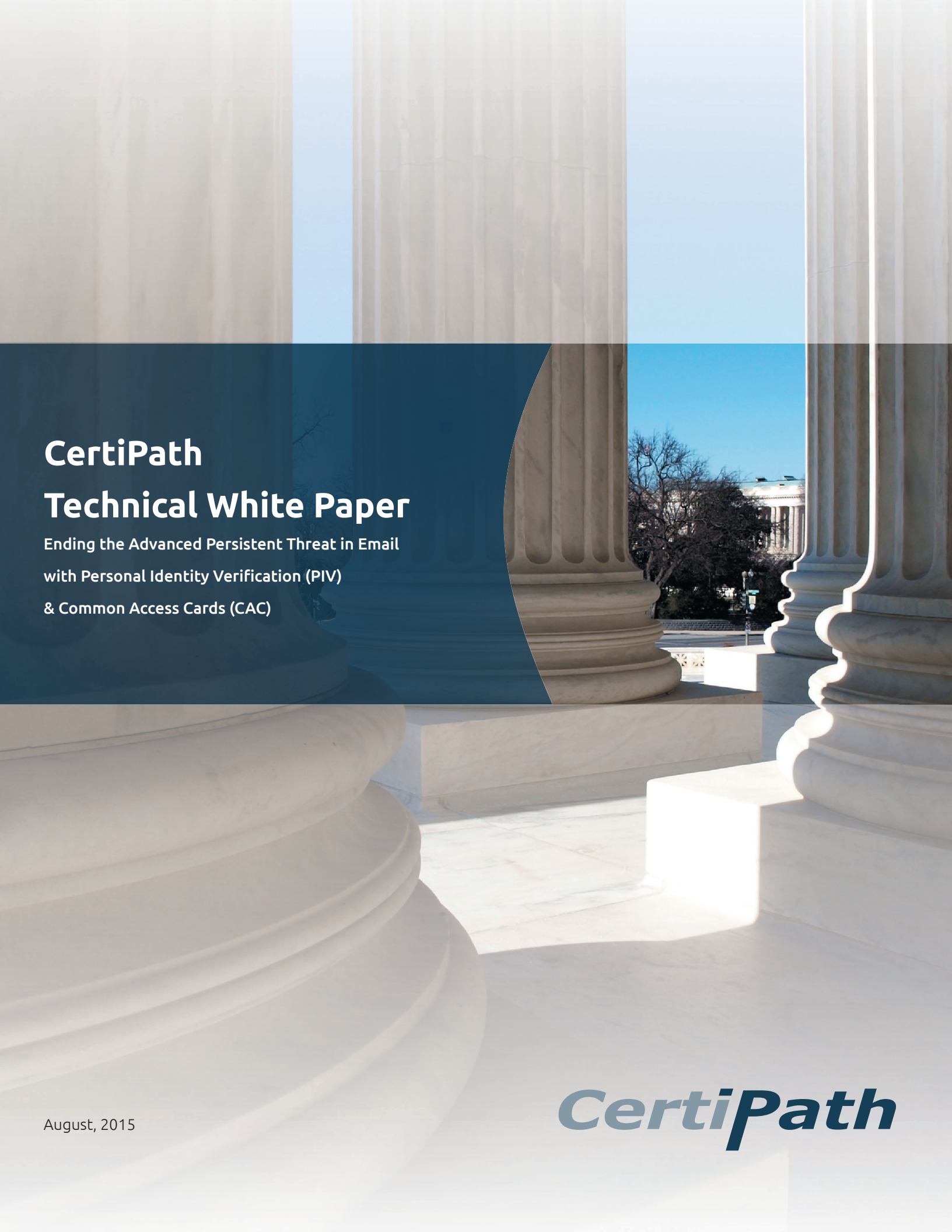


CertiPath Technical White Paper

Ending the Advanced Persistent Threat in Email with Personal Identity Verification (PIV) & Common Access Cards (CAC)

August, 2015

CertiPath

Contents:

Executive Summary

E-mail continues to be the primary point-of-entry chosen by advanced persistent attackers, credit card thieves, and malware authors. The platform has remained the same, but the attacks are more effective than ever. Phishing schemes, the most common type of attack performed against e-mail recipients, are carried out by an attacker that 'spoofs' or fakes the sender field of an e-mail message, usually also including a malicious attachment or hidden link, with the typical goal of infecting the recipients computer with a virus or surveillance software by tricking the recipient into believing the email they received was from a trusted sender.

The U.S. Government and organizations that deal with sensitive personal information are also at risk from an evolved form of phishing called 'Spear-Phishing' which is known to be much more targeted, and much more effective in its application. The success of Spear-Phishing campaigns is largely based on the attacker's ability to gain personal information about the targeted individual or group in order to craft more trustworthy phishing e-mail content.

For example, Government worker's with a health issue would be more likely to click on a link related to a cheaper source medication than a healthy worker.

Unintended Consequences

The recent breach of the large health insurer Anthem Inc., where a database was accessed that included the personal information of 78.8 million people, including 60 million to 70 million of Anthem's current and former customers & employees has had the unintended consequence of helping advanced persistent attackers by providing them the key information needed on many Government workers to increase the effectiveness of targeted Spear-Phishing campaigns. - Investigators Suspect Anthem Breach Began with 'Phishing' of Employees.

In April 2015 the Office of Personnel Management (OPM) disclosed that the personnel data of "4.2 million current and former Federal government employees had been stolen", including Social Security Numbers (SSN)'s that can be used to identify employee medical records, in a campaign carried out using phishing attacks that had distinct similarities to the prior widely publicized Anthem breach. Following the Anthem breach, the breach at OPM has made the risk of Spear-Phishing against Government workers more tangible than ever. - Information about OPM Cybersecurity Incidents.

The success of attacks using very simple, widely known 'mistake-of-identity' tactics combined with slow-to-respond value-rich Agency targets has made phishing/spear-phishing one of the most widely reported threats to the U.S. Government in 2015. Information suggests that most Government Agencies do not know whether or not they are currently being targeted by these types of attacks until, and would not know till a compromise actually occurred, even though there is a sentiment across Government that a persistent threat always exists. A recent breach of the U.S. Postal Service (USPTO) prompted the Agency to release a statement that workers be on the lookout for suspicious emails that may be phishing attempts following a compromise which effected the personal information of 800,000 employees - China suspected of breaching U.S. Postal Service computer networks.

The USPTO's response time to the incident has also been criticized; disclosure of the attack by the Agency did not take place until approximately 1-month later, due to the time it took the Agency to confirm whether a data-theft had even occurred. The inability for Agencies to identify when a breach has occurred has many industry security experts apprehensive that personal data stored by other Agencies is under the same risk of being compromised.

Even more concerning is that the source of many of the largest attacks appears to have originated from overseas government entities. These nation state actors have allegedly already been successfully carrying out wide-spread spear-phishing campaigns against many organizations including the U.S. Department of Defense, defense contractors, and political activist organizations.

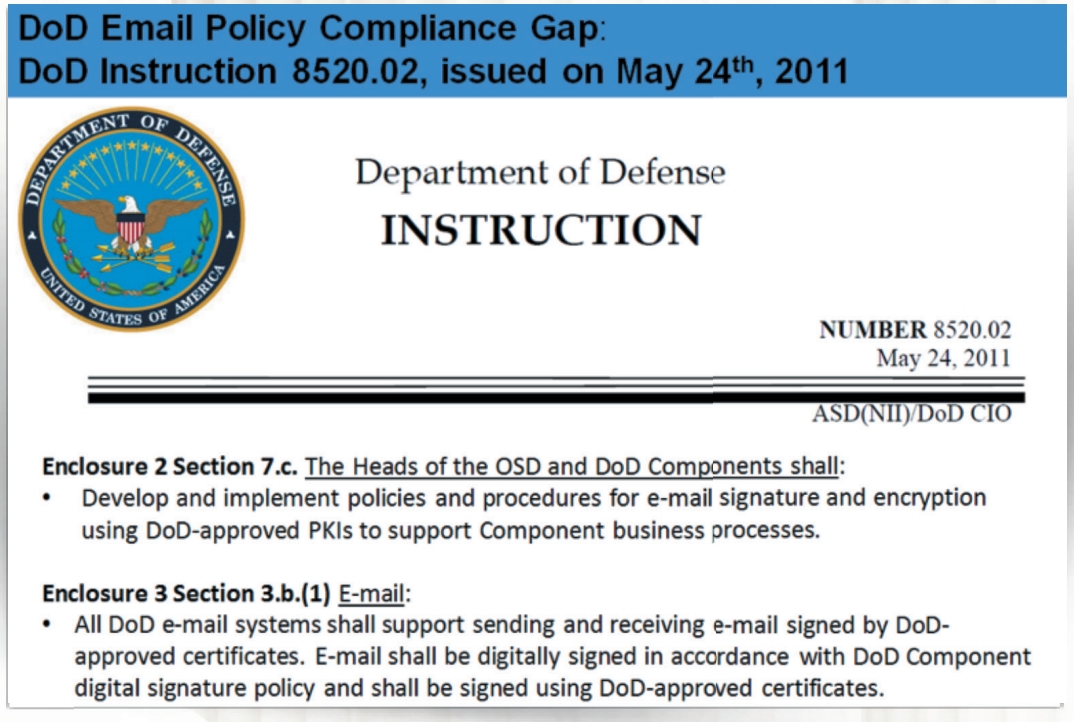
Catching up with Phishing

The most advanced attackers now are using spoofing techniques that gain the trust of both the e-mail recipient, in order to trick the recipient into opening a malicious link or attachment, and the e-mail filters meant to stop bad attachments & links from reaching employee inboxes.

The U.S. Government is planning to fight back to protect identity by expanding the use of their Personal Identity Verification (PIV) badges to prove e-mail senders' 'digital identities', making spoofing impossible without compromising a Government worker's PIV badge. The U.S. Department of Defense has already released similar guidance to use its own Common Access Card (CAC) badges & cross-certified approved partner e-mail certificates for digital proof of identity for e-mail.

"Spear-phishing messages… have evolved to the point where even experienced end users have a hard time spotting faked messages among their authentic emails. These messages, which target specific individuals with a well-crafted message… Emails with a trusted name and a logo, even if spoofed, carry more weight than the old-school spam messages touting pharmaceuticals or watches. And if the messages have a call to action that is familiar to recipients, such as a notice about a recent order, or a delivery tracking number, users will be further enticed to click on links contained in the email."

- Cisco's 2015 Annual Security Report



DoD Email Policy Compliance Gap:
DoD Instruction 8520.02, issued on May 24th, 2011

Department of Defense

INSTRUCTION

NUMBER 8520.02
May 24, 2011

ASD(NII)/DoD CIO

Enclosure 2 Section 7.c. The Heads of the OSD and DoD Components shall:

- Develop and implement policies and procedures for e-mail signature and encryption using DoD-approved PKIs to support Component business processes.

Enclosure 3 Section 3.b.(1) E-mail:

- All DoD e-mail systems shall support sending and receiving e-mail signed by DoD-approved certificates. E-mail shall be digitally signed in accordance with DoD Component digital signature policy and shall be signed using DoD-approved certificates.

All U.S. Government e-mail systems not yet utilizing PIV badges for e-mail communications are leaving Agency inboxes at risk, and the slow adoption of e-mail security policy has security experts worried that the next Agency breach will be just around the corner - with mounting concern in the financial sector that a major bank could experience a breach of a size similar to what happened at Anthem.

Implementing Digital Message Signatures will greatly reduce the wide-open e-mail attack surface for Agencies; however, the average user of an e-mail system that incorporates 'digital signatures' is typically not aware that all signed emails cannot be trusted equally. As a result, the threat of spoofing is still high even when digital signatures are being used, and the number of sophisticated hacks employing seemingly legitimate credentials is on the rise.

"… Decoy documents attached to spear phishing emails are frequently indicators of intended targeting because threat actors generally tailor these emails to entice their intended targets, who typically work on related issues, to click on the attachments and infect themselves."

- APT30 and the Mechanics of a Long-Running Cyber Espionage Operation

A Trusted Seal

The use of a 'seal' to verify a message senders identity goes back to the first civilizations. Early forms of trusted seals were created using melted wax imprinted with a stamp, creating a 'Wax Seal' that protected letters during their transit by couriers. Metal stamps were commonly formed into rings called 'signet rings', well individuals that communicated by courier frequently would often create personalized signet rings.

Receiving a letter that contained a Wax Seal stamped by a personalized signet ring allowed recipients to:

- Identify who the letter is from based on the graphic contained by the Wax Seal,
- Determine whether the letter had been read by the courier if the Wax Seal was intact, and to
- Provide an assurance that the letter was not sent to the recipient by mistake.

When a trusted seal can be easily duplicated, all three values become compromised. If a signet ring's graphic was copied, it was possible to spoof letters 'signed' as the ring-holder, or to inspect the content of letters in-transit by resealing letters after opening and reading their contents.

Using Government issued PIV cards to 'digitally sign' e-mail messages provides the same three intended purposes that Wax Seals provided, without the risk that the seal itself will leave the messages susceptible to spoofing.

Unless e-mail clients fail to differentiate for user's the difference between a valid digital signature, and a trustworthy one.

Misuse of Certification Authorities

Using 'under-the-hood' digital signatures in web applications has been commonplace for sensitive financial transactions that take place online such as e-commerce and banking for many years, its use in everyday communications like e-mail is less routine and typically only employed by those with a heightened sense of security.

U.S. Government PIV Certification Authorities (PIV-CAs) issue digital identities to Government employees & contractors, most CAs are entities that provide digital identities to websites and people for specific purposes like signing communications. The difference between PIV-CAs and their commercial counter parts lies in the process used to verify the real-world identity of the person applying for a digital identity, and the differences are stark.

In order to be issued a PIV card, U.S. Government employees & contractors must be able to provide 2-forms of Government issued identification documents (e.g., Drivers License or Passport) and go through a fingerprinting process. In comparison, the effort required to obtain a free certificate that can be used for e-mail signature is very low. Attackers do not typically need to compromise a CA in order to obtain an e-mail signing certificate from a commercial free CA. E-mail signing certificates can easily be obtained by anyone that is able to provide a valid e-mail address to a CA that may or may not belong to the certificate requestor.

Commercial CAs also lack the security controls PIV-CAs have in place. Commercial CAs that provide free certificates are not run against requirements as strict as the Federal Information Security Management Act (FISMA) controls that are mandatory for all PIV-CAs.

E-mail clients inadvertently create a false sense of security for users by promoting that any digitally signed email is a trustworthy e-mail by the way presenting users with trusted seals for every digitally signed e-mail is handled, regardless of CA trustworthiness. As we have seen with a number of high profile breaches across both commercial and Government sectors, the way e-mail clients represent which messages are trustworthy has been an enabler for Spear-Phishing attacks, just like it was in the days of Wax Seals.

The evolving security landscape has demonstrated that not all CAs are created equal, and trusting communications based only on the presence of a digital signature is risky. The fact that an e-mail has been digitally signed does not ensure it is authentic and from who the sender claims to be unless the digital identity of the e-mail sender can be verified as being from a trusted CA, and the implementation of PIV for e-mail will only make Spear-Phishing easier without implementing a solution to what researchers have coined 'Trusted Impersonation' in industry, where a Spear-Phishing e-mail is enhanced by attaching a valid-but-untrustworthy digital signature to their message to appear more credible.

Questioning Authority

Web browsers contain the ability to provide 'Extended Validation' checks and additional information on CAs that have issued certificates to certain websites, indicating that the website owner has gone through additional steps to prove their identity, but no similar mechanisms are available for the inbox today to do the same checks against the identities behind e-mail signatures.

For digitally signed emails, there is no scoring system in place to observe, analyze, and inform users or systems administrators of the potential risks associated with incoming emails, attachments, or embedded links. While some security administrators may regularly refresh their list of trusted CAs and /or maintain a Certificate Revocation List (CRL), there is no reliable means for enforcing this with the average corporate email user.

Trusted identity remains one of the biggest and least recognized problems facing the secure commercial and Government organizations today.

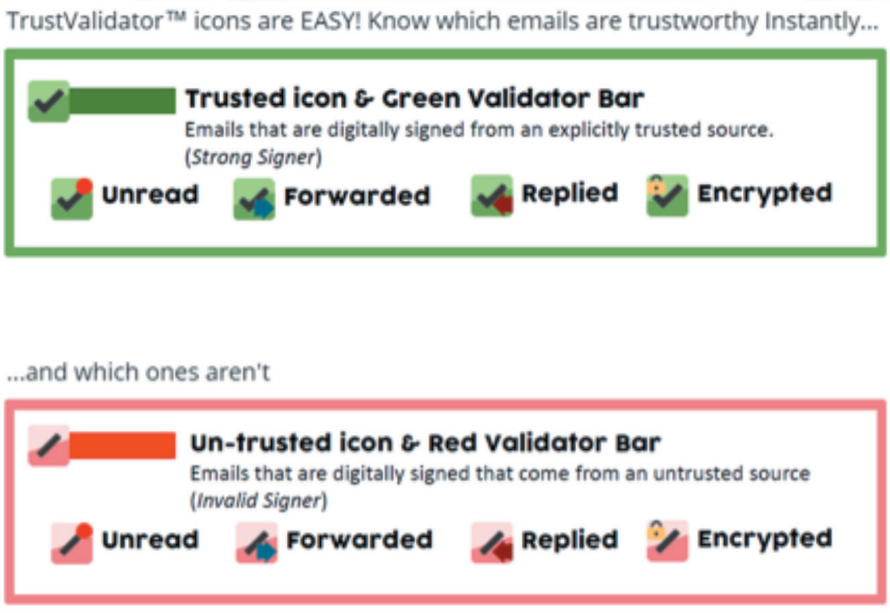
The CertiPath TrustValidator Solution

CertiPath's TrustValidatorTM is an enterprise platform for evaluating incoming emails that analyzes and reports the strength of e-mail signatures in order to give users better indicators of which e-mails can actually be trusted to be from their declared sender.

CertiPath has brought to market the only solution that protects against both Phishing & Spear-Phishing attacks on the inbox that has been specifically designed to be compatible with U.S. Government-issued identities that is based on CertiPath's years of experience in the identity industry advising commercial and Government entities on implementing trusted identities in both physical and logical access controller systems used globally to protect billions of dollars in real & digital assets.

TrustValidator works by replacing generic e-mail icons with new graphics that convey different levels of trustworthiness more effectively than systems that display only a 'Trusted or Not-Trusted' indicator for digitally signed e-mails. Having descriptive icons and a color-coded status bar in e-mail clients enables users to perform a quick evaluation of which e-mails are authentic and which e-mails might warrant suspicion.

Figure 1.2



The user-interface has never been more important as a tool that equips users to make better choices about which attachments to open and which links to click.

Users of TrustValidator are able to see immediately whether any e-mail was sent by a source that your organization trusts or whether the message should treated with caution, and TrustValidator can be installed without sending your employees off to yet another security workshop/seminar.

Trust and Validation

Trustworthy signed e-mails are typically those from members of your organization or known external partners & contractors using credentials explicitly trusted by your organization. These messages will appear in your inbox with a green colored status bar and icon.

Signed e-mails from a source to which your organization assigns conditional trust will appear with a yellow colored status bar and icon. Attachments and links may be disabled by administrators for these messages in addition to the cautionary icon and status bar to further reduce the risk of user's accidentally downloading or navigating to malicious content. These e-mails are likely from whom they claim to be but were signed with credentials not high enough assurance to be certain.

Signed e-mails from an untrusted source, or a credential level not explicitly trusted, will appear with a red colored status bar and icon in a user's inbox. Digitally signed e-mails that appear with a red status bar and icon are often from untrustworthy sources that may be part of a Spear-Phishing attack, or are messages that have been tampered with or modified in-transit. Attachments and links are disabled by default for all untrusted messages, user's that receive invalid e-mails are able to forward detailed error information to support staff with the click of a button, and messages marked as invalid for any reason can be quarantined automatically to reduce the risk user error.

In addition to distinguishing trustworthy emails with unique icons and a trust status bar, TrustValidator provides security tools for users and IT or security support staff that enable them to quickly troubleshoot issues when they occur. Users are able to view the signing certificate of any email and explore the certificate path information that was used to validate each message.

TrustValidator addresses significant risks in secure email today. Whether you have already deployed digital signatures or are looking to, this tool provides you true insight that your emails will not be exploited as an attack vector.

How it Works

TrustValidator improves both the security and usability of your inbox. It provides full validation of digitally signed e-mails you receive and makes your users more confident that their signed e-mails are coming from a trustworthy source.

Using a cloud based Server-based Certificate Validation Protocol (SCVP) server to perform validation, TrustValidator guarantees a more stable, consistent, and constantly updated source of trust-information about CAs. SCVP works with both encrypted and unencrypted e-mails.

Using (SCVP) as the backend, TrustValidator creates a single-point-of-success for updating to new algorithms and centrally managing against trust-based threats to email:

1. When an e-mail message is received, on-receive event triggers

2. Emails that are encrypted are not evaluated until decrypted by the user; unencrypted emails are assessed by plug-in immediately

3. Message integrity is verified by checking that the e-mail signature block is intact

4. The e-mail signing certificate is packed into an SCVP call that gets sent to an SCVP-server instance

5. The SCVP server evaluates whether the e-mail signing certificate is:
   a. Valid and was issued by a known Certificate Authority
   b. Meets the enterprise's identity policy requirements (e.g., is the signer verifiably by a PIV or medium hardware assurance level credential)

6. Based on the established enterprise policy, the SCVP server digitally signs a response with trusted keying material and sends the validation response back to the e-mail client with detailed validation status information

Deployment in Enterprise

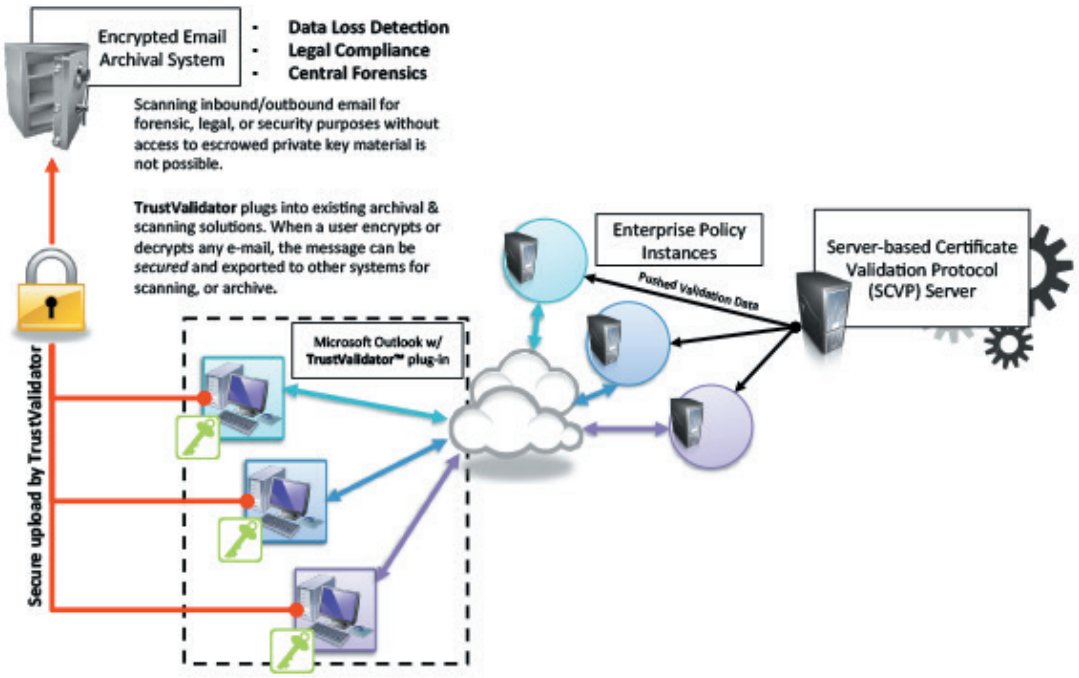
TrustValidator deployment consists of a three-part solution:

1. An SCVP server, which sits on the enterprise network working in tandem with an e-mail Exchange server, or deployed to a stand-alone location

2. A Outlook Inbox plugin (or other e-mail clients), installed as part of approved desktop configuration

3. Connections into existing e-mail scanning and archival solutions for data loss detection, malware scanning, e-mail classifications, etc. (Optional)

Example Deployment Architecture



Summary

CertiPath's TrustValidator offers some very unique benefits for protecting enterprise email. Simple color-coded icons alert users to the trustworthiness of emails before they are opened and expose users' systems to possible malicious content or attachments. With this platform enterprise IT and security professionals will be able to:

- Detect spoofed digital identity that hide e-mail based attacks
- Centralize digital signature policy management
- Prompt informed user decisions of email authenticity
- Establish certificate authority and revocation list monitoring
- Easily incorporate and track new certificate authorities real-time global insight from the cloud on certificate relationships and safety
- Create analytics to measure and benchmark user behavior and risk management
- Capture encrypted e-mails/attachments in plaintext
- Maintains a list of trusted Certification Authorities
- Work with multiple types of PKI-based credentials (PIV, CAC, and industry PIV-I)

About CertiPath

CertiPath provides monitoring and validation services to support the trusted identities used by enterprise IT, aerospace, and defense firms. Founded in 2004 by security and identity policy experts, CertiPath has become a recognized industry thought leader for identity standards, policies, and specifications.

In addition to creating and maintaining The CertiPath Bridge - an identity policy hub used by DoD contractors, CertiPath has developed a framework for identity monitoring and analytics to address the rising occurrences of identity-related gaps in the IT services and systems security.

CertiPath's products and services make secure credentials and online identities safer and more efficient to use enabling enterprises to establish and leverage a reliable Trust Fabric that can insure your critical assets are being accessed by valid and vetted users.

About Carillon

Carillon Information Security Inc. provides a complete spectrum of identity management solutions that are designed to prevent identity theft, promote the migration from paper to electronic authentication, and avoid loss of intellectual property. From consulting services, to validation software and managed identity services, Carillon can provide the skill sets and tools to help companies take control of their corporate digital credentials.

References & Resources

Investigators Suspect Anthem Breach Began with 'Phishing' of Employees

http://www.insurancejournal.com/news/national/2015/02/10/357051.htm

Information about OPM Cybersecurity Incidents

https://www.opm.gov/cybersecurity/#WhatHappened

China suspected of breaching U.S. Postal Service computer networks

https://www.washingtonpost.com/blogs/federal-eye/wp/2014/11/10/china-suspected-of-breaching-u-s-postal-service-computer-networks/

Cisco 2015 Annual Security Report

https://www.cisco.com/web/offers/pdfs/cisco-asr-2015.pdf

APT30 and the Mechanics of a Long-Running Cyber Espionage Operation

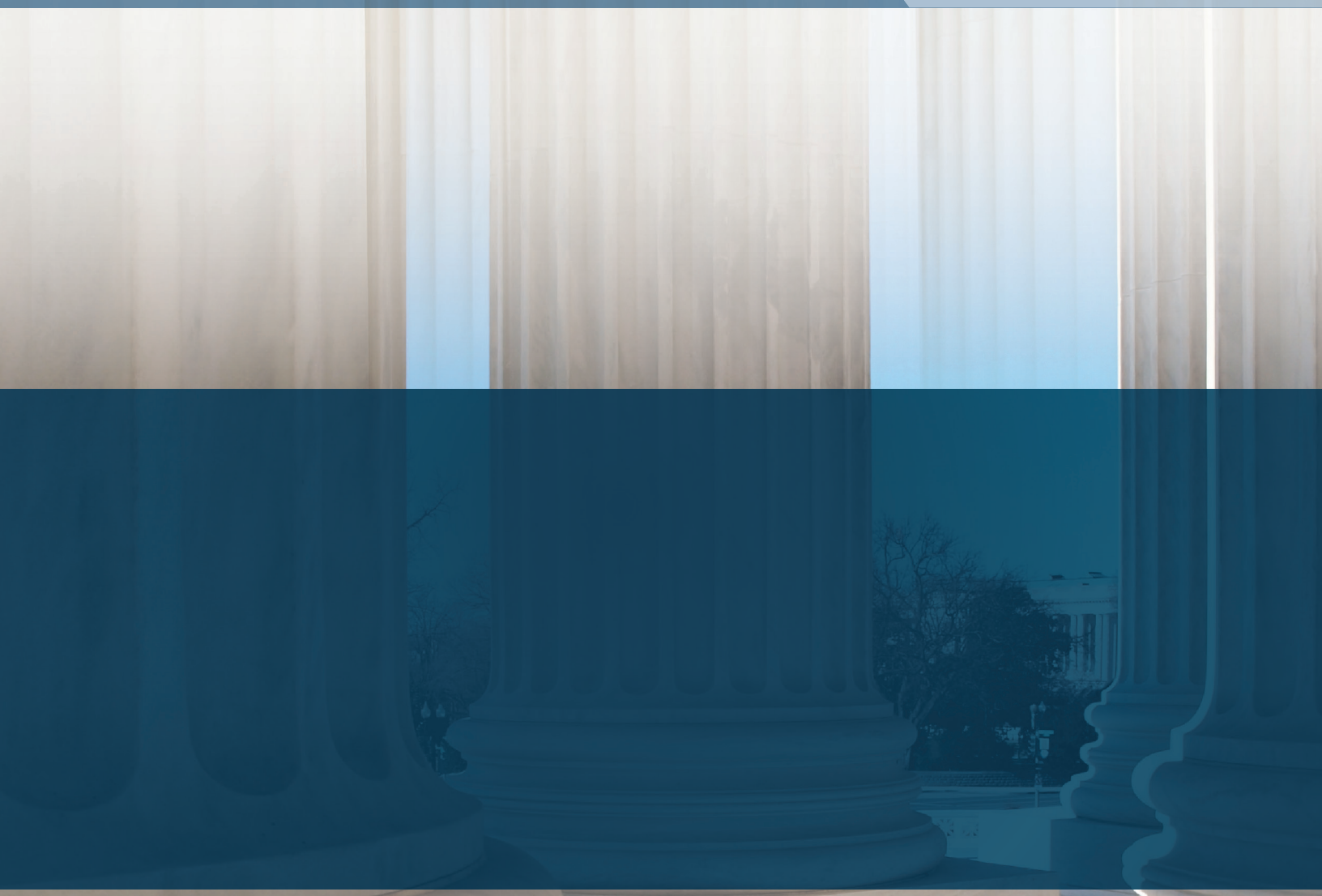
https://www2.fireeye.com/rs/fireye/images/rpt-apt30.pdf

August 20, 2015

CertiPath Contact Info

11921 Freedom Drive
Suite 710
Reston, VA 20190, USA

Toll Free: 1.855.758.0075
Phone: 1.703.793.7870
General: info@certipath.com
Sales: sales@certipath.com
Support: support@certipath.com



CertiPath

Headquarters
11921 Freedom Drive
Suite 710
Reston, VA 20190 USA

Toll Free: 1.855.758.0075
Phone: 1.703.793.7870
Fax: 1.571.375.0815

www.certipath.com