



SNS COLLEGE OF TECHNOLOGY

(Autonomous)
COIMBATORE – 35



DEPARTMENT OF COMPUTER SCIENCE AND ENGINEERING (UG & PG)

Third Year Computer Science and Engineering, 5th Semester

UNIT III - CYBERCRIME: MOBILE AND WIRELESS DEVICES

Topic Name : Laptops

Concept of Laptops

As the price of computing technology is steadily decreasing, usage of devices such as the laptops is becoming more common. Although laptops, like other mobile devices, enhance the business functions owing to their mobile access to information anytime and anywhere, they also pose a large threat as they are portable. Wireless capability in these devices has also raised cyber security concerns owing to the information being transmitted over other, which makes it hard to detect.

The thefts of laptops have always been a major issue, according to the cyber security industry and insurance company statistics. Cybercriminals are targeting laptops that are expensive, to enable them to fetch a quick profit in the black market. Very few laptop thieves are actually interested in the information that is contained in the laptop. Most laptops contain personal and corporate information that could be sensitive.

Physical Security Countermeasures

Organizations are heavily dependent upon a mobile workforce with access to information, no matter where they travel. However, this mobility is putting organizations at risk of having a data breach if a laptop containing sensitive information is lost or stolen. Hence, physical security countermeasures are becoming very vital to protect the information on the employees laptops and to reduce the likelihood that employees will lose laptops.

- Cables and hardwired locks: The most cost-efficient and ideal solution to safeguard any mobile device is securing with cables and locks, specially designed for laptops. Kensington cables are one of the most popular brands in laptop security cable. These cables are made of aircraft-grade steel and Kevlar brand fiber, thus making these cables 40% stronger than any other conventional security cables. One end of the security cable is fit into the universal security slot of the laptop and the other end is locked around any fixed furniture or item, thus making a loop. These cables come with a variety of options such as number locks, key locks and alarms.

- Laptop safes: Safes made of polycarbonate - the same material that is used in bulletproof windows, police riot shields and bank security screens-can be used to carry and safeguard the laptops. The advantage of safes over security cables is that they protect the whole laptop and its devices such as CD-ROM bays, PCMCIA cards and HDD bays which can be easily removed in the case of laptops protected by security cables.
- Motion sensors and alarms: Even though alarms and motion sensors are annoying owing to their false alarms and loud sound level, these devices are very efficient in securing laptops. Once these devices are activated, they can be used to track missing laptops in crowded places. Also owing to their loud nature, they help in deterring thieves. Modern systems for laptops are designed wherein the alarm device attached to the laptop transmits radio signals to a certain range around the laptop.
- Warning labels and stamps: Warning labels containing tracking information and identification details can be fixed onto the laptop to deter aspiring thieves. These labels cannot be removed easily and are a low-cost solution to a laptop theft. These labels have an identification number that is stored in a universal database for verification, which, in turn makes the resale of stolen laptops a difficult process. Such labels are highly recommended for the laptops issued to top executives and/or key employees of the organizations.

Other measures for protecting laptops are as follows

- Engraving the laptop with personal details
- Keeping the laptop close to oneself wherever possible
- Carrying the laptop in a different and unobvious bag making it unobvious to potential thieves
- Creating the awareness among the employees to understand the responsibility of carrying a laptop and also about the sensitivity of the information contained in the laptop
- Making a copy of the purchase receipt, laptop serial number and the description of the laptop
- Installing encryption software to protect information stored on the laptop
- Using personal firewall software to block unwanted access and intrusion
- Updating the antivirus software regularly
- Tight office security using security guards and securing the laptop by locking it down in lockers when not in use
- Never leaving the laptop unattended in public places such as the car, parking lot, conventions, conferences and the airport until it is fitted with an anti theft device;
- Disabling IR ports and wireless cards and removing PCMCIA cards when not in use. Information systems security also contains logical access controls.

This is because, information, be it corporate or private, needs high security as it is the most important asset of an organization or an individual. A few logical or access controls are as follows:

- Protecting from malicious programs/attackers/social engineering.
- Avoiding weak passwords/ access.
- Monitoring application security and scanning for vulnerabilities.
- Ensuring that unencrypted data/unprotected file systems do not pose threats.
- Proper handling of removable drives/storage mediums /unnecessary ports.
- Password protection through appropriate passwords rules and use of strong passwords.
- Locking down unwanted ports/devices.
- Regularly installing security patches and updates.
- Installing antivirus software/firewalls / intrusion detection system (IDSs).
- Encrypting critical file systems.