International Journal of Trend in Scientific Research and Development (IJTSRD)
Volume 3 Issue 5, August 2019 Available Online: www.ijtsrd.com e-ISSN: 2456 – 6470

Designing Security Assessment of Client- Server System using Attack Tree Modeling

Sandar Pa Pa Thein, Phyu Phyu, Thin Thin Swe

University of Computer Studies, Pathein, Myanmar

How to cite this paper: Sandar Pa Pa Thein | Phyu Phyu | Thin Thin Swe "Designing Security Assessment of Client-Server System using Attack Tree Modeling" Published in International Journal of Trend in Scientific Research and Development (ijtsrd), ISSN: 2456-6470, Volume-3 | Issue-5, August 2019, pp.1628-1633, **https://doi.org/10.31142/ijtsrd26727**

IJTSRD26727

ABSTRACT

Information security has grown as a prominent issue in our digital life. The network security is becoming more significant as the volume of data being exchanged over net increases day by day. Attack trees (AT) technique play an important role to investigate the threat analysis problem to known cyber-attacks for risk assessment. The technique is especially effective in assessing and managing the risks from hostile, intelligent adversaries. It is useful for analyzing threats against assets ranging from information systems to physical infrastructure. By using attack tree modeling analysis an organization can understand the ways in which they will be attacked, determine the likelihood and impact (damage) of these attacks and decide what action to take where the risks are unacceptable. This paper describes the attack tree model for organization based on Client-Server Network. It provides the ways for defending and preventing sensitive information from attackers. Attack tree modeling provides for effective security solutions, cost effective security solutions and defensible risk mitigation decisions.

KEYWORDS: *attack tree, threat, effective security solution, Client-Server Network, preventing information*

I. INTRODUCTION

Computer and Network systems are an important part of everyday life to many people across the world. Computers in the hands of consumers who lack the knowledge of protection tools and who have limited administrator skills are vulnerable to virus attacks.

Attackers exploit vulnerabilities in the software layers to install malicious programs on user machines to steal secret data for financial gains. Security protocols have been in place for some time to counter the threat posed by the attacks.

However, despite the presence of such measures, the number of attacks on consumer computers is growing rapidly. A recent trend in attacks has been the attempt to disable security protocols in place at the host machine. This type of attack leaves the host computer completely defenseless and vulnerable to many further exploits through the Internet.

Confidential information including customer information, business plans and financials has become one of every organization's most important assets. Yet technology advancements, new business models and increasingly sophisticated and globally interconnected business processes have outpaced not only regulations designed to ensure the privacy and protection of personal and other data but also many organizations' own ability to effectively secure sensitive business information. At the same time, with employees accessing that information from mobile devices and through sophisticated collaboration tools, companies must find ways to protect it, whether it's in storage or being transmitted across networks [8].

There is a need for assurance that these records are securely protected from attacks. For client- server system, the number of possible attacks is potentially very large. In this paper, a threat modeling methodology, known as attack tree, is employed to analyze attacks affecting confidential information in client-server systems.

II. Motivation

Nowadays the security of computer systems is a very important area in the information technology industry. By the increasing cross-linking of computer systems and the associated risks like Trojans, viruses and Distributed Denial of Service (DDoS) attacks this industry gains more significance. The associated possible threats like the unintentional stealing of passwords, the destruction of data or the attempt to make computer networks unattainable can be life threatening for a company. To deal with new security threats, computer companies spend much money. Before money is spent for security issues, the causes and the attack possibilities respectively have to be worked out. For this task the risk analysis can be consulted.

As a part of the risk analysis, the Attack Tree analysis offers possibilities to find out such attacks and causes – obvious threats as well as initially not regarded threats. Since these can produce harm to security relevant systems, the Attack Tree analysis helps to secure systems by finding preferably all attacks. The advantage of the Attack Trees is the easy understanding of this method and the possibility of receiving fast results. Thus, it is usable for both beginners and professionals [4].

III. ATTACKERS AND VULUNERABILITIES

To plan and implement a good security strategy, first be aware of some of the issues which determined, motivated attackers exploit to compromise systems. But before detailing these issues, the terminology used when identifying an attacker must be defined (Virus, worms Trojans, Spyware, Backdoors and so on) [7].

A. Virus

A virus is a computer program that can spread across computers and networks by making copies of itself, usually without the user's knowledge. Viruses can have harmful effects. These can range from displaying irritating messages to stealing data or giving other users control over your computer. A virus program has to be run before it can infect your computer. They can attach themselves to other programs or hide in code that is run automatically when you open certain types of file. Sometimes they can exploit security flaws in your computer's operating system to run and to spread them automatically. Viruses used to play pranks or stop your computer working, but now they compromise security in more insidious ways [7].

B. Worms

A worm is a program that propagates across a network by exploiting security awes of machines in the network. The key difference between a worm and a virus is that a worm is autonomous. That is, the spread of active worms does not need any human interaction. As a result, active worms can spread in as fast as a few minutes. The propagation of active worms enables one to control millions of hosts by launching DDoS attacks, accessing confidential information, and destroying or corrupting valuable data [7].

C. Spyware

Spyware is software that enables advertisers to gather information about a computer user's habits. Spyware programs are not viruses but they can have undesirable effects. You can get spyware on your computer when you visit certain websites. The spyware then runs on the computer, tracking your activity and reports it to others, such as advertisers. Spyware also uses memory and processing capacity, and can slow or crash the computer [7].

D. Trojans

A Trojan horse, or Trojan, is a non-self-replicating type of malware which appears to perform a desirable function but instead facilitates unauthorized access to the user's computer system. Trojans do not attempt to inject themselves into other files like a computer virus. Trojan horses may steal information, or harm their host computer systems. Trojans may use drive-by downloads or install via online games or internet-driven applications in order to reach target computers. The term is derived from the Trojan Horse story in Greek mythology because Trojan horses employ a form of "social engineering," presenting themselves as harmless, useful gifts, in order to persuade victims to install them on their computers [7].

E. Backdoors

A backdoor is an unusual way which an attacker can use it to get into the system. Normal users use login boxes and password protected ways to use the system. Even system administrator may add some security features to this system to make it more protect, but the attacker can easily use installed backdoor to get into system without any password or authenticating. Most of attackers like to protect their backdoor on victim system. They do not like that some another attacker use the same vulnerability to get into victim system and change their configurations. Although the system could be in a company and somebody else use that for working, but attacker is the owner of system and can install any application or use stored infractions which is exists on that system.

Sometimes attacker makes a very secure backdoor even much safer than normal way to get into system. A normal user may use only one password for using the system but a backdoor may needs many authentications or SSH layer to let attacker use the system. Usually it is harder to get into the victim system from installed backdoor in compare with normal logging in [7].

IV. CLIENT-SERVER NETWORK

Generally, a client-server system is composed of several components as shown in Fig. 1. These components closely reflect the various services such as a client downloads confidential information from the server, update and then store theses information to the server. Additionally, a component is usually implemented as a client-server application that employs a request-reply protocol. Client-server architecture facilitates secure access for multiple authorized users. These applications may be provided by different vendors [8].

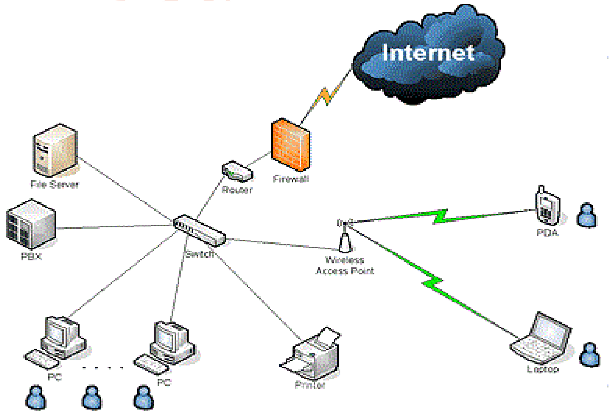

Fig.1 Client-Server network system

V. ATTACK TREE

An attack tree is a conceptual tree that represents possible attacks on a system. Developing the tree provides a systematic methodology to enumerate possible attacks on a given system, and captures interdependencies between these attacks. In this methodology, attacks are depicted as a tree structure where the root represents the goal of the attack, and the children nodes represent means to achieve this goal. The tree may be represented either graphically or in textual form.

In an attack tree, a node represents an attack that succeeds when the node's direct children are true. Specially, node's children form preconditions for the attack to happen. These preconditions (children) are combined using two logical operators: OR and AND. When combined with an OR operator, an attack succeeds if any of the preconditions is true. When combined with an AND operator, an attack succeeds if all of the preconditions are true ([1], [4], [6]).

VI. MODELING THE ATTACK TREE FOR PROPOSED NETWORK

Each tree has a root note that represents the attacker's goal, and the leaf nodes represent different paths to the root, each child node represents the steps an attacker can take. Modeling the attack tree involves associating a logical AND and a logical OR with each node ([1], [4]). In essence, a node of an attack tree can be decomposed into an AND or an OR node. An AND node or an OR node decomposition can be represented in graphical or textual formats. Both the AND and the OR decomposition can be represented in graphical or textual format as shown in (Fig. 2 and Fig. 3).

There are possible 128 scenarios help the user how to prepare and prevent their confidential information in Client-Server against form attackers according to (Fig. 2 and Fig. 3).

[GS11, GS21, GS31, GS41, GS51, GS61], [GS11, GS21, GS31, GS41, GS51, GS62], [GS11, GS21, GS31, GS41, GS52, GS61], [GS11, GS21, GS31, GS41, GS52, GS62], [GS11, GS21, GS31, GS42, GS51, GS61], [GS11, GS21, GS31, GS42, GS51, GS62], [GS11, GS21, GS31, GS42, GS52, GS61], [GS11, GS21, GS31, GS42, GS52, GS62], [GS11, GS21, GS32, GS41, GS51, GS61], [GS11, GS21, GS32, GS41, GS51, GS62], [GS11, GS21, GS32, GS41, GS52, GS61], [GS11, GS21, GS32, GS41, GS51, GS62], [GS11, GS21, GS32, GS42, GS51, GS61], [GS11, GS21, GS32, GS42, GS51, GS62], [GS11, GS21, GS32, GS42, GS52, GS61], [GS11, GS21, GS32, GS42, GS52, GS62], [GS11, GS21, GS331, GS332, GS41, GS51, GS61], [GS11, GS21, GS331, GS332, GS41, GS51, GS62], [GS11, GS21, GS331, GS332, GS41, GS52, GS61], [GS11, GS21, GS331, GS332, GS41, GS52, GS62], [GS11, GS21, GS331, GS332, GS42, GS51, GS61], [GS11, GS21, GS331, GS332, GS42, GS51, GS62], [GS11, GS21, GS331, GS332, GS42, GS52, GS61], [GS11, GS21, GS331, GS332, GS42, GS52, GS62], [GS11, GS22, GS31, GS41, GS51, GS61], [GS11, GS21, GS31, GS41, GS51, GS62], [GS11, GS22, GS31, GS41, GS52, GS61], [GS11, GS21, GS31, GS41, GS52, GS62], [GS11, GS22, GS31, GS42, GS51, GS61], [GS11, GS21, GS31, GS42, GS51, GS62], [GS11, GS22, GS31, GS42, GS52, GS61], [GS11, GS21, GS31, GS42, GS52, GS62], [GS11, GS22, GS32, GS41, GS51, GS61], [GS11, GS21, GS32, GS41, GS51, GS62], [GS11, GS22, GS32, GS41, GS52, GS61], [GS11, GS21, GS32, GS41, GS51, GS62], [GS11, GS22, GS32, GS42, GS51, GS61], [GS11, GS21, GS32, GS42, GS51, GS62], [GS11, GS22, GS32, GS42, GS52, GS61], [GS11, GS21, GS32, GS42, GS52, GS62], [GS11, GS22, GS331, GS332, GS41, GS51, GS61], [GS11, GS21, GS331, GS332, GS41, GS51, GS62], [GS11, GS22, GS331, GS332, GS41, GS52, GS61], [GS11, GS21, GS331, GS332, GS41, GS52, GS62], [GS11, GS22, GS331, GS332, GS42, GS51, GS61], [GS11, GS21, GS331, GS332, GS42, GS51, GS62], [GS11, GS22, GS331, GS332, GS42, GS52, GS61], [GS11, GS21, GS331, GS332, GS42, GS52, GS62], [GS121, GS122, GS21, GS31, GS41, GS51, GS61], [GS121, GS122, GS21, GS31, GS41, GS51, GS62], [GS121, GS122, GS21, GS31, GS41, GS52, GS61], [GS121, GS122, GS21, GS31, GS41, GS52, GS62], [GS121, GS122, GS21, GS31, GS42, GS51, GS61], [GS121, GS122, GS21, GS31, GS42, GS51, GS62], [GS121, GS122, GS21, GS31, GS42, GS52, GS61], [GS121, GS122, GS21, GS31, GS42, GS52, GS62], [GS121, GS122, GS21, GS32, GS41, GS51, GS61], [GS121, GS122, GS21, GS32, GS41, GS51, GS62], [GS121, GS1221, GS21, GS32, GS41, GS52, GS61], [GS121, GS122, GS21, GS32, GS41, GS51, GS62], [GS121, GS122, GS21, GS32, GS42, GS51, GS61], [GS121, GS122, GS21, GS32, GS42, GS51, GS62], [GS121, GS122, GS21, GS32, GS42, GS52, GS61], [GS121, GS122, GS21, GS32, GS42, GS52, GS62], [GS121, GS122, GS21, GS331, GS332, GS41, GS51, GS61], [GS121, GS122, GS21, GS331, GS332, GS41, GS51, GS62], [GS121, GS122, GS21, GS331, GS332, GS41, GS52, GS61], [GS121, GS122, GS21, GS331, GS332, GS41, GS52, GS62], [GS121, GS122, GS21, GS331, GS332, GS42, GS51, GS61], [GS121, GS122, GS21, GS331, GS332, GS42, GS51, GS62], [GS121, GS122, GS21, GS331, GS332, GS42, GS52, GS61], [GS121, GS122, GS21, GS331, GS332, GS42, GS52, GS62], [GS121, GS122, GS22, GS31, GS41, GS51, GS61], [GS121, GS122, GS21, GS31, GS41, GS51, GS62], [GS121, GS122, GS22, GS31, GS41, GS52, GS61], [GS121, GS122, GS21, GS31, GS41, GS52, GS62], [GS121, GS122, GS22, GS31, GS42, GS51, GS61], [GS121, GS122, GS21, GS31, GS42, GS51, GS62], [GS121, GS122, GS22, GS31, GS42, GS52, GS61], [GS121, GS122, GS21, GS31, GS42, GS52, GS62], [GS121, GS122, GS22, GS32, GS41, GS51, GS61], [GS121, GS122, GS21, GS32, GS41, GS51, GS62], [GS121, GS122, GS22, GS32, GS41, GS52, GS61], [GS121, GS122, GS21, GS32, GS41, GS51, GS62], [GS121, GS122, GS22, GS32, GS42, GS51, GS61], [GS121, GS122, GS21, GS32, GS42, GS51, GS62],[GS121, GS122, GS22, GS32, GS42, GS52, GS61], [GS121, GS122, GS21, GS32, GS42, GS52, GS62], [GS121, GS122, GS22, GS331, GS332, GS41, GS51, GS61], [GS121, GS122, GS21, GS331, GS332, GS41, GS51, GS62], [GS121, GS122, GS22, GS331, GS332, GS41, GS52, GS61], [GS121, GS122, GS21, GS331, GS332, GS41, GS52, GS62], [GS121, GS122, GS22, GS331, GS332, GS42, GS51, GS61], [GS121, GS122, GS21, GS331, GS332, GS42, GS51, GS62], [GS121, GS122, GS22, GS331, GS332, GS42, GS52, GS61], [GS121, GS122, GS21, GS331, GS332, GS42, GS52, GS62],

[GC1, GC2, GC31, GC41, GC5, GC6, GC71], [GC1, GC2, GC31, GC41, GC5, GC6, GC72], [GC1, GC2, GC31, GC42, GC5, GC6, GC71], [GC1, GC2, GC31, GC42, GC5, GC6, GC72], [GC1, GC2, GC31, GC431, GC432, GC5, GC6, GC71], [GC1, GC2, GC31, GC431, GC432, GC5, GC6, GC72], [GC1, GC2, GC32, GC41, GC5, GC6, GC71], [GC1, GC2, GC31, GC41, GC5, GC6, GC72], [GC1, GC2, GC32, GC42, GC5, GC6, GC71], [GC1, GC2, GC31, GC42, GC5, GC6, GC72], [GC1, GC2, GC32, GC431, GC432, GC5, GC6, GC71], [GC1, GC2, GC31, GC431, GC432, GC5, GC6, GC72], [GC1, GC2, GC33, GC41, GC5, GC6, GC71], [GC1, GC2, GC31, GC41, GC5, GC6, GC72], [GC1, GC2, GC33, GC42, GC5, GC6, GC71], [GC1, GC2, GC31, GC42, GC5, GC6, GC72], [GC1, GC2, GC33, GC431, GC432, GC5, GC6, GC71], [GC1, GC2, GC31, GC431, GC432, GC5, GC6, GC72], [GC1, GC2, GC34, GC41, GC5, GC6, GC71], [GC1, GC2, GC31, GC41, GC5, GC6, GC72], [GC1, GC2, GC34, GC42, GC5, GC6, GC71], [GC1, GC2, GC31, GC42, GC5, GC6, GC72], [GC1, GC2, GC34, GC431, GC432, GC5, GC6, GC71], [GC1, GC2, GC31, GC431, GC432, GC5, GC6, GC72]

[GN11, GN12, GN21, GN31, GN41], [GN11, GN12, GN21, GN31, GN421, GN422], [GN11, GN12, GN21, GN32, GN41], [GN11, GN12, GN21, GN32, GN421, GN422], [GN11, GN12, GN22, GN31, GN41], [GN11, GN12, GN21, GN31, GN421, GN422], [GN11, GN12, GN22, GN32, GN41], [GN11, GN12, GN21, GN32, GN421, GN422]

A. Attacker goals

As a first step in developing the attack tree, we need to specify attacker goals. The main goal is to break and access confidential information in server, which is then divided into the following sub-goals:

- Compromise Client
- Compromise Server
- Compromise Network

An attacker most likely would target the visible components of the system; namely the client(s), the server(s) or the network.

The identified attacker goals are further elaborated resulting in the attack tree shown in Figure 1. The tree comprises 128 attacks where some are technical and some are not. For instance, performing man-in-the-middle attack requires technical knowledge, while social engineering does not. This demonstrates the flexibility of attack trees in representing different types of attacks. In some respect, the confidential information in Client-Server system is the main assets of the system. Technically, security means ensuring their confidentiality, integrity, and availability. These three key principles of information security are implicitly embedded in the proposed attack tree. For instance, compromising the network may result from either eavesdropping traffic, modifying or injecting traffic, or making the network unavailable. These network attacks correspond to breaching confidentiality, integrity, and availability respectively.

In this system, clients are probably the most visible parts of the system. They also play the key role of viewing, entering and modifying information. Also, as more clients download the confidential information in Server, and then update information and upload/store to Server. Sometimes clients forget to delete the updated information in their computers. Therefore, they are expected to be attacked the most. As listed in the attack tree, some attacks can be as simple as shoulder surfing. Considering all the attacks, compromising a server is probably the most serious attack. Damages to the system may include exposing, altering and/or destroying confidential information. From an attacker viewpoint, however, it is probably the most rewarding attack. In particular, gaining a remote access grants a complete control of the entire system. Compromising the network is yet another attractive goal. Two factors are helping in this regard. One is the vulnerability of wireless technologies. The second is share data among clients' machines. Both factors give an attacker more chances to attempt eavesdropping, modifying or injecting confidential information ([2], [3], [6]).

B. Protecting Confidential Information

Viruses infect and damage unsuspecting computers, so it is vital to take preventive steps. To avoid virus infection, needed to do following:

- Develop a virus protection plan
- Identify the entry points for virus
- Specify responsibilities and authority
- Describe the installation and use of antivirus tools
- Install antivirus and data integrity software
- Scan ,update and upgrade automatically
- Backup your data regularly
- Consider every disk, program and email attachment as a threat
- Use caution when download files from the internet
- Be aware of virus hoaxes
- Educate users

C. Attack Tree Refinement

As shown in the flow chart of Fig. 4, an attack tree can be refined from the root node compromise as a combination of manual extensions and pattern applications. Manual extensions depend greatly on the security expertise of the person developing the attack tree. Pattern application also depends on such expertise, but to a lesser extent. Some of this security expertise is built into an attack pattern library. Henceforth, we assume such a library already exists.

A good attack pattern library provides a set of attack profiles that are rich enough to characterize the attacks that may take place on a broad range of enterprise architectures. Refining a particular enterprise's attack tree involves first finding those attack profiles that are consistent with the enterprise architecture. The developer searches the attack patterns of consistent attack profiles for a refinement of an attack path contained in the enterprise attack tree. Once found, the developer can appropriately instantiate and apply the attack pattern to extend the enterprise attack tree. This process of pattern application intermixed with manual extension continues until the attack tree is sufficiently refined.

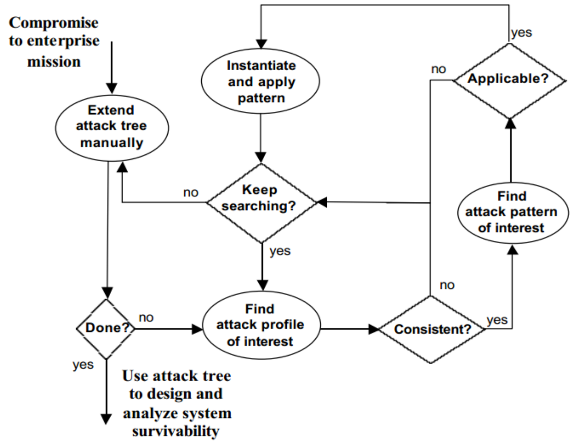
Compromise to enterprise mission
Extend attack tree manually
Instantiate and apply pattern
no
Applicable?
yes
Keep searching?
no
yes
Find attack pattern of interest
Done?
no
yes
Find attack profile of interest
Consistent?
no
yes
Use attack tree to design and analyze system survivability

Fig.4 Attack tree refinement process

VII. CONCLUSION

Every business company needs assurance that their confidential data and information are protected from current and future attacks. Additionally, the promising benefits of adopting the client-server systems will be greatly affected should their security is compromised. A tool like attack tree can prove effective in enumerating such attacks (technical or non-technical). It can be used to account for different types of attacks that threaten complex systems such client-server systems. Early attacks analysis would help in planning for countermeasures, and would greatly reduce the impacts of these attacks.

References

[1] Amenaza Technologies Limited, *Creating Secure Systems through Attack Tree Modeling*, 10 June 2003

[2] Andrew P. Moore, Robert J. Ellison,Richard C. Linger, *Attack Modeling for Information Security and Survivability*, March 2001

[3] Arpan Roy,Dong Seong Kim,*Cyber Security Analysis using Attack Countermeasure Trees.*

[4] BRUCE SCHNIER, *Attack Tree*, 8 October 1999

[5] Eric J. Byres, *The Use of Attack Trees in Assessing Vulnerabilities in SCADA Systems*, Group for Advanced Information Technology, British Columbia Institute of Technology.

[6] Schneier, B., *Attack Trees: Modeling Security Threats*, Dr.Dobb's Journal, December 1999.

[7] http://en.wikipedia.org/wiki/Computer_virus

[8] http://www.functionx.com/networking/Lesson06.htm

```
GOAL: (G0) Gain Confidential Information in Client-Server
OR GS0.Compromise Server
        OR GS1.Grain remote access
                GS11.Use default user name/password
                AND GS12.Use exploit
                GS121.Find open port
                GS122.Identify working exploit
        OR GS2.Gain local access
                GS21.Gain physical access
                GS22.Obtain administrator username/password
        OR GS3.Make Server slow or unavailable
                GS31.Flood with traffic
                GS32.Flood with requeset
                AND GS33.Destroy or steal server
                        GS331.Gain physical access
                        GS332.Use suitable tool
        OR GS4.Determine Server's Firewall access control
                GS41.Search for specific default listing ports
                GS42.Scan ports broadly for any listening ports
        OR GS5.Identifing Server's OS and type
                GS51.Scan OS services banners for OS characteristic information
                GS52.Probe TCP/IP stack for OS characteristic information
        OR GS6.Exploit store's server vulnerabilities
                GS61.Acces confidential information in database directly
                GS62.Access confidential information in database breaking the
password OR GC0.Compromise Client
        OR GC1.Shoulder surfing
        OR GC2.Use unattended logged-on client
        OR GC3.Obtain administrator username/password
                GC31.Social engineering
                GC32.Network interception
                GC33.Key-logging
                GC34.Phishing emails
        OR GC4.Infect with malware
                GC41.Deliver malware through Email. attachment
                GC42.Lure into visiting a malicious website
                AND GC43.Run infected programs
                        GC431.Gain local access
                        GC432.Obtain valid username/password
        OR GC5.Steal Client if portable
        OR GC6.Destroy Client
        OR GC7.Exploit Client vulnerabilities
                GC71.Access share confidential resource directly
                GC72.Share access confidential resource from privileged account
OR GN0.Compromise Network
        AND GN1.Eaverdrop traffic
                GN11.Capture packets
                GN12.Decode traffic
        OR GN2.Modify or inject traffic
                GN21.Perform man-in-middle attack
                GN22.Perform replay attack
        OR GN3.Make network unavailable
                GN31.Cut network cables
                GN32.Destroy wireless access points
        OR GN4.Get network address
                GN41.Directly access via Ethernet
                OR GN42.Access via wireless channel
                        GN421.Directly access by open channel
                        GN422. Break WEP password using BruceForce Technique
```

Fig. 2 Textual description for Client-Server attack tree

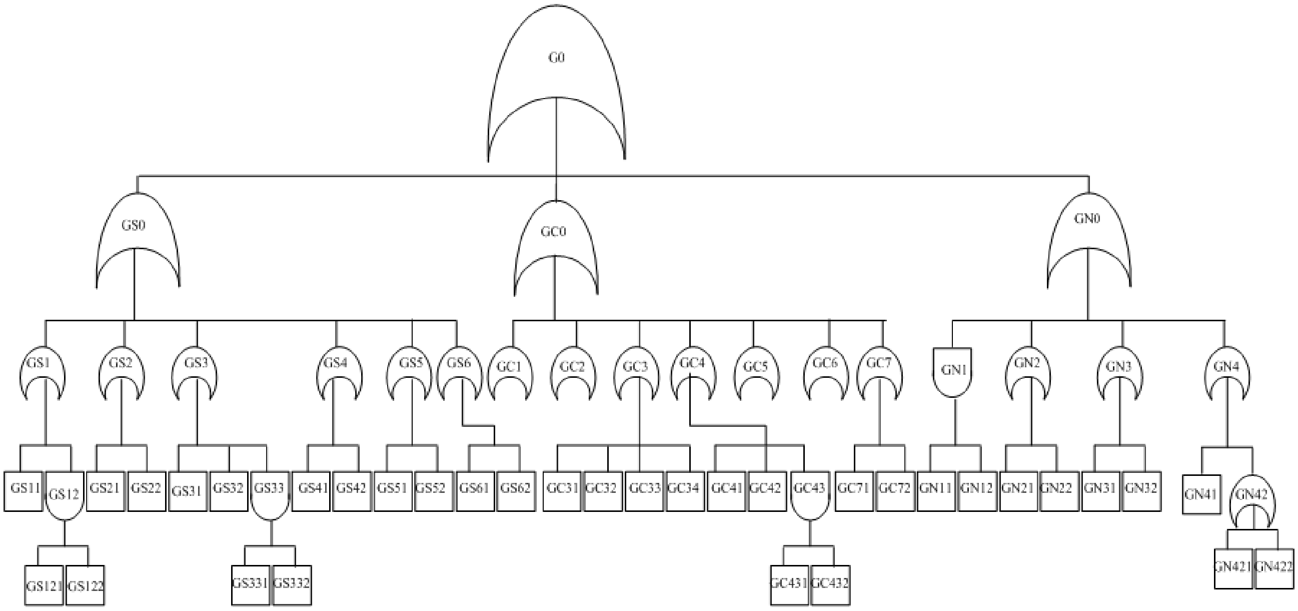

Fig.3 Graphical representation of an attack tree described in Fig.2