DNSSEC Enables Secure Mail

Jaap Akkerhuis
(proxying)

NLnet Labs

Secure Mail Project

- The Players
  - Fraunhofer IAO
  - ISC
  - Microsoft
  - NCCCE
  - NIST
  - NLnet Labs
  - Secure64

The (Open Standard) Parts

- SMIME
- TLS
- DNSSEC
- CERTS
  - Self signed
  - Well Known Certs
  - Private Certs

} Dane

NLnet Labs

The MUA Parts

- Microsoft Office
- Thunderbird
- Also with Apple Key Chain Utility

The MTA Parts

- Postfix
- Dovecot
- Exchange

The DNS Parts (1)

- ISC
  - BIND
- Microsoft
  - Active Directory and DNS Server

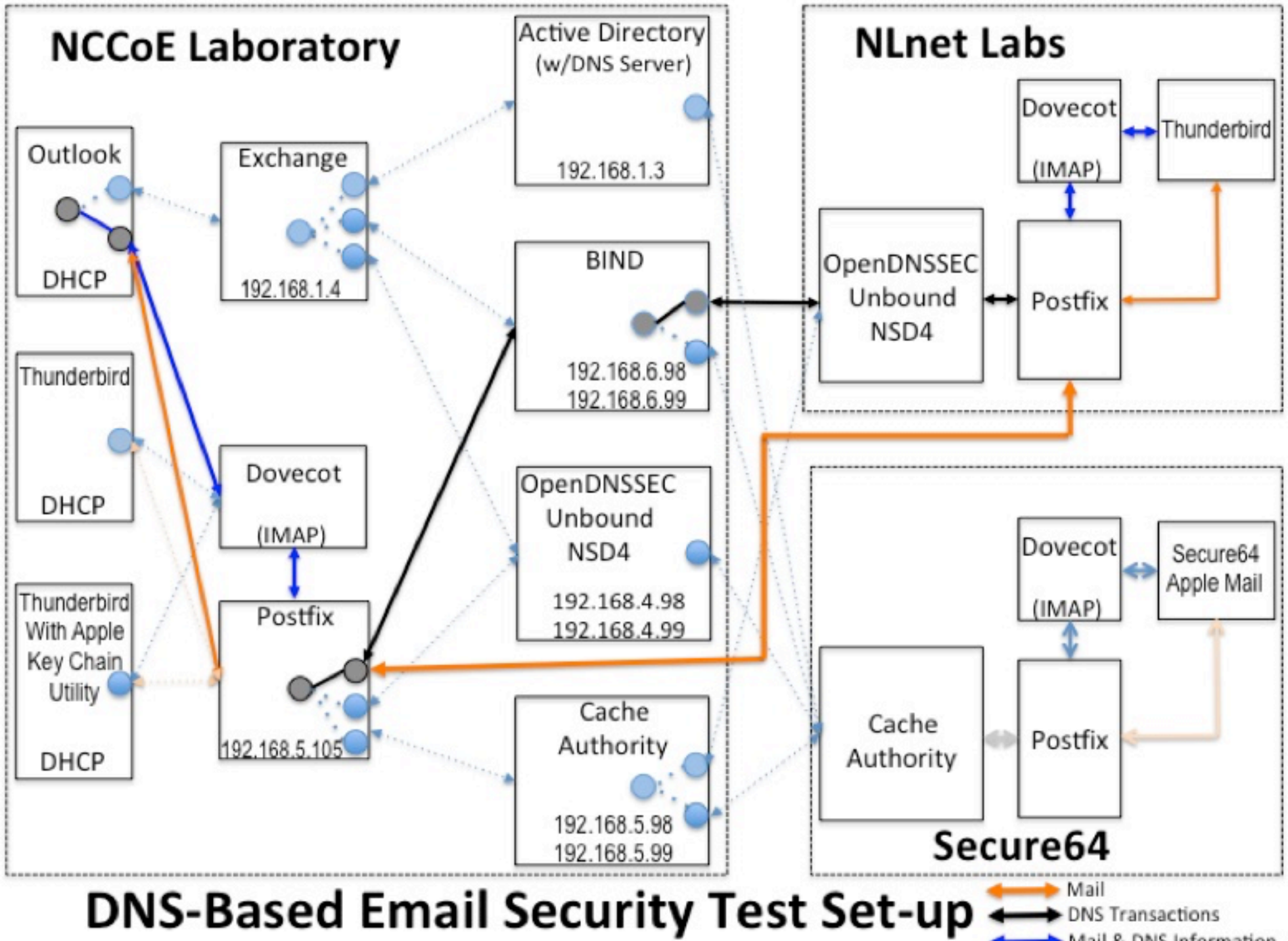
The DNS Parts (2)

- NLnet Labs
  - nsd4, Unbound, OpenDNSSEC
- Secure64
  - DNS Signer, DNS Cache, DNS Manager, Apple Keychain Utility

The Product

- NIST Publication: Practice Guide SP 1800-6
  - A HowTo
  - Tested example configurations
- There will be a Public Comment Period
- Breaking news: Report published
  - https://nccoe.nist.gov/projects/building_blocks/secured_email

Environment



DNS-Based Email Security Test Set-up

Main Scenarios

- Transport security
  - TLSA DNSSEC
- End-to-End Security
  - S/MIME Signed mail
  - Encrypted

Well defined tests

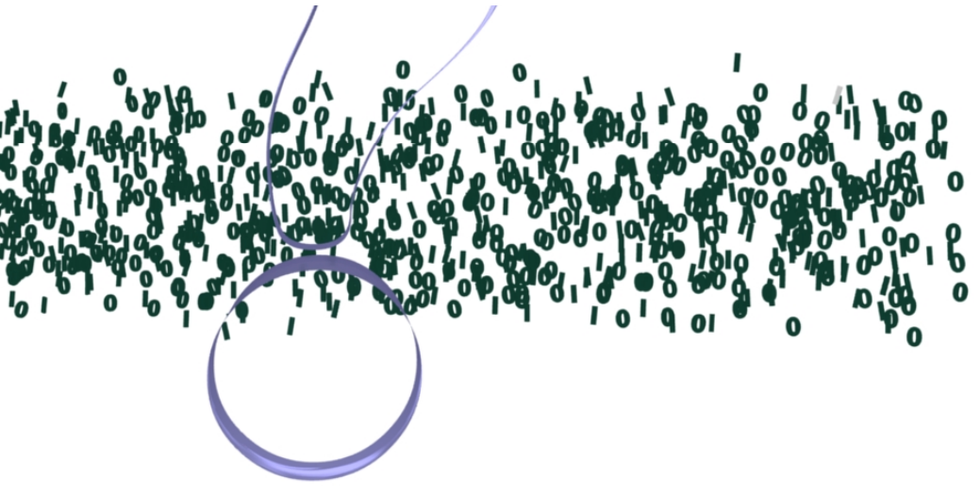
Sequence 3	NCCoE Lab	Legitimate Remote Site	Certificate on Receiver Side	Legitimate Remote Site	
Event	MUA	MTA	DNS Service	Secure 64	Certificate on Receiver Side
13	Outlook	Exchange	Active Directory	Thunderbird on MacBook, Postfix/ Dovecot, DNS Authority/ Cache/ Signer Local CA issued (CU=2)	Local CA (CU=1)
14	Thunderbird	Postfix/ Dovecot	NSD4/ Unbound/ OpenDNSSEC	Same as 13	Local CA issued (CU=1)
15	Thunderbird on MacBook	Postfix/ Dovecot	DNS Authority/ Cache/Signer	Same as 13	Local CA issued (CU=1)
16	Outlook	Exchange	Active Directory	Same as 13	Self-Signed Cert (CU=3)
17	Thunderbird	Postfix/ Dovecot	NSD4/ Unbound/ Open DNSSEC	Same as 13	Self-Signed Cert (CU=3)
18	Thunderbird	Postfix/ Dovecot	BIND	Same as 13	Self-Signed Cert (CU=3)

Results

- No surprises here
  - Tests met expectations
- Analyses of tampering attempts from logfiles

Role of DNSSEC

- Enables verification of trust in the applications



Questions

NLnet Labs