Cryptography best practices and resource portfolio business plan example

Sociology, Communication

Cryptography Best Practices and Resource Portfolio:

For the purpose of the presentation, the company that will be the focus of this project is Amazon. com. Its central offering is online shopping where consumers are able to search for the items they'd like to purchase online. They are also able to pay for their purchases online and have the items delivered to their home. In this e-business, the categories of information that may need applications of cryptography are the users' or consumers' passwords and their credit card or checking account numbers.

Public Key Infrastructures

A Public Key Infrastructure (PKI) is an architecture that is developed to increase the level of confidence when exchanging information over the Internet, which is becoming more and more insecure (ArticSoft Technologies Limited, 2012). However, it can also be used for information exchange over private and corporate internal networks. Moreover, it can be used to ensure that cryptographic keys are securely delivered between users, devices, or servers. In addition, it facilitates " other cryptographically delivered security services" (ArticSoft Technologies, Limited, 2012).

Some experts also use the term PKI to refer to the use of a pair of public key and private key for the proof and authentication of content. With the use of a PKI, users are assured of the quality of information that is electronically sent and received, as well as the source and destination of the said information. In addition, it assures the user of the time and timing of information, its privacy, and its validity when introduced as evidence in court proceedings. It should be noted that these functions are facilitated by public key

cryptography, which is a mathematical technique that uses 2 related cryptographic keys for verifying the sender’s privacy and for ensuring privacy.

Internet Protocol Security and Architecture

With the Internet Protocol Security (IPSec) and Architecture, the data that is being communicated is secured at the Internet protocol (IP) layer for the reason that the IP layer “ can capture all packers sent from the higher-layer protocols and applications and all packets received by the lower-layer network protocols” (Cheng, Garay, Herzberg & Krawczyk, 1998). Moreover, the security at this layer is not dependent on the lower-layer protocols. As well, it’s possible for the security at this layer to be made transparent to higher layer applications and protocols. In addition, the environments that can benefit from IPsec include system-to-system or site-to-site communication, telecommuting, and mobile-to-base communication.

Internet Key Exchange

The Internet Key Exchange (IKE) protocol “ is a key management protocol standard, which is used in conjunction with the IPsec standard” (Cisco Systems, Inc., 2001, p. 3). Although it’s possible to configure IPSec without IKE, IKE can improve the IPSec standard through the addition of more features, the ease of configuration, and flexibility. In particular, IKE manages the IPsec security associations on behalf of IPsec. It also enables the automatic negotiation of “ protection policies between IPsec peers” (Cisco Systems, Inc., 2001, p. 3).

A hybrid protocol, IKE is based on ISAKMP (Internet Security Association and Key Management Protocol), which allows for the authentication of the remote peer, the cryptographic protection of the management session, and the information exchange for key exchange. In addition, IKE implements parts of the Oakley and SKEME protocols.

Secure Socket Layer

Originally developed by Netscape, the Secure Socket protocol ensures the secure transportation and routing of data through the LDAP, HTTP, or POP3 layer. With the Secure Socket Layer's (SSL) design, it is able to use TCP as a communication layer in order to provide an authenticated and a reliable end-to-end secure connection between 2 points over a network, an example of which is the connection between the server and the service client. In addition, it can be used to protect transmitted data over any network service, which is mostly used in client applications and HTTP servers. Today, most HTTP servers have the capability of supporting an SSL session while Netscape Navigator and Internet Explorer come with SSSL-enabled client software.

SSL authenticates the client and the server. It also ensures data integrity and data privacy. Furthermore, it should be noted that SSL does not consist of only a single protocol but is made up of a set of protocols, which are divided into the following layers: 1.) the protocol that ensures data integrity and security (SSL Record Protocol); and 2.) the protocols that establish an SSL connection (SSL Alert protocol; SSL ChangeCipher SpecProtocol; and SSL Handshake protocol).

S/MIME Functionality

After the development of S/MIME version 2, S/MIME becomes the standard for message security (Microsoft, 2012). The two main security services that S/MIME provides are digital signatures and message encryption, both of which also serve as the bases for message security.

Digital signatures, which is the more commonly used S/MIME service, serve as the digital counterpart of the legal and traditional signature on a printed document. Digital signatures provide authentication of one's identity. It also enables nonrepudition. In particular, digital signatures are unique, which means that the owner cannot disown them. In addition, it provides data integrity in that it assures the recipient that the message received was the same message that was signed and sent.

While digital signatures provide data integrity, they do not provide confidentiality as the digital signatures are in cleartext. To ensure confidentiality, message encryption is required. Message encryption changes the format of the information to one that is not readable and understandable until it is changed back to a format that can be read and understood. However, it should be noted that while message encryption provides confidentiality and data integrity, it does not provide authentication and nonrepudiation.

Secure Electronic Transaction (SET)

A protocol that can potentially become a dominant force in the security of electronic transactions, Secure Electronic Transaction (SET) has been

developed jointly by Visa and MasterCard, together with the top computer vendors such as IBM (“ Secure Electronic Transactions,” n. d.). It is an open standard that is used for ensuring the authenticity and for protecting the privacy of electronic transactions.

SET is dependent on the science of cryptography. In particular, the SET protocol uses two encryption algorithms, namely RSA and DES. SET is not a payment system but a set of formats and protocols that enable users to use the existing credit card payment infrastructure on the Internet (Stallings, 2002). The services that SET provides include privacy, digital certificates, and secure communication. Privacy is ensured by making the information available only to the parties involved at the required time and place. The use of X. 509v3 digital certificates promotes trust. On the other hand, the use of a secure communications channel provides security among the parties involved.

References

ArticSoft Technologies Limited. (2012). An introduction to PKI (Public Key

Infrastructure). Retrieved from http://www. articsoft.

com/public_key_infrastructure. htm

Cheng, P.-C., Garay, J. A., Herzberg, A. & Krawczyk, H. (1998). A security architecture for the

Internet protocol. IBM Systems Journal, 37 (1), 42-60

Cisco Systems, Inc. (2001). Internet key exchange protocol. Retrieved from http://www. net130. com/tutorial/cisco-pdf/4T_IKE_Bcamp. pdf

Microsoft. (2012). Understanding S/MIME. Retrieved from http://technet. microsoft. com/en-us/library/aa995740(v= exchg. 65). aspx

Onyszko, T. (2004, July 22). Secure socket layer. Retrieved from http://www. windowsecurity. com/articles/secure_socket_layer. html

Secure Electronic Transactions: An overview. (n. d.). Retrieved from http://www. davidreilly. com/topics/electronic_commerce/essays/secure_electronic_transactions. html

Stallings, W. (2002, May 17). Introduction to Secure Electronic Transaction (SET). Retrieved