Volume 6, Issue 7, July 2016 ISSN: 2277 128X
International Journal of Advanced Research in Computer Science and Software Engineering
Research Paper
Available online at: www.ijarcsse.com

Cryptography Based E-Commerce Security

Ritu
Assistant Professor, Department of Computer Science & Applications,
Hindu Kanya Mahavidyalaya, Dhariwal,
Punjab, India

Abstract: ***E-commerce is a powerful tool for business transformation that allows companies to enhance their supply-chain operation, reach new markets, and improve services for customers as well as for providers. Implementing the E -commerce applications that provide Many businesses and consumers are wary of conducting business over the Internet due to a perceived lack of security. Electronic business is subject to a variety of threats such as unauthorised access, misappropriation, alteration and destruction of both data and systems. E-commerce has presented a new way of doing transactions all over the world using internet . computer use requires automated tools to protect files and other stored information and use of networks and communications links requires measures to protect data during transmission.This paper explores the major security concerns of businesses and users and describes the cryptographic techniques used to reduce such risks, explain the importance of E-commerce security and will discuss pretty good privacy, secure E-commerce protocol, public key infrastructure, digital signature and certificate based cryptography techniques in E-commerce security.***

Keywords: Trusted Third Party, Pretty Good Privacy, Public Key Infrastructure, Certificate Authority, Digital Signature, Secure Socket layer,

I. INTRODUCTION

A basic understanding of computer networks is requisite in order to understand the principles of network security .security must be part of the design. Security mainly specifies that how a particular "information" is protected. i.e., protection. Security makes the information to in access it by the third party. Any action that comprises the security of information wont by any organization. It mainly constitutes security attacks (Interruption, Interception, Modification, Fabrication). E-commerce refers to a wide range of online business activities for products and services. Security is the basic need to secure information on internet [1]. The success or failure of an e-commerce operation hinges on myriad factors, including but not limited to the business model, the team, the customers, the investors, the product, and the security of data transmissions and storage. Data security has taken on heightened importance since a series of high-profile "cracker" attacks have humbled popular Web sites, resulted in the impersonation of Microsoft employees for the purposes of digital certification, and the misuse of credit card numbers of customers at business-to-consumer e-commerce destinations. Security is on the mind of every e-commerce entrepreneur who solicits, stores, or communicates any information that may be sensitive if lost. An arms race is underway: technologists are building new security measures while others are working to crack the security systems. One of the most effective means of ensuring data security and integrity is encryption[2]

II. SECURITY AND E-COMMERCE

Security is one of the principal and continuing concerns that restrict customers and organizations engaging with ecommerce. The aim of this paper is to explore the perception of security in e commerce B2C and C2C websites from both customer and organizational perspectives [3] E-commerce businesses are growing, more secure technologies are being developed and improved every day. The current internet security polices and technologies fail to meet the needs of end users. The success or failure of an E-commerce operations hinges on myriad factors, including but not limited to the business model, the team, the customers, the investors, the product, and the security of data transmissions and storage. Any business that wants to have a competitive edge in today's global marketplace should adopt a comprehensive security policy in consultation with partners, suppliers, and distributors that will provide safe environment for the coming proliferation of E-commerce [4][5]. Public Key Infrastructure (PKI) refers to the notion that the best way to establish a system of secure communications over networks is to establish an infrastructure that will support public key encryption. The PKI would create an environment where any Internet user could "carry" certificates around that identify them in a variety of ways. Authentication of parties could become very cheap and easy. Some e-commerce proponents suggest that creation of a seamless and robust PKI would have enormous implications for speeding the growth of e-commerce, see figure 1.

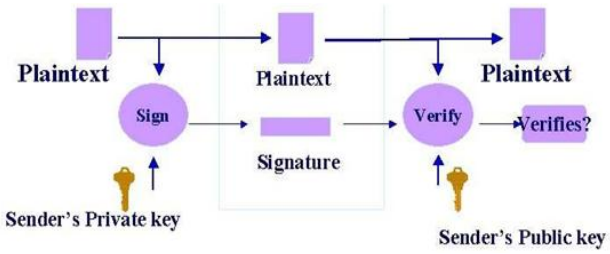

Figure 1: public key Infrastructure (PKI)

E-commerce software packages should also work with secure electronic transfer (SET) or secure socket layer (SSL) technologies for encryption of data transmissions. (SSL) protocols, which allow for the transmission of encrypted data across the Internet by running above the traditional TCP/IP protocols.

In cyberspace, both the customer and the vendor have difficulty in proving their identity to each other with certainty, particularly during a first transaction. How does the buyer securely transmit sensitive information to the seller? How does the seller know that this is a legitimate purchase order? How do both parties know that a nefarious third party has not copied and/or altered the transaction information? These questions and others, describe the problem effecting commercial transactions over the internet, or any public network.

Customer (clients) need to be sure that:-

1- They are communicating with the correct server.
2- What they send is delivered unmodified
3- They can prove that they sent the message.
4- Only the intended receiver can read the message.
5- Delivering is guaranteed.

On the other side, vendors (severer) need to be sure that:

1- They are communicating with the right client
2- The content of the received message is correct.
3- The identity of the author is unmistakable.
4- Only the author could have written the message.
5- They acknowledge receipt of the message.

All of the concerns listed above can be resolved using some combination of cryptographic method, and certificates methods[7].The type of risk involved resulting from inadequate security is:

1- Bugs or miss-configuration problems in the web sever that can cause the theft of confidential documents.
2- Risks on the Browsers' side i.e. breach of user's privacy, damage of user's system, crash the browser etc
3- Interception of data sent from browser to sever or vice versa. This is possible at any point on the pathway between browser and the server i.e. network on browser's side, network on server's side, end user's ISP (Internet Service Provider), the server ISP or either ISP's regional access.

III. CRYPTOGRAPHY

Cryptography schemes are often utilized to meet the basic security requirements of confidentiality and integrity in networks. But as the sensor nodes are limited in their computational and memory capabilities,the well-known traditional cryptographic techniques cannot be simply transferred to WSNs without adapting them.

3.1 Symmetric Cryptography

Symmetric encryption(also called as secret-key cryptography) uses a single secret key for both encryption and decryption as shown in Figure 2.

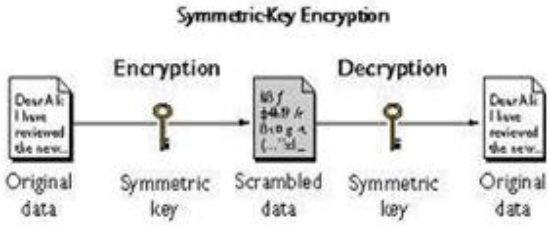

Figure 2: Symmetric -Key Cryptography

This key has to be kept secret in the network, which can be quite hard in the exposed environment where WSNs are usedto achieve the security requirements, several researchers have focused on evaluating crypto graphical algorithms in WSNs and proposing energy efficient ciphers. Symmetric key algorithms are much faster computationally than asymmetric algorithms as the encryption process is less complicated. Examples are AES, 3DES etc.

We first focus on Symmetric Cryptography due to the assumption that symmetric cryptography has a higher effectiveness and require less energy consumption, in contrast to public key cryptography.

According to [8]public key is used in some applications for secure communications eg.SSL(Secure Socket Layer) and IPSec standards both use it for their key agreement protocols.But it consumes more energy and it is more expensive as compared to symmetric key.

[9] has given a reason that public key consumes more energy due to great deal of computation and processing involved ,which makes it more energy consumptive as compared to symmetric key technique e.g. a single public key operation can consume same amount of time and energy as encrypting tens of megabits using a secret key cipher.

According to [10],the more consumption of computational resources of public key techniques is due to the fact that it uses two keys. One of which is public and is used for encryption ,and everyone can encrypt a message with it and other is private on which only decryption takes place and both the keys has a mathematical link, the private key can be derived from a public key.In order to protect it from attacker the derivation of private key from public is made difficult as possible like taking factor of a large number which makes it impossible computationally.Hence,it shows that more computation is involved in asymmetric key techniques thus we can say that symmetric key is better to choose for WSN.

According to [11] the cost of public key is much more expensive a s compared to symmetric key for instance, a 64 bit RC5 encryption on ATmega 128 8 MHZ takes 5.6 milliseconds,and a 160 bit SHA1 function evaluation takes only 7.2 millisecond's.These symmetric key algorithms are more than 200 times faster than Public key algorithms.

Public Key cryptography is not only expensive in computation but also it is more expensive in communication as compared to symmetric key cryptography.According to [12] to send a public key from one node to another, at least 1024 bits required to be sent if the private key is 1024 bits long.

Two types of symmetric ciphers are used: block ciphers that work on blocks of a specific length and stream ciphers that work bitwise on data. A stream cipher can be seen as a block cipher with a block length of 1 bit.

Law et al. [13] investigate in their survey in the evaluation of block ciphers for WSNs, based on existingliterature and authoritative recommendations. The authors do not only consider the security properties of thealgorithms, but additionally they try to find the most storage- and energy-efficient ones. To compare the differentblock ciphers, benchmarks are conducted on the 16-bitRISC-based MSP430F149 considering different cipher parameters, such as key length, rounds and block length; anddifferent operation modes, such as cipher-block chaining(CBC), cipher feedback mode (CFB), output feedback mode(OFB) and counter (CTR). Based on a review of differentcryptographic libraries, such as OpenSSL, Crypto++,Botan and Catacomb, most of the code was adapted fromOpenSSL [14]. Ciphers without public implementationswere implemented based on the original papers. For thecompilation of the sources the IAR Systems' MSP430 CCompiler was used. The evaluation results of the conductedbenchmarks show that the most suitable block ciphers forWSNs are Skipjack, MISTY1, and Rijndael, depending onthe combination of available memory and required securitylevel. As operating mode ―Output Feedback Mode (OFB)‖for pair wise links, i.e. a secured link between two peers, issuggested. In contrast, ―Cipher Block Chaining (CBC)‖ isproposed for group communications, for example, to enablepassive participation in the network.

Fournel et al. [15] investigate in their survey streamciphers for WSNs. The chosen stream cipher algorithms(DRAGON, HC-256, HC-128, LEX, Phelix, Py and Pypy,Salsa20, SOSEMANUK) are all dedicated to software usesand were originally submitted to the European ProjectEcrypt in the eStream call (Phase 2). To extend the selectionof stream ciphers, the famous RC4, SNOWv2 and AESCTRwere considered for evaluation. The performedbenchmarks on an ARM9 core based ARM922T aimedat finding the most storage-efficient and energy-efficientstream ciphers for this platform. Based on the methodologyof the eStream testing framework [16], four performancemeasures were considered: encryption rate for long streams,packet encryption rate, key and IV setup, and agility.Furthermore, the code size required for each algorithm onthe ARM9 platform was investigated. The used streamcipher algorithms, originally developed in C for thetraditional PC platform, were executed on the ARM9platform without any optimizations. The results of thebenchmarks show that the stream ciphers Py and Pypy, thetwo most efficiently running algorithms on traditional PCplatforms, do not work as fast on the ARM9 architecture. Incontrast, SNOWv2, SOSEMANUK and HC-128 performed similarly fast on both platforms. For SOSEMANUK, thekey setup was very huge in comparison to the key setup onthe traditional PC platform

3.2 Asymmetric Cryptography

Asymmetric encryption (also called public-key cryptography) uses two related keys (public and private) for data encryption and decryption, and takes away the security risk of key sharing. The private key is never exposed.

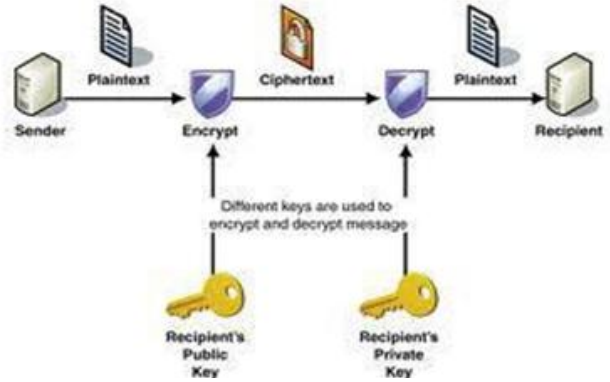

Figure 3: Asymmetric Key Cryptography.

A message that is encrypted by using the public key can only be decrypted by applying the same algorithm and using the matching private key. Likewise, a message that is encrypted by using the private key can only be decrypted by using the matching public key. Examples are RSA,ECC etc.

Public key Cryptography was omitted from the use in WSN because of its great consumption of energy and bandwidth which was very crucial in sensor network. Now a days a sensor become powerful in terms of CPU and memory power so, recently there has been a change in the research community from symmetric key cryptography to public key cryptography. Also symmetric key does not scale well as the number of nodes grows[17].

Arazi et al. [18] describe the efficiency of public-key cryptography for WSNs and the corresponding issues that need to be considered. Particularly, ECC is highlighted as suitable technique forWSN which provides a good trade-off between key size and security.

Liu and Ning [19] also emphasize that ECC is oneof the most efficient types of public key cryptographyin WSNs. The steps of design, implementation andevaluation of TinyECC, a configurable and flexible libraryfor ECC operations in WSNs, are presented. The libraryprovides a number of optimization switches that can becombined according to the developer's needs for a certainapplication, resulting in different execution times andresource consumptions. The TinyECC library was alsoevaluated on several sensor platforms; including MICAz,Tmote Sky, and Imotel; to find the most computationally efficient and the most storage efficient configurations.

In Public key Cryptography mostly two algorithms RSA and ECC use. The ECC is offer equal security for a far smaller key size than any other algorithm.So that it reducing processing and communication overhead. For example, RSA with 1024 bit keys (RSA-1024) provides a currently accepted level of security for many applications and is equivalent in strength to ECC with 160 bit keys (ECC-160) .To protect data beyond theyear 2010, RSA Security recommends RSA-2048 as the new minimum key size which is equivalent to ECC with 224 bit keys (ECC-224)[20].

[21]described the efficiency of public-key cryptography for WSNs and the corresponding issues that need to be considered. Particularly, ECC is highlighted as suitable technique for WSN which provides a good trade-off between key size and security. Lopez, 2006 focused on the security issues by analysing the use of symmetric cryptography in contrast with public-key cryptography. The author also discussed the important role of elliptic curve cryptography in this field.

A. RSA algorithm

A method to implement a public key cryptosystem whose security is based on the difficulty of factoring large prime numbers was proposed in [22].*RSA* stands for Ron Rivest, Adi Shamir and Leonard Adleman, who first publicly described the algorithm in 1977. Through this technique it is possible to encrypt data and create digital signatures.It was so successful that today *RSA* public key algorithm is the most widely used in the world.

IV. SUMMARY

The wireless sensor networks continue to grow and become widely used in many applications. So, the need for security becomes vital. However, the wireless sensor network suffers from many constraints such as limited energy, processing capability, and storage capacity, etc. There are many ways to provide security, one is cryptography. Selecting the appropriate cryptography method for sensor nodes is fundamental to provide security services in WSNs. Public Key based cryptographic schemes were introduced to remove the drawbacks of symmetric based approaches.

1. To be on the cutting edge of e-commerce, you need to understand how to best utilize cryptography to offer secure services for your customers over the Internet.
2. The success or failure of an e-commerce operation hinges on myriad factors, including but not limited to the business model, the team, the customers, the investors, the product, and the security of data transmissions and storage. Data security has taken on heightened importance since a series of high-profile "cracker" attacks have humbled popular Web sites, resulted in the impersonation of Microsoft employees for the purposes of digital certification, and the misuse of credit card numbers of customers at business-to-consumer e-commerce destinations.
3. Public Key Encryption ostensibly creates a world in which it does not matter if the physical network is insecure. Even if - as in the case of a distributed network like the Internet, where the data passes through many hands, in the form of routers and switches and hubs - information could be captured, the encryption scheme keeps the data in a meaningless form, unless the cracker has the private key.

REFERENCES

[1] William Stallings, "Cryptography and Network Security", 3rd edition, Prentice
[2] http://cyber.law.harvard.edu/ecommerce/encrypt.html
[3] Mohanad Halaweh, Christine Fidler -" Security Perception in E-commerce: Conflict between Customer and Organizational Perspectives". Proceedings of the International Multiconference on Computer Science and Information Technology, pp. 443 –449, ISBN 978-83-60810-14-9-2008- IEEE
[4] Paul A. Greenberg, "In E-Commerce We Trust ... Not ", E-commerce Time, February 2, 2001, URL:http://WWW.ecommercetimes.com/perl/story/?id=7194.
[5] Dave Chaffey, "E-Business and E-Commerce", 2nd , Prentice Hall, 2005
[6] V.SRIKANTH "ECOMMERCE ONLINE SECURITY AND TRUST MARKS". IJCET ISSN 0976 –6375, Volume 3, Issue 2, July September (2012)
[7] William Stallings, "Cryptography and network Security", 3rd edition, Prentice Hall,2003

[8] Ning P, Wang R and Du W (2005), ―An efficient scheme for authenticating public keys in sensor networks‖, Proceedings of the 6th ACM international symposium on Mobile ad hoc networking and computing, Chicago, IL, USA, pp. 58-67.

[9] Goodman J and Chandrakasan P (2001), ―An Energy Efficient Reconfigurable Public Key Cryptography Processor ‖, IEEE journal of solid state circuits, pp. 1808-1820, November 2001.

[10] RSA Security (2004), ―Cryptography ‖, Available at: http://www.rsasecurity.com/rsalabs/node.asp?id=2152.

[11] Ganesan P, Venugopalan R, Peddabachagari P, Dean A, Mueller F and Sichitiu M (2003), ―Analyzing and modelling encryption overhead for sensor network nodes ‖, In Proceeding of the Ist ACM international workshop on Wireless sensor networks and application, San Diego, California, USA, September 2003.

[12] Ling Tan, Shunyi Zhang, and Yanfeng Sun, Jing Qi ―Application of Wireless Sensor Networks in Energy Automation‖, Sustainable Power Generation and Supply, 2009. Supergen '09.International conference

[13] Y.W.Law,J.Doumen,andP.Hartel,*Survey and benchmark of block ciphers for wireless sensor networks*,ACM Transactions on Sensensor Networks(TOSN),2(2006),65-93.

[14] E.A.Young,T.J.Hudson,and R.S.Engelschall,*OpenSSL*.Availableonline:http://www.openssl.org/,2010

[15] N. Fournel, M. Minier, and S. Ub´eda, *Survey and benchmark of stream ciphers for wireless sensor networks*, in Information Security Theory and Practices: Smart Cards, Mobile and Ubiquitous Computing Systems, D. Sauveron, K. Markantonakis,A. Bilas, and J.-J. Quisquater, eds., vol. 4462 of Lecture Notes in Computer Science, Springer-Verlag, Berlin, 2007, 202–214.

[16] C. De Canni`ere, *eSTREAM Optimized Code HOWTO*. Available online: http://www.ecrypt.eu.org/stream/perf/, 2005.

[17] A. Liu and P. Ning, *TinyECC: a configurable library for elliptic curve cryptography in wireless sensor networks*, in Proc. of the International Conference on Information Processing in Sensor Networks (IPSN '08), St. Louis, MO,2008, 245–256

[18] The Scheme of Public Key Infrastructure for improving Wireless Sensor Networks Security Zhang Yu

[19] Arazi,B.,Elhanany,L.,Arazi,O.,Qi,H.,2005:Revising public –key cryptography for wireless sensor networks. IEEE Computer,38(11):103-105

[20] R.L.Rivest,A.Shamir,and L.Adleman,‖A method for obtaining digital signatures and public-key cryptosystems‖,Communications of the ACM,21(2):120-126,1978

[21] Kristin Lauter, Microsoft Corporation , ―The Advantages Of Elliptic CurveCryptography For Wireless Security IEEE Wireless Communications ,Vol 3,pp 22-25,February 2004.

[22] R.L.Rivest,A.Shamir,and L.Adleman,‖A method for obtaining digital signatures and public-key cryptosystems‖,Communications of the ACM,21(2):120-126,1978.

