International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 5 Issue 05, May-2016

Vulnerability Assessment of Clients in an E-Business Network using Hybrid Threat Assessment Algorithm

Okengwu U. A[1]
[1]Dept. of Computer Science,
University of Port Harcourt,
Port Harcourt, Nigeria

Eke B. O.[2]
[1]Dept. of Computer Science,
University of Port Harcourt,
Port Harcourt, Nigeria

***Abstract*—This Modern E-business network may be expected to be safe since the users are often business partners and organizations that may have been involved in genuine business offline. These networks are often vulnerable to attack by new organizations looking for business secrets and malicious ones who want to destroy trade relationships or steal money. This paper proposes a vulnerability assessment - Hybrid Threat Assessment Algorithm, for assessing client's nodes that connects to an e-business network. The assessment is done by carrying out threat degree verification on the client's vulnerability level using the Vulnerability Analyzer engine and the security policies of the e-business network. If the threat degree value of the client is low, full connection is given, if the threat degree value of the client is medium, the client is quarantined, but if the threat degree value of the client is high, the client is disconnected from the network. The node vulnerability assessment algorithm is also useful in the creation of trusted path which the e-business uses in transmitting critical business data.**

Keywords*— *Vulnerability, Assessment, Threat Degree, Analyzer Engine, Trusted network path

I. INTRODUCTION

Vulnerability assessment is a proactive and systematic strategy to discover a weakness or flaw in a system [1]. It is practiced to discover unknown problems in the Network system used by e-businesses. E-business is the combination of "modern information technology" and "business", to some extent. In modern time, various e-businesses are interconnected via the internet as well as other local or wide area network. These networks provide for the clients easy interaction, access to resources, business interactions and information dissemination. It also provides means of transmitting various business needs to all the points where solutions can be provided [2]. Some e-businesses rely heavily on the network for its day to day transaction creating a need for effective monitoring of the network to prevent intruders from causing problem on the network. The monitoring can be achieved by subjecting the clients to verification and quarantining the vulnerable clients before they are allowed access to the network. The quarantining of such vulnerable clients provide a measure of confidence to the clients connecting to the network and the e-business running on the network. Trust and confidence are very important factors for the sustenance and growth of any business. If the site or network used by a business is viewed as being unsafe the confidence of the clients will be destroyed leading to a collapse in the business.

The expansion of scale and scope of the market has created a trend for software project management to be complicated and short cycled [3], hence security of the network for an e-business is a critical part of managing e-business projects. Most e-businesses are interconnected with various other clients via the computer network. Wan [4] identify the risks of an e-business Group which is working at software outsourcing projects between Hong Kong and Guangdong and the causal relationships among the risk factors, and constructs corresponding risk structure model with ISM. Wan [5] examined the relationship between risk factors of implementation of the information technology service management (ITSM) project and e-business activities. They found out that risk due to system vulnerability abound and needed to be addressed to make the e-business system reliable and mitigate other risks such as project communication risk, risk of system design, and risk of project cooperation.

This paper proposes a Hybrid Threat Assessment Algorithm of Target-oriented Threat Assessment and Non-Target Oriented Threat Assessment algorithms. The Algorithm and its associated Vulnerability Analyzer Engine assesses clients in an e-business network environment with the goal of identifying those that poses risk and makes the system vulnerable to attack. It also creates a dynamic trusted path for routing critical e-business information in business network environment where new clients are often needed but are also major sources of attack on the network.

E-business network provide for the clients easy interaction, information dissemination and business interaction within the network. It also provides means of transmitting various business needs to all the points where solutions can be provided, some business rely heavily on the network for its day to day transaction. This heavy reliance creates a need for effective monitoring of the network to prevent intruders from causing problem on the network. This check is actually achieved by subjecting the clients to verification and identifying the vulnerable clients, before they are allowed access to the network. The identification of such vulnerable clients provides a measure of confidence to the clients connecting to the network and the e-business environment. Trust and confidence are very important factors for the sustenance and growth of any business. If the network is viewed as being unsafe the confidence will be destroyed leading to a collapse in the business.

Today, security is treated as custom work, built on patchwork systems that are inflexible, isolated, and hard to manage. Organisational groups focus on different aspects of security development, policies may differ across business unit, and implementations will vary widely. Organisations have struggled for decades to answer "How do you apply the right security solution to manage the business risks?". This research work offers one of such solutions at list in theory.

II. E-BUSINESS SECURITY VULNERABILITY

A. *E-Business Security*

E-business security is evolving from the old notion of turning the enterprise into an information fortress, to a new more comprehensive model of privacy and trusted e-business network. This privacy is usually compromised by programs with the ability to reproduce by modifying other programs to include a copy of itself-Virus.

Viruses and Worms from Melissa in 1999 to Netsky and MyDoom in 2004 have become a prevalent problem for internet users illustrated in short case study of lastminute.com [6]. In 2015, Sony website in USA was allegedly hacked by Chinese clients or Hackers posing as Clients which causes business raw between the two countries, damaging a measure of confidence. A recent report found that greater percent of Fortune 100 companies were infected by worms, spy wares and other malicious software[3].

This is significant because Fortune 100 companies are presumably well protected by firewalls, antivirus software, intrusion detection systems, and anti spyware managed by highly trained IT staff. After previous experience with the devastating Slammer and Blaster worms in 2003, organisations have learned to guard against new worm outbreaks. The inadequacy of current security is due to the difficulty of protecting the system by antivirus software and software patching only. New vulnerabilities in operating systems and applications are being continually discovered at an average rate of 48 percent. These vulnerabilities are rated as highly severe and 69 percent are considered easy to exploit. The need for frequent patching places a considerable strain on large organisations with many computer users. In addition, many new windows viruses and worms are being discovered almost every week on average. Antivirus software signatures require constant updating to detect new viruses and worms.

The ineffectiveness of firewalls after a network perimeter has been penetrated, creates many avenues to bypass perimeter defences, and for example a notebook brought into an organisation could carry malicious code [7]. It takes only a single infection within an organisation to effectively circumvent perimeter security.

B. *Vulnerability*

The word vulnerability is derived from the word vulnerable. Something is said to be vulnerable if it is weak and easily hurt physically [8]. It is the intersection of a system susceptibility or flaw, attacker access to the flaw, and attacker capability to exploit the flaw [9]. Network Systems are meant to share information with client, from e-business perspective, customers and partners; new customers are equally expected to connect to the network and share information with fellow customers. The policy of e-business network in an organization, is the yardstick for the measurement of level of strength or weakness of a connecting computer. Any computer that does not meet the required policy standard is generally referred to as being a vulnerable system.

Vulnerability also deals with the concept of network risk or loophole, the possibility of successful attacks from the weakness and the severity of losses. In other to assess vulnerability we will examine the threat of attack degree, the attack itself and the influence of the victim node characteristics as proposed by Zhihong [10].

The Threat of attack Degree (A_d) is a Two tuple (Ac,H) , Ac is Attack complexity, used to evaluate the difficulty degree of attack. H is attack harmfulness,

$$H = (Ae,Ca,Ni). \qquad (1)$$

Where, Ae is the effect of attack on the security network. Ca is correlation of attacking the nodes in the network. Ni is the network integrity related to access trust relationship between the host and the client. A remote user with valid credentials could connect to a network with a computer that does not have the following:

i. Correct service pack or latest security patches installed.
ii. Correct antivirus software and signature files installed
iii. Routing disabled. A remote access client computer with routing enabled, might pose a security risk, providing an opportunity for malicious user to access corporate network resources through the client computer, which has an authenticated connection to the private network.
iv. Firewall software installed and active on the internet interface.
v. A password –r with an adequate wait time.

Despite the efforts made, within the e-business organisations, to ensure that computers used internally, comply with network policy. Systems used by customers, partners and even from employee's homes for remote access can still present significant risk to the network [11].

C. *Vulnerable Client*

Client computers are the computers connected to the servers and depend on the servers for co-operative computing. They are single-user computers that provide user interface services and appropriate database and processing services as well as connectivity services to the servers [12]. Customer's nodes with weak system that can be easily hurt by virus, worms and hackers are said to be vulnerable networks or clients. They are clients whose Threat_of_attack Degree is significant.

However, when the clients are weak or do not meet the security policy they are vulnerable to the entire network; they can also be the source of the security breach. Distributed computing technology is evolving faster in the e-business environment than our ability to properly monitor it. System designers and security developers need to make intelligent decisions about examination and validation method for data, processes, and interfaces when designing network control applications. Since there are no generally accepted standard for network model in e-business system the main assessment will have to focus at the point of connection. It is this assessment that provides the condition for access control. Access to the network can then be arranged in the form that is similar to fuzzy logic system.

In this case a request for access to the network can receive the results NO-ACCESS, WAIT or YES- ACCESS. In the case of NO-ACCESS, access is denied, WAIT is what we can refer to as quarantine, YES-ACCESS is allowed full connection and communication to the network.

Others have ways of running their decision tree to save time and minimise the risk of overloading the target systems. There are many variations within these three phases, some will try to brute force passwords on accounts. Others assume a friendly environment and connect to servers with administrative access to look for problems at the system level. Some are more devious and will evade a network IDS [11]. In figure 1,

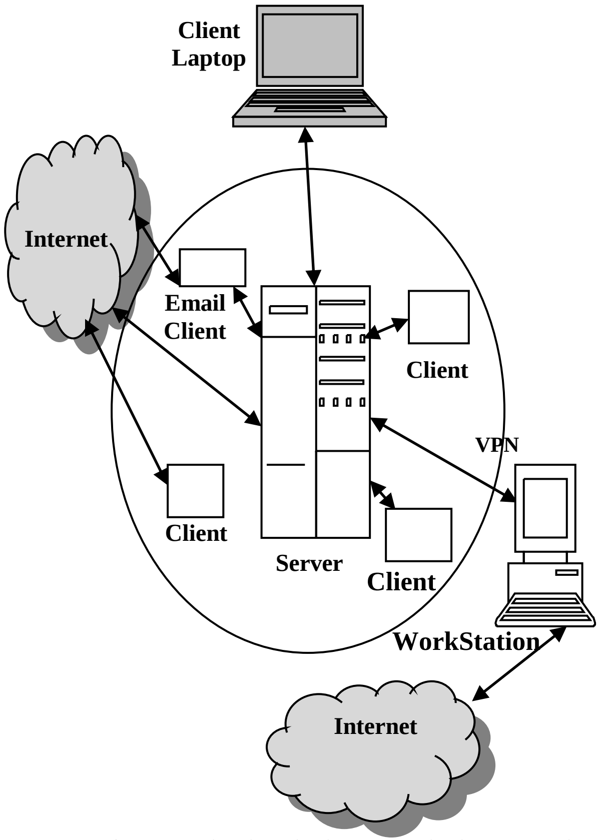

Fig. 1. Routes of worm or virus introduction to organization’s network

Client Laptop, Email Client, other Clients and WorkStation are connected to the organizational server via the LAN. The Email client, other Clients and the WorkStation are also connected to the Internet from were virus and worm can infiltrate into the network.

III. Vulnerability Assessment Using Hybrid Network Threat Degree System

In this paper we are proposing a hybrid network threat degree system for use in the assessment of network for vulnerability. The hybrid is from Target Oriented Threat degree system and Non-target Oriented Threat degree system.

1)Target Oriented Threat System: The target oriented threat degree system is developed using Dijkstra’s algorithm [13], which is the classical shortest path algorithm, used to calculate the shortest path from a single source to all other nodes. Its characteristics are suitable for target oriented threat degree assessment. But the application of Dijkstra algorithm in graph theory is only a single path based on node. Network vulnerability correlation is modelled by Petri net. The challenge with this algorithm is that the excitation transition place between nodes can be more than one, but the client attacker can adopt different attack methods to achieve the same objective on the same node, so there is a need for the Dijkstra algorithm to be improved which gives rise to the non-target oriented model.

The Dijkstra's algorithm uses a greedy approach with a trusted graph used to represent the map of the network. The idea is to know which path from source to destination is the trusted path. The node with the highest priority is selected as the trusted node to reach the destination. If two or more nodes have the same priority we will use Dijkstra's algorithm to decide the node to select. In other words the Dijkstra's algorithm identifies the more vulnerable nodes and less vulnerable nodes by following the priority assigned to each node in an effort to creating a trusted path.

Input: Weighted graph G= {E, V} and source vertex v∈V, such that all edge weights (priority values) are nonnegative.

Output: Lengths of the trusted paths themselves from a given source vertex v∈V to all other vertices. Dijkstra's algorithm psuedocode is shown below:

```
prior[s] ←0                (priority to source vertex is zero)
for  all v ∈ V–{s}
    do  prior[v] ←∞         (set all other prioritys to infinity)
S←∅                 (S, set of visited vertices is initially empty)
Q←V          (Q, the queue initially contains all vertices)
while Q ≠∅            (while the queue is not empty)
do   u ← minpriority(Q,prior)
                 (select the element of Q with the min. priority)
    S←S∪{u}                (add u to list of visited vertices)
    for all v ∈ neighbors[u]
        do  if   prior[v] > prior[u] + w(u, v)
                                  (if new trusted path found)
then   d[v] ←d[u] + w(u, v)  (set new value of trusted path)
                     (if desired, add traceback code)
return prior
```

In the target oriented threat assessment the most vulnerable nodes are target of attack and if the system use the trusted path it creates a network path less vulnerable to attack making the attack on nodes highly selective. But often attackers don't give a dime they are always ready to attack any node of their choice.

2)Non-target oriented Threat system: Non-target Oriented Threat system checks vulnerability for the network attack in which any node on the fragile state are likely to be the goal of the attacker, in this case, the network administrator needs to obtain threat value of each fragile state, in order to evaluate the nodes and the weak state threatened the largest in complete attack information network. The Non-target oriented Algorithm proposed by Zhihong [10] is shown below:

Algorithm: Non-target Oriented Threat Assessment
Input: Network Nodes
Output: Each node threat N_t or Vulnerability

```
Build three-dimensional array  C[n][n][v] stored change complexity of each  node in Network model. C[i][j][k] shows complexity of attack  $t_k$ from initial $P_i$ node to final node $P_j$.
Initialize: P is network library set,  S = { $p_o$ },  $N_0$ = 0 network library
For˜ (all $P_i \in$ P-S)
AT($P_i$) = max($\alpha$* (1-C[0][i][0]) + $\beta$ * H[0][i]…, $\alpha$* (1-C[0][i][k]) + $\beta$ * H[k][i])
Generated  tok($P_i$), tok($P_i$).AT = AT($P_i$).rout = $P_0$ ,$t_h$ ,$P_i$
For ( i = 0; i < n ;  i++ )                    .
$N_k$ = max {Tok(˜ $P_i$.AT | $\forall$ $P_i \in$ P-S)
f($N_k$ == 0 )
Break
S = S $\cup$ { $P_k$ }
For˜ (all $P_j \in$ P-S)
      For (h = 0; h < v; h++)
If (Tok($P_j$).AT < exp(-C[0][a][b] - C[a][c][d] - …- C[e][k][f]*(a*(1 - C[k][j][h]) + $\beta$ *H[h][j]))
Tok($P_j$).AT = $AT_k$
Tok($P_j$).rout = Tok($P_j$).rout + " $t_h$ , $P_j$" )
If ( Tok($P_j$).AT = $AT_k$ )
{Create a new token $Tok_{new}$($P_j$)
$Tok_{new}$($P_j$).AT = $AT_k$;   $Tok_{new}$($P_j$).rout = Tok($P_k$).rout + " $t_h$ , $P_j$" }
$N_k$ = Tok($P_j$).AT
For ( J = 1; J < N ; J++ )
For ( All $P_j \in O_j$ )
AT($O_j$ ) + = $N_k$
Output $N_k$, AT($O_j$ )
```

Non-target Oriented Threat Assessment (N O T A) algorithm [10] can obtain the optimal token *T o k p* in network, which records the corresponding threat degree value and path information of experience. This can be used instead of the priority assignment on the network nodes which can improve the lists of the vulnerability information on the nodes.

On the selected nodes where NOTA is used for the vulnerability information of the node the attack complexity will be very low. The path that will be created will be dynamic because the complexity of change on the nodes is the same. This is necessary since a malicious attacker can attack an intranet weak node and from there proceed to an internet server linked to the node and this attack strategies are key in our vulnerability assessment of network systems.

3) Hybrid Oriented Threat Assessment: This is a hybrid of Target –oriented Threat assessment and Non-target oriented Threat Assessment system. It is the vulnerability check for the network attack in which any node could be a target of attack and where the attacker starts from a perceived vulnerable node. The system obtains the value of each fragile state and then use the values to create trusted path dynamically in other to make attack more difficult for the attacker. The Hybrid Threat Assessment algorithm is proposed in this paper.

Algorithm: Hybrid Threat Assessment (HTA)

Input: Network Nodes arranged as a Graph
Output: Each node threat N_t or Vulnerability

```
Build three-dimensional array  C[n][n][v] stored change complexity of each  node in Network model. NN[s] Network Nodes arranged as a Graph $N_i$ node to final node $N_j$.
Initialize NN[s]
NOTA[s] ←0                (optimal token T o k in source node is zero)
for  all v ∈ V−{s}
   do  NOTA[v] ←∞          (set all other threat_degree to infinity)
S←∅                       (S, the set of visited nodes is initially empty)
Q←V                       (Q, the queue initially contains all nodes
while Q ≠∅                (while the queue is not empty)
do  u ← min_NOTA(Q,threat_value)
                    (select the element of Q with the min.threat_degree)
   S←S∪{u}                (add u to list of visited node)
   for all v ∈ neighbors[u]
      do  if   NOTA[v] > NOTA[u] + w(u, v)
                          (if new trusted path found)
   then      d[v] ←d[u] + w(u, v)  (set new value of trusted path)
                          (if desired, add traceback code)
   return optimal_Token
```

The Hybrid Threat Assessment algorithm uses the Non Target –Oriented Threat assessment algorithm in producing the Threat_value and the value is used instead of nodal priority in computing the trusted path for the nodes in the Network.

IV. VULNERABILITY ANALYSER ENGINE

The first task of a Vulnerability Analyzer is examination of unprotected communication lines or paths and assessment of unsecured network architecture that is to discover the nodes in the network, and what node can be easily compromised. Using the hybrid Oriented threat assessment system a path can be found of minimum threat possibility. In addition to discovering vulnerable systems. The Vulnerability Analyzer Engine (VAE) scans the software, files and hardware components of the clients. It has additional techniques for discovering resources and what TCP/IP network services are on each system. It also correct that identify TCP/IP network services on a system isn't sufficient for most network managers; they want to know what services are actually running on what ports. Example, it's easy to assume that port 80 is running HTTP, but what if it's running SMTP server, or assuming someone has started an HTTP server on port 25. These kinds of exceptional configurations point to holes in a security infrastructure. A critical vulnerability in a network may involve incorrect identification of an operating system.

The Vulnerability Analyzer is needed most when Transport layer security (TLS) and secure sockets layer (SSL) protocols for transmitting information privately over the internet are deployed. These protocols have many important B2C applications. For example, many websites use them to collect sensitive information such as credit card numbers during online transactions. TLS and SSL use cryptographic techniques to allow client/server applications to communicate data so that the data are impossible to eavesdrop on or tamper with when https is deployed [14].

In figure 2 a vulnerability analyzer designed based on the Hybrid Oriented Threat assessment is illustrated. In the design the VAE is first applied on the intranet before migrating to the internet servers locations connecting to the intranet all forming a graph of network system which a business organization may be operating.

In figure 2, all the clients both fully connected clients and new clients connect to the E-business network via the socket connector where the VAE resides and each node is scanned for threat degree level. The nodes with very high threat degree level are disconnected by making sure that business transaction packets are not moved via those nodes or within their paths. The nodes with mere high threat degree level are quarantined. Only those that have low threat degree level form the secured E-business network deployable in the system. The clients quarantined are actually allowed to carry packets with loss valuable e-business data not high valuable data packet which can be easily compromised by malicious attackers in the e-business network. In the VAE a firewall configured to make sure packets does not move along quarantined network nodes are clearly indicated between fully connected clients and the vulnerable clients. The disconnected clients are on the other hand totally disconnected from the e-business network pending a new attempt at reconnecting to the network. When they attempt reconnection they are treated as New clients and the VAE reassess them allover.

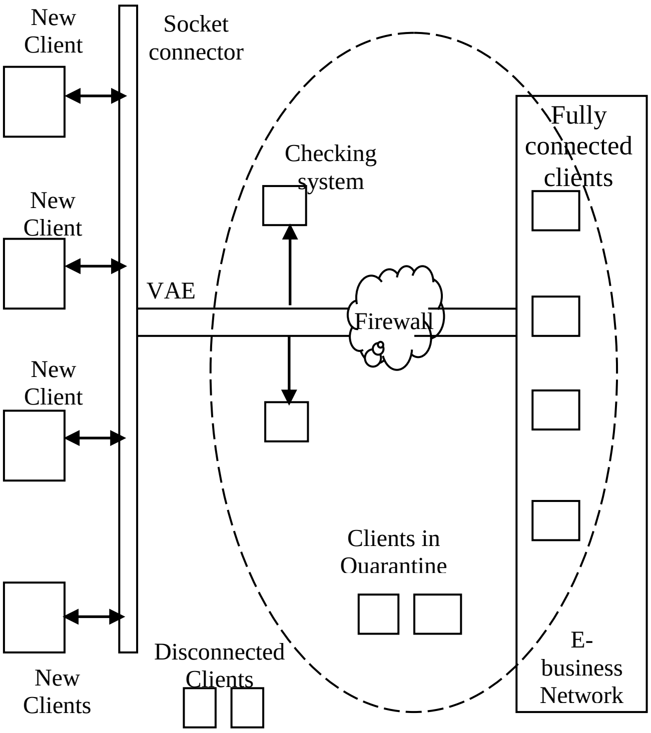

Fig. 2: Vulnerability Analyser

Vulnerable Client Quarantine

The quarantine of vulnerable clients allow the new clients get connected using the system socket connector, the Vulnerable Analyzer engine (VAE) scan the new clients testing the level of each network node threat degree using the Hybrid Threat Assessment (HTA) algorithm. Systems or Nodes within the e-business network that do not meet the requirement are Quarantined. The quarantined clients can be updated for another analysis dynamically. The Vulnerability Analyzer Engine (VAE) checks the hardware and software configuration of the system considering the organisation's network policy.

A new client makes connection with the system socket and the vulnerability analyzer checks the organisation's network security policy on the system software and hardware, when the organisation's network security policy are not met the new client is totally disconnected from the network. In situations where either hardware or software policies are not met, the policy is said to be "partially met". All clients that did not meet all organisation's network security policies go into the quarantine mode waiting to be upgraded to meet the organisation's network security policies. Once the vulnerable client is upgraded to meet the organisation's network security policies, it is subjected to another check. The checked system can still be sent to another quarantine mode waiting to be upgraded to meet the organisation's network. If the client satisfies the policy it will be reconnected to the e-business network. The number of times a vulnerable client can be quarantined and checked depends on the organisational network security policy specified by the organisation's network administrator and configured in the Vulnerability Analyzer Engine (VAE). This cycle provide a dynamism required to keep the e-business network away from known security breach.

From this perspective, it is clear that system quarantine is not a curative measure rather it is a control measure. The period this system is waiting to be updated to company’s security policy level is known as quarantine period -when the system is not denied access nor granted access.

When a node is quarantined, the VAE use the HTA to create a new trusted path for the e-business network to use in routing its packets. This trusted path is also dynamically adjusted when the client is upgraded making it more difficult for the attacker to hit the network. When a remote client computer initiates a connection to another computer, the remote computer is assigned an IP address. However, if the connection is placed in quarantine mode, the network access is limited. When the customer’s remote access computer complies with current network policies, quarantine mode is removed and remote access computer is granted normal access.

The quarantine restrictions placed on individual remote client access connections consists of the following:

i. Quarantine filters, that restrict the traffic that can be sent to and from a quarantined remote access client.

ii. Quarantine session timer that restricts the amount of time the client can remain connected in quarantine mode before being disconnected.

Quarantine Client restriction makes sure that nodes that are quarantined do not get selected in the process of creating trusted path in the e-business network. The filters make sure that traffic that are critical to the e-business network does not get to the quarantine network nodes. Traffics originating from the quarantined nodes are also restricted from getting to fully connected network nodes. The recheck system responsible for redirecting the network node to be rescanned by the VAE uses the quarantine session timer to restrict the amount of time the client remain in quarantine mode before they can be rescanned. Within this time the quarantine node is expected to improve on its policy compatibility and threat degree level. If the time expires without any improvement on the quarantine client node then the network client node could be disconnected from the system returning it to the status of an entirely new client which may need an entirely new connection before it can get back to the e-business network.

In figure 3, the process design of quarantining a vulnerable client clearly illustrates new client connect to network socket of the e-business system. In other to allow the system to get really connected to the e-business network the network client is checked using the Vulnerable Analyzer Engine (VAE) for threat_degree value of the client and the network policy compliance of the connecting node and report made.

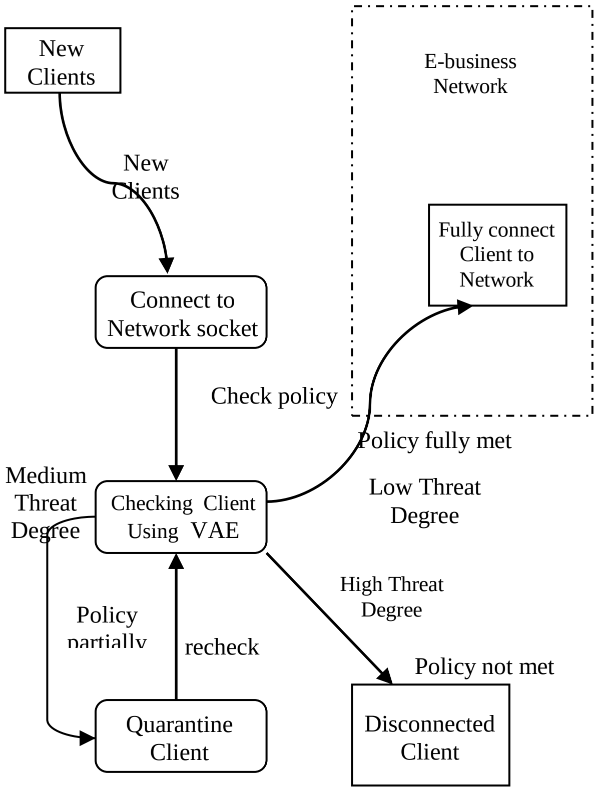

Fig. 3: Process design of quarantining a vulnerable client

If the VAE check show high threat degree and inability to meet policy of network then the client is disconnected but if the check show low threat degree the client is fully connected to the network . However, the process design illustrates that if the VAE check show medium Threat degree, the client is quarantined to be further rechecked for policy compliance and threat degree. This recursive procedure ends up to a disconnection or a fully connected client.

V. NETWORK SECURITY POLICY SIMULATION

In explanation of policies that the nodes can be subjected to, apart from the Threat Degree, we present a simple simulation of network security policy which can be deployed in an implementation system. We assume that we have an e-business company known as XYZ Nig Ltd. The company does not want too much restriction that will scare potential customers who need to get connected to its network.

It therefore decided to formulate the following policies:

a) All servers running on any operating system should have password.

b) Null session not properly configured are not allowed (NetBIOS)

c) NetBIOS must not be turned off over TCP/IP.

d) Buffer overflow problem not allowed

e) Operating system updates should be up-to-date.

f) Application bugs must be patched

g) The registry key must be tested

h) System must have updated Antivirus and Antispyware

The policies listed above are used to check all systems to be connected to the e-business network. When the client socket is connected the policies simulated is used to check the client and assess the vulnerability of the network reporting three risk levels: low, medium, and high.

VI. CONCLUSION

E-businesses need to be secured and any client connecting to the network needed to be checked for vulnerability. The entire network also needed to be continuously checked and trusted path created for the routing of data packets critical to the e-business network. Policies also needed to be created to serve as a measure of check to all clients attempting to connect to the e-business. The result of the check will determine the permission state of the connecting client, the permission state could be **disconnect** if the threat degree is high, **quarantine** if the threat degree is medium and **connect fully** if the threat degree is low. This paper establishes the threat degree assessment by proposing a hybrid oriented threat assessment algorithm which is deployed in the development of vulnerability analyzer engine used in the assessment process of the clients and servers within the e-business network and for the creation of trusted network path for use in critical data flow within the network. The vulnerability analyzer engine is more accurately to grasp the network attack behavior and assess vulnerable network nodes.

ACKNOWLEDGMENT

We thank Mr Emeka Okereke for his pressure that made this paper get ready earlier than thought. We also acknowledgment the contribution of Oyol Computer Consult, Inc in providing us with their office resources in typing and editing the paper.

REFERENCES

[1] Jignesh D., Bhushan T.(2015) Comparison of Vulnerability Assessment and Penetration Testing, International Journal of Applied Information Systems (IJAIS) – ISSN : 2249-0868 Foundation of Computer Science FCS, New York, USA Vol. 8 (6), – www.ijais.org

[2] Boehm, B.W. (1991) Software Risk Management: Principles and Practices. IEEE Software, 8, 32-41. http://dx.doi.org/10.1109/52.62930

[3] Jiangping W., Zhong W. (2015) Case Study on E- Business V Corp. Software Project Risk Management with Interpretive Structural Modeling, Open Journal of Social Sciences, 3, 1-7. http://www.scirp.org/journal/jss http://dx.doi.org/10.4236/jss.2015.34001

[4] Wan, J.P., Wan, D. and Zhang, H. (2010) Case Study on Business Risk Management for Software Outsourcing Service Provider with ISM. Technology and Investment, 1, 257-266. http://dx.doi.org/10.4236/ti.2010.14033

[5] Wan, J.P. and Wan, D. (2011) Analysis on the Mindbugs in Information Technology Service Management Project Implementation. Technology and Investment, 2, 184-192. http://dx.doi.org/10.4236/ti.2011.23019

[6] Chaffey, D. (2009) E-business and e-commerce management. (Harlow: Financial Times/ Prentice Hall, 2009) fourth edition [ISBN 9780273719601].

[7] Kordy, B., Mauw, S., Radomirović, S. v., & Schweitzer, P. (2011). Foundations of attack-defense trees. Paper presented at the Proceedings of the 7th International conference on Formal aspects of security and trust, Berlin, Heidelberg.

[8] Sally, W. (2003): Oxford Advanced learners Dictionary of Current English DAS Hornb. Oxford University Press, 2003.

[9] Dhanamma J., And Rohini T. (2013) The Unified Approach For Organizational Network Vulnerability Assessment, International Journal Of Software Engineering & Applications (IJSEA), Vol.4, No.5, India

[10] Zhihong W. (2015) Network Threat Analysis based on Vulnerability Relation Model, International Journal of Security and Its Applications Vol.9, (1), 357-368

[11] Synder J. (2003): What is vulnerability analysis?. Information Security Publishers, March, 2003.

[12] Zachman, J. (1987): Framework for Information Systems Architecture, IBM Systems Journal 26, 3, March 1987.

[13] Yash S., Kevin G., and Arush V.e (2015) Prevention against Hacking using Trusted Graphs, International Journal of Advanced Research in Computer and Communication Engineering Vol. 4, Issue 11, November 2015.

[14] Cordella A., Martin A., Shaikh M. and Smithson S. (2011) Management and innovation of e-business, London School of Economics, University of London, IS3167, 2790167 .