

# BITS

FINANCIAL SERVICES  
R O U N D T A B L E

## **SECURE WEB BROWSER RECOMMENDATIONS**

**DECEMBER 2009**

**A PUBLICATION OF THE BITS SECURITY WORKING GROUP**

BITS  
1001 PENNSYLVANIA AVENUE, NW  
SUITE 500 SOUTH  
WASHINGTON DC 20004  
(202) 289-4322  
[WWW.BITS.ORG](http://WWW.BITS.ORG)

## TABLE OF CONTENTS

I. EXECUTIVE SUMMARY .....	3
II. DEFINING THE PROBLEM .....	4
III. QUANTIFYING LOSSES.....	4
IV. IMPROVING MUTUAL AUTHENTICATION .....	5
EXTENDED VALIDATION CERTIFICATES .....	5
PASSWORD STORAGE MODEL.....	6
REPUTATION RATING SYSTEM.....	8
V. IMPROVING THE OPERATING ENVIRONMENT.....	10
STRICTER SECURITY POLICIES FOR WEB APPLICATIONS .....	10
IV. CONCLUSION.....	11
VII. ACKNOWLEDGEMENTS.....	12

### DISCLAIMER

THIS DOCUMENT IS FOR INFORMATION PURPOSES ONLY. Neither the individual members, nor the member institutions of BITS or The Financial Services Roundtable, make any warranty or assume any legal liability or responsibility for the accuracy, completeness, or usefulness of the information contained in this document, or represent that this document's use would not infringe privately-owned rights. Reference to any special commercial products, processes, or services by trade name, trademark, service mark, manufacturer, or otherwise, does not necessarily constitute or imply its endorsement or recommendation, or favoring by BITS or The Financial Services Roundtable.

## I. EXECUTIVE SUMMARY

Web browsers are now a primary means of interaction between financial institutions and their customers and between customers and the rest of the Internet. Web browser security is a continuous challenge for browser manufacturers and an ongoing risk to financial institutions and their customers. Hackers are increasingly using the web browser as a vector of attack to engage in malevolent behavior. These attacks often result in the installation of malicious software on customer computers, which is then used to trick or transparently exploit customer behavior into compromising the integrity of financial transactions in the online environment. While there are no “silver bullet” solutions, web browser manufacturers are in a position to mitigate some of these risks by improving mutual authentication mechanisms and the overall operating environment.

In 2009, members of the BITS Security Working Group embarked on a project to enhance the security and integrity of the web environment. The goals of the BITS Secure Web Browser Project were to:

- Enhance the general security and integrity of web browsers;
- Reduce the risk of compromise through normal web browsing behavior;
- Increase the opportunities for mutual authentication;
- Strengthen the ability of financial institutions to prevent unauthorized third-party code from interacting with online transactions (e.g., cross-site scripting); and
- Improve reliability of the online transactional channel for customers and their financial institution.

The BITS Secure Web Browser Subgroup recommends the speedy adoption or improvement of four available technologies by the web browser manufacturer community:

- **Extended Validation Certificates** – A mutual authentication and encryption technology
  - Standardize client-side user interface display across all browsers;
  - Implement improved detection of invalid certificates; and
  - Strengthen EV Certificate creation standards at the root.
- **Password Storage Model** – A method to manage passwords for multiple websites
  - Build and expand upon existing browser password manager capabilities; and
  - Utilize available data to authenticate validity of a website.
- **Reputation Rating System** – A third-party service to automatically identify malicious or phishing websites
  - Deliver a non-invasive and reliable assessment of websites directly to the user prior to clicking a web link.
- **Stricter Security Policies for Web Applications** – A transparent backend security control
  - Enable website owners to white list authorized third parties.

Each of these technologies exists today in various forms, including as third-party add-ons to modern web browsers.

## **II. DEFINING THE PROBLEM**

BITS and its financial institution members believe the broad adoption of additional, transparent and straightforward security features and controls by the web browser will improve the integrity of information exchange between financial institutions and their clients. The key reasons for engaging in this effort are to improve the web browser security and to increase customer confidence in the online channel.

## **III. QUANTIFYING LOSSES**

It is a challenge to quantify the losses to customers and financial institutions, as consolidated sources to measure losses for both constituencies are currently unavailable.

One group that attempts to take on this challenge is the Computer Security Institute (CSI). The CSI Computer Crime and Security Survey (2008)<sup>1</sup> reported the average cost of financial fraud to be \$500,000 per incident, while botnet related loss averaged \$350,000 per incident. The average annual overall loss reported was a staggering \$300,000 per incident.

Browser manufactures and financial services firms share the same interests: secure the browser and reduce the risk of web-based crime for our mutual customers.

---

<sup>1</sup> <http://www.docstoc.com/docs/9484795/CSI-Computer-Crime-and-Security-Survey-2008>

## IV. IMPROVING MUTUAL AUTHENTICATION

### EXTENDED VALIDATION CERTIFICATES

#### A. PROBLEM STATEMENT

The Secure Socket Layer (SSL) certificates depend on reputable Certificate Authorities (CA) verifying the legitimacy of organizations to which they are issuing. Standard SSL certificates have lost their integrity given the plethora of CAs that issue certificates with little or no verification of the domain owner.

#### B. SOLUTION DESCRIPTION

Extended Validation (EV) SSL certificates allow for more extensive validation by registrars of the organization to whom the certificate is being issued. The financial services sector, as with other industries' increasing dependence on the Internet, is interested in using EV certificates to increase customer confidence when interacting with their websites, and help reduce the success rate of phishing. These standards-based X.509 certificates do not require additional changes to web server architecture, which allows them to be implemented with little additional overhead to the requesting organization.

Modern web browsers should have the following characteristics:

- 1) Full support of EV SSL so that it is clearly presented to the end-user on a valid EV SSL certificate. The present method of simply presenting a “green” status is not sufficient as it is not apparent to users. Valid EV SSL certificates should have a more apparent detection method.<sup>2</sup>
- 2) Require “hard” stops on the detection of certain types of invalid EV SSL certificates. The hard stop should require the user to accept warnings if they choose to continue to visit the site.
- 3) The EV certificate standards should specify the acceptable hashing algorithms for creating EV certificates. In current deployments, the SHA family of hashing algorithms is used to create digital signatures in EV certificates. The EV standard allows the MD5 hashing algorithm to be used to create digital certificates for EV Root CAs. Security researchers have demonstrated significant problems with MD5. Fortunately, there are only a few Root CAs capable of creating EV certificates, which all use SHA instead of MD5.

#### C. SOLUTION BENEFITS

Standard user interface (UI) notifications of the presence of EV Certifications would make it more difficult for fraudsters to spoof valid websites. EV SSL would allow end-users to regain trust in certificate information that is being presented.

We also propose eradicating MD5 from the EV certificate specification. We believe the impact of this change will be minimal because MD5 is not currently used for any EV certificates. The browser

---

<sup>2</sup> The Financial Services Technology Consortium (FSTC) is currently defining a project in this space. For more information, visit <http://www.fstc.org>.

green bar can be doubly leveraged to indicate that a website is “MD5 free” – further instilling customer confidence.

#### **D. IMPACTS AND CONSIDERATIONS**

The successful implementation of EV SSL consists of two factors:

- 1) Organizational adoption of EV SSL. Enterprises must make a more conscience effort to deploy EV SSL. The current adoption rate is low.
- 2) Clear and concise presentation of EV SSL certificate status to end-user.

### **PASSWORD STORAGE MODEL**

#### **A. PROBLEM STATEMENT**

It is well known that end-users choose poor passwords, and reuse passwords between sensitive and non-sensitive websites when sound security practices would favor users making different password choices. However, users are the unwitting victims bearing the burden of expanding and arduous security requirements by websites that still do not offer adequate security. To make things worse for end-users, different sites have conflicting password requirements, often requiring a slightly different password for each site. The mental burden on users to remember each of these logins and passwords incents users to take shortcuts such as sharing passwords.

It is all the more problematic for users that they can be easily tricked into divulging credentials on the wrong site, or be tricked by malicious code or pharming attacks – often through no fault of their own. The lack of reliable mechanisms to accurately authenticate websites and thereby prevent users from making seemingly dangerous decisions does not help the situation (see the [Extended Validation Certificates](#) section).

Existing browser password management systems are a solid foundation for solving some of these problems. Users need the ability to access and manage their password repositories with ease. Existing systems lack portability and cross-browser integration that hinder a users’ ability to rely on the system instead of memorized passwords.

Furthermore, existing password management systems in browsers are lacking additional safeguards against malicious attacks and basic controls, such as idle timeouts, thereby making them a potential source of compromise<sup>3</sup>.

#### **B. SOLUTION DESCRIPTION**

Browser manufacturers should build and expand upon existing browser password manager capabilities.

Adding cross-platform and cross-browser portability for password databases will ease the users’ ability to rely on their password managers to store more complex and varied passwords. Supporting plug-and-play USB Key password storage for databases would further enhance the ability to use these credentials across different computers (e.g. work and home). In the long view, USB Key fobs

---

<sup>3</sup> <http://www.w3.org/TR/wsc-usecases/#password-manager>

may be used to apply strong cryptographic mutual authentication and biometrics may become an important identity factor.

Browser manufacturers should remedy the existing known weaknesses with password managers. It is documented in various sources, such as the Browser Security Handbook<sup>4</sup>, that the repository of passwords is guarded from attack and does not introduce additional attack vectors.

Browsers should implement these additional controls:

- Controls for auto-locking the password repository after x minutes (protects against physical attacks as well as malicious man-in-the-browser or XSS attacks).
- Capabilities for auto-clearing the clipboard after x seconds. Otherwise, the user passwords will be vulnerable to clipboard attacks.
- Periodic clearing of cached credentials in all memory locations.

Furthermore, password managers should take advantage of website certificates, not just URLs, when auto-populating credentials so as to bind the credentials to the proper website. Password managers could detect common passwords across multiple sites and coach users into making better password choices. Even better, such password managers could help do away with users needing to hand-type their passwords, so, over time, users would become suspicious of sites where their password does not auto-populate.

### **C. SOLUTION BENEFITS**

Password managers with these types of features would be invaluable in providing phishing prevention and detection capabilities. They would help prevent password cross-site vulnerabilities or phishing attempts. Such changes to the existing technology would detect passwords being typed into the wrong site by comparing password hashes to existing stored passwords and prevent the release of password credentials to invalid websites.

In addition, password managers can result in improved password quality since users can rely on securely stored passwords instead of memorized passwords. Users should set stronger passwords to prevent brute force attacks. The Conficker worm was enormously successful in attacking sites using a list of just 200 common passwords. The benefits of improving password quality by allowing users to easily vary passwords for different sites would further insulate users against multi-site attacks.

### **D. IMPACTS AND CONSIDERATIONS**

Competition in browser design and development may hinder collaboration between those developing cross-browser and cross-platform capabilities. Typically, “standards by consensus” is a poor way to arrive at the optimal and secure solution (e.g. WEP). If appropriate, existing identity management frameworks such as Microsoft Windows CardSpace<sup>5</sup> and the Higgins open-source project<sup>6</sup> should be reviewed and leveraged.

---

<sup>4</sup> <http://code.google.com/p/browsersec/wiki/Main>

<sup>5</sup> <http://www.microsoft.com/windows/products/winfamily/cardspace/default.aspx>

<sup>6</sup> <http://www.eclipse.org/higgins/>

User awareness training should be automatically available at the “teachable” moment to inform users of the security benefits associated with Password Storage features. Warning messages should be clear and concise. Designs should avoid depending on users to make security decisions.

Working off the foundation of the Password Storage Model, browser manufacturers should consider further password manager extensions to increase security and user involvement in site validation. Examples of two options are:

- **Pet name management.** Allows users to establish their own pet name/image for a website to help users visually detect phishing sites (avoids the man-in-the-middle attack against current server-side solutions, and allows users to add this feature to any site).
- **PwdHash.** Allow users to specify a password that is hashed together with site-specific attributes to result in a stronger password and unique per-site passwords automatically. This option only works if users can rely 100% on their password database rather than memorized passwords.

## REPUTATION RATING SYSTEM

### A. PROBLEM STATEMENT

Phishing and malicious websites continue to be a problem on the Internet. The effectiveness of security awareness programs has been diluted by changing attack methods, including complex URLs that appear to be legitimate. A method for alerting users of websites with poor reputations would be advantageous.

### B. SOLUTION DESCRIPTION

Internet Explorer and Mozilla’s Firefox use some form of reputation analysis to indicate the security of websites to customers.

Website reputation rating systems rely on two primary methods of identifying phishing/malicious sites:

- 1) Analysis of Domain Name Systems (DNS) and other technical behavior.
- 2) Gathering the opinions of users or rating agencies integrated with a reputation rating system.

The output of these methods results in a list of suspected phishing sites that provides alerts directly to the browser, warning users of potentially malicious websites.

This solution is available in different forms in Firefox since version 2.0 and in Internet Explorer since version 7. Both were released in 2006.

### **C. SOLUTION BENEFITS**

The potential value of delivering a reliable assessment of websites, directly to browsers, and therefore users, is very high. Recent research indicates that it is possible that 10% of all websites on the Internet contain malicious content.<sup>7</sup>

Another report indicates that one major reputation system has achieved as much as a 97% accuracy rate in identifying phishing websites.<sup>8</sup>

Any reputation analysis system should also allow for websites that may have been improperly identified to be disputed and removed from the black lists. All of the well-known solutions have a formal process for correcting possible errors.

### **D. IMPACTS AND CONSIDERATIONS**

Even with good technology and knowledgeable reviewers, mistakes will occur. While a 3% error rate seems good, this will hardly seem reasonable to a business whose website has been improperly identified as a phishing site for even a short period.

As the use of reputation systems grows in importance, it is possible that attacks against these systems will increase as well. Currently there are well-documented vulnerabilities that may limit the value of these systems, but there are no known attacks against the systems themselves.

Vendors and organizations will have to remain vigilant against the potential of attacks against these systems, especially as we increasingly rely on them to determine the validity of websites.

Corporations must continue to structure security awareness campaigns so that customers do not become complacent and rely on any single control layer as the ultimate solution. We encourage use of the Anti-Phishing Working Group landing page during “teachable” moments.<sup>9</sup>

---

<sup>7</sup> The Ghost In The Browser: Analysis of Web-based Malware; Provos et al

<sup>8</sup> Evaluating the Wisdom of Crowds in Assessing Phishing Websites; Moore, Clayton

<sup>9</sup> <http://education.apwg.org/r/en/index.htm>

## V. IMPROVING THE OPERATING ENVIRONMENT

### STRICTER SECURITY POLICIES FOR WEB APPLICATIONS

#### A. PROBLEM STATEMENT

The addition of JavaScript, Java and other active content interpretation capabilities to web browsers has greatly increased functionality beyond simple HTML rendering engines to quasi-operating environments. However, not all content is benevolent and the exploitation of active functionality is increasingly used for fraudulent and criminal purposes. Certain classes of attacks<sup>10</sup> take advantage of implicit user-trust via social engineering, architectural, design and implementation flaws allowing malicious code to execute within the context of a web page, loading malicious content from arbitrary websites resulting in an attack on the user and their data. Several of these documented exploits render standard server side controls ineffective.

#### B. SOLUTION DESCRIPTION

Several solutions to the above attacks have been proposed. These high-impact solutions utilize silent and automated communication between client web browsers and web servers, thereby eliminating reliance on user decisioning. These handshake communications inform the web browser of domain-specific content restrictions and conversely may provide information to the server of the origin of a client-side request, allowing website hosts to determine if a request is valid or made by a nefarious third party.

A number of competitive and arguably complementary models are currently under proposal to various groups and standards bodies. Without prejudice, these models include Application Boundaries Enforcer<sup>11</sup>, Content Security Policy<sup>12</sup>, and Origin Header<sup>13</sup>.

#### C. SOLUTION BENEFITS

The transparent exchange of additional information in the handshake gives both the server and the client increased ability to mitigate common attack vectors. This type of control will allow both the browser and the web server to automatically determine the safety of a particular request and to take the appropriate action to protect the end-user.

Another important feature of these proposals is the backwards compatible nature of the changes. While both the browser and the server must be configured to understand the policy communications, if either party is not upgraded, the webpage may still behave as expected, though without the improved security controls.

#### D. IMPACTS AND CONSIDERATIONS

The key consideration for the adoption of any of these models is the need for the browser and server to both recognize and enforce the policy restrictions. Any changes to the server model must maintain backwards compatibility in the interim adoption period. These security models may require changes to existing W3C-defined standards and will require significant changes to security policies within the client web browser.

---

<sup>10</sup> For example, Cross-Site Scripting, Cross-Site Request Forgeries and Click-jacking

<sup>11</sup> <http://noscript.net/abe>

<sup>12</sup> <http://people.mozilla.org/~bsterne/content-security-policy/>

<sup>13</sup> <http://people.mozilla.org/~bsterne/content-security-policy/origin-header-proposal.html>

## IV. CONCLUSION

The design of web browsers carefully balances the demand for a generalist feature set against the need for the integrity and security of the communications medium. Technology currently does not exist to eliminate all of the web-related threats posed by sophisticated online fraudsters. However, technologies do exist to mitigate and reduce the effectiveness of many of these threats. The BITS Security Working Group has identified a number of these technologies as important to the continuous effort to improve web browser security and mutual authentication.

While this document includes specific recommendations for each technology, there are also several overall recommendations:

- Encourage immediate updates to all unsupported browsers still in use.
- Promote awareness of safe online practices.
- Engage with peers, standards bodies, and the Financial Services Technology Consortium (FSTC) to strengthen technical specifications.

The BITS Security Working Group and the FSTC are willing to directly engage leading browser manufacturers and other stakeholders in collaboratively developing and implementing these and other recommendations.

## VII. ACKNOWLEDGEMENTS

BITS would like to thank the following individuals for their contributions to this document:

Wayne Anders, Regions Financial Corporation  
Jason Axley, JPMorgan Chase & Company  
Chris Howser, Wells Fargo & Company  
Jeff Jancula, Wells Fargo & Company  
Erik Johnson, Bank of America Corporation  
Arve Kjoelen, Wells Fargo & Company  
Bruce Onweller, Capital One Financial Corporation  
Michael Ortega, Harris Bankcorp, Inc.  
Doug Pelton, Wells Fargo & Company  
Alex Popowycz, Fidelity Investments  
K. Scott Vowels, Comerica Incorporated  
Andrew Kennedy, BITS  
Paul Smocer, BITS

## VIII. ABOUT BITS AND THE BITS SECURITY PROGRAM

**BITS** is the technology policy division of The Financial Services Roundtable, created to foster the growth and development of electronic financial services and e-commerce for the benefit of financial institutions and their customers. BITS focuses on strategic issues where industry cooperation serves the public good, such as critical infrastructure protection, fraud prevention, and the safety of financial services by leveraging intellectual capital to address emerging issues at the intersection of financial services, operations and technology. BITS' efforts involve representatives from throughout our member institutions, including CEOs, CIOs, CISOs, and fraud, compliance and vendor management specialists. The Financial Services Roundtable represents 100 of the largest integrated financial services companies providing banking, insurance, and investment products and services to the American consumer. Member companies participate through the Chief Executive Officer and other senior executives nominated by the CEO. Roundtable member companies provide fuel for America's economic engine, accounting directly for \$84.7 trillion in managed assets, \$948 billion in revenue, and 2.3 million jobs. For more information, go to <http://www.bits.org/>.

The mission of the **BITS Security Working Group** is to strengthen the security and resiliency of financial service by:

- Sharing and developing best practices to secure infrastructures, products and services;
- Maintaining continued public and private sector confidence; and
- Providing industry input to government agencies and regulators on policies and regulations.

The priorities of the Security Working Group are determined by the Security Steering Committee and reviewed by the BITS Advisory Board and Roundtable Technology Committee. The focus of the Security Program may vary year to year but includes four major areas: Application Security, Infrastructure Security, Data/Information Security and People-related Security.