International Journal of Innovative Research in Science and Engineering
Vol. No.2, Issue 02, February 2016
www.ijirse.com
ISSN: 2454-9665

# STRENGTHENING DATA CONFIDENTIALITY IN COMPUTER NETWORKS

**M.Janaki[1], P.Geetha[2]**

[1]*Research Scholar, Department of Computer Science, Bharathiar University, Coimbatore.*
*Assistant Professor, Dr.Umayal Ramanathan College for Women, Karaikudi, Tamilnadu, (India)*
[2]*Research Scholar, Department of Computer Science, Alagappa University, Karaikudi.*
*Assistant Professor, Dr.Umayal Ramanathan College for Women, Karaikudi, Tamilnadu, (India)*

**ABSTRACT**

*Computing systems becomes more useful when connected in networks. Though networks provides several advantages as ease of data sharing, fast data transmissions, it is also concerned with some security issues such as attacks and theft. More and more researches is needed in this area to develop trust worthy security solutions which will solve the problem of security issues. The main security problem is ensuring data confidentiality of data. This paper describes various vulnerabilities, threats and attacks, also discusses about hacking and finally propose the controls as the solutions for the security breaches.*

***Keywords: Network Security, Attack, Threat, Control, Vulnerability, Ethical Hacking, Encryption .***

## I. INTRODUCTION

The possibility of crime in computing systems is bad enough. In the event of a crime, most of the organizations will not investigate due to the fear that it will damage their public image. Even when organizations try to take action against cyber crime, the investigation can be hindered by statutes that do not recognize electromagnetic signals as property. Each network node itself is a computing system, it multiplies the problem of computer security. The following are the aspects for the need of security in today's corporate environment. (i) Fast growth of computer networks for information sharing. (ii) Business company systems connected in network share confidential information. (iii) Several tools and resources are available on internet that may be used to attack systems. (iv) Due to increase in threat of attacks. (v) Newly launched computing products give attention to ease of use than on security. (vi) Resources allotted for securing systems is very less in number. Security is an inevitable part in this world connected via internet. As the connectivity increases, the concern over securing one's data also increases[6].

Computing system is referred to as a collection of hardware, software, storage media, data and people that are used to perform computing task. The variety of targets and attacks makes security in computing as a difficult task. The computing system will have three valuable components i.e. hardware, software and data. Security analysis of a computing system can be done by the ways in which the system or its information is subject to a loss or harm. It should be made sure that no data are accessed by unauthorized users and also authorized users have access to the data.

ISSN: 2454-9665

### 1.1 Literature Survey

Weingart, S.H. , White, S.R. , Arnold, W.C. , Double, G.P, says that Physical security technology is being used more often to protect the integrity of computing systems and the assets they contain. A physical security rating system is defined in terms of the difficulty of mounting a successful physical attack against it, quality assurance documentation and system testing [1]. Judith M. Myerson have shown how coordinated denial-of-service can attack a network. This article looks at whether to identify assets or threats as the first step in risk assessment[2]. Kristopher Daley, Ryan Larson, Jerald Dawkins have described a modeling framework that provides a foundation for classifying multi-stage network attacks in a compassable, functional structure. It identifies the need to move beyond the paradigm of unstructured text based attack specification and signatures, to a more systematic means of describing multi-stage attacks. The approach described here provides a method for correlating attacks and expressing the capabilities they permit[3]. Richard C. Hollinger, have surveyed of computer crime victims indicate that the typical computer criminal is an employee, not an outsider trying to "hack" into the system. In trying to explain this paradox, comparisons are made with earlier historical periods when highwaymen and train robbers were also viewed by law enforcement as criminals but considered by their peers as folk[4] .

## II. ATTACKS IN THE NETWORK

The weakness in the security system is called as *vulnerability*, that might be used to cause loss or harm to the computing system. For example, if a system is not verifying identity of a user before permitting to access data, then the system is vulnerable to unauthorized data manipulation. The set of circumstances that has ability to cause loss or harm to a computing system is known as *threat*. Probably a human or a system will attack a system by exploiting its vulnerability is called an *attack*. The action or device or technique that deletes or minimize a vulnerability is known as *control*. Control can be used as a protective measure. The relationship among attack, threat, control and vulnerability can be described as, *"An Attack is avoided through blocking a Threat by Control of a Vulnerability"*.

The following example shows the concepts of attack, threat, control and vulnerability. There is a lion inside a cage and caretaker is outside. There is a door for giving food to the lion. The door is protected with the lock. The lion will make an attack on the care taker when the door is not locked. Lock is the control and the door is the vulnerability. Caretaker may be harmed by the lion is the threat.

### 2.1 Threats in the Network

There are four kinds of threats available that exploits vulnerabilities of the assets in the computing systems. The threats are interception, interruption, modification and fabrication. *Interception* denotes that an unauthorized user gaining access to an computing system in order to copy a program or data in a network. *Interruption* means hardware, software or data in a system is made unavailable or unusable. If an unauthorized user changes the asset of a computing system, it is called as *modification*. When an unauthorized user inserts new transfer or records in the existing system is called fabrication. Owing to a massive amount of personal data stored and exchanged on networks and the simplicity of gaining access to the vast majority of data using illegitimate methods like social engineering techniques, these services are highly vulnerable to privacy intrusion threats[7].

ISSN: 2454-9665

### 2.2 Security Goals

Usually The three important aspects of a computer security is confidentiality, integrity and availability. The first aspect *confidentiality* make sure that computer-related assets are accessed only by authorized users. Confidentiality can be called as secrecy and privacy. The second aspect *integrity* indicates that computer-related assets can only be modified by authorized users. The third aspect *availability* means that the computer-related assets are accessible to the legitimate users at appropriate times. Availability can also be known by its antonym denial of service.

## III. DIMENSIONS OF VULNERABILITIES

Attackers can exploit through the vulnerabilities in hardware, software and data. . Hardware is easy to attack, since it is more visible which is composed of physical objects. Hardware attacks are done by adding devices, changing them, removing them, flooding them with traffic. There are two kinds of attack in hardware, (i) *Involuntary machine slaughter* i.e. accidental acts such as people spilling food items, mice chewing cables, hardware drenched with water, burned, frozen which are not done intentionally. (ii) *Voluntary machine slaughter* i.e. someone intentionally do harm to the computer hardware by shooting with guns, bombs, stabbed with knives, shorting-out circuit boards and other components.

### 3.1 Software Vulnerabilities

The Software vulnerabilities allows the attack in the software by replacing, changing, destroying, modifying, deleting them and makes it no longer runs. Software is quite easy to delete and modify which causes it to fail or to perform an unexpected task. There are four categories of software modification are logic bomb, virus, trapdoor and information leaks. *Logic bomb* is a program that is maliciously modified to fail when certain conditions are met. *Virus* is a malicious program used to spread unintended information from one computer to another. *Trapdoor* is a malicious program that act like a secret entry point for performing attacks. *Information leaks* is performed by a malicious code which enables access to unauthorised users. Unauthorized copying of software is a attack, which is to be stopped by strict copyright laws.

### 3.2 Data Attacks

Data attacks are more serious issues than software or hardware attacks because people knew more about data items, how to use or how to interpret data. Hence data vulnerabilities should be taken care more. Data can be classified in to sensitive data and normal data. Sensitive data leaked or unauthorisedly modified can even cost human lives. The three goals of security is also applicable to data. Data confidentiality prevents unauthorized access to a sensitive data. Data integrity prevents unauthorized modification of sensitive data. Data availability allows authorized access to sensitive data.

## IV. COMPUER CRIMINALS

Computer crime is any crime that affects the computer related assets causing serious issues. In order to prevent the crimes we should be aware of who commits the crime and why. Computer crime is not expected to decrease in the foreseeable future. The number of investigations will continue to increase at a staggering rate. As such,

ISSN: 2454-9665

investigators require assistance with digitally derived evidence, digital crime scenes, and logically, assistance in dealing with those criminals engaged in computer crimes[5].

Computer criminals can be categorized in to amateurs, crackers, career criminals and terrorists. *Amateurs* are normal people especially ordinary computer professional or users who discover some access to a unknown system while doing their job and utilize cash or other valuable things. *Crackers* are often students at high school or college level who tries to log in a unknown system, to see whether it can be done. Actually crackers attempt to unauthorized access for fun and enjoy causing loss or harm to others. *Career criminals* are professional people who understands the targets of computer crime more. They perform organized crime for good payoff. *Terrorists* can use the computers for making attacks and to send message to many people.

## V. METHODS OF DEFENCE

Harm occurs when a threat is made through a vulnerability. The possibility for the occurrence to the harm is called risk. Harm can be dealt in the following five ways, prevent, deter, deflect, detect and recover. Harm can be prevented by blocking the attack or closing the vulnerability. Harm can be deterred i.e. made the attack harder. Harm can be deflected i.e. throw out of sight by making other target more attractive. Harm can be detected before or after it happens. Harm can be recovered from its effects after it happened.

## VI. DISCUSSION ON HACKING

Hacking is the method to gain unauthorized access to data. Hacker is a person who performs hacking for learning the details of computer systems. Cracker is a person who performs hacking for malicious practice. Hacking can be used as a preventive methodology to provide solutions to the security concerns in all possible ways to a computing system. Ethical hackers work as crackers to find out the vulnerabilities of a computing system and provide counter measures against the vulnerabilities. The end goal of ethical hackers is to learn system vulnerabilities so that they can be repaired for community self-interest - and as a side-product also the common good[9].

The hacking process consists of five phases. The first phase is *Foot printing* which is the process of gathering required data about the target computing system. The second phase is *Scanning* in which hacker uses various tools and techniques to detect vulnerabilities in a computing system. The third phase is *Gaining access* in which access to the target computing system is gained by denial of service or spoofing. The fourth phase is *Maintaining access* in which the hacker can use the access to secure the computing system to work as an ethical hacker or damage the computing system to work as a cracker. The last phase is *Covering tracks* in which the hacker tries to hide themselves on the target computer system. An ethical hacker should be aware of all techniques used by crackers for attacking the system, in order to protect the computing system from possible attacks.

### 6.1 Classification of Hackers

Based on the activities performed by the hackers, they can be classified in to four types. (i) Black Hats are hackers those who become crackers by using their computer skills for causing harm to computing systems. (ii) White Hats are the hackers those who act like security analyst by using their computer skills for protecting the

ISSN: 2454-9665

computing system. (iii) Grey Hats are hackers those who work as crackers or system analyst at different situations. (iv) Blue Hats are hackers those who work as computer security consultant to test a system for its security before launching it. Technology is ever growing and we are encountering tools that are beneficial to the general public, but in the wrong hands can create great controversy, breaching our basic right to privacy, respect and freewill[10].

## VII. SOLUTION TO SECURITY PROBLEMS

Ultimate There are many controls available to protect the computing systems from attacks. The most powerful tool in providing computer security is done with scrambling the data i.e. though the data is hacked by the cracker, it will not be in the useful form. Encryption is the term given for denoting the scrambling process. The original data in the understandable format is called plain text. Using encryption the data is transformed into a scramble format called as cipher text. Security professionals nullify virtually the possibility of interception, modification and fabrication. Encryption is the best method for ensuring all aspects of computer security[8].
Software controls can be implemented by using several tools and techniques. Software programs can be prevented by applying them in the design level itself. Hardware controls can be created by using locks, firewalls and intrusion detection systems. Apart from the application of software or hardware controls, agreed-on procedures and policies among the users can be enforced for better security.

## VIII. CONCLUSION

The fundamental challenge in the networks is securing the sensitive data. A better solution for securing sensitive data is using strong encryption techniques. Several encryption algorithm either symmetric or asymmetric is available today. From which algorithm can be chosen individually, two or more algorithms can be combined, a new encryption algorithm can be created, existing algorithm can be revised. Not only the encryption algorithms is important, key generation and management is also to be done efficiently for successful results. Once a better cryptography approach along with good key management concepts is created then data sharing in networks can be an be done effectively without any security fraught.

## REFERENCES

[1] Weingart, S.H. , White, S.R. , Arnold, Double, G.P, "An evaluation system for the physical security of computing systems"Computer Security Applications Conference, 1990.

[2] Judith M. Myerson, "Identifying enterprise network vulnerabilities", International Journal of Network Management, Volume 12, Issue 3, pages 135–144, May/June 2002.

[3] Kristopher Daley, Ryan Larson, Jerald Dawkins, "A Structural Framework for Modeling Multi-Stage Network Attacks", Proceedings of the International Conference on Parallel Processing Workshops (ICPPW'02) 1530-2016/02 $17.00 © 2002 IEEE.

[4] Richard C. Hollinger, "Hackers: Heroes of the Computer Revolution ?", Computers & Society, Vol. 21, No. 1 - June 1991.

[5] Marcus K. Rogersa, Kathryn Seigfriedb , Kirti Tidkea, "Self-reported computer criminal behavior: A psychological analysis", . Published by Elsevier Ltd. Doi:10.1016/j.diin.2006.06.002.

[6] Gupta, K. , Gupta, V., "Security threats in sensor network and their possible solutions", Instrumentation & Measurement, Sensor Network and Automation (IMSNA), 2012 International Symposium on (Volume:1 ).

[7] Seyedhossein Mohtasebi, , Ali Dehghantanha, "A Mitigation Approach to the Privacy and Malware Threats of Social Network Services", Digital Information Processing and Communications, Volume 189 of the series Communications in Computer and Information Science pp 448-459.

[8] NIV AHITUV, YEHESKEL LAPID and SEEV NEUMANN, "Processing Encrypted Data", Communications of the ACM, September 1987 Volume 30 Number 9.

[9] Bryan Smith William, Yurcik David Doss, "Ethical Hacking: The Security Justification Redux", 0-7803-7824-0/02/%10.00 62002 IEEE.

[10] DANISH JAMIL, MUHAMMAD NUMAN ALI KHAN, "IS ETHICAL HACKING ETHICAL?", International Journal of Engineering Science and Technology (IJEST), ISSN : 0975-5462 Vol. 3 No. 5 May 2011.