Authentic Web.

ENTERPRISE DOMAIN MANAGEMENT FOR THE NEW TLD ERA

THE SSL CERTIFICATE IMPERATIVE

HTTPS EVERYWHERE

BRAND TRUST • SEO • ENGAGEMENT

A DISCUSSION BRIEF

"Operating web properties without HTTPS will increasingly compromise brand market trust, impacting SEO performance and limiting web engagement. Browser and search firms are forcing all web managers to implement HTTPS everywhere."

Peter LaMantia, CEO, Authentic Web Inc.

RISKS AND NEW BEST PRACTICES IN A ZERO TRUST WORLD

The Internet is an increasingly risky place for users. Enterprises and their customers are particularly vulnerable as nefarious actors target commercial operations and their digital stakeholders. Organizations, customers, employees and vendor/partners are all at risk.

Enterprise digital transformation is a near-universal phenomenon. It's what we as consumers demand, yet it comes with increasing risk to the enterprise. As corporate and personal data, and applications move to the cloud, the enterprise "attack surface" is expanding beyond perimeters we can easily see, much less defend. In a cloudified world, ingress to enterprise networks is the sum of all users, devices, roles, classifications and applications. The castle moat security paradigm is now obsolete. A new paradigm of **Zero Trust** (Forrester) demands positive authentication on a per user basis using micro-segmentation. A zero trust network forces positive confirmation of every system and user connection:

Who are you?
Where are you from?
Where are you going?
Why are you going there?

Against this backdrop, browser firms in collaboration with the CA/Browser Forum (cabforum.org) continue efforts to help make the Internet a safer place. Encryption and authentication go hand-in-hand in this endeavor. Google, Mozilla and Apple have announced new standards for their respective handling of HTTPS with implications that every website operator needs to be aware of.

SSL certificates*, correctly deployed and managed can help enterprise and their website visitor-customers in three ways:

1. *Encryption prevents parties from seeing data exchanged on an Internet session*
2. *Encryption prevents parties from impersonating webpages for fraudulent purposes*
3. *The correct type of validation further assures site visitors that the corporate entity (brand) relationship to the domain is authentic.*

HTTPS adoption has increased dramatically in recent years - more so now that the browsers are implementing new measures to drive adoption of HTTPS. SSL/TLS encryption is no longer recommended only for transactional web pages. All forms of web page content should be encrypted, including brochure-ware and domain redirects to those destinations.

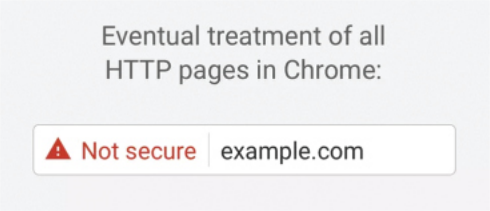
Note: This paper uses the terms SSL (TLS) Certificates and HTTPS Certificates interchangeably, as is common in the marketplace. We believe our readers will understand what we mean when using either of these terms.

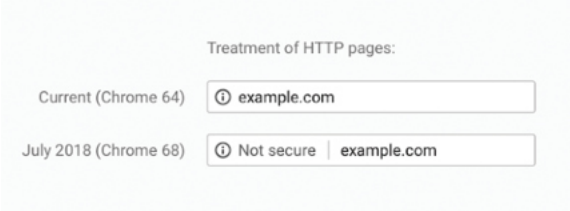
ENCRYPTION EVOLUTION IN MAJOR BROWSERS

Enterprise web managers have used SSL certificates for years on transactional and flagship web pages. Google's commitment to a "secure web" has led to new browser policies that require HTTPS encryption. Failure to adopt HTTPS everywhere has consequences.

GOOGLE CHROME

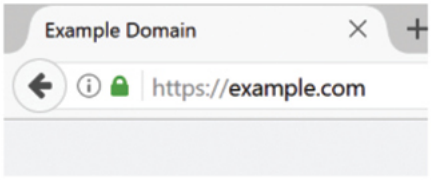
Effective July 2018, Chrome 68 began identifying all HTTP pages as "not secure" within the browser window, regardless of the type of web page an individual is visiting. Chrome 70 is expected to go further, emphasizing the "not secure" alert in red.



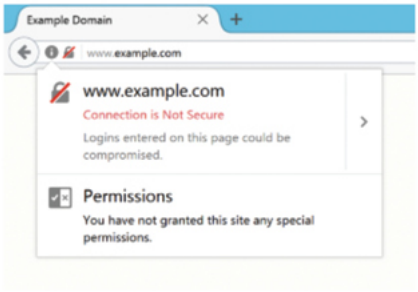


Google's search algorithms have favored HTTPS pages over HTTP pages since 2014. Their argument is, "Users should expect that the web is safe by default." It can be expected that HTTP pages will be further disadvantaged with successive releases of Chrome.

MOZILLA (FIREFOX) AND APPLE (SAFARI) ARE FOLLOWING SUIT:

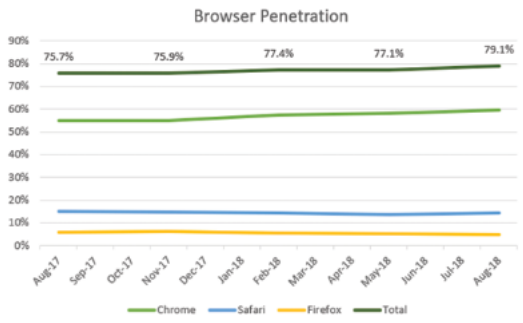


Current secure (HTTPS) connection



As of August 2018, Chrome, Safari and Firefox comprise almost 80% of all browser traffic.

As browser firms and the CAB Forum continue to promote encryption via HTTPS, IT and Web Managers have little choice but to implement SSL encryption everywhere.



Data Source: http://gs.statcounter.com
(Ironic Note: This site is not secure)

IMPLICATIONS FOR ENTERPRISE

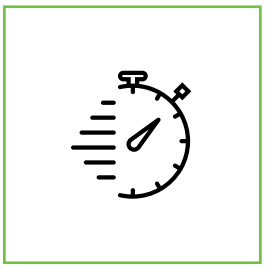
Here are **4** reasons why enterprises must adopt a 100% HTTPS coverage approach:

1. CUSTOMER TRUST AND BRAND REPUTATION

Brands without secure sites will be exposed by the browsers. Cyber Security is a big deal and customers expect you to be secure. Browsers are shaming all website owners into locking down their web properties with https.

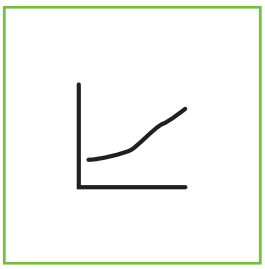
2. CUSTOMER SECURITY

Lack of encryption opens the door to cyber attacks on your users. What brand would willingly place its online customers at risk? Regulations including GDPR put teeth behind these best practices. Brands must do everything they can to protect customer data.



3. DIGITAL PERFORMANCE:

As browser firms adopt more graphically apparent ways to flag unencrypted websites, it's expected that site abandonment will increase from unencrypted web pages. Customer/visitor engagement drives digital business performance.



4. SEARCH ENGINE OPTIMIZATION

Google announced improved SEO ranking for encrypted sites in 2014. Experts predict further degraded Search Engine Results Page (SERP) rankings for unencrypted sites as search engines move towards a safer Internet.

MAPPING CERTIFICATE TYPES AND COSTS TO WEB PROPERTY TYPES

"Which pages should a website site owner encrypt?" The best answer is: ***"ALL of them!"***

There is a cost to expanding one's use of HTTPS certificates. A closer look at the various types of certificates can help point web managers to the best options for HTTPS coverage.

HTTPS ENCRYPTION PRIORITIES

The ideal encryption certificate for a given digital property i.e. the type of content or web page is a function of the level of protection the brand wishes to offer.

Technically, a cert is a cert whether it is Domain Validated (DV), Organization Validated (OV) or Extended Validation (EV). Properly implemented, a DV certificate solves the encryption security requirement of the browsers. Certificates with additional CA requirements provide additional levels of trust. The point is you need a policy, a budget and the software tools for your teams to effectively manage the environment.

Below is a guide for commercial certificates by web page type including redirects, all of which need to be secured with HTTPS encryption.

Page Type	*Examples*	*Cert Type*	*Volume[1] (% of Portfolio)*	*Cost[2] (Year/Cert)*
Transactional	Main site, E-Commerce, payments, financial data collection	OV or EV Preferred for added trust	**Low: 1-2%** main site	*$100 - $1,000*
Private Data	Registration sites, forms, any pages requesting personal or private data	OV or EV Preferred for added trust	**Moderate: 3-5%** Campaign pages, forms, customer interactive	*$100 - $1,000*
Brand Identity	High traffic branded properties.	DV unless brand seeks more trust with and OV or EV	**Moderate 3-5%** Campaign, product or service microsites,	*$15 - $30*
Brochure or Read only	Blog sites, text-only sites, (No forms or data exchange)	DV unless brand seeks more trust with an OV or EV	**High 10-20%** Depends on type of business and digital strategy	*$15 - $30*
Redirects to any site or deep link	Pages that redirect to another domain page must be encrypted under https	Recommend utilization of an HTTPS redirect service solution.	**Very High 50-70%** Redirects to relevant destinations inside websites, campaign or product pages	*$7 - $12*

[1] Depending on the digital business, % of the portfolio of domains related to a type of site can vary greatly. We have included ranges we see on typical domain portfolios.

[2] SSL certificate prices vary by CA and Reseller as well as volume purchase agreements. We have provided price ranges for the three basic types and do not include options such as Wildcard or SANS/UCC certificates. Some new certificate types (e.g. Let's Encrypt) are free. Contact info@authenticweb.com for SSL/TLS cert pricing and solutions.

OPERATIONAL CHALLENGES IN MANAGING SSL CERTIFICATES

It's easy to budget for the right certificates on domains, subdomains and redirects where they are needed. Much harder is the task of efficiently operationalizing an HTTPS encryption policy with control, visibility and automation. Managing SSL certificates can be error-prone and administratively costly.

Browser display changes in 2018 aren't the only forces acting on encryption standards. The certificate market eco-system led by the CA/Browser Forum (CAB Forum), and the CA community at large are wrestling with many SSL certificate management issues, CA failures and TLS vulnerabilities. Here are five issues of which enterprise should be aware.

1. TLS CERTIFICATE ADMINISTRATION IS PAINFUL

Examples abound of enterprise certificates expiring without warning or being mis-configured.

It's easy to see why, given the laborious, manual processes involved.

SOLUTION

Adopt robust and modern Domain/DNS and TLS management systems to control, visualize and automate the change management process.

2. TLS ENCRYPTION WITHOUT DNSSEC

Encryption is important, but so is authentication. DNSSEC is an essential and logical complement to HTTP encryption ensuring that DNS data is valid for the intended destination.

SOLUTION

Implement DNSSEC as an added security measure to help reduce the risk of your site visitors being tricked or compromised by Man-in-the-Middle (MITM) exploits.

3. CERTIFICATE AUTHORITY (CA) COMPROMISES

Certificate Authorities (CAs) and their processes are all expected to be rock-solid. They aren't! Accounts of human error (on the enterprise and the CA sides) and system faults have been known to invalidate or otherwise compromise numerous high profile certificate authorities. Point: not all CAs are the same.

SOLUTION

Configure the correct certificate types for your domain end points. Manage all SSLs under a single pane of glass control system that monitors endpoints with tamper-proof audits, change management digests and remediation.

4. UNENCRYPTED REDIRECT DOMAINS

Most enterprises have hundreds or even thousands of redirected domains pointing to deep links within their websites. Most redirects are not encrypted owing to oversight or the mistaken idea that they don't require encryption. In fact, endpoints that rely on redirected domains absolutely require that the origin domain be encrypted. Even if the endpoint (destination) domain is HTTPS, an HTTP origin (redirected) domain will negate the encryption. This creates an attack vector for nefarious actors to inject code to compromise your customers.

SOLUTION

Source and enable an HTTPS redirect solution on all your redirecting domains.

5. MANAGING CHANGE IN TLS CIPHER SUITES

Over time, SSL protocols have been replaced with TLS versions from TLS 1.0 to 1.3. Community groups determine when older versions require updates, which are ongoing. It is important for IT security teams to ensure that the ciphers installed on endpoint servers are current. This is an onerous but critical task. HTTPS certificates on older TLS cipher suites may expose users to known risks.

SOLUTION

Adopt SS management control systems that can monitor and report that the correct TLS cipher versions are in use.

SUMMARY

Brand TRUST is critical to your digital enterprise. Compromised brand trust can negatively and irreparably harm your customer relationships.

HTTPS ENCRYPTION EVERYWHERE is quickly becoming the new standard for enterprise brands, expected by customers. Browsers are displaying clear, graphic warnings on unencrypted sites. Eventually search links to unsecure web pages may be disabled entirely. The short-term impacts from unencrypted web pages include eroded brand trust, increased abandonment rates and degraded SEO rank performance.

2018 is a watershed year as browsers and search engines mandate that every web property be https enabled. Below are best practice take-aways for enterprise Web and IT Managers.

1. *Establish a Baseline and ID the GAP: Audit Your Domain Portfolio*
   Conduct an audit to reveal your baseline TLS security posture, identifying gaps in coverage and potential security risks. Design, resource and implement a plan to close the gap.
2. *Define your SSL Security Policy: Map Web Properties to SSL Types*
   Define your SSL Security Policy. Map SSL types to hosts based on the type of sites you serve audiences. Implement and monitor hosts for compliance to the stated SSL Security Policy.
3. *Know Your Cipher Suites and Update Webservers to Support TLS 1.3*
   In your SSL Policy, define compliant cipher suites. As of late 2018, TLS 1.3 is recommended. Install TLS 1.3 everywhere. Monitor and enforce versions in use with systems.
4. *Implement DNSSEC*
   DNSSEC is critical to fortify encryption with DNS route look up assurance (authentication). Utilize systems to automate the signing and maintenance of DNSSEC on your zone files.
5. *Ensure Redirect Domains are Properly Encrypted*
   Unencrypted redirected domains are an emerging security gap. Audit for compliance and implement systems to force https redirects to destination web properties.
6. *Modernize your Systems: Domains, DNS and TLS Security*
   Security demands effective change management, monitoring and remediation control systems. Domains, DNS and TLS security should be managed under a single, secure and compliant DNS control system. Research confirms that manual processes and operational silos are the main factors behind brand security risk. A modern system will dramatically improve your encryption and authentication strategy.