Classification of Habitual Activities in Behavior-based Network Detection

Deris Stiawan, Abdul Hanan Abdullah, and Mohd. Yazid Idris

Abstract— this paper presents a new method to detect network traffic threats based on packet classification which is result from the identification of insider's habitual activities. We assess the habitual activities by examining regular expression of web applications use by insiders together with the existing server activities log and rules pattern from global update. We capture the packets, analyze the packet and finally, categorize into three main categories whether it is normal, suspicious or malicious. Our method is able to detect threat with low false alarm rate and provides event list handler to rate the risk for prevention purposes. We apply our method to evaluate system security for help security officer (IT Manager and Administrator) to be aware of status network activities.

Index Terms— Intrusion prevention, Accuracy, Precision Alarm, Behavior-based, Habitual Activity

1 Introduction

According to CSI/FBI (www.gocsi.com), over 44 percent of all computer crime and insider abuse comes from internal system. The study asks respondents to rate "internal systems" in 2008. Furthermore, defense systems can identify and recognize intruder attack that is breaking into system. There are several factor, such as : (i) many tools/script to hacking attack from Internet, (ii) behavior user (skill / ability), and (iii) weakness in the internal system. Meanwhile, reports from CERT (cert.org/stats/cert_stats.html), show that the number of incident reported total of catalogue vulnerabilities has increased from only 5.990, to 6.058 Quarterly in 2008.

In general, insider users have privilege as authentication and authorization access to resources. In this case, distinguish between insider threat and outsides /external attack is an insider has greater privilege and knowledge of their organization and can face greater penetration to resources than external attackers (e.g. topology, devices location, mapping network, security control, privilege mechanism and application of assets or targets). Therefore, steps and stages insider attack to penetration attack resource can be possibly easy than penetration from outside attacker. Additionally, In this case reports from CERT (cert.org/insider_threat) corroborate this fact, which is the number of incident reported has evolved from 2004 until in 2010.

The paper is organized as follow. Interaction behavior user with environement resources is describes in Section 2. Section 3 presents the detail threat assessment mechanism. Section 4 we proposed accuracy and risk rating mechanism to identify and recognized threat. Conclusion and future work are shown in Section 5.

- *Deris Stiawan is Ph.D Candidate in Faculty of Computer Science & Information System, Universiti Teknologi Malaysia.*
- *Abdul Hanan Abdullah is a Professor at Faculty of Computer Science & Information System, Universiti Teknologi Malaysia*
- *Mohd. Yazid Idris.Ph.D is a team leader Intrusion and Threat Detection (ITD) group at Faculty of Computer Science and Information System, Universiti Teknologi Malaysia.*

2 Interaction Behavior User

According to [1], proposed the categorized behavior user, such as (i) user characteristics, (ii) user attitude (iii) user knowledge & capabilities, and (iv) user time space. They and explained between technology and behavior and examined the relationship man-made environment and psychological process. As in Figure 1, we present a component of the model and their interaction given network technology and user. In mark A : there are (i) network resources, such as Database, query, dataset, etc, and (ii) environment technology, such as router, switched, firewall, authentication systems, etc, in this section network resources and environment technology is concerned about update, standard interface, proprietary, system connections, and reliability.

While in mark B, mapping show 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 / human computer interface (HCI) is a middleware to become translated and query interaction / processing between A and B. Therefore, we see that the implication of this interaction is ethical.

This idea from proposal [5], their was analyzed of user activity is a natural approach to detect intrusion, experience has showed that it is far from being accurate. It is possible to identify several causes for this change.

Propsosal [3], present malicious motivation, that it comes from personal gain, revenge, ideology or all of the above. They reported 80% insider threats are committed by the most technical and privilege users, with 50% of that event being committed accidentally.

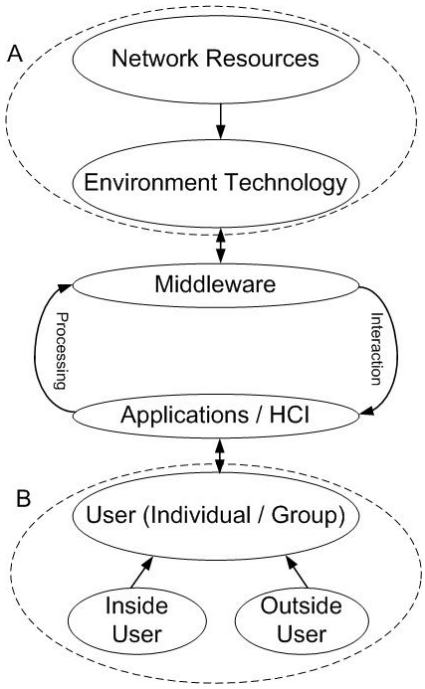

Figure 1. Interaction user with environment resource

According to [4], the concluded survey was evidenced as seen above, there are many naïve user behaviors that are not intended but many 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 behavior.

We assume the skill / ability users have almost the same average. As we shall discuss in this section, the correlation security system highly dependent on behavior habitual activity.

3 Traffic Threat Assesment

Based on these opinion experimental results, we identify habitual activity liked black, white and gray, (i) normal activity: a system consists in observing it while it is working under normal conditions, which is used to measure normality, related to this behavior at one or several time activity, (ii) suspicious activity: conditions of uncertainty between known activity and malicious, (iii) malicious activity : justification detection from anomalies and suspicious attacks, mechanism and method of attack. Thus, the effect is inaccuracy for recognizing and not being able to detect it, and (iv) unknown activity: intersection between normal and suspicious and suspicious and malicious, that implies several consequences and is inconvenience to detecte before update rule in list database.

The ideal approach is to identify and recognized its from variants behavior. An habitual activity can be defined as a properties of network, such as (i) Payload (IP Address, MAC Address, flags, protocol, port, packet size / length, header, fragment, TTL, frame, checksum, type, etc), (ii) characteristics of attack, (iii) match with signature rules of databases global, and (iv) pattern of normal behavior.

3.1 Known Activity

Unfortunately, it is very complex to identify and recognized normal activity, suspicious or malicious, we proposed a mechanism to recognize when any traffic is allowed to pass from other defense system to any host outside or resource in our network. Below as part of TCP/UDP [5], we have as follows:

1. Packets with low TTL values
2. Packets with the same source and destination port
3. Packets containing private IP address and/or other address violations
4. Packets with invalid TCP flags
5. Packet containing zero port number
6. Packet with strict source routing option
7. Too short packet

Characteristics of malicious threat with srcIP = source IP, dstIP = destination IP, srcPort = source port, dstPort = destination port, and proto = protocol, as follows in Table 1. Characteristics malicious event [6], as follows:

1. Network, system, services and information reconnaissance (profiling)
2. Access to assets (profiling)
3. Illicit Data extraction (e.g. printing, write to removable disk)
4. Installation and control of data loggers or malicious software Communication Usage (e.g. P2P, VoIP, encrypted messaging, steganography)
5. Changing file permission
6. Altering file content
7. Erasing file/data

Table 1. Characteristic of malicious threat

Model	src IP	dst IP	src Port	dst Port	Port
Attack	1	N	N	1	135
Attack	1	N	N	N	1025 2745 6129
Buffer Overflow	1	1	1	N	Any
DoS	1	1	N	1	Any
DDoS	N	1	N	1	Any
Spam	1	N	N	N	25 5060
Scanning	1	1	N	1	Any
Port Scan	1	1	N	N	Any

Table 2. Characteristics of normal

Model	src IP	dst IP	src Port	dst Port	Port
Web	1	N	1	N	80
Chat	1	N	1	N	4661
Games	1	N	1	N	4821
DNS	1	N	1	N	53
FTP	1	N	N	N	20
					21
Streaming	1	N	N	1	554
					6970
Mail	1	N	1	N	25
					113
P2P	1	N	N	1	6346
Mail Server	1	N	1		143
					110
					25
					53
					113

3.2 Habitual Activity

From our observation, we can describe profiles user with convention continuously activity access, it is called habitual activity. Proposal [10] present social cognitive theory postulates the reciprocal nature of interaction among behavioral, personal and environmental factors, they use analysis survey with questioner about security aspect in organization. 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 obvious extended user motivation.

Furthermore, from proposal [11],[12], we can include behavior user for mapping habitual activity to our approach, especially interaction behavior and attitude user with the new emergence web 2.0 applications. In addition, as a basis, we hold from them to identify the new emergence application have a special characteristic can be used for habitual activity motivation to provides the obviously extended user motivation.

We divide to distinguish normal or curious activity with classes/types number of connection. Connection one to one (i.e. Remote login), one to many (i.e. Bit Torrent / Slammer), many to one (i.e. DoS/ DDoS), and many to many (i.e. Ragnarok). Furthermore, 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 follows in Table 3 and Table 4.

As in Figure 2, we describe and classify interconnection habitual activity with number of connection of activity user in Table 5.

Table 3. Level of higher transaction size, between more transactions per connection

Activity	Applications
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 4. Level of concurrent connection, between higher connection rates

Activity	Applications
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

Table 5. Number of connection of activity user

Connection	Activity User
A (1 to 1)	1. WWW 2. E-commerce 3. Remote login 4. Remote VNC 5. Data replication 6. FTP 7. Update process 8. Download-upload 9. Mail 10. VoIP
B (1 to N)	1. Peer sharing 2. Internet messaging 3. Collaborative workspace 4. Streaming video 5. Scanning 6. Spamming
C (N to 1)	1. Flooding (DoS / DDoS)
D (N to N)	1. Games online

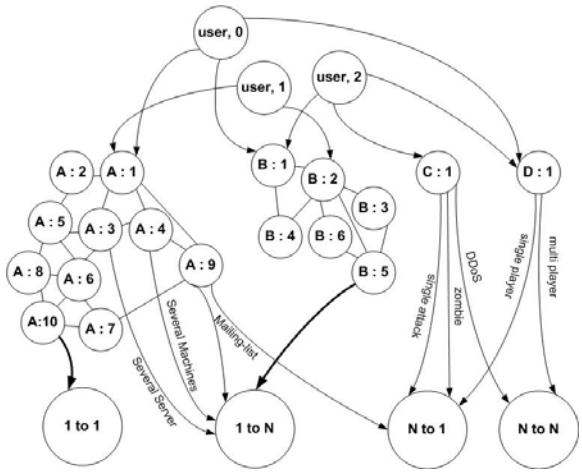

Figure 2. Simple of Classifying

4 Accuracy & Risk Rating

4.1 Accuracy

We believe that the overall performance of this hybrid architecture is better to appropriately identify and recognized threat in network traffic. In our design, we divided three modules which has task. We use modules, (i) filtering and screening, (ii) threat assessment, and (iii) data classify. Furthermore, the module uses two ways to composite, (i) OR-based composite, one (ii) AND-based composite. On security violations we matched, an alarm raised to trigger event response.

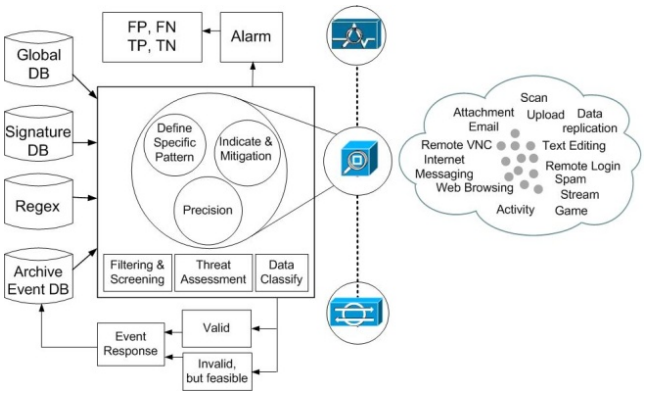

Figure 3. Combining event and list database

As in **Fig**. 3, we depict our approach to increasingly accuracy and precision intrusion threat. We use data mining approach, as the intrusion detection method. This algorithm is capable of solving the match network traffic with database. We utilize data mining technique to construct a filter identify packet data to decrease false alarm. Packet traffic inbound-outbound from router devices in layer network, our approach do not handle of the routing configuration.

In our approach sensor module in interface outbound and inbound by considering each category behavior activity. This is an approach combination with other criteria from collecting in database (regex, achieve, archive event, and signature). Therefore, for one module to connecte database machine, we use spread database to store the events, such as: (i) global database, from update rules identifications global database, (ii) signature database, we uses snort rules, the signature have to be update in the database for future verification process, (iii) regex: regular expression that can be used in selectors to define ranges of values instead of defining each possible value separately, and (iv) archive database: event database, logging system, operating system event, application logs, file system information and reporting log.

(i) *Global database*

```
drop tcp $HOME_NET any -> $EXTERNAL_NET $HTTP_PORTS
(msg:"D BACKDOOR trojan agent.aarm runtime detection -
download other malware"; flow:to_server,established; uri-
content:"/retadpu.php?"; nocase; uricontent:"version=";
nocase; uricontent:"configversion="; nocase; uricon-
tent:"GUID="; nocase; uricontent:"cmd="; nocase; uricon-
tent:"p="; nocase; content:"Host|3A|"; nocase; con-
tent:"wr.mcboo.com"; distance:0; nocase;
pcre:"/^Host\x3a[^\r\n]*wr\x2emcboo\x2ecom/smi"; class-
type:trojan-activity; sid:14083;)
```

```
alert tcp $HOME_NET any -> $EXTERNAL_NET $HTTP_PORTS
(msg:"A POLICY XBOX avatar retrieval request";
flow:to_server,established; uricontent:"/avatar/"; con-
tent:"User-Agent|3A| Xbox Live Client/"; con-
tent:"Host|3A|avatar.xboxlive.com|0D 0A|";  class-
type:policy-violation; sid:15172;)
```

```
logging tcp $EXTERNAL_NET any -> $HOME_NET 5003 (msg:"D
EXPLOIT Symantec Discovery  buffer overflow";
flow:established, to_server; content:"|ED ED|"; depth:2;
offset:2; content:!"|ED|"; depth:1; isdataat:1176; con-
tent:!"|00|"; depth:976; offset:200; classtype:attempted-
admin; sid:11670;)
```

(ii) *Signature database*

```
BACKDOOR Pushdo client communication attempt - ID 15165
Flow to_server,established,infected files
:%System%\rs32net.exe | xcommsvr.exe
|vsserv.exe|vsmon.exe|symlcsvc.exe
sspfwtry2.exe|safensec.exe
```

```
1000 IP options-Bad Option List
1200 IP Fragment buffer full
2000 ICMP Echo Reply
3005 TCP FIN Port Sweep
11010 Swapper File Request
11200 Yahoo Messenger Activity
11251 Skype Client Activity
19500  Oracle Stack-based buffer overflow vulnerability
20759 TheWebForumLogin.php Username Param SQL Injection
```

(iii) *Regular Expression database*

Regex are specified using a keyword the keyword PCRE, which stand for Perl Compatible Regular Expression. PCRE is more powerful and complicated. Regex can match with pattern recognizing in layer 7 applications firewall mechanism and the attribute always contains just a single pattern.

Tabel 6. Sample data regex

Suspicious	Regex String
edonkey	^[\xc5\xd4\xe3-\xe5].?.?.?.?([\x01\x02\x05\x14\x15\x16\x18\x19\x1a\x1b\x1c\x20\x21\x32\x33\x34\x35\x36\x38\x40\x41\x42\x43\x46\x47\x48\x49\x4a\x4b\x4c\x4d\x4e\x4f\x50\x51\x52\x53\x54\x55\x56\x57\x58[\x60\x81\x82\x90\x91\x93\x96\x97\x98\x99\x9a\x9b\x9c\x9e\xa0\xa1\xa2\xa3\xa4]|\x59.....?[-~]|\x96....$)
BitTorrent	.*[Ii][Nn][Ff][Oo]_[Hh][Aa][Ss][Hh]=.*
IRC	^(nick[\x09-\x0d -~]*user[\x09-\x0d -~]*:|user[\x09-\x0d -~]*:[\x02-\x0d -~]*nick[\x09-\x0d -~]*\x0d\x0a)
YM!	^(ymsg|ypns|yhoo).?.?.?.?.?.?[lwt].*\xc0\x80?
SSH	([A-Za-z0-9._-]+) sshd\[([0-9]+)\]: \[[^]]+\]
X11	^[lb].?\x0b userspace pattern=^[lB].?\x0b userspace flags=REG_NOSUB
Quicktime	user-agent: quicktime \(qtver=[0-9].[0-9].[0-9];os=[\x09-\x0d -~]+\)\x0d\x0a

(iv) *Archieve database*

In fact, on archive event database, while sensor refers trigger alarm, attempt, penetration, and misuse. An attacker will capture and labeling to specify stored in archive event. For example event databases as following.

```
2006:04:19-00:20:50 host ulogd[1848]: UDP_FLOOD: IN=br0
OUT= MAC=00:07:0e:9c:6d:62:00:04:9a:ef:d3:a0:08:00
SRC=204.16.208.11
2 DST=202.93.35.204 LEN=449 TOS=00 PREC=0x00 TTL=57 ID=0
DF PROTO=UDP SPT=38689 DPT=1027 LEN=429
```

```
# Oct 17 15:34:04  202.146.176.45  222.73.238.152 33945
33903    17  0x0    29    70   0x4000   0x0
```

```
/usr/sbin/logwatch
/etc/log.d/logwatch.conf
/etc/log.d/conf/services/syslogd.conf
/etc/log.d/scripts/services/syslogd
/etc/cron.daily/00-logwatch
```

From our experiment, we have test several global database to improve and associate with our approach, such as blacklist categorized for defense system (http://cri.univ-tlse1.fr/blacklists/index_en.php).

Depicted, as in **Fig.** 3, the implementation of our approach consists of three main modules. Here, this system is updated regularly, the system will initially check the payload and Regex, and it checked with database for its existence, if it exists, the system will take an appropriate action to trigger alarm. We assumed, each database will contain more than 500,000 event list. Furthermore, the event still frequent automatic updates.

The fundamental accuracy for identify threat is low (FP) and (FN) between high (TP) and (TN) rates. We observe that the accuracy affects the correctness of deciding whether an attack exists in real-traffic, notifying the logging system of an attack based on the list in the database. To summarize the four possible cases, Accordingly, TN as well as TP is to identify operation detector, which is labeled as normal or known activity. On the contrary, FP and FN are the events that undermine the detection performance when unknown or suspicious is not identify. From our review, these high-level alarms can be used as the base to perform further higher-level threat analysis. By using our approach, every unknown activity or suspicious threat has labeling.

4.2 Risk Rating

Risk rating (RR) can describe a threat rating based on numerous factors besides just the attack severity. The RR is calculated according to not just the severity of the attack but also (i) event response, (ii) signature fidelity, and (iii) asset value of target. Wherefore, the RR detects an attack the rule set get rate mark to reduce FP Alarm.

The target value RR enables to configure an asset rating from specific habitual activity. Therefore, from our observations, there are two habitual behavior activities, which the asset RR can be one of the values: (i) media rich with activity higher transaction size, and (ii) transactional with activity concurrent connection. For the present RR calculating, we uses the concept of likehood, it can be useful when prioritazing risk and evaluating the effectiveness of potensial threat.

The likehood estimation is subjective to combination and is typically expressed as a RR of high, medium and low. Additionally, in previous work [7] and [8], they describe relations accuracy with RR to increasingly recognized threat. As mentioned above, we shown one potential model for calculating likehood as in Table 7, from Table 4 and Table 5, we show simple example of calculating risk by relative likehood that the habitual activity from inside user can occur and the value of the expected incurred loss.

Likehood of Threat **(TL)** :
(i) 1 = Least Likely, (ii) 2 = Probabily Likely, and
(iii) 3 = Very Likely.

Expected Incurred Loss **(LE)** :
(i) 1 = Low Risk, (ii) 2 = Moderate Loss, and (iii) 3 = Critical Loss.

Risk = **TL** x **LE** :
(i) 1,2 = Low Risk, (ii) 3-4 = Medium, and (iii) 6-9 = High Risk.

Obiviously, RR provides profile users with valuable insight into the overal risk of an even. It can be the event response to develop policies for the prevention of network attack to better identify and recognizied threat.

Table 7. Simple Risk Calculation of Habitual Activity

Activity	TL	LE	Risk
WWW	3	2	High
Collaborative Workspaces	2	2	Medium
Download - Upload	3	3	High
Streaming video	2	3	High
Data Replication	1	3	Medium
Remote Login	2	1	Low
Remote VNC	1	3	Medium
Mail	3	1	Medium
E-Commerce	2	1	Low
Internet Messaging	3	1	Medium
VoIP	2	2	Medium
Game online	3	3	High
Scanning	2	1	Medium

5 Experimental & Results

In this section, we represent dataset to collecting data from popular dataset intrusion domain and the overall system existing topology as shown in Figure 4.

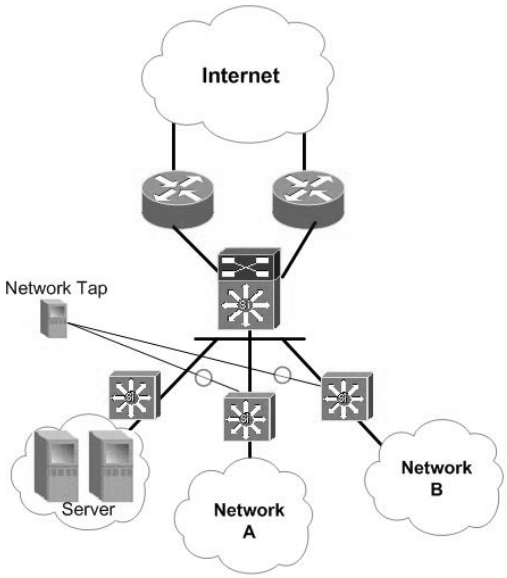

Figure. 4. Topology network experiment

We have core network to connected distribution and access layer network. To running and composite two ISP, we use load balancing based for optimized the bandwidth. We located and provided one server running Fedora to tapping traffic. Furthermore, wireshark were set up on the machine to captured traffic from interface network A. The network used for this observed with over 200 user. We show in Table 8, the packet processing from network tapping in 6 days with reach out average packet /second 97.963 from 2.300.547 totally packet.

Table 8. Packet Processing

Day	Packet	Avg/ sec	UDP	TCP	None
Day 1	272.009	20.573	44.94%	54.51%	0.55%
Day 2	477.583	15.698	59.84%	39.31%	0.8%
Day 3	317.115	13.850	89.51%	8.93%	1.56%
Day 4	406.448	15.292	88.61%	10.09%	1.30%
Day 5	416.850	14.458	84.82%	14.06%	1.12%
Day 6	410.542	18.092	47.79%	51.42%	0.79%

As it can be observed in Table 9, we show taxonomy steps of attack with commonly used script applications:

1. Probe, the attack looks for a vulnerability of system, the attacker usually execute ping command, interrogation of DNS or domain
2. Scan, the attack uses tools to find a vulnerability holes to compromise the host, scanning is try to find information vulnerable a system, it is can produce information, such as IP Address devices, scheme of topology, and application systems of running
3. Intrusion, the attack installs something on system, uses the compromised host to attack other systems, the attacker try and error to penetration,
4. 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.

Table 9. Identify & Recognized Suspicious Threat

Steps	Script	Detection
Probe	Http Spyware	95.55%
	ICMP Ping	95.67%
Scan	Nmap	100%
	Nessus	100%
	Traceroute	100%
Intrusion	ARP Poison	99.99%
	Brute force attack	99.99%
	DoS	99.99%
	Worm trojan	75.50%
	Input injection	86.79%
	Spammer	90%
	Keylogger	99.99%
Goal	Rootkit	100%
	Backdoor	100%

6 Conclusion & Future Work

In this paper we have present a new method to detect network traffic threats based on packet classification which is result from the identification of insider's habitual activities. The result shows the false alarm rate detection is low. The finding shows our risk rating technique applied in this new method able to prevent a similar malicious habit from repeatedly occurs. Throughout this pa-

per, we apply our new model distinguish normal/unknown habitual activity with observe regular access user and involved risk rating calculation. In the future, we plan to apply this method with Behavior-based attack algorithm in a real-traffic network.

REFERENCES

[1] P.P Verbeek, et all "User Behavior and Technology Development : Shaping Sustinable Relations Between Consumers and Technology, pp. 385-399, Springer, 2006.

[2] K.V Kumar., "Securing Communication using function extraxtion technology for malicious code behavior analysis", Computer & Security 28 (2009), pp. 77-84, Elsevier, 2009.

[3] T. Walker, et al, "Practical management of malicious insider treat – An enterprise CSIRT perspective", Information Security Technical Report I3 (2008), pp. 225-234, 2008

[4] H.S. Rhee, et al "Self-efficacy in information security :it influence on end users information security practice behavior", Journal Computer & Security 28, 2009.

[5] J.M.E. Tapiador, et al, " Anomaly detection method is wired networks: a survey and taxonomy, Computer Communication 27 (2004), pp.1569-1584, Elsivier, 2004

[6] G. Doss, et al," Developing Insider Attack Detection Model : A Grounded Approach, ISI 2009, 2009

[7] A. D. Todd, et al, "Alert Verification Evaluation Through Server Response Forging" LNCS, vol. 4637, pp. 256-275, Springer, 2007

[8] T. Abbes, et al, "A Traffic Classification Algorithm for Intrusion Detection", IEEE 21st International Conference on Advanced Information Networking and Application Workshops (AINAW'07), 2007

[9] M. Mark, et al, "Analysis and detection of malicious insiders, In 2005 International Conference on Intelligence Analysis, 2005

[10] Hyeun-Suk Rhee, et al "Self-efficacy in information security : it influence on end users information security practice behavior", Journal Computer & Security 28, 2009

[11] W. Kim, et al, "On social Web sites", Journal of Information Systems, Volume 35, Issue 2, pp. 215-236, Elsevier, 2010.

[12] C.Y.Wang, et al, "Emotion and Motivation : Undestanding User Behavior of Web 2.0 Application", International Conference on Information Technology : New Generations, 2009

Deris Stiawan. Holds an M.Eng from University of Gadjah Mada, Indonesia, since 2006, he is Computer Science faculty member at University of Sriwijaya, Indonesia. He is IEEE member and currently pursuing his Ph.D degree at Faculty of Computer Science & Information System, Universiti Teknologi Malaysia working in intrusion prevention system. He joined research group Information Assurance and Security Research Group (IASRG) at Universiti Teknologi Malaysia. His professional profile has derived to the field of computer network and network security, specially focused on intrusion prevention and network infrastructure.

Abdul Hanan Abdullah.Ph.D, Receive the B.Sc. and M.Sc from San Francisco, California, and Ph.D degree from Aston University, Birmingham, UK, in 1995. He is a Professor at Faculty of Computer Science & Information System, Universiti Teknologi Malaysia. His reseach interest is in Information Security. He is also a head of Pervasive Computing Research Group (PCRG) UTM and member of ACM.

Mohd. Yazid Idris. Ph.D, is a senior lecturer at Faculty of Computer Science and Information System. He obtained his M.Sc and Ph.D in the area of Software Engineering, and Information Technology (IT) Security in 1998 and 2008 respectively. In software engineering, he focuses on the research of designing and development of mobile and telecommunication software. His main research activity in IT security is in the area of Intrusion Prevention and Detection (ITD). He is currently active in various academic activities and involves in university-industry link initiative in both areas, and recently received a prestigious award in the mobile software invention by the government of Malaysia and telecommunication leading industry.