Is Internet Explorer More Secure than FireFox?

eb connections. Using this example we discuss best practices in choosing an encryption product (assuming data should be encrypted). We then end with a discussion emphasizing how important it is for security professionals to create a security culture within an organization and how to handle the struggle between usability and security in a real world setting....

Is Internet Explorer More Secure than FireFox?

GIAC Gold Certification

Author: Lawrence Fortier, 4guys@centurytel.net

Adviser: Jim Purcell

Outline

Abstract

It is common practice to compare web browser security based on known exploits but this paper raises the idea that security is a broader concept and that there are other important issues that need to be considered. In this paper we look at how it is possible to circumvent a company’s security policy by using a web browser. Specifically, we compare Internet Explorer with FireFox web browser when connecting to a website that is not FIPS-140 compliant and the companies policy is to use FIPS-140 complaint algorithms for web connections. Using this example we discuss best practices in choosing an encryption product (assuming data should be encrypted). We then end with a discussion emphasizing how important it is for security professionals to create a ‘security culture’ within an organization and how to handle the struggle between usability and security in a real world setting.

1. Introduction

There was a significant increase in the amount of attacks against web applications in 2006 (Symantec Internet Security Threat Report, 2006). The Symantec report states that 7 of every 10 new vulnerabilities were in Web applications. This trend of attackers focusing increasingly on web based attacks, has fueled debate about which Web browser platform is the most secure (Richards, 2005; Yarden, 2004; Faas, 2005;Wildstrom, 2004). This paper will examine how you could put your organization at risk by not using Microsoft Internet Explorer with Microsoft Windows XP Professional SP2 and show that when comparing the security of different web browsers there is more to address than just software security vulnerabilities and exploits.

Internet Explorer is an integral part of Microsoft Windows XP Professional. It is an embedded component of the Windows XP Professional operating system and many windows applications rely on Internet Explorer to function properly. For example, some websites are designed to render properly for Internet Explorer only. More importantly, there are security settings that can be configured in Windows XP Professional to lock down Internet Explorer. These settings can be applied globally using the security configuration manager or with other Microsoft tools.

The security configuration manager allows an administrator to define specific security templates. These templates define a standard configuration for an Operating System which can be applied globally to all Windows XP Professional desktops. This can save time for administrators and, when properly applied, results in a consistent application of security policy throughout an organization.

One of the security settings that can be defined in a security template is the "System cryptology: Use FIPS compliant algorithms for encryption, hashing and signing" (Microsoft, 2005). This is a new setting introduced with windows XP Service Pack 2 (Microsoft, 2005).

When enabled, this setting forces strong encryption to be used by applications needing cryptographic services. Specific applications affected by this setting include Microsoft Internet Information Services (IIS), Microsoft Internet Explorer, Terminal Services, and the Encrypting File system (EFS). In this paper we will examine only the effect on Internet Explorer. When a client attempts to connect to a web server using Internet Explorer with the FIPS setting enabled they are allowed to use the TLS_RSA_WITH_3DES_EDE_CBC_SHA cipher suite only to establish the connection. This setting allows a secure (HTTPS) session to be initiated only if a FIPS 140-2 (Federal Information Processing Standard) approved algorithm for traffic encryption, key exchange, authentication and hashing is also used by the web server.

The National Institute of Standards and Technology (NIST) issues standards and guidelines to aide the Federal Government in the field of computer security (see http://csrc.nist.gov/publications/fips/index.html for a listing). These guidelines are referred to as the Federal Information Processing Standards (FIPS). The FIPS 140-2 list security requirements for cryptographic modules. These requirements are created by a group of cryptology experts in the government and private-sector. The National Institute of Standards and Technology recommends enabling the FIPS setting (NIST, 2005).

The Federal government and all its agencies are mandated to use only hardware or software which uses FIPS approved encryption algorithms to comply with regulations. Some websites do not use FIPS approved algorithms to negotiate TLS/SSL connections. What happens when business requirements do not match the security requirements? How does a company decide which cryptographic services they will use to protect the confidentiality, integrity, and availability of their data? In the discussion section we will examine these issues further. For now we will look at how the FIPS security policy affects the two different web browsers when negotiating a connection to a web server that does not support the TLS_RSA_WITH_3DES_EDE_CBC_SHA cipher suite.

2. Demonstration

For this demonstration we test a connection to www.mail.yahoo.com using either Internet Explorer 6 or Mozilla Fire Fox 2.0. This website does not use the TLS_RSA_WITH_3DES_EDE_CBC_SHA cipher suite to negotiate secure connections. Thus we will test site connection success with Firefox 2.0 and Internet Explorer 6.0 with the FIPS setting both enabled and disabled. Wireshark was used to capture the packets for the website connection attempt.

The default setting for Internet Explorer does not have TLS 1.0 checked. For this example this setting was selected and the attempt to connect to www.mail.yahoo.com was made. Figure 1 displays a portion of the client and server handshake where the SSL protocols are negotiated. You can see that at this point Internet Explorer offered 17 different ciphers to be used to initiate the connection. Ciphers are needed to protect the confidentiality and integrity of the data while it is in transit, for verification of the server, and possibly for verification of the client. Many ciphers are available to encrypt data and authenticate connections. How do client and server decide which to use? First, the server needs to support the selected cipher. Second, the client generally does not have any control over the protocol that will be used in the session. Thus, trust is given to the web site owner that a secure protocol will be used and that the server will choose the strongest of the clients' available ciphers.

The cipher suite chosen by the server in the aforementioned case was TLS_RSA_WITH_RC4_128_MD5. As can be seen in Figure 2, when attempting to connect with FireFox, the client offered 28 different cipher suites to the server. The server and client agreed to use the TLS_RSA_WITH_AES_256_CBC_SHA cipher suite. Both web browsers were able to connect to the web server in this case.

We then tested the connection with the "System cryptology: Use FIPS compliant algorithms for encryption, hashing and signing" security setting enabled. The client portion of the connection for Firefox offered up the same 28 cipher suites and the server used the same TLS_RSA_WITH_AES_256_CBC_SHA cipher suite to negotiate the connection. When trying to connect with Internet Explorer this time, the client only offered up one Cipher suite, the TLS_RSA_WITH_3DES_EDE_CBC_SHA (See Figure 3). This was the result of the security setting forcing the client to use this strong cipher to initiate TLS/SSL connections. However, the web server was not compliant with this cipher and the connection was not established. As can be seen, Firefox was unaffected by the FIPS security setting. This is because Firefox bypassed the enforced security policy of always using FIPS approved cryptographic services for encryption. The user was able to access the website and presumably would be able to complete their task. If this were a business related task then it would seem that Firefox succeeded where Internet Explorer failed. However the user did not know that by connecting to the website without a FIPS approved algorithm they were actually running afoul of company security policy.

3. Discussion

The main thrust of this analysis was the delineation of a specific instance where use of a particular web browser had negative impact on a company's security posture. It was shown how the FireFox web browser ignored a specific security setting that had been enabled in Windows XP Professional. Certainly, given the many security vulnerabilities for Internet Explorer, one must investigate possible alternative software for accessing the World Wide Web. However, as this paper indicates, there are other security issues that need to be taken into account before one reacts by replacing one piece of software for another. The take away message from this paper is that any time we evaluate the security of a certain piece of software we need to be aware of the environment in which the software will be used.

It is very important to have good security policies in place, but there also must be a way to ensure that these policies are being enforced. A policy for approving and testing software is required before it is installed on production systems. It is imperative to know your systems and how the different software applications interact together. Security is full of trade offs. As in the given example, prevention of one type of attack, such as ActiveX exploits, by using

Firefox Browser in place of Internet Explorer opened the door to other potential weaknesses by bypassing company security policy. Unfortunately there are many known flaws with Internet Explorer (Browser helper objects, ActiveX exploits) that need addressing. These vulnerabilities do increase a companies' vulnurability to attack; however, administrators must not create new security risks while trying to fix another.

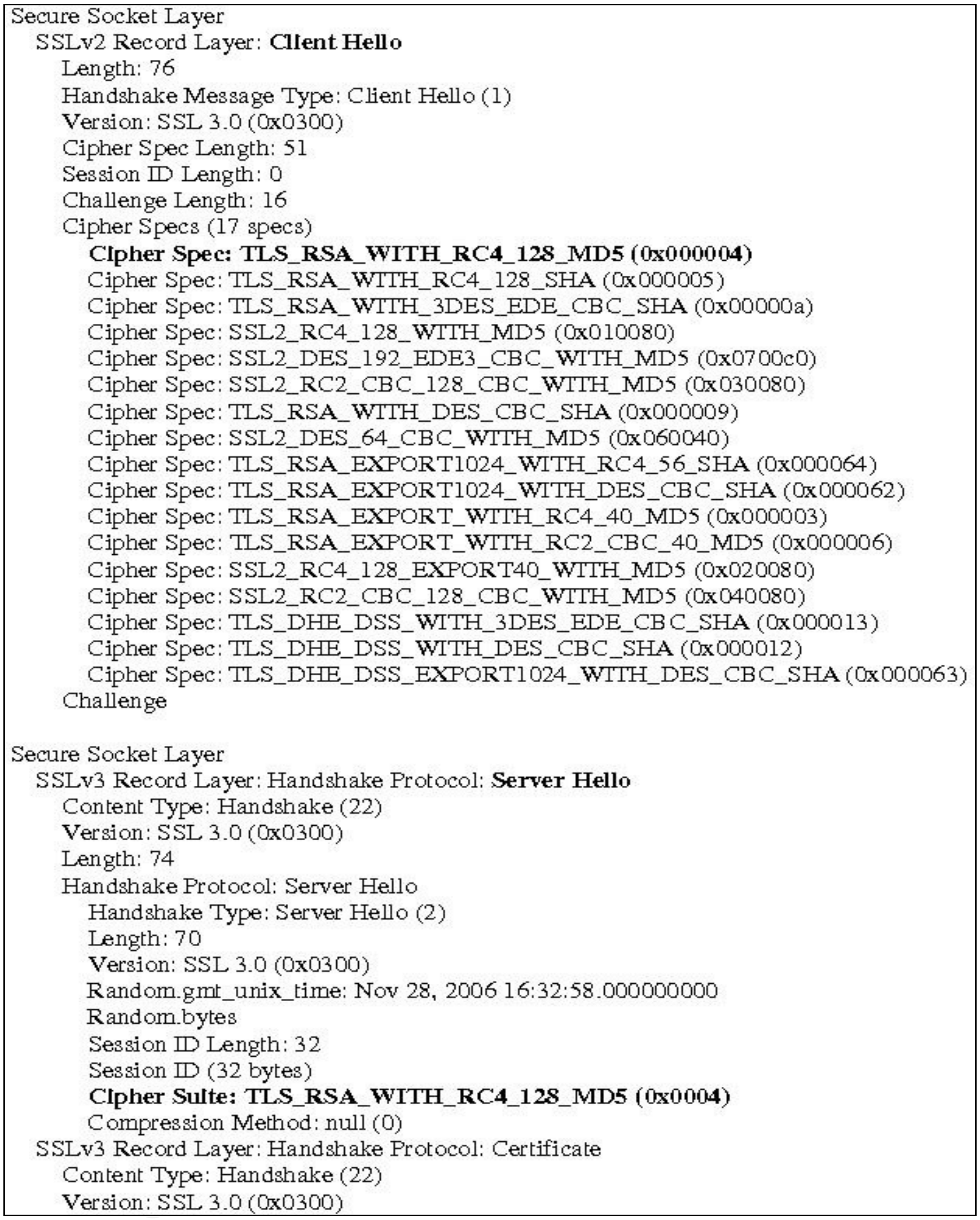
How can a company decide on an encryption policy that is, what to use and when? This paper discussed how NIST creates standards and certifications that are used by the Federal Government and this may be a good baseline for other companies to use for setting their own policy on which encryption products to use. However, it is also worth noting that not everyone believes in the value of certifying an encryption product. Bruce Schneier, a well-known expert in the field of cryptology, thinks that certification is largely a marketing tool (Salkever, 2002). He believes the true benefit comes when a cryptographic module is open source and that no single company alone can match the power or money that the Government can supply for analysis of Open Source Software (Schneier, 1999). It is from this position that Open Source Software for security becomes the best choice.

So, what happens when business requirements (such as accessing a web site to procure a sole source product) and security requirements (use only FIPS approved algorithms) differ? Should security requirements always trump business requirements in these cases? From a purely technical security standpoint, the answer should be yes. However, if a company cannot do business then there is no need for security. This is the age old standoff between security and business. In real world situations security professionals need to be flexible and must work to find appropriate alternatives, if in fact the security polices prevent business requirements to be fulfilled. This could help ease tensions between security professionals trying to do their job and business managers and executives trying to do their job.

It is becoming more and more important to create a 'culture of security' in any IT environment whether it is in the Government or Private sector. Each case will be different because there are different individuals who control the process. Some managers will be very aware of how important it is to secure companies data where others will be less so inclined. However, with the costs associated with data storage decreasing more data is being stored for longer periods of time. In order to protect this proliferation of data new regulations are being enacted which hold IT security professionals to a higher standard of accountability then in the past.

2. Figures

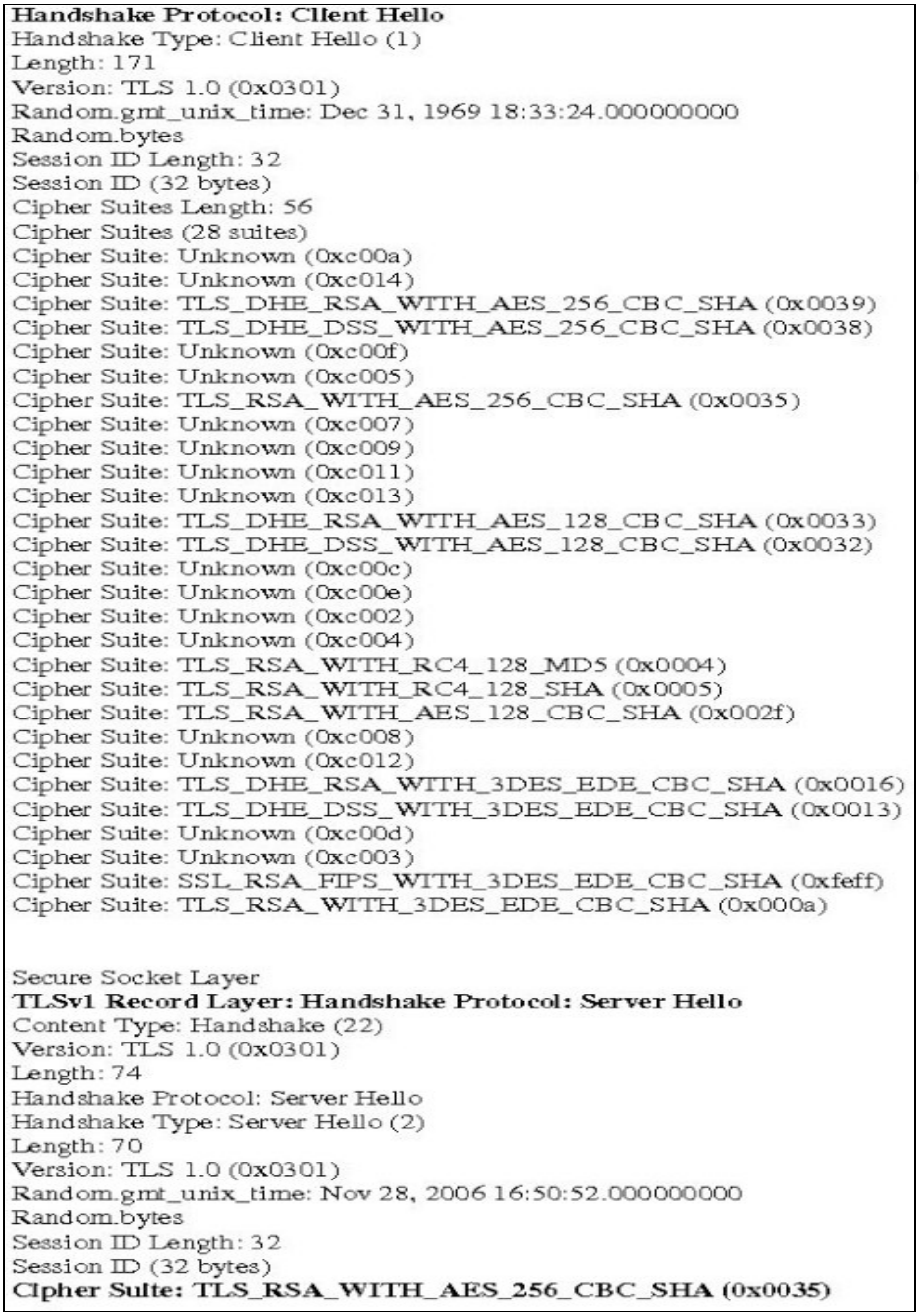
Figure 1 Wireshark packet capture for Internet Explorer with FIPS setting disabled



```
Secure Socket Layer
  SSLv2 Record Layer: Client Hello
    Length: 76
    Handshake Message Type: Client Hello (1)
    Version: SSL 3.0 (0x0300)
    Cipher Spec Length: 51
    Session ID Length: 0
    Challenge Length: 16
    Cipher Specs (17 specs)
      Cipher Spec: TLS_RSA_WITH_RC4_128_MD5 (0x000004)
      Cipher Spec: TLS_RSA_WITH_RC4_128_SHA (0x000005)
      Cipher Spec: TLS_RSA_WITH_3DES_EDE_CBC_SHA (0x00000a)
      Cipher Spec: SSL2_RC4_128_WITH_MD5 (0x010080)
      Cipher Spec: SSL2_DES_192_EDE3_CBC_WITH_MD5 (0x0700c0)
      Cipher Spec: SSL2_RC2_CBC_128_CBC_WITH_MD5 (0x030080)
      Cipher Spec: TLS_RSA_WITH_DES_CBC_SHA (0x000009)
      Cipher Spec: SSL2_DES_64_CBC_WITH_MD5 (0x060040)
      Cipher Spec: TLS_RSA_EXPORT1024_WITH_RC4_56_SHA (0x000064)
      Cipher Spec: TLS_RSA_EXPORT1024_WITH_DES_CBC_SHA (0x000062)
      Cipher Spec: TLS_RSA_EXPORT_WITH_RC4_40_MD5 (0x000003)
      Cipher Spec: TLS_RSA_EXPORT_WITH_RC2_CBC_40_MD5 (0x000006)
      Cipher Spec: SSL2_RC4_128_EXPORT40_WITH_MD5 (0x020080)
      Cipher Spec: SSL2_RC2_CBC_128_CBC_WITH_MD5 (0x040080)
      Cipher Spec: TLS_DHE_DSS_WITH_3DES_EDE_CBC_SHA (0x000013)
      Cipher Spec: TLS_DHE_DSS_WITH_DES_CBC_SHA (0x000012)
      Cipher Spec: TLS_DHE_DSS_EXPORT1024_WITH_DES_CBC_SHA (0x000063)
    Challenge

Secure Socket Layer
  SSLv3 Record Layer: Handshake Protocol: Server Hello
    Content Type: Handshake (22)
    Version: SSL 3.0 (0x0300)
    Length: 74
    Handshake Protocol: Server Hello
      Handshake Type: Server Hello (2)
      Length: 70
      Version: SSL 3.0 (0x0300)
      Random.gmt_unix_time: Nov 28, 2006 16:32:58.000000000
      Random.bytes
      Session ID Length: 32
      Session ID (32 bytes)
      Cipher Suite: TLS_RSA_WITH_RC4_128_MD5 (0x0004)
      Compression Method: null (0)
  SSLv3 Record Layer: Handshake Protocol: Certificate
    Content Type: Handshake (22)
    Version: SSL 3.0 (0x0300)
```

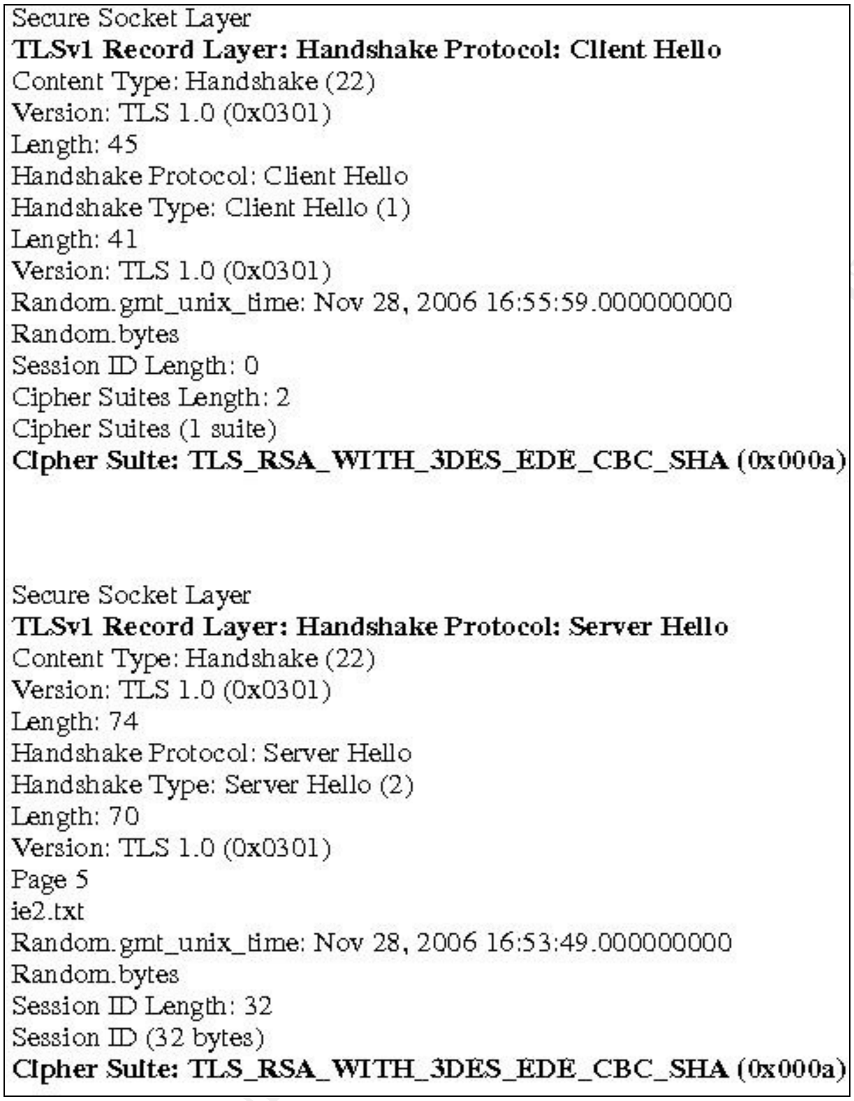
Figure 2 Wireshark packet capture for Mozilla Firefox with FIPS setting disabled



```
Handshake Protocol: Client Hello
Handshake Type: Client Hello (1)
Length: 171
Version: TLS 1.0 (0x0301)
Random.gmt_unix_time: Dec 31, 1969 18:33:24.000000000
Random.bytes
Session ID Length: 32
Session ID (32 bytes)
Cipher Suites Length: 56
Cipher Suites (28 suites)
Cipher Suite: Unknown (0xc00a)
Cipher Suite: Unknown (0xc014)
Cipher Suite: TLS_DHE_RSA_WITH_AES_256_CBC_SHA (0x0039)
Cipher Suite: TLS_DHE_DSS_WITH_AES_256_CBC_SHA (0x0038)
Cipher Suite: Unknown (0xc00f)
Cipher Suite: Unknown (0xc005)
Cipher Suite: TLS_RSA_WITH_AES_256_CBC_SHA (0x0035)
Cipher Suite: Unknown (0xc007)
Cipher Suite: Unknown (0xc009)
Cipher Suite: Unknown (0xc011)
Cipher Suite: Unknown (0xc013)
Cipher Suite: TLS_DHE_RSA_WITH_AES_128_CBC_SHA (0x0033)
Cipher Suite: TLS_DHE_DSS_WITH_AES_128_CBC_SHA (0x0032)
Cipher Suite: Unknown (0xc00c)
Cipher Suite: Unknown (0xc00e)
Cipher Suite: Unknown (0xc002)
Cipher Suite: Unknown (0xc004)
Cipher Suite: TLS_RSA_WITH_RC4_128_MD5 (0x0004)
Cipher Suite: TLS_RSA_WITH_RC4_128_SHA (0x0005)
Cipher Suite: TLS_RSA_WITH_AES_128_CBC_SHA (0x002f)
Cipher Suite: Unknown (0xc008)
Cipher Suite: Unknown (0xc012)
Cipher Suite: TLS_DHE_RSA_WITH_3DES_EDE_CBC_SHA (0x0016)
Cipher Suite: TLS_DHE_DSS_WITH_3DES_EDE_CBC_SHA (0x0013)
Cipher Suite: Unknown (0xc00d)
Cipher Suite: Unknown (0xc003)
Cipher Suite: SSL_RSA_FIPS_WITH_3DES_EDE_CBC_SHA (0xfeff)
Cipher Suite: TLS_RSA_WITH_3DES_EDE_CBC_SHA (0x000a)


Secure Socket Layer
TLSv1 Record Layer: Handshake Protocol: Server Hello
Content Type: Handshake (22)
Version: TLS 1.0 (0x0301)
Length: 74
Handshake Protocol: Server Hello
Handshake Type: Server Hello (2)
Length: 70
Version: TLS 1.0 (0x0301)
Random.gmt_unix_time: Nov 28, 2006 16:50:52.000000000
Random.bytes
Session ID Length: 32
Session ID (32 bytes)
Cipher Suite: TLS_RSA_WITH_AES_256_CBC_SHA (0x0035)
```

Figure 3 Wireshark packet capture for Internet Explorer with FIPS setting enabled



```
Secure Socket Layer
TLSv1 Record Layer: Handshake Protocol: Client Hello
Content Type: Handshake (22)
Version: TLS 1.0 (0x0301)
Length: 45
Handshake Protocol: Client Hello
Handshake Type: Client Hello (1)
Length: 41
Version: TLS 1.0 (0x0301)
Random.gmt_unix_time: Nov 28, 2006 16:55:59.000000000
Random.bytes
Session ID Length: 0
Cipher Suites Length: 2
Cipher Suites (1 suite)
Cipher Suite: TLS_RSA_WITH_3DES_EDE_CBC_SHA (0x000a)



Secure Socket Layer
TLSv1 Record Layer: Handshake Protocol: Server Hello
Content Type: Handshake (22)
Version: TLS 1.0 (0x0301)
Length: 74
Handshake Protocol: Server Hello
Handshake Type: Server Hello (2)
Length: 70
Version: TLS 1.0 (0x0301)
Page 5
ie2.txt
Random.gmt_unix_time: Nov 28, 2006 16:53:49.000000000
Random.bytes
Session ID Length: 32
Session ID (32 bytes)
Cipher Suite: TLS_RSA_WITH_3DES_EDE_CBC_SHA (0x000a)
```

3. References

1. Turner, D. (Ed.). (2006). Symantec Internet Security Threat Report (ed., Vol. 10). California

2. Richards, Ian (2005). Migrating to Mozilla Firefox: the Pros, Cons & Installation. Retrieved November 22, 2006, from Tech Support Alert Web site: http://www.techsupportalert.com/firefox.htm

3. Yarden, Jonathan (2005,10 14). Why you should think twice before ditching Internet Explorer. Retrieved November 22, 2006, from Tech Republic Web site: http://articles.techrepublic.com.com/5102-1009-5890288.html

4. Faas, Dennis (2005, 5 17). Which web browser is the most secure?. Retrieved November 22, 2006, from InfoPackets Web site: http://www.infopackets.com/channels/en/windows/gazette/2005/20050517_which_web_browser_is_the_most_secure.htm

5. Wildstrom, Stephen H. (2004, 6 29). Internet Explorer Is Just Too Risky. Retrieved November 22, 2006, from BW Online Web site: http://www.businessweek.com/technology/content/jun2004/tc20040629_7734_tc120.htm

6. Microsoft, (2005, 01). System cryptography: Use FIPS compliant algorithms for encryption, hashing, and signing. Retrieved March 23, 2007, from System cryptography: Use FIPS compliant algorithms for encryption, hashing, and signing Web site: http://technet2.microsoft.com/WindowsServer/en/library/6ff574cb-30c4-4ad9-8d5e-aee697c65b9b1033.mspx?mfr=true.

7. Microsoft, (2005, 01). FIPS 140 Evaluation. Retrieved March 23, 2007, from Microsoft TechNet Web site: http://www.microsoft.com/technet/archive/security/topics/issues/fipseval.mspx?mfr=true

8. National Institute of Standards and Technology. (2005). Guidance for Securing Microsoft Windows XP Systems for IT Professionals: A NIST Security Configuration Checklist (NIST Special Publication 800-68). MD: NIST.

9. Salkever, Alex (2002, October 1). Can software security be certified?. Retrieved January 19, 2007, from BW Online Web site: http://www.businessweek.com/technology/content/oct2002/tc2002101_6896.htm

10. Schneier, Bruce (1999, September 15). Crypto-gram newsletter. Retrieved January 19, 2007, from Crypto-Gram: September 15, 1999 Web site:http://www.schneier.com/crypto-gram-9909.html

Last Updated: May 25th, 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**
Digital Forensics & Incident Response Summit 2013	**Austin, TXUS**	**Jul 09, 2013 - Jul 16, 2013**	**Live Event**
SANS London Summer 2013	**London, GB**	**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&reg; 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**
SANS Thailand 2013	**Bangkok, TH**	**Aug 19, 2013 - Aug 31, 2013**	**Live Event**
SANS Virginia Beach 2013	**Virginia Beach, VAUS**	**Aug 19, 2013 - Aug 30, 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**