Network Security: Analysis of Network Crimes and Data Protection Methodologies

C. K. Adhikarinayake, V. W. Baddegama, G. M. Bandara, E. L. B. H. Erabadda and M. S. R. Senarathna
Department of Computer Science & Engineering, University of Moratuwa

Abstract — *Computers have replaced majority of file based systems. File sharing has become essential for any company and for any individual with increasing usage of technology. Use of secure networks is essential for these systems to be successful. In this paper we have discussed how security of computer based systems can be threatened due to various reasons and how these threats can be minimized adopting various methodologies. We bring up current solutions implemented in the current world and some new theoretical designs. The paper is mainly focuses on the users at the end points of the network. The security aspect related to provide secured connections between them (data encryption, etc.) is not discussed in the paper.*

Index Terms — Network security, Protection, Network crimes

I. Introduction

Ensuring the security of a network is not an easy task, but it is the most crucial aspect of majority of the networks. The purpose of this document is to summarize the threats identified for network security, problems that are solvable and problems that are not solvable. First the document talks about the threats to network security and the types of crimes that are carried out over networks. Then, prevention of these threats and crimes is addressed by suggesting various methodologies. The document then concludes by presenting some common types of technologies that are used for networking and how security can be achieved in those techniques.

At present, computers have become an important asset to a majority of business firms since they can provide accurate and timely information for decision making. Network technologies have progressed through increasing levels of sophistication and resource distribution. The use of data communication to interconnect computerized storage devices and to provide wide access to the databases has increased widely. However, over the years, increasing use of computers to store, organize and retrieve data on demand has raised new concerns. [1]

II. Types of Network Computer Crimes

Network computer crimes can be divided roughly into four large categories: financial fraud and theft, program theft, services theft, and vandalism.

A. Financial Fraud

Financial fraud and theft is the greatest and most widely recognized computer crime in almost all organizations which use computer networks. It includes altering computer records to obtain money, stealing proprietary information stored in computers, and manipulating financial data to produce fraudulent financial reports. The items which are being stolen include non-current assets of the organization such as equipments, products, services, and many other company resources. The small crime schemes that are being identified often take one or more of the following forms: [1]

- Inventory lists being stolen.
- Cash sales entries being altered.
- Goods being stolen by deceitful employees after gathering internal information.
- Valuable materials being substituted with false ones.
- Use of false destination addresses.
- Sales commissions and discounts being altered to show higher values.

B. Program Theft

Much program theft is a result of what is known as the "differential association" theory. Most people feel that it is not necessarily a crime to copy computer programs from the office. They experience no guilt as a result of engaging in this type of crime. However, the outcome of such theft is that the owners of these programs suffer a loss. To compensate this loss, the prices of these programs are increased and then the legal users have to shoulder the burden of the cost for illegal use.

C. Services Theft

The most common kind of services theft is using the company's computer facility and time to do personal work. Gaining access to the confidential files of others without prior authorization is also considered data abuse. This form of crime sometimes entails a dishonest employee copying files and selling them to his or her company's competitors. Service theft can also take the form of a dishonest company employee inserting fraudulent data into the firm's computer for the purpose of creating fictitious claims such as life, health, accident, and casualty insurance cases.

III. Prevention of Network Attacks

Security of networks has three main elements namely confidentiality, integrity and availability. When the security of a network is reviewed, it is essential to review all the three factors. It should be considered as a responsibility of management to take care of the security of the company network, rather than leaving it to technical people to take care, as security of the network is of prime interest .There are

certain steps to be taken when handling security of a network[2]. They are:

- Controlling environment
- Controlling communication lines
- Controlling people
- Controlling machines

(a) Controlling Environment

There are two main objectives in environmental control. One is to prevent unauthorized access to network. Next is to protect the system as a whole against various unauthorized activities. To fulfill these objectives, due steps should be taken. [2]

- Restrict the right of access to hardware to authorized users.
- All types of users should be identified at the time of installation of computers.
- Identification should be worn by staff all the time.

(b) Controlling Communication Lines

There are many types of media that can be used as network cables and the selection of the type of the media to be used affects the security of the system. Therefore fundamental security action in controlling communication lines is to identify the correct type of cable type to be used. This is because, if any external cable can be connected to the network without prior authorization, password authentication is going to have less value. [2]

(c) Controlling People

When controlling people, attention should be given on following factors.

- Who people are
- What those people can do on the system
- When and how people can do those
- Who else needs to be involved

The objective of controlling people can be achieved by having a security policy to control access. The basic control mechanism is to segregate responsibilities of various user groups. These groups include operators and programmers, and data entry staff and data control. Additionally, most organizations have departments which process data separately in a discrete manner. It is important to give differing privileges to different groups depending on the tasks they carry out. [2]
To control access, various authentication mechanisms can be used. This may be either something person knows or something person has. Or this can be further extended to authenticate with what the person is using sophisticated psychological measurements such as retinal eye pattern, finger print, and signature.

(d) Controlling Machines

Once background controlling has been laid out, next controlling the network and computer devices is needed. For a small network, using a keyboard lock may be sufficient. But for a larger network, more security measurements need to be taken.

A. Practices and Concepts to Maintain Security in Networks

(a) Security plans

To run a network efficiently administrators need to have a plan. A Security plan

- Helps you define and organize your security system into manageable pieces.
- Can provide a historical context.
- Helps to find that the goals of management and of the network's users.

A properly designed and implemented security plan can change the way everyone views the network. Implementing a good security plan takes time and patience. Security threats can be prevented with adequate security plans in conjunction with adequate programs.
There are a few steps that should be followed when implement a security system

- Create a list of all the users on your network
- Design and complete a security assignment chart. Verify that each person on the list has clearly defined boundaries to their authority.
- Use network's utility to add all the users to the user list.
- Organize the user list and a copy of the network's written policy in a way that encourages you to review them on a regular basis when you review your lists.

(b) Menu systems

Menu systems allow the users access to the required parts of the system without allowing them access to sensitive areas. The only way that the users could bypass the menu is if you create a poor implementation allowing them access to the command line. LAN Select, WordPerfect Office, and Direct Access are some of menu programs. There are two elements that must be considered in creating a secure environment using a menu system: the benefits to the user (data protection) and the benefits to administrators (higher system reliability in the long run reducing downtime and maintenance).

(c) Continuous User Authentication to Detect Masquerades

Intrusion detection is based on the matching the user's current stream of events against his previously learned patterns of behavior. The assumption used here is "*users' behavior includes sequential and temporal regularities that can be detected and coded as a number of patterns. Sequential pattern describes a sequence of events that a user repeats time after time in same consecution. A temporal pattern describes temporal regularities that are observed to hold among events' time length and intervals*". [3]

User profile creation is a search for regularities in users' activities analyzing audit trails. In this approach these regularities are aggregated to use profiles. Classes and Instances are used to build behavioral patterns.

Architecture of this prototype consists of three components. They are a detection server, control centre and host agents. Host agents are compatible with UNIX type operating systems. When an operating system on a workstation starts the host agent is loaded in to memory. Then it is send a message to the control centre and is controlled by the centre. Local agents collect information about user action and send to the detection server in an encrypted channel. Detection server decrypts the data and instantiate the application server for each active user in received data. Application server analyzes the data and if it sees a new action deviate highly from stored temporal and sequential behavior, it informs the system administrator. Otherwise update the user profiles.

Training of the system consists of two phases. Training itself and calculation thresholds. In first phase user profiles are created and system learns patterns of users' behaviors. In second phase system creates threshold values for each profile.

Changing the behavior of users' is a main issue in this approach. Therefore the effective lifetime of a static user profile is limited. So the constantly update of the user profile is required. Classification of actions consists of two parts. Classification time for actions inside a sliding window and time necessary to update the coefficient of reliability before moving the window, can be stated as follows. A workstation with AMD 1.4 GHz, 512MB of memory and Linux 7.1 spends 28.2s to classify 461,540 actions. According to the observations fast systems does not improve performance of the system. The amount of information sent over a local network depends only on the number of active users. The classifier's detection accuracy lies in the (0; 0.71) interval.

(d) The aggregation Method

Debar and Wespi (2001) proposed an aggregation and correlation components. It used predefined rules for correlation analysis. In these rules, redundant and causal relationships between alerts were defined. The main shortcoming of this method lies in a lack of a comprehensive consideration to relationships among alerts and a lack of correlation of unknown attacks. Aggregation method is one of the core methods in all kinds of security event management systems in different appearances.

We can identify four definitions of aggregation method.

- Minimum granularity.
  Aggregation of security events of the same node, port, and attack type triggered by an atomic attack action from different SES (State Emergency Service)s
- Medium granularity.
  Aggregation of security events of the same node and attack type triggered by an atomic attack action from different SESs
- Large granularity.
  Aggregation of security events of the same node, port, and attack type triggered by the congener atomic attack action from different SESs
- Super-large granularity.
  Aggregation of security events of the same node and attack type triggered by the congener atomic attack action from different SESs

The aggregation method reduces redundancy obviously. Using a weak queue length instead of the time window solved the problem that time window was difficult to determine. Using the expression of all HSE (Higher Speed Ethernet) s of a node in cache guarantees quality of real time and allows the following sequence correlation correlating multi-step attacks performed within enough period of time. The method does not include other parameter which is difficult to determine and has no misstatements. In summary, the aggregation method is suitable for real-time management of difficult issues to resolve massive security events.

B. Security of a Web Based System

The security of a web based system should be ensured in four fronts

- Web clients
- Data transport
- Web servers
- Operating system

There are number of architectures and technologies that can be used to protect web clients, email clients, etc. These architectures have either proposed as methodologies or actual implementations.

C. Methodologies

(a) Reference monitor security model

Reference monitor is a controlling element in hardware and operating system to regulate access of subjects to objects. It uses security kernel database to check privileges for each subject [4]. There are some major problems related to reference monitor concept [6]

- Too complex and requires the developers to start with totally new operating system design
- High overhead

But these can be implemented as part of prevailing systems.

(b) Firewall Concept

Fire wall is a protecting mechanism created based on set of rules to prevent or grant access to specific users. It prevents unauthorized access while permits legitimate communications to pass. A firewall has to be configured properly in order to become an effective type of network security method. Firewalls are classified as three main categories [4].

Packet filters

It filters packets based on the information containing in the packet itself. If the packet matches the set of rules of the packet filter, it allows the packet. Else it rejects the packet and sends error message. This type of firewall operates at the first three layers of the OSI reference model [5].

Circuit gateways

This is also known as 'stateful filters'. It uses rules in packet filter firewall and check the position of each packet in the data stream. This filter operates at the first four layers of the OSI reference model.

Application level gateways

This can "understand" certain applications and protocols. It helps to detect if an unwanted protocol is trying to access through on a non-standard port or if a protocol is being abused in any harmful way.

However they cannot help in the detection of spyware that is masquerading in programs that use the network for legitimate purpose.

(c) Virtual Machine Concept

Virtual machine is software designed to imitate an actual machine. Any software running inside the virtual machine environment can only access the resources allocated to this environment. Some of them are emulators. Others provide behaviors of an actual machine or a system. They are system independent and they do not contact with operating system, they provide better security [4]. Java Virtual Machine, VMware are some of the examples.

The main disadvantage of this is less efficient than an actual machine when it access hardware indirectly.

D. Software Implementation

(a) Java Sandbox

Java sandbox is java's security model by which any untrusted java applet must abide. It prevents malicious code behavior, thus protecting a network client from possible attack[4]. This is a security mechanism to separate running programs. It is used to test untrusted applications, applets, etc. this method is used widely in preventing malicious codes which comes through network to harm a host machine.

This method is used to check applets. It provides save mechanism to execute untrusted code embedded in web pages. Java sandbox contain following technologies [4]

1. byte code verifier
2. applet class loader
3. security manager

These technologies prevent an applet from abusing restricted privileges.

(b) Code Signing

The programmers sign components and the user decides based on the signatures which components to allow on the computer. Code signing does prove the integrity and authenticity of a piece of software purchased or downloaded over the internet. But it does not promote accountability [4].

IV. Types of Network Technologies and Their Security Techniques

A. Code Mobility

As a result of the internet as an open and global programming environment, new programming paradigms based on mobile entities such as Mobile Agents (MA) have been introduced. But the mobility increases potential of security breaches because of the injection of possibly malicious Mobile Agents. Protecting MA against integrity and secrecy attack has become a part of network security.

(a) What Is a Mobile Code

"*The mobile code paradigm encompasses programs that can be executed on one or several hosts other than the one that they originate from.*"[6] Mobile code can be downloaded to the client workstation and execute in on the clients workspace. Unlike in client server architecture, the overhead in networks can be reduced by using code mobility Mobile code systems range from simple applets to intelligent software agents. These systems offer several advantages over the more traditional distributed computing approaches: flexibility in software design beyond the well-established object oriented paradigm and bandwidth optimization are some of them. Increase in the flexibility can cause increase in vulnerability. This can cause security issues for code user. Sergio Loureiro, RefikMolva, Yves Roudier [6] discuss about the threats and the methods to prevent them.

(b) Mobile Code Security Threats

A mobile code generated by a malicious outsider can attack the host environment when it is executed. This bears similarity to Trojan horse but it aims at transparency, automation, and a wider scale of execution.

When protecting a host from potentially malicious code, code mobility imposes the following security features [6].

- Mobile code's origin must be authenticates because the host and the mobile code bear separate identities.
- Host must verify the integrity of the mobile code because it is exposed through the network.
- The actions of the mobile code should be controlled using access control mechanism by the host.

Mobile code is not limited to a single host. It can be used throughout the network. A malicious host can infect a mobile code. As a result mobile code must be protected from the hosts.

(c) Protection of a Host from a Mobile Code

The simple method for protecting a host is simply limit the functionality of the execution environment in order to limit the vulnerabilities.

Following methods are used to protect a host from a malicious mobile code. [6]

- Sandboxing

Here the code is executed in a restricted environment called "sandbox". This approach is used in Java in order to enable applet to run within a browser anywhere on the internet.

- Access Control

This method contains the best parts of the code signing method and sandbox method. The actions performed by a mobile code can be restricted to some resources while it permits at the same time to write and run really useful software. Yet, the enforcement of the access scheme has a cost, since it is performed dynamically, at runtime.

(d) Mobile Agent vs. Mobile Code

"*A mobile agent is a specific form of mobile code. However, in contrast to the Remote evaluation and Code on demand programming paradigms, mobile agents are active in that they can choose to migrate between computers at any time during their execution. This makes them a powerful tool for implementing distributed applications in a computer network*" (Wikipedia).

Commercial or wide-network deployment of Mobile Agent Systems is not possible without satisfying security architecture. Following are some of them.

There are two main types of attacks on mobile agents and platforms [7]

- Active attacks -These attacks try to modify the system and cause different behavior of system.
- Passive attacks -Collect data without authorization. (e.g., eavesdropping)

There are many systems that are suggested and implemented to provide secure network environment.

B. Suggested systems to provide better security for mobile agents

(a) Mobile Agent Security Using Proxy Agents and Trusted Domains

Nikola Mitrovi´c and UnaiArronateguiArribalzaga[7] propose architecture for mobile agent security using proxy agents and trusted domains in their paper. According to them, the existing approaches are based on security services at the level of agent system or specific objects. The suggested system uses proxy agents to enable transparent security services.

When a system is more secure, it gets more difficult to build and more complex to maintain. If it is a simple system, then it can be vulnerable. These two aspects have to be managed to provide better efficient security system.

Proposed system uses a proxy agent to facilitate security. Security proxy agent is mobile agent that provides security services to both agents and/or agent systems. These agents provide the security for their agents. It reduces the complexity. Our architecture relies on the concept of Trusted Domains. [7]

(b) P2P Network Security

P2P means sharing services between the same level of hosts. It does not have either master or slaves. Since the privileges that the peers have the same, P2P networks are more vulnerable to attacks.The main threat to P2P network is the Polipvirus, which is in the top of the Symantec malicious program list 2006. It is polymorphic which means it can change itself as the environment changes. Once it is downloaded to a computer it configures the computer to lower security configuration and make that PC more vulnerable to other attacks. Future Polip like viruses may be more difficult to track, as they will be custom designed to circumvent the reactive computer security and take the advantages of the new network configurations. [11]

(c) Network and internet pricing model

This is a proposed model that associates the impact that a new link in a network has on the overall security of the network with the price charged to make that link. Specifically, a pricing model is proposed that impacts how resistant or vulnerable a network is to the propagation of malicious code. However, due to the diversity of P2P configurations, a single P2P network security pricing approach may not be practical. Therefore, it is essential to recognise the desired characteristics for a viable P2P.

Network security pricing models [11]:

Online pricing should encourage users to choose links that improve the network's resistance to the spread of malicious code in the network.

Online pricing should take into account the current state of network security with respect to its resistance to the spread of malicious code.

Online pricing should be calculated in real time or "on the fly" as the network configuration changes due to the creation of new nodes and new links.

Over time, online pricing should yield networks more resistant to malicious code propagation through the pricing mechanism's influence on the growth of the network.

Essentially, the network security pricing model applies an incentive compatible mechanism that yields more secure networks. Users are charged higher prices for choosing to download files that degrade a network's resistance to the spread of malicious code and lower prices for downloads that will increase a network's resistance to the spread of malicious code.

(d) Wireless Home Security

Bradley Mitchell who graduate from Massachusetts Institute of Technology (M.I.T.) has explained very simple facts that we can be aware of, in order to make home network secure. As he says the first thing to do is to change the default usernames and passwords for administrators. Most of the users do not change the password of their routers so others can hack into the routers using the default passwords.

The second point he tries to point out is, using an encryption method. What he suggests is to use WPA/WEP encryption as it is understandable by most of the devices when it comes for decrypting. He also suggests using separate

firewalls for separate computers and separate routers and using static IP addressing over dynamic IP addressing.

Other two important tips are changing the default SSID and using MAC address filtering. Manufacturers ship their devices with default access points called SSID. Knowing the SSID is not helpful for an attack, but one can take the initial step for an attack. Using MAC addressing filtering allows only home network devices to communicate through the network.

V. Conclusion

Network security is a prominent feature of the network ensuring accountability, confidentiality, integrity, and all protection against many external and internal threats. Nowadays Computer criminals are common and they may harm your systems, steal or destroy your personal data and properties. Depending on the type of network various types of technologies are used to detect and prevent the masqueraders. Basically to achieve the security of a network based system four factors should be considered: Controlling environment, controlling communication lines, controlling people and controlling machines.

References

[1] Michael T. Tang ,"Collaring the Computer Criminal: An Analysis of Information Security for Network Computing" Managerial Auditing Journal, Vol. 6 Iss: 3, pp 14 - 17

[2] Rob Melville, (2007) "COMPUTER SECURITY-Network and Communications Security", Journal of Financial Crime, Vol. 3 No 2, pp 163-168

[3] AlexandrSeleznyov, SeppoPuuronen, (2003)"Using continuous user authentication to detect masqueraders "

[4] Victoria Skoularidou, DiomidisSpinellis, (2003) "Security architectures for network clients", Information Management & Computer Security, Vol. 11 Iss: 2, pp.84 – 91

[5] William R. Cheswick, Steven M. Bellovin, Aviel D. Rubin (2003). Firewalls and Internet security: repelling the wily hacker

[6] Sergio Loureiro, RefikMolva, Yves Roudier ,(2000) "Mobile Code Security" , ISYPAR 2000 (4ème Ecoled'Informatique des SystèmesParallèles et Répartis), Code Mobile, Toulouse, France, February 1st-3rd

[7] Nikola Mitrovic, UnaiArronategui, (2002) "Mobile Agent security using Proxy-agents and Trusted Domains" In Second International Workshop on Security of Mobile Multiagent Systems (SEMAS 2002) , pp. 81-83

[8] Olaf Winkel, (2007) "Electronic government and network security: a viewpoint", Transforming Government: People, Process and Policy, Vol. 1 Iss: 3, pp.220 - 229

[9] Rob Melville, (1995) "Network and Communications Security", Journal of Financial Crime, Vol. 3 Iss: 2, pp.163 - 168

[10] Antonio Corradi, Rebecca Montanari, CesareStefanelli, (2001) "Security of mobile agents on the Internet", Internet Research, Vol. 11 Iss: 1, pp.84 - 95

[11] Daniel O. Rice, (2007) "Protecting online information sharing in peer-to-peer (P2P) networks: A proposal for a P2P network security pricing model", Online Information Review, Vol. 31 Iss: 5, pp.682 - 693

[12] MarekBialoglowy, (2010) , "Bluetooth Security Review, part 1, Symantec Connect Community" , http://www.symantec.com/connect/articles/bluetooth-security-review-part-1

[13] Bradley Mitchell, "10 Tips for Wireless Home Network Security", http://compnetworking.about.com/od/wirelesssecurity/tp/wifisecurity.htm

[14] Zhitang Li, Yangming Ma, Li Wang, Jie Lei, Jie Ma, (2011) "A novel real-time aggregation method on network security events", Kybernetes, Vol. 40 Iss: 5/6, pp.912 – 920

[15] Robert Loew, Ingo Stengel, UdoBleimann, Aidan McDonald, (1999) "Security aspects of an enterprise-wide network architecture", Internet Research, Vol.9 Iss:1,pp.8-15