KanSec Abstract Submission

Jason Smith

Graduate Student

Masters of Liberal Studies

Concentration in Information Assurance

Fort Hays State University

Risk Mitigation in Remote Access:

Managing risks associated with company owned and employee/vendor owned devices

More and more people are seeking the freedom to access corporate resources from locations outside the control of the corporate information security infrastructure. These locations often include public internet access sites prominently located in hotel lobbies, airport terminals and the coffee shops on nearly every corner. Mobile computing is a reality that is difficult to avoid and with it brings new attack vectors and security risks that must be planned for and mitigated.

When it comes to mobile computing there are essentially two types of access – access by devices that the company owns and controls and access by devices owned by employees and vendors. Each brings unique risks that must be reduced to an acceptable level to ensure the integrity and confidentiality of data accessed remotely.

With corporate owned devices, there is some level of control that can be asserted to secure the physical device from outside penetration and ensure data integrity in the event of theft or loss of the device. This includes security policies that require the use of strong passwords, full disk encryption, and the deployment of anti-virus and firewall software on the machine. While these measures are affective in protecting the security and integrity of the system itself, they do little to protect the transfer of the data between the remote computer and the corporate network. I will demonstrate how, in a lab setting, I was able to easily sniff packets going across a common LAN and intercept confidential data as it was communicated.

With employee owned or vendor owned devices, no assumptions can be made to the security and integrity of the device. Because companies cannot expect users to implement reasonable security measures on their personal devices they must accept that a high level of risk is involved in allowing such devices to connect to their networks. Not only do the standard risks associated with corporate owned devices apply but are also magnified by an inability to ensure the security and integrity of the device. Businesses must be leery of allowing the download of confidential data to devices outside of their control.

This presentation discusses the risks associated with mobile computing and offers a solution to mitigate such risks in the forms of access control, VPN communications, application control and URL filtering, and desktop virtualization. I will demonstrate findings on how such measures can reduce the risks associated with mobile access computing to acceptable levels using tools and products currently on the market.