2010

# Behaviour profiling on mobile devices

Fudong Li

Nathan Clarke
*Edith Cowan University*

Maria Papadaki

Paul Dowland

10.1109/EST.2010.26

# Behaviour Profiling on Mobile Devices

Fudong Li[1], Nathan Clarke[1,2], Maria Papadaki[1], Paul Dowland[1]

*[1] Centre for Security, Communications and Network Research (CSCAN), School of Computing & Mathematics, University of Plymouth, Plymouth, PL4 8AA, United Kingdom*
*info@cscan.org*
*[2] School of Computer and Information Science, Edith Cowan University, Perth, Western Australia*

## Abstract

*Over the last decade, the mobile device has become a ubiquitous tool within everyday life. Unfortunately, whilst the popularity of mobile devices has increased, a corresponding increase can also be identified in the threats being targeted towards these devices. Security countermeasures such as AV and firewalls are being deployed; however, the increasing sophistication of the attacks requires additional measures to be taken. This paper proposes a novel behaviour-based profiling technique that is able to build upon the weaknesses of current systems by developing a comprehensive multi-level approach to profiling. In support of this model, a series of experiments have been designed to look at profiling calling, device usage and Bluetooth network scanning. Using neural networks, experimental results for the aforementioned activities' are able to achieve an EER (Equal Error Rate) of: 13.5%, 35.1% and 35.7%.*

## 1. Introduction

Over the last decade, the mobile device has changed significantly; becoming a multimedia and multi-functional device. The mobile telephone alone, a subset of the mobile devices, has over 4.1 billion subscribers around the world. The modern mobile device is capable of providing a wide range of services over several network connections on a continual basis. As a result, many people rely upon these services and information to complete their business and personal tasks. Such tasks can include accessing email via a wireless network, online shopping through a 3G network, sharing pictures over a Bluetooth connection, and reading documents. The nature of many of these activities is likely to be either personally or corporately sensitive.

While people enjoy the convenience and pleasure the mobile device provides, it can also bring several security concerns, such as service fraud, lost or stolen handsets, SIM (Subscriber Identity Module) card cloning [1], malware, information disclosure, and Denial of Service (DoS) [2]. For the malware alone, although it was discovered a few years ago, the number of incidents is growing significantly every year. For instance, Kaspersky have already identified a total number of 106 mobile malware families with 514 modifications since 2004 [3].

To counter these security threats, various mobile security solutions have been proposed and developed in the area of authentication, firewalls and antivirus. However, given the increasing sophistication of the threats, additional countermeasures present in the desktop environment are being considered for use on a mobile device. Intrusion Detection Systems (IDSs) are one such technology. Unfortunately, the current nature of IDSs deployed within the desktop environment is significantly different to the mobile environment, with differing stakeholders, requirements and capabilities. In addition, research to date in the area of mobile IDS has been limited to identifying specific threats rather than taking a comprehensive approach [4]. This paper focuses upon presenting the findings from a feasibility study into utilising behavioural profiling to successfully identify mobile device misuse.

This paper begins by introducing the threats associated with a mobile device, and general security controls. Section 2 identifies the key research completed to date. Section 3, presents the methodology for a series of experimental studies on three aspects of mobile user's behaviours: telephony, device usage, and Bluetooth scanning. The results from the experiments are presented along with the discussion in section 4. The paper then proceeds to propose a Host-based Multi-Level Behaviour Profiling Mobile IDS framework. The paper concludes with highlighting the future work.

## 2. Mobile Intrusion Detection System

The IDS is an established research area for more than 20 years. There is extensive research on computer-based IDSs, but limited emphasis has been given so far on mobile IDSs. So, the focus of this section is to review existing research on mobile IDS: namely behaviour-based and signature-based IDSs.

978-0-7695-4175-4/10 $26.00 © 2010 IEEE
DOI 10.1109/EST.2010.26

### 2.1. Behaviour Based Mobile IDS

The research for mobile IDS started around 1995 with preliminary focus upon detecting telephony service fraud. By monitoring users' calling behaviour and migration activity, the aforementioned attack can be detected.

The telephony based mobile IDS monitors user's calling features (e.g. start time of call, duration of call, dialled telephone number and national or international call). By using the combination of these features, a historical profile is acquired. Any deviation between the current calling session and the historical profile that exceeds a threshold, is identified as an intrusion. Several studies were proposed by using this procedure, such as the European ASPECT (Advanced Security for Personal Communication Technologies) project [5], [6], and [7].

Migration based mobile IDS monitors the mobile user's migration activities through mobile cell networks. By profiling a mobile user's migration mobility or migration itinerary activities, telephony service frauds could be detected. A number of studies have been carried out by using users' migration activity: [8-9] employed user's mobility, and [10] used user's migration itinerary.

In generally, behaviour based mobile IDS has an average high detection rate; also, as the detection process is carried out by the network operator, there is no overhead for the mobile device. On the other hand, as the mobile device has changed significantly, the network operator could not monitor all the behaviour any more such as Internet surfing over WiFi networks.

### 2.2. Signature Based Mobile IDS

It is widely recognised that the battery plays a key role in a mobile device. Attacking the battery is a major threat for the mobile device's availability; as the battery runs out, the device becomes unusable. In order to counter battery consumption as a result of security threats, such as malware and DoS, several studies on signature based mobile IDS have been conducted: such as, Power Secure Architecture [11], and Gibraltar [12]. They work in a similar fashion: each mobile application consumes unique power and so does the malware. As a result, by analysing battery activities, attacking signatures can be obtained. By comparing the current battery status with attacking signatures, any matches will be identified as an intrusion.

The advantage for the signature based mobile IDS is it has a low false alarm rate and meaningful descriptions for the intrusion. However, obtaining mobile malware's signatures can be a difficult task; furthermore, it can not provide detection for service related attacks such as abusing the telephony service or data modification on the mobile device.

### 2.3. Summary Of Current Mobile IDS

From the aforementioned literature, it suggests that the behaviour based mobile IDS is able to detect telephony service fraud attacks and the signature based mobile IDS can identify possible malware and DoS attacks. However, in practice it can be seen that the calling and migration behaviours were monitored by a single network provider, rather than being host-based, and the signature based mobile IDSs have limited signatures in the database and thus cannot provide much detection for user related activities. In addition, as increased functionality, usability and compatibility, users are now experiencing a far larger set of mobile activities illustrated in the last column of Table 1. Therefore none of the current research in mobile IDS truly provides a compressive protection against device misuse independent of service or application being used. 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.

**Table 1. Taxonomy of mobile usage**

| Category | Behaviours | Examples |
|---|---|---|
| Application level | Telephony | Call a friend |
| | Text | Send greeting through SMS |
| | MMS | Send picture through MMS |
| | File access | Write and save a document |
| | Data | Create a copy of work data |
| | Web | Read news from the internet |
| Network level | 3G | Access emails |
| | Bluetooth | Share picture |
| | Wi-Fi | Connect to a Wi-Fi network |
| Machine level | CPU | 16% CPU is in use |
| | Memory | 12M Memory is allocated |
| | Battery | An application consumes 1% of the battery |

## 3. Feasibility of host-based Behavioural Profiling

When looking to develop an IDS for a mobile device, the traditional network-based approaches are infeasible given the various networking technologies a single device is able to use and the differing stakeholders that own them. Therefore a host-based approach must be considered. Given the difficulty of establishing signatures in the first instance [12], and their inability to detect unknown attacks, a profiling was taken. However, little literature to date has tested the discriminative nature of service utilisation. Building upon the taxonomy identity in Table 1, a series of experiments have been conducted within each category or level: application, network and machine.

### 3.1. Experimental Procedure

An MIT Reality dataset was utilised. The dataset contained 94 participants' mobile device activities recorded from September 2004 to June 2005 [13]. The data was collected from the Nokia 6600 phone which was preinstalled with automatic logging software.

**Table 2. The MIT Reality dataset**

| Activity | Number Of Logs | Information Contains |
|---|---|---|
| Application | 662393 | Application name, date and time of usage |
| Bluetooth scanning | 1994186 | Date, time of each scan along and individual device's MAC address |
| Charge | 11506 | Date and time when the mobile is in charge |
| Device usage | 574788 | Date and time the mobile has been in use |
| On | 13012 | Date and time when the phone is turned on |
| SMS | 5607 | Date, time and number of texting |
| Voice | 54440 | Date, time, number of calling and duration |

As shown in Table 2, the dataset contains a rich volume of information which covers all the levels of mobile device usage. The experiment analysed the telephony, device usage, and Bluetooth scan activities; as representative of application level, machine, and network levels.

Telephony service was the first service invented for the mobile device. People use it to communicate with other people over a voice channel. The telephony service still dominates the mobile market along with increasing revenues across the globe [14]. The prior literature shows that the calling behaviour has been studied a number of times over the telecommunication service provider's network environment and it can be used to discriminate users. However, within the mobile host environment, the calling features have changed slightly, such as the IMSI can not be utilised anymore. Hence, it is important to establish whether the calling features still remain a positive attribute that can be used within a host-based environment.

Once the mobile device is in use, it becomes active; otherwise it may be either idle or switched off. When the mobile device is in the active mode, the following three scenarios would happen: a) the user views whatever information appears on the home screen, but does not interact with any applications; b) the user utilises one application, then sends the device to idle mode; c) the user uses more than one application to perform a task over one active session. For example, the user takes a photograph, views it, and emails it to a friend over a Wi-Fi connection. Whilst the example shows that the user utilises at least three applications to perform one big task over an active session, this particular experiment is simply focussed upon whether the device is in use and how unique and discriminative this information is.

Bluetooth is one of the short range networking technologies employed by the mobile device to communicate with nearby Bluetooth enabled devices. In order to do this, the mobile device has to scan nearby Bluetooth enabled device. Each scan may come up with a list of devices. Each device has a unique MAC address. Given the nature of a Personal Area Network (PAN) certain Bluetooth MAC address(es) may keep showing up on the scan list. For example, a user has a Bluetooth enabled headset, so its MAC address should appear on the Bluetooth scan list. Therefore it is possible to hypothesise, that a mobile device will encounter a familiar set of MAC addresses during normal activity – particularly within home and work environments. By learning those familiar Bluetooth MAC addresses, certain locations and potential trust can be established.

For data processing reasons, the experiment employed the first 30 users' activities over the first 10-month period. For each experiment however, only one month's activities were extracted for each individual activity in order to minimise any resulting inaccuracy, as it is likely that user's behaviour could change over time [15]. Template renewal or refresh is something that will be tackled once the feasibility of such an approach is proven. A series of iterative experiments were conducted across the three activities and complete time period.

## 4. Result and Discussion

### 4.1. Telephony

Table 3 shows the experimental results for the first 30 users one month's calling behaviour. Five calling features were utilised: the calling number, the day of calling, the time of calling, the duration of the conversation, and the weekday. The weekday feature was calculated by using the day feature; as people's activity on different weekdays could be different [4] [12]. A Radial Basis Network (RBF) was utilised in favour of other approaches given its previous success in [4] [7]. The configuration of which was iteratively modified to optimise performance. By using all five features, the best average Equal Error Rate (EER) achieved is 15.6% and it was achieved by using 150 neurons. Apart from the calling number, every other feature was removed from the neural network configuration in turn to understand the value that feature had upon performance. The best average EER was 13.5% and this was achieved by using 125 neurons with number of calling, the day, weekday, and duration. By using number of calling, time of calling, weekday and duration, the system got the highest average EER of 17.7%.

Table 3. Experimental result on calling

| Neurons | Features | Average EER | Best user |
|---|---|---|---|
| 150 | Number, day, time, week, duration | 15.6% | 0% |
| 130 | Number, time, week, duration | 17.7% | 7.1% |
| 125 | Number, day, week, duration | 13.5% | 0% |
| 135 | Number, day, time, duration | 13.6% | 0% |
| 140 | Number, day, time, week | 15.4% | 0% |

As shown in Table 3, the overall result for calling behaviour is positive – remembering the nature of this type of profiling is unlikely to result in EER in the same order of magnitude as physiological biometrics. As the number of features decreases, the number of required neurons also decreases; indicating that proper selection of the strong and positive features would save a significant amount of computing power. This is especially important in the mobile device environment: fast, accurate detection by using minimal computer power.

### 4.2. Device Usage

The device usage behaviour study also employed the first 30 users' information from the MIT Reality dataset. For the active behaviour, the following features were extracted from the dataset: the day, time, duration and weekday. Within table 4, the best average EER is 35.1% and this was achieved by using 5 neurons with the time, day, duration and weekday. The best individual user EER is 1% by using 7 neurons in the RBF neural network with the day, duration and weekday features. Interestingly, with the same neuron network configuration, 43% of the whole population achieved less than 30% of the EER, although majority of them have an EER in the region of 20%-30%.

Table 4. Experimental results on active

| Neurons | Features | Average EER | Best user | Proportion of users EER<30% |
|---|---|---|---|---|
| 5 | Time, day, duration, weekday | 35.1% | 3.87% | 36.7% |
| 7 | Time, day, duration | 35.8% | 3.82% | 40% |
| 7 | Day, duration, weekday | 36.2% | 1% | 43% |
| 5 | Time, day, weekday | 36.4% | 3.1% | 33.3% |

As there is no indication that what purpose the device has been used for, only knowing a usage occurred, the usability for distinct mobile users reduces significantly. However, this could be improved by knowing what has happened during the active duration: such as, one text message was sent. Moreover, the result does indicate that device usage can be used for identifying a subset from the entire mobile population; as at least 1/3 of the users have an EER rate less than 30%.

### 4.3. Bluetooth Scan

As the mobile device's Bluetooth scan performs passively every 5 minutes, a huge amount of information was available for processing. Given the repeated nature of the scans, samples may keep reappearing if the user stays in one location for a while, for example watching a film in the cinema or taking a lecture in the classroom. As a result, the experiment employed the first 30 users' Bluetooth scans which performed at 10 o'clock each day. However, due to the aforementioned restriction, only the MAC address, the day, and the week features were extracted from the sub dataset. Table 5 describes the experimental result on the Bluetooth scanning activities. By using 20 neurons with the MAC address and the day as the inputs, the RBF neural network achieved the best average EER of 35.7%. By using the same configuration, 30% of the experiment users have less than 30% EER. For the best individual user's EER, 0% was achieved in both RBF neural configurations.

Table 5. Experimental results on Bluetooth scanning

| Neurons | Features | Average EER | Best user | Proportion of users EER<30% |
|---|---|---|---|---|
| 15 | MAC address, day, week | 36.1% | 0% | 26.7% |
| 20 | MAC address, day | 35.7% | 0% | 30% |

Table 5 does show a positive set of results from Bluetooth scan behaviour, although the result is a little bit noisy. It may cause by the nature of Bluetooth scan behaviour, as the content of a Bluetooth scan list heavily relies on other Bluetooth enable devices. For example, in an office environment, a mobile user's Bluetooth scan list may contain colleagues' Bluetooth enabled device and a number Bluetooth enabled desktop PCs; as the colleagues come in and out the office, the user's Bluetooth scan list will change accordingly. The scan list may change slightly but within a familiar set of MAC addresses. Also, the experimental results show that a proportion of users' Bluetooth scanning behaviour are quite predictable as 30% of them have an EER less than 30%.

From the above three experiments, the positive results identify that the calling, device usage and Bluetooth scanning behaviours used to profile mobile users. However, the level of performance is such that no single feature could be utilised to make decisions over misuse – the inconvenience of being wrongly identified would be too high. This suggests that a new mobile IDS could have a behaviour selector for each individual user to choose correct behaviour accordingly. Moreover, it can also be seen that the individual user's performance with each activity differs – thereby suggesting that an IDS system capable of weighting the input features on an individual user basis would be better suited to optimising overall performance. Finally, whilst individual results will go someway in understanding the legitimacy of a user, the combination or fusion of multiple inputs would only serve to support the decision making process [16, 17].

## 5. Host Based Multi-level Behaviour Profiling Mobile IDS Framework

With the aim of providing accurate and robust detection of misuse, a proposed framework is presented in Figure 1. The Host-based Multi-level Behaviour Profiling Mobile IDS framework is capable of processing multiple user activities from all levels of the taxonomy identified in Table 1 and intelligently interpreting the results to provide a more robust decision making process.

As shown in Figure 1, all the user's mobile behaviours can be used as the system input; the input can be one activity or the combination of multiple behaviours. For example: Wi-Fi activity from the network level. Also, the system can select a combination of multiple inputs; for example, when a user surfs the Internet, surfing features (explorer, web address, day and time of visiting) from the application level, network features (network type, number of data packets, and transmission rate) from the network level, and CPU usage from the machine level. As each individual user may have a different way to use the mobile device, therefore the system employs a Multi-Level Behaviour Selector to choose appropriate inputs accordingly. The selection process is carefully considered and the selection criteria are defined differently for individual behaviour. For example, the percentage of unique dialled numbers: when it is bigger than the threshold, the calling activity will be selected; as the user makes a unique set of calls, it is much easier to profile the user's behaviour. Another example is the frequency of application usage; when it is smaller than the threshold, that application's features will not be used as the input; as if an application is not regularly used, there will not be enough information to help the profile building. Also, as the user's behaviour may change over time, the Multi-Level Behaviour Selector will update the input selection accordingly.

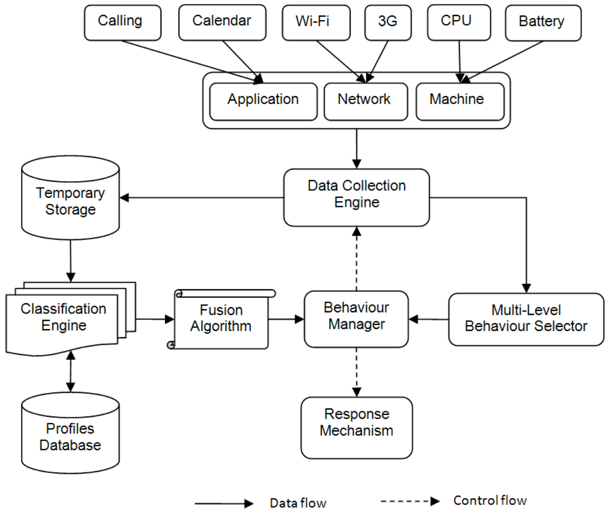

**Fig. 1. Host based multi-level behaviour profiling mobile IDS framework**

Following by the information provided by the Multi-Level Behaviour Selector, the Behaviour Manager sends a command to the Data Collection Engine to collects the user behaviour features accordingly. Depending on the selected inputs, the Classification Engine can use various classification methods to compare the current activity against the profile: such as neural networks, fusion functions, and decision trees. The result will be further processed by the Fusion Algorithm. The Fusion Algorithm calculates the weight for each activity as each behaviour has a different impact on the decision making; for example, a more regular used application will have more weight on the decision when compared with others. The Behaviour Manager then sends the decision to the Response Mechanism, such as launching antivirus software, restricting access to certain applications, or even locking down the mobile device.

As the Host based Multi-Level Behaviour Mobile IDS framework takes all the possible activities as the inputs, so it will provide full detection for all the mobile applications, the network connection and machine levels. Moreover, the framework will operate independently for each individual mobile user.

## 6. Conclusion

It is essential that new approaches are developed to enable real time detection of mobile misuse on both known and unknown threats. Given the personal nature of the mobile device, behavioural profiling provides an opportunity to closely map an individual's use of a device. The experiments have demonstrated that individual activities can indeed be profiled and used to identify legitimate and illegitimate use.

The strength of this identification however is highly variable between users with some experiencing very high levels of classification and others not. Given this variability no single technology would be stable for uniform deployment but rather through the utilisation of multiple activities within an appropriately flexible and robust framework, a more secure yet convenient approach can be realised.

Future work will seek to identify further activities that can be used for classification. Focus will also be given to the theoretical and practical issues surrounding the proposed framework.

## 7. References

[1] Rao, J.R., Rohatgi, P., Scherzer, H., Tinguely, S.: Partitioning Attacks: Or How to Rapidly Clone Some GSM Cards. In: the 2002 IEEE Symposium on Security and Privacy, pp. 31--41. IEEE Computer Society, Washington, DC, USA (2002)

[2] Swami, Y. P.,Tschofenig, H.: Protecting mobile devices from TCP flooding attacks. In: Proceedings of first ACM/IEEE international workshop on Mobility in the evolving internet architecture, pp.63--68. ACM, New York (2006)

[3] Kaspersky Lab, http://www.viruslist.com/en/analysis?pubid=204792080, date of access: 02 February 2010.

[4] Li, F., Clarke, N.L., Papadaki, M.: Intrusion Detection System for Mobile Devices: Investigation on Calling Activity. In: Proceedings of the 8th Security Conference, April, Las Vegas, USA (2009)

[5] Gosset, P.:ASPeCT: Fraud Detection Concepts: Final Report. Doc Ref. AC095/VOD/W22/DS/P/18/1, (1998)

[6] Samfat, D., Molva, R.: IDAMN: an Intrusion Detection Architecture for Mobile Networks. In: IEEE Journal on Selected Areas in Communications, vol. 15, pp.1373--1380. IEEE (1997)

[7] Boukerche, A., Nitare, M.S.M.A.: Behavior-Based Intrusion Detection in Mobile Phone Systems. In: Journal of Parallel and Distributed Computing, vol. 62, Issue 9, pp. 1476-1490. Academic Press, Inc. Orlando, FL, USA (2002)

[8] Buschkes, R., Kesdogan, D., Reichl, P.: How to increase security in mobile networks by anomaly detection. In: proceedings of the 14th Annual Computer Security Applications Conference, pp. 3--12. IEEE Computer Society, Washington, DC, USA (1998)

[9] Sun, B., Chen, Z., Wang, R., Yu, F., Leung, V.C.M.: Towards adaptive anomaly detection in cellular mobile networks. In: the IEEE Consumer Communications and Networking Conference, 2006 (CCNC 2006), Vol. 2, pp. 666--670. IEEE (2006)

[10] Hall, J., Barbeau, M., Kranakis, E.: Anomaly-based intrusion detection using mobility profiles of public transportation users. In: the Proceeding of IEEE International Conference on Wireless And Mobile Computing, Networking And Communications, 2005 (WiMob'2005), vol. 2, pp. 17--24. IEEE (2005)

[11] Martin, T., Hsiao, M., Ha, D., Krishnaswami, J.: Denial-of-Service Attacks on Battery-powered Mobile Computers. In: Second IEEE International Conference on Pervasive Computing and Communications, pp. 309--318. IEEE Computer Society, Washington, DC, USA (2004)

[12] Jacoby, G.A., Hickman, T., Warders, S.P.: Gibraltar: A Mobile Host-Based Intrusion Protection System. In: Proceedings of the 2006 International Conference on Security & Management, pp.207--212, Las Vegas, Nevada, USA (2006)

[13] Eagle, N., Pentland, A., Lazer, D.: Inferring Social Network Structure using Mobile Phone Data. In: Proceedings of the National Academy of Sciences (PNAS), vol 106, pp.15274--15278. PNAS (2009)

[14] Ofcom, http://www.ofcom.org.uk/research/cm/cmr09/cmr09.pdf, date accessed: 15 February 2010

[15] Biermanna, E., Cloeteb, E., Venterc, L.M.: A comparison of Intrusion Detection systems. In: Computer & Security, Vol 20, pp.676--683. Elsevier (2001)

[16] Lerouge, E., Moreau, Y., Verrelst, H., Vandewalle, J., Stoermann, C., Gosset, P., Burge, P.: Detection and management of fraud in UMTS networks. In: Proceeding of the Third International Conference on The Practical Application of Knowledge Discovery and Data Mining (PADD99), pp. 127--148. (1999)

[17] Furnell, S., Clarke, N., Karatzouni, S.: Beyond the PIN: Enhancing user authentication for mobile devices. In: Computer Fraud & Security, Vol 2008, Issue 8, pp. 12--17. Elsevier (2008)