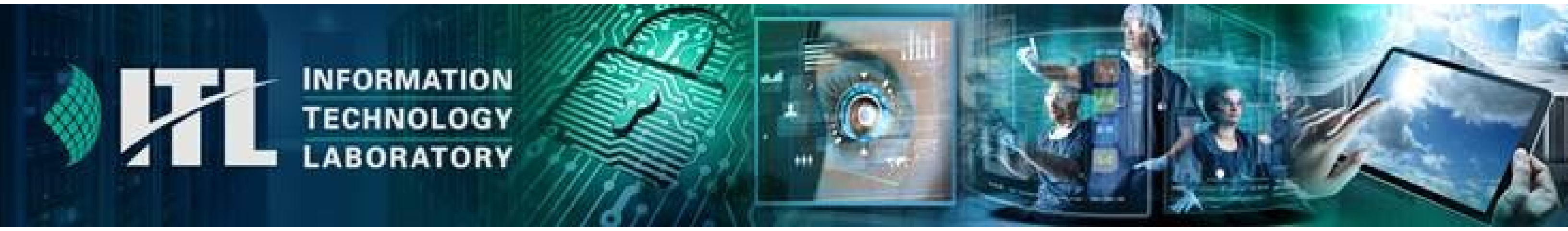


ITL BULLETIN FOR APRIL 2018

IMPROVING THE TRUSTWORTHINESS OF EMAIL, AND BEYOND!

Scott Rose, Larry Feldman,[1] and Greg Witte,[1] Editors
Information Technology Laboratory
National Institute of Standards and Technology
U.S. Department of Commerce

Introduction

Each of us relies heavily on electronic mail (email) exchanges at home and at work, but the integrity of these transactions is often at risk. By one count,[2] in the time it takes to read this sentence, 18,730,509 emails will have been sent somewhere on the Internet. (Unfortunately, 12.5 million of those will likely be spam!) Many emails include financial, proprietary, and privacy-related information that needs to be protected.

This article introduces some of the work that is being done to address solutions for providing digital signature technologies to authenticate and protect the integrity of email on an end-to-end basis, protecting confidentiality of email in transit among organizations. These tools have been available but not widely adopted in the past. Yet, operating an email system without taking advantage of these security and privacy tools increases risks unnecessarily. NIST's Information Technology Laboratory, through the National Cybersecurity Center of Excellence (NCCoE), recently published Special Publication (SP) 1800-6, *Domain Name System-Based Electronic Mail Security*, as a guide for how to architect, install, and configure a security platform for trustworthy email exchanges across organizational boundaries.

The Challenge

Both private industry and the government are concerned about email security and the use of email as an attack vector for cybercrime. Business operations rely heavily on email exchanges and need to protect the confidentiality of business information, the integrity of transactions, and the privacy of individuals. Some protections are in place; cryptography is often used to authenticate the source of email messages, safeguard against undetected, unauthorized alteration of messages in transit, and maintain message confidentiality. Policies support reliance on mail servers to provide cryptographic protection for email rather than on end-to-end security operated by individual users.

[1] Larry Feldman and Greg Witte are Guest Researchers from G2, Inc.

[2] http://www.internetlivestats.com/one-second/#email-band

Organizations need to protect their server-based email security mechanisms against intrusion and man-in-the-middle attacks during automated cryptographic service negotiation. In the absence of an appropriate combination of Domain Name System (DNS) Security Extensions (DNSSEC) and certificate-based protections, any of these attacks can result in disclosure or modification of information by unauthorized third parties.

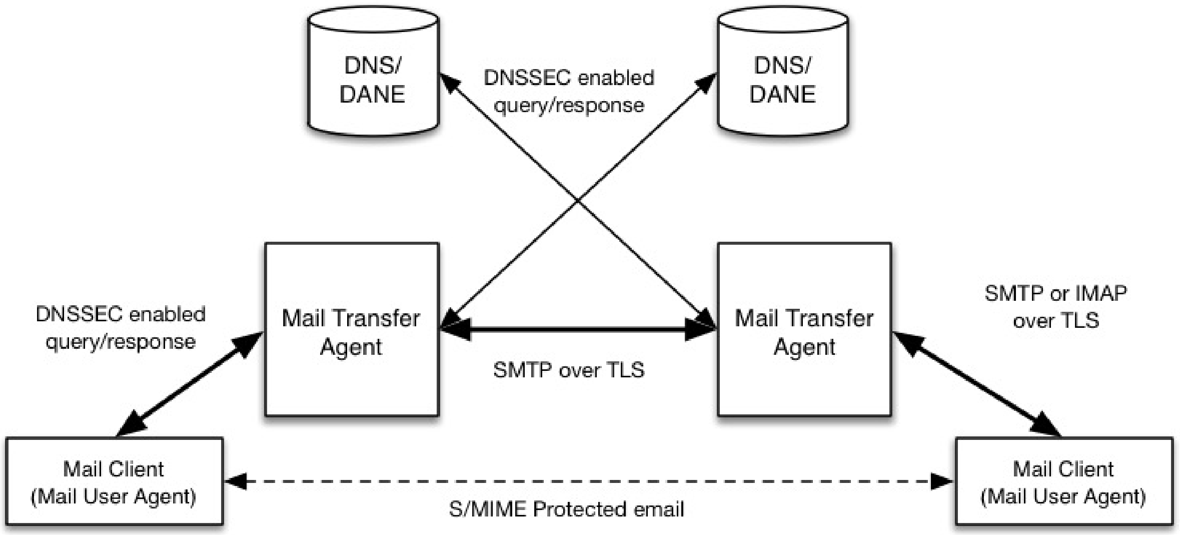
The attacks can also enable an attacker to pose as one of the parties to an email exchange and send email that contains links to malware-ridden websites. Inclusion of links to malware is a major factor in most confirmed data breaches. Three significant consequences of such breaches are: 1) exposing sensitive or private information; 2) enabling fraudulent activity by the attacker posing as the victimized user; and 3) disabling or destroying the user's system—or that of the user's parent organization. Beyond avoiding the negative consequences to users, improved email security can also serve as a marketing discriminator for email service providers.

There have been several impediments to implementation of DNSSEC and DNS-Based Authentication of Named Entities (DANE) in the past. A shortage of easily used software libraries, deployment tools, and DNSSEC-enabled applications reduced usage. Moreover, some email applications of the protocols respond to DNSSEC failures by deferring or terminating the delivery attempt, often failing to alert the mail server that failure to deliver is based on a DNSSEC issue. Mail delivery failure becomes a roadblock to larger DNSSEC/DANE deployment.

A Solution

DNSSEC protects against unauthorized modifications to domain name information to prevent connection to spoofed or malicious hosts. The NCCoE initiated a collaborative project with industry partners to develop a proof-of-concept security platform that provides trustworthy mail server-to-mail server email exchanges across organizational boundaries. Products composing the security platform include client mail user agents (MUAs), DNS servers, mail transfer agents (MTAs), and X.509 cryptographic key certificate sources.

The network infrastructure products are similar to those found in every enterprise and used to perform basic IT functions and handle email. The certificate utilities are needed to produce X.509 certificates for mail servers and end users to support Transport Layer Security (TLS) and Secure/Multipurpose Internet Mail Extensions (S/MIME). This project focused on Simple Mail Transfer Protocol (SMTP) over TLS and S/MIME. The figure below shows the security enhancement offered by this project.


DNS/ DANE
DNSSEC enabled query/response
DNS/ DANE
DNSSEC enabled query/response
Mail Transfer Agent
SMTP over TLS
Mail Transfer Agent
SMTP or IMAP over TLS
Mail Client (Mail User Agent)
S/MIME Protected email
Mail Client (Mail User Agent)

This project demonstrated a security platform, consistent with NIST SP 800-177, *Trustworthy Email*, which provides secure and reliable email exchanges across organizational boundaries. The project included authentication of mail servers, digitally signing and encrypting email, and binding cryptographic key certificates to the servers. The software library issue was addressed in Volume C of NIST SP 1800-6 by providing installation and configuration instructions for using and maintaining existing software libraries (including installation support applications). At the same time, inclusion of software developers and vendors in the development and demonstration process revealed software and implementation guidance shortcomings that have been corrected.

While a suite of commercial products was used to address the challenge, NIST SP 1800-6 does not endorse these 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 build solution or tailor the solution using their currently deployed system; also, this guide can be used as a starting point for tailoring and implementing parts of a solution.

In summary, SP 1800-6 provides the following information. The document:

- 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.

Scenarios and Findings

NIST SP 1800-6 provides security evaluation that involved assessing how well the reference design addresses the objectives of the two scenarios that it was intended to support.

Scenario 1 involved the ordinary exchange of email between two organizations' email servers carried over TLS, where the TLS key management was protected by DANE and DNSSEC. Private certificates were generated by either well-known Certificate Authorities (CAs), enterprise local CAs, or self-signed certificates. User connections to their organizations' respective mail servers were established and maintained within a physically protected zone, and email was encrypted between mail servers using TLS.

The confidentiality of encryption keys was maintained such that no unauthorized third party had access to the keys. The mail servers used X.509 certificates to encapsulate and transport public keys to establish the TLS channel. DNSSEC ensured that each sending mail server receives the IP address to the legitimate and authorized receiving mail server and (if applicable) validates its X.509 certificate using DANE DNS Resource Records (RRs). DANE binds the cryptographic keying material presented by the receiving server to the appropriate domain in the DNS. TLS was used to protect the confidentiality of the email exchange. Encryption of the email message was accomplished by the originator's email server, and decryption of the email message was accomplished by the recipient's email server using standard cryptographic libraries.

The tests included an attempt by a fraudulent mail server to pose as the legitimate mail receiver for a domain. The tests also included a man-in-the-middle attack to attempt to disrupt the TLS connection, with the objective of achieving an unencrypted transmission of the email. Both attempts failed, due to the use of DNSSEC and DANE. In both cases, an indication was made available to the sending email server when the DNSSEC signature associated with the domain data was determined to be invalid.

Scenario 2 involved end-to-end signed email, where email exchanges between organizations were carried over TLS, the email messages were signed and verified with S/MIME on the end users' client devices, and the S/MIME key management was protected by DANE and DNSSEC. Private certificates were generated by well-known and enterprise local CAs. Self-signed certificates were not used. Individuals established connections to their domains' respective mail servers within a physically protected zone of control.

Cryptographic digital signatures were applied to messages to provide authentication and integrity protection for the email. S/MIME was the protocol used for digital signing. These certificates were then encoded in the DNS using the appropriate DANE DNS record type. DNSSEC ensured that each originating user's mail server connects to the intended recipient's mail server. DANE bound the cryptographic keying material to the appropriate server and individual user digital signature certificates. TLS protected the confidentiality of the email. Digital signing of email messages was accomplished by the originator's mail client and checking the validity of the signature—hence the integrity of the authorization provided in the email message—was accomplished by the recipient's MUA.

The tests in this scenario included an attempt by a fraudulent actor to pose as an originator of the email. This attempt failed due to the use of DNSSEC and DANE. The receiving MUA could detect that the fraudulent email was signed using a different certificate by using a third-party tool that uses the DNS to obtain all necessary certificates. This tool was used to associate an end entity certificate or public key stored in the DNS (using the SMIMEA RR type) with the associated email address.

Future Build Considerations

Both public sector and private sector enterprises depend heavily on web-based technology other than email for e-commerce and other public-facing applications. Fraudulent websites pose at least as great a security and privacy problem as fraudulent email. Further, as email becomes a more difficult medium for malicious entities to use as a penetration vector, other web-based media will be more intensively exploited. Already, emerging communications trends appear to be replacing email exchanges among individuals with social media (e.g., Facebook, LinkedIn, Twitter, WhatsApp). Therefore, an extension of the current project that focuses on the use of improved DNSSEC applications, such as DANE for web applications other than email, may be justified.

Additionally, the test scenarios did not include the Exchange for Office 365 mail servers to demonstrate Scenario 1. Future builds might be considered to demonstrate this capability.

Finally, utilities are currently under development that would provide improved support for SMIMEA and improved system notification of failed DNSSEC signature validation events. Future builds might be considered to demonstrate these capabilities, as well.

ITL Bulletin Publisher: Elizabeth B. Lennon
Information Technology Laboratory
National Institute of Standards and Technology
elizabeth.lennon@nist.gov

Disclaimer: Any mention of commercial products or reference to commercial organizations is for information only; it does not imply recommendation or endorsement by NIST nor does it imply that the products mentioned are necessarily the best available for the purpose.