System Security Essay, Research Paper

System Security System security is the amount of protection against unforeseen events, which might cause the system to fail. The amount of security in a given system depends upon the value of the information contained within the system. As the information becomes more valuable, the amount of money spent on protecting the information also increases. An example of this would be someone keeping their valuables in a home fire safe whereas a bank might keep their valuables in a time-controlled vault. Data security is the protection of data through emergency recovery plans and the controlling of end user privileges. This is the actual maintenance of the data itself. Through emergency recovery plans, data is protected from natural disasters and hardware failures. An emergency recovery plan should include a regular schedule for back-ups to be made of the system data. It should also allow for large disasters sometimes referred to as acts of God. Recovery plans allow for these disasters by having a back-up that is located off-site. This means that if the building collapsed in an earthquake, there would still be a copy of the system data at a site that wasn t effected. Now to be really effective the back-ups have to be maintained regularly. This way there isn t too much lost data when the back-up is restored as the main system. The back-ups should be maintained at a certain regular schedule and several back-ups should be maintained. This allows for data corruption. If the data was corrupted before the last back-up was run then that back-up would also contain the errors. By keeping multiple back-ups, the system can be restored from a previous back-up that hadn t had a chance to become corrupted yet. Another form of data security is the controlling of user privileges. Operating systems such as Novel NetWare and Unix allow for the controlling of individual users access to files and directories. By allowing only authorized users access to sensitive files, the system can be more fully protected against malicious use of the data or from errors caused from incompetence. In controlling the users on a system care should be taken in the assignment of passwords. Passwords should contain letters and at least one number or special character. If at all possible, passwords shouldn t be names or standard dictionary words. Passwords aren t effective if they can be guessed in any small amount of time. Lastly if there is any doubt on the security a password offers, change it often. This technique makes it much harder for an unauthorized user to gain access more than once. A system should also be protected from out-side sources that necessarily are not directly related to the users of the system. Protection from outside attacks is increasingly more important in our electronic commerce community. Any data transfer, which takes place outside of a corporate network, is free game for whoever wants to try and read it. Encryption Encryption is the answer that has been developed to protect information from eyes that were never meant to see it. Codes and ciphers have been around for hundreds of years. The secret decoder ring is a classic example of a simple code. Each letter of the alphabet is replaced by an offset. In this scenario A would be C and B is replaced by D, and so on. This allows for the sending of an unreadable message that can be decoded by the person that knows the proper offset. When a line of text is in normal readable form it is considered to be plaintext. Once plaintext is encrypted it becomes ciphertext. The ciphertext produced by present encryption standards follows the same idea as the decoder ring but the algorithms involved are much more complex. Now in today s world a simple cipher couldn t protect sensitive data with any measure of real security. There have come about several different approaches to how data is encrypted. They generally fall into two categories normal encryption and public-key encryption. In a standard encryption scheme the message is encrypted with a certain key word that the receiver of the message needs to know to decrypt the message. In public-key encryption the key used to encrypt the message is different from the key used to decrypt the message. This scenario allows one of the keys to become public. In this way the sender can encrypt a message to his friend, using the friends public-key, and there would be no need for any other contact between them for the friend to read the message. This was a problem with standard encryption because the channel used to send the key to the recipient would have to be secure otherwise there would be no reason to use encryption. It s interesting to note that when using public-key encryption to send an encrypted message, the sender can t read his own message once it has been encrypted. The only person who is able to read the message is the receiver. Due to the fact that the receiver is the only one who knows the secret key needed to decrypt the message. DES or Data Encryption Standard is one of the popular computer encryption algorithms in use today. It is an international standard that has been around since the 1970 s. It was created to allow different companies to create coding devices that would be able to work together. Another advantage of the Data Encryption Standard was that it was tested to be secure. The testing of the algorithm was accomplished by trying to break the code with a great amount of resources. This algorithm passed the National Security Agencies testing process and they deemed it secure. DES has since been used for a number of government communication links and data storage. Within the past decade it has become part of many commercial security applications. This type of encryption is a one key form of encryption, which means the channel for the key has to be secure and that the same key is used for decryption. More applications are moving towards the use of RSA encryption. RSA was named using the initials of its creators Rivest, Shamir, and Adleman. RSA is a public-key encryption algorithm. RSA gets its security from the difficulty of factoring large numbers. The public and private keys are functions of a pair of large (100 to 200 digits or even larger) prime numbers. Recovering the plaintext from the public-key and the ciphertext is conjectured to be equivalent to factoring the product of the two primes. 1 An important part of RSA encryption is that the keys can also be used to authenticate a message. The encrypted public-key can be used as a signature for the person who sent the message. The most recent use of encryption technologies has been to protect business transactions across the Internet. More to the point transactions through a World Wide Web based medium. SSL or Secure Sockets Layer is a protocol that was designed by Netscape to provide security during the transmission of sensitive data over the Internet. It uses the RSA encryption algorithm to protect data that is transferred between the browser on your home PC and the server of the Web site. The key length for the encryption algorithm controls how strong or weak the code is to break and also the speed at which the code can be decrypted with the key. If you ever bought anything online you might have noticed that it takes a little longer for the page to load up when using a secure connection. Although SSL is fairly secure some measure of caution should be used when sending information across secure channels. The key length for any server outside the U.S. and Canada is limited to 56 bits or less. The RSA algorithm is able to be broken at that level. Within the borders of the U.S. and Canada the key size is limited to 128 bits. With enough computing power this is also able to be broken but it would take much longer than a 56 bit key. With encryption it often comes down to the speed at which the algorithm works weighed against the length of time the data needs to be protected. I might not agree to online banking or stock trades over SSL but I might purchase things with my credit card. The amount of damage that someone could do to you, by acquiring data about you should be taken into account when conducting transactions online.

The whole reason that data should be encrypted across networks is due to the fact that just about any system administrator can view data that passes through his system. The Internet is just a network of networks, and all along the path between you and the server you re communicating with, there could be someone listening. This eves-dropping on network traffic is generally referred to as sniffing. When data is sent across the Internet it is broken down into chewable pieces called packets. Now the packets each have the address they re trying to get to and the order in which they re supposed to be read in, encoded on them. Each individual packet will find its own way between you and the web site you re surfing. If somewhere along that line someone makes a copy of a packet or two, of yours, they might be able to find out information that you don t want them to know. This technique has been used to gain access to systems by sniffing usernames and passwords off the network. It has also found some publicity in individuals identities being stolen and huge debts being run up on their credit cards. Sniffing tools have been developed for the purposes of debugging network configurations and such. There is always going to be the ability for a malicious person to receive information that wasn t intended for them. Due to this ability, it reinforces the importance that strong encryption has on Internet commerce and the importance that it will continue to have into the future. Firewalls Other than information that is traveling outside the corporate Intranet there isn t too much worry about network security. Many corporations are setting up filtering routers or Unix hosts that filter the network traffic coming into their system. This method of filtering network traffic is called a firewall. A firewall is a combination of hardware and software components that provide a choke point between a trusted network and an untrusted network such as the Internet. The firewall provides a certain level of control as to what can go between the two networks. 2 As sniffing can be used maliciously by an attacker, it has also started to become a tool used by corporations to monitor traffic flow across their networks. Corporations have been trying to cut back on web surfing by employees and extraneous emails. The access to the Internet has been, counter productive to some employees. The firewall provides an excellent point for network monitoring to take place. By monitoring the network traffic the corporation can be sure that the employees aren t wasting time or downloading anything that might be dangerous to the system. Recently there has been a scare about a macro virus named Melissa. A computer virus is a program that, when executed, tries to duplicate itself. They generally either infect the boot record of a disk or attach themselves to some kind of executable file. In this manner they have ample opportunity to be executed. The Melissa virus was a Microsoft Office Macro that was designed to spread using the names in the victims Outlook address book. It would email itself to the first fifty entries where once opened by the recipients, it would start the process over again. The computer virus can cause big losses in productivity from downed systems and corrupted data. For the virus to duplicate it tries to copy itself to a new location and in doing so can cause data to be over written. In systems that are Unix based there isn t too much of a problem with viruses. The design of the operating system doesn t give programs the freedom to roam as much as the PC architecture does. On Windows based machines there should be a current virus scanner running, to help keep virus losses to a minimum. The scanner should also be updated fairly regularly. By taking some preventative steps in advance your system can be more reliable and less likely to give you problems. Some attackers have also begun building their own network packets to get by the firewalls. An Internet Protocol packet can be designed to be source routed, which means the source gives the directions on how to get to the destination. By using source routed packets some attackers have been able to by pass a firewall. The majority of firewall packages have now accounted for this, so that if a packet is source routed it will automatically be filtered. The best protection a system can have is an aware system administrator. The U.S. Department of Energy has an advisory called CIAC (Computer Incident Advisory Capability). This advisory keeps track of newly discovered software or configuration faults, which might allow an unauthorized person, to gain access to your system. There is also the CERT (Computer Emergency Response Team) which also puts out advisories covering system security concerns. These advisories should be checked fairly often. Besides checking the advisories a system administrator should have some type of logging set up on their system. Unix systems have this already built in and plus there is a program called tripwire which gives some extra logging and checksum functionality. The logs show things such as failed login attempts and system errors. Tripwire is used also to log port connections and to prevent the insertion of Trojans on to the system. Trojans are programs that look like they do one thing but actually do something else, usually to gain access to a system. Tripwire protects against this by doing a byte by byte check of all the executables on the system. Even though your system is very secure and you check the logs daily there still needs to be physical controls put in place. Physical Controls Physical controls are the last line of defense against an outside attack on the system. One of the most often over looked physical controls is to just place consoles in secure areas. Any computer terminal should be behind a locked door of some kind. Computers tend to be rather expensive and they tend to walk off by themselves if not within a secure environment. Not too mention that an open terminal can give someone an anonymous point of entry into your system. One of the oldest and still the best physical control is the shredder. Hard copy is to be shredded. All information that a corporation deals with is in paper form at one time or another so why should one spend so much time and money on security when they just take the information and throw it in a dumpster. In conclusion information is power and in this world of databases and networks it is going to be ever more important to pay attention to the details of how that information changes hands.

325