BUILDING BLOCK

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

NCCoE NATIONAL CYBERSECURITY CENTER OF EXCELLENCE

DNS-BASED EMAIL SECURITY

The National Cybersecurity Center of Excellence (NCCoE) addressed the challenge of securing email transactions through collaboration with members of the IT community, including vendors of cybersecurity solutions. The example solution is detailed in NIST Cybersecurity Practice Guide SP 1800-6, *Domain Name Systems-Based Electronic Mail Security*. The NCCoE solution is not the only one available in the fast-moving cybersecurity technology market. Please contact us at dns-email-nccoe@nist.gov with suggestions and comments.

CHALLENGE

Email has become the dominant method of electronic communication for both private and public sector organizations, fueled by low costs and fast delivery. However, typical cryptographic implementations often leave email transactions vulnerable to attack. Unauthorized parties can use email to gain access to enterprise systems or information, insert malware into a system, or alter the contents of a message. While protocols such as Domain Name System Security Extension (DNSSEC), Transport Layer Security (TLS), and Secure/Multipurpose Internet Mail Extensions (S/MIME) are capable of providing the necessary security protections, the lack of instructions and resource guides to software libraries have limited their adoption.

SOLUTION

The NCCoE has produced a proof of concept security platform that demonstrates trustworthy email exchanges across organizational boundaries. The example solution uses the Domain Name System Security Extension (DNSSEC) protocol to authenticate server addresses and certificates used for Transport Layer Security (TLS) to DNS names. 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 development of this example solution is documented in NIST Cybersecurity Practice Guide 1800-6: *Domain Name Systems-Based Electronic Mail Security*. Organizations can use some or all of the guide to implement the solution in their own environment using NIST and industry standards. Commercial and open source standards-based products, such as the ones used in this example, are readily available and interoperable with commonly used information technology infrastructure and investments.

BENEFITS

The example solution described in the guide has the following benefits:

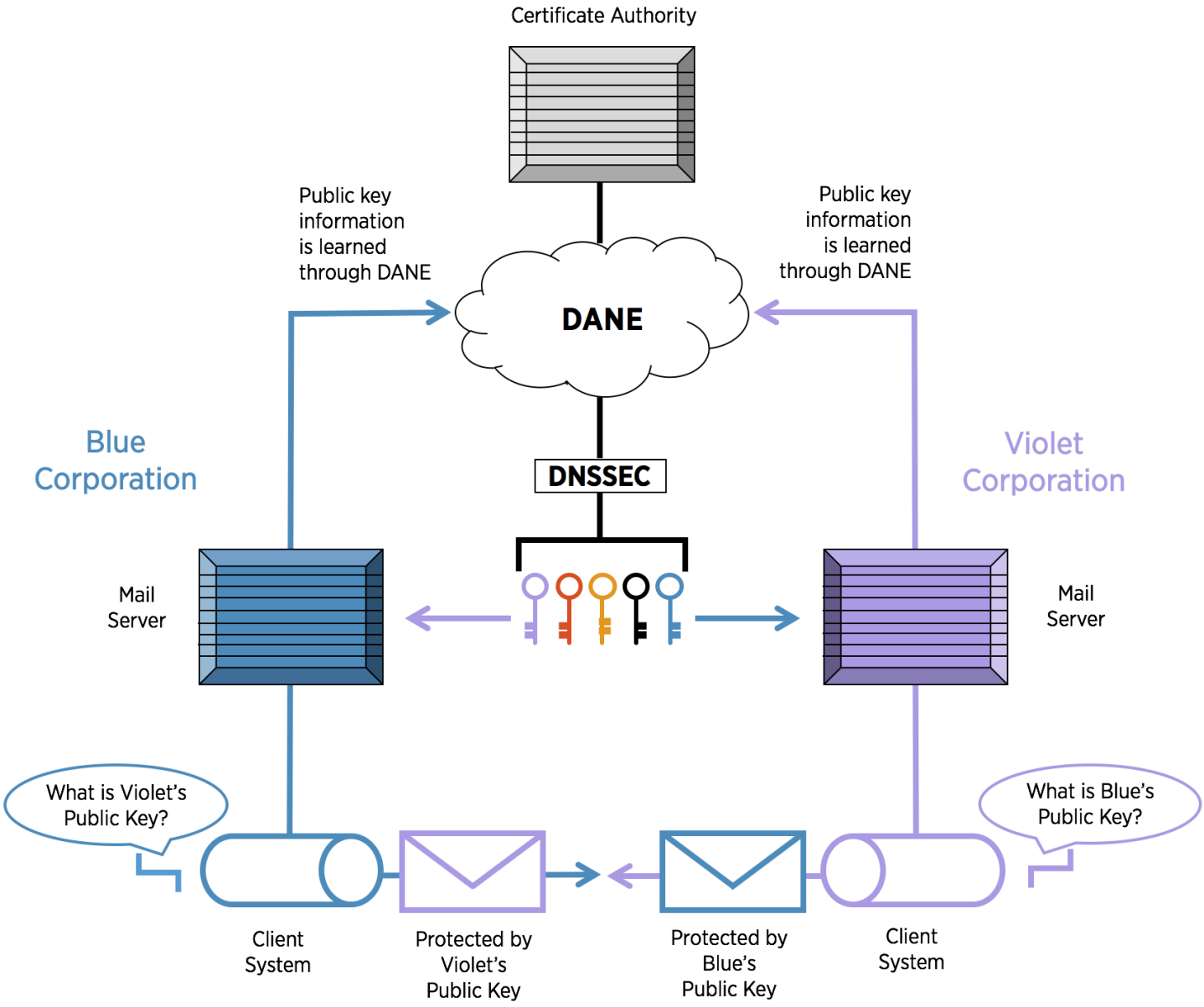
- enables more efficient use of existing security products with minimal impact to email service performance
- enables employees to exchange personal and enterprise information via email with reduced risk of disclosure or compromise
- integrates capabilities into various server and client IT infrastructure environments
- enhances visibility for system administrators into email security events, providing for 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
- can be extended to other enterprise information exchange technologies (e.g., text messages, chat)

ARCHITECTURE

In the project test scenarios, encryption the email servers performed encryption on bulk exchanges between organizations. This addresses the main security concerns in enterprise environments, which are the target of the project, but not necessarily those of individual users who may also want to reduce information disclosure to their email providers. Per-message encryption was not included in the project, with the only per-message security being S/MIME digital signatures generated and validated by email client systems.

LEARN MORE ABOUT NCCOE
Visit https://nccoe.nist.gov

CONTACT US
dns-email-nccoe@nist.gov
301-975-0200



TECHNOLOGY PARTNERS/COLLABORATORS

The technology vendors who participated in this project submitted their capabilities in response to a call in the Federal Register. Companies with relevant products were invited to sign a Cooperative Research and Development Agreement with NIST, allowing them to participate in a consortium to build this example solution. Technology collaborators on this project include:

Fraunhofer IAO · ISC Internet Systems Consortium · Microsoft · NLnet Labs · SECURE64

Certain commercial entities, equipment, products, or materials may be identified 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, equipment, products, or materials are necessarily the best available for the purpose.

DOWNLOAD THE PRACTICE GUIDE

For more information about this project, visit:
https://nccoe.nist.gov/projects/building_blocks/secured_email

HOW TO PARTICIPATE

As a private-public partnership, we are always seeking insights and expertise from businesses, the public, and technology vendors. If you have feedback on the architecture or the relevance and usefulness of this Practice Guide, or would like to schedule a demonstration, please email dns-email-nccoe@nist.gov.

January 2017