International Journal of the Physical Sciences Vol. 7(4), pp. 624 - 637, 23 January, 2012
Available online at http://www.academicjournals.org/IJPS
DOI: 10.5897/IJPS11.1381
ISSN 1992 - 1950 © 2012 Academic Journals

Full Length Research Paper

Intrusion threat detection from insider attack using learning behavior-based

Deris Stiawan*, Mohd. Yazid Idris, Md. Sah Hj Salam and Abdul Hanan Abdullah

Faculty of Computer Science and Information System, Universiti Teknologi Malaysia.

Accepted 5 December, 2011

In recent years, intrusion prevention system (IPS) had been developed as a new approach system to defend networking systems, which properly combines the firewall technique with the intrusion detection. When an attack is identified, intrusion prevention immediately blocks and logs the offending data. The primary IPS uses signature to identify activities in network traffic and the host will perform detection on inbound – outbound packets and would block that activity before the damage happens or the access is reached to the network resources. Signature is the primary factor in intrusion prevention, to identify something and then stopping it must be through the distinct characteristics. In this paper, we propose Behavior-based prevention to trigger mechanism and analyze correlation outbound traffic from inside user. We describe the habitual activity from outbound traffic, which is normal activity, suspicious threat or malicious threat uses traffic assessment. This paper also describes an algorithm for the complexity of the suspicious response.

Key words: Behavior-based detection, hybrid intrusion prevention, identify habitual.

INTRODUCTION

In the last few years, the Internet has experienced an explosive growth. Along with the widespread evolution of new emerging services, the quantity and impact of attacks have been continuously increasing. Defense system and network monitoring has become an essential component of the computer security to predict and prevent attacks. According to North American, Network Operators Group (www.nanog.net) examines the statistical data of Internet traffic trends and experienced explosive growth.

Computer system security has become a major concern over the past few years; many system devices and other tools are available to help counter the threat of these attacks. The attack from inside a network is very difficult to detect, because defense system will think that it is a normal activity. Furthermore, network traffic from inside user is not filtered and recognized by security check point. Intrusion detection was developed to identify and report attack in the late 1990s, as hacker attacks and network worm began to affect the Internet. It can detect hostile traffic and send alert but can do nothing to stop the attacks (Kim et al., 2010). In other words, intrusion detection is passive, cannot expect to detect all malicious and malicious activity all the time and incompatible to integrate with control restriction to stop traffic inbound-outbound from attacking. Hence, it means that it can only detect attack actions, without taking any prevention action.

Intrusion prevention system (IPS) is a new approach system to defend networking systems, which combine the technique firewall with the intrusion detection properly. It is a proactive technique that prevents the attacks from entering the network by examining various data record and detection demeanor of pattern recognition sensor (Stiawan et al., 2011; Stiawan et al., 2010a). When an attack is identified, the intrusion prevention blocks and logs the offending data. The primary intrusion prevention uses signature to identify activity in network traffic and host where it performs detection on inbound – outbound packets taken place and will block that activity before damage and access to the network resources was gained.

*Corresponding author. E-mail: deris@ieee.org.

In recent years, many organizations had devoted their significant resources to control suspicious threats imposed, by using a combination of unified threat management: (i) Anti-virus/anti-spyware software; (ii) Firewall, intrusion detection and prevention system, and (iii) Network monitoring management. The current intrusion detection technologies are not very effective against prediction of new mechanism of attack. There are several limitations, such as the performance, flexibility, and scalability.

Some work focused on technology environment to represent interrelation technology and behavior over this year has been done where a few of this research were paying attention to observation effect of inside user for security violations. According to CERT (www.cert.org/insider_threat), the threat of attack from insider is real and substantial; insider threat always involves current or former: employee, service provider or contractor.

Evidently, the majority (55%) reported that at least one insider event (up from 39% the year prior). Following result from CERT survey, which began in 2004 until 2007, 51% respondents who experienced a cyber security event were still victims of an insider attack in 2010. Increasingly security threat will happen in this situation. Unfortunately, in previous effort which focuses on the signature system, attack from outside, and taxonomy model attack without discussing how to analyze and recognize normal activity of trusted users from inside network. In our thoughts and observations, attack from the inside is unpredictable, able to beat defense system, at last gaining success to access. There are some factors that increase this threat, such as: (i) Many tools/script to hack/attack from internet; (ii) Behavior user (skill/ability), and (iii) weakness in the internal system.

The main contributions of this paper are: (i) Enhancement method of a learning phase to identify and recognize normal or malicious threat from behavior user; (ii) Provide awareness about the attack from inside user; (iii) Balance prevention, detection and response from threat; (iv) To identify common knowledge as an activity profile between new algorithms for identifying the normal behavior of user activities.

We proposed new system architecture for IPS, named pitcher flow (Stiawan et al., 2010b), which is a behavior-based detection mechanism to detect, identify, recognize, and react to a suspicious threat (Stiawan et al., 2010c). The proposed method also addresses how to identify common knowledge as an activity profile between new algorithms for identifying the normal behavior of user activities.

Furthermore, in this paper, we described interrelation between habitual activity user with security affect, and we proposed new approach for detection, controlling and responding in identifying outbound traffic from inside user. The method used is expected to help security officers (IT Manager and Administrator) to be aware of user profile's status and activities.

BACKGROUND AND RELATED WORK

There are some works on integration component for increasing the accuracy detection with behavior users. According to Mizutani et al. (2009), they have behavior rule based intrusion detection method to analyze correlation of communication behavior using rules. They use auxiliary variables approaches in each behavior rule to figure out various correlations between event and communication behavior of various software and attack scenario. In 2004 (Yin et al., 2004) the behavior of the system was analyzed to find out the probability if the Markov chain model of the norm profile supports the observed behavior or not. They concluded from the experiment test effectiveness of the temporal signature on different applications as an alternative for intrusions. Performed work (Rhee et al., 2009), was proposed as a model and test relationship among self-efficacy in information security was tested in order to practice behavior and motivation to strengthen security effort. They conclude that self-efficacy in information security does have a substantial explanatory power regarding individuals information security practice behavior both in term of technology use and security conscious care behavior.

On other side, user behavior is a widely used term that is loosely defined; it could have different meaning and be measured differently depending on the research area. For example, in the human-computer interaction (HCI) field, user behavior means accommodation of human diversity, which in the social science and computer design field may have more value on human engineering (Wang et al., 2009). According to Qiao et al. (2007) behavior analysis-based learning framework for host-based intrusion detection, they focus on the verification of unknown and new types of attacks based on host behavior analysis, from this experiment they have described more accurately and comprehensively with a set of indicators: User profile, program profile, and system resource access.

Proposal work (Rhee et al., 2009) concluded the survey as evidenced previously, there are many naïve user behaviors that are not intended to harm but many had cause detrimental effects on information security. The survey which use social cognitive theory and explore its viability as a framework for understanding factors influencing end users control-enhancing behavior. In the performed observation by Wang et al. (2009), HCI uses one of three approaches to gather user behavior information: (i) Video taping of user activities; (ii) Recording user activities via logging data from a particular application, and (iii) Using an unobtrusive application that exists in the background across all the application installed on the index machine.

In some instances, peek traffic in network can be of effect from packet flooding, broadcast storm or worm action. Nevertheless, some application is voracious with bandwidth (that is, streaming video, games, and peer to

peer). Voracious traffic looks like suspicious activity on screen monitoring network. Thus, ambiguity is involved during the process of classifying intrusion from normal activities. Previous researcher (Verbeek, 2006) describes the categorized behavior user, such as, (i) user characteristics, (ii) user attitude (iii) user knowledge and capabilities, and (iv) user time space. For an adequate understanding of the complex relationships between behavior activities and suspicious attack from habitual user, it is not sufficient to simply identify the mutual influences between technologies and human actions. This context is important because the attitude and ability of each user varies, which in turn has implication for the activity of higher transaction size and concurrent connection which then definitely affects the reliability of the overall network. Additionally, proposal (Rhee et al., 2009) present social cognitive theory which postulates the reciprocal nature of interaction among behavioral, personal and environmental factors; they uses analysis survey with questioner about security aspect of an organization. What is essential in network security is to monitor and analyze network traffic for profiling user behavior.

A robust defense system has to hold parameters representing both normal and abnormal user behavior patterns, and such parameters were require to be recalibrated consistently to adjust for changes in network and user behavior over the time. From our observation, we can describe profiles user with convention continuously activity access, it is what we call habitual activity.

For an adequate understanding of the complex relationships between behavior activities and suspicious attack from inside user or insider threat, it is not sufficient to simply identify the mutual influences between technologies and human actions. This context is important because attitude and ability of each user varies, which in turn has implication for the activity of higher transaction size and concurrent connection, which definitely affects the reliability (Performance, Availability and Security) of the overall network.

Therefore, we can summarize that the behavior is an effective way to identify and detect threat from habitual activity. Additionally, as a basis, we have a special characteristic unique that can be used for habitual activity motivation to provide the obviously extended user motivation. These proposals have a novel approach to improve monitoring behavior user in stream network.

From habit activity of user, we can generate profiles of user behavior. The user profiles have to be updated periodically to include the most recent changes frequently. From the proposal (Yin et al., 2004), it describes method for anomaly intrusion detection on linear prediction and Markov chain model; they combine it with signature verifi-cation to detect attacks more efficiently. They introduced a method for detecting intrusion based on the temporal behavior of application that used data from University of New Mexico (cs.unm.edu/~immsec/data-sets.htm).

PROBLEM ANALYSIS

The essential thing in network security is to monitor and analyze network traffic for profiling user behavior. A robust defense system has to hold parameters representing both normal and abnormal user behavior patterns, and such parameters require to be recalibrated consistently to adjust for changes in network and user behavior over time. Therefore, we can summarize the behavior as an effective way to identify and detect threat from habitual activity. Kim et al. (2010) presents the behavior of the user who uses social website and also how to attempt to organize their status, uses, and issues of social web site into comprehensive framework. This is for discussing, understanding, using, building and forecasting the future of social web sites. There was mapping behavior user who uses the social website (behavior user individual, businesses and government). Thus, from the proposal (Wang et al., 2009), the influence of user motivations and emotions factors on user behavior in the web 2.0 environment has been examined. Like wise, the proposal (Oh and Lee, 2003), present taxonomy in which the most relevant features of current solutions are included. Thus, the network feature were analyzed; the type of behavior model and the scale of analysis have been proposed as basic criteria to classify current methods as well as key notions to the problem itself. They present the methods based on the analysis traffic flows with divided case study. Additionally from Frias-martinez et al. (2009), they have clustering automatically into cluster that define the access policies; experiment show that the mechanism is effective in detecting attack.

From habit activity of user, we can generate profiles of user behavior; user profiles have to be update periodically to include the most recent changes frequently.

Unfortunately, in previous work, researchers focused on the signature system, attacked from outside, and taxonomy model attacked without discussing how to analyze and recognize normal activity of trusted users from inside network. In our thoughts and observations, attack from inside is unpredictable, able to beat defense system, at last success to access.

The performance of IPS is measured by how well the system can accurately predict and prevent intrusion and low false positive rate in stream network. Currently, accuracy for identify attack (with low False Negative), threat assessment and content application analysis is the main object of the research. Another important which needs to be detected is the sensor's ability to understand and interact with other layer in network protocol stack. This is due to each layer a sensor interacts to perform analysis using a range of data analysis techniques. We assumed accurate and timely detection of security violation event critically depends on the location of sensors in a networked system. The proposed system will overcome the limitation of the existing system and it also includes some additional features.

Furthermore, as mentioned previously, this raises the questions of: (i) How to improve the accuracy of detection and reduce the false alarm? (ii) How to efficiently and effectively design and implement an intrusion prevention based on behavior-based to detect know and novel attack? and (iii) How to identify security threat in peek network that demand new monitoring measured to be deployed, especially attacker that are the inside users.

Behavior user

Here, we described a mapping from various disciplines and areas of the interaction process between technology and user. We focus on concepts that are useful to describe and analyze relation between users and network system; these concepts may be determinants, but in disciplines area, such as researcher in psychology and social area term that encompass more complex activities via logging data from a particular application, and (iii) methods. For a

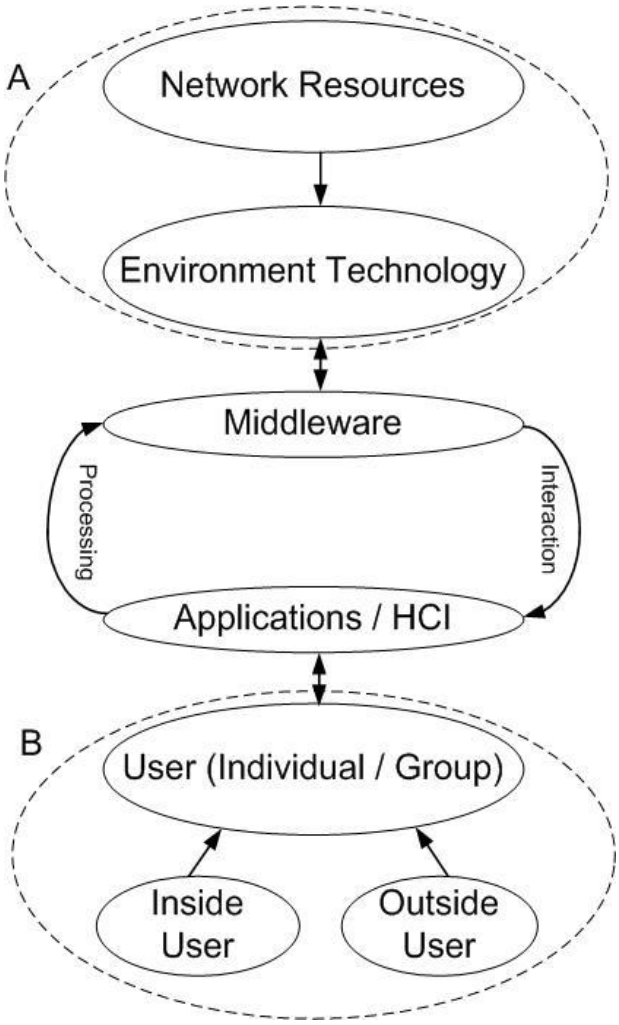


Figure 1. Interaction users and network.

comprehensive understanding of the complex relationships between behavior activities and suspicious attack from inside user, it is not sufficient to simply identify the mutual influences between technologies and human actions.

Verbeek (2006) proposed explanation between technology and behaviour is examined on relation of man-made environment and psychological process. As in Figure 1, we present a component of the model and their interaction based on given network technology and user. In mark A; there are (i) network resources: Database, query, dataset, etc, and (ii) environment technology: router, switched, firewall, authentication systems, etc. Here, network resources and environment technology are very concerned about update, standard interface, proprietary, system connections, and reliability.

While in mark B, mapping shows that there are several conduct from user, such as attitude (naïve or loutish), habitual activity, perceived control, subjective norms intention, occasion timing, planning, and ability. Two user categories are divided inside and outside, that have similarities in mark B. Layer applications/ HCI is a middleware to become translated and query interaction / processing between A and B. Therefore, we see the implication of this interaction is ethical. In performed observation by Wang et al. (2009), HCI uses one of three approaches to gather user behaviour information: (i) Videotaping of user activities; (ii) Recording of user. Using an unobtrusive application that exists in the background across all the application installed on the index machine.

According to Qiao et al. (2007) which present behaviour analysis-based learning framework for host-based intrusion detection, they focused on the verification of unknown and new types of attacks based on host behaviour analysis. From this experiment, they have described more accurately and comprehensively with a set of indicators which are the user profile, program profile, and system resource access. Performed work (Rhee et al., 2009) concluded the survey as evidenced previously, there are some naïve user behaviours that are not intended but some may cause detrimental effects on information security, which use social cognitive theory and explore its viability as a framework for understanding factors influencing end users control-enhancing behaviour.

Insider user

Attacks that come from inside the network are very difficult to detect, because defense system will think that it is a normal activity. Previously, Rhee et al. (2009) proposed security practice behavior and motivation as a mean to strengthen security efforts. From result of a study where they provide support, there are several hypothesize relationship between user behavior and security factor. Proposed work by Kim et al. (2010) identified effect of behavior, and they present typical access uses of social web site, and Wang et al., (2009) demonstrated that emotions affected users perceived belief in the new emergence applications with positive and negative emotion. Our previous work (Stiawan et al., 2010b) proposed an idea to combine data of payload with regular expression (Regex) by comparing the signatures between log of data records to identify and recognize the suspicious packet. Regex can provide a flexible means for identifying strings. Câmpeanu and Yu (2004) and Lo et al. (2008), also suggest the same approach and introduce Regex to identify the string matching and bits-parallelism algorithm can match some regular expression.

Meanwhile, hackers initiate attacks on target machines through multiple attack actions and mechanisms using application script. These multiple single attack actions belong to an attack plan indeed, which the general steps to taxonomy attack. According to top web vulnerability of hacking: (cert.org), (sectools.org), (insecure.org), between rules of intrusion detection (cvs.snort.org) and vulnerability exposures (cve.mitre.org), we assume there are many application script to attack and penetrations vulnerability hole of system.

On the other hand, from the attacker sides (Liu et al., 2008), taxonomy of attack: (i) Probe, the attack looks for a vulnerability of system, the attacker usually do ping addresses, interrogation of DNS and domain; (ii) Scan, the attack uses tools to find a vulnerability holes it finds to compromise the host; scanning is try to find information on how vulnerable a system is; it is can produce information, such as IP address devices, scheme of topology, application systems of running, etc; (iii) Intrusion, the attack installs something on system, uses the compromised host to attack other systems, the attacker try and error to penetration, and (iv) Goals, damage occurs, either through malicious intent or huge amount of network traffic because of propagations, after that, attacker installed backdoor to be easy re-enter the system.

As mentioned previously, we will explore the connection between user behavior and security issues. We assumed that the skills / user's abilities are at the same level. As we shall discuss here, the correlation security system is highly dependent on behavior habitual activity.

Traffic threat assessment

In 1990s, intruders from outside network reflected the predominant

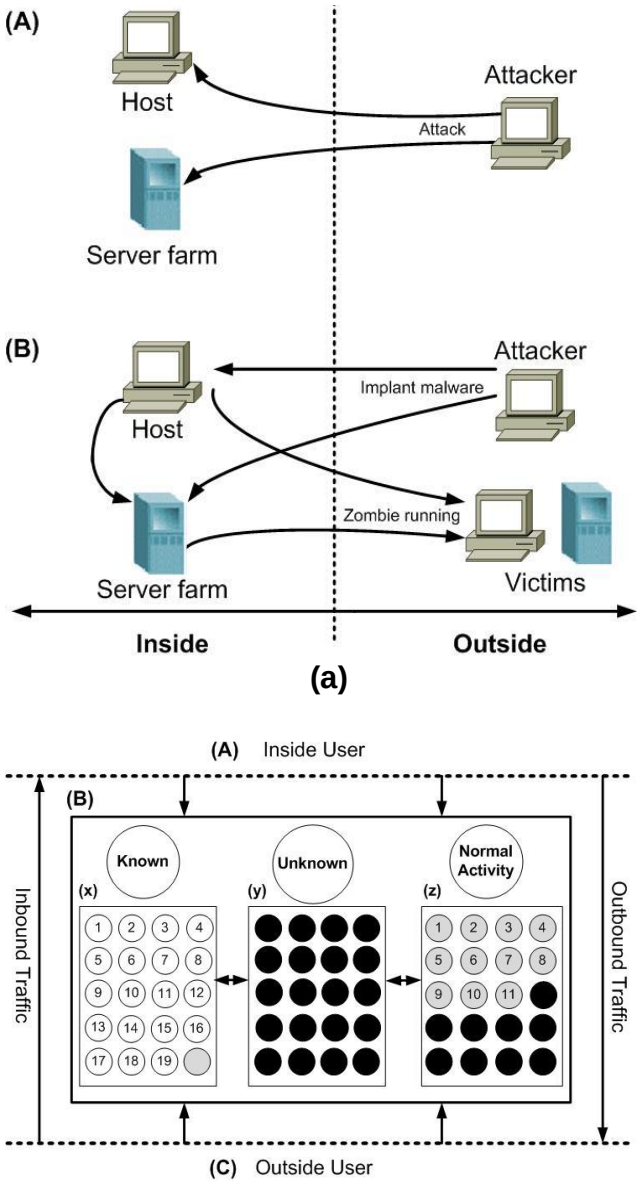


Figure 2. (a) Mark attacker uses host; (A) show simple attacker to system, mark (B) implant malware often attempt to infect and control of privileged. (b) Model of attack. In the mark A, attacker direct penetration to attack network resources. Meanwhile, in the mark B, attacker uses host or server farm to attack network resources.

mode in the defense system technology solutions focused on outsiders gaining unauthorized access to exposed network resources: Servers Farm (web, mail, FTP, database, DNS, and application). Furthermore, refering to RFC 1918 and statistical data from our training data, inside user can also be a serious threat. In the mark B from Figure 2a, we describes how the attacker uses host to attack inside or outside network resource, which is implant malware often attempt to infect and control of privileged. After that, the infected host/server can be a zombie for attack later.

Here, we described the approach in reducing the amount of traffic analyst whereby the user must inspect first before the activity damage and network resources are accessed. Unfortunately, it is very complex to identify and recognize a normal activity, suspicious or malicious. We proposed a mechanism to recognize whenever any traffic is allowed to pass from other defense system to any host in outside or resource to our network.

In mark A and C from Figure 2, we divided user into two which is the inside user and outside user, we categorized inside user as a user / groups from our internal or has authentication valid from our system. In mark B(x, y, z) we described as known, unknown and normal activity, suspicious threat, as shown in Table 1.

Furthermore, in mark B (y), we identified as unknown suspicious threat, this condition is unknown / undetected, which we can put regulation rules to allow and log or deny, because some activity need a new emergence application which is not included in database signatures. We identified several applications and resources undetected as suspicious threat or malicious threat, this will be a threat after detection of intrusion. In Figure 3, we proposed two typical interrelation data, (a) Unknown activity have become part suspicious threat, and (b) Unknown can be part of normal activity and suspicious threat. Meanwhile, in mark B (z) we identified the set of normal activity; from our observation, the habitual behavior activity is classified as normal, as shown in Table 2.

Result from the observations is an enabling correlation between mark A in Figure 3, with B (x) and B (z) as in Equation (1).

$$S = \{1, 2, 3, 4, 5, 6, 7, 8, 9, 10 \ldots 29\}$$

$$A \leftrightarrow B(x) = \{1, 2, 3, 4, 6, 7, 8, 12, 13, 14, 16, 17, 18\}$$

$$A \leftrightarrow B(z) = \{19, 20, 21, 22, 23, 24, 25, 26, 27, 28, 29\}$$

$$B(y) \notin \{B(x) \cup B(z)\}$$

$$B(y) = \{\emptyset, \{\ \}\}$$

$$\lambda = \text{condition unknown / undetected / unpredictable} \quad (1)$$

where, B (x) = know suspicious threat; B (y) = unknown / undetected, and B (z) = normal activity.

Meanwhile, there are correlation between mark C in Figure 3, with B (x) and B (z) as in Equation (2).

$$S = \{1, 2, 3, 4, 5, 6, 7, 8, 9, 10 \ldots 29\}$$

$$C \leftrightarrow B(x) = \{1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 16, 17, 18\}$$

$$C \leftrightarrow B(z) = \{19, 20, 21, 22, 23, 24, 25, 26, 27, 28, 29\}$$

$$C(y) \notin \{B(x) \cup B(z)\}$$

$$C(y) = \{\emptyset, \{\ \}\}$$

$$\lambda = \text{condition unknown / undetected / unpredictable} \quad (2)$$

HABITUAL ACTIVITY

From habit activity of user, we can generate profiles of user behavior; user profiles have to be update periodically to include the most recent changes frequently. Qiao et al. (2007) propose a behavior analysis-based learning framework. They use a cluster-based outlier detection algorithm detect for anomalous data and describes behavior set factor of user profile, program profile and system resource usage. Framework that is made is sufficient to analyze behavior in host-based intrusion without explaining about how to capture data in stream network and result of the alerts to be forwarded to response mechanism after identifying attack. Lim and

Table 1. List of known threat.

Mark	Know suspicious threat
B(x)	Virus
	Worm (Trojan, botnet, keylogger, spam)
	Buffer over flow
	Scanning (port scan)
	Input attack (SQL Injections, Cross site script (XSS), RSS Feeds, Google Add sense
	DoS/DDoS (ARP-syn flood, ICMP-UDP Flood, Ping of the death, UDP Stream, Syslog)
	Physical attack (cable tapping, theft)
	Password attack (brute force, dictionary)
	Mail bomb
	Web hacking (spoofing, phishing)
	DNS attack (poison, rebinding, domain redirect)
	Wireless hacking (SSID, phishing/ pharming)
	Malware, spyware, botnet, adware
	Rootkit
	Routing attack (BGP & OSPF poison)
	Network attack (ARP poison, MAC Clone, broadcast storm, ICMP hijacking)
	Java active X
	Social Engineering

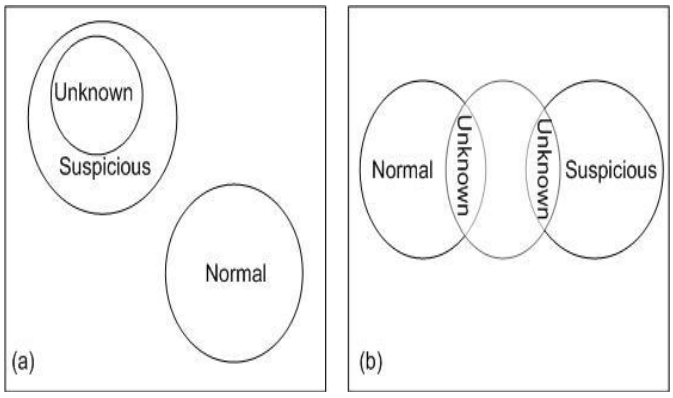


Figure 3. Typical interrelation data.

Table 2. Normal Behavior activity.

Mark	Normal activity
B(z)	WWW
	Collaborative Workspaces
	Download - Upload
	Streaming video
	Data Replication
	Remote Login
	Remote VNC
	Mail
	E-Commerce
	Internet Messaging
	VoIP

Jones (2008) present taxonomy of anomaly detection technique in network-based intrusion. They confirmed the extent of the use misuse-based has been dominant strategy for countermeasure from suspicious attack and divided two approaches for building the behavior model, learning-based and specification-based. On the other hands, Koch (2009) propose using fast-learning modular with neural network based on pre-processed component.

Previously, Galassi et al.'s (2005) experiments described in the following investigate the possibility of automatically constructing a user profile from the logs users activity, and the result from other work (Galassi et al., 2005). is the standard formalism for regular expressions adopted for describing episodes and profiles. This mean, regular expression syntax contains meta-symbols for denoting disjunction and iteration.

We divided and distinguished the normal or curious activity with classes/types number of connection. Connection one to one (that is, Remote login), one to many (that is, Bit Torrent/Slammer), many to one (that is, DoS/ DDoS), and many to many (that is, Ragnarok). In Figure 4, we described and classified the interconnection habitual activity and Table 3, showed number of connection activity user.

Therefore, we can summarize that the behavior is an effective way to identify and detect threat from habitual activity. In Kim et al. (2010), behavior user in using social website and how they attempt to organize the status, uses, and issues of social web site into comprehensive framework for discussing, understanding, using, building and forecasting the future of social web sites. They was mapping behavior user to uses of social website (behavior user individual, businesses and government). Wang et al. (2009) has examined the influence of user motivations and emotions factors on user behavior in the web 2.0 environment. Like wise, Oh and Lee (2003) presented taxonomy in which the most relevant features of

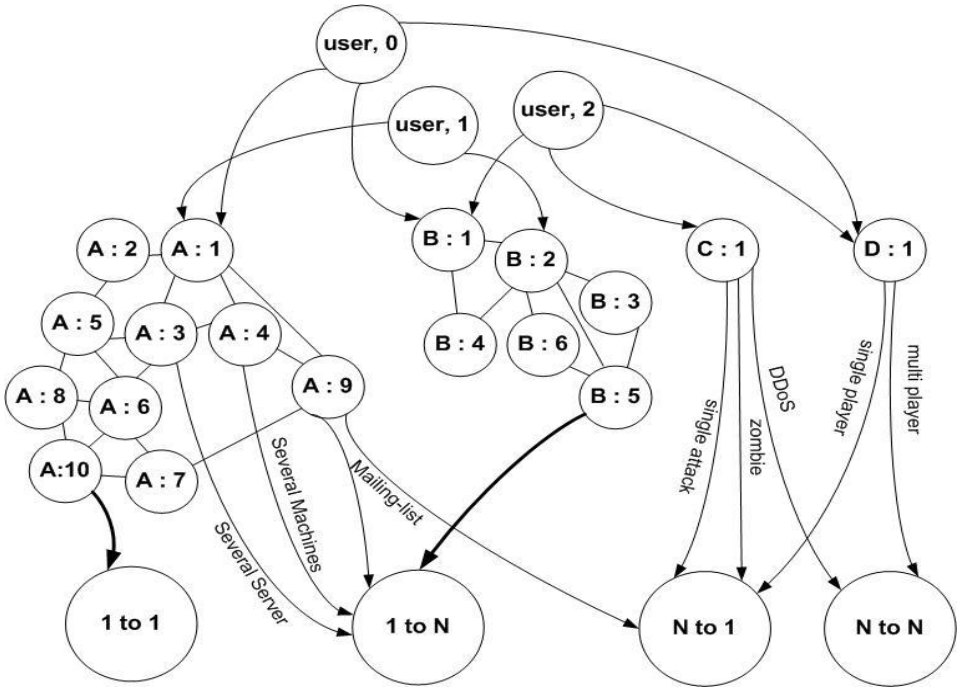


Figure 4. Classify and identify behavior user.

Table 3. Number of connection of activity user.

Connection	Activity user
A (1 to 1)	WWW
	E-commerce
	Remote login
	Remote VNC
	Data replication
	FTP
	Update process
	Download-upload
	Mail
	VoIP
B (1 to N)	Peer sharing
	Internet messaging
	Collaborative workspace
	Streaming video
	Scanning
	Spamming
C (N to 1)	Flooding (DoS / DDoS
D (N to N)	Games online

current solutions are included. Thus, the network feature analyzed, the type of behavior model and the scale of analysis have been proposed as a basic criteria to classify current methods as well as key notions to the problem itself. They present the methods based on the analysis traffic flows with divided case study.

From our observations, there are two habitual behavior activities; (i) media rich with activity higher transaction size, and (ii) transaction with activity concurrent connection, as shown in Tables 4 and 5.

Intrusion prevention system

In real traffic, there are many packet data, audit data were manually inspected to identify network traffic which is impossible and was expensive, time-consuming, and inaccurate due to the extremely large amount of data to be audited. Whereby, solution to identify and recognize security violation is urgently needed. Intrusion Detection System (IDS) have been actively investigated by researchers for about two decades. Obviously, IDSs is one of the solutions of defense system for organization and in other sides many researchers continue to develop it.

Currently, IDS technologies are not very effective against predicting a new mechanism of attack. There are several limitations, such as performance, flexibility and scalability. In other words, Intrusion detection is passive, and cannot be expected to detect all malicious and malicious activity at all time and uncompatible to integrate with control restriction to stop traffic inbound-outbound from attacking, which means only to detect attack actions, without preventing it.

Some reported work (Fuchsberger, 2005; Ahmad et al., 2010), describes of the fundamental IDS and IPS; currently IDS can be seen as a traditional second line of defense system, which is becoming more difficult to apply security access control. On contrary, IPS can be used to alarm on attacks within a network and provide for acting on attack preventive with Firewall and IDS function mechanism. Ollmann (2003) outline the future trends of IPS is functionality such as: Gateway appliance, perimeter defense appliance, all-in-all capability, and network packet inspection/ prevent. Shaikh et al. (2009) challenges intrusion detection for early detection. We argue the intent early detection is main concept of

Table 4. Level of higher transaction size, between more transactions per connection.

Activity	Application
WWW	Browsers, http
Collaborative workspaces	Google Apps, Google Readers, blogs
Download - upload	P2P, FTP, updates process: System Operation, Anti Virus, Applications
Streaming video	You Tube, Real time, Quick time, YM Webcam.
Data replication	Backup data, mirroring data in other sites.
Remote Login	SSH access, WinSCP, Putty
Remote VNC	(Remote desktop), to other remote PCs in network.
Mail	SMTP, POP, IMAP

Table 5. Level of concurrent connection, between higher connection rates.

Activity	Application
E-Commerce	https
Internet messaging	YM!, mIRC, ICQ, Pidgin, Adium, GTalk, Skype.
VoIP	Skype, YM Voice.
Game online	Ragnarok, HalfLife, Age of Empires, Ayo Dances
Scanning	Scanning port using script tools

IPS. They describes toward trend of behavior analysis to efficient data collection, improve the performance of sensors in the real-traffic network, due to network traffic capture on high-speed links is always a challenge to capacity issues.

Intrusion detection and prevention system must address three challenges comprehensively: Accuracy, performance and reliability. Accuracy is concerned with identify and recognized threat with produce alarm; performance is measured by impact to accurate task of each system, and reliability encompasses overall accuracy and performance system. Schultz (2004) and Schultz and Ray (2007) defined IPS as consisting of classes of harmful system behavior. The types of events they attempt to produce in the targeted system prevent systems from engaging in certain action.

Recently, intrusion detection system uses management traffic in real-traffic for accuracy detection, increasing and decreasing false alarm rate. In some instances, intrusion prevention system adopts techniques from intrusion and early detection, such as detection approach, monitoring sensor, and alert mechanism, as illustrated comparison of IDS and IPS in Figure 5. Fortunately, IPS is a new approach system which combines the technique firewall with that of the intrusion detection properly. Defense system has become essential component of computer security to predict and prevent attacks; it needs the framework that cooperates with several connected and related components for accurate, intelligent, adaptive and extensible which consists of components that are composite to an integrated system.

Experiment and data sets

For the observation research, there are four segmentation network chosen for sampling data for a data set. As shown in Figure 6, we illustrated the topology network. We use SNORT for packet analysis and multi-router traffic graph (MRTG) network management, freely available tools under the terms of the GNU General Public License for monitoring traffic and network utilization. MRTG can generate HTML pages containing graphical images that provide a near-real-time visual representation on this traffic. In this case, we compare result from MRTG and Netflow to define a flow in RFC 3954.

In this experiment environment, we use network existing to captured and monitor data in real-traffic. The experimental of this approach was integrated into the one subnetting of the Universiti Teknologi Malaysia network, which comprises 100 computers. In the existing network topology, they connected to distribution and access layer network. Running well and composite connected to ISP, we use load balancing based to optimize the bandwidth.

The machines run well on Fedora 11 with 2.0 GHz Xeon processor, using 2 GB RAM to tap a stream traffic network, and wireshark and Snort to tap the stream network. It was set up on the machine to capture traffic from interface network. Therefore, we have produce payload 150 MB/s from tapping captured overall process.

CAPTURING DATA

In this case, as illustrated in Figure 6, we must find a way to capture network traces: (i) SPAN ports: Switched Port Analyzer, for this research, we called it port monitoring, the main reason we used this method is because SPAN port is a popular packet collection of tools as they preserve full duplex link, and (ii) Taps: taps located between two network devices, such as router or firewall, main switching and distribute switching, or host and an access switching. Taps preserve the full duplex nature of modern switched links.

We use Gigabit Ethernet card with 33 MHz Peripheral Component Interconnect (PCI) slot on a server. We capture using wireshark to examine stream traffic from Ethernet 0 and Ethernet 1; (i) sensor 1 uses its interface eth0 to capture traffic sent to it from the routing and filtering function; access to this interface by other packets should be denied by firewall rules, and (ii) sensor 2, uses its interface eth1, to capture traffic set to it packet from inside network.

EXPLORATORY OF OUR APPROACH

Here, we described the process of recognizing a detailed suspicious threat. We identified the habitual activity previously mentioned,

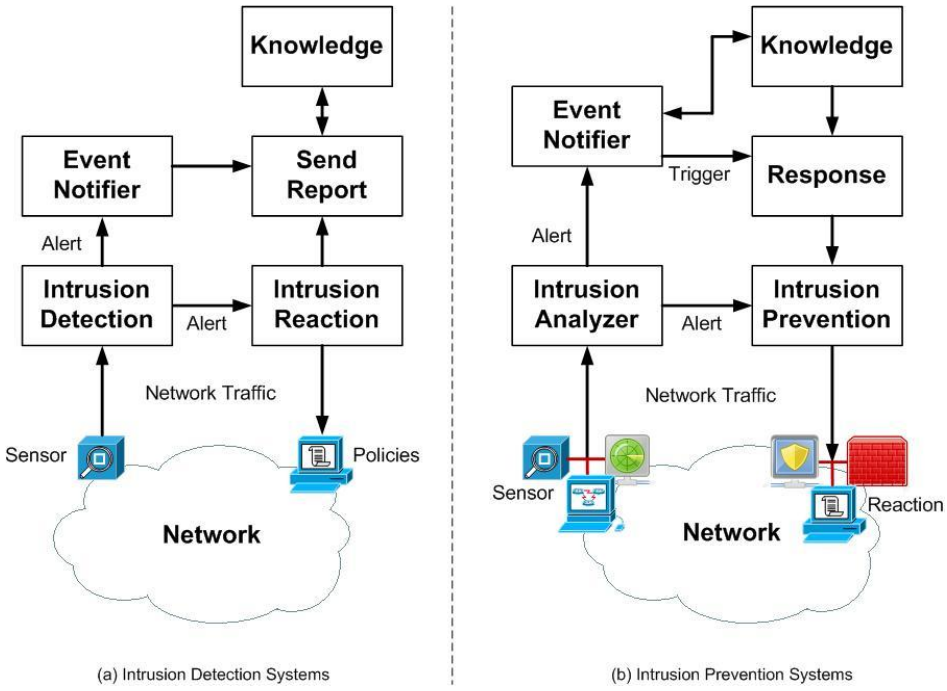


Figure 5. Illustrated comparison IDS and IPS.

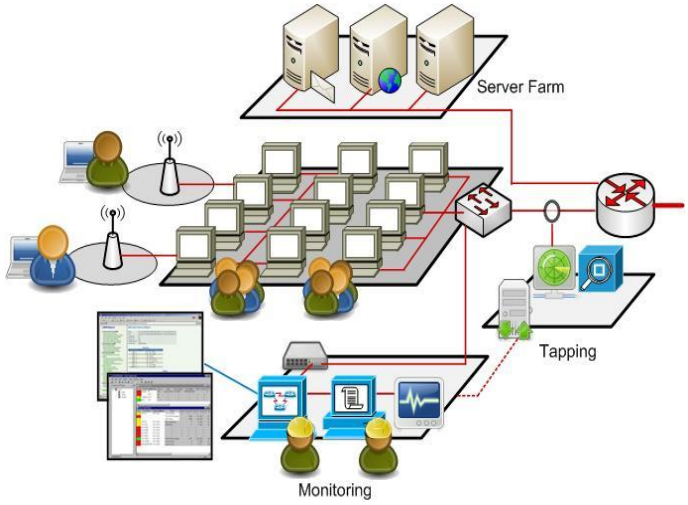


Figure 6. Topology of network.

which are the behavior activity levels. We described the Algorithm 1 in order to identify and recognize mechanism clearly. Algorithm 1 list as follows:

Algorithm 1: Identification and declaration packet data

type packet_data record, Parameters *on* Table 1
precision identification result
r_r risk rating
packet_data = 1//input data between real-time detection
while packet_data <> 0 do
identification (precision)
risk_rating (precision, rr)
trigger (precision)
event_response (precision, r_r)
end while
Procedure Identification (precision)
read (packet_data)// refers from Table 1
if packet_data = rule **then**
precision is block
else if packet_data ≠ rule **then**
precision is allow
else if packet_data ≠ rule and suspect **then**
precision is log
else
precision is report
end if
end procedure

procedure trigger (precision)
read (precision)
if precision= allow **then**
alarm = TN
else precision = block **then**
alarm = TP
else if precision = log **then**
alarm = FP
else
alarm = FN
end if
end procedure
Procedure
risk_rating (precision, r_r) //precision
if precision = block **then**
r_r is high
else if precision = log **then**
r_r is medium or r_r is low
else precision = report **then**
r_r is low or r_r is information
end if
end procedure

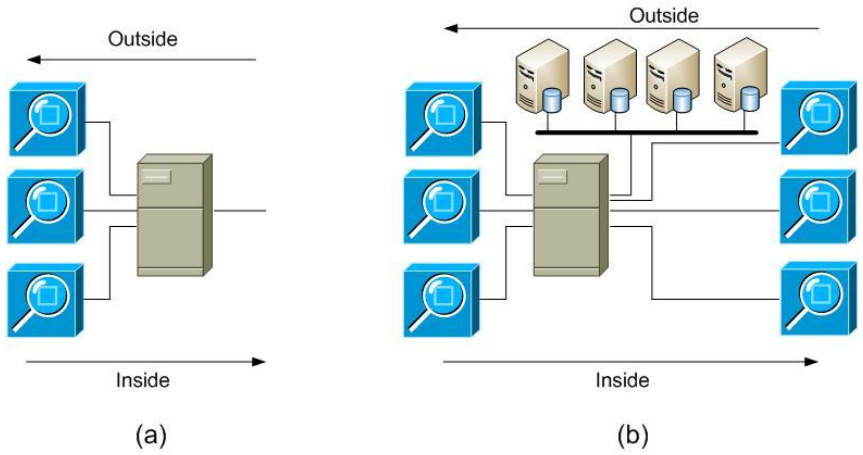


Figure 7. In mark (a) we illustrated the machine with single processor with spread sensors, and mark (b) we uses multiple sensors paired with multiple processors.

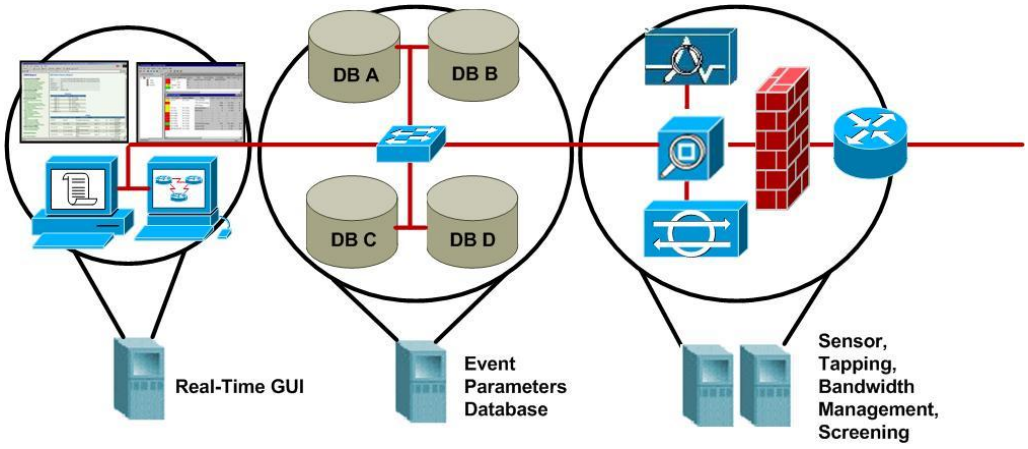


Figure 8. Prevention environment.

Implementations

We located and provided one server running Fedora to tapping traffic. Furthermore, Wireshark were set up on the machine to captured traffic from interface every segmentation network. An essential in network security is to monitor and analyzed network traffic for profiling user behavior. A robust defense system has to hold parameters representing both normal and abnormal user behavior patterns, and such parameters require to be recalibrated consistently to adjust for changes in network and user behavior over time. From our observation, we can describe profiles user with convention continuously activity access, it is we called habitual activity. Therefore, we can summarize that the behavior is an effective way to identify and detect threat from habitual activity. Additionally, as a basis, we have a special characteristic unique that can be used for habitual activity motivation to provide the obviously extended user motivation.

In this initial research, we used two designs strategies for testing and implementation hybrid machine in real-traffic network; (i) single processor paired with multiple sensors, and (ii) multiple processors with heterogeneous sensors. For betterment, it is more appropriate if we categorize the scopes of network topology based on amount of traffic and user: (i) Small Office Home Office (SOHO); (ii) Small Medium Business (SMB), and (iii) Enterprise.

We use four servers for this system, as illustrated in Figure 8; (i) Operating System Fedora 11 with 2.0 GHz Xeon processor and 2 GB RAM, which is running, tapping using tcpdump and wire shark, filtering and screening based IP Tables, and bandwidth management using CBQ; (ii) Machine for Running of Snort based on Fedora 11; (iii) Running well in Windows 2003 with SQL server to running event parameter four relationship databases with 1 GB RAM and Pentium 2.7 GHz Dual-Core processor; and (iv) Based on Fedora 11 to run the network management and control security management with BASE. Furthermore, this machine was located in node. This approach allows a set of active firewall and intrusion prevention to analyze, identify and screen stream packet on subnet broadcast.

EXPERIMENT RESULTS

The captured data is performed for six days continuously available processing package, presented in Table 6. The

Table 6. Packet processing.

Day	Packet	Avg/s	UDP (%)	TCP (%)
1	36.637	65.886	14.87	80.99
2	311.961	20.421	44.43	50.00
3	787.252	25.726	47.83	45.97
4	907.860	17.410	31.90	56.50
5	449.217	26.761	32.12	65.56
6	347.777	31.891	39.71	57.75

Table 7. Application running by user.

Activity	Application
Websites	Technologies such as XHTML, CSS 2.0, Ajax, Flex (www.go2web20.net) with dynamic content Social network (FB, Twitter, MySpace, Flickr, Multiply, etc)
Blogging	WP, Blogger, etc
Video treaming	youtube, mivo.tv, real time player, http://utmotion.utm.my
Chatting	YM!, MiRC, etc
E-learning	http://elearning.utm.my
Radio streaming	Real player
Teleconference	Skype
VoIP	Skype, YM! Voice, etc
Games	Ragnarok, Ayo Dance
Download – Upload	P2P, Update antivirus, SSH Connection, FTP Connection , Backup / restoration data
Collaboration groups	Google reader, Google.com/ig , Google Calendar, scholar, Google Map, Google news, Google blogs, etc

network topology is an active network that is used in everyday activities, then by controlling the content for the Web 2.0 look, where the arrangement is done by dividing the number of users to run a particular application at the specified time to see the pattern.

We divide the user to run multiple applications jointly for the purpose to obtain a unique pattern of Web 2.0 looks. There are several applications running by users, presented in Table 7. Results from wireshark processed by generating a csv file was compared with the results of the output from netflow and weather map which is device supports SNMP.

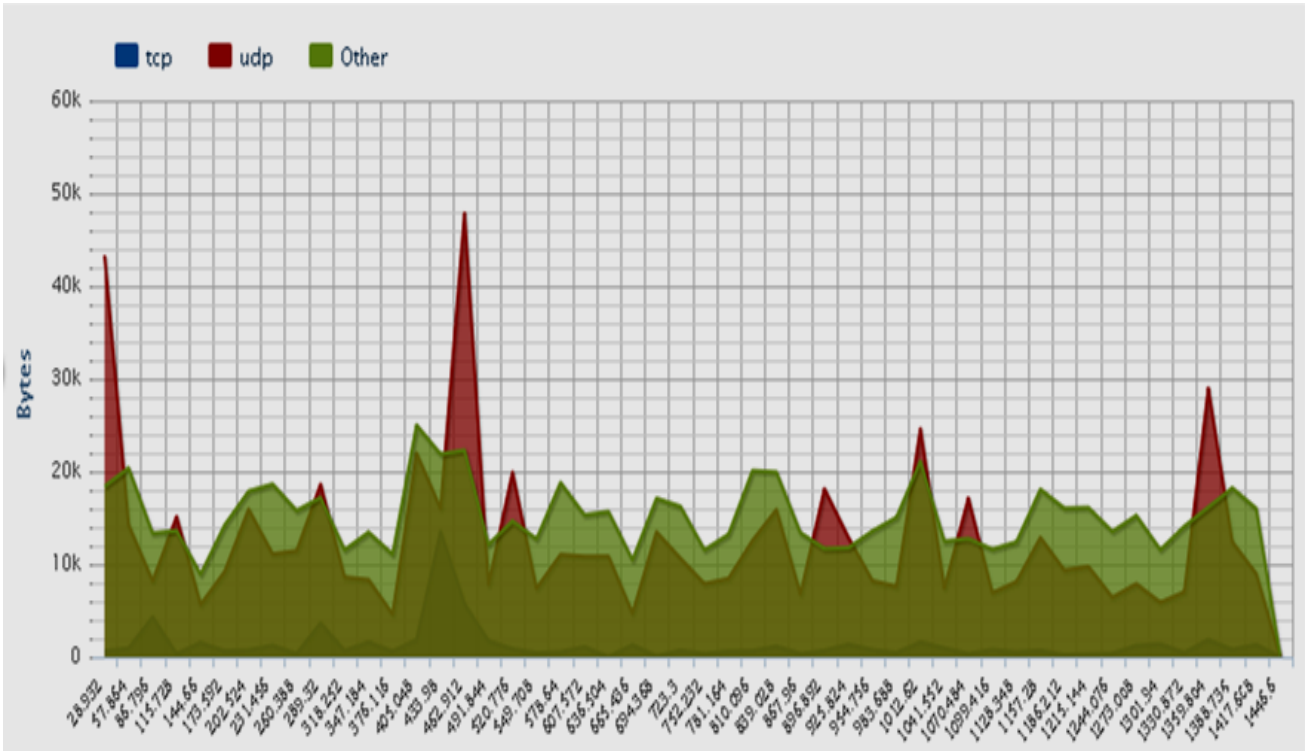
In Figure 9, mark (a) is presented utilizing the dominant protocol used, mark (b), shows the IP addresses of users in interacting within the network at a certain time where it is seen that some high interaction were used to the gateway and to a certain IP. Results from the processing process of user utilization, calculated by byte are presented in mark (c). Furthermore, mark (d) shows the network graph in real-traffic on the network.

The differences between Shouman et al. (2010), Zhang et al. (2008), Dutkevych et al. (2007) and our approach method are as follows: (i) This approach uses network-based and behavior-based to evaluate habitual activity from inside users; (ii) our approach emphasizes more on accuracy and precision to identify and recognize intrusion threat, and responses for this event; (iii) our system checks each packet only once on its way to its destination, which function in layers data link, network and application; and (iv) this system emphasizes more on the accuracy of attack, matching with events in parameters database.

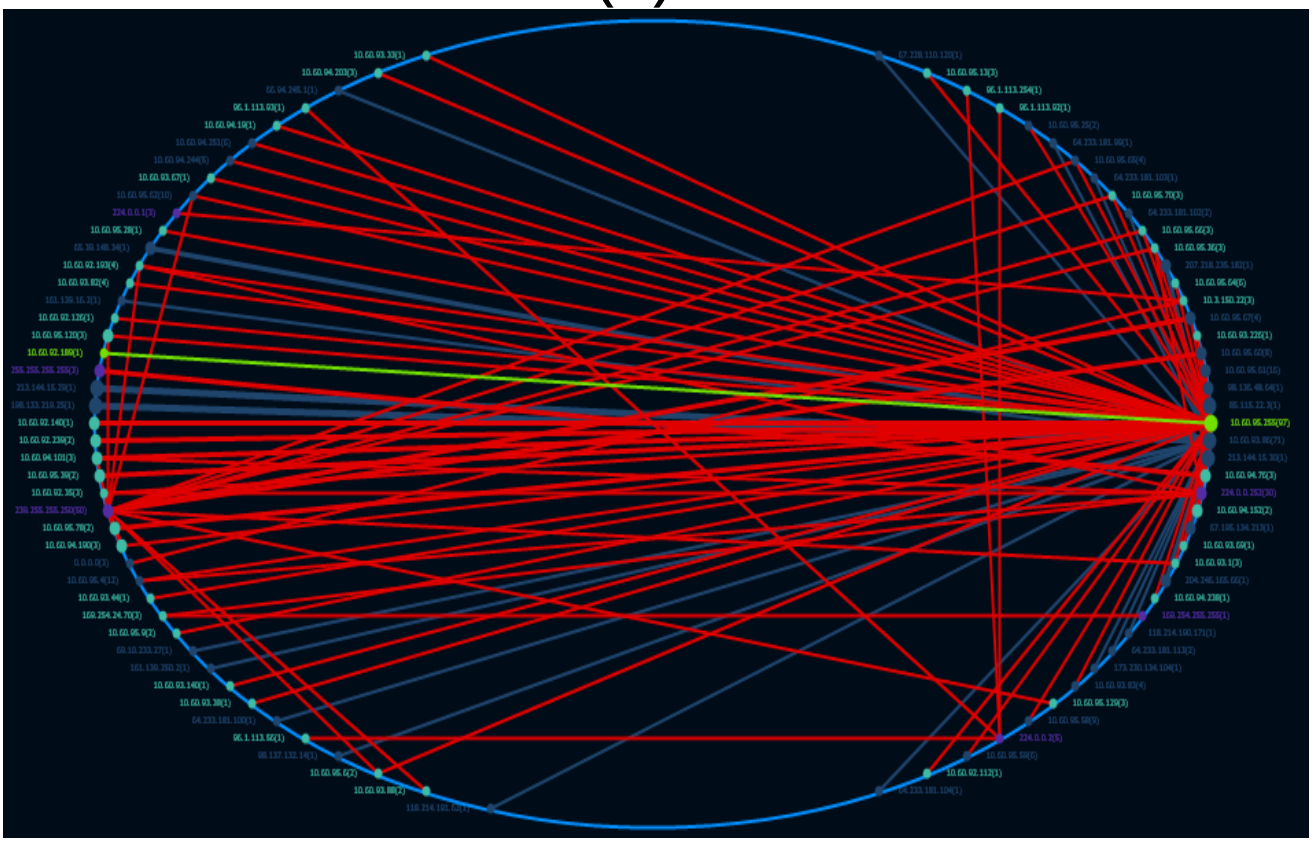
CONCLUSION AND FUTURE WORKS

IPS has successfully become an integrated solution for integrated security system solutions; today many researchers are performing experiment and research for an integrated security system solutions based on IPS, which continue to develop an integrated research to improve various aspects of major issues in social studies, such as accuracy, precision, prevention, and response algorithm

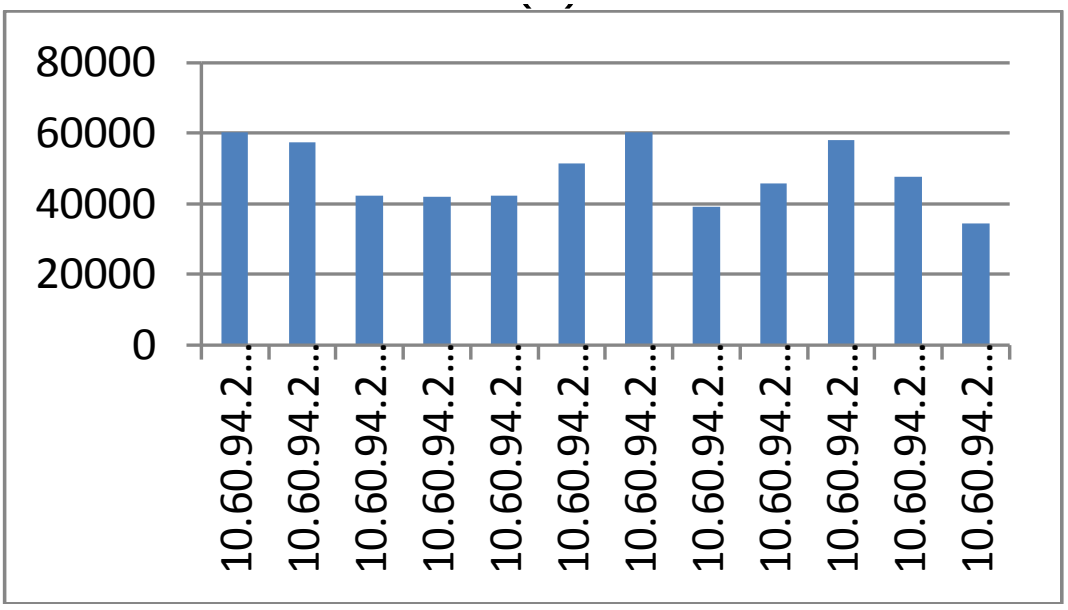
The Behavior-based detection is complex. In fact, multiple problems can be identified by real-time traffic from internal users, under a variety of normal activities. In this paper, we presented the identification and recognition through the behavior-based detection and prevention of an attack with analyzed real-traffic from habitual activity of internal users. Indeed, we have suggested an



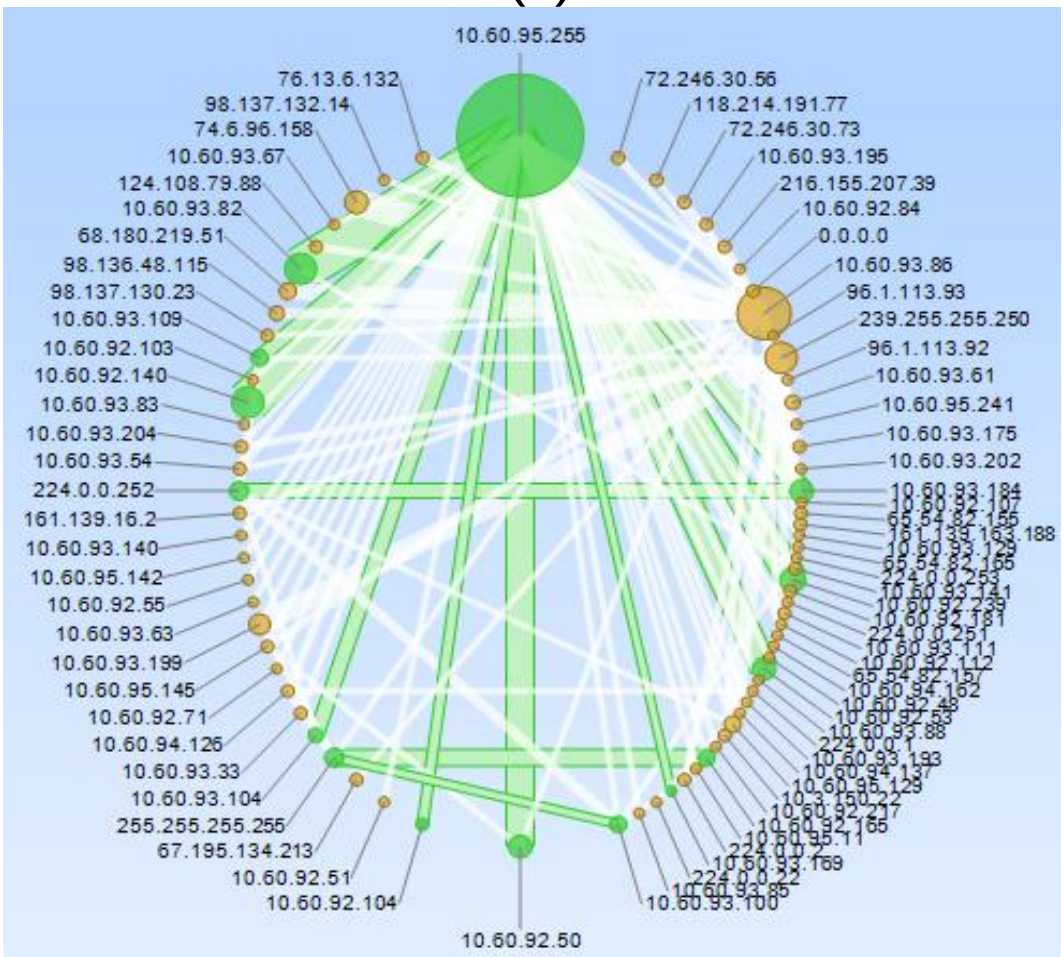
(a)



(b)



(c)



(d)

Figure 9. User profiling statistics. Graphs (a) illustrate protocol usage at each node, (b) top 100 network IP Address, (c) user usages, and (d) IP conversation.

IPS technique which is based on habitual activity from inside user. This approach proves interrelation between behavior user and security factor, attack classification with traffic threat assessment, and describes accuracy sensor with algorithm approach. In the future, we will experiment with a benchmark of algorithm with other approach in a real-traffic network.

ACKNOWLEDGEMENTS

This research is supported by The Ministry of Higher Education and collaboration with Research Management Center (RMC) Universiti Teknologi Malaysia with Vot Number: Q.J130000.7128.00J40.

REFERENCES

Ahmad I, Abdullah, A, Alghamdi A (2010). Towards the selection of best neural network system for intrusion detection. Int. J. Phys. Sci., 5(12): 1830-1839.

Câmpeanu C, Yu S (2004). Pattern expressions and pattern automata. Informat. Proc. Lett., 92: 267-274. doi:10.1016/j.ipl.2004.09.007

Dutkevych T, Piskozub A, Tymoshyk N (2007). Real-Time Intrusion Prevention and Anomaly Analyze System for Corporate Networks. IEEE International Workshop on Intelligent Data Acquisition and Advanced Computing Systems Technology and Application, pp. 599-602.

Frias-martinez V, Sherrick J, Stolfo SJ, Keromytis AD (2009). A Network Access Control Mechanism Based on Behavior Profiles. Annual Computer Security Applications Conference, pp. 3-12. doi:10.1109/ACSAC.10

Fuchsberger A (2005). Intrusion Detection Systems and Intrusion Prevention Systems. Information Security Technical Report, 10: 134-139. doi:10.1016/j.istr.2005.08.001

Galassi U, Giordana A, Mendola D (2005). Learning User Profile from Traces. 2005 Symposium on Applications and the Internet Workshops (SAINT 2005 Workshops), 166-169. Ieee. doi:10.1109/SAINTW.2005.1620003

Kim W, Jeong OK, Lee SW (2010). On social Web sites. J. Inform. Syst., 35: 215-236. doi:10.1016/j.is.2009.08.003

Koch R (2009). Changing Network Behavior. 2009 Third International Conference on Network and System Security, 60-66. doi:10.1109/NSS..55

Lim SY, Jones A (2008). Network Anomaly Detection System: The State of Art of Network Behaviour Analysis British Telecommunications plc ., Security Research Centre, Ipswich, United Kingdom. Int. Confer. Converg. Hybrid. Inform. Technol., pp. 459-465. doi:10.1109/ICHIT.96

Liu Z, Wang C, Chen S (2008). Correlating Multi-Step Attack and Constructing Attack Scenarios Based on Attack Pattern Modeling. 2008 International Conference on Information Security and Assurance, pp. 214-219 doi:10.1109/ISA.2008.11

Lo C, -tien D, Tai Y.-gang, PK, Antonio S (2008). Hardware Implementation for Network Intrusion Detection Rules with Regular Expression Support. Design, pp. 1535-1539.

Mizutani M, Takeda K, Murai J (2009). Behavior Rule based Intrusion Detection. ACM International Workshop CoNEXT, pp.57-58.

Oh SH, Lee WK (2003). An anomaly intrusion detection method by clustering normal user behavior. Computers. Security, 22(7): 596-612.

Ollmann G (2003). Intrusion Prevention Systems (IPS) destined to replace legacy routers. Network Security, 11: 18-19.

Qiao H, Peng J, Feng C, Rozenblit JW (2007). Behavior Analysis-Based Learning Framework for Host Level Intrusion Detection. Proceedings of the 14th Annual IEEE International Conference and Workshops on the Engineering of Computer-Based Systems (ECBS07).

Rhee HS, Kim C, Ryu YU (2009). Self-efficacy in information security: Its influence on end users' information security practice behavior. J. Comput. Security, 28: 816-826.

Schultz E (2004). Intrusion prevention. Computers & Security, 23: 265-266. doi:10.1016/j.cose.2004.04.004

Schultz EE, Ray E (2007). Future of Intrusion Prevention. Comput. Fraud. Security, pp. 11-13.

Shaikh SA, Chivers H, Clark JA (2009). Towards scalable intrusion. Network Security, June (6), pp. 12-16. Elsevier Ltd. doi:10.1016/S1353-4858(09)70064-9

Shouman M, Salah A, Faheem HM (2010). Surviving cyber warfare with a hybrid multiagent-based intrusion prevention system. IEEE Potentials, pp.32-40.

Stiawan D, Abdullah AH, Idris MY (2010a). The Trends of Intrusion Prevention System Network. International Conference Education Technology and Computer (ICETC) 4: 217-221). Shanghai, China: IEEE. doi:10.1109/ICETC.2010.5529697

Stiawan D, Abdullah AH, Idris MY (2010b). The Prevention Threat of Behavior-based Signature using Pitcher Flow Architecture. Int. J. Comput. Sci. Network Sec., 10(4): 289-294.

Stiawan D, Abdullah AH, Idris MY (2010c). Classification of Habitual Activities in Behavior-based Network Detection. J. Comput., 2(8): 1-7.

Stiawan D, Abdullah AH, Idris MY (2011). Characterizing Network Intrusion Prevention System. Int. J. Comput. Appl., 14(1): 11-18. doi:10.5120/1811-2439

Verbeek PPEA (2006). User Behavior and Technology Development : Shaping Sustinable Relations between Consumer Technology, pp. 385-399. Springer.

Wang CY, Chou S.-cT, Chang H-c (2009). Emotion and Motivation : Understanding User Behavior of Web 2.0 Application. IEEE Computer Society Seventh Annual Communication Networks and Services Research Conference, pp. 1341-1346. doi:10.1109/ITNG.2009.205

Yin Q, Shen L, Zhang RU, Li X, OC, Science C, Engineering H et al (2004). Based on Behavioral Method Based on Behavioral Model. Analysis IEEE Proceeding of the 5th World Congress on Intelligent Control and Automation, pp. 4370-4374.

Zhang J, Zulkernine M, Haque A (2008). Random-Forests-Based Network Intrusion. MAN and Cybernetics, 38(5): 649-659.