From: [redacted] via 800-171comments
To: Pillitteri, Victoria Yan (Fed)
Cc: Ross, Ronald S. (Fed); 800-171comments@list.nist.gov; 800-53comments@list.nist.gov; [redacted]
Subject: [800-171 Comments] Proposed NIST 800-53 / 800-171 Control
Date: Monday, January 22, 2024 2:55:29 PM
Attachments: Proposed NIST Control.pdf

Hi Victoria,

I hope this email finds you well.

A few months ago, we met at the CMMC Ecosystem Summit Conference. After your presentation, we briefly discussed how 800-53 and 800-171 do not directly address email authenticity. I expressed concern that this introduces unnecessary integrity and confidentiality risks within federal and non-federal systems. After our discussion, you gave me your card and asked me to send you a proposal to address this gap.

I have attached our proposal to add a new control to NIST 800-53 and 800-171 to address the aforementioned security gap. We recognize it will take significant time for our proposal to make its way into either publication, if at all. Still, we believe that efforts to address this gap and work to mitigate it should be undertaken, which is why we have taken the time to write this proposal and submit it to you.

I sincerely hope you and your team will take the time to read our proposal and begin internal discussions about adding email authentication mechanisms into NIST control frameworks.

If you have any questions or concerns with our proposal, please let me know, and I'd be happy to discuss it further.

Sincerely,

Samuel Anderson, CISSP-ISSAP, CISM, CISA
Senior Solutions Architect
Arnold Magnetic Technologies
770 Linden Avenue
Rochester, New York, USA 14625
[redacted]

Proposed NIST 800-53 / 800-171 Control

External Email Authentication

January 2024

Prepared by:

Samuel Anderson, ISSAP, CISSP, CISM, CISA
Mitchell Moliterni, CISSP, CISM, CRISC, CCSP, CASP+

Contributors:

David Pecora, CISSP, CPP, PCI, PSP
Ken Michael, CISSP, CISA, CRISC, CCP, ECSA
Victor Wainwright, CISSP
Daniel Safford, CISSP

Introduction

Email has become the most widely used and ubiquitous communication method between organizations and government entities. Hence, it has undoubtedly become the most widely used tool for adversaries to exploit organizations and their information systems. Cyber-related incidents that occur through email often involve spoofing a legitimate person or entity with whom someone is already familiar. Trained cybersecurity professionals may be able to spot these spoofed emails, but a large portion of the average user base cannot. Even if a person has been trained to spot common indicators of spoofing, i.e., a wrong domain name, an unusual sense of urgency, poor grammar, or incorrect sender alignment, they may still be unable to detect a well-constructed spoofed email when the spoofed domain and recipient have not implemented adequate authentication mechanisms.

We believe there is a significant gap in the current NIST 800-53 / 800-171 controls, as external email authenticity is not directly addressed in either publication. Although government agencies and specific organizations may infer a requirement to authenticate external emails using existing controls, for example, 800-53 IA-3 or 800-171 3.5.1 and 3.5.2, there is no direct requirement that can be cited to compel them to do so, should they interpret the controls differently. Neither 800-53A nor 800-171A mentions the need to authenticate external emails. This void creates an unreasonably high risk for government agencies and organizations subject to the controls outlined in 800-53 / 800-171. We strongly believe email authentication is critical enough to be cited directly and added as its own standalone control. Adding our proposed control to NIST 800-53 / 800-171 enables government regulators to address this critical gap throughout government agencies and applicable organizations.

Our proposed control would require the government or any organization under the control's scope to authenticate inbound emails and properly sign outbound emails, allowing third parties to authenticate their legitimacy.

The Control

We propose adding the following control to the Identification and Authentication family of NIST 800-53 as a moderate baseline control and adding it as a basic control in NIST 800-171.

Implement authentication mechanisms for email information systems located at external boundaries.

Inbound emails:

Authenticate all inbound emails using SPF, DKIM, and DMARC standards, and quarantine emails that fail the sender domain's authentication requirements. Inbound emails should be checked for the following criteria:

1) **That they were sent from authorized servers (SPF).**
2) **That they have not been altered (DKIM).**
3) **That they pass or fail the sending domain's authentication requirements (DMARC).**

For emails received from a domain that has not published SPF or DMARC records or did not include a DKIM signature, the email must be flagged as unverified before delivering it to the intended internal recipient.

Outbound emails:

Publish SPF records to restrict the domain's authorized servers to only trusted servers or services under the organization's control. Sign all outbound emails for the domain using a valid DKIM signature with a corresponding published public key. Publish a DMARC record that requires the use of SPF and DKIM for the domain and request emails that fail to be quarantined.

Justification

As email is the most adopted and straightforward choice of communication between organizations, government agencies, and other third parties, efforts to protect its authenticity to help mitigate spoofing should be implemented. Unfortunately, the modern implementation of Simple Mail Transfer Protocol (SMTP), which is the universally used method of sending emails through the internet, does not address email authentication directly. There is no native mechanism to authenticate email using the current SMTP standard published in the Internet Engineering Task Force (IETF) Request for Comments (RFC) 5321, or any of the standards obsoleted by RFC 5321. To quote directly from RFC 5321 section 7.1

"SMTP mail is inherently insecure in that it is feasible for even fairly casual users to negotiate directly with receiving and relaying SMTP servers and create messages that will trick a naive recipient into believing that they came from somewhere else. Constructing such a message so that the "spoofed" behavior cannot be detected by an expert is somewhat more difficult, but not sufficiently so as to be a deterrent to someone who is determined and knowledgeable. Consequently, as knowledge of Internet mail increases, so does the knowledge that SMTP mail inherently cannot be authenticated, or integrity checks provided, at the transport level."

Several standards have been developed to mitigate the void created by the original SMTP standards that act as a "patch" to add additional layers of security to the existing SMTP protocol. Of all the available standards, we believe Sender Policy Framework (SPF), Domain-Keys Identified Mail (DKIM), and Domain-based Message Authentication, Reporting, and Conformance (DMARC) are the quickest and most cost-effective to implement. However, wide-scale adoption of these standards has been slow. For example, RFC 4408, which created the original SPF standard, was published in 2006 and updated in 2014 as RFC 7208, and we still have not seen universal adoption of this common-sense standard. We fear that without adding our proposed control or similar control that addresses the need to authenticate external emails to 800-53 / 800-171, we can expect government agencies and reluctant organizations to continue the slow adoption of the SPF, DKIM, and DMARC standards. This leaves the government and industry vulnerable to sophisticated, coordinated spoofing attacks that mimic legitimate domains and users. These attacks are frequently used to enumerate organizations, plant malware, extract information, steal money or intellectual property, or alter objectives.

Attackers can and do use spoofing attacks to extract, alter, or destroy Controlled Unclassified Information (CUI), Personal Identifiable Information (PII), Federal Contract Information (FCI), Export Controlled Information, and other sensitive information within a government agency or contractor. Therefore, we believe it is essential to address this critical vulnerability with clear and concise control language that leaves little room for interpretation regarding the minimum standard of protection when verifying an email's legitimacy. This additional control should be incorporated into NIST 800-53 and NIST 800-171 to ensure that non-federal organizations that store or process Controlled Unclassified Information (CUI) or Federal Contract Information (FCI) apply the same level of protection that would be required of the government itself.

In September 2016, NIST published the original 800-177 Trustworthy Email, and released Rev 1 in February 2019. This publication emphasizes the need to adopt SPF, DKIM, and DMARC, and it can be used as a baseline of existing NIST recommendations to provide adequate email authenticity verification. Should NIST adopt and incorporate our proposed control into NIST 800-53 and 800-171, references to NIST 800-177 should be made, as it goes into deep detail, providing NIST-created guidance on implementing email authentication controls.

Impact

By incorporating our proposed control into the existing NIST 800-53 / 800-171 publications, we expect that government agencies and applicable organizations will begin to universally adopt and enforce the use of SPF, DKIM, and DMARC standards. We expect this to have a dramatic impact on the overall security of all parties involved. As the use of these standards becomes more universally accepted and implemented at scale, there will be a significant increase in a user's ability to detect and report spoofing attempts, as systems will be required to flag or quarantine emails that fail to meet the minimum standards of protection. This will reduce overall risk commensurate with objectives outlined in the Federal Information Security Modernization Act (FISMA).

References

Klensin, J., "Simple Mail Transfer Protocol", RFC 5321, DOI 10.17487/RFC5321, October 2008

Klensin, J., Ed., "Simple Mail Transfer Protocol", RFC 2821, DOI 10.17487/RFC2821, April 2001

Postel, J., "Simple Mail Transfer Protocol", STD 10, RFC 821, DOI 10.17487/RFC0821, August 1982

Kitterman, S., "Sender Policy Framework (SPF) for Authorizing Use of Domains in Email, Version 1", RFC 7208, DOI 10.17487/RFC7208, April 2014

Wong, M. and W. Schlitt, "Sender Policy Framework (SPF) for Authorizing Use of Domains in Email, Version 1", RFC 4408, DOI 10.17487/RFC4408, April 2006

Crocker, D., Ed., Hansen, T., Ed., and M. Kucherawy, Ed., "DomainKeys Identified Mail (DKIM) Signatures", STD 76, RFC 6376, DOI 10.17487/RFC6376, September 2011

Kucherawy, M., Ed., and E. Zwicky, Ed., "Domain-based Message Authentication, Reporting, and Conformance (DMARC)", RFC 7489, DOI 10.17487/RFC7489, March 2015

Levine, J., "Email Authentication for Internationalized Mail", RFC 8616, DOI 10.17487/RFC8616, June 2019

[SP 800-53] Joint Task Force Transformation Initiative (2013) Security and Privacy Controls for Federal Information Systems and Organizations. (National Institute of Standards and Technology, Gaithersburg, MD), NIST Special Publication (SP) 800-53, Rev. 4, Includes updates as of January 22, 2015.

[SP 800-171] Ross RS, Pillitteri VY, Dempsey KL, Riddle M, Guissanie G (2020) Protecting Controlled Unclassified Information in Non-federal Systems and Organizations. (National Institute of Standards and Technology, Gaithersburg, MD), NIST Special Publication (SP) 800-171, Rev. 2.

[SP 800-177] Rose SW, Nightingale S, Garfinkel SL, Chandramouli R (2019) Trustworthy Email. (National Institute of Standards and Technology, Gaithersburg, MD), NIST Special Publication (SP) 800-177, Rev. 1.

Federal Information Security Modernization Act of 2014 (Public Law 113-283; December 18, 2014)

Contact Information

Samuel Anderson | Senior Solutions Architect | Arnold Magnetic Technologies | [redacted]

Mitchell Moliterni | Chief Information Officer | Arnold Magnetic Technologies | [redacted]

David Pecora | Systems Engineer | Mainline Information Systems | [redacted]

Ken Michael | Vice President | Dox Electronics | [redacted]

Victor Wainwright | Owner/CEO | Security101 Rochester | [redacted]

Daniel Safford | Information Security Engineer | Dartmouth College | [redacted]