ITL BULLETIN FOR OCTOBER 2016

MAKING EMAIL TRUSTWORTHY

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

Introduction

Email is a core application of computer networking and has been since the early days of Internet development. In those early days, networking was a collegial, research-oriented enterprise. Security was not a consideration. The past forty years have seen diversity in applications deployed on the Internet, and worldwide adoption of email by research organizations, governments, militaries, businesses, and individuals. At the same time, there has been an associated increase in Internet-based criminal and nuisance threats.

The Internet's underlying core email protocol, Simple Mail Transport Protocol (SMTP), was adopted in 1982 and is still deployed and operated today. However, this protocol is susceptible to a wide range of attacks, including man-in-the-middle content modification and content surveillance. The basic standards have been modified and augmented over the years with adaptations that mitigate some of these threats. With spoofing protection, integrity protection, encryption and authentication, properly implemented email systems can be regarded as sufficiently secure for government, financial, and medical communications.

NIST has been active in the development of email security guidelines for many years. For example, NIST Special Publication (SP) 800-45 Version 2, *Guidelines on Electronic Mail Security*, was published in February 2007. The document provides recommendations for securing the environments around enterprise mail servers and mail clients to help prevent security compromises of servers and workstations.

The recently released NIST SP 800-177, *Trustworthy Email*, complements NIST SP 800-45 by providing up-to-date recommendations and guidance for email digital signatures and encryption via Secure/Multipurpose Internet Mail Extensions (S/MIME). The document provides recommendations regarding aspects of email system deployment and configuration, including ways to help protect against unwanted email (spam).

[1] Larry Feldman and Greg Witte are NIST Associates from G2, Inc.

The major goal of the document is to provide guidelines on how to combat possible threats before a user opens an email. This guidance applies to federal IT systems and will also be useful for other organizations, including small and medium-sized businesses.

Security Threats to an Email Service

NIST SP 800-177 starts with a discussion of the core email protocols and the main components such as Mail Transport Agents (MTA), Mail Submission Agents (MSA), Mail Delivery Agent (MDA), and Mail User Agents (MUA). It discusses security threats to canonical functions of email service applications, including: message submission (at the sender's end), message transmission (transfer), and message delivery (at the recipient's end).

The publication classifies threats to the core email infrastructure functions as follows:

- **Integrity-related threats to the email system,** which could result in unauthorized access to an enterprises' email system, or spoofed email used to initiate an attack;
- **Confidentiality-related threats to email,** which could result in unauthorized disclosure of sensitive information; or
- **Availability-related threats to the email system**, which could prevent end users from being able to send or receive email.

The document recommends mitigations for the following integrity-related threats to email system and security:

- Unauthorized email senders within an organization's Internet Protocol (IP) address block;
- Unauthorized email receivers within an organization's IP address block;
- Unauthorized email messages from a valid Domain Name System (DNS) domain;
- Tampering/modification of email content from a valid DNS domain;
- DNS Cache Poisoning; and
- Phishing and spear phishing.

Authenticating a Sending Domain and Individual Mail Messages

NIST SP 800-177 discusses the protocols and techniques that a sending domain can use to authenticate valid email senders for a given domain. This includes protocols such as Sender Policy Framework (SPF), DomainKeys Identified Mail (DKIM), and Domain-based Message and Reporting Conformance (DMARC).

SPF uses DNS to allow domain owners to create records that associate the envelope-From: address domain name with one or more IP address blocks used by authorized MSAs. A receiving MTA must check an SPF TXT record in the DNS to confirm the sender of a message to the listed approved sending MTA. If

the sender is not authorized to transmit email messages for the domain listed in the envelope-From: address, a message may be flagged, quarantined, or rejected.

The DKIM protocol allows a sending MTA to digitally sign selected headers and the body of the message with an RSA signature and include the signature in a DKIM header that is attached to the message prior to transmission. The DKIM signature header field includes a selector that the receiver can use to retrieve a public key from a DNS record to validate the DKIM signature over the message. Validating the signature helps to assure the receiver that the message has not been modified in transit, other than additional headers added by MTAs en route which are ignored during the validation. Use of DKIM also ties the email message to the domain storing the public key, regardless of the From: address (which could be different).

Deploying SPF and DKIM may help curb illicit activity against a sending domain, but the sender gets no indication of the extent of the beneficial (or otherwise) effects of these policies. Sending domain owners may choose to construct pairwise agreements with selected recipients to manually gather feedback, but this is not a scalable solution. The Domain-based Message Authentication, Reporting and Conformance protocol (DMARC) institutes such a feedback mechanism. DMARC provides a way to publish policy statements regarding actions the receiver domain could take (e.g., deliver, quarantine, reject) when messages fail both SPF and DKIM checks. Such a failure might indicate an individual or bulk attack scenario. Email receivers can return DMARC aggregate and/or failure reports of email dispositions to the domain owner, who can review the results, determine the proportionate effectiveness of their SPF and DKIM policies, and potentially refine the policies.

Protecting Email Confidentiality

Mail messages in clear text could be intercepted and read by anyone. Email transmission security can be assured by encrypting the traffic along the path. The Transport Layer Security (TLS) protocol protects confidentiality by encrypting bidirectional traffic, thus preventing passive monitoring. TLS relies on public key cryptography and uses X.509 certificates to encapsulate the public key, and the Certificate Authority (CA) system to issue certificates and authenticate the origins of keys.

In recent years, the CA system has become the subject of attack and has been successfully compromised on several occasions. The DNS Authentication of Named Entities (DANE) protocol is designed to overcome problems in the CA system by providing an alternative channel for authenticating public keys using DNS Security Extensions (DNSSEC). As a result, the same trust relationships used to certify IP addresses can be used to certify servers operating on those addresses. NIST SP 800-177 describes the mechanisms that combine to improve the assurance of email transmission security.

Encryption at the transport layer gives assurance of the integrity of data in transit, but senders and receivers who want end-to-end assurance—i.e., mailbox to mailbox—of confidentiality have two alternative mechanisms for achieving this goal. S/MIME and Open Pretty Good Privacy (OpenPGP) are both capable of digitally signing (for authentication) and encrypting (for confidentiality) messages. The S/MIME protocol is deployed to sign and/or encrypt message contents, using keys stored as X.509 certificates and a Public Key Infrastructure (PKI). OpenPGP uses a different certificate and a Web-of-Trust model for authentication of identities. Both of these protocols have the issue of trustworthy certificate publication and discovery. These certificates can be published through the DNS by a different implementation of the DANE mechanism for S/MIME and OpenPGP. NIST SP 800-177 discusses S/MIME and OpenPGP, with their strengthening by DANE authentication.

Reducing Unsolicited Bulk Email

Some unsolicited email is from legitimate marketing firms, but its use may sometimes be a nuisance to recipients and/or can also lead to increased resource usage in the enterprise. Unsolicited bulk email (UBE) can fill user inbox storage, congest network bandwidth, and consume end users' time as they sort through and delete unwanted email. However, some UBE may rise to the level of legitimate threat to the organization in the form of fraud, illegal activity, or the distribution of malware.

NIST SP 800-177 describes techniques, such as approved/non-approved sender lists, domain-based authentication techniques, and content filtering, that an email administrator can use to reduce the amount of UBE delivered to end users' inboxes. Enterprises can use one or multiple technologies to provide a layered defense against UBE since no solution is completely effective against all UBE. Administrators should consider using a combination of tools for processing incoming and outgoing email.

End User Email Security

In terms of the canonical email processing architecture, the client may play the role of the MUA. The document discusses client interactions and constraints through protocols such as Post Office Protocol Version 3 (POP3), Internet Message Access Protocol (IMAP), and SMTP. An end user usually interacts with a mailbox using one of two classes of clients—webmail clients and stand-alone clients—which communicate with the mailbox in different ways. For example, browser-based clients often use HTTPS (Hypertext Transfer Protocol Secure), while desktop or mobile client applications may use IMAP or POP3 for receiving and SMTP for sending. The document examines the security of both classes of clients.

Conclusion

NIST SP 800-177 offers recommendations and guidelines for enhancing trust in email, including recommendations for supporting core SMTP based on DNS security, email transmission security, and

email content security. This includes providing guidance to help meet the Department of Homeland Security (DHS) Federal Network Resilience (FNR) Division recommendation to use domain-based authentication techniques for email as part of the FY16 FISMA metrics for anti-phishing defenses.

Using the new publication as a reference, the current National Cybersecurity Center of Excellence (NCCoE) project "DNS-Based Secured Email" is building a proof-of-concept security platform—composed of commercial off-the-shelf (COTS) components—that demonstrates trustworthy mail server-to-mail server email exchanges across organizational boundaries.

Next steps for email trustworthiness include continued research and development into the deployment and improvement of the technologies described in NIST SP 800-177, based on lessons learned. Automated and opportunistic technologies like these will continue to improve the way the community secures email.

Additional Resources

NIST High Assurance Domain Website –
https://www.nist.gov/programs-projects/high-assurance-domains

National Cybersecurity Center of Excellence (NCCoE) Project: *DNS-Based Secured Email* –
https://nccoe.nist.gov/projects/building_blocks/secured_email

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