"Research on Security Strategy of Electronic Commerce Industry Websites"

Gong, S. and Wang, Y. (2015). Research on Security Strategy of Electronic Commerce Industry Websites. In *International Conference on Advances in Mechanical Engineering and Industrial Informatics.* Atlantis Press.

Abstract: The rise in electronic commerce requires a building of trust between consumers and businesses. Security protocols used in ecommerce must control information security threats and build the consumer's perception of security. The advantages of ecommerce are discussed, as well as currently used security mechanisms. Current mechanisms include information transfer between customer and merchant, then between merchant and third-party security technology, then transfer between the third-party and the bank. The security technology is composed of an interface that includes security protocol (SSL or SET), certification center, and encryption. The authors also diagram another security model containing four layers and provide suggestions for future website regulation, including government regulation.

Review: This paper was not very detailed in describing their security mechanism. The diagram is very simple, and they do not provide any explanation of how the modules interact. It is also written in very poor and hard to follow English, and they do not cite any sources for their research.

"Analysis of Security Algorithms used in E-Commerce and ATM Transactions"

Sethi, R. (2015). Analysis of Security Algorithms used in E-Commerce and ATM Transactions. *International Journal of Engineering Research and Development*, 11(8), 19-24.

Abstract: E-Commerce creates great opportunity for business but also carries great risk. This paper details two mechanisms for securing electronic transactions: SET and a modified SET. The authors then discuss the adaptability of these algorithms to mobile transactions. Any e-commerce protocol must include confidentiality, integrity, availability, reliability, speed, and ease of data sharing. The paper outlines the step-by-step process of the SET algorithm. The modified SET is similar except that the transaction details are encrypted and decrypted at every step in the transaction. The paper also details TIC authentication, SMS authentication, public key algorithm, and message authentication. The authors propose a secured fingerprint payment system for mobile transactions. The authors conclude that security can be enhanced by using the modified SET, though it will take longer, and security can be further enhanced with biometrics.

Review: This paper gave some of the formulas and algorithms for sending secure messages over the internet, which may be helpful. However, SET is not widely used. Further, the paper does not really discuss any of the risks associated with online transactions and how their research helps to overcome any particular risks.

"A Secure Electronic Payment Protocol Design and Implementation"

El Ismaili, H., Houmani, H., and Madroumi, H. (2015). A Secure Electronic Payment Protocol Design and Implementation. *International Journal of Computer Science and Network Security*, 15(5), 76-84.

Abstract: Secure Sockets Layer (SSL), Secure Electronic Transaction (SET), and VISA's 3D-secure protocols for e-commerce security are discussed. SET is not widely used due to implementation issues, while SSL is commonly used even though it does not address all security issues. The authors outline a new secure and efficient protocol they call Secure Electronic Payment Protocol (SEP) that provides confidentiality, data integrity, authentication of participants, and non-repudiation. The paper details the steps of registration, purchase request, authorization request, response, cardholder authentication, and response and payment. The authors claim their SEP system is usable, flexible (can be used on any PC), affordable, reliable, available (unlike 3D secure), fast, and interoperable.

Review: This paper gives good detail of their proposed system, unlike the other papers. Some things remain unclear: how does their system address any security vulnerabilities of SSL (and what are those vulnerabilities)? The author also says that the consumer and merchant require installation of plug-ins, so it is not clear how this system is flexible or interoperable.