Automatic Campus Network Management using GPS

JAYAKUMAR.S
Assistant Professor (Jr)
School of Information Technology and Engineering
VIT University,
Vellore, Tamil Nadu, India

SENTHIL JAYAVEL
Assistant Professor (Sr)
School of Computing Science and Engineering
VIT University,
Vellore, Tamil Nadu, India

NITHYA.S
Assistant Professor
School of Information Technology and Engineering
VIT University,
Vellore, Tamil Nadu, India

Abstract: **The Organization Network is the place where large number of attacks is happening. The attackers are using different methodologies to capture the information from the end user without the knowledge of the end-user. This paper introduces the concepts of Campus Management and Emergency log by using Medium Access Control (MAC) and Global Positioning System (GPS). By using the IP address of an attacker, the MAC address can be found and the attacker's machine can be blocked access with the help of firewall. Using the GPS we can be able to navigate the attacker's position with the help of the position log. The log keeps updating for each and every 10 seconds. The attacker can be identified as if he used his own system or victim (3rd party) system. An emergency response log has been created to record each emergency incident response process. The role of the log is more important with an increasing accumulation of information with the log; Network Engineer/Administrator can determine the type of inevitable emergency incidents grouped into evitable events, in order to improve the system reliability of emergency response.**

Keywords: GPS, MAC, Network Monitoring, Log, Organization network, Network Security, Block

1. Introduction

When you think of threats to your Organization /Campus IT Security, what comes to mind? Hackers? Viruses? Laptop PC thieves? The reality is that every Organization/campus is vulnerable to a myriad of security threats. Keeping one step ahead of IT security issues can give even the most prepared IT department a headache, but you don't have to go it alone. Here this paper provides the solution such that users, student and staffs can safely access the network 24/7.

1.1 About Network Log

The Network log file contains events that are logged by the server system components. These events are often predetermined by the server system itself. Network log files may contain information about Network access, device changes, device drivers, system changes, events, operations and more

1.2 Organization/Campus System

In an Organization/Campus system's we need some sudden response for the unexpected warning in the network. So according to warning level, network administrators are need to response for the different levels of warnings to avoid the major crack-up in the network.

1.3 Supporting system

The other functional divisions also need some sudden response for the unexpected warning in the Organization /Campus network. To protect different functional divisions can't completely manage with each other when sudden warnings occurs, clear setting ahead liability of the different functional divisions in network to prevent to avoid it completely within the time of sudden event occurs.

1.4 Technical System

Technical system means when a sudden warning occurs in the Organization/ Campus Network that should be solved in the shortest path time to prevent the network returning to the usual mode. We have to find solution one by one addressing common network problems and technology systems to the network to continue to avoid new problems.

A Sudden reaction scheme is included in the above three parts because the Campus/Organization system and support system are dissimilar to the various organization, research center, universities and colleges. We will describe about the network monitoring and Security log with Media Access Control (MAC) and Global Positioning System (GPS) it put ahead to help us to record and summarize the proposed occurrences. How to design and use the log will be described in the second part and the conclusion at the last.

2. Technology System Based on Emergency Log

2.1 Levels of Response

According to the principle of sudden response approach, network and Information security emergency response can be divided into seven stages

Get Read -> Detection -> Restriction -> Extermination -> Recovery -> Track-> Analyze

2.1.1 Get Read is avoidance oriented, which includes software and hardware preparation, measurement and programs to proposed occurrence. Well knowledge managers are essential. Every day back-up of valuable records are e nable security audit log, update the system patch in time, keep ready for firewall, Interruption detection system, anomaly and G PS(Global Positioning System) monitoring system and other often used tools are general methods that well known.

2.1.2 Detection is to discover and determine the nature of the event. Detection method is d ependent on the relative software, trough a n umber of i ndications to conclude whether there are harmful code, files and directories is being altered with or other set of codes are discovered. When aberrant effect are found, the following actions may obtain a high return: Take to examine aberration, start th e audit function or add the amount of audit information, backup system as soon as possible, to avoid attackers trac k the system or clea r the trace of the attack a nd record what is happening on the emergency/sudden response log. Administrators have to calculate the appraisal the range and degree of incident influence and report the process to the leader.

2.1.3 Restriction refers to instantaneous activity which absolute the scope of the attacks and limits th e abeyant deficit injury. The R estriction Protocol includes close system, disconnected from the network, modify the firewall filtering rules, block or delete the account of devastating acts and so on. Although the methods are simple, the basic target of inh ibition is to fi nd out attackers or m alicious program and backdoor set up in the system.

2.1.4 Extermination means enduring healing portion by extermination the causes of occurrence. We must recognize the base/ core causes of the occurrence. Take off all the viruses from the memory, system and backup files, identify and take off the Trojan horse, recovery key documents and information and so on.

2.1.5 Recovery is to rec over the sy stem from backup. It should entirely return the destroy system and network equipment to the actual work situation. We usually re-install the system and the n restore the data, restore the entire system from a backup, inst all the operati ng system and firewall patches, repair the inadequacy in routers and other network equipment, remove temporary securing portion in the abolition and Extermination phase.

2.1.6 Track concern about the security situation after the system recovery. This is most likely to be overlooked phase of all e mergency response process. We review and merge relevant information on the events so to contribute to th e event handlers to sum up experience and i mprove skills. Any lessons learned from the pr ocess can be use d as training materials for new m anagers. By using emergency/sudden response log, once can trace the element, track attacks, analyze and study the entire incide nt, summary a report of the formation of the emergency response. This is also an im portant step for the ha ndlers to improve technical level.

2.1.7 Analyze is to analyze the a ttackers path to c heck whether the attacker is use d their own system or vi ctim system.

2.2 Working with Emergency Response Log

2.2.1 Design Log

Organization Network Emergency response systems are often in lower input and require a high level. So we have to use high-tech systems to make up for lack o f input. If the network administrator can authorize emergency response log to archive knowledge in credentials with the amplify amount of emergency response information, the log is special higher role i n emergency response because some occurrence will gradually from a q uestion – set with a practical solution-set. By an alyzing the features of the question-set, a rou tine defending issue set will g radually established which can decide the general emergency events, and the solution-set will become excellent and the best.

2.2.2 Form of the emergency response log

Logging information should include the causes of t he events; the a ffected extent, processes and c ountermeasures analysis etc see Table1.

When we find the sudden difficulty or problem in the system or server at that tim e we are tracking the IP address of the attacker. After fi nding the IP addres s of the attacker

Copyright (c) 2012 International Journal of Computer Science Issues. All Rights Reserved.

we are blocking that IP address in firewall to stop the further usage in the network. After blocking the IP address we are using the technology called ARP - Address Resolution Protocol included with TCP/IP makes it possible to find the MAC address. Using ARP, each computer maintains a list of both IP and MAC addresses for each device it has recently communicated with. Most computers allow you to see the list of IP and MAC addresses that ARP has collected there. In Windows, Linux and other operating systems, the command line utility "arp" shows this information. Using "arp," you can in fact determine the MAC address of some computers from their IP address. ARP works only within the small group of computers on a local area network (LAN), though, not across the Internet. ARP is intended for use by system administrators and is not generally useful as a way to track down computers and people on the Internet.

After finding the MAC address, blocking the MAC address in the firewall by doing this that system can’t able to access any more in network. Be cause the MAC address is permanent physical address of the system provided in the machine. By using IP and MAC address GPS start tracking the attacker position and keeps updating into the log table.

If the attacked system want to use the network anymore then administrator want to remove the MAC address from the firewall to access the system in network for anymore.

The Table1 is created for each and every log.

The GPS Table (Table 1) is created for every log separately and the link is provided in the field No. of the Table 2. The GPS table is updating of each and every 10 second from the GPS receiver and Network monitoring tool, the administrator as responsible to stop this updating log.

2.3 GPS – Table (Table I)

In the GPS table the field No is defined as number of updates from the starting time to the end time.

In the GPS table the field Place is defined as the Attacker first place in the first column and keeps updating of other columns if the attacker in roaming the place keeps changing. The place shows the full details of the attackers place.

This GPS table is saved defined according to the current year month and day (GPS-yyyymmdd). If there is more than one event in one day, we can use GPS-yyymmdd_n to record it.

When we find the sudden difficulty or problem in the system or server at that time we are tracking the IP address of the attacker. After finding the IP address of the attacker we are blocking that IP address in firewall to stop the further usage in the network. After blocking the IP address we are using the GPS (Global Positioning System) to track the IP address and Provider of the attacker and keep tracking the IP address by using GPS whether the attacker is attacking from one place or in roaming by keep tracking of this IP address and updating the log of each and every 10 seconds of the attacker.

2.4 Emergency Response Log – Table (Table II)

The field No. is defined according to the current year month and day (yyyymmdd). If there is more than one event in one day, we can use yyymmdd_n to record it. When an incident is reported or discovered, we have to propose the incident at first and fill the log when we have time or with 24 hours.

The field Incident Name is defined as whether it is Evitable or Inevitable event.

The field IP address is defined as it provides the attacker IP address, host and service provider.

The field MAC address is defined as it provides the MAC address of the attacker

The field System is defined as whether the attacker used their own system or victim (third party) system, and also its show how the system is connected to the server (via wifi or Lan).

The field Impact Range is defined as the details of how long and how many systems and servers are affected by the attacker.

The field Cause is defined as the problem occurred by the attacker’s code or program run by him.

The field process is defined as the process done by the system administrator.

The field Repair-Time is defined as the time taken to solve the entire problem.

The field Solution is defined as solution for the attacker’s problem

The field Improved Methods is defined as best improvised solution for the attacker’s problem.

Copyright (c) 2012 International Journal of Computer Science Issues. All Rights Reserved.

The field Technician is defined as the name of the administrator who locked and solved the problems is the network.

2.5 Use of Emergency log

Emergency events may be divided into two types: Evitable events and inevitable events. Evitable events refer to those events that have clearly defined type and process it may be inside the organization network. Next is an instance event that servers in center of organization network are found being attacked by hackers. The instance in Fig.1 shows how to use emergency response log in the process.

Table 1 – GPS

Name: Date:

(Sample values)

No of Updates (from start to end time)	Place
19.10	#1, MB, vit university, vellore
19.20	#1, MB, vit university, vellore

Table 2 - Emergency Response Log

Register: Date:

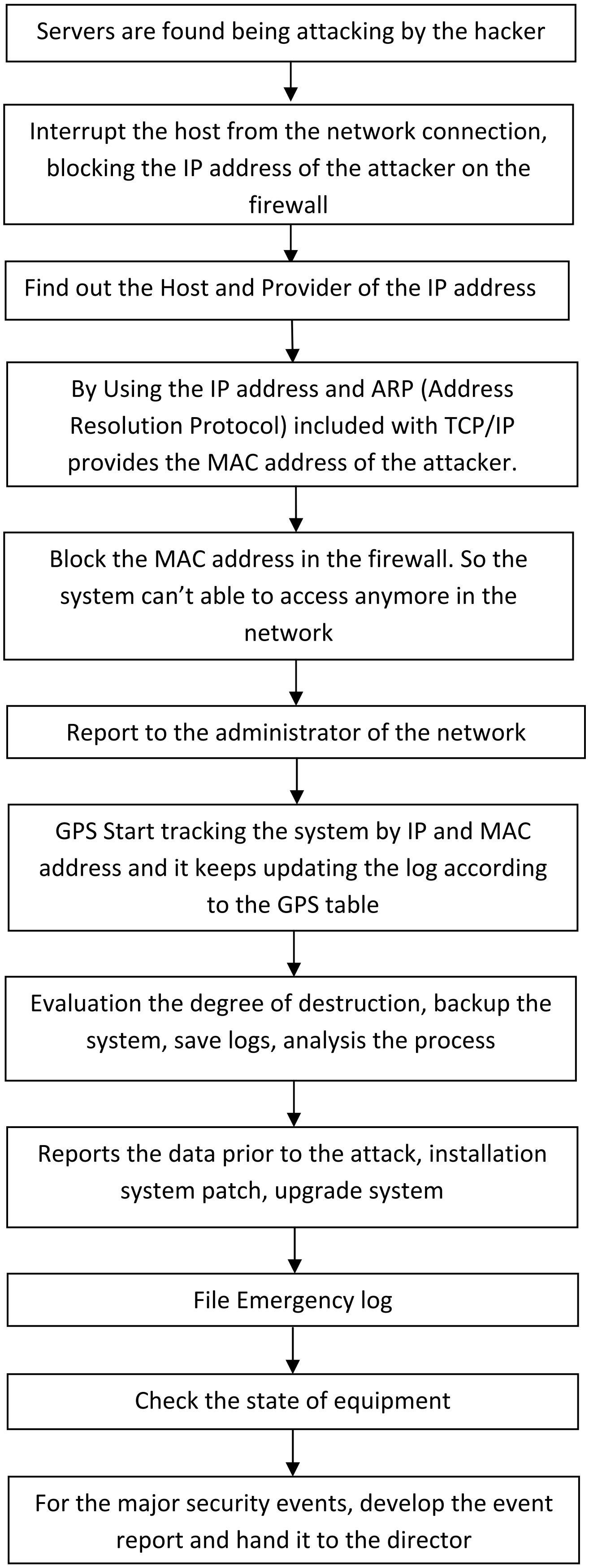
(Sample values)

NO.	Incident Name	IP address	MAC address	System	Impact Range	Cause	Process	Repair-Time	Solution	Improved Methods	Technician
20110101	Evitable	192.168.1.1 Service Provider: Earth Link Cable	0C-0C-0B-14-CD-E7	Laptop (direct system) (wifi)	Affected 10 systems	Not running any programs	Restoring the data	2.15hr	Scanned and deleted the virus	Updated the patches and blocked the ports	Jayakumar

In the events of attacking, the process is as follows (fig.1):

Figure 1 – Use of Emergency Log

Copyright (c) 2012 International Journal of Computer Science Issues. All Rights Reserved.


Servers are found being attacking by the hacker
Interrupt the host from the network connection, blocking the IP address of the attacker on the firewall
Find out the Host and Provider of the IP address
By Using the IP address and ARP (Address Resolution Protocol) included with TCP/IP provides the MAC address of the attacker.
Block the MAC address in the firewall. So the system can't able to access anymore in the network
Report to the administrator of the network
GPS Start tracking the system by IP and MAC address and it keeps updating the log according to the GPS table
Evaluation the degree of destruction, backup the system, save logs, analysis the process
Reports the data prior to the attack, installation system patch, upgrade system
File Emergency log
Check the state of equipment
For the major security events, develop the event report and hand it to the director

The Establishment of emergency response system is to protect network resources. Any protection system should be based on prevention. So we have estimate the security of campus/organization network. Emergency response log is practical and high detection level of taking preventive measures in the technical system. The key is established emergency response plan lies in the co-ordination of interaction between the different components. The log is also the base of the plan.

4. REFERENCES

[1] Shengzhong YUAN, Wei WANG by A Campus Network Security Emergency Response Technical System Based on Emergency Log e-Business and Information System Security (EBISS), 2010 2nd International Conference on 22-23 May 2010

[2] Improve GPS Positioning Accuracy with Context Awareness by Jiung-yao Huang, Chung-Hsien Tsai

[3] QIN Runmei, Guangxi Internet Security Emergency Response and Countermeasures [J], Guangxi Communication Technology, 2008 (2):7-9.

[4] Schultz. E Translated by DUAN Haixin, Response to the Network Security Incidents [M]. Beijing, Posts & Telecom Press, 2002.

[5]Ensuring GPS Navigation Integrity using Receiver Autonomous Integrity Monitoring by William R. Michalson

[6] Julia H, Allen CERT, Safety Guide [M], Beijing, Tsinghua University Press, 2002.

[7] LIU Zhenfeng, Discussion of the Emergency Response on Network Information Security Incidents [J], Technology Research and Application, 2007 (2):44-47

5. WEBSITES

[1] http://people.richland.edu/dkirby/141macaddress.htm

[2] http://www.wisegeek.com/what-is-a-mac-address.htm

[3] http://www.cert.org/stats/cert_stats.html

[4] http://www.gps.gov/

[5] http://www8.garmin.com/aboutGPS/

[6] http://en.wikipedia.org/wiki/Global_Positioning_System

Copyright (c) 2012 International Journal of Computer Science Issues. All Rights Reserved.