FPKIMA Newsletter

Winter 2022 | Volume 8, Issue 1

Federal PKI Management Authority
Enabling Trust

Inside This Issue

ALPACA

In August 2021, a group of German researchers presented a clever hack against Transport Layer Security (TLS) protected websites with the nickname ALPACA, which stands for "Application Layer Protocols Allowing Cross-Protocol Attack."[i] Essentially, this attack works by injecting malware into a non-protected site using either HTTP or another protocol such as FTP or SMTP and then redirecting the user from the intended HTTPS site to the corrupted site. In order to work, the non-protected site must have an address that matches the domain name in the TLS certificate for the protected HTTPS site. The attack is possible where more than one site using different ports share the same domain name, or where wildcard certificates are used. As a result of this demonstration, NSA issued a Cybersecurity Information Sheet, "Avoid Dangers of Wildcard TLS Certificates and the ALPACA Technique"[ii] in October 2021.

Wildcard certificates contain an asterisk "*" that permits the certificate to represent any subdomain that falls under a base domain. Wildcard certificates are commonly used for high volume systems with load balancing, so that a single certificate and its associated private key can be installed on all of the associated systems. Wildcard certificates are also used to support elasticity in a cloud-based system, where the certificate and its corresponding private key are cloned each time a new instance of the server is stood up. In some instances, wildcard certificates are used as a cost saving measure so that a single certificate can be used across multiple servers.

To mitigate the risks of ALPACA and other attacks that leverage wildcard certificates, NSA recommends that all agencies do the following:

- Review existing wildcard certificates and ensure that all copies of the private key associated with the certificate are stored using a security posture that is commensurate with the requirements for all applications within the certificate's scope
- Where possible, restrict the scope of wildcard certificates to servers hosting the same application
- Use an application gateway or web application firewall in front of servers, including non-HTTP servers that includes functionality to filter traffic based on the TLS server name indication extension thereby preventing traffic misdirection
- Use encrypted DNS and validate DNS security extensions to prevent DNS redirection
- Where possible, enable application-layer protocol negotiation (ALPN). However, note that support for ALPN varies across user platforms, so agencies should confirm that user environments support ALPN prior to broadly implementing it
- Maintain web browsers at the latest version with current updates

APPLE S/MIME

Apple publicly posted the requirements[iii] and submission process for inclusion in their publicly trusted Root Store program. This includes advance notices that beginning April 1,2022, S/MIME certificates must not include a validity period greater than 825 days. This restriction should not immediately affect signature certificates issued within the FPKI as the Federal Common Policy CA G2 is not included in the Apple Root Store program. However, Apple has set a precedent for transitioning restrictions initially imposed only on publicly trusted certificates to include all certificates. If your agency uses native Apple products for S/MIME, on either iOS or MacOS, with 3-year signature and key management certificates, you may want to contact Apple at certificate-authority-program@apple.com and request this validity period restriction not be extended to enterprise managed S/MIME certificates.

CA/Browser Forum Expansion

The CA/Browser Forum has expanded and now includes working groups developing baseline requirements for publicly trusted S/MIME and code signing certificates in addition to server authentication certificates used with TLS. In place of browsers, these other groups include "certificate consumers" who are vendors that develop commercial products that will be the relying party application for these certificate types. What appears to be missing from the S/MIME working group is representatives from organizations that configure and rely on both the certificates and relying party email applications. The S/MIME group has drafted certificate profiles[iv] for the end-user S/MIME certificates divided into categories for email-validated only, organization-validated, sponsored-individual, and personal individual certificates. In addition, each category contains 3 types of profiles: one strictly for certificates limited in use to only email-protection, multi-use certificates that may contain EKU for additional uses like document signing, and one labeled legacy that attempts to capture what is currently in certificates being used for email-protection.

Post Quantum Cryptography: A Q&A with NIST's Matt Scholl

NIST invited their chief of the Computer Security Division, Matt Scholl to discuss the future of quantum machines and risk to our data[v]. Matt Scholl and NIST have been working on identifying and standardizing new encryption algorithms to eliminate the risk of being broken by quantum machines. The goal is to develop encryption standards that work with current machines and future threats from quantum machines. Scholl recommends that individual organizations begin to assess which data is most important and its encryption vulnerabilities. Planning for the future will help organizations to prioritize data when new standards are implemented.

NISTIR 8360– Machine Learning for Access Control Policy Verification

"Proposes an efficient and straightforward method for access control policy verification by applying a classification algorithm of machine learning" You can see the full release here

SP 800-213 IoT Device Cybersecurity Guidance for the Federal Government: Establishing IoT Device Cybersecurity Requirements

This document provides recommendations for incorporating IoT devices. You can see the full release here

SP 800-108 Rev.1 (Draft)- Recommendation for Key Derivation Using Pseudorandom Functions

NIST released a draft of SP 800-108 Rev.1. The comment period for SP 800-108 is closed as of 1/18/22.

Where Can I Find More Information about the FPKIMA?

For more Information about the FPKIMA, go to https://www.idmanagement.gov/governance/ficam/#federal-public-key-infrastructure-management-authority or the FPKI Guide website at https://playbooks.idmanagement.gov/fpki/.

PKI in the Cloud

During the November FPKI Technical Working meeting, PKI in the cloud was discussed. The group reviewed FISMA requirements in the FPKI Overlay to 800-53 compared with FedRamp requirements. FedRAMP requirements are not written with enough specifics to ensure they meet FPKI Common Policy requirements. The main conclusion from the discussion is that the PKI in the cloud must still meet FPKI requirements and simply pointing to a FedRAMP ATO is not sufficient; they must be able to demonstrate the compliance with each annual PKI Compliance Audit.

NIST's International Cybersecurity and Privacy Resources Website

NIST recently launched a new International Cybersecurity and Privacy Resources Site[vi]. This site will assist international colleagues as NIST cybersecurity and privacy resources continue to be used throughout the world to manage cyberthreats and privacy risks. The new site includes translations of Cybersecurity Framework in languages such as Arabic, Indonesian, Japanese, and Polish. The translation of other NIST documents and frameworks can be found listed including Privacy Framework, NICE Framework, and IoT Cybersecurity Program Documents. Along with translations of NIST framework, the site includes adaptations that incorporate and reference content from NIST.

Federal PKI Working Group Updates

The **Certificate Policy Working Group (CPWG)** Audit and Archive Work team met throughout the quarter to review and clarify existing audit and archive policy requirements. The team recommended updates to the Federal Common Policy, which the FPKIPA subsequently approved. The CPWG also distributed proposed updates to the Federal Bridge CA Certificate Policy for review at the end of the year.

The most recent **FPKI Technical Working Group (TWG)** was held on November 2, 2021. In addition to the S/MIME updates, the group discussed if a PKI in the cloud could meet the FPKI requirements.

Do you have a topic that you would like to be addressed during an upcoming TWG? Please send any topics or question to fpki-help@gsa.gov.

The next TWG meeting will be held on the third Wednesday starting February 16,2022 with topics alternating between FPKI focused topics and those of a broader interest to the ICAM community. The February agenda may include the impact of TIC Break and Inspect Services on cross Agency use of SMIME and mutual TLS for authentication services.

Participation in Federal PKI working groups is limited to Federal employees, contractors, and invited guests.

Ask the FPKIMA

How do I view the certificates on my PIV on Google Chrome browser?

Google Chrome has become a popular web browser choice for users and Google Workplace products are used by federal agencies. To view the certificates on your PIV within Chrome follow the steps below:

1. Open Google Chrome
2. Select **Settings> Security and Privacy> Security**
3. Under Advanced click on “Manage Certificates”
4. The certificates on your PIV will be listed under the Personal tab. If you have used more than one PIV on the system, look for the certificates with the latest expiration date.

You can subscribe to system notification and other issues by signing up for a GitHub account and watching the FPKI guide repository at https://github.com/GSA/ficam-playbooks.

References

i https://alpaca-attack.com/ALPACA.pdf.

iihttps://www.nsa.gov/Press-Room/News-Highlights/Article/Article/2804293/avoid-dangers-of-wildcard-tls-certificates-the-alpaca-technique/

iii https://www.apple.com/certificateauthority/ca_program.html

ivhttps://docs.google.com/spreadsheets/d/1gEq-o4jU1FWvKBeMoncfmhAUemAgGuvVRSLQb7PedLU/edit

V https://www.nist.gov/blogs/taking-measure/post-quantum-cryptography-qa-nists-matt-scholl

vi https://www.nist.gov/cybersecurity/international-cybersecurity-and-privacy-resources

Need help?

Certificate doesn’t validate?Unsure which certificate to use?

ASK THE FPKIMA

fpki-help@gsa.gov

Request for Topics

Do you have a topic or a question that you would like to be covered in an upcoming newsletter? Would you like to contribute on a topic? Please send any topics or questions to ***fkpi-help@gsa.gov***