NIST SPECIAL PUBLICATION 1800-6A

Domain Name System-Based Electronic Mail Security

Volume A:
Executive Summary

Scott Rose
Information Technology Laboratory
National Institute of Standards and Technology

William Barker
Dakota Consulting
Silver Spring, MD

Santos Jha
Chinedum Irrechukwu
The MITRE Corporation
McLean, VA

Karen Waltermire
National Cybersecurity Center of Excellence
National Institute of Standards and Technology

January 2018

This publication and its additional content is available free of charge from:
https://doi.org/10.6028/NIST.SP.1800-6

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

NCCoE
NATIONAL CYBERSECURITY CENTER OF EXCELLENCE

Executive Summary

Both public and private-sector business operations are heavily reliant on electronic mail (email) exchanges, but the integrity of these transactions is often at risk, including financial and other proprietary information, as well as the privacy of employees and clients.

Tools exist that are capable of providing the needed email security and privacy protection, but a number of factors have impeded the adoption of these existing security and privacy capabilities. These include:

- The absence of comprehensive configuration instructions for composed sets of trusted electronic mail components,
- The absence of easily accessible information that points systems administrators to easily implemented software libraries and software applications, and
- A perception that email security measures negatively impact the performance of email systems.

However, operating an email system without employing the available security and privacy tools invites attackers to breach sensitive enterprise information by introducing false addresses into mail messages, disrupting secure communication signaling, and improving the probability of successfully inducing enterprise users to open malicious attachments – still the most common method for introducing malware and breaching enterprise systems.

The National Cybersecurity Center of Excellence (NCCoE) developed a set of example email security solutions that can help organizations to more easily implement security and privacy tools and protocols, thus reducing the likelihood of a data breach. The example security platforms described in this guide are consistent with the guidance and best practices contained in government and industry security standards. How these platforms address specific security requirements and best practices is addressed in Volume B of this guide.

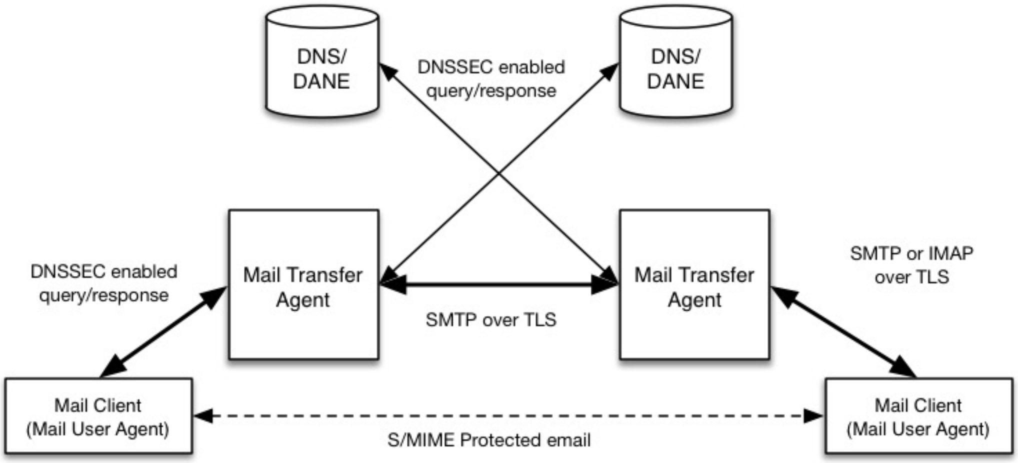
The NCCoE's approach permits the use of both open source and commercially available products that can be included alongside the current mail products in existing infrastructure. The example solution set is described in Volume C, a "How To" guide that shows how to implement a set of standards-based, commercially available cybersecurity technologies in the real world.

CHALLENGE

Whether the security service desired is an authentication of the source of an email message or an assurance that the message has not been altered by or disclosed to an unauthorized party, organizations must employ some cryptographic protection mechanism. Economies of scale and a need for uniform security implementation drive most enterprises to rely on mail servers and/or Internet service providers (ISPs) to provide security to all members of an enterprise. Many of these server-based email security mechanisms are vulnerable to, and have been defeated by, attacks on the integrity of the cryptographic implementations on which they depend. The consequences of these vulnerabilities frequently involve unauthorized parties being able to read or modify supposedly secure information, or to use email as a means to insert malware into the system in order to gain access to enterprise systems or information. Protocols exist that can provide the needed email security and privacy, but the adoption of these existing protocols has been limited by impediments such as the unavailability of easily implemented software libraries, and software application characteristics that complicate the operation of email systems.

SOLUTION

This project has produced a set of proof-of-concept security platforms that demonstrate trustworthy email exchanges across organizational boundaries. The goals of the project included the authentication of mail transfer agents, signing and encryption of email, and binding cryptographic key certificates to the servers. The Domain Name System Security Extension (DNSSEC) protocol was used to authenticate server addresses and certificates used for Transport Layer Security (TLS) to DNS names. The business value of the security platforms demonstrated by this project includes improved privacy and security protection for users' operations and improved support for the implementation and use of the protection technologies. The platform also expands the set of available DNS security applications and encourages wider implementation of DNSSEC, TLS and S/MIME to protect internet communications. The security enhancements offered by this project are shown below.



The major types of mail components (users' mail clients and enterprises' mail transfer agents) are shown together with the supporting DNS infrastructure used to send and secure email. Each protocol used in email transactions (and the supporting DNS) has an accompanying security extension (such as DNSSEC) or a secure transport option (Transport Layer Security, or TLS for mail).

The project involved the composition of a variety of components provided by a number of different technology providers, including Microsoft Corporation, the Internet Systems Consortium, Secure64, Fraunhofer IAO, and Stichting NLnet Laboratories. Each of these collaborators entered into a Cooperative Research and Development Agreement (CRADA) with NIST to participate in this consortium effort.

While a suite of commercial products was used to address this challenge, this guide does not endorse these particular products, nor does it guarantee compliance with any regulatory initiatives. An organization's information security experts should identify the products that will best integrate with the existing tools and IT system infrastructure. An organization can adopt this solution or one that adheres to these guidelines in whole, or this guide can be used as a starting point for tailoring and implementing parts of a solution.

The guide:

- Identifies the security characteristics needed to sufficiently reduce the risks to information exchanged by email;
- Maps security characteristics to standards and best practices from NIST and other organizations;
- Describes a detailed example solution, along with instructions for implementers and security engineers on efficiently installing, configuring, and integrating the solution into existing IT infrastructures; and
- Provides an example solution that is operationally practical and evaluates the performance of the solution in real-world scenarios.

BENEFITS

The example solution:

- Reduces risk so that employees are able to exchange personal and enterprise information via email with significantly reduced risk of disclosure or compromise;
- Enables the use of existing security protocols more efficiently and with minimal impact to email service performance;
- Integrates capabilities into various server and client IT infrastructure environments;
- Enhances visibility for system administrators into email security events, providing for a recognition of authentication failures that could result in device and data compromises;
- Implements both commercial and open source industry standard network and email security controls, reducing long-term costs and decreasing the risk of vendor lock-in; and
- Can be extended to other enterprise information exchange technologies that are growing in use (e.g., text messages, chat).

SHARE YOUR FEEDBACK

The guide can be reviewed or downloaded at https://nccoe.nist.gov/projects/building-blocks/secured-email. Help us make it better by sharing your thoughts with us. If you adopt this solution for your own organization, please share your experience and advice. We recognize that technical solutions alone will not fully enable the benefits of our solution, so we encourage organizations to share lessons learned and best practices for transforming the business processes associated with implementing it.

To provide comments or to learn more by arranging a demonstration of the solution, contact us at dns-email-nccoe@nist.gov.

TECHNOLOGY PARTNERS/COLLABORATORS

Organizations participating in this project submitted their capabilities in response to an open call in the Federal Register for all sources of relevant security capabilities from academia and industry (vendors and integrators). The following respondents with relevant capabilities or product components (identified as "Technology Partners/Collaborators" herein) signed a Cooperative Research and Development Agreement to collaborate with NIST in a consortium to build this example solution.

Certain commercial entities, equipment, products, or materials may be identified by name or company logo or other insignia in order to acknowledge their participation in this collaboration or to describe an experimental procedure or concept adequately. Such identification is not intended to imply special status or relationship with NIST or recommendation or endorsement by NIST or NCCoE; neither is it intended to imply that the entities, equipment, products, or materials are necessarily the best available for the purpose.

The National Cybersecurity Center of Excellence (NCCoE), a part of the National Institute of Standards and Technology (NIST), is a collaborative hub where industry organizations, government agencies, and academic institutions work together to address businesses' most pressing cybersecurity challenges. Through this collaboration, the NCCoE applies standards and best practices to develop modular, easily adaptable example cybersecurity solutions using commercially available technology.

LEARN MORE

Visit https://nccoe.nist.gov
nccoe@nist.gov
301-975-0200