DNS-based email security

Ralph Dolmans
Benno Overeinder
{ralph, benno}@nlnetlabs.nl

Industry partners

Email exchange integrity is at risk

- Disclosure or modification of message.
  - STARTTLS (MTA-MTA)
  - StripTLS
- No source authentication.
  - S/MIME signing (MUA-MUA)
  - Have to trust all Certificate Authorities
  - Difficult to find certificates

Solution: Use DNS to bind keys to names

- TLS keys (TLSA)
- S/MIME (SMIMEA)

- Must validate using DNSSEC!

Solutions exist, but adoption is limited

- Guidance and recommendations needed

- NIST/NCCoE project:
  - Demonstrate using available standards-based software

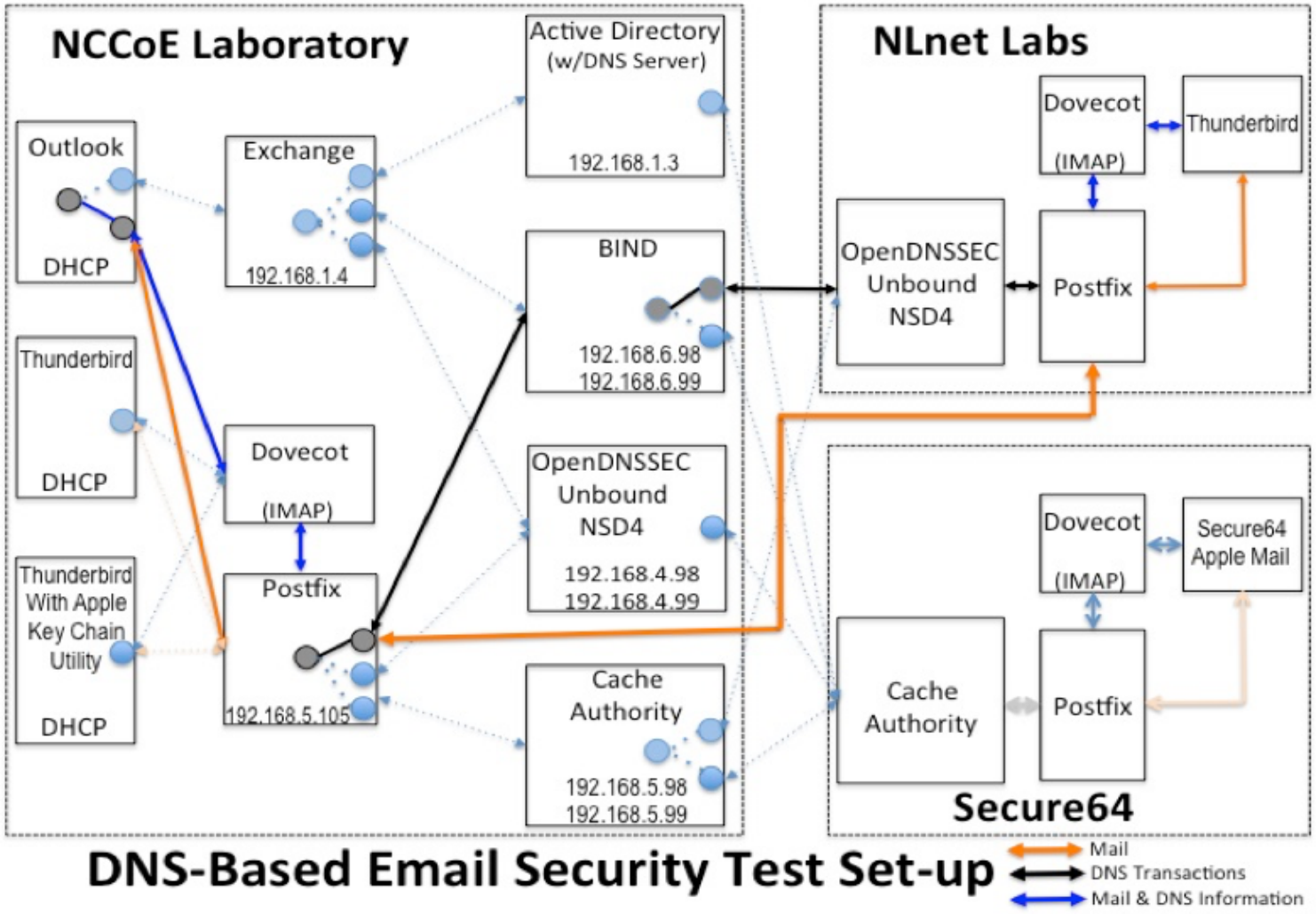
Approach

- Map security characteristics to NIST best practices
  - NIST Special Publication 800-177 (SP800-177), Trustworthy Email
- Describe example solution, **with instructions from implementers**
- Evaluate example solution

Building blocks

- MUA
  - Microsoft Office, Thunderbird
- MTA
  - Postfix, Exchange
- DNS
  - **NSD, Unbound, OpenDNSSEC**
  - BIND, Secure64

Test environment



Test scenarios

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)

DNSSEC enables verification of trust

- Test scenarios successfully executed!
- See: NIST Cybersecurity Practice Guide (1800-6)