ISSN : 2347 - 8446 (Online)
ISSN : 2347 - 9817 (Print)
Vol. 3, Issue 3 (July - Sept. 2015)
International Journal of Advanced Research in Computer Science & Technology (IJARCST 2015)

Best Plan for System Security

Gaurav Kumar
Dept. of Information Technology, Bengal College of Engineering and Technology, Durgapur, West Bengal, India

Abstract
System Security is a major issue in the Internet world and Information technology world. Computer or System is Electronic or electromagnetic device which work under predefine set of instruction example simply calculator, IT professional are working on large volume of data or information are responsible for safe the company from the attack, cyber-attack or protect the information from leaking, an intentional or unintentional act may cause serious damage to information. In this paper, first we have explained the concept of System Security, security issues and explain plan of System Security. Experimental results show that the new proposed method works successfully.

Keyword
Security, Software attacks, System Security.

I. Introduction

System Security refers the protection of information system from the damage to the software as well as hardware [1]. It includes physical access to hardware as well protecting to the harm data, harm come via internet or code access [2]. Safe data from the intentional and accidental cases [3]. Generally system is a device that work on predefine set of instruction given by human being, IT profession are work on large volume of data, they are responsible for safe your data from the unauthorized source, virus ,cyber attack and information leak [4]. Computer security covers all mechanism and process where information, digital equipment and service are safe from the unauthorized source [5].

II. Background

1. Types of Attack

Backdoors

Backdoors refers to in an algorithm or computer system is any secret method of bypassing security control.

Denial of Service Attack

Denial of service attack are design to make a network resource to intended user means attack entering wrong password enough time cause that the victim account to be locked and overload the capability power of network and blocked all user at once.

Direct Access Attack

In this type of attack an unauthorized user or attacker gaining physical access of system to download directly data from it. They compromise security using installing software worms, operating system modification. Disk encryption is used to protect from these attack.

Spoofing

Basically spoofing of user identity tells a situation in which one program successfully masquerades of another falsifying data.

Privilege escalation

Privilege escalation tells some knowledge where attacker able to access some level of restricted area without authorization.

Social Engineering

Basically social engineering refers the aim to user disclose private data such as card number, password etc. Example: impersonating a bank [6].

2. System At Risk

Financial System

Financial system refers the website that store bank information such as credit card, bank account they are targeting to hacking because potential of money transfer and making purchase.

Industrial Equipment

The function utility likes powergrid coordination of telecommunication, nuclear power plant [7].

Aviation

The aviation industry is reliant on complex system which could be attack.

Consumer Device

Computer system are commonly infected with malware either to gather password.

Government

Government and military system are commonly attacker want attack on it because lot of hidden information and intelligence report are store on the system that why they are attacked by activists [8] and foreign power [9]. Regional government infrastructures such as traffic light control, police communication are use to stored in them.

Large Corporation

Large Corporation are commonly targeted by hacker, in many time it has been seen that they are aimed to financial gain via identity theft and involve data bench they result that lost of client credit card details by home depot [10]. Not all the attack are financial purpose other purpose like security etc.

Automobile

It gains the to the internal controller area network of car's [11], it is possible to control the steering wheel, as well as disable break. Computerize engine timing door locks, air bag, cruise control, advance driver assistance system make disruption on these possible.

ISSN : 2347 - 8446 (Online)
ISSN : 2347 - 9817 (Print)

III. Best Plan of System Security

Security Incidents

1. Area
FIRST ASSET OWNERSHIP-
You are taking responsibility of data, that are legal tell by you this data is under our responsibility?
WHAT ASSET IS PROTECTED BY US-
The data are mark by you?

2. Plan
WHAT LEVEL OF RISK CAN BE TAKEN BY US-
The level of risk we take for data?
WHAT WE COMMITMENT TO SECURITY-
Our commitment to Security means what you tell about security?

3. Trail Run
HOW MUCH RISK WE TAKEN FOR EACH ASSET
Commitment to the risk that taken for each asset?
HOW MUCH SEROUIS ARE THE THREAT TO OUR ASSET-
Your seriousness to assets.

4. Security Control
HOW THE RISK KEPT TO ACCEPTABLE LEVELS
The risk taken we acceptable levels.

5. Suitableness
WHICH ASSET ARE PROTECTED BY WHICH ASSET-
You define the asset that protects other asset?

6. Business Flow
WHAT IS THE PRIORITY FOR OUR BUSINESS-
How to give advantage for business?
ARE WE ACHIEVEING SET SERVICE LEVEL MEASURE.

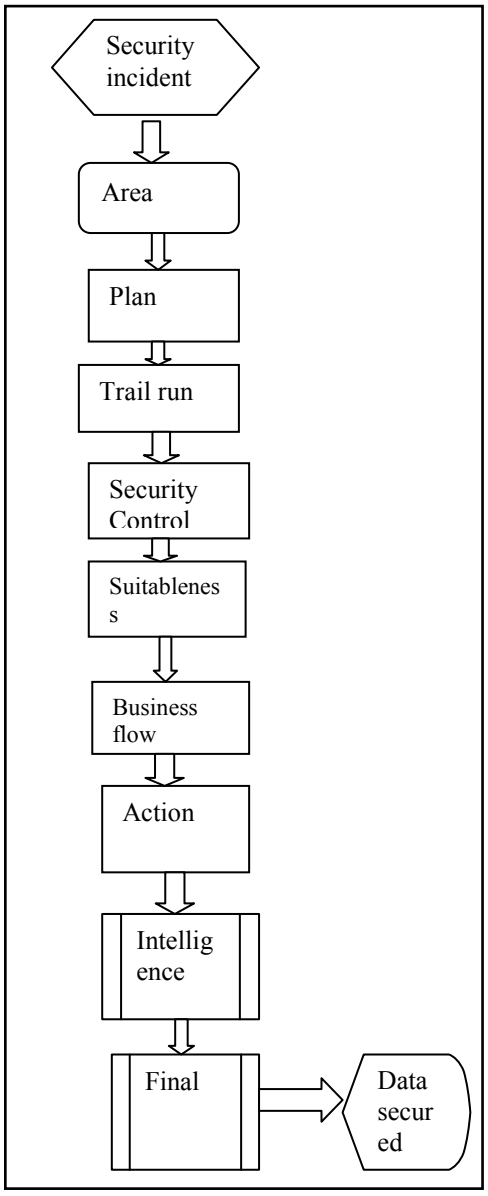
7. Action
HOW WE DO ALL THIS
Think of how to do all this?

8. Intelligence
TAKE CARE OF ALL THE ABOVE PROCESS-
Take care of above 1 to 7 process that work proper or not if any one of the not work or not satisfy our policy just inform about that.

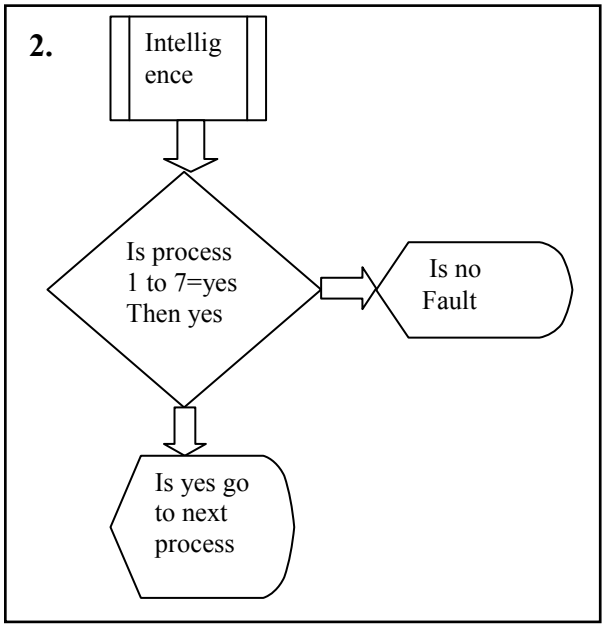
9. Final
AFTER A CERTAIN TIME CHECK THE PROCESS 8-
Within a certain Time interval that given by us check the process 8.

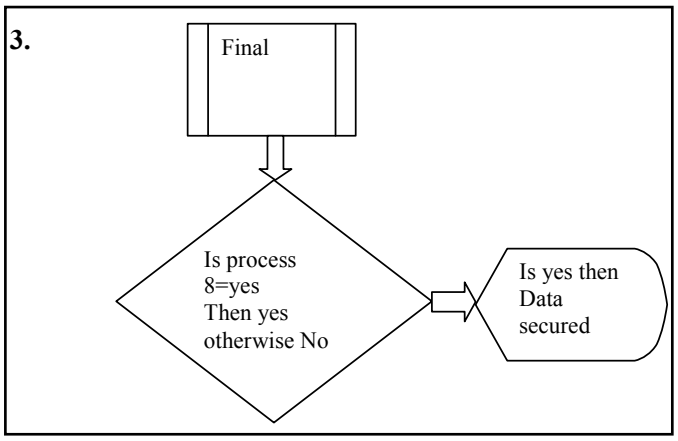
IV. Flowchart of Plan

1.



2.





V. Experimental Result

Theoratical Proof

The concept of above new business plan of system security and procedure, if an organization that work on data is work on the proposed method, data will be highly secure and the chance of data lost never happen and also high profit business, market value, market name, market trust become high in the IT field, the year 2008 data lost UK, in year 2010 lost encryption key these type of case never happen so from my point of view if the organization are work on the project data lost case not happen, start with the process one for organization work, first one is (Area)-first asset ownership, what type of asset are we protecting. Second process is (Plan)- we work on plan ,what level of risk can be taken by we, what we commitment to security. Third process is (Trail run)-we work on trail run, how much risk can be taken for each asset, how much serious are the threat to our asset. Fourth one is (Security control)-how is risk kept to acceptable levels. Fifth one is (Suitableness)- which asset are protected by which asset. Sixth One is the (Business flow)-we work on the business flow, what are priority for our business, are we achieving set service level measure. Seventh one is the (Action)-in the process we work on action, how we do all this. The main process is eight and nine for better data security, eighth one is the (Intelligence)- we work on intelligence ,take care of all the above seven process means one to seven, means if the process eight see any fault in any process between one to seven they just inform about that. The ninth process is the (Final)-we work on final, within a certain time given by us check the process eight. If process nine check any fault in process eight just inform about that and the procedure our data are safe no chance of leak. The process eight and nine are highly secure zone the both are only operated by organization or administrator.

VI. *Conclusion*

In this work we see that if we start work on the proposed or an organization work on the proposed method System Security, the system security become high, we can protect us from the security incident and also business continuity, market brand value become good of our organization. Or we can easily say we are safe for the cyber attack .the process 8 and 9 are main concept of method and finally we can safe from the attack.

References

[1]. Gasser, Morrie (1988). "Building a Secure Computer System (PDF)". Van Nostrand Reinhold. p. 3. ISBN 0-442-23022-2. 15 September 2015.

[2]. "Definition of Computer Security". Encyclopedia. Ziff Davis, PCMag. 15 September2015.

[3]. Rouse, Margaret. "Social engineering definition". TechTarget. 15 September 2015.

[4]. Gaurav Kumar, "Novel Method and Procedure for System Security", International Journal Of Advance Engineering and Global Technology, Vol. 3, 2015.

[5]. http://www.evolllution.com/opinions/cybersecurity-understanding-online-threat/ on 16 September 2015.

[6]. Arcos Sergio. "Social Engineering" (PDF).

[7]. Pagliery, Jose. "Hackers attacked the U.S. energy grid 79 times this year". CNN Money. Cable News Network.15 September 2015.

[8]. "Internet strikes back: Anonymous' Operation Megaupload explained". RT. January 20, 2012. Archived from the original on May 5, 2013. 15 September 2015.

[9]. "NSA Accessed Mexican President's Email", October 20, 2013, Jens Glüsing, Laura Poitras, Marcel Rosenbach and Holger Stark, spiegel.de

[10]. Melvin Backman (18 September 2014). "Home Depot: 56 million cards exposed in breach". CNNMoney

[11]. http://www.vox.com/2015/1/18/7629603/car-hacking-dangers on 16 September 2015.

Acknowledgement

I would like to thanks www.wikipedia.com for provide me help, mr. Aaryan Jha and National Computing Centre for some valuable input.

Author's Profile

GAURAV KUMAR: - He is pursuing the degree under Maulana Abul kalam Azad University of Technology (formerly known as West Bengal University of Technology), Kolkata .His major research and study area are Information Security, Digital Image Processing, Digital Watermarking, Data structure Design and Analysis of Algorithm, JAVA, C, C++, PYTHON, Computer Architecture, Operating System and Cloud Computing.