLSA record
- But: domains' MX records must also be protected by DNSSEC
  - only **71,176** domains which really benefit

Domain-Scoped Results: OPENPGPKEY and SMIMEA

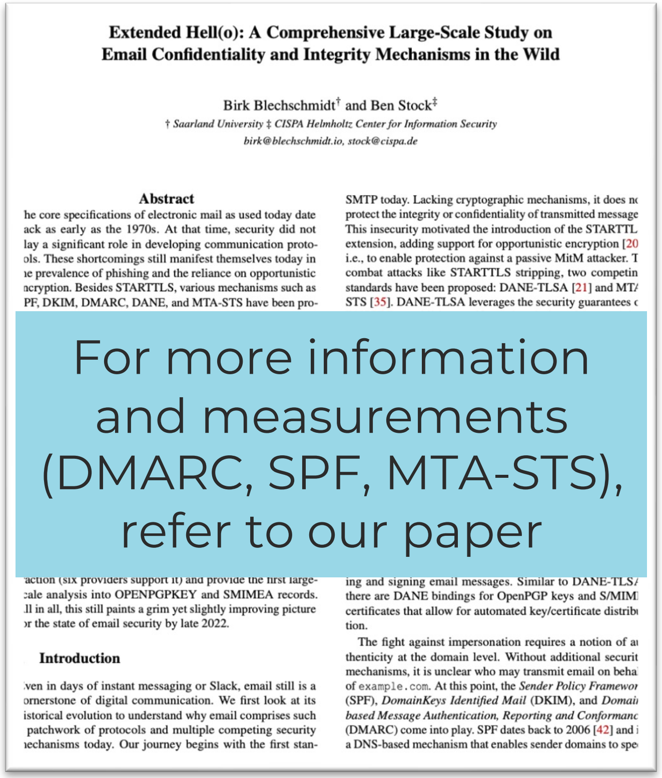
- DNS Empty Non-Terminals allow us to find potentially supporting domains
  - If *anything*`._openpgpkey.example.org` exists, `_openpgpkey.example.org` does not return *NXDOMAIN*
- NSEC zones allow for trivial key strength measurement
  - We use a custom hashcat module for cracking zones with NSEC3

- Mostly used by specialized entities well-known in the tech community
  - 100 OPENPGPKEY and 26 SMIMEA supporting zones



Conclusion

- We all use email every day, yet it suffers from severe deficiencies
- Providers lack behind in implementation of security checks (e.g., only 7/46 support TLSA, all allow unencrypted outgoing connections)
- Ecosystem shows TLS certificates are not well-managed
- Complexity of DNSSEC and plethora of protocols as major hindrances to security
- Automated end-to-end encryption is futile and badly implemented


Extended Hell(o): A Comprehensive Large-Scale Study on Email Confidentiality and Integrity Mechanisms in the Wild

Birk Blechschmidt† and Ben Stock‡

† Saarland University ‡ CISPA Helmholtz Center for Information Security

birk@blechschmidt.io, stock@cispa.de

Abstract

he core specifications of electronic mail as used today date ack as early as the 1970s. At that time, security did not lay a significant role in developing communication proto- ols. These shortcomings still manifest themselves today in ie prevalence of phishing and the reliance on opportunistic ncryption. Besides STARTTLS, various mechanisms such as PF, DKIM, DMARC, DANE, and MTA-STS have been pro-

action (six providers support it) and provide the first large- cale analysis into OPENPGPKEY and SMIMEA records. ll in all, this still paints a grim yet slightly improving picture r the state of email security by late 2022.

Introduction

ven in days of instant messaging or Slack, email still is a ornerstone of digital communication. We first look at its istorical evolution to understand why email comprises such patchwork of protocols and multiple competing security iechanisms today. Our journey begins with the first stan-

SMTP today. Lacking cryptographic mechanisms, it does n protect the integrity or confidentiality of transmitted message This insecurity motivated the introduction of the STARTTL extension, adding support for opportunistic encryption [20 i.e., to enable protection against a passive MitM attacker. T combat attacks like STARTTLS stripping, two competin standards have been proposed: DANE-TLSA [21] and MT/ STS [35]. DANE-TLSA leverages the security guarantees

ing and signing email messages. Similar to DANE-TLS/ there are DANE bindings for OpenPGP keys and S/MIM certificates that allow for automated key/certificate distrib tion.

The fight against impersonation requires a notion of a thenticity at the domain level. Without additional securit mechanisms, it is unclear who may transmit email on beha of example.com. At this point, the *Sender Policy Framewo* (SPF), *DomainKeys Identified Mail* (DKIM), and *Domai based Message Authentication, Reporting and Conformanc* (DMARC) come into play. SPF dates back to 2006 [42] and i a DNS-based mechanism that enables sender domains to spe

For more information and measurements (DMARC, SPF, MTA-STS), refer to our paper