System security

_____ Grade _____ d: 2008-12-21 System Security System security over the last twenty years has gone through a tremendous series of ups and downs where the focus of providing security is to minimize uncertainty by measuring the probability of a threat event.

Initially the secure and financial data were not on the internet directly so at that time the most common threat to a computer system or to a land environment was the virus attack. Criminal minded geniuses were designing the virus to destroy a system partially or completely. This provided an edge to the antivirus companies to scan, remove, and protect from virus attacks. The virus attack can only be possible to a system via removable storage devices (zip drive, jazz drive, and floppy drive) which mean a system can be protected from such attacks if the external removable devices are pre-scanned before its usage.

During the current era of globalization, every LAN is connected to the biggest LAN i. e., internet one way or the other. Nearly all the financial institutions and government bodies have connected their systems over the internet to give their authorized users an ease of access from any part of the world. On one hand this has alleviated the boundaries between different countries and made communication possible in real-time between two ends of the world but on the other hand it has given an edge to the cyber criminals to breach through the complex systems by finding its loopholes.

Due to the threat of hacking, none of the national security and financial data is safe from these cyber criminals unless well protected by using different pro-active techniques such as: 1) Data encryption 2) Firewalls 3) Identifying the loopholes in the current system and creating a patch for it. The encryption technique has been successfully used for data transfer between

two ends over the internet because even if the data is tapped by a hacker, he cannot decrypt it since he is inaccessible to the public key for decryption. The firewall softwares are used to guard against the brute force attacks and access from an invalid domain but due to the loopholes which exist in the current operating systems these firewall softwares occasionally fail.

Up till now the hackers are usually focusing on financial institutions for the monetary benefits, but in the future these hackers could also be used to manipulate the national security data and the personal ids to wage any degree of chaos as desired. This situation is expected only because we have created the space for this threat by ourselves by storing every personal data and information over the internet, having mobiles in our pockets to be tracked down anywhere.

Chip and other biometric technologies have also made our lives miserable for loosing the privacy and monitoring our body functions throughout the year (Levant, http://www. rense. com/general64/freewill. htm). What can be worst than the situation when humans start becoming slaves to the governmental bodies – being implanted and analyzed with RFID chips.

Work Cited

Levant Nancy, Accessed from