Computer Privacy Essay, Research Paper

Computer Privacy Issues

An issue of concern at is Computer privacy. Computer privacy techniques have been developed to protect single computers and network-linked computer systems from accidental or intentional harm. The main reason for protecting these computers is to keep them from physical loss of data, deception of computer users and the deliberate invasion of databases by unauthorized individuals.

Computers and the information they contain are considered confidential systems as they are used mostly to a limited number of users. Confidentiality and the possession of information can be violated by unauthorized users who shoulder surf or by observing another user’s computer screen.

Also by tricking authorized users into revealing confidential information, wiretapping, or listening in on or recording electronic communications people who wont to invade our privacy can easily do so.

Several techniques are used to prevent computer crimes such as Encryption, Approved Users, Passwords, Fire Walls, Security Servers, Integrity and availability.

Encryption

Using encryption is a very good way of preventing our privacy being violated, with this information can be scrambled and unscrambled using mathematical equations and a secret code called a key. Two keys are usually used one to encode (make the calculation) and the other to decode (calculate the equation) the information. The keys that encodes the data are called the private key and are only kept in the hands of the sender. The key that decodes the data which is called the public key can be possessed by several receivers. Keys are modified periodically, keeping unauthorized access and making the encrypted information difficult to decode if it comes in the hands of someone else.

Approved Users

Another technique to prevent computer crime is to limit access of computer data files to approved users. Access-control software is a good way of keeping privacy as it verifies computer users and limits their privileges to view and change files. Records can be kept of what files are accessed, so that users can be caught if they notice any of their actions to be unlawful. Military organizations use the approved users technique to give the right amount of access to classified, secret, or top secret information according to the security clearance level of the user.

Passwords

Passwords one of the best ways to insure privacy are confidential sequences of characters that give users access to computers. Effective passwords are ones which are difficult to guess. Many passwords contain a mixture of characters and symbols that are not real words therefore making it difficult for imposters to get in computer systems. One of the ways in which computer systems make guessing difficult is by limiting the number of attempts to enter a correct password then terminating the account after failing to enter it correctly.

Firewalls

Firewalls which are used for Computer networks are particularly vulnerable to computer crimes. Information on networks can be protected by a firewall which is a computer placed between the networked computers and the network. The firewall prevents unauthorized users from gaining access to the computers on a network, and also ensures that information received from an outside source does not contain computer viruses or self-replicating computer programs that interfere with a computer’s functions.

Security Servers

Special computers called security servers provide secure connections between networked computers and outside systems, such as database-storage and printing facilities. These security computers use encryption in the initiation of the electronic exchange, which prevents a connection between two computers unless the identity of each is confirmed to the other.

Integrity and Authenticity

The integrity and authenticity of information are threatened by modifying, removing, or misrepresenting existing data.

For example, omitting sections of a bad credit history so that only the good credit history remains violates the integrity of the document, and requesting a cash advance using a stolen credit card violates the authenticity of that transaction.

The most serious threats to integrity and authenticity of information comes from those entrusted with access privileges who commit crimes. An example of this is secretly transferring money in financial networks, and committing payroll fraud. Crimes such as these can be prevented by using such techniques as checksumming (mathematically comparing a file before and after it is accessed), authenticating the source of messages, and limiting the amount of money that can be transferred through a computer.

Availability

The availability of information is affected as long as access to the information is prevented. If the data is moved, lost or damaged it is useless. Computers and components such as floppy or hard disks are easily damage, and a computer’s memory can be erased or the computer’s hardware can be damaged by flooding, fire, or dust.

To keep the information safe several backup copies of data should be made and stored in another location. Businesses such as , that rely on computers need to keep in mind that there might be a time where they will lose information and therefore should keep back up copies of it, and have a disaster recovery plans that are periodically tested and upgraded.

One of the most used operating systems, Windows was found to have security holes which if used to someone’s advantage can do serious harm or come to information which is confidential. With the use of a program someone may remotely take over a computer running Windows ‘95 and ‘98 without the user’s knowledge. This causes a serious threat to many people as if they are unknowledgeable that someone is watching their every move they may be violated in many ways.

The creator of the program states . ” … You can reboot a remote machine; you can lock up a remote machine.”

The program is known as Back Orifice and the maker, Sir Dystic member of a hacker group called Cult Dead Cow says “a remote user can do pretty much anything that the local user can do and more … including controlling the full file system, grabbing video from any cameras they have hooked up, seeing what they see on the screen, getting a log of what they type into the keyboard.”

Also with the use of the program people can also get all the system passwords and use them to their knowledge, such as using the hacked persons Internet or view files and download them off their computer.

“Privacy is a huge issue on the Internet, and people take it entirely for granted. Back Orifice may point out to people that privacy may not be as cheap as they think it is.” says Sir Dystic at a Def Con hacker conference in Las Vegas.

This is relevant to my workplace because at all the computers are attached to the main server and if there we to be any virus such Back Orifice the one above could cause problems. This is as people who are on the Internet could provide a link into the server and people could access it with out their knowledge.

To be safe from unauthorized people accessing your computer one should not run programs sent by people they do not know, not download files from web sites they wouldn’t normally trust and have a virus scanner to check your computer periodically.

328