Home-Based Intrusion Detection System

Mohd Nizam Omar, Guled Yusuf Mihile Guled, Haryani Zakaria,
Angela Ampawan and Roshidi Din
InterNetworks Laboratory, School of Computing,
Universiti Utara Malaysia, 06010 UUM Sintok, Kedah, Malaysia.
niezam@uum.edu.my

***Abstract*—Wireless network security has an important role in our daily lives. It has received significant attention, although wireless communication is facing different security threats. Some security efforts have been applied to overcome wireless attacks. Unfortunately, complete attack prevention is not accurately achievable. Intrusion Detection System (IDS) is an additional field of computer security. It is concerned with software that can distinguish between legitimate users and malicious users of a computer system and make a controlled response when an attack is detected. The project proposed to develop IDS technology on the windows platform. The IDS adopted misuse detection, which is based on signature recognition. The main objective of this proposal is to detect any network vulnerabilities and threats that concern home-based attacks or intrusion. There are five steps in our methodology: The first step is to create awareness of the problem by understanding the purpose and scope of the learning, as well as the problem, which are necessary to be solved. The second step is to make suggestion that the intrusion detection system is protecting the network of the homes. The third step is to develop signature by establishing a set of rule thorough processes for testing IDS. The fourth step is evaluating and testing the system that has been developed. This design used the sensor to find and match activity signatures found in the checked environment to the known signatures in the signature database. Finally, the conclusion in this phase showed the results of the study and the achievement of the objectives of the study. This IDS project will contribute to the efforts to protect users from the internal and external intruders.**

***Index Terms*—Intrusion Detection System (IDS); Home-Based IDS; Hacking; Intrusion.**

I. INTRODUCTION

Security is a major concern in every aspect of our daily life. New equipment and methods have been invented to ensure privacy. However, computer networks still face many threats. There are basically three stages to achieve security in computer system, networks prevention, detection and correction. Prevention is preferable to detect and correct, but it is impossible to prevent 100 percent of attacks. Moreover, detection techniques provide more accurate results in detecting malicious attackers than correction techniques (Perrig, Stankovic, & Wagner, 2004).

Wireless network security has grown in recent years. While different security-protection systems, such as firewalls, authentication and encryption have arisen, most of the wireless systems are still opened to attacks. However, complete attack prevention in wireless networks is not possible due to the openness of the wireless medium, configuration, complexity of the system and abuse by legal users, administration errors, lack of centralized observation, dynamically changed network topologies and management points.

According to Heady, Luger et al. (1990) "Intrusion Detection (ID) is one of the greatest reliable and tested technologies to observe inbound and outbound network traffic to identify unauthorized usage and mishandling of computer system networks. ID also identifies the activity of malicious attackers. It is the process of observing the events happening in a computer system or network and analyzing them for signs of intrusions. Intrusions are attempts to compromise the integrity, availability and confidentiality of a computer or network or to bypass its security mechanisms. They are caused by attackers accessing a system from the Internet, by authorized users of the systems who try to gain additional privileges for which they are not legal, and by authorized users who misuse the privileges given to them".

One of the well-known safety strategies nowadays, is that many of the homes will guard their network or system using a firewall. The greatest common misunderstanding is that a firewall will protect a home computer facility. However, firewall is just one component of an effective security model to be used. According to SCS Computer System Sdn. Bhd, (2004), additional component or layers should be added to offer an effective security model within the company, although firewall alone may not be able to secure enough security as most of the intruders are nowadays.

II. RELATED WORK

This related work will give some descriptions of home-based intrusion detection system. The home-based intrusion system is a system that protects the network of homes or houses from illegal access of someone else. To be safe and secure, it is necessary for the data of stored items in household computers to use this type of network security. IDS is a way of identifying an unauthorized and misused activity of computer system. External attacks are not the only problem: The threat of authorized users misusing and abusing their privileges is an equally pressing problem that demands concern. In addition, the spreading of mixed computer networks has an additional effect to the intrusion detection system to detect the problem. For example, the increased connectivity of mainframe systems enabled access for outsiders, and made it easier for intruders to cover their tracks sufficient enough to break through the firewall easily and access to the network system.

According to Bulajoul, James, & Pannu (2013),the various and increasingly malicious attacks on networks and wireless systems, traditional security tools such as anti-virus programs and firewalls are not sufficient to provide free, integrated, reliable and secure networks. Firewalls have their

limitations. The firewall cannot protect against attacks that bypass the firewall and it may not fully protect against internal threats, such as a disgruntled employee or an employee who accidentally cooperates with an external attacker.

The benefits of HBIDS are detecting attacks or intrusion and any other security violations in home-scale network, and evaluating the effectiveness of HBIDS through experiment. Further, comparison between HBIDS, Antivirus and firewall for preventing problem-behaviors can be done by increasing the perceived risk of discovery and taking action for those who would attack or otherwise abuse the system.

Signature based detection systems can be easily avoided by attackers who revise known attacks and target systems that have not been updated with new signatures that detect the alteration. The signature based methodology requires important resources to keep up with the potential infinite number of modifications to known dangers. Signature based methodology is simpler to modify and improve since its performance is mainly based on the rules deployed (Yurcik 2002)

Snort is a network-based intrusion detection that scans the traffic and tries to find suspicious activities using a set of rules. A rule is a set or a collection of specific byte pattern that indicates a particular attack. This type of IDS is usually called signature based intrusion detection system. Snort also contains firewall such as Fw-snort, Port Scan Attack Detector (PSAD), Firewall Knops and Port knocking among the few activities attached to it. It is one of the most widely used with a large number of predefined signatures and continuously updated (Laing, 2000). Hence, the aims of IDS are to use available information in order to identify both attacks drawn from misuse of insiders and external hackers

The idea of IDS was initially presented by Anderson, (1980), to set off straight computer security methods. Anderson mentioned that intrusion is an attempt or a danger to use deliberate illegal action. Anderson has suggested the following three factors to protect unauthorized hackers, namely access information, control information, and render a system unusable. Most of the IDS have been focused on outsider intrusion detection for operators, network and database systems. However, little attention has been given to intrusion detection for the application systems, such as banking and finance systems, which contain lots of business security information. Most of the intrusion detection approaches for application systems focus on outsider intrusion, but not much is available for insider intrusion, such as malicious codes created by malicious software engineers (Puketza, Zhang et al. 1996).

A. Intrusion Detection System (IDS)

An intrusion is defined by Rehman, (2003) as any action of the group to cooperate confidentiality or integrity of a resource. IDS evaluates all the system activities in order to sense the intrusion. It examines security violation events and recognizes illegal access. The intrusion can be put in different forms such as, using workers' personal to try to access resources on a system or network, and malicious programs that spoils the system incomes, damages the system concerned and operates the system data. In addition, legal personnel may also try to gain additional treats or access to trusted information, thus co-operating the system security policy.

B. Types of IDS

Active IDS is famous as Intrusion Detection and Prevention essential for an operator. IDPS have benefits of offering real-time corrective action in response to an attack. System(IDPS) mechanically designs block suspect attacks without any interface. Passive IDS is a method that is configured to a single observer to examine network traffic action and make aware to operator the future weaknesses and attacks. A passive IDS is not skillful to show any defensive or helpful functions on its own.

Network Intrusion Detection System (NIDS) comprises a network appliance with network interface controller operating in promiscuous mode and a spread management interface. The IDS is placed along a section. Network segment and evaluates all traffic. Host intrusion detection system and software applications are installed on terminals, which they examine. The mediators display the operational system and write data to log files and/or trigger alarms.

C. Network Security

Physical software can be protected and measured by network security to keep the basic networking infrastructures from illegal access, misuse, malfunction, alteration and destruction as well as the making of secured platform for mainframes, users and programs to show their permission of critical functions within a protected environment. The purposes of network security are to get accessibility, confidentiality, integrity, intrusion, detection, usability, manageability and performance (Vokorokos, Kleinová et al. 2006).

Network Security Tools. Snort is a network based IDS that scans the traffic and tries to find suspicious activities using a set of rules. A rule set is a collection of specific byte pattern that indicates a particular attack. This type of IDS is usually called a signature based intrusion detection system. Snort can also be configured to work as a packet sniffer and packet logger. Snort shows protocol, examines, matching or content searching, and it is usually used to vigorously block or passively sense a diversity of attacks and probes, such as buffer overflows, stealth port scans and web application. Snort security tool contains Fw-Snort, Port Scan, combining Psad, and Fwsnort, FwKnop and Port knocking (Stanley 2009).

D. Home-based IDS (HbIDS)

Home-based intrusion detection system main function is to determine unauthorized access to monitor the computer network by examining traffic on the network for signs of malicious activity. Protecting a wireless network is very significant because, even though the hackers could not use your internet connection, he or she can still access your files and checking what you are doing. Even the hackers can access your internet connection to upload illegal materials. Home-based intrusion detection system help to secure the network of home or house to prevent illegal access by someone else: A safe and secure data are stored in the computers.

E. Types of Attack in HbIDS

Scanning Attack: Scanning Attacks are used to integrate information about the system being attacked. In this method, the attacker gains topology information, types of network traffic permitted through firewall, active host on the network, OS and kernel of hosts on a network. Using this

evidence, the attacker can open attacks expected at more specific misuses.

Denials of Service Attack (DOS): Denials of service attack have two main types: flaw exploitations and flooding. Flooding attacks can be easily implemented. For example, you can implement or launch DOS attacks by using the ping command. If the attacker has contact to a greater bandwidth than the victim, this will simply and rapidly overcome the victim. That is the reason why the victims need to half open transmission control protocol connection. The victim will send a transmission control protocol - Synchronization. Or Acknowledgment packet, and wait for an acknowledgment in response. Since the acknowledgment never comes, the victim finally will consume available resources waiting for acknowledgments from a non-existent host.

Penetration Attack Penetration attacks comprise all the attacks made by the unauthorized attacker and the capability to receive access to system resources, treats or data. This attack would deliberate a penetration attack. Being able to arbitrarily compile code as a root offers attackers to have access to whatever system resource that they may think of. However, this could permit the user to launch other types of attack on this system, or even attack other systems from the cooperated system.

F. Home-based IDS (HbIDS) Related Work on HbIDS

Remote home server is intended as a trusted third party. When the system switches from the right hand side 2 (RHS-2) mode to the RHS-1 mode, that is, the straight connection between an authentic user, including an attacker and the HAS (RHS-2) is disabled, while the connection between the authentic user and the HAS is preserved through the RHS, as indicated by the interconnections (Gill, Yang et al. 2012).

Wireless, smart home is one of the promising applications of pervasive computing. The empirical study shows that wireless sensor nodes have the potential to provide a reliable solution in a smart home environment. The ZigBee communication technology in smart home scenario is used for integrating sensors WSN (Usman, Muthukkumarasamy et al. 2012).

Home area networks (HANs) are subsystems within advanced metering infrastructure which are answerable for information transfer among the smart meters and household electrical devices and appliances. Future use of wireless communications is beig located in a physically unsafe environment making the HAN as one of the weakest systems in the smart grid (Jokar, Nicanfar et al. 2011).

Using MHLRC protocol, the system reduces the frequent activities of homes, when it receives a demand for the update copy from a non-home node. For this choice, the two conditions are verified, if the conditions are not fulfilled, The first condition is that there is no modification to the home copy of the home node during the current interval. An interval begins with each special access, such as a release and acquire. The second condition is that the page must not be a page that is just moved in the current interval (Abe and Okamoto 2 003).

In the following implementation design and evaluating test, configuring snort IDS with windows operating system is explained based on Figure 1 (Alsafasfeh & Alshbatat, 2011).

After downloading and installing all requirements for snort IDS to work with windows operating System, snort IDS can be used as a detection system to monitor all packets that are sent or received. The Snort engine is distributed both as source code and as binary distributions windows. It is authoritative to note that the Snort engine and Snort rules are spread separately. After installing snort on windows operating system, it must be configured to work correctly and capture packets. Monitoring network traffic to determine which attack is to be prevented or which one is not allowed to access the network is to be terminated. Snort depends on the following rules (Rehman 2003).

Configuration the snort.conf File. Snort.conf file is the main file in snort operation and must be configured before running snort, this file will be read by the detection engine and preprocessors. Snort.conf file is located in etc folder in snort path. Snort.conf file contains sample of snort configuration. To create a custom configuration, we need to take these actions: Set the network variables, configure the decoder, configure the base detection engine, configure dynamic loaded libraries, configure preprocessors, configure output plug-in, customize your rule set, customize preprocessor and decoder rule set and customize shared object rule set.

Running Snort as Firewall. Snort is an open system which works as a firewall to control access. Using snort, a new rule contains all specifications and requirements for the operation must be done. To make snort as a firewall, you have to create new rules. The first one is used to monitor websites access and tell network administrator about the whole connections between network nodes and external network. The second one is to block the access to a specific website.

Configuration Snort for Monitoring Access. Snort based on a set of rules, these rules contain a set of operations that allows network administrators to monitor all network traffics. To create a new rule that has the authority to monitor all accesses from our network to external networks, you must write all primary contents of the rule header and rule options. Making snort as a monitoring system is telling the network administrator who is trying to access the network (Muthuregunathan, Siddharth, Srivathsan, & Rajesh, 2009).

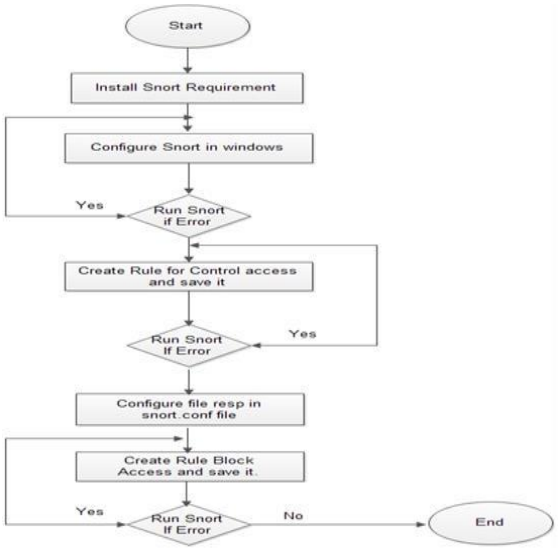

Figure 1: Implementation of the Research

III. RESULTS

New rules have been created to allow snort to monitor access and get alerts for system administration. Alert file contains all data that describe the connection between two entities, IP address for two entities (sender and destination) and the access time. Detection engine in snort has checked packet contents with rule options and when matching is found, the snort engine will send alert to the network administrator with a message telling him or her who is accessing the network. Figure 2 and 3 display how the snort checks the packets content in home-based.

Figure 2: Snorts Get Alerts Large UDP packet and Host Attempt Attack

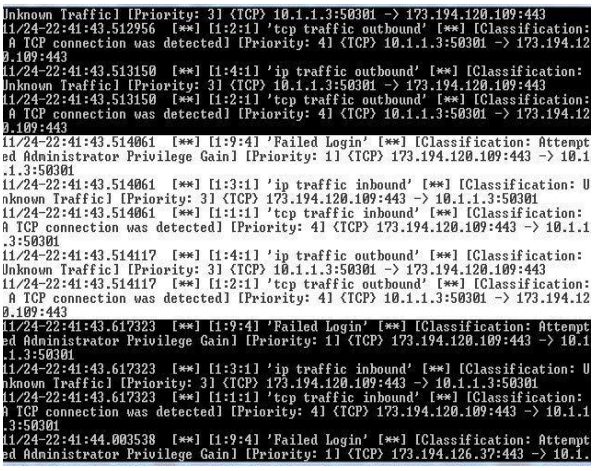

Figure 3: Snorts Get Alert Failed Login

Table 1 shows all information on how to protect Home-based network and its related connection between the user and the intruders.

Table 1
Experiment and Result

Experiment	Result
Wrong Password	[**] 'Failed Login' [**] 11/24-22:40:59.164311 199.59.148.23:443 -> 10.1.1.3:49612 TCP TTL:49 TOS:0x0 ID:49778 IpLen:20 DgmLen:286 DF ***AP*** Seq: 0x9510BCCD Ack: 0xF3C93056 Win: 0x3E9 TcpLen: 20
DOS Attack UDP	[**] 'Suspect of Large UDP and ICMP Packet' [**] 11/24-11:41:47.562685 173.194.126.39:443 -> 10.1.1.1:53414 UDP TTL:55 TOS:0x0 ID:27963 IpLen:20 DgmLen:1126 Len: 1098
Attempt Host Access	[**]' ATTACKS in Host command *access* attempt ' [**] 11/24-10:18:56.752093 10.1.1.2 -> 10.1.1.1 ICMP TTL:128 TOS:0x0 ID:1220 IpLen:20 DgmLen:60Type:8 Code:0 ID:1 Seq:9 ECHO

Table 2 shows all information on how to protect Home-based network and its related connection between the user and the intruders using a firewall.

Table 2
Result and Discussion

Experiment	Rule-based	Results
Wrong Password	Windows Firewall and AGV Antivirus	Null
DOS Attack UDP	Windows Firewall and AGV Antivirus	Null
Attempt Host Access	Windows Firewall and AGV Antivirus	Null

IV. CONCLUSION

Snort is the best alternative system based on our result of Home-based network security. It is considered as the heart of Intrusion Detection System at home-based network. In this paper, IDS with snort has been implemented and configured with windows-based environment. From this research, it was found that HbIDS can detect failure of login to a software package used to remotely control and administer hosts. Further, DOS Attack of UDP and intrusion attempt host was accessed to compare with the use of current security-based product, antivirus and firewall.

REFERENCES

[1] Alsafasfeh, M. H., & Alshbatat, A. I. 2011. Configuring Snort as a Firewall on Windows 7 Environment. *JUSPN,* 3(2): 73-77.

[2] Amita Pandit, Sunita Gond. 2013. Analysis for Improving Intrusion Detection System in Wireless Network. *International Journal of Advanced Research in Computer Science and Software Engineering.*

[3] Anderson, James P. 1980. Computer security threat monitoring and surveillance: Technical report, James P. Anderson Company, Fort Washington, Pennsylvania.

[4] Anderson, J. P. 1980. Computer security threat monitoring and surveillance: Technical report, James P. Anderson Company, Fort Washington, Pennsylvania.

[5] Bass, T. 2000. Intrusion detection systems and multisensor data fusion. *Communications of the ACM,* 43(4): 99-105.

[6] Bejtlich, R. 2004. The Tao of network security monitoring: beyond intrusion detection: Pearson Education.

[7] Baker, Zachary K, & Prasanna, Viktor K. 2000. A methodology for synthesis of efficient intrusion detection systems on FPGAs. *Paper presented at the Field-Programmable Custom Computing Machines, 2004. FCCM 2004. 12th Annual IEEE Symposium on.*

[8] Balepin, Ivan, Maltsev, Sergei, Rowe, Jeff, & Levitt, Karl. (2003). Using specification-based intrusion detection for automated response. *Paper presented at the Recent Advances in Intrusion Detection*

[9] Brentano, James, Snapp, Steven R, Dias, Gihan V, Goan, Terrance L, Heberlein, L Todd, Ho, Che-Lin, Smaha, Stephen E. 1991. An architecture for a distributed intrusion detection system. Paper presented at the *Proceedings of the 14th DOE Computer Security Group Conference*, pages.

[10] Bulajoul, Waleed, James, Anne, & Pannu, Mandeep. 2013. Network Intrusion Detection Systems in High-Speed Traffic in Computer Networks. Paper presented at the *e-Business Engineering (ICEBE), 2013 IEEE 10th International Conference on.*

[11] Carver, C., Hill, J. M., Surdu, John R, & Pooch, Udo W. 2000. A methodology for using intelligent agents to provide automated intrusion response. Paper presented at the Proceedings of *the IEEE Systems, Man, and Cybernetics Information Assurance and Security Workshop,* West Point, NY.

[12] Cox, K. J., & Gerg, C. 2004. Managing security with snort & ids tools: O'Reilly Media, Inc.

[13] Fang, B., Leung, C. H., Tang, Y. Y., Tse, K., Kwok, P. C., & Wong,

Y. (2003). Off-line signature verification by the tracking of feature and stroke positions. Pattern recognition, 36(1), 91-101.

[14] Foo, Bingrui, Wu, Yu-Sung, Mao, Y-C, Bagchi, Saurabh, & Spafford, Eugene. 2005. ADEPTS: adaptive intrusion response using attack graphs in an e-commerce environment. Paper presented at the *Dependable Systems and Networks, 2005. DSN 2005. Proceedings. International Conference on.*

[15] Gleichauf, R. E., Randall, W. A., Teal, D. M., Waddell, S. V., & Ziese, K. J. 2001. Method and system for adaptive network security using network vulnerability assessment: Google Patents.

[16] Heady, R., Luger, G., Maccabe, A., & Servilla, M. 1990. The architecture of a network-level intrusion detection system: Department of Computer Science, College of Engineering, University of New Mexico.

[17] Jahnke, Marko, Thul, Christian, & Martini, Peter. 2007. Graph based metrics for intrusion response measures in computer networks. Paper presented at the *Local Computer Networks. LCN 2007. 32nd IEEE Conference on.*

[18] Kemmerer, R. A. (2004). A Comprehensive Approach to Intrusion Detection Alert Correlation. Computer Science Department University of California Santa Barbara.

[19] Kher, Vishal, & Kim, Yongdae. 2005. Securing distributed storage: challenges, techniques, and systems. Paper presented at the *Proceedings of the 2005 ACM workshop on Storage security and survivability.*

[20] Lee, W., & Stolfo, S. J. 1998. Data mining approaches for intrusion detection. Paper presented at the Usenix Security.

[21] Lee Yew Loon. 2004. Intrusion Detection System(IDS) for Detecting Network Threats and Vulnerabilities. Kebangsaan Malaysia: Faculty of Technology and Communication Technology.

[22] Lee, Wenke, Fan, Wei, Miller, Matthew, Stolfo, Salvatore J, & Zadok, Erez. 2002. Toward cost-sensitive modeling for intrusion detection and response. *Journal of Computer Security.* 10(1):5-22.

[23] Laing, B. 2000. How to guide-implementing a network based intrusion detection system. http://www. snort. org/docs/issplacement. pdf.

[24] Mell, P., Hu, V., Lippmann, R., Haines, J., & Zissman, M. 2003. An overview of issues in testing intrusion detection systems: US Department of Commerce, National Institute of Standards and Technology.

[25] Mujtaba, M. 2012. Analysis of Intrusion Detection System (IDS) in Border Gateway Protocol.

[26] Muthuregunathan, R., Siddharth, S., Srivathsan, R., & Rajesh, S. 2009. Efficient Snort Rule Generation Using Evolutionary Computing for Network Intrusion Detection. Paper presented at the *Computational Intelligence, Communication Systems and Networks, 2009. CICSYN'09. First International Conference on.*

[27] Mudzingwa, David, & Agrawal, Rajeev. (2012). A study of Methodologies used in Intrusion Detection and Prevention Systems (IDPS). *Paper presented at the Southeastcon, 2012 Proceedings of IEEE.*

[28] Nasr, Khalid, El Kalam, Anas Abou, & Fraboul, Christian. 2011. A holistic methodology for evaluating wireless intrusion detection systems. Paper presented at the *Network and System Security (NSS), 2011 5th International Conference on.*

[29] Puketza, Nicholas J., Zhang, Kui, Chung, Mandy, Mukherjee, Biswanath, & Olsson, Ronald A. 1996. A methodology for testing intrusion detection systems. *Software Engineering, IEEE Transactions on*. 22(10):719-729.

[30] Patcha, A., & Park, J.-M. 2007. An overview of anomaly detection techniques: Existing solutions and latest technological trends. *Computer Networks*, 51(12):3448-3470.

[31] Perrig, A., Stankovic, J., & Wagner, D. 2004. Security in wireless sensor networks. *Communications of the ACM*, 47(6): 53-57.

[32] Rehman, R. U. 2003. Intrusion detection systems with Snort: advanced IDS techniques using Snort, Apache, MySQL, PHP, and ACID: Prentice Hall Professional.

[33] Ragsdale, Daniel J, Carver Jr, Curtis A, Humphries, Jeffrey W, & Pooch, Udo W. 2000. Adaptation techniques for intrusion detection and intrusion response systems. Paper presented at the *Systems, Man, and Cybernetics, 2000 IEEE International Conference on.*

[34] Shanbhag, S., & Wolf, T. 2009. Accurate anomaly detection through parallelism. *Network, IEEE*, 23(1): 22-28.

[35] Srinivasan, Vijay, Stankovic, John, & Whitehouse, Kamin. 2008. Protecting your daily in-home activity information from a wireless snooping attack. Paper presented at the Proceedings of the *10th international conference on Ubiquitous computing.*

[36] Stakhanova, Natalia, Basu, Samik, & Wong, Johnny. 2007. A taxonomy of intrusion response systems. International *Journal of Information and Computer Security,* 1(1): 169-184.

[37] Toth, Thomas, & Kruegel, Christopher. 2002. Evaluating the impact of automated intrusion response mechanisms. Paper presented at the *Computer Security Applications Conference. Proceedings*. 18th Annual.

[38] Vaishnavi, V., & Kuechler, W. 2004. Design research in information systems.

[39] Wu, S. X., & Banzhaf, W. 2010. The use of computational intelligence in intrusion detection systems: A review. *Applied Soft Computing*, 10(1): 1-35.

[40] Yurcik, W. 2002. Controlling intrusion detection systems by generating false positives: squealing proof-of-concept. Paper presented at the Local Computer Networks, 2002. Proceedings. *LCN 2002. 27th Annual IEEE Conference on.*

[41] Zhang, Ran, Qian, Depei, Ba, Chongming, Wu, Weiguo, & Guo, Xiaobing. 2001. Multi-agent based intrusion detection architecture. Paper presented at the *Computer Networks and Mobile Computing, 2001. Proceedings. 2001 International Conference on.*