Secure Network Communication Using Vulnerability Assessment Technique

Preethi.S Vinodhini.T

***Abstract*-Vulnerability assessment has become an area of interest in distributed network communication which is capable of detecting the penetrations, break-ins and other form of computer abuse. The communication between a team and Management Information Base (MIB) within an organization which is out of the scope of firewall authentication can be made possible with the help of this system. In this paper, we propose an intrusion detection mechanism which is capable of detecting heterogeneous wireless sensor network (WSN) by characterizing intrusion detection with respect to the network parameters (Destination IP). The intention of this system is to reduce susceptibility using vulnerability assessment algorithm which covers the process of identifying and ranking the vulnerabilities in a system while ensuring required information is transferred securely without any failure in the middle of transaction. The three basic ideas involved are Furtive enigma, Destination IP address and Unlock key. It mainly focuses on system security by detecting the intruders and their system can be crashed by displaying a gray screen on it by comparing the IP address with the available IP address list.**

***Index Terms*- vulnerability assessment algorithm, Management Information Base (MIB), Wireless Sensor Network (WSN), Internet Protocol (IP), Furtive Enigma.**

I. INTRODUCTION

The vulnerability assessment considers the potential impact of loss from a successful attack as well as the vulnerability of the facility/location to an attack. Impact of loss is the degree to which the mission of the agency is impaired by a successful attack from the given threat. A key component of the vulnerability assessment is properly defining the ratings for impact of loss and vulnerability. Threats and vulnerabilities to a transit system cover a wide array of events, virtually none of which can be totally eliminated while still operating the system. Since no system can be rendered totally secure, once threats and vulnerabilities are identified, their impact on the total system must be assessed to determine whether to accept the risk of a particular danger, and the extent to which corrective measures can eliminate or reduce its severity. Threats entering the organization from outside could be easily identified using some security mechanisms which already present example: firewall

Once threats and vulnerabilities have been systematically identified, they should be assessed to determine their impact on the entire system. This helps the system decide whether to accept the vulnerability, or to implement corrective measures to bring the vulnerability to an acceptable level. Proper threat and vulnerability identification should include security testing and inspections, which are geared to promoting and ensuring that equipment is operating properly, is readily available when needed, and that employees are proficient in the use of the equipment. To accomplish this, systems must design a testing program that not only assesses the current state of security, but can also be used to upgrade staff effectiveness through training.

The development of recognition technology of system threats is fundamentally important for securing the distributed computing systems. However, existing intrusion detection systems (IDSs) are inefficient in coping with real-time online detections, especially to new attacks without prior knowledge/profiles. Some of the intrusion detection systems which proposed earlier were inspired by Human Immune System (HIS) that could be self-adaptable to the threats which occur continuously or rewritable with the help of agent based corrective mechanism. Since it is not practical to completely prevent potential computer attacks, we expect intrusion detection systems (IDSs) to minimize the hazards caused by various attackers. Research on IDSs is generally classified into three categories: (i) statistical features-based approaches, correlation analysis, signal processing techniques (ii) AI, rule-based system and agent based systems and (iii) data mining-based approaches. Different methods have different strength and weakness, and the selection of different methods is dependent on specific tasks. To protect computer users from malicious intrusions, Intrusion Detection Systems are designed to monitor network traffic and computer activities and to raise intrusion alerts to network administrators or security officers. IDS can be categorized into host-based Intrusion Detection Systems or network-based Intrusion Detection Systems according to their targets and into signature based IDS or anomaly-based IDS according to their detection methodologies.

The proposed system indented to provide security for each system under surveillance and to protect them from internal intruders who may present within the organization. Destination Internet Protocol (IP) address is the main string to identify intruder (who are not authorized to view information about the particular team's project) since no system can change its Internet Protocol (IP) address assigned for it in an organizational environment.

Manuscript received March 9, 2014

Preethi.S , Computer Science, Sri Sairam Engineering College, Chennai, India, Mobile no.8012115375, (e-mail:preethisg11@gmail.com).
Vinodhini.T , Computer science,Sri Sairam Engineering College,Chennai, India, Mobile no. 9941897307, (e-mail: vinodhini033@gmail.com)

Intrusion detection systems (IDSs) and intrusion prevention systems (IPSs) Are designed to counter this type of hacker threat. In addition to using such systems, organizations can consider restricting remote logons to specific IP addresses and/or use virtual private network technology. One of the results of the growing awareness of the intruder problem has been the establishment of a number of computer emergency response teams (CERTs).These cooperative ventures collect information about system vulnerabilities and disseminate it to systems managers. Hackers also routinely read CERT reports. Thus, it is important for system administrators to quickly insert all software patches to discovered vulnerabilities. Unfortunately, given the complexity of many IT systems, and the rate at which patches are released, this is increasingly difficult to achieve without automated updating. Even then, there are problems caused by incompatibilities resulting from the updated software. Hence the need for multiple layers of defense in managing security threats to IT systems.

In the computer security context, a hacker is someone who seeks and exploits weaknesses in a computer system or computer network. Hackers may be motivated by a multitude of reasons, such as profit, protest, or challenge. The subculture that has evolved around hackers is often referred to as the computer underground and is now a known community While other uses of the word hacker exist that are not related to computer security, such as referring to someone with an advanced understanding of computers and computer networks, they are rarely used in mainstream context. They are subject to the long standing hacker definition controversy about the true meaning of the term hacker. In this controversy, the term hacker is reclaimed by computer programmers who argue that someone breaking into computers is better called a cracker, not making a difference between computer criminals (black hats) and computer security experts (white hats). Some white hat hackers claim that they also deserve the title hacker, and that only black hats should be called crackers.

The model is based on the hypothesis that security violations can be detected by monitoring a system's audit records for abnormal patterns of system usage. The model includes profiles for representing the behavior of subjects with respect to objects in terms of metrics and statistical models, and rules for acquiring knowledge about this behavior from audit records and for detecting anomalous behavior. The model is independent of any particular system, application environment, system vulnerability, or type of intrusion, thereby providing a framework for a general-purpose intrusion-detection expert system. We describes a model for a real-time intrusion-detection expert system that aims to detect a wide range of security violations ranging from attempted break-ins by outsiders to system penetrations and abuses by insiders.

The development of a real-time intrusion detection system is motivated by four factors: (1) most existing systems have security flaws that render them susceptible to intrusions, penetrations, and other forms of abuse; finding and fixing all these deficiencies is not feasible for technical and economic reasons; (2) existing systems with known flaws are not easily replaced by systems that are more secure -- mainly because the systems have attractive features that are missing in the more-secure systems, or else they cannot be replaced for economic reasons; (3) developing systems that are absolutely secure is extremely difficult, if not generally impossible; and (4) even the most secure systems are vulnerable to abuses by insiders who misuse their privileges.

We assess the internal correlations of vulnerability, autonomy and adaptability in the communication system. The proposed immunology initiated multiple layer thread awareness system proves to be useful in risk assessment and vulnerability analysis. The vulnerability bound is employed as a reference result that builds up a bridge between deterministic information and uncertainties in the complex system environment.

II. TERMINOLOGIES

FURTIVE ENIGMA

Enigma is a secret word which could be used as an authentication key to get information from the Management Information Base (MIB).client or liquidator will get the word through e-mail which is sent by the MIB which will be generated for each user request.

MANAGEMENT INFORMATION BASE (MIB)

Management Information Base (MIB) provides naming service to the managed elements. By providing managers with the interfaces of the managed devices, managers can maintain or monitor the requested management information through the instantiation of Simple Network Management Protocol agent operations and RMON (remote monitoring) protocols .MIB provides an interface between the identification of hardware level devices and software-enabled maintenance.

DESTINATION INTERNET PROTOCOL (IP)

Internet Protocol (IP) is the main string for identifying the intruder from entering the network. Client who entering the network will be compared with the allowable Internet Protocol (IP) address. When the IP address is same information will be transferred to the liquidator. If the IP address is not the same intruder will be warned three times.

UNLOCK KEY

Unlock key should be entered by the authorized liquidator so that required file will be transferred .The unlock key will be sent to client if the client is a valid user.

III. ARCHITECTURE DIAGRAM

A simple example of MIB tree is depicted as follows. MIBs usually have three branches: ISO, user profiles, and vendor profiles. The unique OIDs of MIBs are applied to provide a naming service for each managed object, or MIB object. The MIB is constructed in a hierarchical tree structure. The top level of the tree structure is controlled by ISO and ITU organization. Fig. 1 is an example of a MIB tree structure and naming scheme, and the dotted line represents those subentries that can be added on afterwards in compliance with the new concepts in this paper. In the lower level of this structure, the sub-entries can be altered to cope with new usage. It is feasible to add up more sub-entries in the current MIB structure. These subentries with more attributes and embedded methods and algorithms can be added below (object identifier) OID=1.3.6.1.2.1.In some circumstances, more subentries can be embedded into private enterprise network OID=1.3.6.1.4.1.

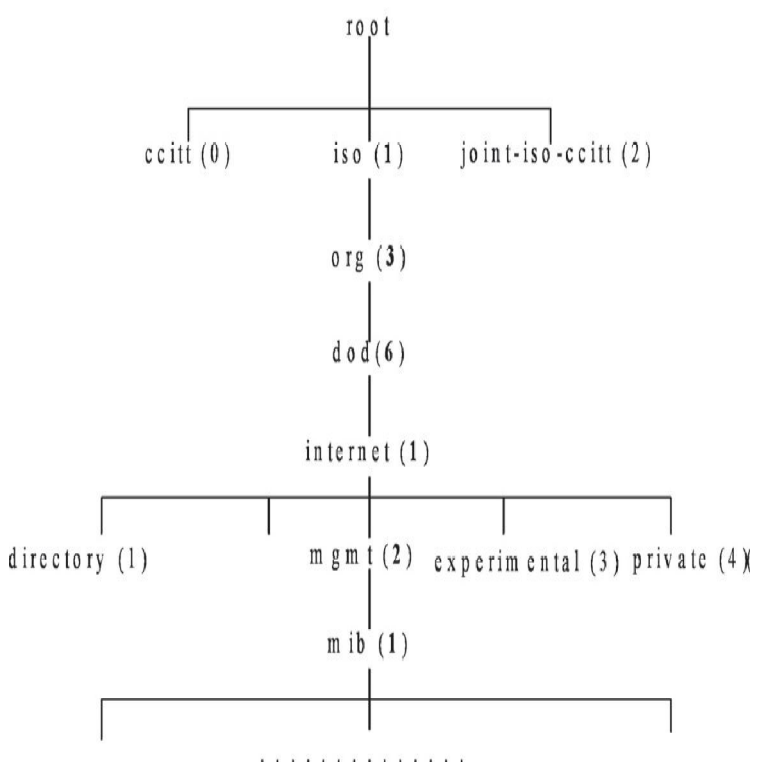


Fig. 1. The functional domain of MIB tree structure

PROCESS INVOLVED IN VULNERABILITY ASSESSMENT

The liquidator is a person who is working in a project for the organization .Management Information Base monitors all the peers connected to it including the intruders who are all present in the organization .The liquidator request for the particular information from the MIB ,it then respose with the secret keyword(furtive enigma) and the liquidator authorise it's connection by sending back the word to the MIB.The management information base then check the IP address of the liquidator by comparing with the available IP address present in the database. Attackers can come from anywhere, so organizations need to quickly mitigate vulnerabilities before they become threats. They need a quick, easy, effective solution for creating security policies. Although it's preferable to have multiple scanners or scanning services, many companies only have one, which significantly impedes their ability to get a full vulnerability assessment. Intruder is the one who will always steals the information from the MIB and they can be detected by their IP address .

The furtive enigma genarated at every time when a particular request is received by the MIB.For every client furtine enigma will be unique which ensures security for the information in the system. Once the liquidator got authorised from the MIB ,it again sends the unlock key to the liquidator through which they can get the access to the data available in it.If a intruder enters into the network they may steal the secret word but,end up in a warning given by MIB by the comparison of the IP address .If still the intruder want to get the access after three times of warning MIB crashes their syatem by displaying a grey screen on their system.

VULNERABILITY ASSESSMENT:

Vulnerability assessment covers the processes of identifying,

Quantifying, and ranking the vulnerabilities in a system. It includes the identifications of the vulnerabilities or potential threats to each party and giving the classified ranking value and therefore acquire the importance to those resources or parties. In most occasions, it also includes the mitigation Or elimination of the most serious vulnerabilities.VA is not determining the exact attacks categories, but rather to identify the potential threats or system flaws that might be exploited. The main functions for VA are focused on (i) Seeking the *right* timing to activate compact security mechanisms while maintaining performance, minimizing the use of the system resources and operational cost, etc. (ii) Seeking the safety bound as the minimum vulnerability bottom line under which the system cannot maintain efficient autonomy anymore.

The vulnerability assessment will be driven by the set of threats and hazards that could affect the facility. Threats refer to malicious insults including both cyber and physical attack or sabotage. Hazards refer to natural disasters or normal accidents that may occur on a random basis. The likelihood and severity of stress should be identified for each type of insults deemed worthy of attention. A computer attack might occur on a daily basis (likelihood) and affect 10 computers (severity). Based on similar facilities experience, arson may occur once every five years (likelihood) and incapacitate the entire facility (severity). Threats and hazards that have occurred in the past should be on the list.

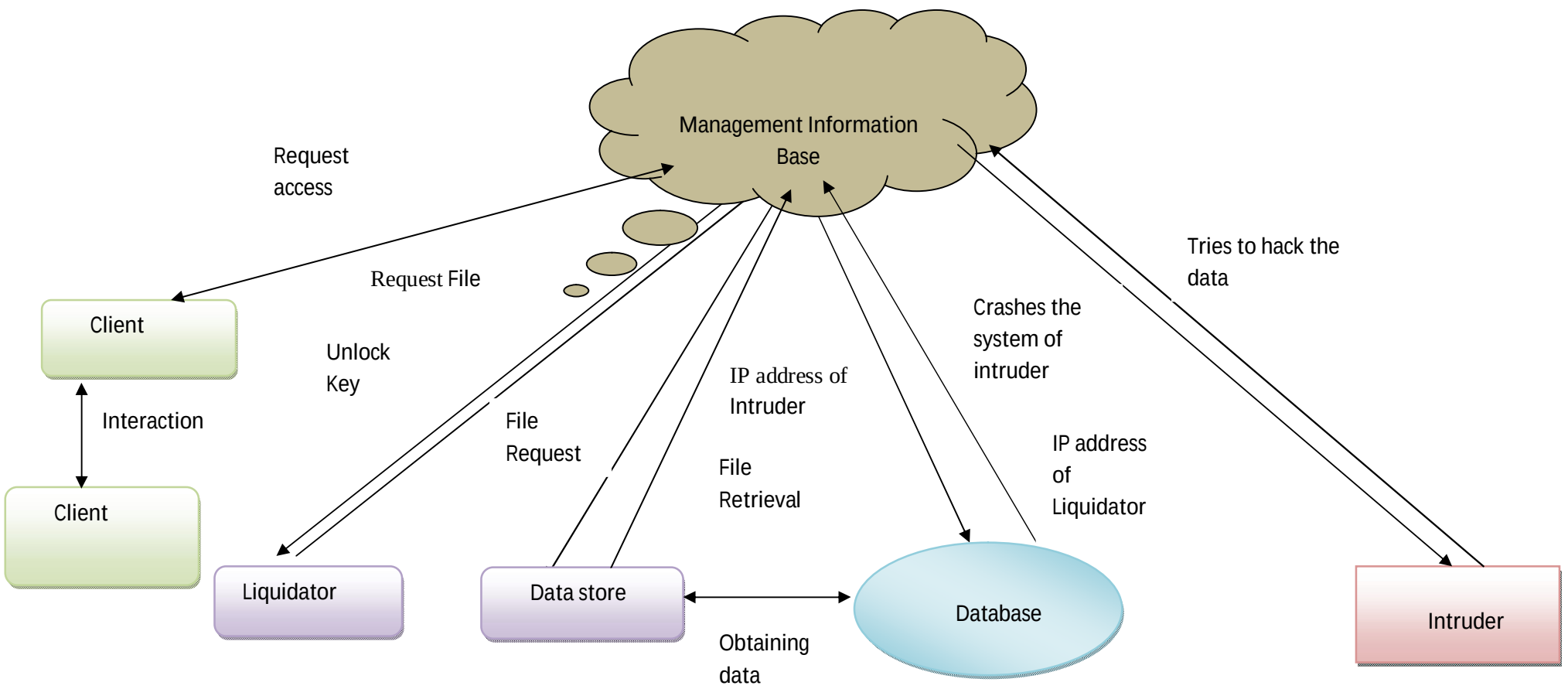
The vulnerability assessment process considers threats that have the potential individually or collectively to affect one or more mission critical systems. Determining which systems will be affected by which threat is obvious in some cases. In other cases it may be necessary to compare the stress levels engendered by the threats/hazards identified with the strengths of exposed system. Once a mission critical system is determined to be vulnerable, trace cascading failures by determining if other dependent systems may cease to function as a result of the initial system's failure.

OBJECTIVES:

The vulnerability assessment process has the following objectives:

1. Understand the facility/organization's mission and mission- supporting systems and functions
2. Identify mission-threatening vulnerabilities of critical facility systems.
3. Understand system design and operation in order to determine failure modes and likelihoods.
4. If possible, identify consequences of system failures in terms of down time, effects on people, and any cascading effects on other systems and organizations.
5. Recommend facility improvements to reduce vulnerability.

III . PROCESS ARCHITECTURE DIAGRAM



IV. ALGORITHM

1. Input: IP address
2. Output: requested file or crash the intruder system
3. Liquidator request for connection
4. MIB generates furtive enigma
5. For each request generate secret word do
6. Send secret word to liquidator through e-mail
7. End
8. Do
9. MIB monitors all connected peers
10. If(Liquidator IP == allowable IP)
11. Send unlock key to liquidator
12. Else
13. {
14. For(i=0;i<=3;i++)
15. Warning message
16. Crash the system by displaying a grey screen
17. }
18. If(liquidator unlock key = unlock key sent)
19. MIB response with a requested file
20. End

VI. MODULE DESCRIPTION

After careful analysis the system has been identified to have the following modules:

- Connection establishment.
- Flinging Furtive.
- Piecing Establishment.
- Guarding the bustle.
- Tidings Handover.

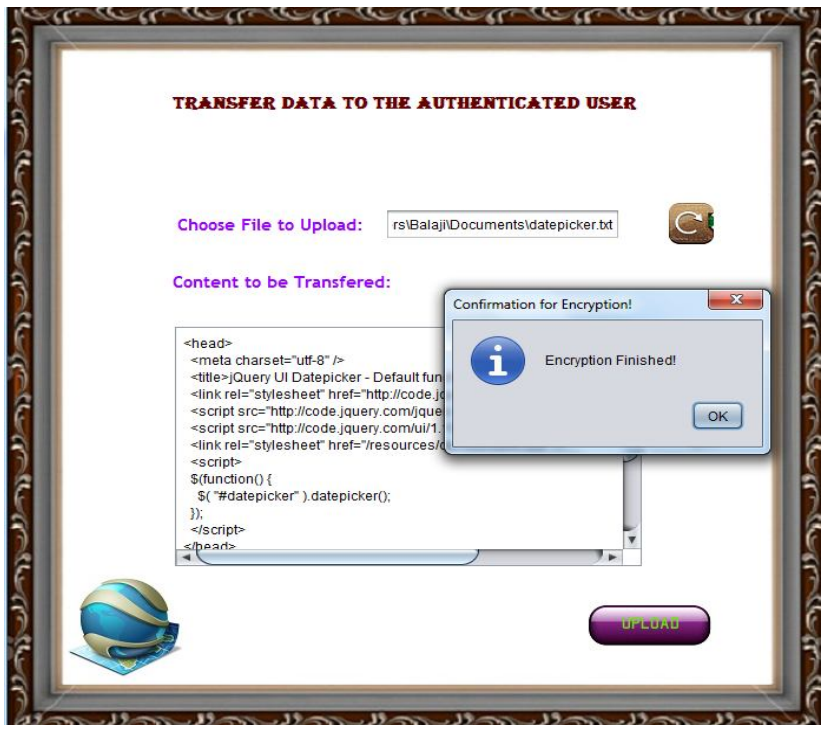
CONNECTION ESTABLISHMENT

Client-server computing is a distributed application architecture that partitions tasks between service providers and service requesters, called clients.Often clients and servers operate over a computer network on separate hardware. A server machine is a high-performance host that is running one or more server programs which share its resources with clients. A client also shares any of its resources; Clients therefore initiate communication sessions with servers which await Incoming requests.

Tie up all the active nodes in LAN. Once the correct destination router is found, an end-to-end peer connection (TCP or IP) is established to carry end-system. This connection remains active as long as the file requested transferred and it is dynamically shut down when not in use, permitting casual, any-to-any communication without the burden of specifying peer connections in advance. It also allows any-to-any routing in large internetworks in which persistent TCP connections between every pair of routers would not be possible.

FLINGING FURTIVE

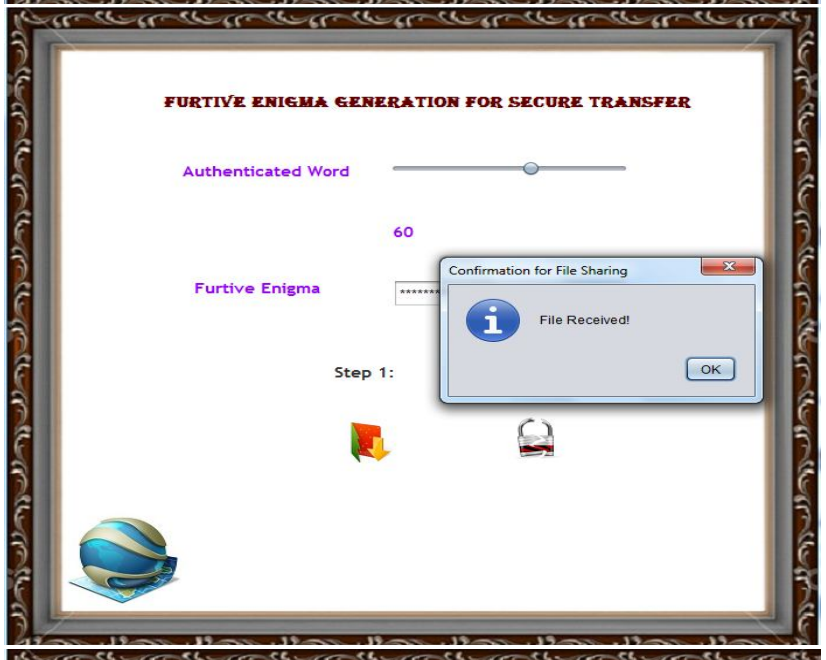
After Communication is established between the nodes the main process begins. The Main Server sends authenticated word and furtive enigma. The Furtive keywords are sending to the Liquidator. Occasionally the furtive keywords can be stealed by the Intruder to receive File Requested. Furtive Enigma can be used by the Intruder to hack details send by the Main Server.



PIECING ESTABLISHMENT

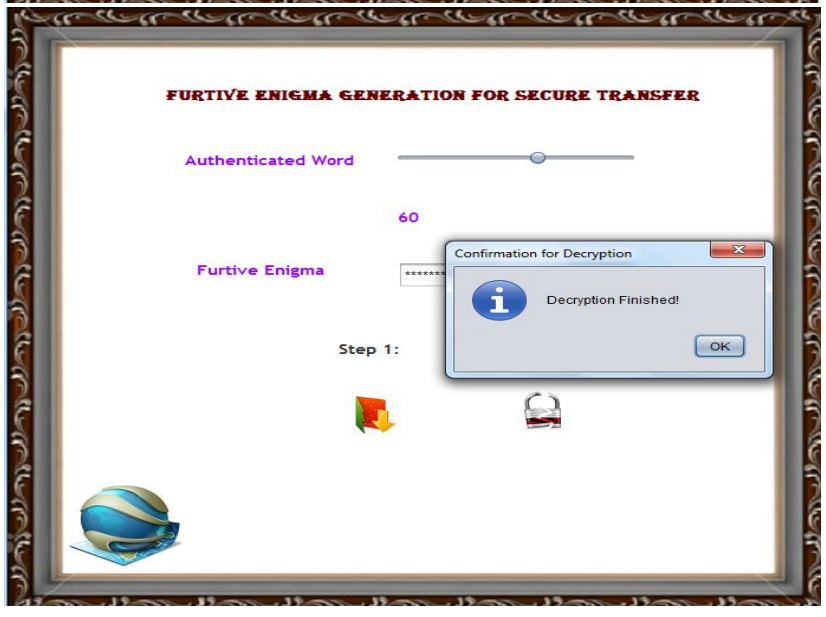
The number of connections to establish between each pair of nodes in a node network .Link is established between each and every nodes for network data communication.

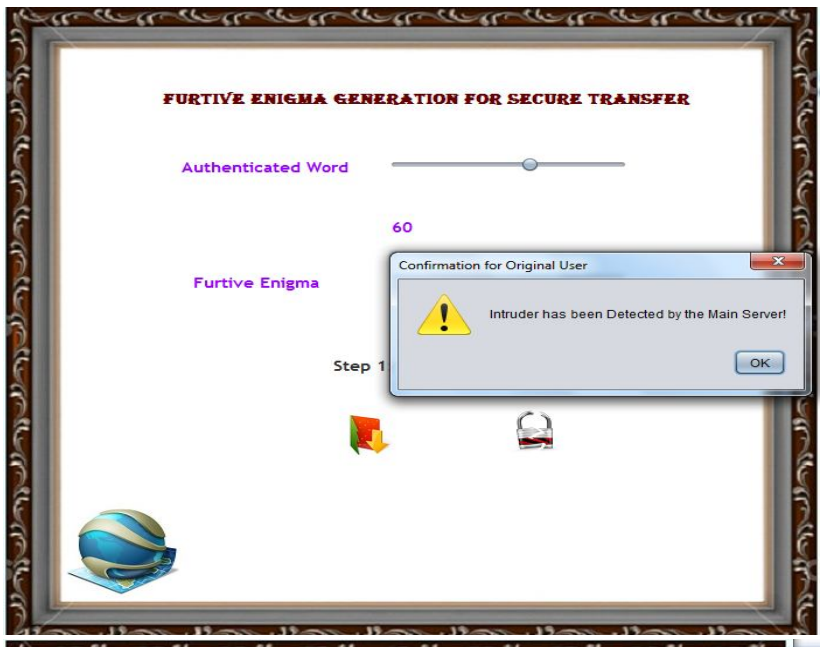
From the source node to the destination node and Intruder node must have connection between source nodes after communicate between combinations of multi node each and every node must be link to each other. In data transmission, send the file requested from source node to destination node.

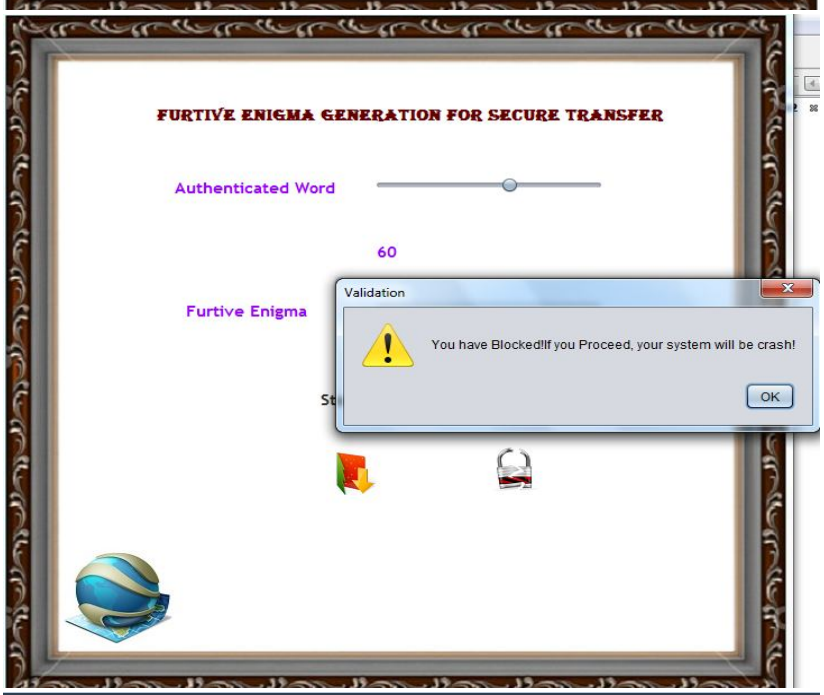


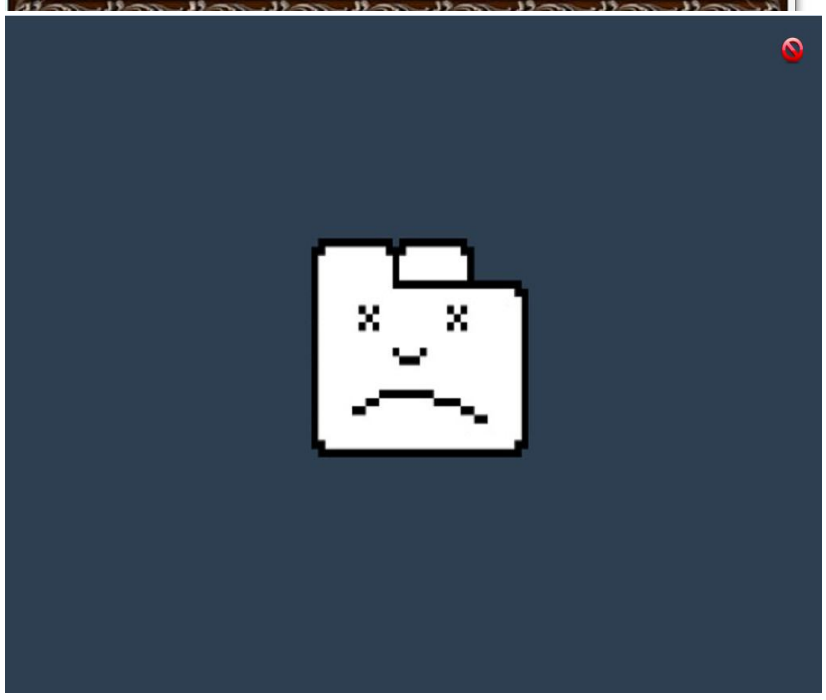
GUARDING THE BUSTLE

The Main Server will guard various bustle. The guarding process is to find out the intruder. Intruder will hack the details provided to the Sub server and he will try to hack the requested details also. After finding the intruder the main server will warn the intruder for 3 times. If also exists then he will make the intruder system to crash. Main Server has the authority to Crash the System.









TIDINGS HANDOVER

Main Server while monitoring finds the intruder and blocks it. He will find the authenticated user and sends the requested data to the sub server. Even the main server finds the authenticated sub server and if he enters the furtive keywords wrongly, the main server won't provide data to the sub server. If the furtive keywords entered are correct then only the tidings will be handover to the sub server.

VII. CONCLUSION

Statistics shows that system compromises are on the rise so we must guard against them using the methods available to us. Vulnerability assessment is a tool to ensure security in a distributed network. This paper covers the idea of identifying the intruder using vulnerability assessment algorithm and crashing their system.

VIII. REFERENCES

[1] C. J. Fung, J. Zhang, and R. Boothbay, "Effective acquaintance management based on Bayesian learning for distributed intrusion detection Networks ," *IEEE Trans. Network and Service Management*, vol. 9, no. 3, pp. 320–332, 2012.

[2] A. Sperotto, M. R. H. Mandjes, R. Sadre, *et al.*, "Autonomic parameter Tuning of anomaly-based IDSs: an SSH case study," *IEEE Trans. Network and Service Management*, vol. 9, no. 2, pp. 128–141, 2012.

[3] A. Lahmadi and O. Festor, "A framework for automated exploit prevention From known vulnerabilities in voice over IP services," *IEEE Trans. Network and Service Management*, vol. 9, no. 2, pp. 114–127, 2012.

[4] Y. Badr, F. Biennier, and S. Tata, "The integration of corporate security Strategies in collaborative business processes," *IEEE Trans. Services Computing vol*. 4, no. 3, pp. 243–254, 2011.

[5] F. Jiang, "Towards a secure and robust context-aware service-oriented Management: a vulnerability assessment approach," to appear, *ACM Transactions on Information and System Security*, 2012.