Cyber Security Issues

**Table of Contents**

* Introduction ……………………………………………………………………. Page 3
* Intrusion Detection Systems………………………………………………….… Page 3
* Access Control …………………………………………………………………. Page 4
* Everyday User Issues …………………………………………………………… Page 5
* Cryptography …………………………………………………………………… Page 6
  + Symmetric cryptography ……………………………………………….. Page 6
  + Public-Key cryptography ……………………………………………….. Page 6
* Cryptology History ……………………………………………………………… Page 7
* Cryptanalysts ……………………………………………………………………. Page 7
* Conclusion ………………………………………………………………………. Page 8
* Works Cited ……………………………………………………………………… Page 9

Cyber security has been a growing issue for the world these past few decades. In the late 1990’s most people only needed to worry about the security of their emails. Fast forwarding to the present everyone must be worried about any type of data they own. Everything relies on computers and the security of data being stored or transmitted. Industries of all variations such as e-stores, automotive on board computers, navigation systems, the health industry, and much more require daily upkeep of security issues and threats. Although there are many issues that relate directly to cyber security it seems that recently most of these issues are revolving around the cloud.

Intrusion detection systems (IDS) are a piece of hardware or software which monitor all events that occur in a computer, servers, or network. The intrusion detection system analyzes any or all of these types of setup for any indication that there has been a violation of the system policies. “Intrusion detection and prevention systems (IDPS) are primarily focused on identifying possible incidents, logging information about them, attempting to stop them, and reporting them to security administrators” (Scarfone, K., Mell, P.). When hackers are monitoring systems and preparing for an attack they will first try to take down whatever intrusion detection or intrusion detection prevention system is in place. They will try to prevent the detection systems that are monitoring the security of the system from detecting their presence.

The intrusion detection prevention system will have a system administrator who maintains the system in its entirety. This person is responsible for creating and removing accounts for each user including other administrators. They will also be in control of the security of the system including constant maintenances and upgrading software as well as hardware. In an intrusion detection prevention system the daily upkeep of all accounts, hardware, software, and other related security devices are the only ways to keep this kind of system as safe as possible. Since technology is rapidly evolving there is no way to truly be 100% secure at any given time. This type of cyber security issue affects big companies, small companies, and all types of users depending on this type of security. They must all be aware that the only way to keep safe is to upkeep the system with daily updates of software and hardware as needed.

Access control is about trying to prevent attacks. It certainly takes an individual who is patient and able to rigorously go through the fine details of permissions to make sure that everything is set correctly. The access control matrix is a control model which is a table of defining permissions. The rows in the matrix represent subjects which are users, groups or systems that are able to execute actions. Each column in the matrix represents an object. The object may be anything such as a directory, file, particular document, or anything that we would have to define access privileges to. The individual cells of the access control matrices are filled with access rights for the correlating subject and object. The advantages to this control model is that the matrices are easy for the administrator to access, read, and manipulate. A major disadvantage of the matrix model is that it can become very big very quickly. Therefore making the readability dreadful. This is why the system administrator must be someone who is patient as well as someone who can pay attention to details. Operating system security starts with the same basics as access control where the administrator has the file permission matrix within all OS platforms. The folders will have their own permissions besides the files having them. Monitoring programs that are running at any given point in time is a job the administrator must adhere to. They will have to look at and judge the files integrity, memory usage, and decide whether or not this is malicious software running on the platform.

The administrator who is responsible for monitoring the intrusion detection prevention system is also someone who has authority over the access control list. This person could be the owner of a small business or a system administrator of a large company. Both scenarios are responsible for large amounts of private data of the company, its clients, vendors, and anyone else we can think of. The trend thus far is maintenance of the system. While security will never be at 100% the system administrator can do as much as possible to keep the system up to date at all times which will increase the overall security and decrease the chances of intrusion.

Average computer users are also constantly at risk of having their data corrupted or stolen by hackers and attackers. Everyday users are the normal people who lock their car doors, lock their front door and make sure that their windows are locked. They take the necessary precautions to secure their property and well-being. When dealing with computer security it becomes an out of sight, out of mind tribulation. With the first occurrence of a Trojan virus, worm, or identity theft people normally wonder how this could have happened. The same types of people in the world that are willing to rob your car, house or hurt you to get what they want are the same people who are willing to fully assault and corrupt your personal data. Everyday users must become as vigilant as a system administrator by keeping their systems up to date as frequently as possible. Security updates are quickly outwitted by cyber criminals who reside in all corners of the world and must not be underestimated at any cost.

Cryptography essentially is a way for at least two entities to safely send one another messages even if an eavesdropper is trying to intercept their communications. The practice of cryptography has grown exponentially past its simplistic design for two parties evolving with technology and modern day attackers. Cryptography encompasses methods for safe and secure communication.

Symmetric cryptography uses a key for encryption and decryption. The U.S. National Institute of Standards and Technology or NIST which is Advanced Encryption Standard (AES) algorithm recommends a symmetric encryption algorithm that is engineered to replace the legacy Data Encryption Standard (DES) algorithm. Cryptanalysis is where practitioners attack cryptosystems. They are the cryptanalysts who know the algorithms for encryption and decryption but lack knowledge of the keys that are used. “Such security by obscurity approach is likely to fail, since there are a number of different ways that such information can be leaked” (Goodrich, M.). A potential flaw with symmetric key encryption is when two users are attempting to communicate with each other they need a secure way to do so. The attacker can easily get the data from the stream.

Public-Key cryptography is the frequent term used for asymmetric-key encryption. It uses two different keys at once. The two different keys are a combination of a private key and a public key. The private key is only by the computer and the public key is given to the computer. In order for the computer to complete the decryption process it must use the public key which was provided by the originating computer with its own private key. The message sent from the originating computer won’t really be secure since the public key that is used for encryption published is available to anyone, but anyone who picks that up and reads it can’t read it without the private key. The key pair is based on prime numbers that are rat her lengthy.

Cryptography is an ancient tool created to conceal messages hidden in writings. The word itself derives from Greek words kryptos (hidden) and graphein (writing). “The need to conceal messages has been with us since we moved out of caves, started living in groups and decided to take this civilization idea seriously. As soon as there were different groups of tribes, the idea that we had to work against each other surfaced and was proliferated, along with rank violence, secrecy, and crowd manipulation” (Damico, T). Cryptography can be dated as far back as Egyptian scribes using hieroglyphics around 1900 B.C. to hide the true meaning from those who could not decrypt the message. A cryptographic tool used by the Greeks was a piece of tape wrapped around a stick. The person sending the message would wrap the tape around the stick and write the message while it was wrapped. To read the message the receiving end would have to use a stick with the same diameter to correctly decipher the message.

Cryptanalysts can perform a number of attacks on a cryptosystem but primarily use four types. The cipher text-only attack takes place when a cryptanalyst has access to the cipher text of one or many messages that were encrypted using the same key. The goal of this attack is to try to determine the plaintext for one or all of the cipher texts and or figure out the key. Another type, known-plaintext attack, the cryptanalyst has access to one or many plaintext-cipher text pairs where each plaintext was encrypted with the same key. The goal of this attack is to figure out the key. Chosen-plaintext attack takes place when the cryptanalyst choses one or many plaintext messages and gets the cipher text that is associated with each one based on the use of the same key. Chosen-cipher text attacks are where the cryptanalyst chooses one or many messages and gets the plaintext associated with each one based on the use of the same key.

All of the cyber topics and issues discussed do not simply have an effect on a single group. They affect everyone in the modern world because everything in our lives revolves around the daily transmission, distribution, collection, and storage of our data. The technology for securing all of this data has not been perfected yet but using techniques like cryptography, encryption storage, encrypted transmissions, and more can lessen the chances of cyber criminals exposing faults in our systems. It takes attention to maintain updates, patience for daily upkeep, and software upgrading when necessary. Just as automobiles need routine maintenance checkups we must also routinely maintain personal computers, servers, networks as well as anything else computerized and possibly on the cloud services.

Works Cited

* Scarfone, K., Mell, P. (2007), Guide to Intrusion Detection and Prevention Systems (IDPS).

http://csrc.nist.gov/publications/nistpubs/800-94/SP800-94.pdf

* Goodrich, M. (2010). Introduction to computer security. Boston, Mass.: Addison-Wesley.
* Brenner, S. (2010). Cybercrime: Criminal threats from cyberspace. Santa Barbara, Calif.: Praeger.
* Damico, T (2009) A Brief History of Cryptography

http://www.studentpulse.com/articles/41/a-brief-history-of-cryptography