NIST SPECIAL PUBLICATION 1800-6B Domain Name System-Based Electronic Mail Security Volume B: Approach, Architecture, and Security Characteristics 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 NIST SP 1800-6B: Domain Name System-Based Electronic Mail Security i This publication is available free of charge from: https://doi.org/10.6028/NIST.SP.1800-6. DISCLAIMER Certain commercial entities, equipment, or materials may be identified in this document in order to describe an experimental procedure or concept adequately. Such identification is not intended to imply recommendation or endorsement by NIST or NCCoE, nor is it intended to imply that the entities, materials, or equipment are necessarily the best available for the purpose. National Institute of Standards and Technology Special Publication 1800-6B, Natl. Inst. Stand. Technol. Spec. Publ. 1800-6B, 72 pages, (January 2018), CODEN: NSPUE2 All comments are subject to release under the Freedom of Information Act (FOIA). National Cybersecurity Center of Excellence National Institute of Standards and Technology 100 Bureau Drive Mailstop 2002 Gaithersburg, MD 20899 Email: nccoe@nist.gov NIST SP 1800-6B: Domain Name System-Based Electronic Mail Security ii This publication is available free of charge from: https://doi.org/10.6028/NIST.SP.1800-6. NATIONAL CYBERSECURITY CENTER OF EXCELLENCE 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 issues. This public-private partnership enables the creation of practical cybersecurity solutions for specific industries, as well as for broad, cross-sector technology challenges. Through consortia under Cooperative Research and Development Agreements (CRADAs), including technology partners—from Fortune 50 market leaders to smaller companies specializing in IT security—the NCCoE applies standards and best practices to develop modular, easily adaptable example cybersecurity solutions using commercially available technology. The NCCoE documents these example solutions in the NIST Special Publication 1800 series, which maps capabilities to the NIST Cyber Security Framework and details the steps needed for another entity to recreate the example solution. The NCCoE was established in 2012 by NIST in partnership with the State of Maryland and Montgomery County, Md. To learn more about the NCCoE, visit https://nccoe.nist.gov. To learn more about NIST, visit https://www.nist.gov. NIST CYBERSECURITY PRACTICE GUIDES NIST Cybersecurity Practice Guides (Special Publication Series 1800) target specific cybersecurity challenges in the public and private sectors. They are practical, user-friendly guides that facilitate the adoption of standards-based approaches to cybersecurity. They show members of the information security community how to implement example solutions that help them align more easily with relevant standards and best practices and provide users with the materials lists, configuration files, and other information they need to implement a similar approach. The documents in this series describe example implementations of cybersecurity practices that businesses and other organizations may voluntarily adopt. These documents do not describe regulations or mandatory practices, nor do they carry statutory authority. ABSTRACT This document proposes a reference guide on how to architect, install, and configure a security platform for trustworthy email exchanges across organizational boundaries. The project includes reliable authentication of mail servers, digitally signing and encrypting email, and binding cryptographic key certificates to sources and servers. The example solutions and architectures presented here are based upon standards-based and commercially available products. The example solutions presented here can be used by any organization implementing Domain Name System-based electronic mail security. KEYWORDS authentication; data integrity; digital signature; domain name system; electronic mail; encryption; internet addresses; internet protocols; named entities; privacy NIST SP 1800-6B: Domain Name System-Based Electronic Mail Security iii This publication is available free of charge from: https://doi.org/10.6028/NIST.SP.1800-6. ACKNOWLEDGMENTS We are grateful to the following individuals for their generous contributions of expertise and time. Name Organization Bud Bruegger Fraunhofer IAO Victoria Risk Internet Systems Consortium Eddy Winstead Internet Systems Consortium Paul Fox Microsoft Corporation Janet Jones Microsoft Corporation Nate Lesser National Cybersecurity Center of Excellence Karen Waltermire National Cybersecurity Center of Excellence Doug Montgomery NIST ITL Advanced Networks Technologies Division Ralph Dolmans NLnet Labs Benno Overeinder NLnet Labs Joe Gersch Secure64 Saksham Manchanda Secure64 NIST SP 1800-6B: Domain Name System-Based Electronic Mail Security iv This publication is available free of charge from: https://doi.org/10.6028/NIST.SP.1800-6. The Technology Partners/Collaborators who participated in this build submitted their capabilities in response to a notice in the Federal Register. Respondents with relevant capabilities or product components were invited to sign a Cooperative Research and Development Agreement (CRADA) with NIST, allowing them to participate in a consortium to build this example solution. We worked with: Technology Partner/Collaborator Build Involvement Fraunhofer IAO Configuration of DNS Services products and Mail Transfer Agent Internet Systems Consortium DNS Services software Microsoft Corporation Mail User Agent, Mail Transfer Agent, and DNS Services products NLNet Laboratories DNS Services products and configuration of Mail Transfer Agent Secure64 DNS Services and Mail User Agent products and configuration of Mail User Agent and Mail Transfer Agent NIST SP 1800-6B: Domain Name System-Based Electronic Mail Security v This publication is available free of charge from: https://doi.org/10.6028/NIST.SP.1800-6. Contents 1 Summary ............................................................................................1 1.1 Challenge....................................................................................................................... 2 1.2 Solution ......................................................................................................................... 3 1.3 Benefits.......................................................................................................................... 4 2 How to Use This Guide........................................................................5 2.1 Typographical Conventions........................................................................................... 6 3 Approach............................................................................................7 3.1 Audience........................................................................................................................ 9 3.2 Scope ............................................................................................................................. 9 3.3 Assumptions................................................................................................................ 10 3.4 Risk Assessment .......................................................................................................... 11 3.5 Technologies................................................................................................................ 32 4 Architecture...................................................................................... 35 4.1 Usage Scenarios Supported......................................................................................... 35 4.2 Architectural Overview ............................................................................................... 37 5 Outcome .......................................................................................... 45 5.1 The User’s Experience ................................................................................................. 46 5.2 The System Administrator’s Experience ..................................................................... 50 6 Security Characteristic Analysis......................................................... 51 6.1 Assumptions and Limitations...................................................................................... 51 6.2 Build Testing ................................................................................................................ 51 6.3 Scenarios and Findings................................................................................................ 57 7 Future Build Considerations.............................................................. 59 Appendix A List of Acronyms................................................................. 60 Appendix B References......................................................................... 63 NIST SP 1800-6B: Domain Name System-Based Electronic Mail Security vi This publication is available free of charge from: https://doi.org/10.6028/NIST.SP.1800-6. Appendix C Project Mapping to the Framework Core and Informative References........................................................................................ 67 List of Figures Figure 3.1 DNS-Based Email Security Collaborator Contributions ..........................................33 Figure 4.1 DNS-Based Email Security Deployment Diagram ...................................................38 Figure 4.2 DNS-Based Email Security Test Set-up...................................................................39 Figure 4.3 Fraudulent DNS Address Spoofing Configurations................................................. 41 Figure 4.4 Man-In-The-Middle Event Configurations .............................................................42 List of Tables Table 4.1 Client Systems........................................................................................................43 Table 4.2 Mail Transfer Agents..............................................................................................44 Table 6.1 Tests Performed.....................................................................................................53 Table C.1 PROTECT (PR).........................................................................................................67 Table C.2 DETECT (DE) ...........................................................................................................70 Table C.3 RESPOND (RS) ........................................................................................................71 NIST SP 1800-6B: Domain Name System-Based Electronic Mail Security 1 This publication is available free of charge from: https://doi.org/10.6028/NIST.SP.1800-6. 1 Summary This National Institute of Standards and Technology (NIST) Cybersecurity Practice Guide addresses the challenge of providing digital signature technologies to provide authentication and integrity protection for electronic mail (email) on an end-to-end basis, and confidentiality protection for email in transit between organizations. It implements and follows recommendations of NIST Special Publication 800- 177 (SP 800-177), Trustworthy Email. Detailed protocol information and implementation details are provided in SP 800-177. Domain Name System1 protection features are consistent with SP 800-81-2, Secure Domain Name System (DNS) Deployment Guide. The NIST Special Publication 1800-6 series of documents contain: ν rationale for and descriptions of a Domain Name System-based (DNS-based) email security platform that permits trustworthy email exchanges across organizational boundaries and ν a series of How-To Guides, including instructions for installation and configuration of the necessary services, that show system administrators and security engineers how to achieve similar outcomes The solutions and architectures presented are built upon standards-based, commercially-available products. These solutions can be used by any organization deploying email services that is willing to implement certificate-based cryptographic key management and DNS Security Extensions (DNSSEC)2 . Interoperable solutions are provided that are available from different types of sources (e.g., both commercial and open source products) and function in different operating systems environments. This summary section describes the challenge addressed by this Volume B (Approach, Architecture, and Security Characteristics); describes the solution demonstrated to address the challenge; explains the benefits of the demonstrated solution; lists the technology partners that participated in building, demonstrating, and documenting the solution; and explains how to provide feedback on this guide. Section 2, How to Use This Guide explains how each volume of the guide may be used by business decision makers, program managers, and Information Technology (IT) professionals such as systems administrators; and Section 3, Approach provides a more detailed treatment of the scope of the project, describes the assumptions on which security platform development was based, describes the risk assessment that informed platform development, and describes the technologies and components that were provided by industry collaborators to enable platform development. Section 4, Architecture describes the usage scenarios supported by project security platforms, including Cybersecurity 1 Request for Comments (RFC) 1591, Domain Name System Structure and Delegation 2 RFC 4033, DNS Security Introduction and Requirements NIST SP 1800-6B: Domain Name System-Based Electronic Mail Security 2 This publication is available free of charge from: https://doi.org/10.6028/NIST.SP.1800-6. Framework3 functions supported by each collaborator-contributed component. Section 5, Outcome describes any changes in users’ mail processing experience imposed by the additional security functionality, and summarizes changes to systems administrators’ experiences with respect to integrating the new capabilities into their systems and in systems operations and maintenance. Section 6, Security Characteristic Analysis summarizes the test sequences that were employed to demonstrate security platform services, the Cybersecurity Framework functions to which each test sequence is relevant, the NIST SP 800-53-4 controls that applied to the functions being demonstrated, and an overview of platform performance in each of the two application scenarios demonstrated. Section 7, Future Build Considerations is a brief treatment of other applications that might be explored in the future in demonstrating the advantages of broader DNS security adoption. Appendices are provided for acronyms, references, and a mapping of this project to the Cybersecurity Framework Core4 and informative security references cited in the Cybersecurity Framework Core. 1.1 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 are heavily reliant on email exchanges and need to protect the confidentiality of business information, the integrity of transactions, and privacy of individuals. Cryptographic services are used to authenticate the source of email messages, protect against undetected unauthorized alteration of messages in transit, and maintain message confidentiality. Efficiency and policies support reliance on mail servers to provide cryptographic protection for email rather than on end-to-end security operated by individual users. However, organizations need to protect their server-based email security mechanisms against intrusion and manin-the-middle attacks during automated cryptographic service negotiation. In the absence of an appropriate combination of 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. If other content in a fraudulent message successfully motivates the user to click on the link or the user’s system is configured to automatically follow some links or download content other than text, the malware will infect the user’s system. Inclusion of links to malware is a major factor in most confirmed data breaches. Consequences of such breaches can range from exposing sensitive or private information, to enabling fraudulent activity by the attacker posing as the victimized user, to disabling or destroying the user’s system—or that of the user’s parent organization. Beyond 3 Framework for Improving Critical Infrastructure Cybersecurity, Version 1.0, National Institute of Standards and Technology, February 12, 2014, https://www.nist.gov/cyberframework/upload/cybersecurity-framework021214.pdf 4 https://www.nist.gov/cyberframework/ NIST SP 1800-6B: Domain Name System-Based Electronic Mail Security 3 This publication is available free of charge from: https://doi.org/10.6028/NIST.SP.1800-6. avoidance of negative consequences to users, improved email security can also serve as a marketing discriminator for email service providers. Implementation of DNSSEC and DNS-Based Authentication of Named Entities (DANE)5 has been impeded in the past by a shortage of easily used software libraries and by the fact that most available email applications of the protocols respond to DNSSEC failures by terminating the delivery attempt, often failing to alert the mail server that failure to deliver is based on a DNSSEC issue. The consequence of the first impediment is that, unless forced by policy to do so, IT organizations defer DNSSEC/DANE implementation pending availability of more mature software libraries. The consequence of the second is that, when DNSSEC and DANE are turned on, mail servers experience severe service degradation or crashes due to large numbers of retransmission attempts. (Note that this problem is experienced with mail servers, not DNS servers; DNS servers can handle the load.) 1.2 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 comprising the security platform include client mail user agents (MUAs)6 , DNS servers (authoritative and caching/recursive)7 , mail transfer agents (MTAs)8 , and X.509 cryptographic key certificate sources (components and services). 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 certificates9 for mail servers and end users to support Transport Layer Security (TLS)10 and Secure/Multipurpose 5 RFC 6698, The DNS-Based Authentication of Named Entities (DANE) Transport Layer Security Protocol: TLSA 6 According to NIST SP 800-177, an MUA is a software component (or web interface) that allows an end user to compose and send messages to one or more recipients. An MUA transmits new messages to a server for further processing (either final delivery or transfer to another server). 7 According to Section 3.2 of SP 800-177, there are two main types of name servers: authoritative name servers and caching name servers. The term authoritative is with respect to a zone. If a name server is an authoritative source for DNS resource records for a particular zone (or zones) of DNS addresses, it is called an authoritative name server for that zone (or zones). An authoritative name server for a zone provides responses to name resolution queries for resources for that zone, using the records in its own zone file. A caching name server (also called a resolving/recursive name server), by contrast, provides responses either through a series of queries to authoritative name servers in the hierarchy of domains found in the name resolution query or from a cache of responses built by using previous queries. 8 Also, according to SP 800-177, mail is transmitted, in a “store and forward” fashion, across networks via MTAs. MTAs communicate using the Simple Mail Transfer Protocol (SMTP) described below and act as both client and server, depending on the situation. 9 RFC 5280, Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile 10 RFC 5246, The Transport Layer Security (TLS) Protocol Version 1.2 NIST SP 1800-6B: Domain Name System-Based Electronic Mail Security 4 This publication is available free of charge from: https://doi.org/10.6028/NIST.SP.1800-6. Internet Mail Extensions (S/MIME)11. This project focused on Simple Mail Transfer Protocol (SMTP)12 over TLS and S/MIME. This project demonstrated a security platform, consistent with SP 800-177, that provides trustworthy email exchanges across organizational boundaries. The project included authentication of mail servers, digitally signing and encrypting email13, and binding cryptographic key certificates to the servers. The software library issue was addressed in SP 1800-6C 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. 1.3 Benefits Sectors across industries, as well as the federal government, are concerned about email security and the use of email as an attack vector.14 Both public and private sector business operations are heavily reliant on email exchanges. The need to protect the integrity of transactions containing financial and other proprietary information and to protect the privacy of employees and clients are among the factors that motivate organizations to secure their email. Whether the service desired is authentication of the source of an email message, assurance that the message has not been altered by an unauthorized party, or message confidentiality, cryptographic functions are usually employed. Economies of scale and a need for uniform implementation drive most enterprises to rely on mail servers to provide security to the members of an enterprise rather than security implemented and operated by individual users. Many server-based email security mechanisms are vulnerable to attacks involving: ♣ faked or fraudulent digital certificates ♣ otherwise invalid certificates ♣ failure to perform authentication process for connection Even if there are protections in place, some attacks have been able to subvert email communication by attacking the underlying support protocols such as DNS. Attackers can spoof DNS responses to redirect email servers and alter email delivery. DNSSEC was developed to prevent this. DNSSEC protects against 11 RFC 5751, Secure/Multipurpose Internet Mail Extensions (S/MIME) Version 3.2 Message Specification 12 RFC 5321, Simple Mail Transfer Protocol 13 Cryptographic protection, while voluntary for the private sector, has for a number of applications been made mandatory for federal government agencies (see Managing Information as a Strategic Resource, Office of Management and Budget (OMB) Circular A-130). 14 “How Cybercrime Exploits Digital Certificates,” Infosec Institute, General Security, July 28, 2014, http://resources.infosecinstitute.com/cybercrime-exploits-digital-certificates NIST SP 1800-6B: Domain Name System-Based Electronic Mail Security 5 This publication is available free of charge from: https://doi.org/10.6028/NIST.SP.1800-6. unauthorized modifications to network management information and host IP addresses. DNSSEC can also be used to provide an alternative publication and trust infrastructure for service certificates using DANE resource records. The business value of the security platform that results from this project includes improved privacy and security protections for users’ communication, as well as improved management of DNS and email security operations. Addressing the software library and message retransmission issues, respectively, reduces the difficulty and cost of installing and maintaining DNSSEC and DANE. Mitigating the major cause of system errors resulting from faulty deployment of DNSSEC and DANE will encourage use of capabilities already present in many email systems. Demonstration and publication of these improvements encourages wider implementation of the protocols that provide Internet users with confidence that email has been protected and reaches the intended receiver in a secure manner. The demonstrated platform addresses three of the five Framework Core Functions and many requirements of relevant security standards and guidelines. Implementation of the platform will be increasingly important as a market discriminator as public awareness of email security and privacy issues grows. 2 How to Use This Guide This NIST Cybersecurity Practice Guide demonstrates a standards-based reference design and provides users with the information they need to replicate this proof-of-concept security platform that demonstrates trustworthy email exchanges across organizational boundaries. This reference design is modular and can be deployed in whole or in parts. This guide contains three volumes: ♣ NIST SP 1800-6A: Executive Summary ♣ NIST SP 1800-6B: Approach, Architecture, and Security Characteristics – what we built and why (you are here) ♣ NIST SP 1800-6C: How-To Guides – instructions for building the example solution Depending on your role in your organization, you might use this guide in different ways: Business decision makers, including chief security and technology officers will be interested in the Executive Summary (NIST SP 1800-6A), which describes the: ♣ challenges enterprises may face in implementing best practices and standards to strengthen their email systems ♣ example solution built at the NCCoE ♣ benefits of adopting the example solution Technology or security program managers who are concerned with how to identify, understand, assess, and mitigate risk will be interested in this part of the guide, NIST SP 1800-6B, which describes what we did and why. The following sections will be of particular interest: NIST SP 1800-6B: Domain Name System-Based Electronic Mail Security 6 This publication is available free of charge from: https://doi.org/10.6028/NIST.SP.1800-6. ♣ Section 3.4.3, Risk, provides a description of the risk analysis we performed ♣ Section 3.4.4, Cybersecurity Framework Functions, Categories, and Subcategories Addressed by the Project, maps the security characteristics of this example solution to cybersecurity standards and best practices You might share the Executive Summary, NIST SP 1800-6A, with your leadership team members to help them understand the importance of adopting standards-based email security solutions. IT professionals who want to implement an approach like this will find the whole practice guide useful. You can use the How-To portion of the guide, NIST SP 1800-6C, to replicate all or parts of the build created in our lab. The How-To guide provides specific product installation, configuration, and integration instructions for implementing the example solution. We do not recreate the product manufacturers’ documentation, which is generally widely available. Rather, we show how we incorporated the products together in our environment to create an example solution. This guide assumes that IT professionals have experience implementing security products within the enterprise. While we have used a suite of commercial products to address this challenge, this guide does not endorse these products. Your organization can adopt this solution or one that adheres to these guidelines in whole, or you can use this guide as a starting point for tailoring and implementing parts of the DNS-based email solution suite described herein. Your organization’s security experts should identify the products that will best integrate with your existing tools and IT system infrastructure. We hope you will seek products that are congruent with applicable standards and best practices. Section 3.5, Technologies, lists the products we used and maps them to the cybersecurity controls provided by this reference solution. A NIST Cybersecurity Practice Guide does not describe “the” solution, but a possible solution. Comments, suggestions, and success stories will help inform and improve future projects. Please contribute your thoughts to dns-email-nccoe@nist.gov. 2.1 Typographical Conventions The following table presents typographic conventions used in this volume. Typeface/ Symbol Meaning Example Italics filenames and pathnames references to documents that are not hyperlinks, new terms, and placeholders For detailed definitions of terms, see the NCCoE Glossary. NIST SP 1800-6B: Domain Name System-Based Electronic Mail Security 7 This publication is available free of charge from: https://doi.org/10.6028/NIST.SP.1800-6. Typeface/ Symbol Meaning Example Bold names of menus, options, command buttons and fields Choose File > Edit. Monospace command-line input, on-screen computer output, sample code examples, status codes mkdir Monospace Bold command-line user input contrasted with computer output service sshd start blue text link to other parts of the document, a web URL, or an email address All publications from NIST’s National Cybersecurity Center of Excellence are available at: https://nccoe.nist.gov/ 3 Approach As stated in Section 1.1, both public and private sector business operations are heavily reliant on email exchanges. They need to protect the integrity of transactions that may include financial and other proprietary information. The privacy of employees and clients is also a factor that motivates organizations to secure their email systems. Security services such as the authentication of the source of an email message, assurance that the message has not been altered by an unauthorized party, and confidentiality of message contents require the use of cryptographic functions. A need for uniform security implementation drives most enterprises to rely on mail servers to provide security to the members of an enterprise rather than rely on end users to implement a security policy on their own. However, most current 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 frequently involve unauthorized parties being able to read or modify supposedly secure information, or to use email as a vector for inserting malware into the enterprise. Improved email security can help protect organizations and individuals against these consequences and also serve as a marketing discriminator for email service providers as well as improve the trustworthiness of enterprise email exchanges. NIST SP 1800-6B: Domain Name System-Based Electronic Mail Security 8 This publication is available free of charge from: https://doi.org/10.6028/NIST.SP.1800-6. Domain Name System Security Extensions for DNS are technical mechanisms employed by domain owners to protect against unauthorized modification to network management information. DANE is a protocol that securely associates domain names with cryptographic certificates and related security information so that clients can better authenticate network services. Despite 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 email may support increased user demand for DNS security. Follow-on projects might include Hypertext Transfer Protocol Secure (HTTPS), the Internet of Things (IoT), Internet Protocol Security (IPsec) keys in DNS, and DNS service discovery. This project demonstrated proof-of-concept security platforms composed of off-the-shelf components that provide trustworthy mail server-to-mail server email exchanges across organizational boundaries. The DANE protocol was used to authenticate servers and certificates in two roles: (1) by binding the X.509 certificates used for TLS to DNSSEC signed names for mail server-to-mail server communication; and (2) by binding the X.509 certificates used for S/MIME to email addresses encoded as DNS names. These bindings support trust in the use of S/MIME certificates in the end-to-end email communication. The resulting platforms encrypt email traffic between servers and allow individual email users to obtain other users’ certificates in order to validate signed email or send encrypted email.15 The project included an email sending policy consistent with a stated privacy policy that can be parsed by receiving servers so that receiving servers can apply the correct security checks. Documentation of the resulting platform includes statements of the security and privacy policies and standards (e.g., Executive Orders, NIST standards and guidelines, Internet Engineering Task Force (IETF) RFCs). This also includes technical specifications for hardware and software, implementation requirements, and a mapping of implementation requirements to the applicable policies, standards, and best practices. The project involved composition of a variety of components that were provided by several different technology providers. Components included MUAs, DNSSEC-capable DNS servers, MTAs, and cryptographic certificate sources. These components were used to generate and host DNSSEC signed zones and TLS-enabled mail services. This project resulted in demonstration of support to MUAs and MTAs by four secure email platforms and this publicly available NIST Cybersecurity Practice Guide that explains how to employ the suite(s) to meet security and privacy requirements. This guide also provides platform documentation necessary to compose a DNS-based email security platform from off-the-shelf components that composed the prototype platforms. 15 S/MIME can do this now, but DANE makes it easier to actually use. NIST SP 1800-6B: Domain Name System-Based Electronic Mail Security 9 This publication is available free of charge from: https://doi.org/10.6028/NIST.SP.1800-6. 3.1 Audience This guide is intended for individuals responsible for implementing security solutions in organizations’ IT support activities. Current IT systems, particularly in the private sector, often lack integrity protection for domain name services and email. The platforms demonstrated by this project and the implementation information provided in these Practice Guides permit integration of DNS and email integrity services and email confidentiality services with minimum changes to existing infrastructure or impact to service operations. The technical components will appeal to system administrators, IT managers, IT security managers, and others directly involved in the secure and safe operation of the business IT networks. 3.2 Scope This project was consistent with NIST SP 800-177 and demonstrated the use of off-the-shelf TLS, DNSSEC, and DANE components to achieve trustworthy email objectives in a manner consistent with NIST SP 800-81-2. 3.2.1 Transport Layer Security (TLS) The project used TLS to protect confidentiality of email messages exchanged between mail servers. TLS relies on public keys stored as X.509 digital certificates. These certificates can be used to authenticate the identity (server, domain or organization) of the certificate owner. 3.2.2 Domain Name System Security Extensions (DNSSEC) The project used DNSSEC to authenticate and protect the integrity of DNS data.16 DNSSEC uses digital signatures over DNS data to prevent an attacker from tampering with or spoofing DNS responses. Mail servers use the DNS to find the destination of email as well as storing other artifacts necessary for email security (see below). 3.2.3 DNS-Based Authentication of Named Entities (DANE) The project used DANE, a protocol that securely associates domain names with cryptographic certificates and related security information so that they cannot be fraudulently modified or replaced to breach security. DNSSEC binds the X.509 certificates used for TLS to DNS. 16 Note that this project addressed validation of X.509 certificates through the signing chain, not only through DANE. NIST SP 1800-6B: Domain Name System-Based Electronic Mail Security 10 This publication is available free of charge from: https://doi.org/10.6028/NIST.SP.1800-6. 3.2.4 Binding X.509 Certificates with DANE The project also used DANE to bind the X.509 certificates used for S/MIME to email addresses encoded as DNS names verified by DNSSEC. 3.2.5 Demonstration of Digital Signature and Encryption of Email The project demonstrated sending encrypted messages between email systems resident in different DNS domains, where the email exchanges between two organizations’ email servers are carried over TLS, and the integrity of TLS key management connections is protected by DANE and DNSSEC. Signed email was sent between a message originator and a receiving party using end user applications (end-toend) in different DNS domains, where the 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. In addition, the project demonstrated that the use of DNSSEC and DANE could block an attempt by a fraudulent mail server to pose as the legitimate mail server for the receiver of the email. 3.2.6 Demonstration of End-to-End Digital Signature of Mail The project’s digital signature demonstration included sending S/MIME signed email between a message originator and a receiving party using end user applications in different DNS domains. The email exchanges between organizations are carried over TLS, the email messages are signed and verified with S/MIME on the end users’ client devices, and the S/MIME certificates are stored in the DNS and protected by DNSSEC. This aspect of the project also demonstrated that use of DANE could block an attempt by a fraudulent actor to pose as the email originator. 3.3 Assumptions The following assumptions exist for this project. 3.3.1 Security and Performance The email platforms and DNS services demonstrated provided email integrity and confidentiality protection. An underlying assumption was that the benefits of using the demonstrated platforms outweighed any additional performance risks that may be introduced. The security of existing systems and networks was out of scope for this project. A key assumption was that all potential adopters of one of the demonstrated builds, or any of their components, already have in place some degree of network security. Therefore, we focused on what potential new system vulnerabilities were being introduced to end users if they implement this solution. The goal of this solution was to not introduce additional vulnerabilities into existing systems, but there is always inherent risk when adding systems and adding new features into an existing system. NIST SP 1800-6B: Domain Name System-Based Electronic Mail Security 11 This publication is available free of charge from: https://doi.org/10.6028/NIST.SP.1800-6. 3.3.2 Modularity This assumption was based on one of the NCCoE core operating tenets. It is reasonably assumed that organizations already have mail client and server systems in place. Our philosophy is that a combination of certain components or a single component can improve email security for an organization; they may not need to remove or replace most existing infrastructure. This guide provides a complete top-tobottom solution and is also intended to provide various options based on need. 3.3.3 Technical Implementation This practice guide is written from a “how-to” perspective, and its foremost purpose is to provide details on how to install, configure, and integrate the components. The NCCoE assumes that an organization has the technical resources to implement all or parts of the build, or has access to companies that can perform the implementation on its behalf. 3.3.4 Operating System and Virtual Machine Environments This project was conducted primarily in a VMware vCenter server version 6.0.0 Build 3018523 virtual machine environment. It is assumed that user organizations will be able to install the demonstrated applications in cloud-hosted virtual machines (VMs), local virtual machine or local native server client environments. This project uses Centos 7, Windows Server 2012R2, and Windows 10 operating systems. Operating systems were chosen based on the requirements of the software. This project assumes, and is dependent upon, the availability of off-the shelf information security technology. Specific products and expertise on which the project is dependent include those for MUAs, MTAs, DNS servers (authoritative and recursive) and X.509 certificate utilities. 3.4 Risk Assessment According to NIST SP 800-30, Risk Management Guide for Information Technology Systems, “Risk is the net negative impact of the exercise of a vulnerability, considering both the probability and the impact of occurrence. Risk management is the process of identifying risk, assessing risk, and taking steps to reduce risk to an acceptable level.” The NCCoE recommends that any discussion of risk management, particularly at the enterprise level, begin with a comprehensive review of the Framework for Improving Critical Infrastructure Cybersecurity17 (Cybersecurity Framework) and NIST SP 800-39, Managing Information Security Risk: Organization, Mission, and Information System View. The risk management 17 Framework for Improving Critical Infrastructure Cybersecurity, Version 1.0, National Institute of Standards and Technology, February 12, 2014. https://www.nist.gov/sites/default/files/documents/cyberframework/cybersecurity-framework-021214.pdf NIST SP 1800-6B: Domain Name System-Based Electronic Mail Security 12 This publication is available free of charge from: https://doi.org/10.6028/NIST.SP.1800-6. framework (RMF) and its associated references for identified security functions provide a baseline for organizing and relating to organizational objectives of: ♣ the risks to email and the networks it transits ♣ the security requirements to be met in order for the security platform to reduce these risks While this guide does not present a full risk assessment, it does highlight the broad categories of threats and vulnerabilities associated with email. 3.4.1 Threats Below are common threats associated with email: ♣ use of email as a vehicle for introducing malware ♣ use of email as a delivery mechanism for social engineering attacks ♣ theft or destruction of data communicated by email and/or its attachments due to loss or unauthorized/unintentional disposal of messages ♣ unauthorized access to email that results in a loss of privacy ♣ unauthorized modification of information communicated by email ♣ malicious fraudulent creation of messages or attachments attributed to third parties ♣ redirection or duplication of message to other than the intended recipient 3.4.2 Vulnerabilities Vulnerabilities are commonly associated with mail client applications, mail transfer applications, and network applications that are employed in creation, delivery, and reading of email. However, vulnerabilities can be exploited at all levels in the information stack. For up-to-date information regarding vulnerabilities, this guide recommends that security professionals leverage the National Vulnerability Database (NVD). The NVD is the U.S. government repository of standards-based vulnerability management data [https://nvd.nist.gov]. 3.4.2.1 Client System Vulnerabilities Organizations are getting better at protecting network perimeters, and companies with mature security programs usually allow only certain ports through the firewall and harden internet-accessible servers to minimize the attack surface. As a result, attackers are paying closer attention to client-side vulnerabilities on internal workstations. These client-side vulnerabilities often are as simple as unpatched software on a desktop or laptop. Most client systems run at least one operating system and quite a few applications. Listing specific vulnerabilities for each is beyond the scope of this guide, but a current list of vulnerabilities and information regarding patches are available from NIST’s NVD referenced above. Depending on the nature of a vulnerable application, an attacker may exploit it using NIST SP 1800-6B: Domain Name System-Based Electronic Mail Security 13 This publication is available free of charge from: https://doi.org/10.6028/NIST.SP.1800-6. a specially crafted email attachment or by convincing the user to visit a malicious Web site. Web browsers are common targets. Other attractive targets include Adobe Acrobat18, Macromedia Flash19, QuickTime20, and Java Runtime Environment21. 3.4.2.2 Mail Server Vulnerabilities Mail servers have many of the same vulnerabilities as client systems, but we also need to be aware of protocol-based vulnerabilities involving access to valid lists of email addresses, vulnerabilities to relay exploits for malware insertion, vulnerabilities to email header disclosures, and vulnerabilities to viruses and worms. In the case of SMTP, one way that attackers have in the past verified whether email accounts exist on a server is simply to telnet to the server on port 25 and run the VRFY command. The VRFY command makes a server check whether a specific user ID exists. Spammers often automate this method to perform a directory harvest attack, which is a way of gleaning valid email addresses from a server or domain for hackers to use. Scripting this attack can test thousands of email address combinations. The SMTP command EXPN may allow attackers to verify what mailing lists exist on a server. Yet another way to capture valid email addresses is to use applications such as theHarvester to glean addresses via Google and other search engines. In such environments, the best solution for preventing this type of email account enumeration depends on whether you need to enable commands like SMTP’s VRFY and EXPN. In general, it is important to ensure that company email addresses are not posted on the web. Protocols like SMTP relay let users send emails through external servers. Open email relays are not the problem they used to be, but they can still be sources of vulnerabilities. Spammers and hackers can use an email server to send spam or malware through email under the guise of the unsuspecting open-relay owner. In the case of email header disclosures, email servers configured with typical defaults may be vulnerable to divulging information such as internal Internet Protocol (IP) addresses of email clients, software versions of client and email servers along with their vulnerabilities, or host names that can divulge network naming conventions. Email systems are regularly targeted by malware such as viruses and worms. It is necessary to verify that mail servers’ antivirus software is actually working. As in the case of client system vulnerabilities, 18 See https://www.cvedetails.com/vulnerability-list/vendor\_id-53/product\_id-497/Adobe-Acrobat-Reader.html. 19 See https://www.cvedetails.com/vulnerability-list/vendor\_id-73/product\_id-1950/version\_id-8545/MacromediaFlash-Player-6.0.29.0.html. 20 See https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2015-7117. 21 See https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2015-4903. NIST SP 1800-6B: Domain Name System-Based Electronic Mail Security 14 This publication is available free of charge from: https://doi.org/10.6028/NIST.SP.1800-6. NIST’s NVD (https://nvd.nist.gov) is a frequently updated source of vulnerabilities that affect mail servers.