WIDEPOINT WHITE PAPER

What You Can Do Before Zero Day: Mitigating the Risks of Future Threats

This paper explores what the Heartbleed Vulnerability should teach us about making Internet transactions secure and ways we can protect against future threats; we also discuss the importance of properly protecting private keys and what that means, why user authentication must evolve beyond simple usernames and passwords, and what that means for Web users.

Contents

Overview

The announcement of the “Heartbleed Vulnerability” on April 8, 2014, brought to light the threats that exist in security practices prevalent on the Internet today. It also taught us that they can be difficult if not impossible to identify in a timely fashion. The vulnerability is also a harbinger of future threats and raises the possibility of threats yet undiscovered that are currently being exploited without any trace or accountability. It took years for us to learn to look for the little lock in the browser address bar confirming a site was secure and that it was OK to go ahead with your transaction, but what does that lock really mean?

Should website users trust every entity that pays for the privilege of displaying that lock? Does the symbol guarantee that proper care and diligence was taken during the issuance of the SSL certificate behind it? Whether buying something online, accessing personal electronic health information through an insurer’s website, or doing online banking, users learned that the little lock was intended to mean “it’s safe.”

On April 8, 2014, we learned that it fundamentally was not safe—and hadn’t been for two years.

What We Should Learn from Heartbleed

Heartbleed refers to a vulnerability in certain versions of the commonly used open source cryptographic libraries, OpenSSL. These cryptographic libraries are intended to make Internet traffic encrypted and secure. A closer look at the US iCert reports since the announcement indicates similar vulnerabilities exist in other products that use or derive its cryptography from a similar source.

Heartbleed created a 64K-sized “hole” that allowed transaction-related data in an unencrypted state to be exposed. This means that shared secrets such as passwords could have been intercepted, hence the widespread advice to consumers to change passwords.

Although inconvenient to website users, changing passwords is not difficult, and in fact many websites reset their users’ passwords, prompting users to create a new one the next time they log in.

But Heartbleed exposed more than shared secrets and other user information that secure websites are supposed to protect.

The OpenSSL Heartbleed vulnerability made it possible to intercept unencrypted transaction-related data, including passwords.

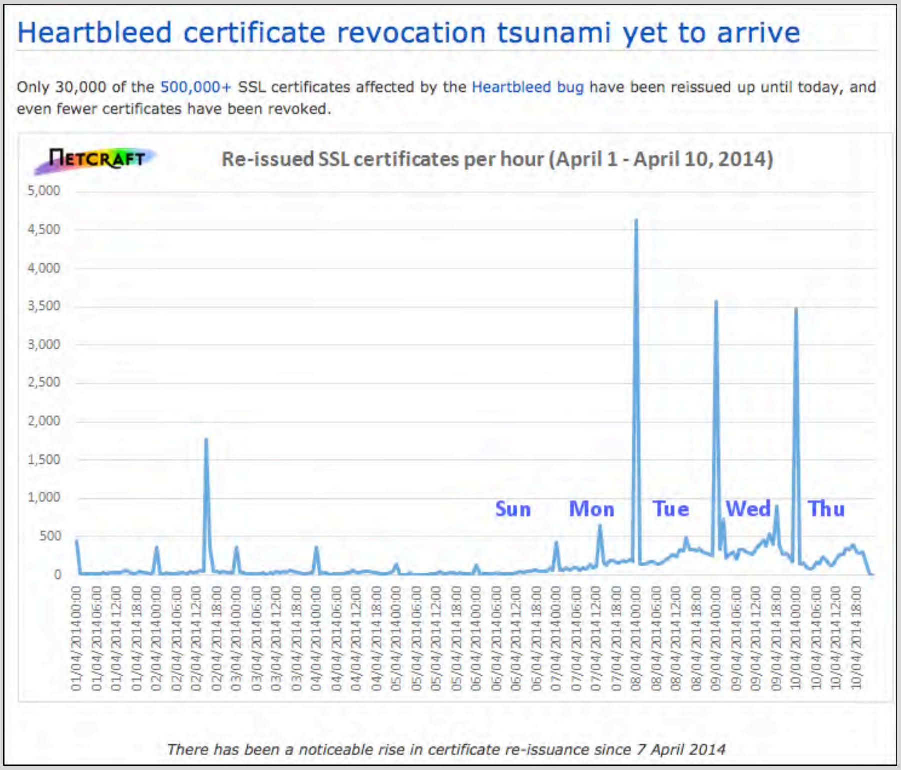
The Importance of Protecting Private Keys

SSL encryption protocols use digital certificates to identify one or both ends of a transaction. Digital certificates are issued to Web servers by trusted third-party Certificate Authorities (CA), like WidePoint, and are used to identify the website you are accessing as well as encrypt the data flowing between your browser and the website. Since the website uses a digital certificate to set up secure communications channels, the private key for that certificate must be available to the Web server in order to establish those connections. This use of the private key is what allowed the exposure of the private key associated with the Web server's digital certificate in Heartbleed.

If a Web server's digital certificate private key is stolen, it can be used or replayed on an unofficial server, leaving the integrity of that website in question. It also puts at risk the security meant to protect the website's users, who may have had their username and password compromised, which in turn exposes their confidential data and personal information.

Since the Heartbleed vulnerability left no trace on the Web server itself, even websites that quickly upgraded their OpenSSL libraries to non-affected versions cannot determine with any certainty that their private keys were not compromised. Therefore, any website that had the potential to be impacted by the Heartbleed vulnerability should have had its original certificate revoked and replaced immediately.

Any website that had the potential to be impacted by the Heartbleed vulnerability should have had its original certificate revoked and replaced immediately



Heartbleed certificate revocation tsunami yet to arrive

Only 30,000 of the 500,000+ SSL certificates affected by the Heartbleed bug have been reissued up until today, and even fewer certificates have been revoked.

There has been a noticeable rise in certificate re-issuance since 7 April 2014

This shows the number of suspected compromises that companies have reported, based on re-issued SSL certificates. However, certificates are not being revoked in the same numbers, which means that the website may still be compromised.

Source: Netcraft (http://www.netcraft.com/)
http://news.netcraft.com/archives/2014/04/11/heartbleed-certificate-revocation-tsunami-yet-to-arrive.html

This graph from Netcraft and its referenced article show that while a significant number of SSL certificates have been re-issued, the corresponding number of certificates has not been revoked.

Why Revoking and Reissuance of Certificates Isn't Enough

Even if every potentially compromised certificate were revoked, this action isn't enough. Vulnerabilities like Heartbleed could go undetected for years (as Heartbleed demonstrates), and it isn't easy to detect a compromise in a timely fashion. Since the compromise leaves no trace, it is also not possible to determine the extent of the compromise going back in time. The username/ password combinations that were also exposed mean that even if the website's SSL digital certificate wasn't compromised, your customers' user accounts very likely were. Revocation of the server certificate only addresses the problem going forward, but doesn't help the reconciliation of past activities or address the viability of trust going forward.

Reducing Your Exposure

While there is no one fix that can cover every security threat, there are ways to mitigate the risks of vulnerabilities like Heartbleed—and other as-yet unknown threats. Taking these four steps can greatly reduce your exposure to vulnerabilities in the future:

1. Assume You Are Vulnerable or Have Been Compromised

It's a pretty good bet! Run your enterprise architecture through a comprehensive vulnerability assessment and assume you have holes. Given those vulnerabilities, determine what other controls you have in place that will mitigate the impact of that vulnerability to your enterprise and your customers.

2. Protect Private Keys for Web Servers With a Hardware Security Module

To protect Web server digital certificates, WidePoint recommends the use of a Hardware Security Module, or 'HSM', for high assurance security needs like protecting private keys.

An HSM solution can be a managed service or on-site implementation. The HSM provides a hardened, tamper-resistant environment for private keys that also supports other security best practices, such as ensuring that no single administrator can manage those keys. An HSM addresses the impact of vulnerabilities like Heartbleed by not allowing access to an entities private key.

WidePoint highly recommends an HSM solution for securing SSL certificates in anticipation of threats and vulnerabilities not yet identified, especially to address the ability to replay websites that collect personally identifiable information (PII), financial, or other sensitive or private information.

3. Move User Community to Client Authentication using Trusted Digital Certificates

Another security hole that the Heartbleed vulnerability exposed is the ongoing use of username/password for account access within these Web servers. Usernames and passwords were made available in clear text and were available to any entity that exploited the vulnerability.

This presents several problems to the website owners, their users, and the Internet community at large. A few of great concern:

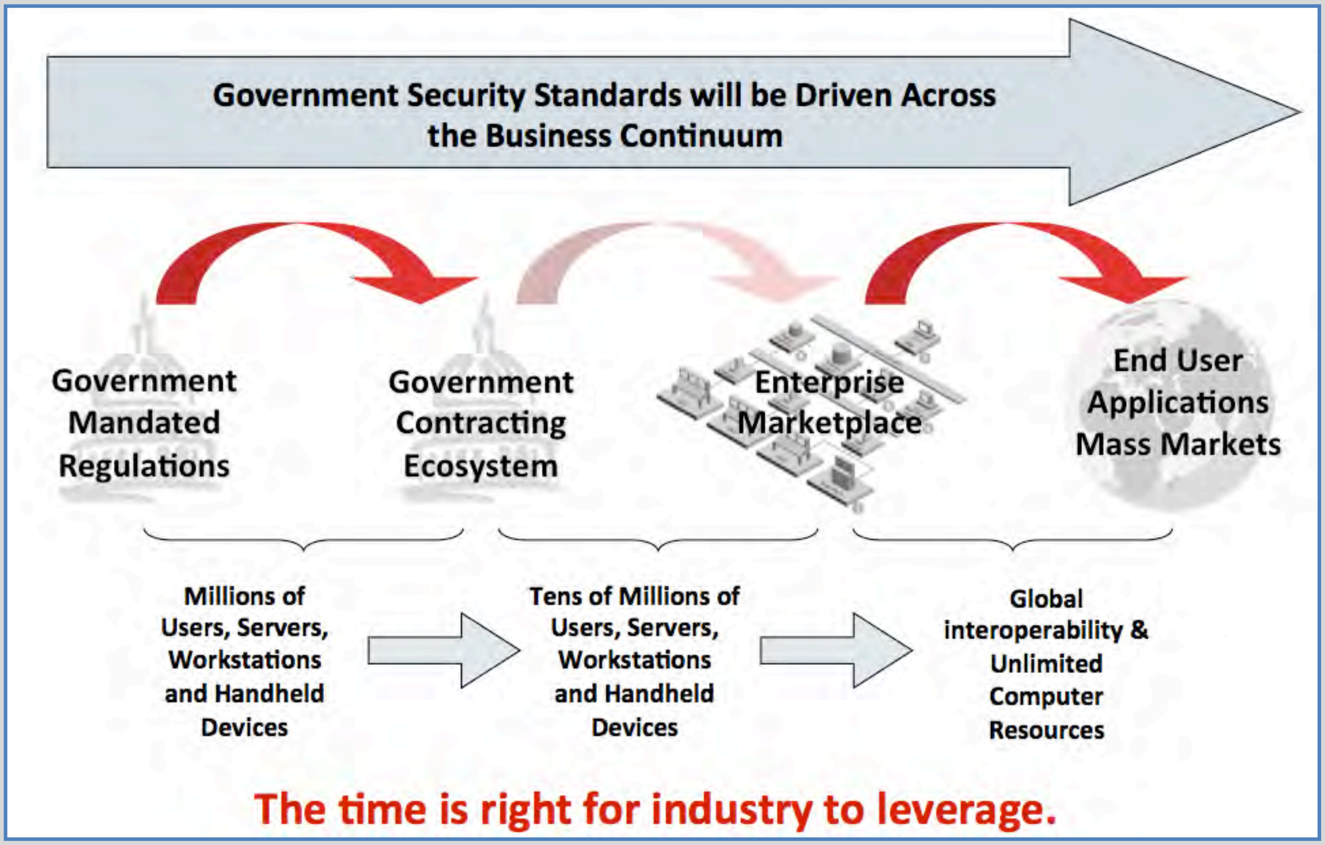
1. First and obviously, user accounts on your website must, for all intents and purposes, be considered compromised. A lack of traceability with this vulnerability limits the extent of your ability to define the scope of the compromise. All accounts must be assumed to be hacked and passwords must be reset. Additionally, a costly and critical review of all previous transactions needs to occur as those are no longer trustworthy.
2. Usernames and passwords are not unique per website. Customers typically have numerous accounts throughout the Internet. Username/password re-use is becoming the norm, which greatly affects the next point.

3. Since username/password re-use is becoming the norm, the integrity of other websites is now at risk, since their username/password data may be compromised even without their Web server having had the Heartbleed vulnerability exposure.

What is an alternative to our familiar username/password authentication? The federal government regulates and approves a number of Trusted Digital Certificate Providers that enable transactions with Web servers based on cryptography that cannot be reused like a common shared secret. This provides benefits in the following ways:

1. By requiring digital certificate client authentication, the Heartbleed vulnerability would have only made available benign public information and a cryptographic hash, creating no security or replay issue. Since the private key is only in the possession of the Web server and can only be invoked by the user, no transaction can be initiated without the user's intervention.
2. The more that digital certificates are used the less burdensome password management becomes, for individual customers as well as organizations that manage many internal users.
3. Trusted Digital Certificates can be revoked, and once revoked, access to websites is automatically restricted without the website administrators having to take manual action to remove access.
4. Trusted Digital Certificates are issued according to strict guidelines imposed by the Federal government that bind a user to their private key. This means you have a high level of assurance or confidence that the person you are dealing with electronically is who they truly are.

When properly implemented within your architecture, mutual authentication based on digital certificates greatly reduces the exposure of your website and syndicates the associated risk.



Government Security Standards will be Driven Across the Business Continuum

Government Mandated Regulations

Government Contracting Ecosystem

Enterprise Marketplace

End User Applications Mass Markets

Millions of Users, Servers, Workstations and Handheld Devices

Tens of Millions of Users, Servers, Workstations and Handheld Devices

Global interoperability & Unlimited Computer Resources

The time is right for industry to leverage.

The federal government must comply with mandated regulations concerning identity and access management, and their security standards are available to be leveraged by enterprise for improved cybersecurity and the benefits of federated identity solutions.

4. Know What Device Your Privileged Users Access Systems With

It is not enough to just authenticate a privileged user’s identity. An organization must able to verify the identity of a device being used to access or administer internal resources. Digital Certificate-on-Device binds device and individual identities to credentials that are used to validate and authorize access to transactions, networks, and applications while protecting the critical data. By leveraging Digital Certificate-on-Device an enterprise can abandon the need for numerous proprietary clients while upgrading to a strong set of credentials that raise the bar on VPN, email, database, application, machine and other critical enterprise authenticated transactions, increasing accountability and reducing non-malicious vulnerabilities.