Interested in learning more about security?

SANS Institute
InfoSec Reading Room

This paper is from the SANS Institute Reading Room site. Reposting is not permitted without express written permission.

# What Secure Site Seals Mean to Consumer

We definitely trust brandname. It is the key to locate the merchant in the great internet world of web sites. Obviously, everyone should learn the difference between Mcdonald.com and Mcdonalds.com. A number of tools can help consumer to know the actual owner of a domain name, such as whois or together with well known search engine like yahoo. Domain name server hijacking is not impossible. Even when we are sure that the domain name is owned by the expected merchant, we still need to check on the content of the web site...

Copyright SANS Institute
Author Retains Full Rights

AD

# Practical Assignment for GSEC Certification

Title of Assignment : What Secure Site Seals mean to Consumer
Version : 1.0
Name : Kwok Kit CHAN
Submitted to certify@sans.org by e-Mail on :2 Oct 2001

## Introduction

What is the first and utmost trust that a consumer will have on a merchant in the Internet ? What is the rule of thumb checking procedures for the consumers to ensure that the web site they are going to provide their credit card information are the genuine sites intended and the web pages they get from these web sites are genuine ones from the merchants they trust ?

We definitely trust brandname. It is the key to locate the merchant in the great internet world of web sites. Obviously, everyone should learn the difference between Mcdonald.com and Mcdonalds.com. A number of tools can help consumer to know the actual owner of a domain name, such as whois or together with well known search engine like yahoo. Domain name server hijacking is not impossible. Even when we are sure that the domain name is owned by the expected merchant, we still need to check on the content of the web site.

In the Internet world, the default method of authenticating the web site is by using SSL server certificates. The PKI service providers are seriously selling PKI technologies claiming that it would help improve the trustworthiness of a web site. The biggest audit consultant firms are selling Webtrust to do something similar. In certain senses, these remedies can be good enough to support the genuineness of the web site and the procedures of the web site owner company on managing the web site and customers' information. However, it is still not a bullet-proof means.

## The Risk

Defacing is the obvious trick of the script kiddies in showing off their hacking skills.

© SANS Institute 2000 - 2002, Author retains full rights.

In certain sense, Attrition.org may be the hall of fame for these hacking learners. Not many of these known defacing incidents were related to commercial crime. However, the same techniques can be used to hijack a web site and steal all the customer information flowing to the web site quietly in the server end. Web sites should implemented change monitoring and recovering tools, such as tripwire, to alert support personnel on any defacing to their web. Web sites should also implement SSL server certificate and object code signing so that important web pages and scripted are protected by SSL and digital signature that customers are able to check the web site and script owner information from the server and code signing certificates. Together with other best practice web site management procedures, the web site owners should have implemented all the protection measures they can build for their web site. However, do the customers know which Internet merchants actually implemented these protection measures ? How can a customer know from their browser the web site they are visiting are showing the genuine web pages from the web site owner ?

## The Secure Site Seal

While we are shopping around in the Internet, we would meet some Secure Site Seal logo issued by well known Certification Authority companies claiming to assure that the web site customers visiting are the genuine site. With a mouse click on this Secure Site Seal logo, the customer will be led to a web page showing more information about the web site owner. Customers would definitely welcome this visible and ease to use sign of genuineness of the web site but does it really solving the problem or just a mislead ?

Verisign is the biggest Certification Authority and it give out the Secure Site Seal logo to its Secure Server ID Certificate customers for putting onto their web pages to serve as an identification of the owner of the web site. Users can click on this logo to run a javascript program which will pop up a windows showing a web page from Verisign on the detailed information of the owner of the Secure Server ID Certificate. The javascript program is something like :

javascript:open_window('https://digitalid.verisign.com/as2/e40958893f6b2d8139ac2d2874782dfa')

© SANS Institute 2 ... as part of GIAC practical repository. Author retains full rights.

Thawte, like its parent company Verisign, also gives out a Thawte Authentic Site logo to its SSL Server Certificate clients. On clicking on the logo, a javascript function program will be run which will show a web page from Thawte that details the certificate owner information. The URL for this web page is like :

https://www.thawte.com/cgi/server/certdetails.exe?code=ZATHAW16-3

GlobalSign is the leading European Certification Authority. It also gives out its Secure by GlobalSign Seal to its ServerSign Secure Server Certificate customers. Unlike Verisign and Thawte, mouse clicking the Seal does not show the certificate content or the certificate owners' information kept by the Certification Authority. It only redirects the user to a web page http://www.globalsign.net/securedby/check/ which only guides users to install root certificate.

The above three are typical Secure Site Seals which commonly used in internet merchant web pages to "strengthen" their secure web site image. Obviously, the GlobalSign's Seal is a little bit more easier to implement that the other two, if we are talking about putting this Seal on all web pages we want to show the assurance. These Seals may be good to show the authenticity of the owner of the SSL Server Certificate and hence the web site. It is not meant to assure the genuineness of the web page content in the web site, however. A defaced web page can still put back these Secure Site Seals on it and faked the true site. It is obviously not difficult to do the same as Verisign and Thawte to show some faked information on the site owner. By knowing the details of the working of these kind of Secure Site Seal, it is not difficult to conclude that relying on these Seals is not secure enough to a consumer. In fact, these logos are only graphics which can be copied by anyone in the Internet and put into a faked page.

## Securing Web Page with Digital Digest

To the consumer, the ultimate solution to ensure that the web pages are not changed from its original version is to have a mechanism built in the browser to show the integrity of the web pages. It should be emphasized that this function should be

© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

provided at the browser level because customers are used to rely on web browser to automatically check the web content while they are surfing in the Internet, for example, the padlock in the browser status line which shows the establishment of SSL conversation session with the web page. Providing such function in the browser level also hits the problem head on as the problem is more on building customers' trust. There has been a number of effort spending on building the standard and architecture on using this function.

BIBLINK project funded by within the Telematics for Libraries programme of the European Commission is one of them. In its study, metadata elements is used to hold a on-way hash function checksum (or message digest) of the resource being described by the URL. The study also touched upon containment of all the inline objects which form the web resource. For example, a diagram in a document, all the linked objects included web pages that are hyperlinked to the original page or that require clicking a button for display. Inline objects that are included in the checksum calculation are <APPLET>, <EMBED>, <OBJECT>, <IMG>, <IMAGE>, <LINK rel="stylesheet">. The solution to explore has to be practical in that only objects controlled by the web site owner should be checked for integrity. Externally linked resources are not involved in the check sum calculation. However, as the main page is intact, there is no chance for breaking the web page to insert malicious objects or defaced part of the web page.

To successfully promote new functions to the stable but evolving internet protocol standards, two critical criteria have to be met. The first one is the standardization, that is, to canonicalize it in a standard format which everyone generally uses. Secondly, browser vendors should implement this function when it is becoming standard.

IETF and W3C has been working for some time on the XML Signature scheme for representing the signature of Web resources, including portions of protocol messages (anything referencable by a URI). Besides, they also study on the procedures for computing and verifying such signatures which web developers are very much concerned. Theoretically, the XML digital signature scheme can envelop whatever information the URI referred. In fact, there is no restriction on what can be signed in the XML Signature specifications, it is all about defining in general signatures to any digital content that can be addressed in or by an XML document. Therefore the XML digital signature scheme can be used for both the server side or the client side. To the interest of web merchant, they would be interested in using the technology to

© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

secure the transaction from the client. To the consumer, it is also a technology to facilitate consumer to authenticate the web owner and assure the source of all the critical information or data from the web site.

XML provides a standard and extensible means to specify data in the conversation in Internet. XML Signature specifications describe the how integrity, message authentication, and/or signer authentication services for data of any type can be provided. The underlying basic elements of the XML digital signature is the Signature element which is a complete specifications covering the signed information, signature method, digest method, digest value, signature value (which includes the public key of the signer), key information and the object to reference. Having the information to sign instead of just making a digital digest is a great improvement over BIBLINK project as signing the digest value binds the referenced resource contents to the signer's key – the owner of the web site. It is the ultimate goal of providing assurance to the Internet consumer.

XML Signature is a standard based well-structured specifications of the web content signature scheme. The structure of it is so nice that it can be detached from the web content but all the information required for the verification of the signature are in one package. The most importance of it is the ease of adoption to web developer and browser developers.

Some XML Security Suite development tools has been initially released to provide digital signature feature that are beyond the capability of the transport-level security protocol such as SSL, which is the target of discussion in this paper. Some of them have released reference implementations of DOMHASH, a proposed canonicalized digest value for XML document. DOMHASH can be a basis for XML digital signature that is being discussed in both IETF and W3C.

The current April 2001 version of XML Signature Specifications is in the Proposed Recommendation state of W3C. We all wish the combination of a standard based web content signature scheme and a user visible browser functionality to support this signature scheme would realize as a real product to benefit the Internet consumer. The ultimate interest of consumer should be protected for electronic commerce to further flourish. Consumers should be able to identify the parties which they are talking with in the Internet, and be assured in ease to use way that all the conversation with the web site is from the genuine web site.

© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

# Reference


1. Domain Hijacking: A step-by-step Guide : http://www.securiteam.com/securitynews/Domain_Hijacking__A_step-by-step_guide.html

2. Verisgn Secure Site Seal : www.verisign.com

3. Thawte Authenticate Site : www.thawte.com

4. Secure Site by GlobalSign : www.globalsign.com

5. BIBLINK project : http://www.ariadne.ac.uk/issue17/biblink/

6. W2C Consortium XML Signature WG : http://www.w3.org/Signature/

7. IBM XML Security Suite : http://www.alphaworks.ibm.com/tech/xmlsecuritysuite


© SANS Institute 2000 - 2002, Author retains full rights.

Last Updated: May 19th, 2013

# Upcoming SANS Training

**Click Here for a full list of all Upcoming SANS Events by Location**

| | | | |
|---|---|---|---|
| **SANS Malaysia @ MCMC 2013** | **Cyberjaya, MY** | **Jun 03, 2013 - Jun 08, 2013** | **Live Event** |
| **SANS Pen Test Berlin 2013** | **Berlin, DE** | **Jun 03, 2013 - Jun 08, 2013** | **Live Event** |
| **Industial Control Systems Security Training - Houston** | **Houston, TXUS** | **Jun 10, 2013 - Jun 15, 2013** | **Live Event** |
| **Security Impact of IPv6 Summit 2013** | **Washington, DCUS** | **Jun 14, 2013 - Jun 16, 2013** | **Live Event** |
| **SANSFIRE 2013** | **Washington, DCUS** | **Jun 14, 2013 - Jun 22, 2013** | **Live Event** |
| **SANS Canberra 2013** | **Canberra, AU** | **Jul 01, 2013 - Jul 13, 2013** | **Live Event** |
| **SANS London Summer 2013** | **London, GB** | **Jul 09, 2013 - Jul 16, 2013** | **Live Event** |
| **Digital Forensics & Incident Response Summit 2013** | **Austin, TXUS** | **Jul 09, 2013 - Jul 16, 2013** | **Live Event** |
| **SANS Rocky Mountain 2013** | **Denver, COUS** | **Jul 14, 2013 - Jul 20, 2013** | **Live Event** |
| **SANS Mumbai 2013** | **Mumbai, IN** | **Jul 22, 2013 - Jul 27, 2013** | **Live Event** |
| **SEC528 SANS Training Program for the CompTIA® New Advanced Security Practitioner (CASP) Certification** | **Washington, DCUS** | **Jul 22, 2013 - Jul 26, 2013** | **Live Event** |
| **SANS San Francisco 2013** | **San Francisco, CAUS** | **Jul 29, 2013 - Aug 03, 2013** | **Live Event** |
| **SANS SEC 560: Network Penetration Testing @ Bangalore 2013** | **Bangalore, IN** | **Aug 05, 2013 - Aug 10, 2013** | **Live Event** |
| **SANS Boston 2013** | **Boston, MAUS** | **Aug 05, 2013 - Aug 10, 2013** | **Live Event** |
| **Critical Security Controls Summit** | **Washington, DCUS** | **Aug 12, 2013 - Aug 18, 2013** | **Live Event** |
| **Industrial Control Systems Security Training - DC** | **Washington, DCUS** | **Aug 12, 2013 - Aug 16, 2013** | **Live Event** |
| **Mobile Device Security Summit 2013** | **OnlineCAUS** | **May 30, 2013 - Jun 06, 2013** | **Live Event** |
| **SANS OnDemand** | **Books & MP3s OnlyUS** | **Anytime** | **Self Paced** |