M3AAWG
Messaging Malware Mobile
Anti-Abuse Working Group

# NIST Email Security Improvements

William C. Barker and Scott Rose

October 22, 2015

M3AAWG 35th General Meeting



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

NCCoE National Cybersecurity Center of Excellence

# Presenters

- Scott Rose
  Computer Scientist, NIST ITL
- William (Curt) Barker
  Guest Researcher, NIST ITL/NCCoE

# Email Related Projects

- High Assurance Domain (HAD)
  - NIST Information Technology Lab (ITL)
  - MoU between DHS Science and Technology, NIST, and Financial Services Sector Coordinating Committee (FSSCC)
- DNS-based Secure Email
  - Nat. Cybersecurity Center of Excellence.

# Previous (Non-NIST) Efforts

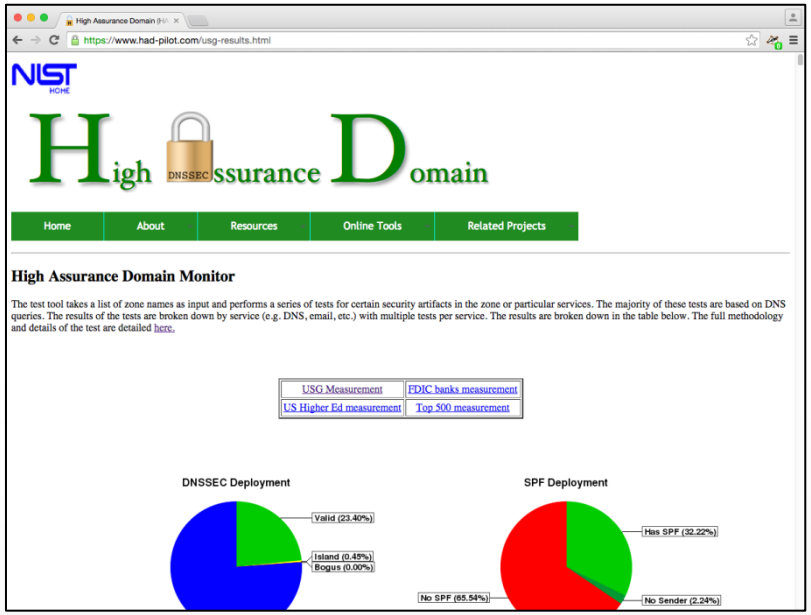
- 2011 DNSSEC and Authenticated Email Tiger Team
  - Goal was to promote use of SPF and DKIM
- DHS Federal Network Resiliency (FNR)
  - Weekly scans of federal .gov space for SPF records
  - Calls out DMARC in FY15 FISMA metrics
    - Asks agencies to report deployment as well as email received that conforms/fails checks.

# The Goal

- Every email sent using a .gov "From" address was sent from an authoritative server for the organization and can be authenticated.
- Every email sent to an .gov email address can be encrypted by an easily obtainable public key.

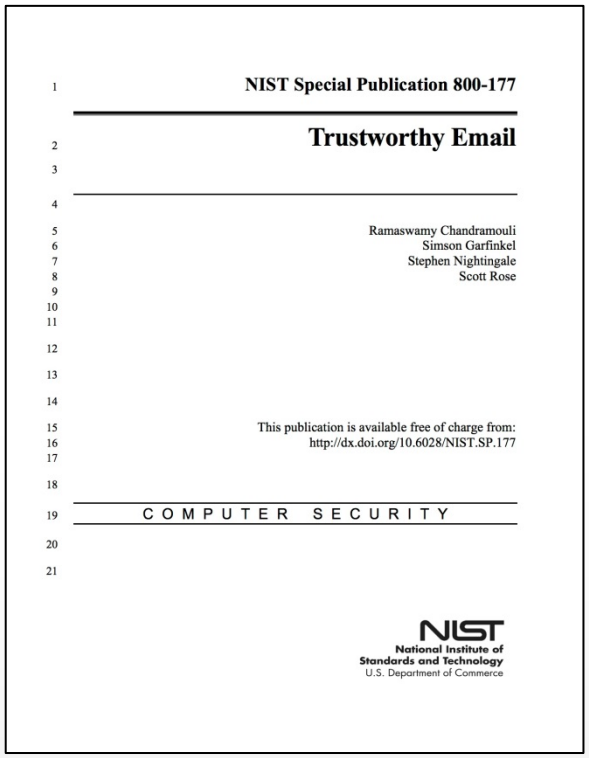
# had-pilot.com Web Tools

- Collection of tools, documents, etc.
  - SPF/DKIM/DMARC test tool
  - DMARC report collection service (beta - .gov only)
  - Deployment measurement tool
  - DANE TLSA Test tool and test tree
    - HTTPS and SMTP (beta)




https://www.had-pilot.com/

# NIST SP 800-177 Trustworthy Email



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.177

COMPUTER SECURITY

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

- Guidance and Recommendations for trustworthy email as a service
- Response to FY15 CIO FISMA metrics
  - Calls out email authentication for all federal agencies
- Public Comment Ends: 11/30/2015

http://csrc.nist.gov/publications/PubsDrafts.html#800-177

# NIST SP 800-177 Recommendations

- Deploy SPF, DKIM and DMARC
  - Calls out federal policy for keys (for DKIM)
- Use S/MIME for digital signatures for email (not OpenPGP)
- If deploying DANE, use DANE-TA for SMTP server certs.
  - Agencies must still do PKIX on all certs per existing policy and obtain certs from “well known CAs”
- S/MIME encrypted email should be stored on encrypted file system, but not using the S/MIME key.

# SMIMEA

- SMIMEA plugin prototype
  - NIST Small Business Innovation Research (SBIR) Grant to Grier Forensics to produce plugin
- SMIMEA-usage Internet-Draft
  - Give implementation and deployment guidance as a companion draft to core SMIMEA spec.

# Coming Soon

- SMIMEA and OPENPGPKEY test tools
  - Including examples (good and bad)
- DANE for SMTP test tree for testing DANE-aware clients.
- Final version of Special Publication with possible input used for NCCoE project.

# National Cybersecurity Center of Excellence

M3AAWG
Messaging Malware Mobile
Anti-Abuse Working Group

- The National Cybersecurity Center of Excellence (NCCoE) provides businesses with real-world cybersecurity solutions —based on commercially available technologies. The center brings together experts from industry, government and academia to demonstrate integrated cybersecurity that is cost-effective, repeatable and scalable.
- Hosted by the National Institute of Standards and Technology (NIST), the Center fosters collaboration with industry to identify and solve using commercially available components today's most pressing cybersecurity challenges.
- The NCCoE's strategy is focused on and driven by the practical cybersecurity needs of the business community.



NIST National Institute of Standards and Technology U.S. Department of Commerce
NCCoE National Cybersecurity Center of Excellence

# Some NCCoE Projects

M3AAWG
Messaging Malware Mobile Anti-Abuse Working Group

## CURRENT NCCoE PROJECTS

- Trusted Geolocation in the Cloud and Hardware Roots of Trust
- Secure Exchange of Electronic Health Information
- Health IT Infusion Pump
- Identity and Access Management in the Energy Sector
- Situational Awareness in Energy Systems
- IT Asset Management
- Attribute Based Access Control
- Mobile Device Security Building Blocks
- Software Access Management Building Blocks

## SOME PROJECTS IN THE PROCESS OF BEING INITIATED

- Derived Personal Identity Verification Credential for Mobile Device Environments
- Domain Name System-Based Electronic Mail



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

NCCoE National Cybersecurity Center of Excellence

# DNS-Based E-Mail Security

## Challenge:

M3AAWG
Messaging Malware Mobile
Anti-Abuse Working Group

- Business operations are heavily reliant on e-mail exchanges.
- Cryptographic functions provide security services for e-mail exchanges.
- Many enterprises rely on mail servers to provide security to the members of enterprises rather than end-to-end security mechanisms:
  - ✧ Economies of scale
  - ✧ Need for a uniform security implementation
- Many current server-based e-mail security mechanisms are vulnerable to, and have been defeated by, attacks on the integrity of their cryptographic implementations that result in unauthorized parties:
  - ✧ Reading or modifying supposedly secure information
  - ✧ Using e-mail as a vector to insert malware that denies access to critical information or processes or damages or destroys system components and/or information.
- Improved e-mail security is needed to protect against these consequences.



NIST National Institute of Standards and Technology U.S. Department of Commerce
NCCoE National Cybersecurity Center of Excellence

# Domain Name System-based Authentication of Named Entities (DANE)

M3AAWG
Messaging Malware Mobile Anti-Abuse Working Group

- Domain Name System Security Extensions (DNSSEC) for the Internet's Domain Name System can be used by service providers to protect against unauthorized:
  - ✧ Modification to network management information and
  - ✧ Connections to devices operated by untrustworthy parties.
- DANE securely associates internet domain names with cryptographic certificates and related security information so they can't be fraudulently modified or replaced.
- In spite of the dangers of failure to authenticate the identities of network devices, adoption of DNSSEC has been slow.
- Demonstration of DANE-supported applications such as reliably secure e-mail may support increased user demand for domain name system security and serve as a mechanism supporting reliably secure e-mail.

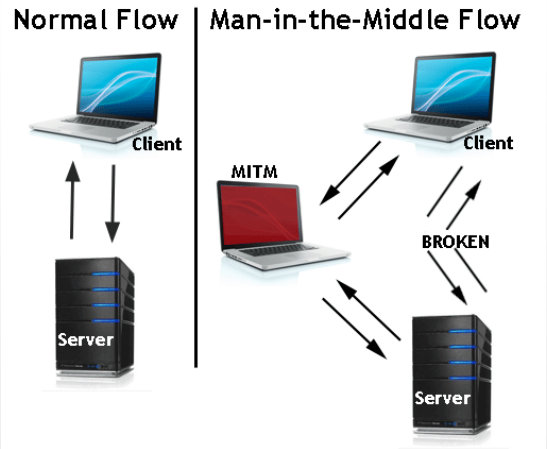


NIST National Institute of Standards and Technology U.S. Department of Commerce
NCCoE National Cybersecurity Center of Excellence

# DNS-Based E-Mail Security Building Block

M3AAWG
Messaging Malware Mobile Anti-Abuse Working Group

- Security platform composed of off the shelf components providing trustworthy server-to-server e-mail exchanges.
- DANE authenticates servers and certificates in two roles by binding the X.509 certificates used for:
  - ✧ Transport Layer Security (TLS) to internet domain names verified by DNSSEC and supporting the use of the certificates for e-mail and
  - ✧ S/MIME protocol-based e-mail security in emailing addresses encoded as DNS names verified by DNSSEC.






NIST National Institute of Standards and Technology U.S. Department of Commerce
NCCoE National Cybersecurity Center of Excellence

# DNS-Based E-Mail Security Building Block

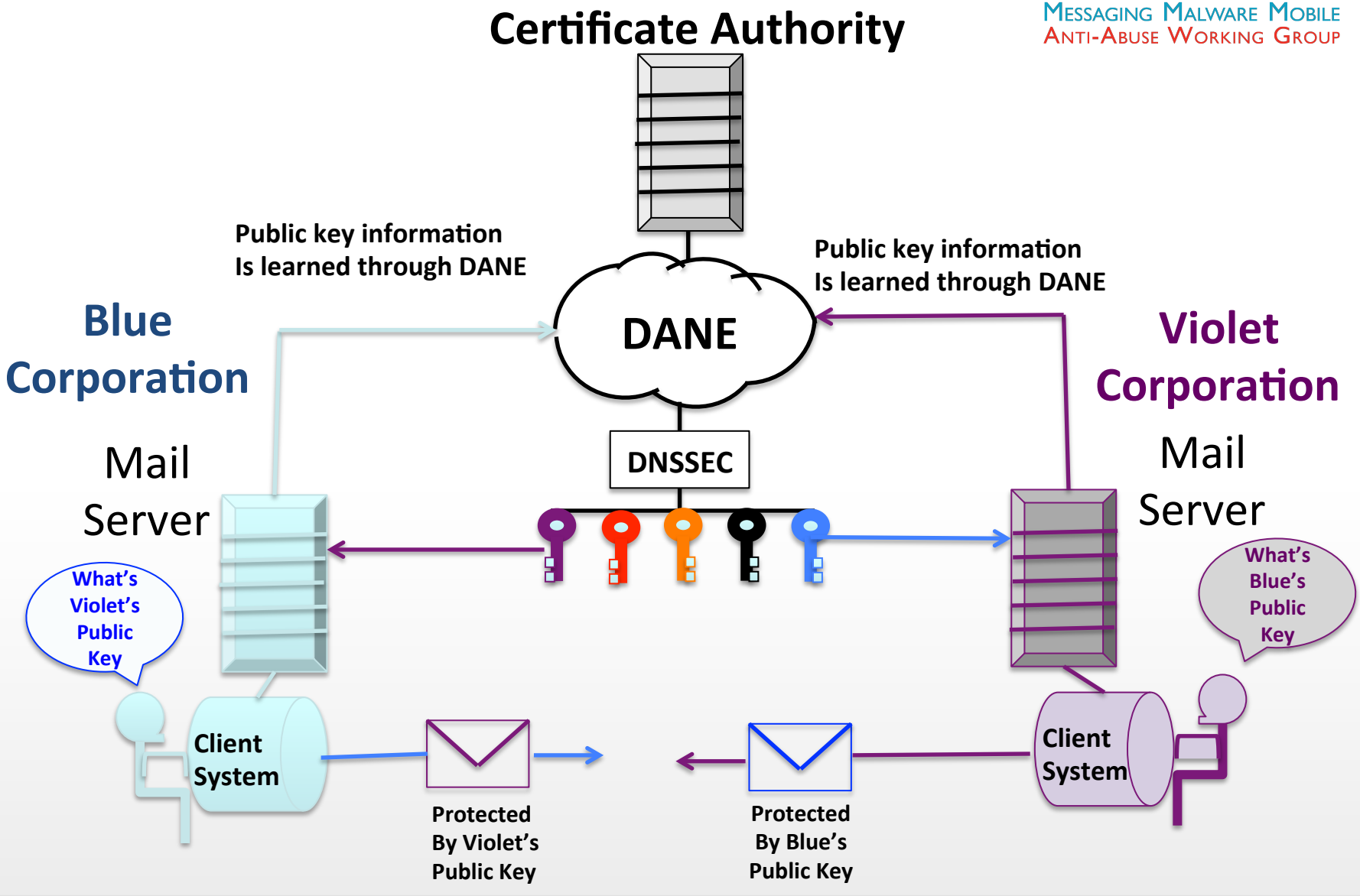
M3AAWG
Messaging Malware Mobile Anti-Abuse Working Group

- The bindings support trust in the use of S/MIME certificates in the end-to-end email communication by:
  - ✧ Encrypting e-mail traffic between servers,
  - ✧ Allowing individual email users to digitally sign and/or encrypt email messages to other end users, and
  - ✧ Allowing individual email users to obtain other users' certificates to validate signed email or send encrypted email.
- E-mail sending policy consistent with a stated privacy policy.
- Documentation of the resulting platform includes:
  - ✧ Specification of hardware and software,
  - ✧ Implementation requirements, and
  - ✧ Mapping implementation requirements to policies, standards, and best practices.



NIST National Institute of Standards and Technology U.S. Department of Commerce
NCCoE National Cybersecurity Center of Excellence

# DNS-Based E-Mail Security



## *Federal Register* invitation to participate in build team

Publication Date: Tuesday, October 06, 2015
URL: https://federalregister.gov/a/2015-25304
Comment Period: 30 Days ending November 5, 2015

Interested parties must contact NIST to request a letter of interest template to be completed identifying the organization requesting participation in the Domain Name System- Based Security for Electronic Mail Building Block and the capabilities and components that are being offered to the collaborative effort. Letters of interest will be accepted on a first come, first served basis.

## Preliminary High Level Design Description

Comments Invited (Per FRN): *http://nccoe.nist.gov/DNSSecuredEmail*

## Cooperative R&D Agreements

Organizations whose letters of interest are accepted in accordance with the process set forth in the *Federal Register* notice will be asked to sign a Cooperative Research and Development Agreement (CRADA) with NIST. A CRADA template can be found at: *http://nccoe.nist.gov/node/138.*

# DNS-Based E-Mail Security Components Sought

M3AAWG
Messaging Malware Mobile Anti-Abuse Working Group

Components are listed in the DNS-Based E-Mail Security Building Block description (http://nccoe.nist.gov/DNSSecuredEmail ) and include, but are not limited to:

- Client systems
- DNS/DNSSEC services
- Mail transfer agents
- DNS resolvers (stub and recursive) for DNSSEC validation
- Authoritative DNS servers for DNSSEC signed zones
- Mail server/mail security systems
- S/MIME certificates
- Extended validation and domain validation TLS certificates

Each interested organization's letter of interest should identify how their product(s) address one or more of the desired solution characteristics in the Building Block description.

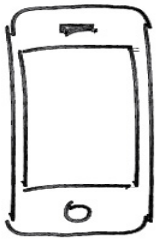


NIST National Institute of Standards and Technology U.S. Department of Commerce
NCCoE National Cybersecurity Center of Excellence

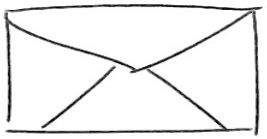
M3AAWG
Messaging Malware Mobile
Anti-Abuse Working Group

240-314-6800

nccoe@nist.gov



# Participate



http://nccoe.nist.gov

9600 Gudelsky Drive
Rockville, MD 20850



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

NCCoE National Cybersecurity Center of Excellence