THE USE OF CRYPTO-ANALYSIS TECHNIQUES FOR SECURING INTERNET TRANSACTIONS IN NIGERIA: CONCEPTS & ISSUES

Ojeme, B. O.
Mathematics & Computer Science Department,
Delta State University, Abraka, Nigeria.
ojeme@yahoo.com

ABSTRACT

Internet Transactions is growing at a rapid rate and has broken the territorial and geographical barriers that characterized traditional commerce. Despite the great potentials of internet transactions, security issues in Nigeria constitute a major challenge to its growth. More people could have embraced it but are constrained by security concerns, such as their personal and credit card information being intercepted by unauthorized persons (hackers). In this paper, the use of crypto-analysis techniques for securing internet transactions and applications was considered, and symmetric encryption technique was recommended to combine with other techniques, such as client-side software, data transaction protocols, web server software, and the network server operating system involved in handling e-commerce, for securing internet transaction. This recommendation will invariable ensure that internet transaction is secured.

Keywords: Cryptography, Encryption, e-transactions, Decryption, Internet Security Protocol, symmetric encryption techniques, web server.

INTRODUCTION

The emergence of internet has changed dramatically the way traditional businesses are carried out. Internet transaction is growing in leaps and bounds and many individuals, as well as organizations, are joining the bandwagon of using and providing e-commerce services.

Today, with the growth of Internet transaction in Nigeria, the consequences of unauthorized persons having access to others' information are grave. Most people shopping online for the first time are scared of using their credit cards to effect payments. They are concerned with what may happen to their credit card information, when supplied to an e-commerce site.

The distributed, concurrent, and real-time behaviour of e-transactions systems increases the complexity of e-commerce applications. Complex systems, naturally introduce many avenues by which they could be attacked. The more complex a system is, the more difficult it is to understand, analyse, and secure (Sommerville, 2007).

Ehikioya (2001) is of the opinion that e-commerce applications provide and ensure a secure environment by having security components for authorizing and authenticating users and encrypting of users' sensitive information for internet transactions. In the light of the above, there is a compelling need to ensure the integrity, privacy, confidentiality, and overall security of e-transactions and applications. The emergence of internet transaction has brought to the fore, the vexed concerns on security. Khalid *et al* (2011) describe security as enforcing policies that describe rules for gaining access to system resources.

Niranjanamurthy and Dharmendra (2013) identify Nonrepudiation, Authenticity, Integrity, Confidentiality, Availability, and Privacy as goals specific to internet or e-commerce transaction security. In the internet environment, Ghosh (1998) identifies four areas of vulnerability, which include: the web client, data communication, web server, and the oper-

ating system. Niranjanamurthy and Dharmendra (2013) and Ghosh (1998) identify Insider Abuse, Sniffing, Denial of Service Attacks, Spoofing, Hacking, Cyber vandalism, Credit card theft and Malicious code as threats to online transaction.

Therefore, this paper examines some cryptoanalysis techniques used in securing internet transactions and applications and, symmetric encryption techniques was recommended to combine with other techniques, such as client-side software, data transaction protocols, web server software, and the network server operating system involved in handling e-commerce, for securing internet transaction. The application of symmetric encryption techniques will go a long way in increasing the confidence of users in e-commerce as well as overall internet transactions.

DEFINITION OF SOME TERMS

Cryptography is the study of mathematical techniques related to aspects of information security such as confidentiality, data integrity, entity authentication, and data origin authentication (Menezes et al., 1998). Rabah (2004) defined it as the art and science of concealing data. Cryptology is also the discipline of cryptography and cryptanalysis combined and is fundamentally based on problems that are difficult to solve. A problem may be difficult because its solution requires some secret knowledge, such as decrypting an encrypted message or signing some digital document (Peter, 2011).

Encryption is the transformation of data into a form that is as close to impossible to read without the appropriate knowledge. Its purpose is to ensure security by keeping information hidden from anyone for whom it is not intended, even those who have access to the encrypted data. Decryption is the reverse of encryption and is the transformation of encrypted data back into an intelligible form.

MATERIALS AND METHODS

The fact-finding techniques used in information gathering were document review as well as research and site visit which entailed exploring the internet to search for information.

With the information-processing and telecommunications revolutions well underway, there is an increasing demand for techniques for keeping information secret, for determining that information has not been tampered with, and for determining who authored pieces of information. Cryptographic techniques are utilized in the areas of the Internet (Secure email, Internet browsers), the Financial Services Industry (E- cash, Instant teller banking), Telecommunications (Fax encryptors, Cable TV), and Wireless Communications (Pagers, Smart cards).

Cryptographic Tools

Cryptography entails the use of cryptographic tools to prevent and detect malicious actions. These are achieved through the use of cryptographic techniques such as Symmetric key encryption, Asymmetric key encryptions, hash functions and digital signatures. A schematic classification of these cryptographic techniques and their relationship according to Menezes *et al.* (1998) is presented in figure1:

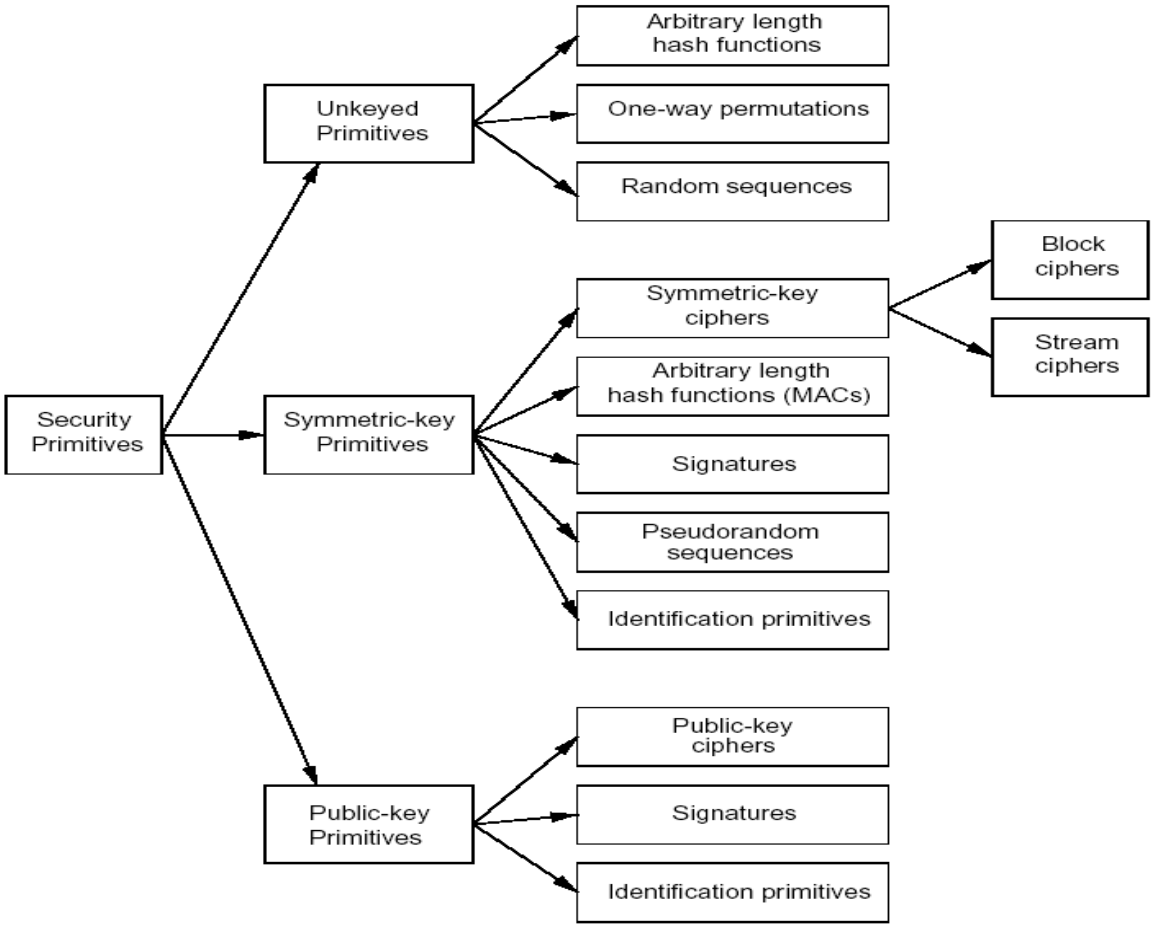

Figure1: A classification of cryptographic technique

Secure / Multipurpose Internet Mail Extensions (S/MIME) is a protocol that adds digital signatures and encryption to Internet MIME (Multipurpose Internet Mail Extensions) messages. MIME is the official proposed standard format for extended Internet electronic mail. Internet e-mail messages consist of two parts, the header and the body. The purpose of S/MIME is to define such services, which itself is the result of cryptographic processing on other MIME body sections. Information on MIME can be found at ftp://ftp.isi.edu/in-notes/rfc1521.txt.

Internet Security Protocols (IPSec) is defining a set of specifications for cryptographically-based authentication, integrity, and confidentiality services at the IP datagram layer. The IPSec group's results comprise a basis for interoperable secured host-to-host pipes, encapsulated tunnels, and Virtual Private Networks (VPNs), thus providing protection for client protocols residing above the IP layer. The protocol formats for IPSec's Authentication Header (AH) and IP Encapsulating Security Payload (ESP) are independent of the cryptographic algorithm, although certain algorithm sets are specified as mandatory for support in the interest of interoperability. The home page is http://www.ietf.org/html.charters/ipsec-charter.html.

Secure Shell (SSH) is a protocol which permits secure remote access over a network from one computer to another. SSH negotiates and establishes an encrypted connection between an SSH client and an SSH server, authenticating the client and server in any of a variety of ways (some of the possibilities for authentication are RSA, SecurID, and passwords). That connection can then be used for a variety of purposes, such as creating a secure remote login on the server (effectively replacing commands such as telnet and rlogin) or setting up a VPN (Virtual Private Network). SSH connections and their forwarding can be cascaded to give an authenticated user convenient secure windowed access to a complete

network of hosts. Other TCP/IP connections can also be tunneled through SSH to the server so that the remote user can have secure access to mail, the web, file sharing, FTP, and other services. More information about SSH is available from http://www.ssh.fi and http://www.vandyke.com.

Encryption Algorithmic Techniques
These are algorithm-based cryptographic tools for securing internet transactions. Such tools are symmetric encryption techniques, asymmetric encryption techniques, digital signature, and digital certificates.

Symmetric Encryption Techniques
In this encryption technique, a message is encoded by using a single key, which is usually a large integer number to encode and decode data (Schneider, 2002). The message's sender and recipient must know the key, since the same key is used for encryption and decryptions. This method is sometimes referred to as private-key encryption.

The merits of symmetric encryption techniques are speed and efficiency. However, the sender and recipient must ensure that the key is not known to anyone else. If the key is known to other persons, the information transmitted will be vulnerable to malicious attackers. The major defect of this technique is the difficulty involved in distributing new keys securely to authorized parties. Examples of this encryption technique are Advanced Encryption Standard (AES), Data Encryption Standard (DES), Triple DES, and RC4 (Chou, 2002). DES is the most widely used symmetric encryption system on the internet. The United States government uses DES for encrypting sensitive information. With respect to internet transaction, this encryption technique could be used in securing e-mails sent by e-commerce service provider to customers, stating the receipt of their orders and the status of the order.

Asymmetric Encryption Techniques
In Asymmetric (public-key) encryption techniques, a message is encoded using two mathematically related numeric keys (Schneider, 2002). In this technique, a pair of key, known as the public-key, is freely distributed to the public and those interested in communicating securely with the holder of both keys. This key is used to encrypt information. The second key, which is known as the private -key, is used to decrypt the encrypted information. Only the person that is to decrypt the message knows this key. Since this key is unique, only one secret key can open the message encrypted with a corresponding public-key and vice versa. A major demerit of this technique is the processor intensiveness of decrypting an encrypted message.

Digital Signature
A digital signature is the electronic equivalent of a personal signature that cannot be faked (Schneider, 2002). Encrypting a phrase with a private-key creates a digital signature (Menezes *et al.,* 1998). The encrypted phrase is attached to a message before it is sent to other persons or websites. Subsequently, the sender encrypts the entire message with the recipient's public-key and sends the message. On receiving the message, the recipient decrypts the message with a private-key. Lastly, the recipient decrypts the signature phrase using the sender's public-key. The problem of

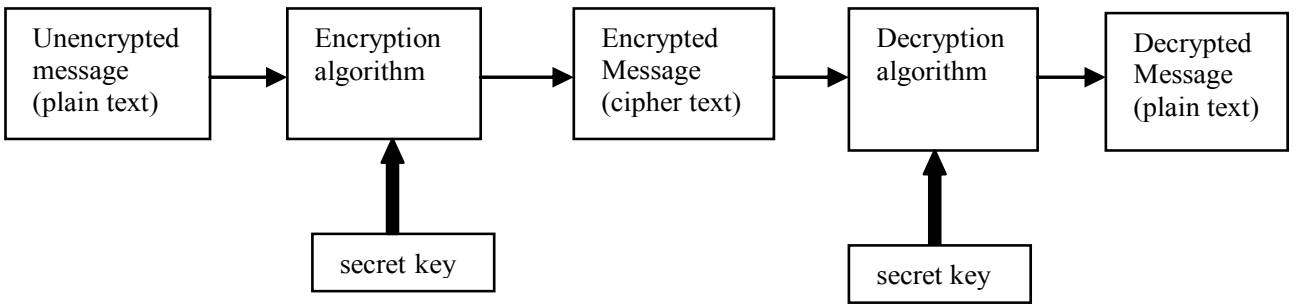

Figure1: A representation of private-key encryption scheme

using digital signatures is, it does not guarantee if the sender is really who he or she claims to be.

Digital Certificates

Digital certificate is the most commonly used algorithm-based cryptographic technique for securing e-commerce applications. It is an electronic signature that verifies the identity of a user or website (Menezes et al, 1998). A Certification Authority (CA) issues a digital certificate to an individual or organization. The digital certificates usually include information about the entity, its expiration date, and the entity's public-key. The CA requires entities applying for digital certificates to provide an adequate proof of identity. Once the CA has ensured that the entity is authentic, it issues the certificate to the entity. Thereafter, the CA signs the certificate by affixing its stamp of approval and encrypts the certificate with its public encryption key. The CA guarantees that the organizations and individuals receiving the certificates are authentic.

The general types of certificate we have are low, medium, and high assurance. Low assurance certificates are normally used to bind e-mail addresses to associated public-keys, while high assurance certificates are normally used for servers and organizations.

Secure Protocols

The aspect of online transaction that is most critical and prone to malicious attack is the data transmission between the web client and the e-commerce server. Expectedly, a lot of attention is being given to the security of this part of internet transaction. When a customer logs into the secured part of an e-commerce site, he inputs some very confidential information. This information is transmitted from the customer's system through a variety of channels before getting to the e-commerce server. The protocols that are used in encrypting the information provided by the client are S-HTTP, SSL and SET.

Secure HTTP (S-HTTP)

This is a connectionless protocol that wraps messages in a secure digital envelope (Schneider, 2002). If a site is secured by S-HTTP, a click on the URL link automatically links you to the secured part of the site's URL starting with https. Negotiations between a customer's web browser and an e-commerce site are complete when the security indicator, usually a padlock icon appears on the status bar. The customer logs into the secured part of the site and carries out the transaction after a negotiation is established.

Secure Sockets Layer (SSL) Protocol

This is the most widely used protocol for securing internet transactions. Netscape Incorporated developed this protocol for securing channels between web clients and web servers that chose to use it for its web sessions (Ghosh, 1998). SSL is a protocol in the network protocol stack that rides on top of the TCP/IP stack. SSL provides application-independent security between any number of application-level protocols that communicate over the internet (Ghosh, 1998). SSL works in two stages, handshake and data transfer. In the handshake stage, the client and server use a public-key encryption algorithm to ascertain the secret-key parameters. In the data transfer stage, both sides use the secret-key to encrypt and decrypt succeeding data transmissions. The client initiates an SSL handshake connection by first transmitting a message, which contains a list of secret-key algorithms and client supports. The server responds with a similar message and selects its preferred secret -key algorithm. After the message, the server sends a certificate, generated, validated, and verified by a certificate authority, which contains the public key. After the client has authenticated the server (the server can also request a certificate from the client), the two public-key algorithms determine secret-key information. After each side has indicated its willingness to use the secret key, the two sides complete the handshake phase with a finished message, which then enters the data transfer. During the data transfer phase, both sides break up their outgoing messages into fragments and append Message Authentication Codes (MACs) to them. For security reasons, the MAC key is different from the secret key; it is also computed during the handshake phase. During transmission, the client or server combines the data fragment, MAC, and

a record header and then encrypts them with the secret key to produce the completed SSL packet. When receiving, the client or server decrypts the packet, computes the MAC, and compares the computed MAC to the received MAC.

SSL In The Future

The major problem with the SSL protocol is that it requires a high amount of CPU processing power to encrypt and decrypt information (Chou, 2002). Chou (2002) posits that the problem with the protocol becomes apparent on the server side, because multiple web clients often connect to a single web server. Therefore, for online transactions, it is important to implement SSL in such a way that does not overstretch the web server's CPU and slow down the entire operation. Like Chou (2002), we propose that the use of SSL adapter cards, (as opposed to the current software implementation of the protocol) could alleviate the burden placed on e-commerce servers, and also believes that this approach will make the protocol more scalable, provide higher performance, provide increased security, and easier to administer.

Secure Electronic Transaction (SET) Protocol

One of the limitations of SSL is that it secures only transmitted data. Once data gets to the web server it does not have the functionality to secure the data at the server side. It cannot also authenticate the sender and recipient of a message. This implies that information, such as customer's credit card numbers on the web server could be vulnerable to malicious attack. These limitations in SSL led to the development of the SET protocol. Some implementations of the SET protocol are Cyber Cash and S/PAY (Ghosh, 1998).

How Set Protocol Works

A typical SET transaction according to Ghosh, (1998) entails (a)The customer sends request for transaction (b) E-commerce service provider acknowledges the request (c) The customer digitally signs a message digest of the order placed by him and encrypts the credit card number. (d) The e-commerce service provider sends the purchase amount for approval with the credit card merchant and the credit card number to the merchant's bank. (e) The e -commerce service provider receives the approval or denial from the credit card merchant. (f) The customer sends a status enquiry to the e-commerce service provider. (g) The e-commerce service provider requests to the purchase status inquiry. (h) The e-commerce service provider requests payment to the bank. (i) The bank sends confirmation of payment to the e-commerce service provider.

CONCLUSION

This paper presented various crypto-analysis techniques for securing e-commerce applications, and in general internet transactions. We recommend that symmetric encryption techniques should combine with protocols such as SET protocol and Internet Security Protocol along with other software components like the client-side software, data transaction protocols, web server software, and the network server operating system to ensure that internet transaction is secured. Compromising the security of any of these components creates a point of vulnerability or weakness. Also, adequate legal framework, policies, and procedures should be put in place to complement the technological framework, in order to safeguard users and e-commerce service providers against unanticipated security violations in the internet industry. However, the attempt at securing internet transactions from vulnerabilities should not result in system inflexibility for users. Hence, adequate balance should be struck between these two contending functionalities.

REFERENCE

Chou, W. (2002). Inside SSL: The Secure Sockets Layer Protocol, *IEEE IT Professional Journal* **4 (4):** 47 –52

Chou, W. (2002). Inside SSL: Accelerating Secure Transactions, *IEEE IT Professional Journal* **4 (5):** 37–41

Ehikioya S.A. (2001). A Formal Characterization of Electronic Commerce Transactions, *International Journal of Computer and Information Science* **2(3):** 97 -117

Ghosh, A.K. (1998). *E-commerce Security: Weak Links, Best Defences,* John

Wiley, New York.

Khalid, H., Muhammad, A., Shoukat, A. and Shazia, Y. (2011). Secure E-Commerce Protocol. *International Journal of Computer Science and Security* (IJCSS), **5 (1):** 132-142.

Menezes, A., Oorschot, P. V. and Vanstone, S. (1998). Handbook of Applied Cryptography, CRC Press, Boca Raton.

Niranjanamurthy, M. and Dharmendra, C (2013). The study of E-Commerce Security Issues and Solutions. *International Journal of Advanced Research in Computer and Communication Engineering* **2 (7):** 2885-2895.

Rabah, K. (2004). Data Security and cryptographic techniques – A review. *Information Technology Journal* **3(1):** 106-132

Peter Schwabe (2011). *High-Speed Cryptography and Cryptanalysis.* University of Technology, Eindhoven.

Sommerville, I. (2007). *Software Engineering,* 8th Edition, Pearson Education Ltd., New Jersey.

Schneider, G. (2002). New Perspectives on E -commerce: Comprehensive, Course Technology Publishers.