INTERNATIONAL JOURNAL OF RESEARCH IN COMPUTER APPLICATION & MANAGEMENT

IJRCM

A Monthly Double-Blind Peer Reviewed (Refereed/Juried) Open Access International e-Journal - Included in the International Serial Directories

Indexed & Listed at:

Ulrich's Periodicals Directory ©, ProQuest, U.S.A., EBSCO Publishing, U.S.A., Cabell's Directories of Publishing Opportunities, U.S.A.

as well as in Open J-Gage, India [link of the same is duly available at Inflibnet of University Grants Commission (U.G.C.)]

Registered & Listed at: Index Copernicus Publishers Panel, Poland & number of libraries all around the world.

Circulated all over the world & Google has verified that scholars of more than 1667 Cities in 145 countries/territories are visiting our journal on regular basis.

Ground Floor, Building No. 1041-C-1, Devi Bhawan Bazar, JAGADHRI – 135 003, Yamunanagar, Haryana, INDIA

www.ijrcm.org.in

CONTENTS

CALL FOR MANUSCRIPTS

We invite unpublished novel, original, empirical and high quality research work pertaining to recent developments & practices in the area of Computer, Business, Finance, Marketing, Human Resource Management, General Management, Banking, Insurance, Corporate Governance and emerging paradigms in allied subjects like Accounting Education; Accounting Information Systems; Accounting Theory & Practice; Auditing; Behavioral Accounting; Behavioral Economics; Corporate Finance; Cost Accounting; Econometrics; Economic Development; Economic History; Financial Institutions & Markets; Financial Services; Fiscal Policy; Government & Non Profit Accounting; Industrial Organization; International Economics & Trade; International Finance; Macro Economics; Micro Economics; Monetary Policy; Portfolio & Security Analysis; Public Policy Economics; Real Estate; Regional Economics; Tax Accounting; Advertising & Promotion Management; Business Education; Management Information Systems (MIS); Business Law, Public Responsibility & Ethics; Communication; Direct Marketing; E-Commerce; Global Business; Health Care Administration; Labor Relations & Human Resource Management; Marketing Research; Marketing Theory & Applications; Non-Profit Organizations; Office Administration/Management; Operations Research/Statistics; Organizational Behavior & Theory; Organizational Development; Production/Operations; Public Administration; Purchasing/Materials Management; Retailing; Sales/Selling; Services; Small Business Entrepreneurship; Strategic Management Policy; Technology/Innovation; Tourism, Hospitality & Leisure; Transportation/Physical Distribution; Algorithms; Artificial Intelligence; Compilers & Translation; Computer Aided Design (CAD); Computer Aided Manufacturing; Computer Graphics; Computer Organization & Architecture; Database Structures & Systems; Digital Logic; Discrete Structures; Internet; Management Information Systems; Modeling & Simulation; Multimedia; Neural Systems/Neural Networks; Numerical Analysis/Scientific Computing; Object Oriented Programming; Operating Systems; Programming Languages; Robotics; Symbolic & Formal Logic and Web Design. The above mentioned tracks are only indicative, and not exhaustive.

Anybody can submit the soft copy of his/her manuscript **anytime** in M.S. Word format after preparing the same as per our submission guidelines duly available on our website under the heading guidelines for submission, at the email address: infoijrcm@gmail.com.

GUIDELINES FOR SUBMISSION OF MANUSCRIPT

1. **COVERING LETTER FOR SUBMISSION:**

DATED: _____

THE EDITOR
IJRCM

Subject: **SUBMISSION OF MANUSCRIPT IN THE AREA OF .**

(e.g. Finance/Marketing/HRM/General Management/Economics/Psychology/Law/Computer/IT/Engineering/Mathematics/other, please specify)

DEAR SIR/MADAM

Please find my submission of manuscript entitled '_____' for possible publication in your journals.

I hereby affirm that the contents of this manuscript are original. Furthermore, it has neither been published elsewhere in any language fully or partly, nor is it under review for publication elsewhere.

I affirm that all the author (s) have seen and agreed to the submitted version of the manuscript and their inclusion of name (s) as co-author (s).

Also, if my/our manuscript is accepted, I/We agree to comply with the formalities as given on the website of the journal & you are free to publish our contribution in any of your journals.

NAME OF CORRESPONDING AUTHOR:
Designation:
Affiliation with full address, contact numbers & Pin Code:
Residential address with Pin Code:
Mobile Number (s):
Landline Number (s):
E-mail Address:
Alternate E-mail Address:

NOTES:

a) The whole manuscript is required to be in ***ONE MS WORD FILE*** only (pdf. version is liable to be rejected without any consideration), which will start from the covering letter, inside the manuscript.
b) The sender is required to mention the following in the **SUBJECT COLUMN** of the mail:
New Manuscript for Review in the area of (Finance/Marketing/HRM/General Management/Economics/Psychology/Law/Computer/IT/ Engineering/Mathematics/other, please specify)
c) There is no need to give any text in the body of mail, except the cases where the author wishes to give any specific message w.r.t. to the manuscript.
d) The total size of the file containing the manuscript is required to be below **500 KB**.
e) Abstract alone will not be considered for review, and the author is required to submit the complete manuscript in the first instance.
f) The journal gives acknowledgement w.r.t. the receipt of every email and in case of non-receipt of acknowledgment from the journal, w.r.t. the submission of manuscript, within two days of submission, the corresponding author is required to demand for the same by sending separate mail to the journal.

2. **MANUSCRIPT TITLE:** The title of the paper should be in a 12 point Calibri Font. It should be bold typed, centered and fully capitalised.

3. **AUTHOR NAME (S) & AFFILIATIONS:** The author (s) **full name**, **designation**, **affiliation** (s), **address**, **mobile/landline numbers**, and **email/alternate email address** should be in italic & 11-point Calibri Font. It must be centered underneath the title.

4. **ABSTRACT:** Abstract should be in fully italicized text, not exceeding 250 words. The abstract must be informative and explain the background, aims, methods, results & conclusion in a single para. Abbreviations must be mentioned in full.

5. **KEYWORDS:** Abstract must be followed by a list of keywords, subject to the maximum of five. These should be arranged in alphabetic order separated by commas and full stops at the end.

6. **MANUSCRIPT:** Manuscript must be in ***BRITISH ENGLISH*** prepared on a standard A4 size ***PORTRAIT SETTING PAPER***. It must be prepared on a single space and single column with 1" margin set for top, bottom, left and right. It should be typed in 8 point Calibri Font with page numbers at the bottom and centre of every page. It should be free from grammatical, spelling and punctuation errors and must be thoroughly edited.

7. **HEADINGS:** All the headings should be in a 10 point Calibri Font. These must be bold-faced, aligned left and fully capitalised. Leave a blank line before each heading.

8. **SUB-HEADINGS:** All the sub-headings should be in a 8 point Calibri Font. These must be bold-faced, aligned left and fully capitalised.

9. **MAIN TEXT:** The main text should follow the following sequence:

INTRODUCTION

REVIEW OF LITERATURE

NEED/IMPORTANCE OF THE STUDY

STATEMENT OF THE PROBLEM

OBJECTIVES

HYPOTHESES

RESEARCH METHODOLOGY

RESULTS & DISCUSSION

FINDINGS

RECOMMENDATIONS/SUGGESTIONS

CONCLUSIONS

SCOPE FOR FURTHER RESEARCH

ACKNOWLEDGMENTS

REFERENCES

APPENDIX/ANNEXURE

It should be in a 8 point Calibri Font, single spaced and justified. The manuscript should preferably not exceed ***5000 WORDS***.

10. **FIGURES & TABLES:** These should be simple, crystal clear, centered, separately numbered &self explained, and **titles must be above the table/figure**. **Sources of data should be mentioned below the table/figure**. It should be ensured that the tables/figures are referred to from the main text.

11. **EQUATIONS:**These should be consecutively numbered in parentheses, horizontally centered with equation number placed at the right.

12. **REFERENCES:** The list of all references should be alphabetically arranged. The author (s) should mention only the actually utilised references in the preparation of manuscript and they are supposed to follow **Harvard Style of Referencing**. The author (s) are supposed to follow the references as per the following:

- All works cited in the text (including sources for tables and figures) should be listed alphabetically.
- Use (**ed.**) for one editor, and (**ed.s)** for multiple editors.
- When listing two or more works by one author, use --- (20xx), such as after Kohl (1997), use --- (2001), etc, in chronologically ascending order.
- Indicate (opening and closing) page numbers for articles in journals and for chapters in books.
- The title of books and journals should be in italics. Double quotation marks are used for titles of journal articles, book chapters, dissertations, reports, working papers, unpublished material, etc.
- For titles in a language other than English, provide an English translation in parentheses.
- The location of endnotes within the text should be indicated by superscript numbers.

PLEASE USE THE FOLLOWING FOR STYLE AND PUNCTUATION IN REFERENCES:

BOOKS

- Bowersox, Donald J., Closs, David J., (1996), "Logistical Management." Tata McGraw, Hill, New Delhi.
- Hunker, H.L. and A.J. Wright (1963), "Factors of Industrial Location in Ohio" Ohio State University, Nigeria.

CONTRIBUTIONS TO BOOKS

- Sharma T., Kwatra, G. (2008) Effectiveness of Social Advertising: A Study of Selected Campaigns, Corporate Social Responsibility, Edited by David Crowther & Nicholas Capaldi, Ashgate Research Companion to Corporate Social Responsibility, Chapter 15, pp 287-303.

JOURNAL AND OTHER ARTICLES

- Schemenner, R.W., Huber, J.C. and Cook, R.L. (1987), "Geographic Differences and the Location of New Manufacturing Facilities," Journal of Urban Economics, Vol. 21, No. 1, pp. 83-104.

CONFERENCE PAPERS

- Garg, Sambhav (2011): "Business Ethics" Paper presented at the Annual International Conference for the All India Management Association, New Delhi, India, 19–22 June.

UNPUBLISHED DISSERTATIONS AND THESES

- Kumar S. (2011): "Customer Value: A Comparative Study of Rural and Urban Customers," Thesis, KurukshetraUniversity, Kurukshetra.

ONLINE RESOURCES

- Always indicate the date that the source was accessed, as online resources are frequently updated or removed.

WEBSITES

- Garg, Bhavet (2011): Towards a New Natural Gas Policy, Political Weekly, Viewed on January 01, 2012 http://epw.in/user/viewabstract.jsp

SECURING E-COMMERCE WEBSITES THROUGH SSL/TLS

PRADEEP KUMAR PANWAR
LECTURER
DEPARTMENT OF MCA
IEC GROUP OF INSTITUTIONS
GREATER NOIDA

ABSTRACT

Since the Web came into usage, more and more organizations are looking forward for providing services 24 by7 and 365 days to their users or customers. Updating the information as and when necessary has become need of the hour. Now a day's all the different transactions can be done online without much delay. Due to which, security has become a concern for the organizations that are providing services to the customer's online using e-commerce websites. But, as more and more options are coming up, websites are becoming vulnerable to attacks by eavesdropper, hackers whose main motive is to collect the information and tampering with the data, which leads to loss in business. Organizations are investing billions of money in securing their businesses. This paper gives an insight about how security could be provided to the E-commerce websites using different security techniques like SSL, basic concepts of SSL working and the existence of TLS for better security

KEYWORDS

Web, Eavesdropper, Hackers, E-commerce, SSL.

INTRODUCTION

The basic prerequisite of successful E-commerce website is the security it provides. And to prevent important information of users such as credit card number and transaction information from stealing and modifying on the internet, the security mechanisms like SSL or TLS have been adopted in present E-commerce websites. The reason for using such security techniques are, that there are many threats to the E-commerce application which takes place each time data is entered. Secure Sockets Layer (SSL), are cryptographic protocols that provide communication security over the Internet. TLS and SSL encrypt the segments of network connections at the Transport Layer, using asymmetric cryptography for key exchange, symmetric encryption for privacy, and message authentication codes for message integrity.

1. LIFE ON THE WEB WITHOUT SSL

Let us compare communications between computers on the Internet and communications between people over the telephone. Without SSL, your computer-to-computer communications suffer from the same security problems from which your telephone communications suffer:

- **Who are you talking to?** In a phone conversation, how can you be sure that the person who picks up the phone at the other end is really the person you are trying to call (especially if you have never spoken to them before)? What if your phone call was intercepted or re-routed, or what if someone else is answering your call recipient's phone? There really is no way to be sure you have reached the right person, especially if they are actively trying to fool you.
- **Eavesdropping?** As you are aware of from watching TV or reading, it is very easy to tap phone lines: the police and spies do this all the time to covertly gather information. It is not easy to detect if your lines are tapped. The same applies with communications over the Internet — how can you be sure that your communications are not being "tapped" and recorded? This is especially problematic in public wifi hotspots.

This results in two very real security issues for communications over the Internet:

1. Knowing for sure that you are connecting to the right servers (i.e. those at your bank and not those at a hacker's or phisher's web site).
2. Knowing that your data is safe from prying eyes during transit to those computers. This is where SSL comes in

2. HOW SSL CAME INTO EXISTENCE

SSL is a Netscape protocol created in 1992, which is basically used to exchange information securely between client browser and the server machine. It is a solution which is provided to implement security over the network to the users who are accessing the web. This is a protocol which sits between the transport layer and the application layer. There are two approaches to implement this protocol. Firstly, it could be provided as part of the underlying protocol suite and therefore be transparent to applications. Secondly, SSL can be embedded in specific packages.

2.1 UNDERSTANDING SSL

Varied options are available to access the Internet, as there exists dozens of independent systems. Due to easy availability unauthorized users can steal credit card numbers, PIN numbers, personal data, and other confidential information.

The Secure Sockets Layer (SSL) protocol was developed to transfer information privately and securely across the Internet. SSL is layered beneath application protocols such as HTTP, SMTP, and FTP and above the connection protocol TCP/IP. It is used by the HTTPS access method. Transport Layer Security (TLS) is the successor of Secure Sockets Layer (SSL); they are both cryptographic protocols that provide secure communications on the Internet for such things as web browsing, e-mail, Internet faxing, instant messaging, and other data transfers.

SSL uses public/private keys to provide a flexible encryption scheme that can be setup at the time of the secure transaction.

In typical encryption schemes the client and server would be required to use a secret key that has been preconfigured in the client and the server machines. In such a scheme, the client would use the secret key to encrypt the data. The server would use the same secret key to decrypt the data. Same logic applies in the server to client direction. These types of preconfigured secret keys are not suitable for Web based secure services that involve millions of users who have no prior secret key arrangement with the secure server.

SSL solves this problem by using asymmetric keys. These keys are defined in pairs of public and private keys. As the name suggests the public key is freely available to anybody. The private key is known only to the server. The keys have two important properties:

(1) Data encrypted by the client using the pubic key can be decrypted only by the server's private key. Due to this property of the keys, the client is able to send secure data that can be understood only by the server.

(2) Data encrypted to by the server's private key can only be decrypted using the public key. This property is useful in a client level authentication of the server. If the server sends a known message (say the name of the server), the client can be sure that it is talking to the authentic server and not an imposter if it is successfully able to decrypt the message using the public key.

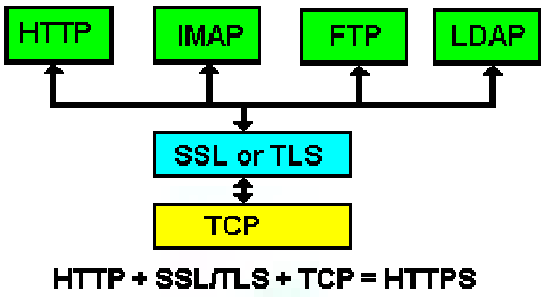
Note that property (1) allows us to use conventional secret keys. A secret key can be sent by the client as data that has been encrypted using the public key. This secret key can be decrypted only by the server. Once the server gets the key, the client and the server are able to communicate using this secret key.

The public/private key based encryption is used only for handshaking and secret key exchange. Once the keys have been exchanged the symmetric secret keys are used. This is done for two reasons:

(1) Public/private key based encryption techniques are computationally very expensive thus their use should be minimized.

(2) The secret key mechanism is needed for server to client communication.

SSL/TLS runs on top of TCP but below the end user protocol that it secures such as HTTP or IMAP as shown in following Figure:



HTTP + SSL/TLS + TCP = HTTPS

2.2 HOW SSL WORKS

The working of the SSL requires a client machine in the form of web server and web site server. The client side initiates the transaction and the server responds to the request for the transaction. During the request- response process SSL follows three different steps.

1. A session is initialised between the client and the server by Handshake protocol.
2. When the server authenticates the handshake protocol, data is transferred under the Record Protocol phase.
3. Alert protocol describes the severity of the message and description of the alert. I there are any alarms during the session, the alert is attached to the questionable packet and handled according to the alert protocol.

The four protocol layers of the SSL protocol (Record Layer, ChangeCipherSpec Protocol, Alert Protocol, and Handshake Protocol) encapsulate all communication between the client machine and the server.

2.2.1 RECORD LAYER

The record layer formats the Alert, ChangeCipherSpec, Handshake and application protocol messages. This formatting provides a header for each message, and a hash, generated from a Message Authentication Code (MAC) at the end. The fields that comprise the five-byte header of the Record Layer are: Protocol Definition (1byte), Protocol Version (2 bytes) and the Length (2 bytes). The protocol messages that follow the header cannot be longer than 16,384 bytes, as specified by the SSL protocol.(Thomas, 70)

2.2.2 CHANGECIPHERSPEC PROTOCOL

The ChangeCipherSpec layer is composed of one message that signals the beginning of secure communications between the client and server. Though the ChangeCipherSpec Protocol uses the Record Layer format, the actual ChangeCipherSpec message is only one byte long, and signals the change in communications protocol by having a value of '1'.

2.2.3 ALERT PROTOCOL

This protocol sends errors, problems or warnings about the connection between the two parties. This layer is formed with two fields: the Severity Level and Alert Description.

- **Severity Level**

The Severity Level sends messages with a '1' or '2' value, depending on the level of concern. A message with a value of '1' is a cautionary or warning message, suggesting that the parties discontinue their session and reconnect using a new handshake. A message with a value of '2' is a fatal alert message, and requires that the parties discontinue their session.

- **Alert Description**

The Alert Description field indicates the specific error that caused the Alert Message to be sent from a party. This field is one byte, mapped to one of twelve specific numbers, and can take on one of the following meanings. Those descriptions that always follow a "fatal" alert message are underlined. (Thomas, 73)

CloseNotify	UnexpectedMessage	BadRecordMAC	DecompressionFailure
HandshakeFailure	NoCertificate	BadCertificate	UnsupportedCertificate
CertificateRevoked	CertificateExpired	CertificateUnknown	IllegalParamete

2.2.4 SSL HANDSHAKE

The client always authenticates the server, and the server has the option of also authenticating the client. In general, Web servers do not authenticate the client during the Handshake Protocol because the server has other ways to verify the client other than SSL. For e-commerce, the Web-site server can verify the credit card number externally from the SSL session. In this way, the server can reserve precious processing resources for encrypted transactions.

During the Handshake Protocol, the following important steps take place: the session capabilities are negotiated, meaning the encryption (ciphers) algorithms are negotiated; and the server is authenticated to the client.

SSL uses symmetric cryptography for the bulk data encryption during the transfer phase; however, asymmetric cryptography, (that is, PKI) is used to negotiate the key used for that symmetric encryption. This exchange is critical to the Handshake Protocol. Note that the server may optionally ask the client to authenticate itself. However, it is not necessary to the protocol.

1. The handshake begins when a client connects to an SSL-enabled server, requests a secure connection, and presents a list of supported ciphers and versions.
2. From this list, the server picks the strongest cipher and hash function that it also supports and notifies the client of the decision.
3. Additionally, the server sends back its identification in the form of a digital certificate. The certificate usually contains the server name, the trusted certificate authority (CA), and the server's public encryption key. The server may require client authentication via a signed certificate as well (required for some on-line banking operations); however, many organizations choose not to widely deploy client-side certificates due to the overhead involved in managing a public key infrastructure (PKI).
4. The client verifies that the certificate is valid and that a Certificate Authority (CA) listed in the client's list of trusted CAs issued it. These CA certificates are typically locally configured.
5. If it determines that the certificate is valid, the client generates a master secret, encrypts it with the server's public key, and sends the result to the server. When the server receives the master secret, it decrypts it with its private key. Only the server can decrypt it using its private key.
6. The client and server then convert the master secret to a set of symmetric keys called a key ring or the session keys. These symmetric keys are common keys that the server and browser can use to encrypt and decrypt data. This is the one fact that makes the keys hidden from third parties, since only the server and the client have access to the private keys.
7. This concludes the handshake and begins the secured connection allowing the bulk data transfer, which is encrypted and decrypted with the keys until the connection closes. If any one of the above steps fails, the SSL handshake fails, and the connection is not created.

Though the authentication and encryption process may seem rather involved, it happens in less than a second. Generally, the user does not even know it is taking place. However, the user is able to tell when the secure tunnel has been established since most SSL-enabled web browsers display a small closed lock at the bottom (or top) of their screen when the connection is secure. Users can also identify secure web sites by looking at the web site address; a secure web site's address begins with https rather than the usual http.

4. SSL CRYPTO ALGORITHMS

SSL supports variety of cryptographic algorithms or ciphers.
→Key exchange algorithm: The asymmetric key algorithm used to exchange the symmetric key. RSA and Diffie Hellman are common examples.
→ Public key algorithm: The asymmetric key algorithm used for authentication. This decides the type of certificates used. RSA and DSA are common examples.
→ Bulk encryption algorithm: The symmetric algorithm used for encrypting data. RC4, AES, and Triple-DES are common examples.
→ Message digest algorithm: The algorithm used to perform integrity checks. MD5 and SHA-1 are common examples.

5. SSL VERSIONS

SSL brought different versions like SSLv2.0, SSLv3.0 but these protocols suffered from various vulnerabilities.
The SSLv2.0 protocol suffers from

- Re-usage of key material (message authentication and encryption) thus, in case of EXPORT ciphers unnecessarily weakening the MAC (not required by export restrictions)
- Ciphers marked as "Export" have an arbitrary small key size and can be cracked easily with today's hardware.
- weak MAC construction and supports only MD5 hash function
- padding length field is unauthenticated
- Downgrade attack – an attacker may downgrade the encryption to the lowest available and after doing so crack the keys.
- Truncation attacks – The attacker may reset the TCP connection.

Then the SSLv3.0 came into existence. In the:

1. SSL Version 3.0 handshake protocol flows are different than SSL Version 2.0 handshake flows.
2. SSL Version 3.0 uses the BSAFE 3.0 implementation from RSA Data Security, Inc. BSAFE 3.0 includes a number of timing attack fixes and the SHA-1 hashing algorithm. The SHA-1 hashing algorithm is considered to be more secure than the MD5 hashing algorithm. Having SHA-1 allows SSL Version 3.0 to support additional cipher suites which use SHA-1 instead of MD5.
3. SSL Version 3.0 protocol reduces man-in-the-middle (MITM) type of attacks from occurring during SSL handshake processing. In SSL Version 2.0, it was possible, though unlikely, that a MITM attack could accomplish cipher specification weakening. Weakening the cipher could possibly allow an unauthorized person to break the SSL session key since the secret material within the generate secret key would be considerable shorter.

Differences between SSLv3 and SSLv2

- Key material is no longer reused in both Message authentication and encryption making suites marked as EXPORT," stronger".
- MAC construction enhanced and support for SHA1 added
- SSLv3 adds protection of the Handshake, server-side can detect downgrade attacks
- SSLv3 adds support for a closure alert.

Both SSL2 and SSL3 have 16-bit (two-byte) version number fields.SSL2 interprets this as a single 16-bit integer, and the official number is 2, e.g. 0x0002.SSL3 interprets two-byte version numbers as a one byte "major" number and a one byte "minor" (or fractional) number. So the value 0x0002 is interpreted by SSL3 as version

Differences between TLS v1and SSLv3

0.2, not2.0.
After SSL, TLS came into existence which supersedes SSL. SSL v3.0 was actually renamed into TLS. SSL version 3.0 and its designated successor protocol Transport Layer Security (TLS) 1.0, which the Internet Engineering Task Force(IETF) published for the first time in 1999 [RFC2246]. The IETF published the most recent Internet-Draft for TLS 1.1 in Oct. 2002 [TLS].The TLS 1.0 specification described itself as being similar to but not backwards compatible with the SSL 3.0 specification. It did include a fallback mechanism for SSL 3.0 if TLS was not available. The IETF made some small changes and clarifications and publishedRFC4346 in 2006 detailing TLS 1.1. There is currently a working draft for TLS 1.2 (RFC Draft 4346) which expired in September 2007. Then came different versions of TLS and every new version is loaded with more security parameters providing safe data transfer over web.

Differences between TLS v1and SSLv3

- Expansion of cryptographic keys from the initially exchanged secret was improved
- MAC construction mechanism modified into an HMAC
- Mandatory support for Diffie-Hellman key exchange, the Digital Signature Standard, and Triple-DES encryption

Differences between TLS v1.1 and TLS v1 3

- The implicit Initialization Vector (IV) is replaced with an explicit IV to protect against CBC attacks4
- Handling of padding errors is changed to use the bad_record_mac
- Alert rather than the decryption_failed alert to protect against CBC attacks
- IANA registries are defined for protocol parameters.
- Premature closes no longer cause a session to be nonresumable.
- Additional informational notes were added for various new attacks on TLS

Differences between TLSv1.2 and TLSv1.1 5

- SHA-256 is the default digest method
- Several new cipher suites use SHA-256
- It has better ways to negotiate what signature algorithms the client supports
- Alerts are mandatory now be sent in many cases
- After a certificate_request, if no certificates are available, clients now MUST send an empty certificate list
- TLS_RSA_WITH_AES_128_CBC_SHA is now the mandatory to implement cipher suite
- Added HMAC-SHA256 cipher suites
- Removed IDEA and DES cipher suites, they are now deprecated.
- Support for the SSLv2 backward-compatible is now optional only.

RECOMMENDATION

After studying about SSL and TLS , it has been seen in paper that TLS provides better security measures for the websites which provides transactions and minimize the risk of tampering the data by the hackers, eavesdropper.

6. CONCLUSION

Security has always been a concern to the organizations which are dealing with the transactions at bulk. And to provide security they are looking for different security techniques which are successful in E-commerce websites. This paper highlights how SSL worked and the algorithms being used and how TLS takes the place and supersedes SSL and provide better security measures before the final transactions take place.

REFERENCES

1. Bartlett, Alan and Richard Silverman "SSH: The Secure Shell The Definitive Guide." 31 July 2001. URL: http://www.snailbook.com/ (3 March 2003)

2. Coleman, Mirean. "HIPAA Electronic Transactions Standards, Code Sets, and the Clinical Social Worker." National Association of Social Workers. July 2002. http://www.socialworkers.org/practice/hipaa/hippa.PDF(9 February 2003)
3. Cotter, Sean. "SSL Reference." 18 October 2000. URL: http://www.mozilla.org/projects/security/pki/nss/ref/ssl/ (10 March 2003).
4. Deitel, Harvey M., Paul J. Deitel & Tem R. Nieto. e-Business & e-Commerce How to Program. Upper Saddle River: Prentice Hall. 2001.
5. Dierks, T. & C. Allen. "The TLS Protocol Version 1.0." January 1999. (16 February 2003)
6. Elgamal, Taher. "The Secure Sockets Layer Protocol (SSL)." April 1995. URL:http://www.ietf.org/proceedings/95apr/sec/cat.elgamal.slides.html (3 March 2003)
7. "How Does Secure Socket Layer (SSL or TLS) Work ",http://luxsci.com/blog/how-does-secure-socket-layer-ssl-or-tls-work.html.
8. HTTP Essentials- *by Stephen Thomas*
9. Network Security with OpenSSL- *by John Viega, et al*
10. "SANS Institute InfoSec Reading Room",http://www.sans.org/
11. SSL & TLS Essentials- *by Stephen A. Thomas*
12. SSL and TLS-*by Eric Rescorla (Author)*
13. "SSL: Foundation for Web Security", The Internet Protocol Journal – Volume 1, No. 1 http://www.phaos.com/sslresource.html
14. "Supported SSL and Transport Layer Security (TLS) protocols", http://publib.boulder.ibm.com/iseries/v5r1/ic2924/index.htm?info/rzain/rzainrzaintls.htm
15. Thomas, Stephen. SSL and TLS Essentials: Securing the Web. New York: John Wiley & Sons, Inc. 2000
16. TLS/SSL hardening and compatibility report 2011, Author Thierry ZOLLER, www.g-sec.lu

REQUEST FOR FEEDBACK

Dear Readers

At the very outset, International Journal of Research in Computer Application and Management (IJRCM) acknowledges & appreciates your efforts in showing interest in our present issue under your kind perusal.

I would like to request you to supply your critical comments and suggestions about the material published in this issue as well as on the journal as a whole, on our E-mail **infoijrcm@gmail.com** for further improvements in the interest of research.

If you have any queries please feel free to contact us on our E-mail **infoijrcm@gmail.com**.

I am sure that your feedback and deliberations would make future issues better – a result of our joint effort.

Looking forward an appropriate consideration.

With sincere regards

Thanking you profoundly

Academically yours

Sd/-

Co-ordinator

ABOUT THE JOURNAL

In this age of Commerce, Economics, Computer, I.T. & Management and cut throat competition, a group of intellectuals felt the need to have some platform, where young and budding managers and academicians could express their views and discuss the problems among their peers. This journal was conceived with this noble intention in view. This journal has been introduced to give an opportunity for expressing refined and innovative ideas in this field. It is our humble endeavour to provide a springboard to the upcoming specialists and give a chance to know about the latest in the sphere of research and knowledge. We have taken a small step and we hope that with the active co-operation of like-minded scholars, we shall be able to serve the society with our humble efforts.

Our Other Journals