Security managementexample narrative flashcard

There are however some limitations of this technology, and they are a small drawback to what is a very efficient and secure networking technology. The technology works very well at preventing eavesdropping or data manipulation in between endpoints however the standards which have been set do not prevent anyone from setting up a certificate, or to go through the processes of trying to acquire a fraudulent certificate.

The service itself also relies on a third party that has to be trusted in order for the system to work efficiently and if this trust is lost or broken, then the system itself is broken. A similar conundrum exists in the legal world, which is burden of proof, and how and what constitutes proof of identity. The different third party authorities may well have different levels of how to identify and prove that identity is correct, this is something the end user or business knows little about.

There is also an issue with various levels of certification and how one organization has needs which are different from another. For example a bank would need a very high level of security on their certificates, compared with a community center for example, which has requirements for a relatively low level of security. The manner in which these different levels of security decided and priced accordingly needs to be clarified and standardized across all of the certificate authorities on the internet.

The differing requirements of organizations which want to transmit information across the internet means that there must be differing levels of security. This has been overcome by implementing domain specific security on SSL certificates to be encrypted for particular domains only which does

help to alleviate the costs and extra security requirements for lower security organizations. Therefore in conclusion, the utilization of SSL in secure web transmission is an essential technology which is able to validate identity based on a system of trust via a third party.

The concept relies on a key based system of encryption and checking by this authority, which had been trusted by both parties which want to conduct communication, to identify and confirm that the transmission can go ahead and is secure and free of data eavesdropping or manipulation. This is essential when considering the different kinds of transactions which occur on the internet daily, from information being sent via email, to secure credit card transactions being carried out by people at home, to application data updates being done by remote connection to a central data repository.

From the most basic of tasks to the most complex and important, the implementation of SSL can be beneficial in many ways from ensuring customer confidence, to creating an efficient and secure system of communication, and by using this protocol it is possible to create new secure functions, and manipulate existing operations to aid business development and efficiency.

The ultimate aim of a network, and the internet itself is no different is to allow different aspects of communication to be integrated together to give a secure and efficient system which is both easy to use and cost effective, and implementing the above protocol when dealing with secure transmission of data will help to achieve these aims.

It should however be remembered that this protocol is not without criticism and there are some issues, however it is an industry standard which has been used for nearly two decades, and like most technologies will be developed and improved to facilitate more secure communication in the future.

References

Cordesman, A. H. , & Cordesman, J. G.

(2002). Cyber-Threats, Information Warfare, and Critical Infrastructure Protection : Defending the U. S. Homeland /. Westport, CT: Praeger.

Retrieved August 10, 2010, from Questia database: http://www. questiaschool. com/PM. qst? a= o&d= 102120447 Donnely, J.

F. (1992, November). A Memorandum of Agreement.

Security Management, 36, 90. Retrieved August 10, 2010, from Questia database: http://www. questiaschool.

com/PM. qst? a= o&d= 5002183972 Mills, L. B. (2005, January). Read Any Good Technology Policies Lately?. School Administrator, 62, 8.

Retrieved August 10, 2010, from Questia database: http://www. questiaschool. com/PM. qst? a= o&d= 5008547616 Cook, R. (2003, February 24). The 5 A’s of functional SAN security.

Retrieved August 10, 2010, from Searchstorage. com: http://searchstorage. techtarget. com/tip/1, 289483, sid5_gci881954, 00.

html