DNSSEC, DANE and SMTP Security

A Mid-level Overview

Wes Hardaker
Parsons

*Downgrade Resistant, Opportunistic Security for Server To Server E-Mail Delivery*
Overview

- Server-to-Server E-Mail background
- SMTP Vulnerabilities
- DANE/SMTP to the rescue
- Implementation and Deployment Status
Server-to-Server Email

1: Alice's Mail User Agent (MUA) sends the email via the configured SMTP server

2: Alice's ISP forwards the message to Bob's ISP

Simple Mail Transport Protocol (SMTP)

Mail Transfer Agent

Mail Transfer Agent

3: Bob's MUA downloads the message via IMAP
Server-to-Server Email

1: Alice's Mail User Agent (MUA) sends the email via the configured SMTP server

2: Alice's ISP forwards the message to Bob's ISP

We're talking about this part today

3: Bob's MUA downloads the message via IMAP

Largely secured today through Manual configuration parameters

wes.hardaker@parsons.com
Server-to-Server Email with DNS

1: Where should I send mail for @bobsISP.com?
2: You should send it to mail.bobsISP.com
   (and the address for it is ....)

3: I've got mail for Bob

Mail Transfer Agent

DNS Server

Mail Transfer Agent
I Wish It Were So Simple

- There can be multiple DNS servers
  - Every domain should have at least two
- Alice's mail server asks her ISP's resolver
  - It doesn't talk directly to the distant DNS server
  - There may be multiple resolvers
- There can be multiple mail servers
Server-to-Server Email
Reality Sets In

1: Where should I send mail for @bobsISP.com?

2: You should send it to mail1, mail2 or mail3

3: Do you have an address for mail1?

4: Yep, it's 192.0.2.3

5: Hi, I'm representing Alice, I have mail for Bob

6: Hi, I'll take mail for Bob; **PS: I don't do security**

7: Here's the mail for Bob from Alice

8: Thanks, I'll make sure he gets it

*(Actually, reality is *even worse* but wouldn't fit on this slide)*
Back To: I Wish It Were So Simple

- There can be multiple DNS servers
  - Every domain should have at least two
- Alice's mail server asks her ISP's resolver
  - It doesn't talk directly to the distant DNS server
  - There may be multiple resolvers
- There can be multiple mail servers
What could possibly go wrong???

- There can be multiple DNS servers
  - Compromised?
- Alice's mail server asks her ISP's resolver
  - It doesn't talk directly to the distant DNS server
  - Compromised?
- There can be multiple mail servers
  - Compromised?
- Man In The Middle

Network Attack

DNS Attack Point!!!
DANE/DNSSEC To The Rescue

- There can be multiple DNS servers
  - Compromised?
- Alice's mail server asks her ISP's resolver
  - It doesn't talk directly to the distant DNS server
  - Compromised?
- There can be multiple mail servers
  - Compromised?
- Man In The Middle

Use DNSSEC

Use DANE
SMTP Vulnerabilities

• MX, A and other DNS records can be spoofed
  – DNS redirects SMTP clients to the...
  – DNSSEC detects this, and clients won't proceed

• Eavesdropping is Easy
  – SMTP is unencrypted by default
  – Opportunistic encryption helps
    • See if they offer a certificate and start encryption
    • However, you may just be encrypting to the...
SMTP Vulnerabilities

- If DNS is spoofed, you get a...
- ...Man In The Middle
  - SMTP is unauthenticated by default
  - SMTP is unencrypted by default
  - They can turn on opportunistic encryption
    - Server indicates “I do security”
    - But a man-in-the-middle can just say “I don't do security”
  - CA based solutions don't help because:
    - The man-in-the-middle says “I don't do security”
    - You've been redirected to a name the attacker controls
DNSSEC/DANE For The Win

• DNSSEC and DANE solves all these problems!
• With DNSSEC: you can believe:
  – The MX that led you here
  – The TLSA is accurately pointing to my certificate
• With DANE's TLSA record:
  – “This is my certificate” or “This is my CA”
    • (accept no others)
  – You MUST expect security!!! (i.e., must do TLS)
  – You connected to the right place
Deployment Options

• Postfix 2.11
  – Server side (receiving mail):
    • Publish a TLSA record: _25._tcp.smtp.example.com
    • smtpd_tls_cert_file = /path/to/mycert.crt
    • smtpd_tls_key_file = /paht/to/mycert.key
  – Client side (sending mail):
    • smtp_tls_security_level = dane
    • smtp_dns_support_level = dnssec
    • CAVEAT: MUST use a secure local resolver
• Exim: Implementation underway (~ 2015)
Known Large Early Adopters

- posteo.de
- mailbox.org
- bund.de
- denic.de
- umkbw.de
- freebsd.org
- unitybox.de
- debian.org
- ietf.org
- nlnet.nl
- nic.cz
Questions?

(See me anytime this week if you want a greater level of detail about how it all works)

wes.hardaker@parsons.com