NIST SP 800-177: Trustworthy Email

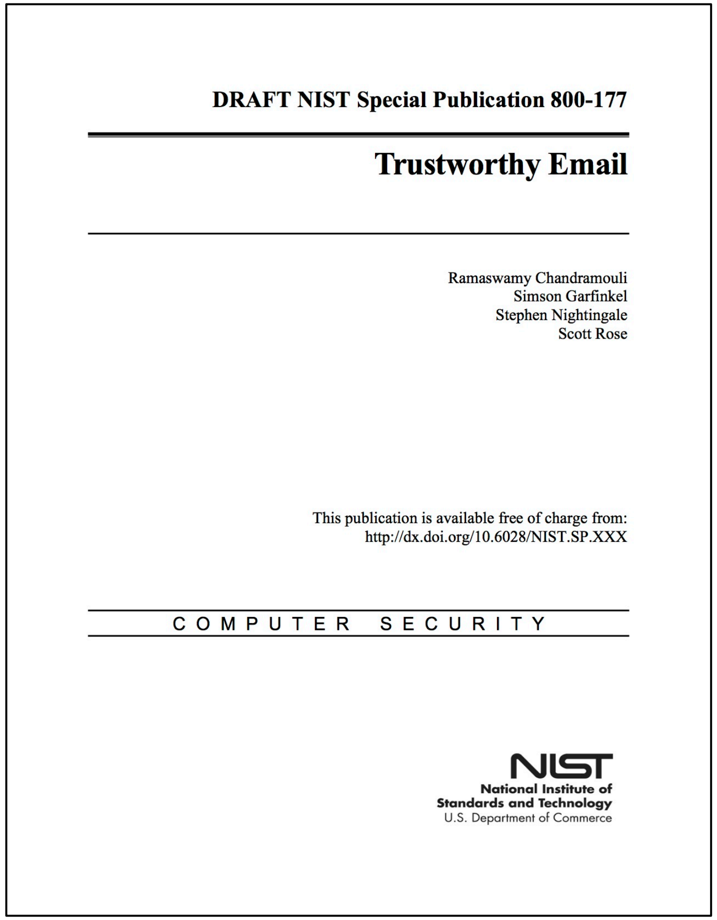
Scott Rose, NIST

FCSM Meeting

4/21/2016

Overview

- SP 800-177 does not obsolete SP 800-42 *Guidelines on Electronic Mail Security*
  - SP 800-177 covers the service of email, not email servers
- Drivers
  - Use of email as core G2G, C2G communication, yet inherently untrustworthy
  - Public awareness of encryption to combat passive monitoring
  - DHS Federal Network Resiliency (FNR) FISMA Metrics call out anti-phishing as key technologies for agencies to deploy



DRAFT NIST Special Publication 800-177

Trustworthy Email

Ramaswamy Chandramouli
Simson Garfinkel
Stephen Nightingale
Scott Rose

This publication is available free of charge from:
http://dx.doi.org/10.6028/NIST.SP.XXX

COMPUTER SECURITY

NIST
National Institute of Standards and Technology
U.S. Department of Commerce

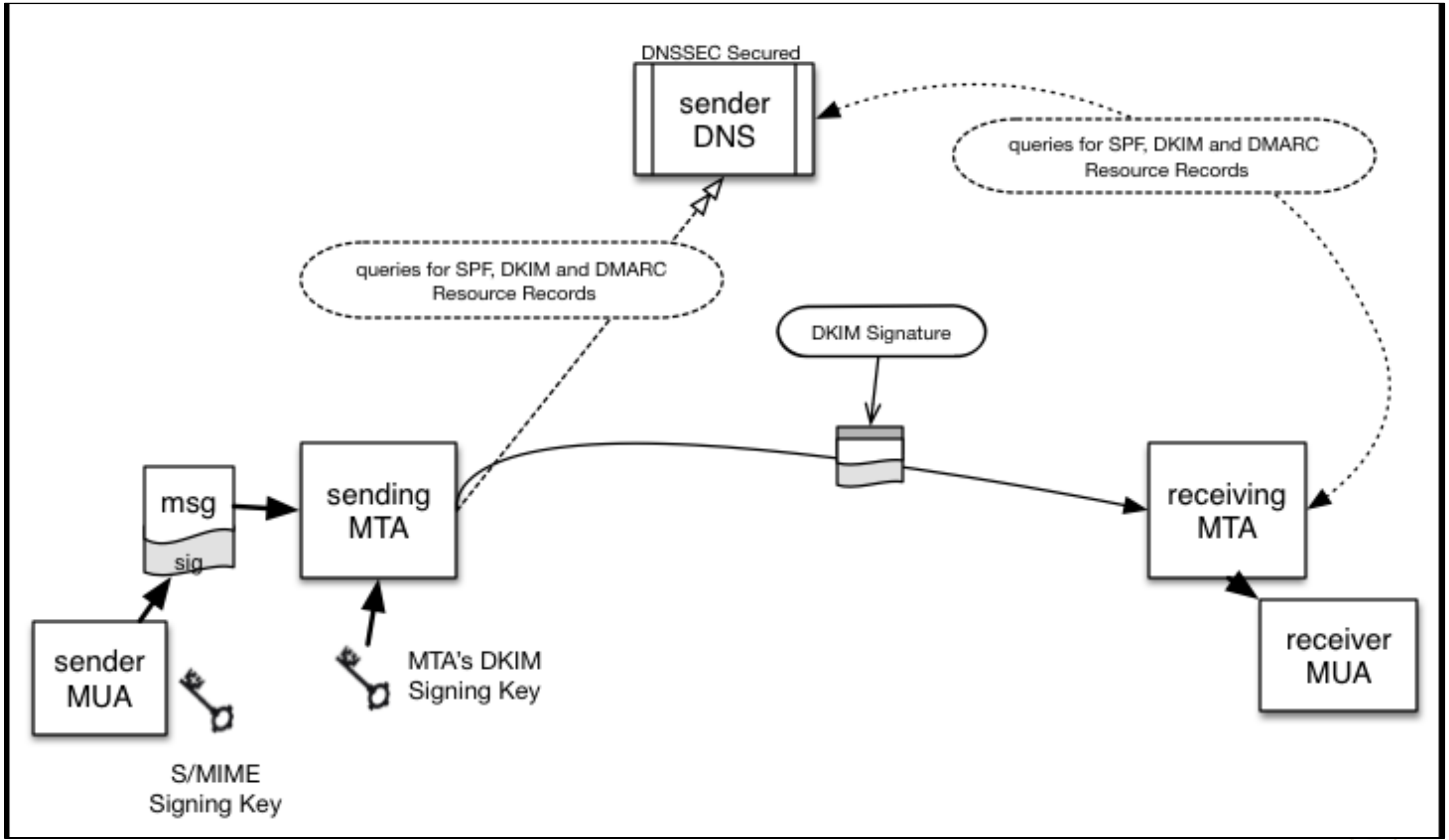
What the Guide Covers

- Overview of core email protocols
  - SMTP, IMAP/POP3, S/MIME, DNS
- Threats to an email service
- DNS-based technologies
  - Sender Policy Framework, DomainKeys Identified Mail, etc.
- Email confidentiality protection
  - SMTP over TLS, S/MIME, OpenPGP
- Reducing Unwanted Bulk Email (i.e. Spam)
- Protecting mail client to mail server communications

What Is Not In the Guide

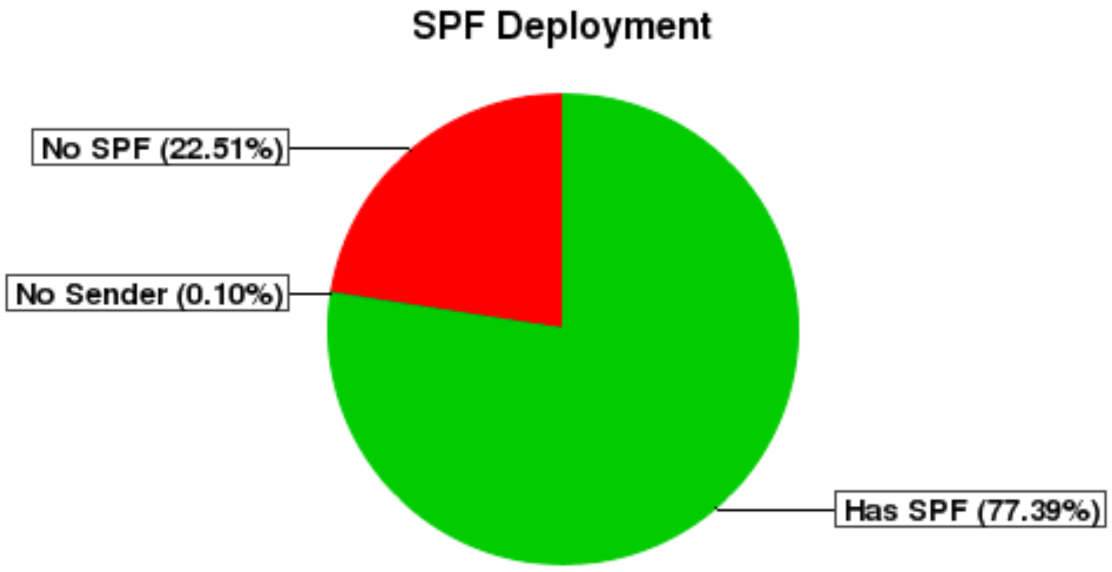
- New Requirements
  - Only guidance and recommendations, Not a new mandate
  - That may come via another source, if not already here
- How-to's
  - Too many varied implementations
  - NCCoE's SP 1800 series document will contain more concrete examples for implementations used in their project.
    - Microsoft Exchange, Postfix, Various DNS servers, Outlook, etc.

Example Email Flow



DNS-Based Email Authentication

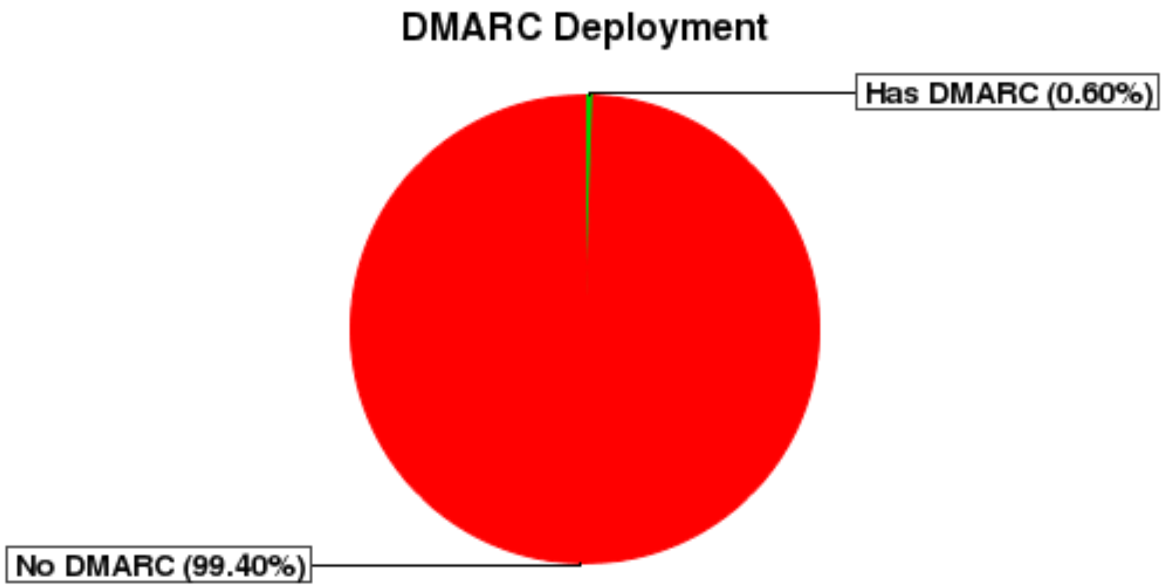
- Sender Policy Framework (SPF)
  - Use DNS Resource Record to list valid senders for a domain
  - Can also state “no senders for this domain”
- DomainKeying Identified Mail (DKIM)
  - Servers digitally sign each message. (Not sender)
  - Public key stored in the DNS.



SPF Deployment in .gov TLD (April 2016)

DNS-Based Email Authentication

- Domain-based Message Authentication and Reporting Conformance (DMARC)
  - Policy encoded into DNS RR to tie SPF, DKIM and sender's domain together.
  - Protocol specifies reporting system where receivers report back to senders how email was disposed (quarantine, delivered, etc.)
  - Also report domain use in phishing by victims to spoofed domain



DMARC Deployment in .gov TLD (April 2016)

Protecting Email Confidentiality

- SMTP over TLS
  - Server-to-server encryption
  - No guarantee all hops will be protected
  - Certificate management recommendations (or use the DNS to publish certs)

- S/MIME
  - End-to-end encryption and/or digital signing of email from sender to receiver
  - No middle systems can see contents (i.e. malware filters)
  - PKIX issues (missing certificate chains)
  - Recommendations (including emerging standards using DNS to publish certs)

- Nat. Cybersecurity Center of Excellence (NCCoE) Project
  - Produce practice guide for SMTP over TLS and S/MIME signing using various available implementations

Next Steps

- 2nd Public comment period ends 4/29
    - Read and Review! Especially anything called out as "Security Recommendation"
- NCCoE DNS-Based Secured Email project
    - Building Block project will produce SP-1800 series document
- Push for deployment?
    - Already called out in FNR's FISMA metrics for FY15 and FY16

Resources

- SP 800-177:
  - http://csrc.nist.gov/publications/drafts/800-177/sp800-177_second-draft.pdf
- NCCoE DNS-Based Secured Email Building Block Project:
  - https://nccoe.nist.gov/projects/building_blocks/secured_email
- NIST High Assurance Domain project:
  - Test tools, Deployment measurement, links to guides, etc.
  - https://www.had-pilot.com/