

# HALON™



Can I haz  
secure email?  
DANE, MTA-STS and much more.

Anders Berggren  
CTO

# What we do

Scriptable email gateway with many security features



# Email

- “Email remains the go-to form of communication in the Business world”<sup>1</sup>
- Why so prevalent?
- Quite insecure today, but worth fixing?

[1] <http://www.radicati.com/wp/wp-content/uploads/2013/04/Email-Statistics-Report-2013-2017-Executive-Summary.pdf>

# Email and TLS

- Misconception that TLS works with email, as it does on the web (HTTPS)
- Especially since Gmail's TLS lock
- **It doesn't**

# Email and TLS

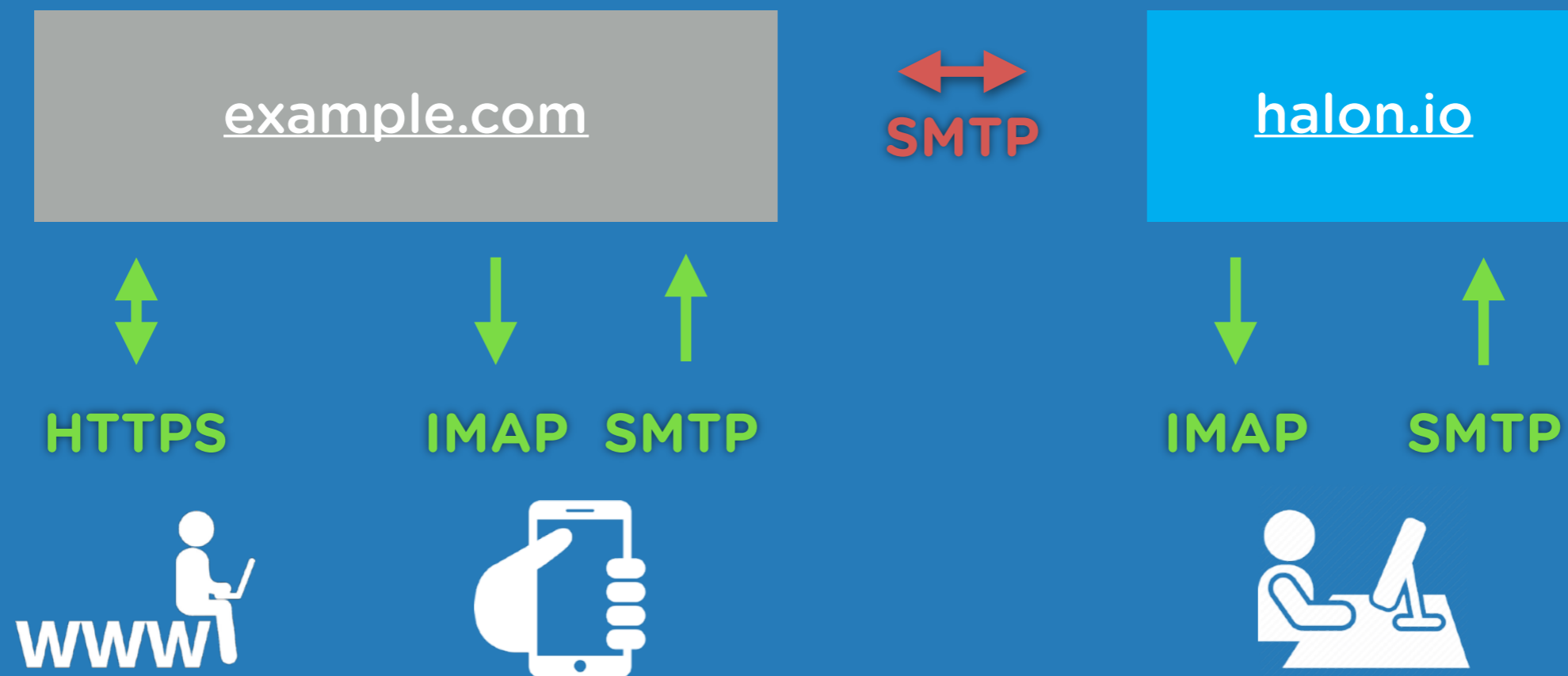


# TLS

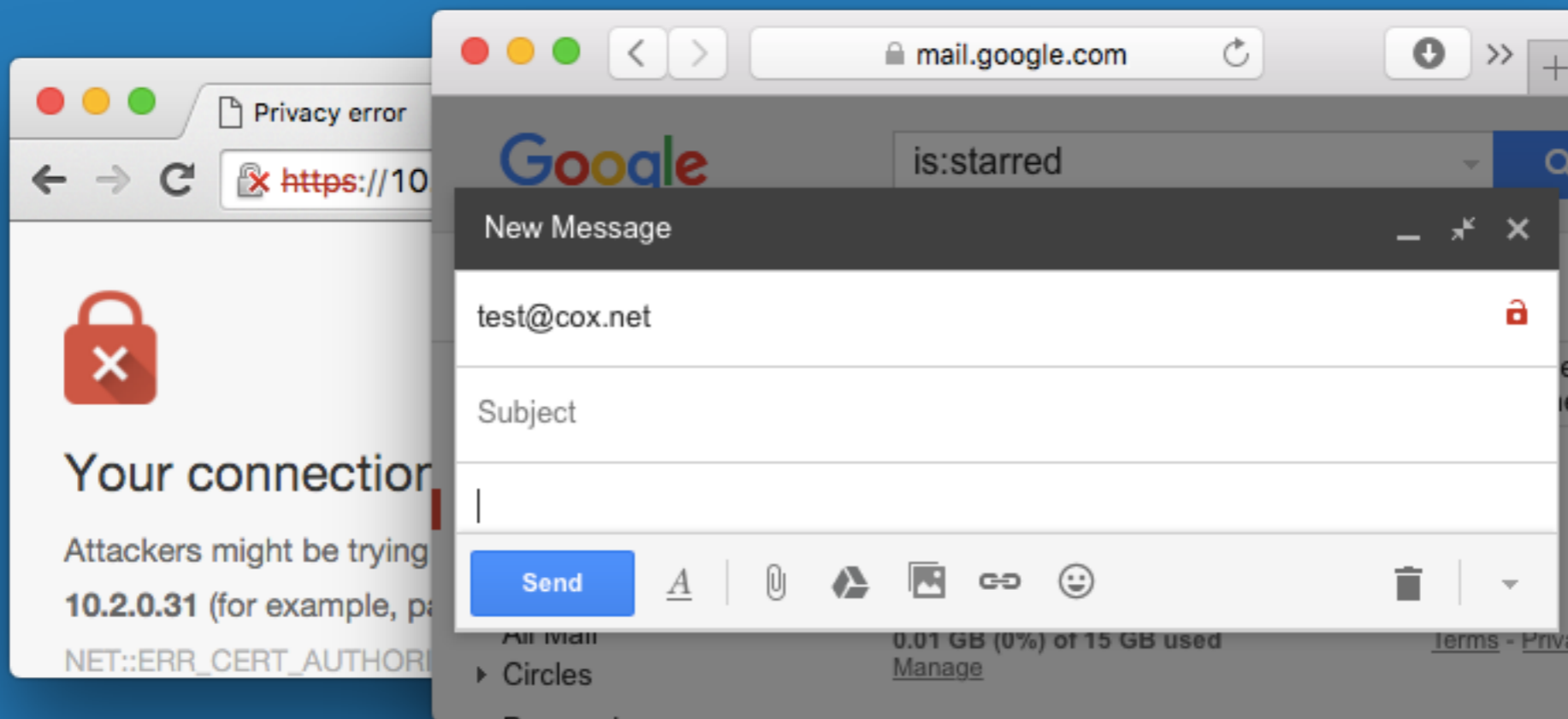
- We've had SSL/TLS for a long time
- HTTPS enabled internet banking, etc
- Email clients (IMAP, SMTP submission) have had it for a long time
- Quite annoying, if not ridiculous, that we don't have it for exchanging email

# Email and TLS

- Required, authenticated TLS
- Opportunistic, unauthenticated TLS

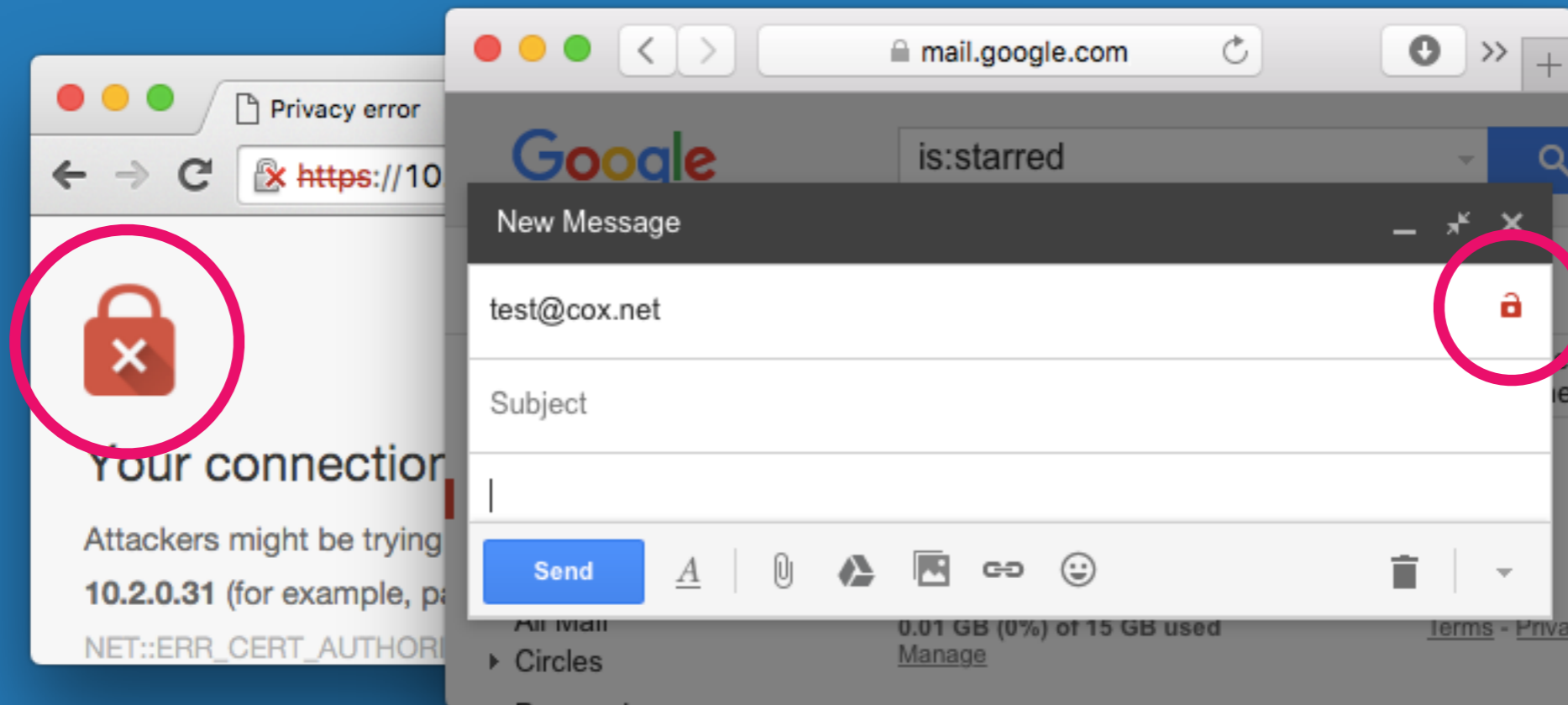


Could be confusing?





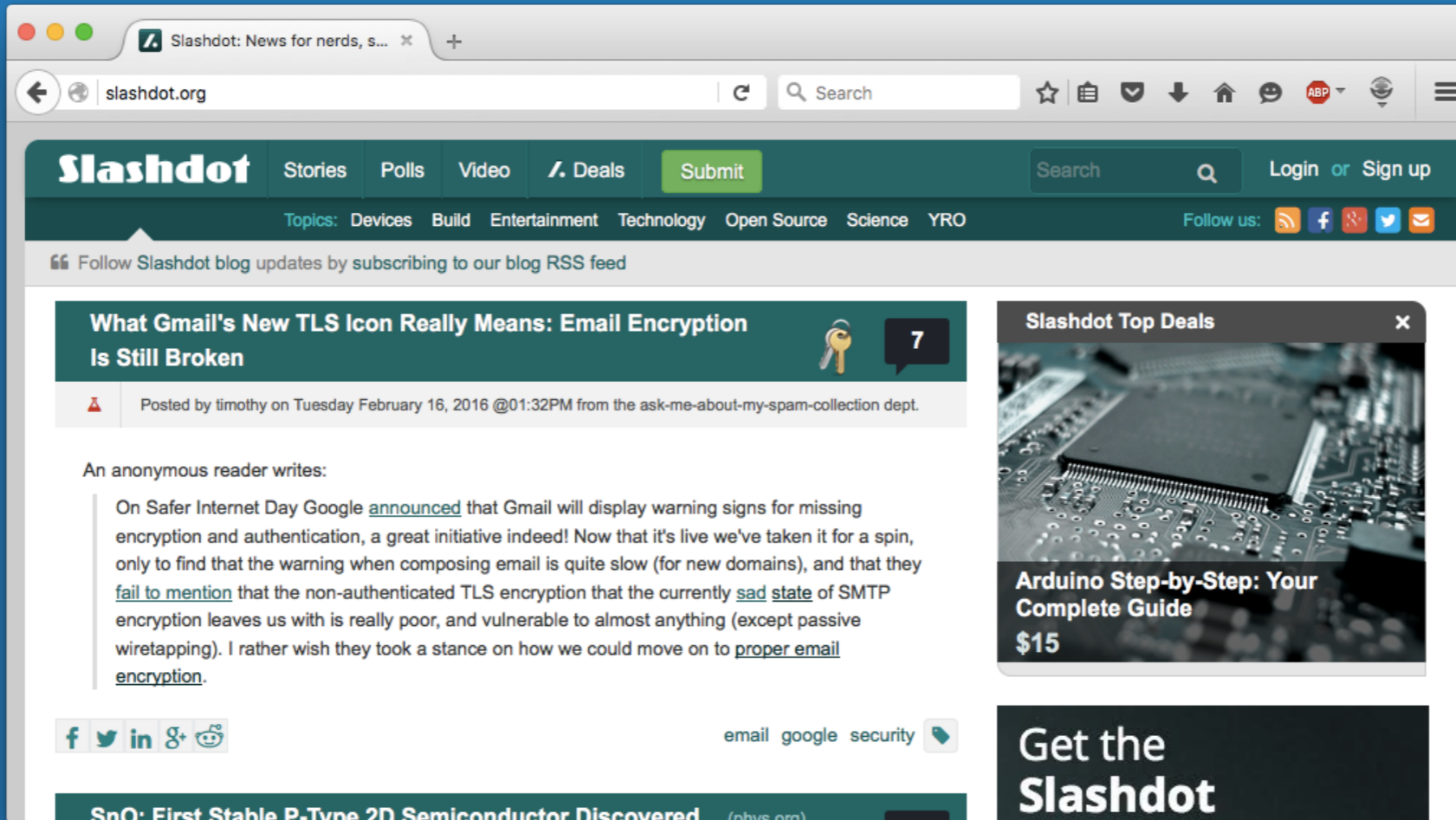
Could be confusing?



TLS validation failed

Opportunistic TLS unavailable

# Getting slashdotted



The screenshot shows the Slashdot website interface. At the top, there's a navigation bar with the Slashdot logo, links for Stories, Polls, Video, Deals, and a Submit button. A search bar and Login/Sign up options are also present. Below the navigation bar, there's a secondary bar with various topic categories like Devices, Build, Entertainment, Technology, Open Source, Science, and YRO. A RSS feed link is also visible.

The main content area features a featured article titled "What Gmail's New TLS Icon Really Means: Email Encryption Is Still Broken" by timothy, posted on Tuesday February 16, 2016. The article text discusses the implications of Gmail's new TLS icon and the state of email encryption. Below the article are social media sharing icons for Facebook, Twitter, LinkedIn, Google+, and Reddit, along with a "email google security" tag.

On the right side, there's a "Slashdot Top Deals" section featuring an advertisement for "Arduino Step-by-Step: Your Complete Guide" priced at \$15. Below this is a "Get the Slashdot" banner.

# TLS and SMTP

- What's so difficult?
- How should we verify the certificate?
  - What name verify? Do “SNI” with STARTTLS?

```
$ dig +short halon.io mx
10 mx.se1.halonsecurity.eu.
10 mx.se1.halonemail.org.
```
- Should we require TLS?
  - Should sender (MUA) choose, like `https://1`, “REQUIRETLS” extension?

[1] <https://www.w3.org/DesignIssues/Security-NotTheS.html>

# TLS and SMTP

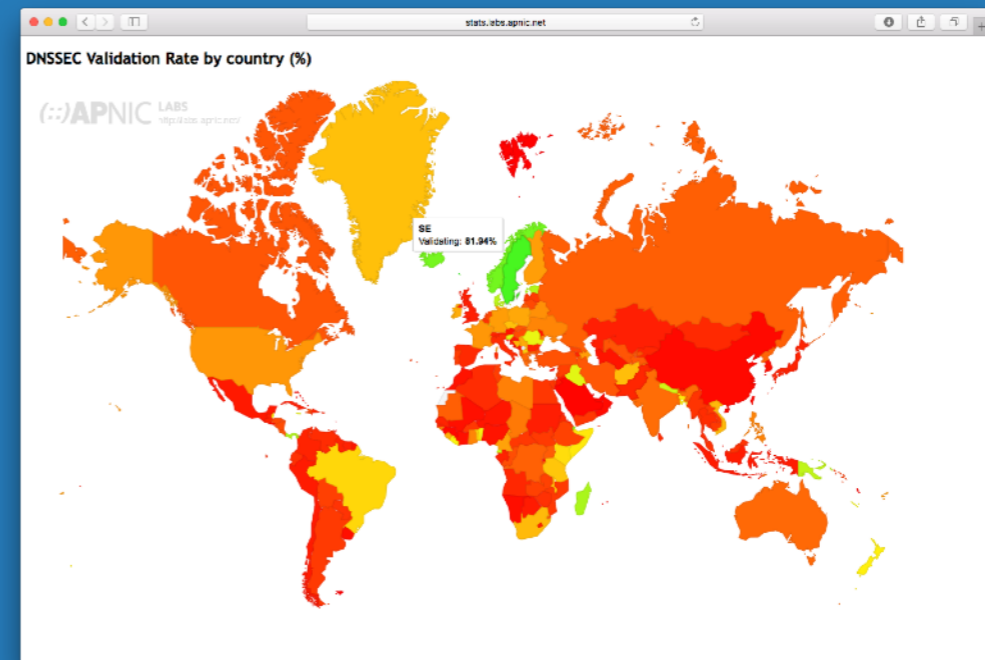
- Trying to mimic https:// = SMTP protocol changes
- **DNSSEC solves all of this, and much more, for email.**

# TLS and SMTP



# DNSSEC

- Root signed in 2010, >90% of TLDs are signed<sup>1</sup>, and ~1% of domains signed<sup>2</sup> (more in .se and 45%<sup>3</sup> in .nl)
- Many resolvers, including Google's 8.8.8.8 and Comcast does validation



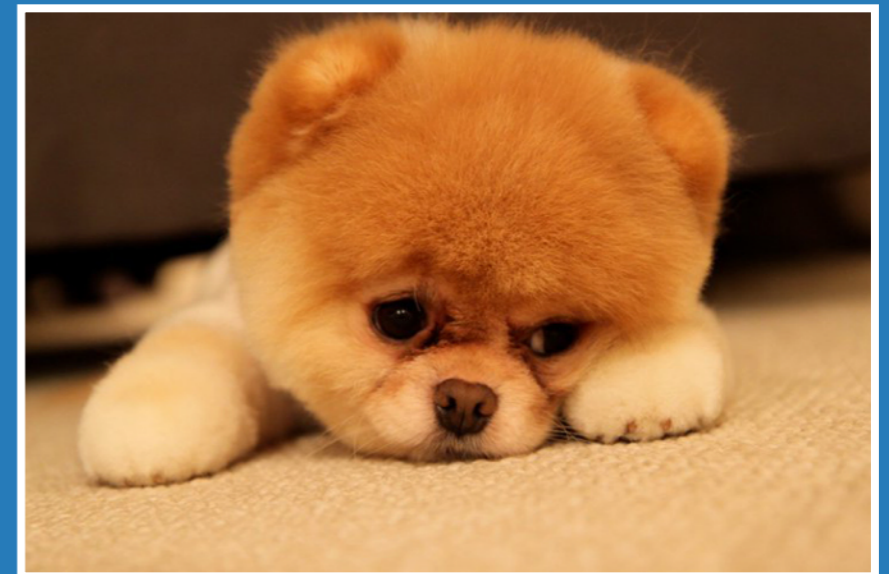
[1] [http://stats.research.icann.org/dns/tld\\_report/](http://stats.research.icann.org/dns/tld_report/)

[2] <https://speakerdeck.com/shuque/next-steps-in-dane-adoption>

[3] <http://stats.sidnlabs.nl/#/dnssec>

# The struggle

- Many big providers doesn't back DNSSEC
- Some are saying that DNSSEC is bad and unnecessary<sup>1,2</sup> 😞
- Maybe it is, for the web, with Certificate Transparency and all



[1] <https://sockpuppet.org/blog/2015/01/15/against-dnssec/>

[2] <https://news.ycombinator.com/item?id=9178783>

# DNSSEC and email

Email  
is the★

**KILLER APP**★  
for  
DNSSEC

- It provides security for:
  - Authenticity (SPF, DKIM and DMARC)
  - Privacy (TLS/DANE)



# DANE

- DANE-SMTP finally (and elegantly) solves email transport encryption with DNSSEC
- **How should we verify the certificate?**
  - Specified by DNSSEC record
- **Should we require TLS?**
  - Specified by DNSSEC record

# DANE

- **DNSSEC does the heavy lifting**
  - No changes to SMTP protocol
  - Straightforward implementation
  - No out-of-band communication (only DNS)

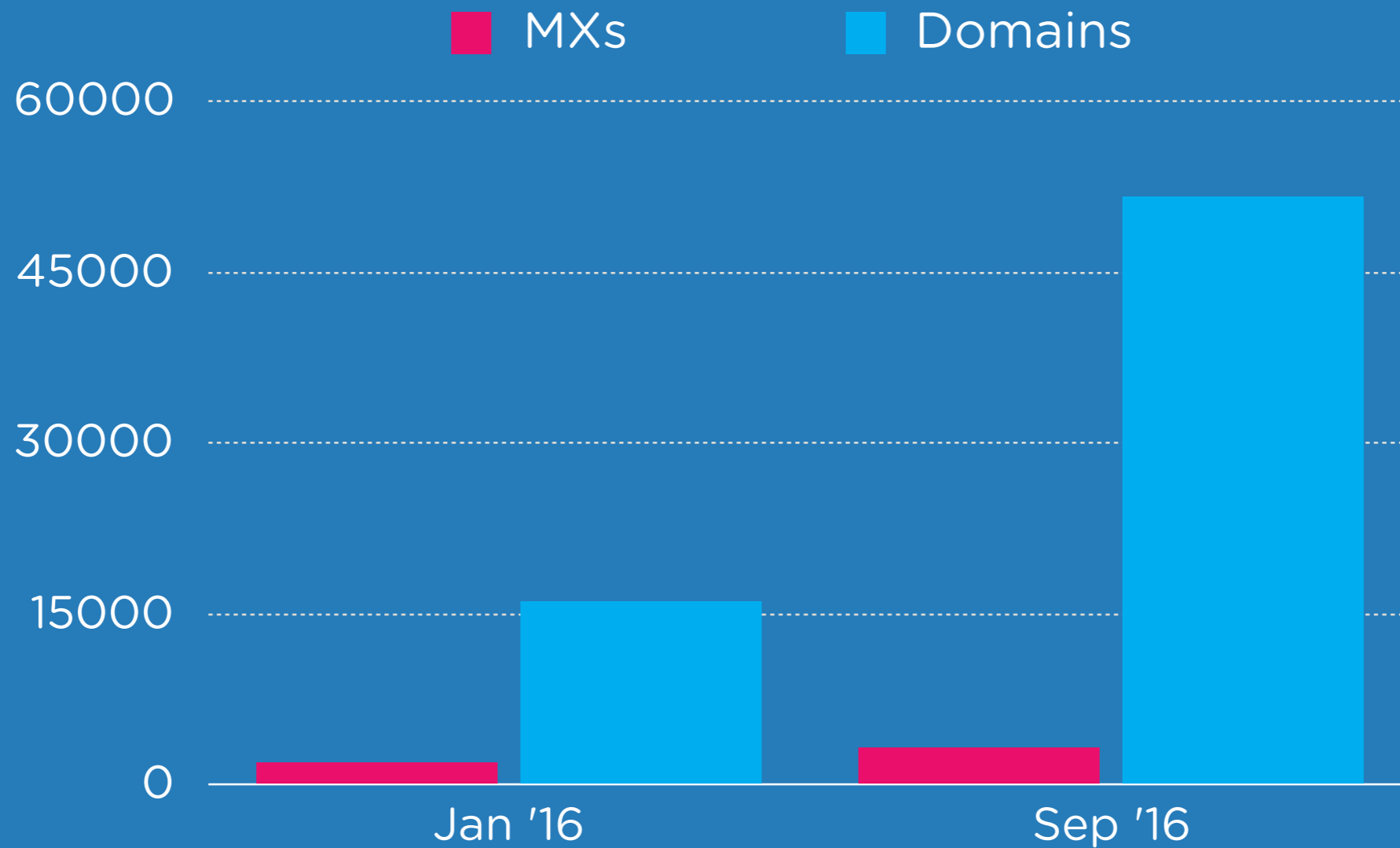
# Implementation

- DANE RFC published 2012
- Postfix support since 2014
- Halon support since 2015
- OpenSSL since 2016

# Deployment

- e-mail-made-in-germany.de (trusted email consortium) members GMX, web.de and 1&1 are live
- All major DNS providers give acceptable TLSA responses (since a few weeks), safe to enable DANE
- The majority of our large hosting provider customers verifies DANE
- ~1% of email traffic from One.com's email servers are protected with DANE

# Deployment



Two nice data points<sup>1</sup> 🤖

[1] <http://secspider.verisignlabs.com/stats.html>

# Future

- DNSSEC providers should allow TLSA records
- Many nordic service providers does DNSSEC for all their customers' domains, by default
- Publish a few TLSA records for your MX, and all customer's domain (with DNSSEC) get it

```
_25._tcp.mx1.provider.com. IN TLSA 3 1 1 ca7e...  
_25._tcp.mx2.provider.com. IN TLSA 3 1 1 ca7e...
```

- Once our customers publish DANE, the chart on the previous page get make a huge bump....

# Future work

- User interface; webmail, etc<sup>1</sup>
- Open-Xchange's TES
- E2E

[1] <https://www.ietf.org/registration/MeetingWiki/wiki/93hackathon>

# Alternatives?

What about those that can't have<sup>1</sup>  
DNSSEC?

[1] Don't like?



# MTA-STS

- Google, and others
- They designed their own protocol, of course 🤖
- Provides “DANE light” while we wait for DNSSEC
- Trust-on-first-use DNS TXT record
- Uses HTTPS for validation (out-of-band)
- Per-domain, not per MX
- Consensus that it’s ok, unless interfering with DANE

# End-to-end

- Of course more “secure” than TLS, but transport security takes us very far
- PGP and S/MIME
- User friendliness achievable with public key stores (DANE?) and client (MUA) support
- Spam filters currently doesn't work with E2E (need to see the body)<sup>1</sup>

[1] <https://moderncrypto.org/mail-archive/messaging/2014/000780.html>

# Summary

- Since email is so prevalent, let's fix it
- DNSSEC makes email much more secure
- The large service providers can make DANE for SMTP happen
- I expect a mix of DANE and MTA-STS; sending servers can support and verify both<sup>1</sup>

[1] <https://www.ietf.org/mail-archive/web/uta/current/msg01513.html>

# HALON™



Anders Berggren  
CTO

 [@halonsecurity](https://twitter.com/halonsecurity)  
 [anders@halon.io](mailto:anders@halon.io)  
 [halon.io](https://halon.io)