VULNERABILITIES OF THE INTERNET AND STRATEGIES FOR COUNTERING CYBER ATTACK

Supported by tetfund TERTIARY EDUCATION TRUST FUND

F.N. Ogwueleka[1*] and E.T. Sode-Shinni[2]

[1]Department of Computer Science, Federal University Wukari, Nigeria

[2]Department of Cyber Security Science, Federal University of Technology, Minna-Nigeria

*Corresponding author: ogwuelekafn@gmail.com;

Abstract: There exist numerous software tools on the Internet both for security and attack. These tools are available as open source (freeware) for anyone including malicious hackers to access. The question is how to secure the Internet in the midst of all the available tools. The simple answer is strategy. This study avoids "reinventing the wheel" and concentrates on strategy. The strategy adopted is a model called the Automated Intelligent Vulnerability Insurance system, which assembles the decentralized security tool to form a centralized security interface that minimizes the end users involvement. The system is modelled and implemented using a web-based virtual internet laboratory, which serves as an interface between the user and the Internet. Implementing this model implies that internet users can worry less about trying to install updates and security patches against vulnerability and the security tools use to counterany cyber-attack. The model produces a higher security against cybercrime and reduces the error that can be made by the user's ignorance. This research also exposes existing cyber technologies employed by hackers to exploit vulnerable systems and various cyber-attacks.

Keywords: Vulnerabilities, internet, cyber-attack, cybercrime, hackers, security, strategy.

Introduction

The security of the internet is becoming more challenging as it continues to expand.One of the most challenging issue on the internet is its vulnerability. A large percentage of internet users are vulnerable to attacks either due to emotional instability or defects that exist in their system(Binational Working Groupon Cross-Border Mass Marketing Fraud, 2006). Various techniques such as phishing sites, key loggers, sniffers, social engineeringand malwares are used by hackers to exploits vulnerability that exist on the internet (Patrick, 2011). Though the presence of vulnerability in a system can pose a great danger to the user, many vendor and government agencies are reluctant to openly disclosure vulnerabilities in their system (Cyber Security Policy Review, 2009). It is reported that a vendor can lose an average of around “0.6% value in stock price, equal to loss in market capitalization value of $0.86 billion”in a single vulnerability announcement/disclosure (Rahul & Sunil, 2004).

The Internet is an interconnection of computer systems and computer networks with the aim of sharing information or resource (Sena, 2012). The internet is described as a global communication network comprising of hardware and software linking smaller computers all over the globe. Cyber space refers to a virtual environment where all computer system exists (Shane, 2007). It is in some context used as a metaphor to describe the entire content on the Internet as well as object created by virtual simulations. For clarity, this research presents the “Internet”, “cloud” and the “cyber space” as a single term describing interlinked computer systems, networks, software, users as well as the virtual simulations created by their interactions.

One vulnerability on the internet can lead to huge volume of loss in terms of time and money. Greater numbers of internet (cyber) crimes are effectively carried out by hackers who are able to exploit vulnerabilities. Knowledge of existing vulnerabilities makes users less vulnerable to such attacks. It is important to analyse vulnerability on a system that has been attacked so as to be able to prevent future attack.

Vulnerability can be seen as a weakness or failure to efficiently counter or resist a threat, disaster or an attack. Vulnerability, simply defined is a flaw which allows an attacker to reduce a system’s information certification. The attacker’s ability to exploit the flaw, system susceptibility and the attacker's access to the flaw is the major rudiments of vulnerability. Identifying the vulnerability of the internet (cyberspace) isclassifying the vulnerabilities in the categorised components that make up the Internet. Vulnerabilities in software, network administration and the users whollyintegrate to create vulnerabilities in the Internet. Vulnerability on the Internet opens the door for exploitation by hackers (Bruce, 2003). Hackers take advantage of loop holes (vulnerabilities) and the poor implementation of cyber laws to perpetuate crimes such as cracking, copyright infringement, child pornography, eavesdropping, password sniffing, phishing scam, impersonation, espionage, financial theft, cyber warfare, computer viruses/malware, fraud/identity theft, denial of service attack, cyber stalking, information warfare and cyber bullying (Bruce, 2003). Most criminals take advantage of the virtual nature of the Internet to hide their identity by using false identity tomanipulate ignorant and unprotected users to cover for their criminal activities (Dinach, 2012).

The Internet "cloud" has generated a lot of attention in the world of computing as most activities that were earlier done manually have now been integrated to the Internet. The Internet is associated with activities like emails, multimedia, instant messaging/chats, voice and video communications, data and even application packages (Tidwell *et al.*, 2001). The new shift to the Internet has not only brought about advancement and ease but has attracted along with it attention of cyber-criminal who now seize the opportunity of its wide spread and usage to carry out their attacks. Attacks usually carried out by hackers include social engineering attack, impersonation, exploit, transitive trust, data driven and denial of service(Bruce, 2003).

Types of vulnerabilities include stack overflow (where a part of a large program parameter is executed carelessly) and password guessing. What hackers commonly do is to get any machine on the target network, then install a

password sniffer and finally use a stack overflow to get to the root account (Tidwell *et al.*, 2001).

Virtually every activity can be carried out on the Internet. Activities range from emailing, chats, instant messaging, electronic banking, video conferencing telephony, cloud computing, live news broadcast (streams), electronic transaction (e-commerce/trade), governance (Craig, 2004). In fact, the Internet is being foreseen as the major tool for advances in various fields including medicine, agriculture, journalism, electronics, mechatronics, etc. The study of the vulnerabilities of the Internet and strategies of combating cybercrime is of utmost importance if the survival of the world is not to be jeopardized as the internet controls and serves as a major channel in all fields of study. Adequate knowledge of the vulnerabilities of the Internet and the strategies for combating cybercrime would equip users on avoidance and protective measures against criminal activities in the cyber space and optimally create a "crime-free" world.

Vulnerability in the internet can be caused by the complexity of a system and unnecessary access points; the use of popular, common or well-knownoperating systems, codes, software, or hardware; uncontrolled user privileges and service authorisation; the use of weak/unprotected passwords especially in unsecured websites, poor system design and policy implementation; browsing unsecured websites that automatically install spywares or adware on the users system; exploitable software bugs left by programmers in software programs; unchecked user input by programs on the assumption that all user's input are safe allowing for unintended non-validated direct execution of SQL commands or statements that is as buffer overflows, SQL injection; and reinventing the wheel of past errors (Rahul & Sunil, 2004).

The suggested solutions are dependent on the area where the vulnerability occurs such as penetration testingby certified ethical hackers to identify vulnerabilities before they are exploited, constant update and patching(Bruce, 2003)."To catch a criminal you have to think like a criminal". Cyber security as a whole is a "game" of strategy. The winner is the one with the best strategy. Most tools used for cybercrimes are the same tools used by the ethical hackers to prevent cybercrime. The conquering party is the one with the best strategy. Both ethical hackers and the crackers (criminals) follow almost the same procedure to penetrate a system. The phases of unethical and ethical hacking (penetration testing) include reconnaissance, scanning, gaining access, maintaining access and covering tracks (Patrick, 2011). A cybercriminal can claim to have successfully carried out an attack only when he has gained penetration and is able to successfully cover his track. It is therefore paramount that any strategy for countering cybercrime should be able to uncover or prevent a successful track covering.

Piessen (2002) in "A Taxonomy of Causes of Software Vulnerabilitiesin Internet Software" gave taxonomy of software vulnerability to cover the analysis phase, the design phase, the implementation phase, the deployment phase and the maintenance phase. His taxonomy covers a standard software development cycle. It revealed the fact that vulnerability can occur at any stage of a software cycle. It must be noted that any methodology proposed to counter vulnerability must consider all the cycles in the development of the system.Previous existing strategies for addressing vulnerabilities are limited to specific vulnerabilities. The Automated Intelligence Multi-layered Insurance system proposed in this thesis eliminates such limitation using a combination of several security tools automated collaborating in an intelligent manner to detect vulnerabilities of the Internet and counter cyber-attack.

The aim of this research is to create a virtualized central security system over the internet using existing security software to efficiently eliminate vulnerabilities of internet users to cyber-attacks. Internet users are educated on the loops and likely ways they could easily become victims of such attacks if not properly protected. The study creates an enlightened community of "cyber-attack protected Internet users" and a secure cyber space where people can communicate freely without fear of an undetected/defendable and untraceable attack.The research exposes the various strategies hackers use in exploiting internet users and guides users on security issues using the Common Vulnerability Exposure (CVE) and SAN's top most critical Internet security risk. An Automated Intelligent Multi-layered Vulnerability Insurance model that eliminates end-user involvement, fortify defence systems and centralize data collation on cyber-attacks. This system addresses drawback on previous vulnerability disclosure systems.

Materials and Methods

The designedsystem is an automated multi-layered vulnerability insurance system (AIMVIS). The automation is aimed at eliminating end-user involvement so as to solve the problem of poor configuration and poor update of patches that could be exploited by hackers. The system's internal security design is multi-layered to solidify its defences. Ahacker would have to try several security defencesbefore he could even exploit a singlevulnerability. The system is intelligent as it is able to audit trail and keep record of log files, incoming and outgoing traffic. The design is a learning agent for a single attack on the system helps the system to learn and give alert to security administrators. The system is centralized and the cost of maintenance shared amongst the internet community. The Internet community is to pay for insurance covers (security certificates). Internet community users that buy this insurance immediately become the responsibility of the implementing security body to secure its incoming and outbound internet traffic.

For the purpose of analysis, data was collected from the internet and test statistics. The internet statistics were collected from renowned security statistical sites including securelist.com, internetworldstats.com, www.netlings.com, www.internetsociety.org, projectwebappsec.org and www.computerweeekly.com/new while the test data was collected from a local cyber cafe.

Global data statistics

Fig.1is pie chart of internet users in the world for year 2011 distributed by world regions.

Data collected by Netlingo athttp://www.netlingo.com/tips/cyber-safety-statistics.phprevealed that 20% of kids age 10-17 and 75% of youths have been sexually assaulted online. About 90,000 registered accounts belonging to sex offenders were deleted on MySpace from 2007- 2009. About 61% of internet users between the ages of 13-17 leave their profiles on social networking sites.

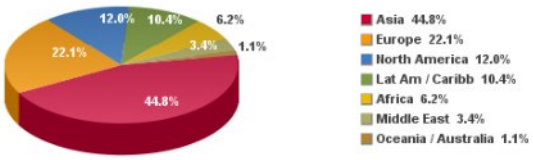


Fig. 1: Internet users in the world for 2011, distributed by world region.
Source: Internet world Stats- www.internetworldstats.com/stats.htm.

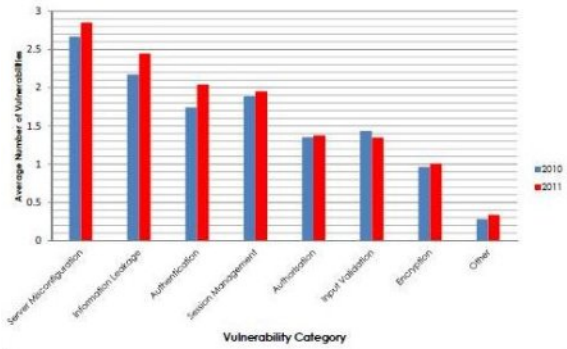


Fig. 2: Average number of vulnerabilities identified within web application from 2010- 2011.
Source: http://www.contextis.com/research/whitepaper/WebApplicationVulnerabilityStatistics 2010-2011

The web application security statistics shows a significant raise in vulnerabilities identified in web application between 2010 and 2011. Fig.2 is a bar chart showing the average number of vulnerabilities identified.The Web Application Security Consortium(http://projects.webappsec.org/w/page/13246991/Web20Hacking20Statistics)revealed that Web vulnerabilities are the most prevalent in servers, 54% of vulnerability exposures in 2008 affects web servers, cross-site scripting (XSS), file include and SQL injection are the most common type of vulnerabilities in web applications. SQL injection became the most prevalent web application vulnerability in 2008 as against cross-site scripting previously. 74% of disclosed vulnerabilities remained un-patched as at 2008 ending.

Local data test statistics

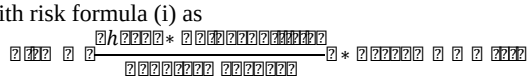
Users were allowed to freely surf the Internet for 14 h period. The following data was gathered during the duration of the research.

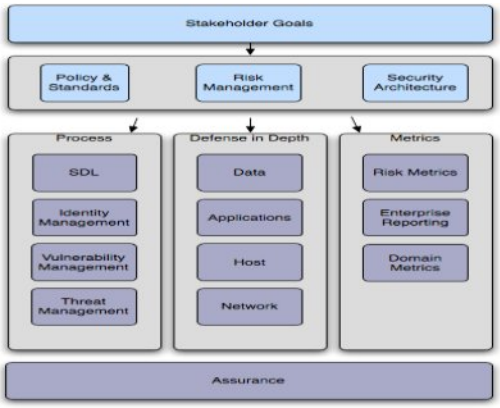
i. Number of users =105
ii. Users below 19 years = 30
iii. Users above 19 years but below 45 years = 51
iv. Users above 45 years = 24

Basic computer users were chosen for this test run. The test showed that over 75% of the total users had a social network account and actually visited it. About 62% of them downloaded freeware or visited one. Less than 3% updated their system software or scanned for viruses. Users were generally less concern of security and were majorly dependent on the existing system configuration.

Sample design

Fig. 3 is a blueprint that guides the design of the Automated Intelligent Multilayered Vulnerability Insurance System (AIMVIS). The design is guided by assets, risk, threats, vulnerabilities and countermeasures with risk formula (i) as





Source: Arctec Group, 2007
Fig. 3: Security architecture blueprint

Statistical test of hypothesis

The test was carried out to evaluate the null and alternate hypothesis using one sample z-statistics. The large statistical data providedevidence infavour of the alternative hypothesis.

i. The data analysis of world's internet usage confirmed that vulnerabilities cross across all age groups of Internet users.
ii. The increase in the number of vulnerabilities recorded in 2011 as compared to 2012 supports the hypothesis that states an increase in vulnerability due to the complexity of technology.
iii. The various categories of vulnerability recorded by CVE and contextis support the fact that internet vulnerability encompasses all vulnerability of the various Internet components as well as users.
iv. The statistics of attack indicates the high number of users exposed to Internet vulnerabilities.

Result of analysis

i. Vulnerabilities cross across all ages of internet users. Children as well as adults can equally be exploited by a vulnerability.
ii. Software, hardware, administrators, users as well as an entire network can be vulnerable and exploited by a hacker.
iii. The numbers of vulnerabilities identified are on the increase.

Various activities, applications and service all combine to form the internet. Just as legitimate users connect to the internet, so also do hackers.Fig.4 shows an illustration of the internet network, various services and activities that occur on the internet. They include social networks, web applications/computing, multimedia, electronic commerce, plug-ins and ad-ons, network of users, wireless/mobile users as well as the hackers.

Fig. 4: Community of Internet network, services and application.

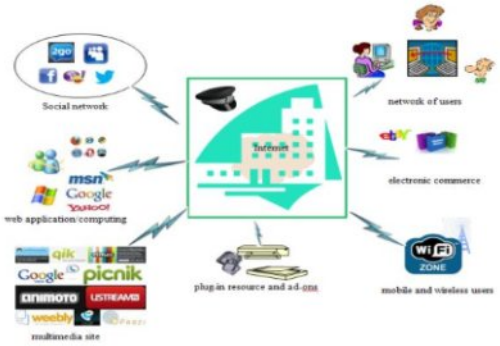


Fig. 6: Broad architecture of AIMVIS

The target of the proposed Automated Intelligent Multi-layered Vulnerability Insurance System is to create an automated vulnerability insured andcentralized database of cyber-attacks. The model is to create a centralised security system to handle internet vulnerabilities. All the decentralised security system is to be integrated into one automated centralised security system called the (AIMVIS). The AIMVIS security system is to monitor all traffics on the internet.The AIMVIS design consist of several vulnerability tools anddefences.

Architecture of the system

Fig. 5 shows a simplified architecture of AIMVIS. The AIMVIS serves as the man in the middle (all-round, automated security). It stands between the insured Internet community users and the open Internet. All traffic to and fro the Internet and the insured Internet community are monitored and secured by the AIMVIS. The broad architecture of AIMVIS is shown in Fig. 6.

Fig. 5: Simplified architecture of AIMVIS

Users that buy into the AIMVIS insurance form the input of the system. The database contains the user ID, the user's location, its IP address, the subscription, activity, date and time. Variable character data type(Varchar) was used as the data type to accommodate for both strings, variable and characters. An administrator is only able to access the input database after a successful login.The output database interface consists of fields and a control. The text field is a drop down menu of name and email.

The graphical user's interface can be visualized from the administrative backend. The administrator logs in using his administrative credentials to view the subscriber's database containing infected files, log in attempts as well as the intrusion attempts. The back end gives the administrator access to integrated security software where he can set schedules and scan options.

Fig.7 is a Unified Modelling Language (UML) class diagram representation of AIMVIS. The diagram shows the system's security, automation and intelligence. The multi-layered nature of the system fortifies its security. This implies that more than a single security package is used to handle a single security challenge. The security package includes antivirus, Intrusion Detection System (IDS) as well as firewalls. These security packages are responsible for the confidentiality, integrity, authenticity, non-repudiation, access control as well as the encryption and decryption of the clients' communication over the Internet.

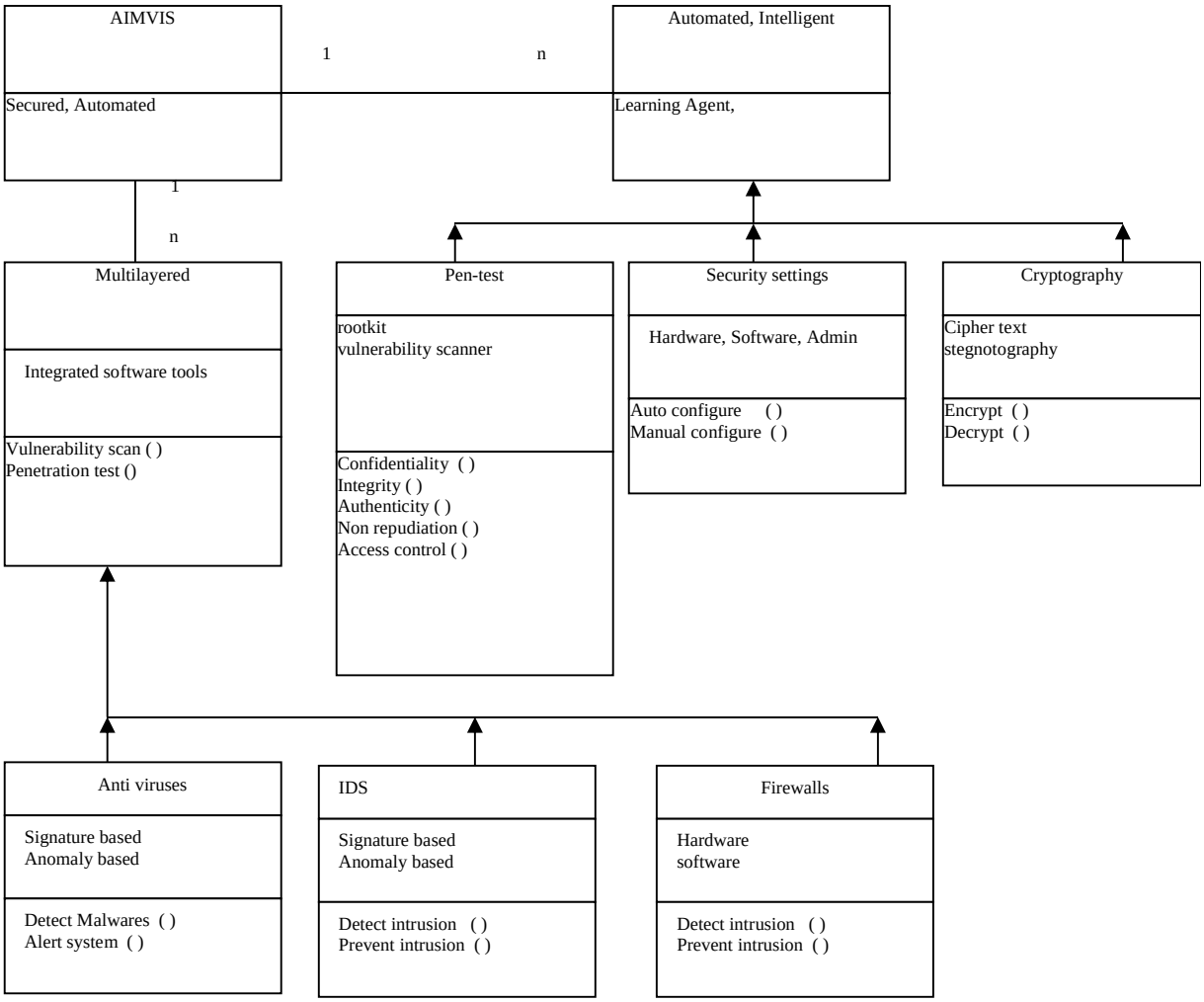


Fig. 7: UML class diagram representation of AIMVIS

The main menu is the login menu and serves as the gateway for registered users to log into AIMVIS services.It also serves as the interface foran administrator to the backend of the system.The sub-system is made up of the internal component of the system. It handles the features embedded in the selected security tools used for the AIMVIS services including encryption, intrusion detection/prevention, firewall and anti-virus operation.

The database design data contains the customer ID, name, clients email ID, IP address, subscription type, log attempts and the infections detected. The customer ID is generated from the customers. It has a varchar character type due to the fact that it can contain both string and character. The name field also consists of the subscriber's first and last names. The email address field is a unique varchar data type field. The IP address is obtained from the subscriber's system locationon the internet. The subscription field is a drop down menu list of subscription options. The log attempts and infections are obtained from the history gathered using the third party security tools.

Error in connection to the system can occur due to low bandwidth, entering invalid credentials and disabling of system. When the bandwidth of the subscriber's internet connection is low, the web interface may not load properly and also when the user enters an invalid credential in the log in session, an error message is displayed, which means the user is unable to launch the system.

Report is generated from the log in session of the main menu in two ways. When a user enters in the correct credential and when the user enters in an invalid credentials. When an invalid credential is entered, it gives a report as;

The ‘proceed’ link takes the user to the signup page where he can sign up for a subscription.

When a user enters correct log in details, it generates a valid log-in report of CONGRATULATIONS! YOU HAVE SUCCESSFULLY LOG-ON TO AIMVIS SERVICES

The query subsystem is designed to retrieve client profile and log files from the database. Administrators can query the system to obtain clients logs either by the user ID or email.The flowchart is shown in Fig. 8. It describes the program flow for the AIMVIS. The user begins by logging into the web interface. A new user is taken to a subscription page where he can register. For an existing user, his credentials are checked for authenticity. If the users credentials matches with that of the database, the

AIMVIS service is activated. When the user's subscription expires, he is sent a notification.

The web interface was developed using hypertext mark-up language (html). Html provides the frame for the web graphical user interface. The functionality was added to the web interface to develop a web application using Java. Java is chosen for this design for its advantage of cross platform compatibility while html was used to design the web interface.

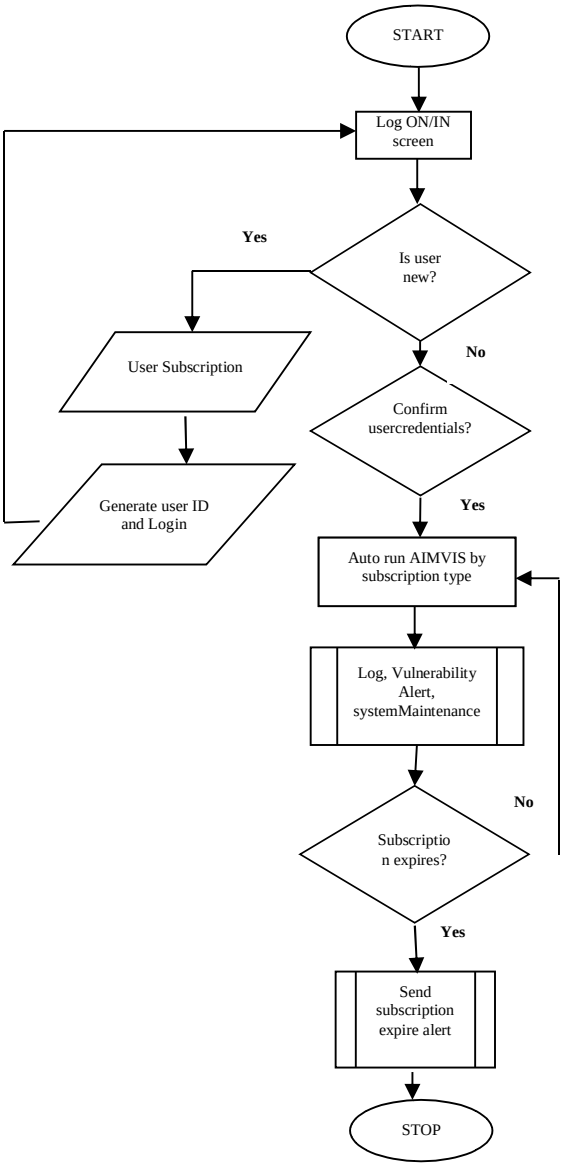


Fig. 8:Flowchart of AIMVIS

Results and Discussion

The system is implemented using Java Development Kit JDK and Oracle database 10g Express edition as drivers.The main menu options include the user registration, subscription and administrative login.The subsystem drivers were implemented using Apache Tomcat. Apache Tomcat was used to provide a model version of the Internet and servers where AIMVIS can communicate with clients.Fig. 9(a) and (b) are the tomcat application manager and program output respectively. It is an engine that helps managers to run all the in-built application packages.

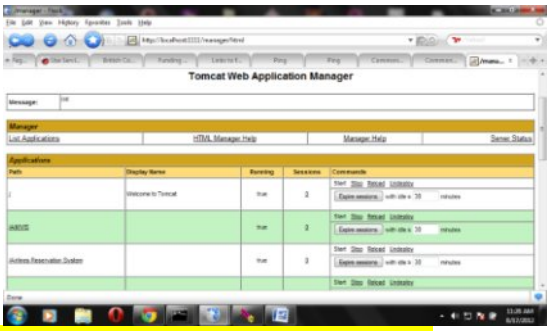


Fig. 9a: Tomcat web application manager.

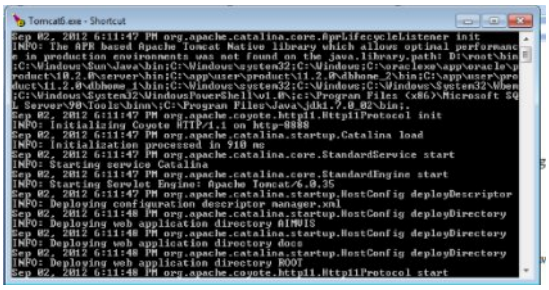


Fig. 9b: Tomcat program.

The database was implemented using Oracle database. Oracle database helps to eliminate data redundancy and downtime. It integrates various tools and secure files, it can be used for data encryption, classification and access and management.Fig. 10 shows the database implementation using oracle database express edition. It displays the back-end list of data residing in the database.Oracle database provided the report generation subsystem driver using its integrated Oracle Structured Query Language(SQL)developer and application express.Fig. 11 is the report generation interface. This interface is used to generate report based on the user ID or email.

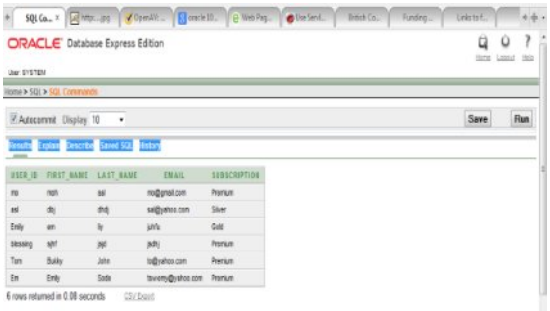


Fig. 10: Database implementation.

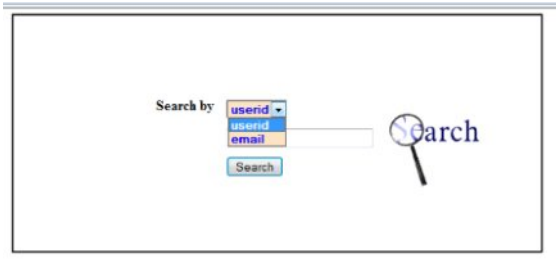


Fig. 11: Report generation interface.

The query subsystem test to see if an entry matches any data in the database and produces an output that confirm or otherwise, alerts the user of a wrong entry. The query is done using SQL commands SELECT data FROM TABLE WHERE data = "user input".The outputs are shown in Figs. 12 and 13. The output is dependent on the user's login information. A match would produce a valid user ID output, while a mismatch produces an invalid user output.

The system integrates third party security tools. The model was tested usingAvast free security guard and a web filter service integrated to the query subsystem of AIMVIS. Clients access the AIMVIS subscription web-based application interface and register for either a gold, silver or premium subscription. The type of subscription registered, determines the duration of service. A gold subscriber is to enjoy a one year subscription, silver six months and premium three months. The system checks registered users for data match and a success launches AIMVIS service while a failure alerts the user of a mismatch and takes the users to a new user registration page. The licensed administrator can login to view log files.

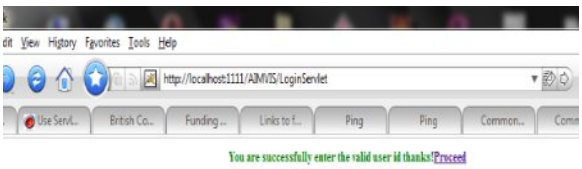


Fig. 12: Query subsystem implementation for a valid entry.

Fig. 13: Query subsystem implementation of an invalid entry

New users were created using the input database interface to populate the databaseas shown in Fig. 14. While an administrator was set using SQL command in the design. A set of restricted web pages were selected to test for the viability of web security while malwares were launch to test for malware detection. The procedureinvolved typing into the URL the restricted web address of dangerous sites.

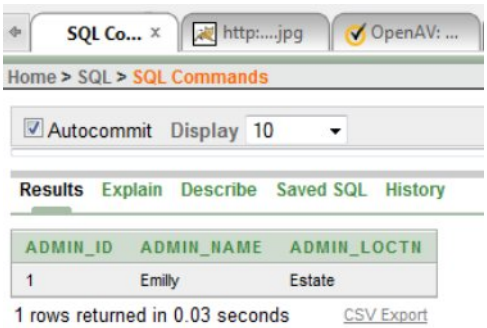


Fig. 14: Test data for admin login.

Fig.15: Test data for user login.

Figs. 15, 16 and 17 test data for user login, test data for restricted websites and test data for malwares respectively.Table 1 shows the expected test result and the actual test result for specific test entries. The test result shows about 83% complete match output and only a 16% partial match.

http://serw.clicksor.com/newServing...	Blocked
http://www.wupload.com/file/26254...	Blocked
http://www.ziddu.com/download/14...	Blocked
http://download.cloudantivirus.com/...	Blocked
http://download.cloudantivirus.com/...	Blocked
http://visicom.antiphishingdomain.c...	Blocked
http://download.cloudantivirus.com/...	Blocked
http://www.9down.com/cyberlink-po...	Blocked
http://blekko.applicationstat.com/dat...	Blocked
http://visicom.antiphishingdomain.c...	Blocked

Fig.16: Test data for restricted web sites.

CRCK_PATCH	Spyware	Removed
WORM_SPYBOT.BMC	Threat	Removed
BAT_QHOST.A	Threat	Removed
TROJ_SPNR.08CG12	Threat	Removed
BAT_QHOST.A	Threat	Removed
BAT_QHOST.A	Threat	Removed
Cookie_Mediaplex	Cookie	Removed
Cookie_Com	Cookie	Removed
Cookie_DoubleClick	Cookie	Removed
Cookie_Apmebf	Cookie	Removed
TROJ_SPNR.08FS12	Threat	Access Denied

Fig. 17: Test data for malwares.

The design has effectively modelled internet vulnerabilities and produced an effective modelled strategy for countering cyber-attack. The database subsystem is able to store a centralised data of users as well as log details. The one sample z-statistics of the local data statistics and global statistics shows a large statistics in favour of the alternative hypothesis.

Table 1: Test result vs. expected result

Entry	Expected Output	Actual Output	Comment
Invalid User entry	Invalid User	This user ID is not valid Proceed to signup new user page	Complete result match
Valid User entry	Valid user	You have successfully entered a valid user ID. Proceed to AIMVIS service	Complete result match
Invalid Admin entry	Invalid entry blocks after 3 attempts	This ID is not valid. Proceed to login screen.	Result partial match
Valid User entry	Valid entry	You have successfully entered a valid ID. Proceed to view backend.	Complete result match
User types in restricted site in URL	Blocks access	Warning this site contains harmful content	Complete result match
Malware detection	Auto scan and auto action	Launch tools to detect malwares and prevents infection	Complete result match

To run the model AIMVIS, Java JDK 6.0 or above and apache tomcat are installed. The AIMVIS package is copied to the apache tomcat web directory and the apache tomcat manager is started up. The AIMVIS project is selected and run. The registration screen allows you to register as a new user. The log in screen allows you to login either as an administrator or an existing user as the case may be.

Conclusion

This research educates internet users on the issue of internet vulnerability, exposes the various areas where internet users become vulnerable to attack and proposes a strategy to counter the current hackers strategy using a model Automated Intelligent Vulnerability Insurance System (AIMVIS). The AIMVIS takes care of internet vulnerability by creating a centralised online security centre using various vulnerability and security tools. The system shields users by serving as an interface between the user and the internet. The AIMVIS is responsible for the complete internet security of the client. It completely eliminates users'challenges of updates, patches and saves the user the cost of purchasing various security tools.

From the analysis and studies carried out in this research, it can be concluded that vulnerability in any component of the Internet including people of all ages, software, hardware, as well as networksopens it up for an attack. In other to combat these attacks, components of the Internet must be shielded from direct access to hackers. The AIMVIS strategy creates the shield between the user and the internet as well as a centralised security system that eliminates users'involvement. The AIMVIS model limits direct access to users by hackers and serves as overallshield against internet vulnerabilities.

The centralization of vulnerability database, the elimination of end user involvement in updates of patches, effective implementation of security policy and program were achieved in this research. Further research can be carried out on the creation and simulation of a virtual internet that can serve as a testing and educational tool for Internet security.

References

Binational Working Groupon Cross-Border Mass Marketing Fraud 2006. Report on Phising, pp. 1-23. http://www.justice.gov/opa/report_on_phishing.pdf

Bruce VH2003. "Ethical Hacking: The Value of Controlled Penetration Tests". pp 1-47, http://www.certconf.org/presentations/2003/Wed/WM4.pdf.

Craig JB 2004.Combating Cyber Crime: The legal (& practical) challenges. Alliance Law Group, pp. 1-17. www.alliancelawgroup.com.

Cyber Security Policy Review 2009.Internet Security Alliance, the Cyber Security Social Contract: Policy Recommendations for Obama Administration and 111th Congress, 5: 1-76.http://www.whitehouse.gov/assets/documents/Cyberspace_Policy_Review_final.pdf.

Dinach 2012.Criminals Pay to Hide Vulnerabilities,p. 1, http://www.dionach.com.

Piessen F2002.A Taxonomy of Causes of Software Vulnerabilities in Internet Software. Dept. of Computer Science, K. U. Leuven, pp. 1-5.

Patrick E2011.*Basics of Ethical Hacking.* Waltham, MA 02451, USA, p. 1-178.

Rahul T & Sunil W 2004.Impact of software vulnerability announcements on market value of software vendors: An empirical investigation, pp. 1-12.

Shane PC2007. Air Force and the Cyber Space Mission defending the Air Force's Computer Network in the future. Center for Strategy and Technology Air War College, pp. 1-38;http://www.au.af.mil/au/awcgate/awccsat.htm.

Sena T2012.How the Internet Works; http://simplytatydesigns.com, pp. 5-23.

Tidwell T, Larson R, Fitch K& Hale J 2001.Modelling Internet Attack.Proceedings of the 2001 IEEE Workshop on Information Assurance and Security United StatesMilitary Academy, West Point, NY, pp 54-59.

Netlingo-*http://www.netlingo.com/tips/cyber-safety-statistics.php*.

The Web Application Security Consortium; *http://projects.webappsec.org/w/page/13246991/Web20Hacking20Statistics.*

http://adventuresinsecurity.com/images/Keystroke_Logging.pdf.

Internet world Stats-*www.internetworldstats.com/stats.htm.*

http://www.contextis.com/research/whitepaper/WebApplicationVulnerabilityStatistics2010-2011.