December 2002

ENCRYPTION AND TRANSACTION SECURITY: OBSERVATIONS AND ANALYSIS

Y. Shin
Campbell School of Business

ENCRYPTION AND TRANSACTION SECURITY: OBSERVATIONS AND ANALYSIS

Y. B. Shin
Campbell School of Business
Berry College
yshin@campbell.berry.edu

Abstract

E-business, business-to-business, and E-commerce are words that emulate the most common uses for the Internet of today and tomorrow. The challenges of using the Internet, as experienced early in the 1980s with desktop computing, is the assurance of the accuracy, credibility, and speed with which each transaction is concluded via the Internet. The global network of to day's business world deals with the passage of information between parties in the conduct of business]. Within that context, each transmission to support a transaction must guarantee the identities of the parties, guarantee the information passed has not be altered, guarantee the confidentiality of the data in transit, and protect against denial of the transaction's intent by one of the parties. The non-repudiation of each transaction must be secured. To meet these exacting demands, the capabilities of encryption hardware and software are paramount to guaranteeing transaction security.

Introduction

Encryption is the conversion of data into a form, called a cipher text, which cannot be easily understood parties or personnel not authorized to 'view' the data. The technology in use over the last number of years scrambles or encodes the original into a form that is unreadable. The 'scrambled' message is shattered into a million fragmented sections remains for transmission and reception. This data stream appears as symbols, letters, and numerals without any discernable form (Storey, 2000).

During World War I and World War II, both Axis and Allies Forces used various forms of ciphers, often incorrectly called "codes," that was employed to keep the enemy from obtaining the contents of many tactical and strategic radio (RF) transmissions. In later year, simple ciphers included the substitution of letters for numbers, the rotation of letters in the alphabet, and the "scrambling" of voice signals by inverting the sideband frequencies. More complex cipher work according to sophisticated computer algorithms that rearrange the data bits in digital signals (whatis.techtarget.com).

In order to easily recover the contents of an encrypted signal, the correct decryption key is required. Decryption is process of converting encrypted data back into its original form. The key used for decryption is an algorithm -a mathematical analogy or formula that "undoes" the work of the encryption process. The more complex the encryption algorithm, the more difficult it becomes to eavesdrop on the communications without access to the keys involved in the information exchange.

The 'key' is a unique stamp or identity pass used to allow the encryption and decryption process to commence. The Public Key Infrastructure (PKI) is a system of cryptography utilized in the e-commerce arena requiring the use of two keys; one in which the possession n maintained by a private entity. The other key is freely given away and is therefore considered public. Embedded within governing software systems on WAN, LAN, or business systems, the keys are proofs of identity that must be validated by a third party in the form of certificates. Third party entities in the e-business world are RSAC, VeriSign, Symantec, and McAfee. A third party issues these certificates to authenticate the identity of the buyer, contractor, or users holding the public key and named on the document.

Public Key (PKI) encryption is used not only in browsers and web transactions also, in secure email. Microsoft, Louts, Netscape, and Novell all support a standard called secure multipurpose Internet mail extensions (S/MIME). This provides the users of secure

email the capability to discuss and exchange sensitive, legally binding, contractual documents among clients. Couple this technology with U.S Congress's enactment of the Electronic Signatures in Global and National Commerce Act 2000, provides for documents and transactions being conducted via the web to have the same legal validity and enforceability as paper records and handwritten signatures (Moss, 2000).

Another encryption system to safeguard business transactions, based on the PKI design is the Secure Socket Layer (SSL). SSL has become the de facto standard for client-to-serve encryption on the Internet (Schultz, 2000). Developed by Netscape, SSL uses both public and private keys to authenticate users. Within a network, the client sends the server its certificate -digitally signed to authenticate the client's identity. Once the key exchange has taken place, a share secret key is used to encrypt all further data transmission between the server and client(s). For the CPU, a very intensive mathematical and performance tasking operation to conduct secure transactions. In small businesses were the server and clients handle the transactions, this is normally standard. In large corporations where CPU performance is sacred to business success, SSL has been incorporated into front-end processors in most Ethernet systems of today. These networks devices have grown from the firewalls, routers, and hubs of earlier network design. The Cyber IQ E-commerce Controller and Intel Net Structure 7115 E-commerce Accelerator separate the SSL functionality from the browsers and servers to allow them to operate as stand alone network, hardware. Positioned between the firewall and the server, these SSL appliances operate as high performance engines that offload the CPU-intensive key negotiation as well as the bulk encryption of the data from the web server. It operates independent of the server, but in concert with the server to ensure network transaction security. Additionally, with a one-to-many relationship, you have to update and manage your server certificates at only one location -the SSL appliance.

An additional device using SSL technology is the advent of the virtual private network (VPN), offering hardware based encryption module that boosts network performance to 90Mbps at 168-bit level of encryption. CISCO's 7140 VPN is an advanced site-to-site device that may serve as a firewall, but will ensure the integrity of e-business transactions (Schultz, 2000).

The National Institute of Standards and Technology (NIST) set the standards for encryption in the U.S.. The Data Encryption Standard (DES) supports key sizes of 40,56,64,80, 112, 128, and 192-bit encryption. Normal U.S. businesses use 1 28-bit SSL encryption with overseas business transactions being limited to the 56-bit SSL option (Johnson, 2000).

Encryption/decryption is especially important in wireless communications. This is because wireless circuits are easier to "tap" than their hard-wired counterparts. Nevertheless, encryption/decryption is a good idea when carrying out any kind of sensitive transaction, such as a credit-card purchase online, or the discussion of a company secret between different departments in the organization. The stronger the cipher --that is, the harder it is for unauthorized people to break it --the better, in general. However, as the strength of encryption/decryption increases, so does the cost.

In recent years, a controversy has arisen over so-called strong encryption. This refers to ciphers that are essentially unbreakable without the decryption keys. While most companies and their customers view it as a means of keeping secrets and minimizing fraud, some governments view strong encryption as a potential vehicle by which terrorists might evade authorities. These governments, including that of the United States, want to set up a key-escrow arrangement. This means everyone who uses a cipher would be required to provide the government with a copy of the key. Decryption keys would be stored in a supposedly secure place, used only by authorities, and used only if backed up by a court order. Opponents of this scheme argue that criminals could hack into the key-escrow database and illegally obtain, steal, or alter the keys. Supporters claim that while this is a possibility, implementing the key escrow scheme would be better than doing nothing to prevent criminals from freely using encryption/decryption.

Encryption advances like PKI, PHI, SSL, and configured devices are all the core technology for the new market place as it is fundamental for enabling secure e-commerce. Today, e-commerce is limited for most people to credit card transaction, in effect, old technologies adapted to a new world. Once underwritten by law, e-commerce can be used for transactions ranging from micro payments to payments of hundreds of millions of euro-dollars. Voting and other community services can be implemented reliably, such as tax returns and driving license applications. The future of e-commerce is bound by the accessibility and security of the Internet.

If this research is accepted, the report presented at the conference will be an up-date on products and technologies to improve overall performance of cyber transactions. Several measurements on the products and emerging technology will be assessed before the conference. Thus the results will be available in time for the conference and should provide interesting and helpful content to those examining emerging technology for e-commerce.

References

Johnson, Margaret, "Commerce Department Se1ects Crypto Standard," Network World (17:41), October 9, 2000, p.44.
Moss, Va]ene, "Congress Enacts New E-Signature Law," Credit Union Magazine (66:9), September 2000.
Schultz, Keith, "Network Infrastructure – SSL in the Driver's Seat," IntemetWeek, Issue 837, November 3, 2000, P. 49.
Schultz, Keith, "Network Infrastructure-The All in One VPN Router," IntemetWeek, Issue 829, Manhasset, September 18, 2000, P. 40
Storey, Domimc, "Securing e-business; Telecommunications, Dedham," International Edition (34:2), February 2000, p.45-47.