GIAC
CERTIFICATIONS

Global Information Assurance Certification Paper

Copyright SANS Institute
Author Retains Full Rights

This paper is taken from the GIAC directory of certified professionals. Reposting is not permited without express written permission.

Interested in learning more?

Check out the list of upcoming events offering
"Implementing and Auditing CIS Controls (Security 566)"
at http://www.giac.org/registration/gccc

The Business Case for TLS Certificate Enterprise Key Management of Web Site Certificates

Wrangling TLS Certificates on the Wild Web

GIAC (GCCC) Gold Certification

Author: Sandra E. Dunn, sandra.dunn@hp.com
Advisor: Stephen Northcutt

Accepted: September xth 2015

Abstract

An Enterprise Key Certificate Management System (EKCM) provides a best-in-class solution for TLS certificate management. It requires a significant financial and resource investment that often causes businesses to table the idea until the next certificate crisis. Enterprise businesses that delay lose significant financial benefits and otherwise positive financial gain from an EKCM implementation. Provided web certificate data captures a comprehensive view of the high cost of poor certificate management, the benefits of deploying HTTPS everywhere, and the positive return for maximizing search optimization. It is important to note the data presented represents the gain from managing TLS certificates installed on web servers, the benefits of TLS / SSL certificate management are amplified when all certificates used for security services such as authentication, whitelisting, and code signing are managed.

1.0 Introduction

Trust is the cornerstone of the Internet economy. SSL/TLS certificates establish this trust by providing a digital identity for trusted and secure communication. Many organizations believe simply deploying certificates is all that is needed to secure their website. They are unaware of the remaining threat and the need for proper certificate management. "The greatest threat to the security of SSL/TLS certificates appears to be the lax controls most organizations exert over securing keys and certificates."(Filkins,

© 2015 The SANS Institute Author retains full rights.

2015). These "lax controls" may be attributed to many single and/or interconnected events. These events include the lack of policy, standards, and specifications for TLS deployment; relying on a manual management process that requires human interaction; and poor role definition in certificate support teams that have a high turnover rate.

The Transport Layer Security (TLS) is a building block for secure internet communication. Often discussions and written documents reference the protocol as SSL/ TLS to represent both the older version (SSL) and the current standard (TLS). TLS will be used since that is the currently secure version.

1.1. Transport Layer Security

The Transport Layer Security Protocol "provides communication security over the Internet. The protocol allows client/server applications to communicate in a way that is designed to prevent eavesdropping, tampering, or message forgery."[RFC5246] The current version of TLS is version 1.2 released in 2008. TLS Version 1.3 has just been released to draft with an expected release date in 2016.

1.2. Trust Negotiations

Negotiated trust of the web server happens through a series of steps where the client asks the server to prove its identity by verifying the public key the server provides at the client's request. The client then confirms that the server can be trusted by looking in the client's trusted list in its own browsers root store. Figure 1 provides the client steps needed to validate site trust when a user accesses a site secured with a TLS certificate.

1. The Certificate Authorities public key is distributed in the web users' browser.
2. To secure their site, a website owner purchases a certificate from a CA that is in most or all of the of the browser's trust lists.
3. A web user validates the website public key in their browser root store. The client initiates the request to communicate over TLS.
4. The server responds with its public key.
5. The client validates the server's key by confirming that it matches with a CA root that is in its trust list.

Sandra E Dunn, sandra.dunn@hp.com

© 2015 The SANS Institute Author retains full rights.

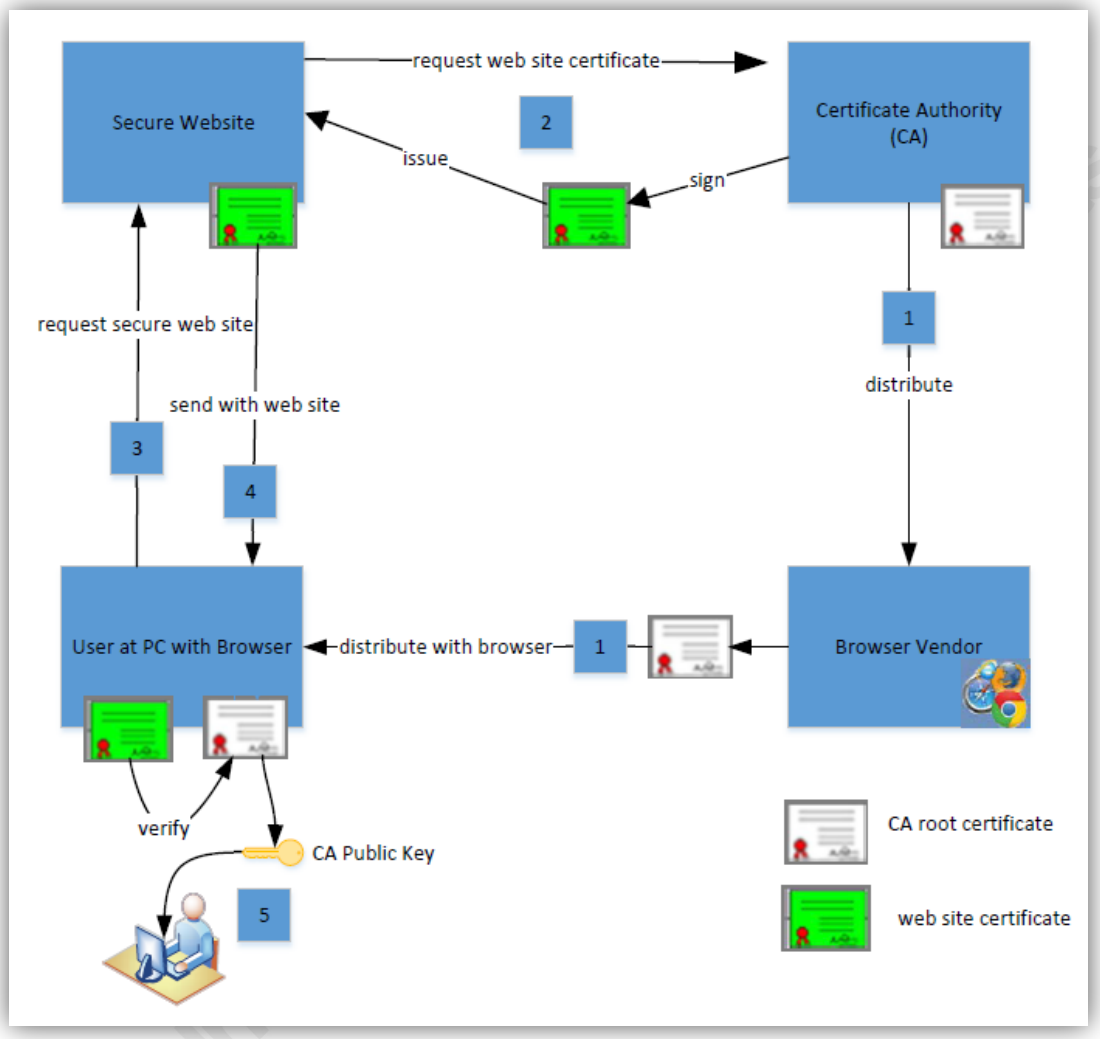


Fig. 1 Client browser validating server identity workflow Rouge-ca.com

Sandra E Dunn, sandra.dunn@hp.com

© 2015 The SANS Institute Author retains full rights.

1.3. Types of TLS Certificates

There are different types of TLS certificates for securing websites that provide different levels of validation by the CA issuing the certificate. The certificates can be purchased for a single domain, for all subdomains, or for multiple sites listed in the subject alternative field on the certificate.

- Domain Validated (DV) certificates validate an organization's domain name and domain control. DV certificates use 256-bit encryption, are the most common types of certificates purchased, and are the least expensive.
- Organization Validation (OV) certificates validate the website owner's organization data, the domain, and the administrator. They are more expensive than DV certificates but are not very common.
- Extended Validation (EV) certificates require the highest level of validation of any domain ownership. Before a CA can offer EV certificates, the CA must go through an independent audit by a web governing body. When requesting an EV certificate, the site owner must confirm its legal identity, documented authorization to purchase the EV certificate, documented operational presence, physical presence, and the legal identity of the website owner. EV certificates are the most expensive and are not very common. Access to a site over HTTPS that changes the URL bar green indicates the site has been issued an EV certificate (CA/Browser Forum, June 2015).
- Self-Signed Certificates are signed by a non-CA Public Key Infrastructure (PKI, and they do not chain to a trusted CA authority.
- The Wildcard option is available for DV and OV certificates. A wildcard certificate secures an unlimited number of first-level subdomains on a single domain name.
- Subject Alternative Name (SAN) certificates provide the option to secure multiple sites listed by their fully qualified domain names on one certificate.

© 2015 The SANS Institute Author retains full rights.

1.4. Rapid Growth in TLS Certificate Use

The increase of negative internet security events has fueled the rapid growth in TLS Certificate deployments. This demand can be attributed to four main causes:

1. increased focus on privacy (the so-called "Snowden effect")
2. CA Security Council initiatives such as Always-on SSL
3. web industry leaders, such as Google, promoting better security
4. government-led requirements

Research provided by the Ponemon Institute's 2015 "Cost of Failed Trust Report: Trust Online is at the Breaking Point" (Ponemon Institute, 2015) shows that deployments of TLS certificates for web servers, network appliances, and cloud services are increasing at an amazing rate of over 34 % growth per year.

An increase in TLS certificates also comes indirectly from search engines, which prioritize HTTPS when weighting search engine results, benefiting businesses that implement TLS certificates. Higher search returns can provide impactful results since the additional web visitor traffic can lead to increased profits from additional purchases (Schwartz, 2014).

1.4.1. The Snowden Effect

History is still being written on whether Edward Snowden is a bold whistleblower or the worst of the malicious insiders (Blake, Gellman, Miller, 2013), but one thing is certain: he attracted attention to protecting data privacy. His disclosure of details of PRISM and NSA surveillance has both businesses and private citizens taking additional precautions to protect their data. Termed the "Snowden Effect", it is a point of reference for security and privacy advocates. Sandvine, a network equipment company, compared the volume of encrypted traffic before Edward Snowden revealed the NSA secret listening to the volume of encrypted traffic after, and found that users encrypting their traffic had more than doubled. (Finley, 2014)

1.4.2. Always-On SSL

The Always-On SSL (AOSSL) initiative has increased the purchase of TLS certificates by government and business. Always-On SSL enforces HTTPS for all communication in a web session, encrypting all communication between the client and

© 2015 The SANS Institute Author retains full rights.

server, not just the login or checkout pages that most commonly was encrypted in the past. Using HTTPS for all page content eliminates the risky practice of sending "mixed content": using both HTTP and HTTPS calls on the same page that could be used to exploit a site visitor. It is important to configure AOSSL so that it uses HTTPS even if a user types "HTTP" into the URL using Strict Transport Security (HSTS). Companies that have moved to AOSSL include Reddit, Google, Microsoft, Facebook, PayPal, Twitter, and Yahoo (Wilson, n.d.).

On June 8, 2015, the U.S Federal Government supported AOSSL with the HTTPS-Only Standard mandate. Tony Scott, the Federal CIO, sent memorandum M-15-13 to the heads of executive departments and agencies, requiring that all publicly accessible Federal websites and web services only provide service through a secure connection. This memorandum requires that Federal agencies deploy HTTPS on their domains using the following guidelines:

- Newly developed websites and services at all Federal agency domains or subdomains must adhere to this policy upon launch.
- Existing websites and services, agencies should prioritize deployment of TLS certificates based on the risk to the data
- Agencies must make all existing websites and services accessible through a secure connection (HTTPS-only, with HSTS) by December 31, 2016.
- The use of HTTPS is encouraged on intranets, but not explicitly required.

Pulse, which is viewable at https://pule.cio.gov and shown in Figure 2, is a public dashboard that tracks the current status of government website migration to the mandated requirement for HTTPS. Pulse was launched on June 2, 2015. The Pulse dashboard provides simple up to date information on which sites have implemented TLS certificates to support HTTPS and the remaining percent of sites that still needs to migrate to the new standard. The Pulse site also tracks the percentage of government sites that have migrated to the new government analytical program that tracks how people use government sites which is the percentage number on the right in Figure 2. (Scott, 2015)

© 2015 The SANS Institute Author retains full rights.

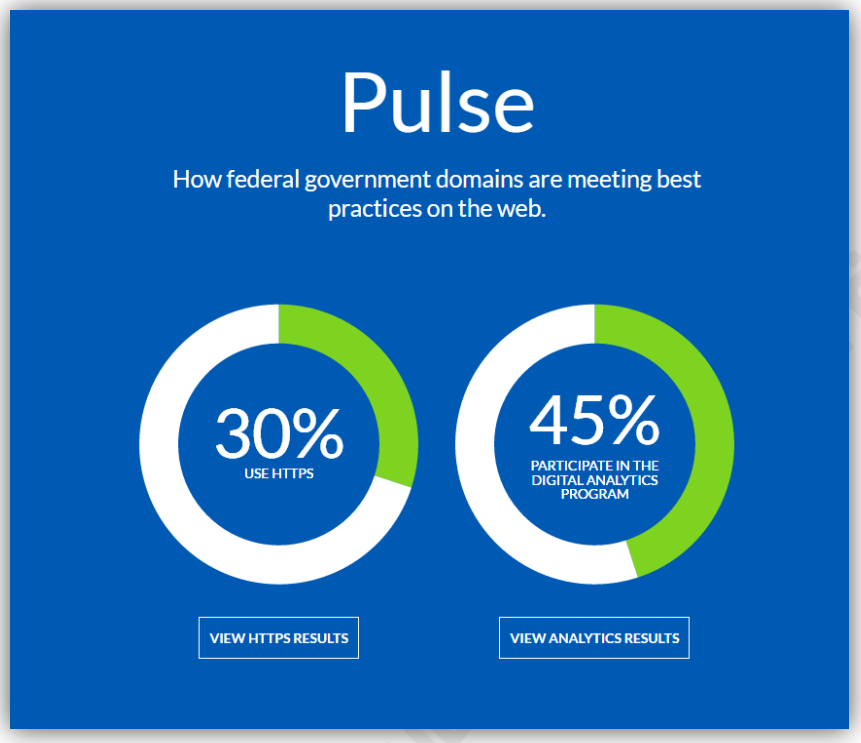


Fig. 2 Screenshot of Pulse dashboard, pulse.cio.gov

The mandate that all U.S. Government websites use TLS certificates is expected to drive the same secure best practices to other website providers.

1.4.3. Stricter TLS Security Warnings

In December of 2014, Google released a developer version of Chrome that included settings that will warn users that a site is insecure if any content is delivered unencrypted over HTTP. Google has not officially announced the inclusion of this feature in a stable release of Chrome, but website owners should prepare to support this stricter version. Google's Chrome browser maintains almost 50% of the browsers used on the desktop and use of any stricter security settings in Chrome has a significant impact on overall user experience. Chrome's browser dominance compared to other browsers is shown in Figure 3.

Sandra E Dunn, sandra.dunn@hp.com

© 2015 The SANS Institute Author retains full rights.

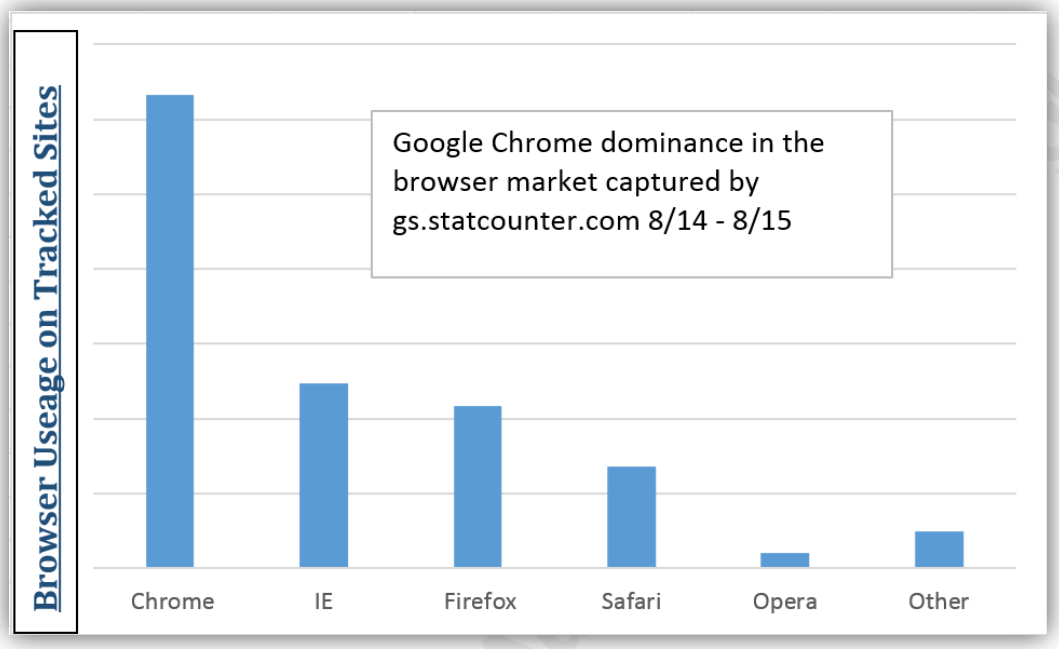


Fig. 3 gs.statcounter.com

1.4.4. Inadequately Secured TLS Certificates

Sites such as the SSL Pulse provide proof of the current state of poor certificate management. SSL Pulse scans TLS-enabled sites monthly based on Alexa's list of the most popular sites and provides a dashboard of the security health. August 3, 2015 data shown in figure 4 shows only a small fraction, 23.4 %, of the currently HTTPS-enabled sites are secure.

© 2015 The SANS Institute Author retains full rights.

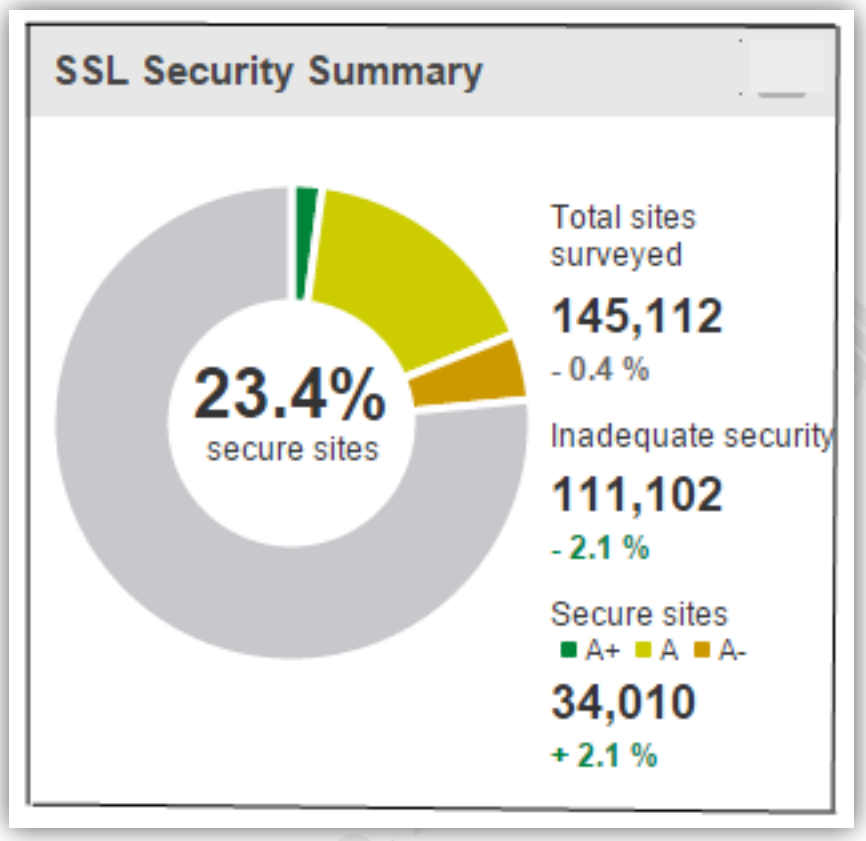


Fig. 4 Sites with secure TLS configuration, trustworthyinternet.org

Users encounter browser warnings so often from mismanaged certificates they mostly ignore them. They numbly click through the warnings without reading them and without considering they may be in danger. The NSA PKI site shown in Figure 5 is an example of how difficult, confusing, and potentially dangerous TLS security is for site users. Visitors to this site, which ironically is on Public Key Infrastructure (PKI) security, could easily be misdirected to a different site since they have been conditioned to ignore the browser warning.

Sandra E Dunn, sandra.dunn@hp.com

© 2015 The SANS Institute Author retains full rights.



Fig. 5 Misconfigured TLS certificate on NSA site, nsaarc.net

1.5. Expensive Impact of Unmanaged and Expired Certificates

The rapid increase of TLS certificates, which are time-consuming and difficult to manage manually, has led to frustrated administrators and insecure environments. A Ponemon study sponsored by e-Security found that 56% of people responsible for TLS certificates rated their pain in managing certificates as a "seven" on a scale of one to ten. (Ponemon Institute, 2015 Global Encryption & Key Management Trends Study). Not only is manually managing certificates time consuming and causing increased risk due to bad manual configuration of certificates, it also misses addessing rogue certificates. This is because a manual process tracks the known certificates not the unknown certificates. Rogue certificates, in most cases, have been purchased or accepted outside of the established policy by a time crunched developer or well meaning, but frustrated platform manager. Unfortunately the rogue certificates could also be there for more sinister reasons, attempting to misguide people's trust for malicious intent. Automating

© 2015 The SANS Institute Author retains full rights.

certificate management saves time, reduces risk from bad manual certificate configuration and also addresses the rogue certificate danger. A full featured automated certificate management tool includes a certificate discovery agent that immediately sends an alert when a rogue certificate is discovered so it can be tracked and remediated.

Poor certificate management can lead to costly service disruption, which is what happened in the case of Microsoft Azure (Mello, 2013). In February of 2013, Microsoft engineers scheduled an update to the TLS certificates with other higher priority updates. This pushed the release of the update of the TLS certificates past the currently deployed TLS certificates expiration date. This push caused a major disruption since the certificates failed client TLS connection attempts. Microsoft provided refunds to customers for 52 of the Azure services, which included XBOX live.

Badly managed certificates have also impacted embedded devices, sometimes called "The Internet of Things." This harrowing scenario was experienced by merchants on December 7, 2014, when older models of the Hypercom credit card terminals quit working. After the 12/14/14 certificate expiration date, when the devices were power-cycled, they displayed a blank screen with no indication of why they weren't working. Panicked merchants contacted Hypercom support, concerned that they had been the victim of a malicious attack, only to discover that the issue was an expired certificate. Updating the certificate in most cases could be resolved with a field call, but some devices had to be shipped back to the manufacturer and then returned to the disgruntled merchant. The total cost to the impacted retailers is not available, but one retailer told Brian Krebs, "Mass extinction of my Point of Sale (POS) devices at the manufacturer level was never on my list of scenarios that would wreck my day at retail. It is now" (Krebs, 2014). .

1.6. The Business Case for Enterprise Key Management

The blue bar in Figure 6 represents all the critical and severe vulnerabilities from Company X's monthly network scan data where unmanaged TLS certificate issues are consistently highest volume and highest risk. The gray bar shows the total number of captured vulnerabilities reduced by 14 % when SSL / TLS certificates were remediated. Managing TLS certificates with an EKCM can easily and efficiently manage TLS

© 2015 The SANS Institute Author retains full rights.

certificates and provide a significant return on investment to the business. These savings are accomplished by reducing the lost hours required for manual certificate management and by reducing the risk from TLS certificates that are unmanaged. Automating certificate management further provides a significant financial benefit from higher search engine results from supporting TLS across all website pages. Many business that manually manage certificates miss the benefits gained from higher SEO search results gained from supporting TLS across their sites because their IT teams can't provide the people resources to maintain the certificates.

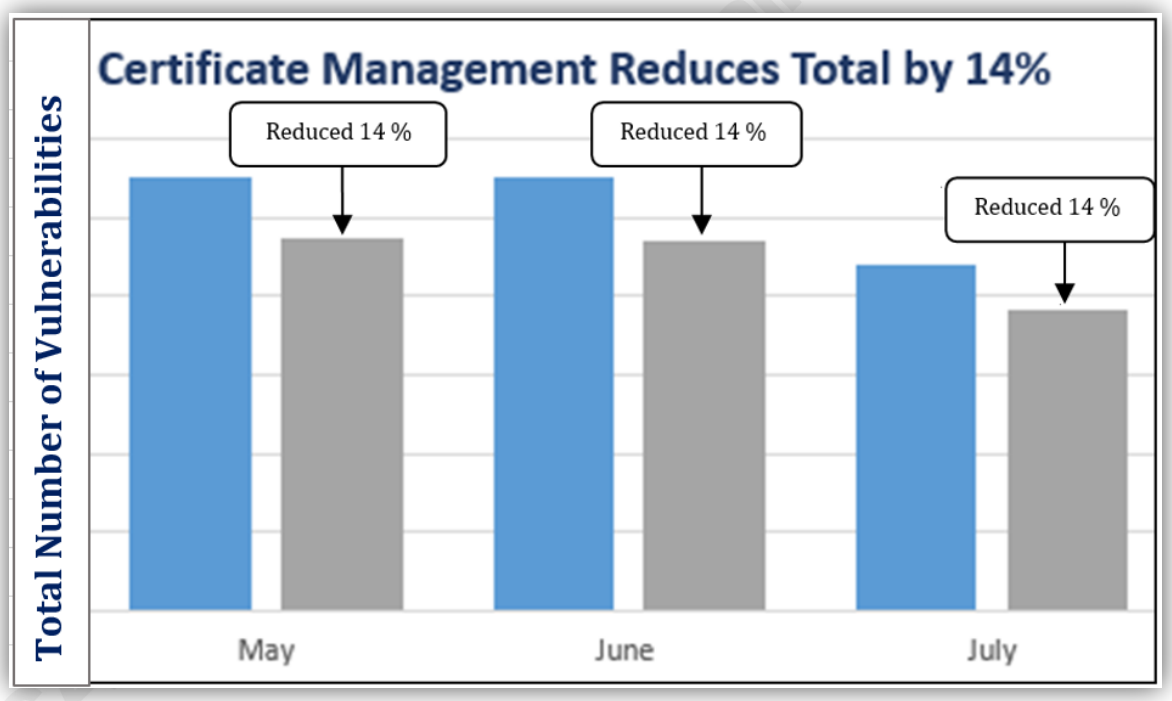


Fig. 6 Total number of vulnerabilities before and after remediating TLS Dunn, Sandra

The data in Figure 7 breaks out the specific types and number of TLS vulnerabilities. The most significant remediation concern is the number of untrusted TLS /SSL server X.509 certificates which is circled in red below.

Sandra E Dunn, sandra.dunn@hp.com

© 2015 The SANS Institute Author retains full rights.

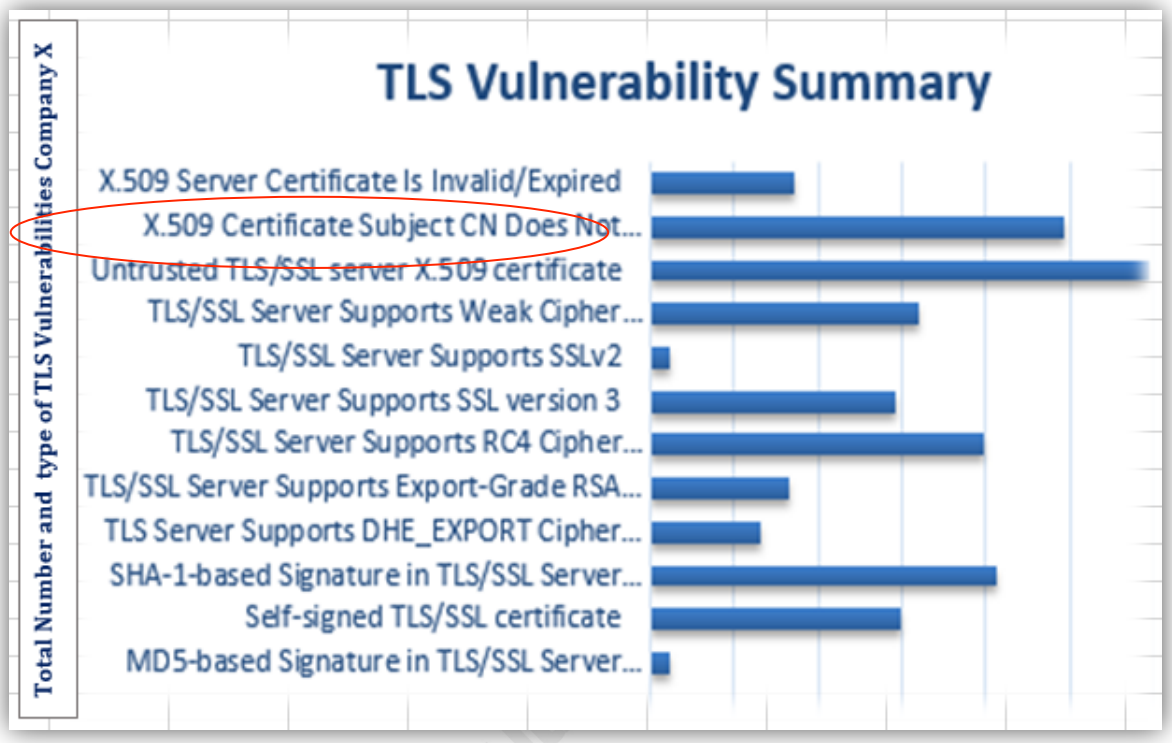


Fig. 7 Volume and type of TLS vulnerabilities Dunn, Sandra

1.7. Difficulties in Certificates Management

Without a policy, managed process, or centrally managed EKCM, website owners or their infrastructure support team are left to solve the TLS certificate deployment on their own. Remediation attempts for Shellshock, Heartbleed, and Poodle fully exposed mismanaged environments. Vulnerability teams discovered how mismanaged the certificates were when trying to track down issue owners. Determining who handled certificate management and remediation was very challenging. Without a documented strategy, it was unclear whose job it was to manage the certificates and who should be held accountable. Assigning responsibility for remediation often resulted in the assigner being sent in a loop, to the application owner, then to the web infrastructure team, then to IT, and back to the application owner. This leaves the remediation team frustrated and the certificate still vulnerable. Another certificate management obstacle is that vulnerability scan data only provides insight into the types and number of TLS vulnerabilities discovered. It does not report a certificate if it is a legitimate TLS certificate deployed

© 2015 The SANS Institute Author retains full rights.

from an unauthorized CA. For example, if Symantec certificates are the only enterprise approved certificate vendor, a vulnerability scan will not report if a certificate roots to the GoDaddy CA. Unless the GoDaddy certificate has vulnerabilities, it goes unnoticed. An Aberdeen group study data used in Venafi Return on Investment (ROI) calculations estimates that manual management of certificates requires an average of 4.5 hours per year per certificate (Aberdeen Group, 2008). Figure 8 provides an example of a manual TLS management workflow that shows the many steps needed for manually managing certificates and why it is so time-consuming.

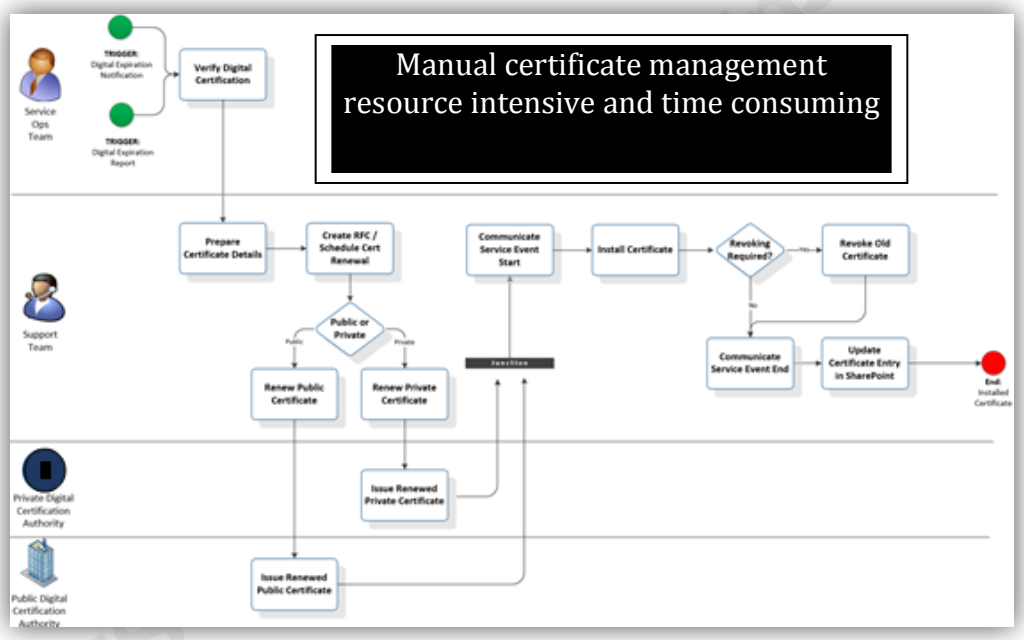


Fig. 8 Workflow of manually managing TLS certificates, Varnell, Bill

For large enterprise environments, transitioning from a manual to an automated certificate management saves time, money, and prevents the misconfigurations that plague manual TLS management processes.

The financial business benefit of automating the TLS certificate process is accomplished by evaluating the total cost of the current manual process and the estimated risk of un-remediated TLS certificate vulnerabilities, and comparing the total to the

© 2015 The SANS Institute Author retains full rights.

investment for an automated TLS certificate management tool. The calculated dollar difference determines if it is a good business investment.

For example, a business that manually manages 7604 certificates with a conservative growth rate of 20 % can reduce the amount of IT money spent on certificate management by over 75 % implementing an EKCM in just the first year. The financial benefits increase to 80 % when comparing manual management and automated management over three years, as shown in Figure 9 (Dunn, 2015).

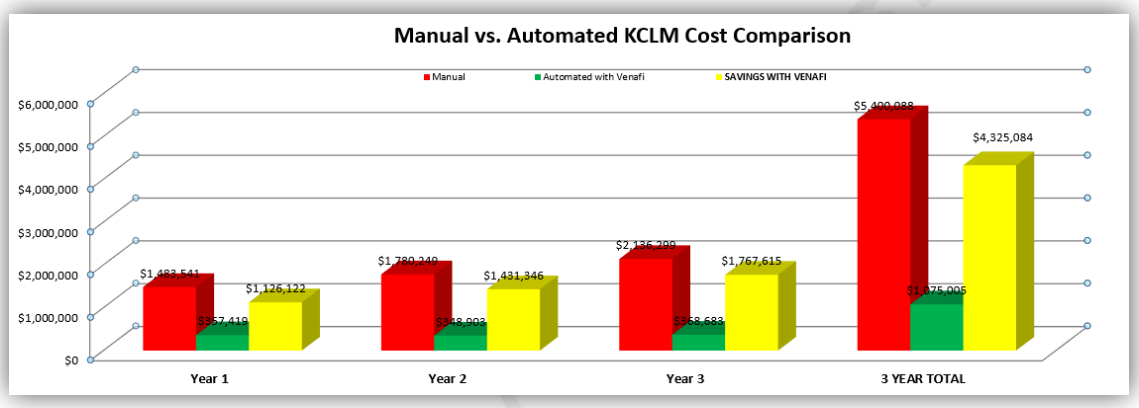


Fig. 9 Estimated savingsVenafi ROI Calculator, Dunn, Sandra

1.8. HTTPS as an SEO Ranking Signal

In August of 2014, Google announced that the use of HTTPS would improve a site's ranking results returned to a querying search engine user. With Google's over 66% percent of market share in search, any change in their SEO ranking can significantly change how many web visitors a site receives. The percentage of searches on Google compared to other search engines are shown in Figure 10. Bing (Microsoft, 2015) and Yahoo (Cowan, 2014) have also announced better rankings for HTTPS-only sites.

Sandra E Dunn, sandra.dunn@hp.com

© 2015 The SANS Institute Author retains full rights.

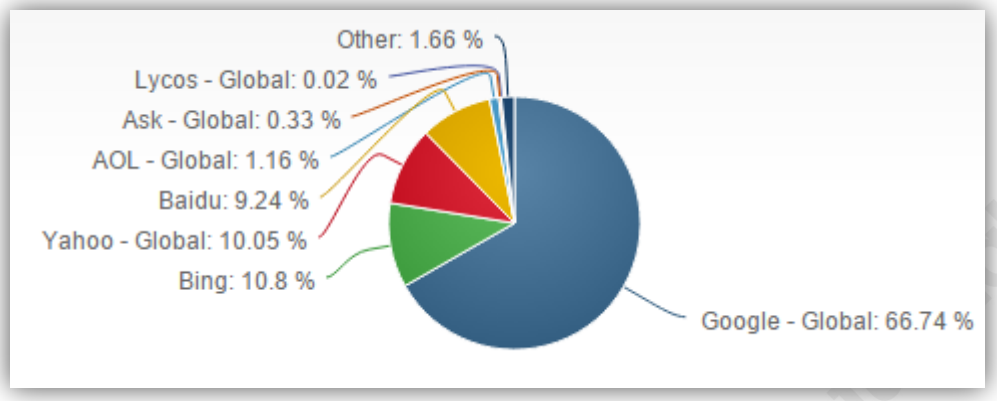


Fig. 10 Google share of web searches, netmarketshare.com

1.8.1. The Importance of SEO Ranking

SEO, or Search Engine Optimization, is the process of using techniques to earn higher ranking placements on Search Engine Results Pages (Tarcomnicu, 2015). Moving the ranking of a specific search to the front page and as high as possible in the search results can result in a significant financial benefit (K. Bocek, personal communication, June 19, 2015).

Vicqui Chan, a Senior Manager of the SEO team at Hewlett-Packard (HP), estimates that a large enterprise can expect 2-3% increase in SEO search ranking gains from supporting HTTPS everywhere. As an example, a large company with a 1.9 % Average Order Size Conversion (AOS) could increase order volume between $570,000 and $855,000 per week by increasing the SEO search by 2 %. Multiply 52 weeks by $570,000 equals $29,640,000 per year. Using a conservative industry average margin of 10 %, a company has the potential of increasing their profits by $2,964,000 implementing TLS certificates for HTTPS across their site (Dunn, 2015).

2. Best Practices for Web Certificate Management

The Council on Cyber Security Top 20 Security Controls is a list of the most important controls for an organization to evaluate as best practices for protecting valuable assets and network hardening. The objective is to prioritize on effectiveness, with a smaller list of controls to provide the best return on investment and to have the highest

© 2015 The SANS Institute Author retains full rights.

positive impact on an organization's overall security landscape (Council on Cyber Security Controls, n.d.). Version 5.1 Critical Security Control 17 targets controls for data protection and includes specific recommendations for TLS management.

2.1. CSC 17-2: Verify that cryptographic devices and software are configured to use Publicly-vetted algorithms

A word of caution for this control; exuberant security operation people may make the mistake of maximizing every key length and disabling all supported previous versions of a cipher suite. This could cause legacy applications to break since they can't support the new changes. The changes disable customers accessing the site, slows performance, and has angry website owners mobbing the security operations cubicles. The best TLS deployment finds the right balance between security and web client usability.

The recommended guidance for this control are to use TLS 1.2 if the client supports TLS 1.2, and the other less secure versions of TLS 1.1 or TLS 1.0 only if there is a negative business impact by not supporting them. The benefits of TLS 1.2 over TLS 1.1 are TLS 1.2 resists the BEAST[1] attack, has stronger cipher suites, and reduces the use of RC4 by cipher suites (Thayer, 2013).

Applications that require TLS 1.0 should go through a formal risk acceptance process since TLS 1.0 is vulnerable to Cipher Chaining Attacks and Padding Oracle attacks (Poodle) CVE-2014-8730 and the business should acknowledge and accept the risk if they use it. Companies that maintain PCI compliance should plan their migration to TLS 1.1 or 1.2 now since TLS 1.0 is prohibited in PCI DSS 3.1 after June 2016. NIST SP 800-51 requires TLS 1.2 or TLS 1.1. TLS 1.0 use has been deprecated and is prohibited for government applications.

For configuration of the private keys use 2048-bit RSA or 256-bit ECDSA private keys for all your servers. If there is a security requirement for a key size larger than 2048 bits ECDSA is a better choice for performance (Ristic, 2015). The private key hashing function should be configured to use SHA2. Moving to SHA2 is required by the end of 2016 and is needed to maintain compliance for PCI and NIST.

Configure servers to use secure TLS Cipher Suites. A "Cipher Suite" is the collective name for the sum of different algorithms used to negotiate TLS between the client and the server. NIST SP-800 52 Guidelines for the Selection, Configuration, and Use of

© 2015 The SANS Institute Author retains full rights.

Transport Layer Security (TLS) Implementations provides detailed guidance on which cipher suites are required to support for government applications. Most TLS cipher suite recommendations refer to this standard.

Cipher suites have the form:

> TLS_KeyExchangeAlg_WITH_EncryptionAlg_MessageAuthenticationAlg. For example, the cipher suite TLS_RSA_WITH_AES_128_CBC_SHA uses RSA for the key exchange, AES-128 in cipher block chaining mode for encryption, and message authentication with HMAC_SHA (NIST.SP.800-52r1, pg 14).

Ensure the server supports Forward Secrecy by using ECDHE suites. Forward Secrecy enables secure conversations that are not dependent on the server's private key. By generating a unique session key for each session that the web client initiates, communication remains protected even if the server's private key was compromised. Disable client initiated renegotiation since there aren't any scenarios where a client would need to renegotiate the connection, and there are attack scenarios where client renegotiation is used in an impersonation attack (Ristic, 2014).

Avoid websites having mixed content where part of the content is delivered over a secure HTTPS using a TLS Certificate and other calls are made over an unsecured HTTP connection. The mixing of types of content calls frequently happens when calls to other resources such as images, files, or JavaScript are requested. To protect clients even when they misguidedly initiate a call over HTTP, enable HTTP Strict Transport Security (HSTS). When HSTS is implemented at the server, it automatically converts HTTP requests to HTTPS requests. (The Critical Security Controls for Effective Cyber Defense, v.5.1, n.d, p.92).

© 2015 The SANS Institute Author retains full rights.

2.2. CSC 17-3: Perform an assessment of data to identify sensitive information that requires the application of encryption and integrity controls

Instead of deploying encryption and integrity controls across the network do the necessary project research to determine what data does need to be protected, who needs access to it, and from where. Often this research determines more data can be declassified from requiring stringent controls and identifies really important data that needs even tighter controls saving both time and money. (The Critical Security Controls for Effective Cyber Defense, v.5.1, nd, p.92).

2.3. CSC 17-10: Only allow approved certificate authorities (CAs) to issue certificates within the enterprise

Review and verify each CA's certificate practices statement (CPS) and certificate policy (CP). The level of trust in an organization's certificate is anchored in the trust of the root CA. Microsoft, Adobe, Oracle, Google, still rely on external CA's and the default root stores provided by browser vendors. The turbulent internet security environment is driving organizations toward needing additional trust layers such as the additional trust layer provided by Google's Certificate Transparency, Key Pinning, TrustNet, or CA Whitelisting.

Google's Certificate Transparency project provides a site where the certificates that have been issued by a CA are publically viewable. That way domain owners can validate that a certificate has not mistakenly been issued for a domain either maliciously or mistakenly [RFC6962].

Key Pinning is another way to add a trust layer. Key Pinning white lists, or stated another way, associates a domain with their expected public key X.509 certificate. Pinning adds a layer of trust by leveraging the knowledge of what the expected public key should be.

Venafi provides the added trust layer with their TrustNet solution. TrustNet scans the internet for misuse and potentially dangerous certificate key and creates a blacklist to avoid them (Venafi, 2015).

Sandra E Dunn, sandra.dunn@hp.com

© 2015 The SANS Institute Author retains full rights.

Dmitry Dain, CTO of Virgil Security, recommends an even more conservative Trust Model. He designs certificate environments where an external CA is viewed as untrustworthy and defaults to deny trust until reviewed, validated, and then accepted as trustworthy (D. Dmitry, personal communication, August 25, 2015). (The Critical Security Controls for Effective Cyber Defense, v.5.1,n.d, p.92).

2.4. CSC 17-11: Perform an annual review of algorithms and key lengths in use for protection of sensitive data

Key lengths and algorithms should be reviewed annually to ensure all previously unknown risks are considered, and sensitive data is still protected. Shellshock, Heartbleed, and Poodle vulnerabilities show how rapidly guidance on which algorithms and key lengths are considered secure can change. To shorten the length of time insecure versions of TLS must be supported for web visitor compatibility consider adding a splash page that reminds web visitors to update their systems to the latest available supported browser versions.

2.5. CSC 17-14: Define roles and responsibilities related to management of encryption keys within the enterprise; define processes for life-cycle

Defining roles and responsibilities ensures certificates are managed, up to date, and user access to certificate keys is controlled, logged, and audited. If there is an unexpected certificate incident, defining roles and responsibilities ensures remediation roles are clear, and remediation is efficient and effective. (The Critical Security Controls for Effective Cyber Defense, v.5.1,n.d, p.92).

2.6. CSC 17-15 Where applicable, implement Hardware Security Modules (HSMs) for protection of private keys (e.g., for sub CAs) or Key Encryption Keys

A Hardware Security Module (HSM) is a hardware device that is designed for one purpose: to protect private keys. Protecting private keys with the additional physical and administrator controls is required when compromise of the key could have a severe financial impact or devastating personal impact to clients such as the loss of health records. HSMs are typically located in secure environments and managed with additional procedural controls. These include isolation on the network, housed in locked cages, and

© 2015 The SANS Institute Author retains full rights.

protected by security cameras. Ensure compliance with FIPS 140-2 Level 3. FIPS 140-2 which is the U.S. Government computer security standard for accrediting cryptographic modules. It has four levels of security that a system can be accredited to with Level one being the lowest and Level four the highest (FIPS PUB 140-2, 2001). (The Critical Security Controls for Effective Cyber Defense, v.5.1,n.d, p.92).

2.7. NIST SP 800-57 Key Management recommendations. The recommendation guides are broken into three parts:

The NIST SP 800-57 Key Management Recommendations are guides that provide the necessary security implementations for managing keys in Federal government environments. NIST standards provide the common baseline that businesses use for minimal security requirements. The guide is broken into three parts (NIST, 2005).

Part 1: General guidance and best practices for managing key material.

Part 2: Best Practices: provides guidance on policy, security planning, documentation

Part 3: Provides guidance on common IT systems. Figure 12 represents the four management stages in the certificate lifecycle.



NIST Key Lifecycle Management

- **Pre-Operational process**: ensures environment is secure to generate keys includes **Key Establishment Key Registration, and Key Distribution**
- **Operational phase**: Keys are in the active state includes **Key Storage, Key Backup, Key Recovery, Key Rekey**
- **Post-Operational Archive** : Key is no longer actively used includes **Key Recovery, Key Deregistration, Key Destruction, and Key Revocation**
- **Destroyed phase: Key is Destroyed**

Sandra E Dunn, sandra.dunn@hp.com

© 2015 The SANS Institute Author retains full rights.

Fig. 12 Dunn, Sandra

3. Conclusion

An Enterprise Key Certificate Management System provides a best-in-class solution for TLS certificate management. An EKCM automates certificate management, reduces manual overhead, eliminates certificates deployed with insecure configurations and minimizes the risk from rogue certificates.

The financial gain of increased SEO ranking from deploying HTTPS across the site makes deploying an Enterprise Key Management System a good security decision and a huge financial win. An average enterprise company can reduce the cost of certificate management by 75 % in the first year and gain $2,964,000 by improving the SEO search results deploying HTTPS across their site. Deploying an Enterprise Key Management System provides both better security and financial gain to a company's bottom line. Automating certificate management provides one of those rare opportunities to combine a security win with economic gain. It's an opportunity for a CISO to be a hero both to their IT staff and in the board room.

1 Researchers Thai Duong and Juliano Rizzo demonstrated the Browser Exploit against SSL /TLS referred to as the Beast attack as a proof of concept on September 23, 2011.

4. References

.

Aberdeen Group,(2008,October) Managing Encryption[PDF] file. Retrieved September 3, 2015, from emc.com: http://www.emc.com/collateral/analyst-reports/rsa-aberdeen-managing-encryption.pdf

Barker, E., Barker, W., Lee, A., (2005, December) Guideline for Implementing Cryptography in the Federal Government. Retrieved September 4, 2015, from csrc.nist.gov: http://csrc.nist.gov/publications/nistpubs/800-21-1/sp800-21-1_Dec2005.pdf

Sandra E Dunn, sandra.dunn@hp.com

© 2015 The SANS Institute Author retains full rights.

Blake, A., Gellman, B., Miller, G., (2013, June 9) Edward Snowden Comes Forward as Source of NSA Leaks, Retrieved September 3, 2015, from washingtonpost.com: http://www.washingtonpost.com/politics/intelligence-leaders-push-back-on-leakers-media/2013/06/09/fff80160-d122-11e2-a73e-826d299ff459_story.html

CA/Browser Forum, (2015, June 25) Guidelines for the Issuance and Management of Extended Validation Certificates, Retrieved September 3, 2015, from caborum.org: https://cabforum.org/extended-validation/

Council On Cyber Security (n.d.) Critical Security Controls v5.1. Retrieved November 02, 2014 from Council on Cyber Security: counciloncybersecurity.org: http://www.counciloncybersecurity.org

Cowan, Jennifer, (2014, January 23) Yahoo Makes Move to Secure Search by Default, Retrieved September 3, 2015, from sitepronews.com: http://www.sitepronews.com/2014/01/23/yahoo-makes-move-secure-search-default/

Dierks, T., Rescorla, R.,(2008, August) The Transport Layer Security (TLS) Protocol Version 1.2, RFC 5246. Retrieved September 2, 2015, from tools.ietf.org: https://tools.ietf.org/html/rfc5246

Dunn, Sandra, (2015, May, June, July) Normalized TLS Research Data. Unpublished raw data.

Evans, C., Palmer, C., Sleevi, R., (2015, April) Public Key Pinning Extension for HTTP, RFC 7469. Retrieved September 4, 2015, from tools.ietf.org: https://tools.ietf.org/html/rfc6962

Filkins, Barbara (2015, June) New Critical Security Controls Guidelines for SSL/TLS Management [PDF file]. Retrieved September 2, 2015 from SANS.org: https:// www.sans.org/reading-room/whitepapers/analyst/critical-security-controls-guidelines-ssl-tls-management-35995

Finley, Klint, (2015, May 16) Encrypted Web Traffic More Than Doubles after NSA Revelations, Retrieved September 3, 2015, from wired.com: http://www.wired.com/2014/05/sandvine-report/

Gerstein, Josh, (2014, January 17) Obama Hits Snowden Over NSA Leaks. Retrieved September 3, 2015, from politico.com:

Sandra E Dunn, sandra.dunn@hp.com

© 2015 The SANS Institute Author retains full rights.

http://www.politico.com/story/2014/01/barack-obama-edward-snowden-nsa-leaks-102316

Krebs, Brian (2014, December) 'Security by Antiquity' Bricks Payment Terminals, Retrieved September 3, 2015, from Krebsonsecurity.com: http://krebsonsecurity.com/2014/12/security-by-antiquity-bricks-payment-terminals/

Laurie, B., Langley, A., Kasper, E., (2013, June) Certificate Transparency RFC 6962. Retrieved September 4, 2015, from tools.ietf.org: https://tools.ietf.org/html/rfc6962

Mello, John P., (2013, February 27) Azure Outage Births Free Cert Monitoring Software. Retrieved September 3, 2015, from csoonline.com: http://www.csoonline.com/article/2133030/security-awareness/azure-outage-births-free-cert-monitoring-software.html

Microsoft, (2015, 15 June) Bing Moving to Encrypt Search Traffic by Default. Retrieved from blogs.bing.com: https://blogs.bing.com/webmaster/2015/06/15/bing-moving-to-encrypt-search-traffic-by-default/

NIST, (2001, May) FIPS Pub 140-2 Security Requirements for Cryptographic Modules. Retrieved September 4, 2015, from csrc.nist.gov: http://csrc.nist.gov/publications/fips/fips140-2/fips1402.pdf

Polk, T, McKay, K., Chokhani, S (2014, April) Guidelines for the Selection Configuration, and Use of Transport Layer Security (TLS) Implementations. Retrieved September 4, 2015, from NVLpubs.nist.gov: http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-52r1.pdf

Ponemon Institute, (2015) Ponemon 2015 Cost of Failed Trust Report: Trust Online is at the Breaking Point. Retrieved September 3, 2015, from Venafi.com: https://www.venafi.com/collateral/wp/ponemon-research-2015-cost-of-failed-trust-report

Ristic, Ivan, (2014, December) SSL/TLS Deployment Best Practices. Retrieved September 4, 2015, from ssllabs.com: https://www.ssllabs.com/downloads/SSL_TLS_Deployment_Best_Practices.pdf

Ristic, Ivan, (2015). Bulletproof SSL and TLS. London U.K.: Feisty Duck.

Sandra E Dunn, sandra.dunn@hp.com

© 2015 The SANS Institute Author retains full rights.

Scott, Tony, (2015, June 8) Memorandum for the Heads of Executive Departments and Agencies: Policy to Require Secure Connections across Federal Websites and Web Services [PDF file]. Retrieved September 3, 2015, from whitehouse.gov: https://www.whitehouse.gov/sites/default/files/omb/memoranda/2015/m-15-13.pdf

Schwartz, Barry, (2014, August 7) Google Starts Giving A Ranking Boost To Secure HTTPS/SSL Sites. Retrieved September 3, 2015, from searchengineland.com: http://searchengineland.com/google-starts-giving-ranking-boost-secure-httpsssl-sites-199446

Tarcomnicu, Felix (2015, March) 40 Most Important SEO Ranking Factors. Retrieved September 4, 2015, from blog.monitorbacklinks.com: https://blog.monitorbacklinks.com/seo/seo-ranking-factors/

Thayer, Wayne (2013, September 19) It's time for TLS 1.2. Retrieved September 5, 2015 from: casecurity.org: https://casecurity.org/2013/09/19/its-time-for-tls-1-2/

Wilson, Ben (n.d) Always-On SSL. Retrieved September 5, 2015, from casecurity.org: https://casecurity.org/whitepapers/

Venafi, (2015) Mitigate Trust-Based Attacks with Global Certificate Reputation Service. Retrieved September 5, 2015, from Venafi.com: https://www.venafi.com/assets/pdf/wp/Veanfi_TrustNet_Global_Certificate_Reputation_Service_white_paper.pdf

Sandra E Dunn, sandra.dunn@hp.com

© 2015 The SANS Institute Author retains full rights.