Computer security: attacks on buffer overflow in regard to computer security

Engineering, Computer Security

Buffer Overflow Attacks

In computer security, a buffer overflow also known as buffers overrun, is an inconsistency where a process while writing information to a buffer, overruns the buffer’s borderline and overwrites surrounding space. This is a unique case of defiance of memory protection. Buffer overflow attacks can be dated back two decades ago in 1988 but until 2007 when the vulnerability of the attack persisted.

A buffer overflow benefits from program that waits for inputs from users. Buffer overflow attacks can be categorized as stack-based and heap-based. Heap-based attacks occupy the volume set aside for use by a program. However, these attack are rare due to the intricacy implicated while carrying out such attacks. The most common attacks are the Stack-based.

Regarding stack-based buffer overflow, stack is used by a program that is being exploited to store inputs from users. Usually, if the program does not require input from users, the stack will always be empty. Then, a return memory address is written by the program which is directed to the stack and then consequently inputs are done from the top. The inputs are then sent to the specified address after the processing of the stack.

Preventing Buffer Overflow Attacks

The easy and effectual way out to the crisis of buffer overflow is to make use secure coding. A library-based defense ensures that functions of a program never exceed the size of the buffer. It also make use of functions of unsafe programs that is re-implemented. For instance, Libsafe project identifies any

trial to run prohibited code found on the stack. The program sends an alert in case of a stack and used in the SecureStack.

Also, runtime compiler-based boundaries, examination to see what recently turned out to be reachable and positively with time and relating with this study, stack overflow is bringing a lot of impact on system administration. The only viable solution is to evade programming errors since there is no ideal solution to the buffere overflow problem.

Assignment 4-1

Type of hash algorithm Size of Digest Number of Rounds Needed in Creating it. Block Size Who Created Where it was Derived From Strengths Weaknesses

Message Digest Hash functions that are one-way and have arbitrary-sized data. Has 128 bits. 4 rounds It outputs a fixed-length has value. Has 512 bits. Created in 1990 by Ronald Rivest. Derived from the method of initializing message. The reset function can be called any time to reset it. Hence, somebody can make it the way they want it to be. Update methods is used to update the data. Wrong data can be updated in the algorithm.

Secure hash algorithm Has 160 bits Has 80 rounds Has 512 bits National Security Agency in 1993 Derived from the hash function of cryptographic Is a strong method since it has gone four series of attacks. In the course of the four series the algorithms has undergone constructive changes. The changes made the algorithms to be strong and persevere other attacks. Found attacks from SHA-1. Cannot handle the attacks from the SHA-1.

Whirlpool

2256 length of bits. 10 rounds 512 bits. Vincent Rijmen Derived from Merkle-Damgard Has resistance against differential and linear attacks. The algorithm is not affected by the linear and differential attacks. Infeasible in detecting correlations. The infeasibility brings about the weaknesses in this algorithm.

RIPEMD 128 bits 60 rounds are needed. 512 bits Bart Preneel, Antoon Bosselaers, Hans Dobbertin It was derived from MD4. MD4 had many weaknesses it was improved and named as RIPEMD. Since it was an improvement of MD4 weaknesses it is strong. Since it is a hash function of cryptographic the same problems experienced by others face them.

Assignment 6-1

What I think is that the hospital will be held answerable for the stolen data. These arise like that since the software providers usually install the software to their clients with some terms and conditions. The terms and conditions are well stated when the installation of the software is done to their clients. Going by the agreement of the company and their clients they may offer training of the software use or not. In most cases, when the software is new in the market, the training is provided. If the software is already there in the market, there is a possibility that the client will know its use and, therefore, training will not be necessary. Hence, further maintenance of the system installed on the client it is according to what they want. The company installing the software may be the one to maintain it, or the client can outsource maintenance from another company. Therefore, in our scenario

about the hospital and the cloud service provider, the hospital should be answerable about the patients lost data. The blame should not go to the cloud service provider.

Once the hospital got the cloud computing service provided their service to the hospital, their job was done. It was left the hospital to ensure that the integrity of the patients' data is maintained. If the hospital do not have evidence that the cloud service provider is the one who hacked into their systems. They cannot judge them to be answerable of the data lost. That makes it clear that companies like Microsoft are not supposed to be held liable for any breach that may be led to the vulnerability in their software. The software holders may remain liable for the software they put on use. Not unless, in some point where the service provider is involved in the maintenance of the software. At such case, they may be held liable.

Assignment 10-1

56768909

If this happens to my password, it can take about 0. 025 seconds for a PC user to crack it. This is because my password constitutes of numbers only. By making use of a symbol, in the password can make it be more secure and original. Also, by using spaces in the passwords can make it stronger since very few hackers will think about spaces when trying to hack the passwords.

ThgfdhGh

If I use the above password, it will be stronger than using numbers alone. This can take a desktop PC user about three hours to crack it. This is because

the password constitutes of letters which are in both upper and lower cases. Also, the letters are not in any organized form to make a name but rather they are disorganized giving no hints of the password.

Smnhf123

If the above password is used, then the normal desktop PC user can take around 15 hours to crack the password. This is because the password is a combination of both numbers and letters making it be stronger. Though, the use of letters at first and then followed by numbers has been the trend used nowadays. Hence, it may take some time to crack it, and finally it can be cracked.

Therefore, according to the three passwords tested above, it results that all of them are weak in their own way. The first is weak since it constitutes of numbers alone. The second constitutes of letters in upper and lower case. The third constitutes of letters combined with numbers. Therefore, to make a password be strong, we have to involve letters, numbers, symbols and spaces. These may help in generating a very strong passwords. After following the instructions in the various sites of testing the passwords, I arrived with the following strong passwords;

56; 76,. 9@9*

T/hg’fd= G&%h.

S[m]? nh; f: 1$! 2 3_

Assignment 11-1

Personal Disaster Recovery Procedure for Your Home Computer.

Information is very essential in any setup; be it in an organization or at home. It is, therefore, important that we kept good maintenance of the computers that hold that information. However, many are the times one's computer hard disk crashes, and the computer fails to boot. This necessitates the need to repair either by connecting it to another computer or by use of other means. Before one can do any work on the crashed drive, you will be required to remove it from the present computer and link it to a different computer as a secondary drive. The paramount method to do this is to use a USB to IDE/SATA connector adapter. If you don't have an available one, then you can connect the drive to another desktop computer internally as a secondary drive. If you connect it, make sure that the machine detects the drive in the BIOS, or you won't access it once the computer boots.

Information on computers should be safeguarded to avoid any possible loss of data. Partitioning of the hard disk also helps a great deal. At times, a disk might develop bad sects in some parts of the disk and having partitioned, you will not lose all the information unlike when the disk is not partitioned one stands the risk of losing every information. Data also requires to be backed up in a different drive, normally quite some distance away from the current location. This helps in cases of fire outbreaks whereby even if the disk burns to ashes, the information can still be recovered. The two locations need to be networked so that the data on the current computer is backed up on the other in real-time processing.

This disaster recovery procedure is sufficient as it would assist in getting back any lost information. However, burglar proofing of the house is important to avoid instances of theft of computer and other valuable assets.