Intrusion Detection System for Mobile Devices: Investigation on Calling Activity

Fudong Li, Nathan Clarke and Maria Papadaki

Centre for Information Security & Network Research, University of Plymouth, Plymouth, United Kingdom
info@cisnr.org

Abstract

In recent years, an increasing focus has been given to the development of security controls to counter current existing mobile security threats; such as Anti-Virus and firewalls, which are both now commercially available. Nevertheless, with the increasing functionality of mobile devices, a need exists for more sophisticated security controls and research is focusing upon other security controls like Intrusion Detection Systems (IDS). Indeed, a number of research efforts on IDS for the mobile device have already been given. However, those mobile IDSs are designed to detect particular security threats related to individual service (e.g. telephony). The aims of this paper are firstly to identify the need for a novel mobile IDS which can provide detection for multiple services and support multi-networks simultaneously; and to identify the positive calling activities' features to discriminate users. This paper begins with investigating the current research on mobile IDS with a view of examining the positive and negative aspects. The paper then processes to describe an experimental study on user's calling activity. The experiment result shows that within the host environment, the number of calling, the time of calling and the duration of calling can be used to discriminate legitimate users and attackers. The paper will conclude with the future research for the mobile IDS.

Keywords: *Intrusion Detection System, mobile devices*

1. Introduction

Currently, the mobile device has become a ubiquitous computing device. It has experienced an evolutionary shift from a purely telephony based handset into a modern computing device with multiple variants, such as the Smartphone, PDA (Personal Digital Assistant), and Ultra-mobile PCs. For the mobile telephone alone, it has over 3.2 billion subscribers around the world (GSM Association, 2008). Indeed, a large number of developed countries are experiencing well in excess of 100% market penetration (ITU, 2007). The modern mobile device is capable of providing a wide range of services over several network connections and is able to store a broad range of information from business to personal data. As a result, many people rely on those services and information to complete their business and personal tasks. Such tasks can include email accessing via wireless network, online shopping through the 3G network, sharing pictures over the Bluetooth connection, and reading word documents. However, those activities can contain sensitive data related to the business and personal private information.

The mobile device faces several security threats. Traditionally, service fraud, handsets being lost or stolen and SIM (Subscriber Identity Module) card cloning were three major

security threats (BBC, 2005; Metropolitan Police Service, 2008; Rao *et al*, 2002). According to the Forum for International Irregular Network Access, the service fraud is estimated to cost telecom service providers $55 billion every year around the world (European Communications, 2005). Recently, with the evolution of the mobile device, it is also experiencing several new security threats, such as malware, information disclosure, and Denial of Service (DoS) (Muir, 2003; Swami and Tschofenig, 2006; Stajano and Anderson, 1999). Although these new threats were discovered a few years ago, the number of incidents grows significantly every year (McAfee, 2007). For instance, there were already more than 100 variants of mobile malware in existence at the end of 2005 (IT-Observer, 2007). To counter those security threats, various mobile security projects have been proposed and developed; such as antivirus, biometrics, encryption and firewalls (F-Secure, 2008; Clarke and Furnell, 2007; Check point, 2008; Anthasoft, 2008). This reveals that a real lack of effective information security still exists (Perelson and Botha, 2004).

Due to the incompatibility of the existing IDS with the mobile device, research for the mobile IDS started in the middle of 1990s. Early mobile IDS research developed mechanisms of detecting traditional attacks; such as the European project Advanced Security for Personal Communications (ASPeCT) for detecting telephony service fraud (Gosset, 1998). More recent mobile IDS studies have focussed upon detecting newer attacks; i.e. the battery based mobile IDS and the mobile agent based IDS (Jacoby *et al*, 2006; Kannadiga *et al*, 2005). However, the amount of mobile IDS research is significantly smaller compared to other aforementioned mobile security projects. Moreover, those existing mobile IDSs were designed to detect the individual security threats: telephony based mobile IDSs only detect telephony service fraud; battery based mobile IDSs only detect battery attacks. Therefore, none of these mobile IDSs is capable of offering the comprehensive detection for the services running on the modern mobile devices.

This paper begins with introducing the concept of the modern mobile device, the threats associated with the device, and general security controls. The main discussion starts with presenting the history of the traditional IDS and follows by a critique of the mobile IDS: their different variants and their working principles, performance, and advantages and disadvantages. In section 3, a behaviour and host based mobile IDS is proposed. The paper describes a research programme underway to design, develop and evaluate a novel mobile IDS. The paper then proceeds to present some initial experimental results and concludes with highlighting the future work.

2. Mobile Intrusion Detection System

In 1980, the first notion of intrusion detection was created in Anderson's paper "Computer Security Threat Monitoring and Surveillance": by using mainframe audit trails to trace misuse actions and to understand users' behaviour in the computer system (Anderson, 1980). In 1987, Denning proposed the seminal work: "An Intrusion Detection Model", which identified basic IDS components and their functionalities (Denning, 1987). Since then, a considerable amount of IDS research has been carried out and a range of prototypes and commercial products were developed (Stefan, 2000). However,

because of the unique characteristics that the mobile device has: low processing power, small storage space, differing network accesses and a unique set of services; these existing IDSs are not suitable to provide detections for the mobile device. Host based IDSs are too complicated for mobile devices to handle; network based IDSs can only monitor a single network at any one time.

The research for mobile IDS started around 1995 with preliminary focus upon detecting telephony service fraud. Telephony service fraud occurs when the mobile device is lost or stolen, or the SIM card is cloned. In the worst case, the owner would not notice the attack until the end of the billing month. At that moment, significant financial damages would have been made for both the owner and the telecom service company. By monitoring users' calling behaviour, the aforementioned attacks can be detected (Samfat and Molv, 1997). With increasing computational power, the mobile device offers more services: such as, accessing emails, and transferring data file over different network connections. However, those services raise new security risks: malware and DoS attacks. As a result, several signature based mobile IDSs have been developed.

2.1. Behaviour based mobile IDS

The modern mobile device provides a wide range of services, however, the way people use those services can be completely different. As a result, people's behaviour on their mobile device can be arguably distinguished. Indeed, the user's calling activity, migration mobility activity and migration itinerary activity have already been utilised to detect telephony service fraud, SIM card cloning and lost or stolen of the device. To date, all behaviour based mobile IDSs are network based systems; as user's behaviours are obtained and monitored by network services providers.

2.1.1. Telephony based mobile IDS

The telephony based mobile IDS monitors user's calling attributes (e.g. international Mobile Subscriber Identity (IMSI), start date of call, start time of call, duration of call, dialled telephone number and National or International call) to detect service fraud, SIM card cloning, and lost or stolen of devices (Moreau *et al*, 1997). By using the combination of those attributes, a historical profile can be acquired. If the deviation between the current calling session and the historical profile exceeds a threshold, an intrusion is identified. There are several telephony based mobile IDSs existing, and they can be separated by their pattern classification techniques. For example, Stormann (1997), and Boukerche and Notare (2002) utilised a supervised method; and Samfat and Molva (1997), and Alves *et al* (2006) employed an unsupervised method. Generally speaking, telephony based mobile IDSs have a good system performance: high detection rate and low false alarm rate. In addition, as the detection process is carried out by the network operator, there is no restriction on the mobile device. The major disadvantage is that they only focused upon telephony services and can not provide any detection for other network services. Moreover, those systems can not provide any detection for data related attacks.

2.1.2. Migration mobility based mobile IDS

By calculating the chance of a mobile user travelling from one mobile cell to another, the migration mobility based mobile IDSs can also detect traditional attacks. If the calculated result exceeds the threshold, a possible intrusion occurs. There are several mobility based mobile IDSs: Buschkes *et al* 1998, Sun *et al* 2004, and Sun *et al* 2006. Among those systems, Sun *et al* 2006 has the best system performance. It employed several methods to achieve this: the high order Markov chain model, the Exponentially Weighted Moving Average Model and the Shannon's entropy theory. As a result, the system has a constantly updated profile, and a suitable threshold. Furthermore, as the user's activities could be extremely different over the weekdays and weekends, two separated profiles were used according to those two periods. From their simulation result, it shows that the system's best detection rate is around 94% and the lowest false positive rate is around 5% when the user travels at the speed of 60 miles per hour. However, the performance decreases dramatically when the user travels on foot. The main advantage for those systems is they are suitable for those long distance regular travellers who spend a lot of time on travelling. However, the number of those travellers is reasonably small within the mobile users' population. Furthermore, those systems can not provide detection for malware and data related attacks.

2.1.3. Migration itinerary based mobile IDS

Whilst similar to migration mobility based mobile IDS, the migration itinerary based mobile IDS also monitors cells to detect traditional attacks. However, instead of only monitoring one cell each time, the migration itinerary based mobile monitors all the cells the user covers from one location to another. People always have the destination in their mind when they travel. Therefore, certain routes will be chosen as regular or favourite routes. As a result, the probability of the mobile user travels over those routes is much higher than when they travel through other routes. To extend this, when an attacker carries other people's mobile device, the route he is going to cover will be probably different in comparison with the owner's routes. In 2005, Hall *et al* have published a paper on using public transportation user's itinerary profile to detect intrusions via an instance based learning pattern classification technique (Hall *et al*, 2005). However, their simulation result was not particularly promising. In addition, the system could only monitor those mobile users who take the public transport system. Moreover, these systems suffer the same problem as the mobility based mobile IDS does: they can not provide detection for malware and data related attacks.

2.1.4. Comparison on behaviour based Mobile IDS

Table 1 illustrates the comparison for all aforementioned behaviour based mobile IDSs. Generally speaking, telephony based mobile IDSs have a better Detection Rate (DR) and False Alarm Rate (FAR) than the migration activity based mobile IDSs do. In addition, the telephony based mobile IDS provides the detection for more users than the migration activity based mobile IDS could. However, the migration activity based mobile IDS does have the potential ability to provide the detection for all services provided by the service provider. The advantages for behaviour based mobile IDSs are: as the detection process is carried out by the services provider, there is no overhead or requirement for the mobile device. Also, those IDSs can identify the telephony service fraud, SIM card cloning and

the lost or stolen of devices. On the other hand, those systems can not detect any other service frauds. Also they can rarely provide any detection against following mobile security threats: malware, information leakage, DoS, and data modification. Furthermore, the mobile user's privacy could also be an issue.

Name	Behaviour	Pattern classification model	DR	FAR
Samfat and Molva, 1997	Itinerary	Mathematical formula	82.5%	4%
	Calls	Mathematical formula	80%	3%
Boukerche and Notare, 2002	Calls	RBF neural network model	97.5%	4.2%
Stormann, 1997	Calls	Rule based	99%	24%
Alves *et al*, 2006	Calls	Distance-based and clustering	91%	NA
Buschkes *et al* 1998	Mobility	Bayes decision rule	87.5%	NA
Sun *et al* 2004	Mobility	High order Markov model	87.5%	15%
Sun *et al* 2006	Mobility	High order Markov model	89%	13%
Hall *et al*, 2005	Itinerary	Instance based learning	50%	50%

Table 1: Comparison for the Behaviour based Mobile IDS

2.2. Signature based mobile IDS

The research on the signature based mobile IDS started in early 2000. The main aim of developing the signature based mobile IDS was to detect malware and DoS attacks for the mobile device. At present, there are four prototype signature based mobile IDSs and they are categorised into two groups: the battery based mobile IDS and the mobile agent based mobile IDS.

2.2.1. Battery based mobile IDS

It is widely recognised that the battery plays a key role in a mobile device, to provide continuous services to the user. If the attacker is able to drain the battery, the mobile device's servicing time will be reduced. Therefore, attacking the battery is a major threat for the mobile device's availability. In order to counter battery attacks, three studies based on analysing the battery activities have been conducted: Power Secure Architecture, Battery Based Intrusion Detection Model and Gibraltar (Martin *et al*, 2004; Jacoby *et al*, 2004; Jacoby *et al*, 2006). These systems all work in a similar fashion. Each mobile application consumes unique power, so does malware. As a result, by analysing current activities, various signatures for either legitimate applications or malicious codes can be obtained. The battery based mobile IDS continually monitors battery activities and compares them with its signatures to detect any anomalies. The advantage for these systems is that by monitoring battery activities, malware attacks and attacks on the battery can be detected. However, obtaining malware's signatures can be a very difficult task.

2.2.2. Mobile agent based mobile IDS

In 2005, Kannadiga *et al* proposed a mobile agent based IDS for the pervasive computing environments (Kannadiga *et al*, 2005). In a pervasive computing environment, various mobile devices can be found: such as mobile phones and PDAs. Their mobile IDS

employs the mobile agent, by moving it from one mobile device to another within the network, collecting information (such as application log files) from mobile devices, to indentify malicious activities on each mobile device. It is reasonable to use mobile agents to detect intrusion for those low computing powered mobile devices. In addition, by knowing the attack on the mobile host, the network threat can also be identified. The major drawback is that signatures are created by monitoring malicious activities on networked static hosts (i.e. virus on the desktop PC); therefore those signatures are more related to static hosts, rather than for mobile devices. As a result, mobile malwares attacks can not be detected. Also, the mobile device can be not protected when it leaves the network.

2.2.3. Comparison on signature based mobile IDS

Table 2 illustrates the comparison for signature based mobile IDSs. For the battery based mobile IDS, their sensors are all allocated on mobile devices' battery. For the mobile agent based mobile IDS, the mobile agent is the sensor. The correlation process is carried out in three different ways: Martin *et al* 2004 is done on the mobile device, Kannadiga *et al* 2005 is executed on the network based server, and Jacoby *et al* 2004 and Jacoby *et al* 2006 can be carried out both locally or on the network based server. Various approaches have been taken to obtain the signature: Martin *et al*, 2004 uses the legitimate services as the signatures, any process' signature not in the database can be identified as malicious. The signature database is reasonably small as the number of legitimate mobile services is currently limited. Both Jacoby *et al*, 2004 and Jacoby *et al*, 2006 employed the most popular network relate attacks as the attacking signature. However, the database is pretty small when compared with the number of existing attacks; moreover, as those network attacks are found in the traditional desktop environment, they are less relevant for the mobile device. The Kannadiga *et al* 2005 also suffers this problem as their attacking signatures are gathered by the static agent from local hosts. The major break through for the signature based mobile IDS is that it can possibly detect the malware and battery attacks. On the other side, it can not provide any protection against data related attacks, and service fraud. Also, obtaining accurate and a wide range of signatures is a very challenging task in practice.

Name	Sensor location	Correlation location	Signatures types	Attacks can be detected
Martin *et al*, 2004	Battery	Host	Legitimate Services	Malware and Power attacks
Jacoby *et al*, 2004	Battery	Host and network	Common network attacks	Common network attacks
Jacoby *et al*, 2006	Battery	Host and network	Common network attacks	Common network attacks
Kannadiga *et al*, 2005	Mobile Agent	Network server	Signatures from the desktop environment	Network related attack

Table 2: Comparison for the Signature based Mobile IDS

2.3. Summary of current Mobile IDS

The behaviour based mobile IDS is able to detect attacks on telephony service fraud. The signature based mobile IDS could identify possible malware and DoS attacks. However, both types fail to provide any detection for other services and network connections as shown in Table 3. This is really worrying as people use these services on the mobile device on a daily basis. As a result, a mobile IDS which can offer the detection for a wider range of services and connections on the mobile device is certainly needed.

	Services				Networks			
	Call\SMS	Internet	Email	Data storage	Cellular network	WiFi	Bluetooth	Cable
Boukerche and Notare, 2002	Y	-	-	-	Y	-	-	-
Sun *et al* 2006	Y	-	-	-	Y	-	-	-
Samfat and Molva, 1997	Y	-	-	-	Y	-	-	-
Martin *et al*, 2004	-	-	-	-	-	-	-	-
Jacoby *et al*, 2006	-	-	-	-	-	Y	-	-
Kannadiga *et al*, 2005	-	-	-	-	-	Y	-	-

Table 3: Mobile IDS VS mobile device's services and networks

3. Experimental studies on a behaviour & host based mobile IDS

As mentioned previously, the usage of the mobile device has changed dramatically. Also, as shown in section two, current existing mobile IDSs can not provide continuous detection for all the services the mobile device offers, along with the information stored on the device. Given the specific requirements, a *Behaviour and Host based Mobile IDS* is proposed. There are several reasons behind this proposal: the behaviour and host based mobile IDS can provide detection for services running on the mobile device against the service fraud, data disclosure and modification attacks. Also, the host based mobile IDS can monitor all network connections which a single network based system is unable to achieve.

It is arguable that people's behaviour on the mobile device can be different due to the purpose of the usage. For example, a user accesses his mobile calendar service to find out what his schedule looks like, the features related to this behaviour can be the time of accessing (7.15 AM), the duration of accessing (1 minutes) and the day of accessing (Monday). However, when an intruder accesses the same calendar service, the intruder may choose a time which the owner would not use the device such as 3 AM in the morning and the duration of accessing should be much longer such as 5 minutes as the intruder wants to explore as much information as possible. As a result, various user's behaviours within the mobile platform should be studied to identify positive behavioural features that could be utilised to discriminate between legitimate users and intruders. In this paper, an experiment study on user's calling behaviour is presented on the following section.

3.1. Telephony based experiment

The prior literature shows that the calling behaviour has been studied a number of times over the telecom service provider's network environment and its features can be used to discriminate users. However, within the mobile host environment, the number of calling behaviour's features reduced significantly: from 6 features for the network based environment down to 3 features within the host platform. According to the Ofcom's "The International Communication Market 2007" research report, the calling service still predominate the mobile communication market (Ofcom, 2007). As taken those two points of views into consideration, the research started with identifying positive calling behaviour's features within the host environment.

The experiment employed 45 participants who had more than four month's calling activity from the existing MIT Reality dataset (MIT, 2008). As the condition is under the host environment, only the *number of dialling*, the *calling time*, and the *duration of the conversation* were extracted from the dataset as these can be established by the mobile host. The dataset for those 45 participants contains a total 15,702 calls. In addition, those 15,702 calls have been formed two sub-datasets: weekdays and weekends as people's activities can be extremely different over those two periods. The datasets were divided into two: the first half was used for training the classifier and the second half was used for the validation. Two neural networks (Feed-Forward Multi-Layered Perceptron Neural Network and Radial Basis Function Neural Network) with a total of 99 configurations were chosen (81 for FF MLP and 18 for RBF).

Table 4 demonstrates a summary of best sets of experiment results with three groups of inputs over three sets of time periods by using various FF MLP Neural network configurations. The results clearly shows that by using the number of calling alone as the input, the FFMLP neural network achieved the lowest Equal Error Rates (EER) with 8.71%, 7.05% and 8.57% for *weekdays*, *weekends* and *weekly* accordingly. With the number of the inputs increases, the FFMLP neural network's performance gets worse. The results indicate that by adding the *time of calling* and the *duration of calling*, those two features made more impact for the *weekends*' performance than they did for the *weekdays*'.

Input(s)/ Features	Periods	Neurons	Epochs	EER
Number of calling only	weekdays	150	150	8.71%
	weekends	150	100	7.05%
	weekly	150	50	8.57%
Number of calling, and time of calling	weekdays	50	150	21.61%
	weekends	50	150	25.80%
	weekly	100	50	21.96%
Number, Time of calling, and duration of calling	weekdays	50	100	22.58%
	weekends	50	100	25.44%
	weekly	50	100	21.03%

Table 4: Experiment result on FFMLP Neural network

Table 5 illustrates all the experiment results by using RBF neural network. Due to too much input data, it is not feasible for the RBF neural network to simulate the weekly situation. In order to compare the performance with the FF MLP neural network, same set of maximum number of neuron has been chosen for the RBF neural networks. The result demonstrates that by using only the *number of calling* as the input and maximum 150 neurons, the RBF neural network obtained the best performance with the EER 6.95% and 6.21% for *weekdays* and *weekends*. With increasing number of inputs, the RBF neural network's performance gets worse; however, the RBF neural network's EER only grew around twice comparing with three times for the FF MLP neural network did. Also when the number of inputs increases, they have more impact for the *weekends*' performance than they do for the *weekdays*'; this pattern is also shown by the FF MLP neural network in Table 4.

Input(s)/Feature(s)	Periods	Neurons		
		50	100	150
Number of calling only	Weekdays	8.12%	7.55%	6.95%
	Weekends	6.80%	6.30%	6.21%
Number of calling, And time of calling	Weekdays	11.82%	9.66%	9.53%
	Weekends	14.23%	12.86%	12.09%
Number of calling, Time of calling, and duration of calling	Weekdays	12.60%	11.24%	10.95%
	Weekends	16.32%	15.44%	16.67%

Table 5: Experiment result on RBF neural network

From the above two set results, they show that by using the *number of calling* alone, the best simulation results were obtained. With the number of inputs increases, the overall performance decreases. This shows that the *number of calling* is a positive discriminate feature and the *time of calling* and the *duration of calling* are having a negative discriminative effect for this particular dataset. By using number of calling only, the *weekends*' performance is better than *weekdays*', this may because over the weekends less numbers have been dialled; or the user may only contact their family and friends over the weekend. With the number of inputs increases, the neural networks got better performance during the weekdays than they do over the weekends. This shows that people may do regular tasks during weekdays and their weekends' activities are much more random.

The experiment results are what would be expected as users regularly call a subset of people. However, using only *number of calling* feature, a category of misuse is missed when people do call the same number. As a result, more analysis has been made on those 45 individual users. Within those 45 users, three groups users have been found: within the first group, 12 users never share any same dialled number with any one; within the second group, 13 users shares between a minimum of 6 and a maximum of 18 dialled numbers between minimum 2 users and maximum 8 users within those 13 users; and for the third group, users only share a few number of same dialled numbers among one or two other users. This reviews that more than 2/3 of users with the 45 users' dataset do not share large amount dialled number with others. The hypotheses is that if the number has been dialled before, the *time of calling* and the *duration of calling* would play positive

discriminate roles to identify the different mobile users. Otherwise, they play negative discriminate roles in the identification process.

More experiments have been carried out to test the hypotheses to identify roles the *time of calling* and the *duration of calling* play for different types of users by using RBF neural network. The reasons for employing the RBF neural network are: simulation results from Table 4 and Table 5 show that the RBF neural network outperformance the FFMLP neural network; similar conclusion has also been found by previous study (Boukerche and Notare, 2002); moreover, during the experiment, the RBF neural network was much more stable comparing with the FFMLP neural network was.

Table 6 demonstrates the experiment result on the first group users which contains total 2811 calls. The best performance is achieved by using the number of calling only with the EER of 3.24%, 3.31% and 4.30% for *weekdays*, *weekends* and *weekly* accordingly. Those results are even better than the results from Table 5. With the number of inputs increases, the performance gets worse and worse. This is due those user do not share any dialled number, by adding more inputs, it will only confuse the neural network and get poorer performance.

Neurons	Input(s)	EER(weekdays)	EER(weekends)	EER(weekly)
50	1*	3.24%	4.60%	4.30%
	2*	5.93%	14.13%	8.10%
	3*	8.50%	15.39%	8.45%
100	1*	3.33%	3.31%	4.74%
	2*	6.64%	11.17%	7.34%
	3*	7.59%	14.60%	8.00%
150	1*	3.33%	3.31%	4.60%
	2*	5.91%	12.11%	7.53%
	3*	8.22%	14.89%	8.32%

Table 6: Experiment result on first group users

1* number of calling 2*: number of calling, and time of calling 3*: number of calling, time of calling and duration of calling

Table 7 illustrates the experiment result on the second group users who do share a number of same dialled numbers with total number of 3966 calls within this dataset. Interesting results are shown by Table 7 as by using only the *number of calling* the neural network has the worst performance. By adding the *time of calling* to the inputs, the neural network's performance improved significantly for all the network configurations; by adding the *duration of calling* to the inputs, the neural network's performance improved slightly for most configurations. This reviews that both of the *time of calling* and the *duration of calling* play a positive role when the number has been dialled before and the *time of calling* has a stronger impact for the performance than the *duration of calling* does. Generally speaking, by using three inputs together, the neural network's performance is better than by *using the number of calling* only, and is worse than by using the *time of calling* and the *number of calling* together.

Neurons	Inputs	EER(weekdays)	EER(weekends)	EER(weekly)
50	$1^{\#}$	20.27%	21.58%	20.70%
	$2^{\#}$	18.35%	18.64%	16.92%
	$3^{\#}$	19.32%	21.31%	19.39%
	$4^{\#}$	19.65%	21.91%	17.41%
100	$1^{\#}$	18.05%	22.17%	20.75%
	$2^{\#}$	17.52%	18.48%	16.17%
	$3^{\#}$	19.35%	21.24%	18.82%
	$4^{\#}$	17.04%	21.15%	17.12%
150	$1^{\#}$	17.78%	22.18%	18.90%
	$2^{\#}$	15.49%	18.18%	16.08%
	$3^{\#}$	19.83%	20.71%	18.62%
	$4^{\#}$	17.74%	21.43%	17.15%

Table 7: Experiment result on second group users

$1^{\#}$: number of calling $2^{\#}$: time of calling and number of calling, $3^{\#}$ number of calling and the duration of calling and $4^{\#}$: number of calling, time of calling and duration of calling.

From the above experiment results, it shows that the *number of calling*, the *time of calling* and the *duration of calling* could all play the positive role to discriminate users. However, the *time of calling* and the *duration of calling* treated differently depend on whether the *number of calling* has been dialled before. If the number has never been dialled before, by adding the *time of calling* and the *duration of calling* can only decrease the classifier's performance. For the number has been dialled before, the performance for the classifier improves by adding the *time of calling* and/or the *duration of calling*; this will help the classifier to detect the data related attacks, as data can be viewed by anyone, however, the time or the duration for the attacker to access the same file may be different with the legitimate users.

4. Conclusion

In this paper, a comprehensive literature view on the mobile IDS has been given. It is clear that people use the mobile device to complete both business and personal work on a daily basis, and an increasing range of threats exist. By studying the positive and negative aspect of current mobile IDSs, a new mobile IDS which can offer the detection to cover a wider range of services is required.

The experimental results show that three positive calling features have been found to discriminate users within a mobile host platform. In order to support the development for a *Behaviour & Host based Mobile IDS*, other user's behavioural features should be studied. The results of these experiments will inform the design of proposed mobile IDS that is capable of detecting and acting upon a wide range of threats in an efficient and effective manner.

5. References

Anderson, J.P. (1980) "Computer Security Threat Monitoring and Surveillance", available at: http://seclab.cs.ucdavis.edu/projects/history/papers/ande80.pdf, accessed: 26 November 2007

Anthasoft (2008) "AnthaFirewall", available at: http://www.anthasoft.com/anthafirewall-firewall-for-mobile-device.php accessed: 26 August 2008

BBC (2005) "Cabs collect mountain of mobiles", available at: http://news.bbc.co.uk/1/hi/technology/4201915.stm date accessed: 25 August 2008

Boukerche, A. and Nitare, M.S.M.A. (2002) "Behavior-Based Intrusion Detection in Mobile Phone Systems", *Journal of Parallel and Distributed Computing*, Vol:62, pp. 1476-1490

Buschkes, R., Kesdogan, D. and Reichl, P. (1998) "How to increase security in mobile networks by anomaly detection", *proceedings of the 14th Annual Computer Security Applications Conference*, pp 23-12

Check Point (2008) "Pointsec Mobile", available at: http://www.checkpoint.com/products/datasecurity/mobile/ date accessed: 01 September 2008

Clarke, NL and Furnell SM (2007) "Advanced user authentication for mobile devices", *Computers & Security*, Vol.26, no.2, pp109-119

Denning, D.E. (1987) "An intrusion-detection model", *IEEE Transactions on Software Engineering*, Volume: SE-13, Issue: 2, pp. 222- 232, ISSN: 0098-5589

European Communications (2005) "Fraud management", available at: http://www.eurocomms.com/features/11905/Fraud_management.html, date accessed: 15 August 2008

F-Secure (2008) "F-Secure Mobile Anti-Virus" available at: http://mobile.f-secure.com/ date accessed: 01 September 2008

Gosset, P (Editor). (1998) "ASPeCT: Fraud Detection Concepts: Final Report", Doc Ref. AC095/VOD/W22/DS/P/18/1, Jan 1998.

GSM Association (2008), available at: http://www.gsmworld.com/index.shtml, date accessed: 21 February 2008

Hall, J., Barbeau, M. and Kranakis, E. (2005) "Anomaly-based intrusion detection using mobility profiles of public transportation users", *the Proceeding of IEEE International Conference on Wireless And Mobile Computing, Networking And Communications*, 2005 (WiMob'2005), Vol: 2, pp: 17- 24, ISBN: 0-7803-9181-0

International Telecommunication Union (ITU) (2007) "ITU World Telecommunication/ICT Indicators Database", available at: http://www.itu.int/ITU-D/icteye/Reporting/ShowReportFrame.aspx?ReportName=/WTI/BasicIndicatorsPublic&RP_intYear=2007&RP_intLanguageID=1, date accessed: 14 August 2008

IT-Observer (2007) "2005: Viruses, Phishing and Mobile Phone Malware", available at: http://www.it-observer.com/articles.php?id=971, date accessed: 13 November 2007

Jacoby, G.A., Hickman, T. and Warders, S.P. (2006) "Gibraltar: A Mobile Host-Based Intrusion Protection System", *Proceedings from the 2006 World Congress in Computer Science, Computer Engineering, and Applied Computing*, Jun 26-29, 2006.

Jacoby, G.A., Marchany, R and Davis, N.J. IV (2004) "Battery-based intrusion detection a first line of defense", *Proceedings from the Fifth Annual IEEE SMC, Information Assurance Workshop*, 2004, pp 272-279, ISBN: 0-7803-8572-1

Kannadiga, P., Zulkernine, M. and Ahamed, S.I. (2005) "Towards an Intrusion Detection System for Pervasive Computing Environments", *Proceedings of the International Conference on information technology: coding and Computing (ITCC'05)*, pp 277- 282, Vol. 2, ISBN: 0-7695-2315-3

Martin, T., Hsiao, M., Ha, D. and Krishnaswami, J. (2004) "Denialof- Service Attacks on Battery-powered Mobile Computers", *Second IEEE International Conference on Pervasive Computing and Communications*, pp. 309-318

McAfee (2007) "McAfee, Inc. Reports Preliminary First Quarter Revenue of $314 million", available at: http://www.mcafee.com/us/about/press/corporate/2007/20070426_181010_l.html, date accessed: 16 September 2008

Metropolitan Police Service (2008) "Safeguarding your mobile phone", available at: http://www.met.police.uk/crimeprevention/phone.htm, date accessed: 26 August 2008

MIT (2008) "MIT Media Lab: Reality Mining" available at: http://reality.media.mit.edu/ date accessed: 10 September 2008

Moreau, Y., Verrelst, H., amd Vandewalle, J. (1997) "Detection of mobile phone fraud using supervised neural networks: A first prototype", *International Conference on Artificial Neural Networks Proceedings (ICANN'97)*, pages 1065--1070, October 1997

Muir, J (2003) "Decoding Mobile Device Security", available at: http://www.computerworld.com/securitytopics/security/story/0,10801,82890,00.html, date accessed: 19 October 2007

Ofcom (2007) "The International Communications Market 2007", research document, available at: http://www.ofcom.org.uk/research/cm/icmr07/icmr07.pdf, date accessed: 09 January 2009

Perelson. S. and Botha, R.A. (2004) “An Investigation into Access Control for Mobile Devices”, *ISSA 2004*, Gallagher Estate, Johannesburg, South Africa

Rao, J.R., Rohatgi, P., Scherzer, H. and Tinguely, S (2002) "Partitioning Attacks: Or How to Rapidly Clone Some GSM Cards", *IEEE Symposium on Security and Privacy*, 2002, sp, p. 31,

Stefan A. (2000) “Intrusion Detection Systems: A Survey and Taxonomy”, Department of Computer Engineering, Chalmers University of Technology, Goteborg, Sweden

Sun, B., Chen, Z., Wang, R., Yu, F and Leung, V.C.M. (2006) “Towards adaptive anomaly detection in cellular mobile networks”, *Consumer Communications and Networking Conference, 2006 (CCNC 2006)*, Vol:2, pp. 666-670, ISBN: 1-4244-0085-6

Sun, B., Yu, F., Wu, K. and Leung, VCM (2004) “Mobility-based anomaly detection in cellular mobile networks”, *Proceedings of ACM wireless security (WiSe’ 04)*, Philadelphia, PA, 2004, pp. 61-69

Swami, Y. P. and Tschofenig, H (2006) “Protecting mobile devices from TCP flooding attacks”, *Proceedings of first ACM/IEEE international workshop on Mobility in the evolving internet architecture*, pp. 63 – 68, 2006