1-1-2011

Behaviour Profiling for Transparent Authentication for Mobile Devices

Fudong Li

Nathan Clarke
Edith Cowan University

Maria Papadaki

Paul Dowland

Behaviour Profiling for Transparent Authentication for Mobile Devices

Fudong Li[1], Nathan Clarke[1, 2], Maria Papadaki[1] and Paul Dowland[1]
[1]University of Plymouth, UK
[2]Edith Cowan University, Perth, Western Australia
info@cscan.org

Abstract: Since the first handheld cellular phone was introduced in 1970s, the mobile phone has changed significantly both in terms of popularity and functionality. With more than 4.6 billion subscribers around the world, it has become a ubiquitous device in our daily life. Apart from the traditional telephony and text messaging services, people are enjoying a much wider range of mobile services over a variety of network connections in the form of mobile applications. Although a number of security mechanisms such as authentication, antivirus, and firewall applications are available, it is still difficult to keep up with various mobile threats (i.e. service fraud, mobile malware and SMS phishing); hence, additional security measures should be taken into consideration. This paper proposes a novel behaviour-based profiling technique by using a mobile user's application usage to detect abnormal mobile activities. The experiment employed the MIT Reality dataset. For data processing purposes and also to maximise the number of participants, one month (24/10/2004-20/11/2004) of users' application usage with a total number of 44,529 log entries was extracted from the original dataset. It was further divided to form three subsets: two intra-application datasets compiled with telephone and message data; and an inter-application dataset containing the rest of the mobile applications. Based upon the experiment plan, a user's profile was built using either static and dynamic profiles and the best experimental results for the telephone, text message, and application-level applications were an EER (Equal Error Rate) of: 5.4%, 2.2% and 13.5% respectively. Whilst some users were difficult to classify, a significant proportion fell within the performance expectations of a behavioural biometric and therefore a behaviour profiling system on mobile devices is able to detect anomalies during the use of the mobile device. Incorporated within a wider authentication system, this biometric would enable transparent and continuous authentication of the user, thereby maximising user acceptance and security.

Keywords: mobile device, behaviour profiling, applications, transparent authentication

1. Introduction

The modern mobile handheld device is capable of providing many services through a wide range of applications over multiple networks as well as on the handheld itself, such as: voice calling through service provider's network, Internet surfing via Wi-Fi hotspots, video conferencing through a 3G connection, road navigating by GPS (Global Positioning System), picture sharing by using Bluetooth pairing, data synchronising with laptop/desktop computers, document creation and modification, and entertainment (i.e. playing music). Indeed, the functionality and interconnectivity of mobile devices only tends to increase with time.

While people enjoy the convenience provided by mobile devices, there are also threats which could make their life less comfortable, such as the loss or theft of the device, service fraud, SIM (Subscriber Identity Module) card cloning, mobile malware, information disclosure, DoS (Denial-of-Service) attacks, Smishing (SMS (Short Message Service) phishing) and Vishing (Voice phishing). Mobile malware could harm the mobile phone in a variety of ways, such as: infecting files and damaging user data. Since discovered in 2004, there are more than 106 malware families with 514 variants having been identified (Securelist 2010). Smishing and Vishing are new types of phishing attacks which are performed by utilising text messaging and telephone calls (FBI 2010). If the phone owner is fooled, its personal information can be exposed and abused.

With the aim to counter mobile threats, a number of security mechanisms have been developed both on the mobile device and the service provider's network. The PIN (Personal Identification Number) based authentication method is the most widely deployed approach on mobile devices. Although widely used, many users do not employ the technique properly (i.e. never changing the PIN) (Clarke and Furnell 2005; Kurkovsky and Syta 2010). Mobile antivirus software and firewall applications are mainly deployed for detecting malware presence and blocking unwanted network traffic. Nonetheless, obtaining the latest virus signatures and updating rules for network traffic are not easy tasks; furthermore, their ability to detect user related activities is limited. As a mobile device has limited computing power, more sophisticated mechanisms, such as IDS (Intrusion Detection System), are primarily deployed on the service provider's network. These systems monitor the mobile users' calling and migration activities to detect telephony service fraud. However, given the modern mobile device has the ability to access several networks simultaneously and accommodate a wide range of services, existing network-based security mechanisms are unable to provide comprehensive protection for the mobile handset. This paper focuses upon presenting the findings from a feasibility study into utilising a host-based behavioural profiling approach to identify mobile device misuse, and providing continued and transparent protection for mobile devices.

This paper begins by introducing various mobile device applications, mobile threats, and general security mechanisms and continues to describe the current state-of-the-art. A series of experimental studies on two aspects of user's applications usage (application-level and application-specific) are presented in Section 3, with the following section describing the results. The paper then proceeds to discuss the results and conclude with highlighting the future direction of the research.

2. Behaviour-based mobile device security mechanisms

Research in mobile device security has been an established area for more than 10 years with a substantial amount of activity focused upon the areas of authentication, antivirus, firewalls, and IDS. Of particular interest however is the research that has been undertaken in behaviour-based mechanisms. This research falls primarily into two categories: behaviour-based network and behaviour-based host mechanisms.

2.1 Behaviour-based *network* mobile security mechanisms

The research for studying mobile behaviour-based mechanisms started around 1995 mainly focusing upon the area of IDS. These mobile IDSs monitor user calling and migration behaviour over the service provider's network, and detect telephony service fraud (Gosset 1998; Samfat and Molva 1997; Boukerche and Nitare 2002). One particularly successful approach is based upon developing a profile of users calling history over a period of time and comparing this historical profile against current usage, with deviations above a predefined threshold resulting in an alarm. Various supervised and unsupervised classifiers were successfully developed to deal with various attributes of the problem-space (known and unknown attack vectors) and the resulting systems were combined so that the strengths of each approach can be capitalised upon (Gosset 1998).

Research has also focused on the use of geo-location information as a basis for detecting misuse. Based upon the hypothesis that people have a predictable travelling pattern, the migration based mobile IDS monitors a user's location activities to detect abnormal behaviour. The user's location information can be obtained either from the mobile cellular network (i.e. cell ID) or via a GPS link (i.e. longitude, latitude). By recording the users' location information over a time period, a mobility profile can be generated. When a mobile user carries their device from one location to another, the probability of the event will be calculated. If this surpasses a threshold, then the current event will be considered as an intrusion. A number of studies have been carried out by profiling user migration activities, such as: Buschkes *et al* 1998, Hall *et al* 2005, and Sun *et al* 2006.

By studying a user's calling or location activities, behaviour based IDSs can achieve a high detection rate and offer the ability to detect unforeseen attacks. In addition, as the classification and identification procedures are processed by the network service provider, it does not require any additional computational power from the mobile device. This has traditionally been critical for mobile devices, as they have limited processing power and space comparing with traditional desktop computers. Nonetheless, if these behaviour-based systems work together to monitor the mobile user's action (i.e. calling a friend) while knowing where the action is taken (i.e. at home), an overall system performance could arguably be increased.

2.2 Behaviour-based *host* mobile security mechanisms

Existing host behaviour-based mobile security systems are mainly authentication-based systems. These systems usually employ one or more characteristics of a user's behaviour to assess the legitimacy of the current user – techniques include keystroke analysis and gait recognition.

Keystroke analysis based authentication systems monitor users' keystroke patterns, typically monitoring the inter-keystroke latency and hold-time. The authentication can be performed in two modes: static (text dependent) and dynamic (text independent). In the static mode, users will be authenticated when a specific word or phrase has been entered. For instance, the system will authenticate the user when they enter a PIN to unlock their mobile devices. In the dynamic mode, a user's legitimacy will be checked based upon their typing speed and rhythm independent of what they type. For example, authentication will transparently occur while the user composes a text message. Previous work in this area include Clarke and Furnell (2006), Buchoux and Clarke (2008), and Campisi *et al.* (2009). With an average experimental EER of 13%, keystroke analysis based authentication systems can be deployed in practice to provide extra security for a mobile device. However, this method is only practical in scenarios with sufficient keystroke activity (i.e. activities such as reading a document or viewing a picture would be unlikely to generate sufficient data to successfully validate a users' identity).

Gait recognition is based upon the theory that people can be discriminated by how people walk when they carry their mobile device (Boyd and Little, 2005). When a user carries their mobile device in their trouser pocket, the user's gait information can be collected (Derawi *et al* 2010). The user's gait data can then be compared with an existing template. If it matches, the user is considered legitimate; otherwise, they are an intruder. The experiment result shows that an EER of 20.1% can be achieved. It shows the possibility to deploy this method on a mobile handset. However, as the authentication process is heavily reliant on user's gait information, this could leave the mobile device unprotected when gait information is not available – for example when the user sits in the office.

2.3 Summary of current mobile behaviour security mechanisms

The aforementioned literature suggests that existing behaviour-based network IDSs can detect calling service fraud attacks. However, in practice it can be seen that the mobile network operator can only monitor calling and migration behaviours, rather than examining every single mobile service. For the existing host-based behaviour authentication system, it could only provide periodically security when the user interacts with the device in the desired manner (e.g. when the keypad is touched or the device is carried in the back pocket). Therefore, none of the current research in mobile behaviour security mechanisms provides a comprehensive and continuous protection against device misuse. Hence, a mobile security mechanism which can offer detection across a wider range of services and connections on the mobile device is needed.

3. Behaviour profiling for transparent authentication for mobile devices

The previous section shows that the network-based behavioural security mechanisms can only monitor network-based services through the service provider's network. As current mobile devices have the ability to access multiple networks simultaneously, a host based approach must be taken into consideration when designing the new system. With the difficulty of obtaining and updating the signatures and the lack of the ability to detect unforeseen threats, a behaviour profiling technique should be taken. As application usage represents an overview of how the user interacts with the device (Miettinen *et al* 2006), and due to the lack of research regarding the discriminatory nature of application usage within a mobile device environment, an experiment was developed focussing upon two aspects: application-level and application-specific user interactions.

3.1 Experiment procedure

The experiment employed a publicly available dataset provided by the MIT Reality Mining project (Eagle *et al* 2009). The dataset contains 106 participants' mobile phone activities from September 2004 to June 2005. By using preinstalled logging software, various mobile data attributes were collected from participants' using Nokia 6600 mobile phones. As shown in Table 1, the MIT Reality dataset contains a large and varied selection of information which covers two levels of application usage: application-level information (general applications) and application-specific information (voice call and Text message).

Table 1: The MIT Reality dataset

Activity	Number of logs	Information contains
General applications	662,393	Application name, date, time of usage and cell ID
Voice call	54,440	Date, time, number of calling, duration and cell ID
Text message	5,607	Date, time, number of texting and cell ID

3.1.1 Application-level analysis

By default, a number of common applications are preinstalled on the mobile device by the manufacture, such as: phonebook, clock and voice calling. With increased computing processing power and storage space and almost 15,000 new mobile applications becoming available on the market every month, mobile users have the freedom of installing any additional applications on the device (Distimo 2010). From a high-level perspective the general use of applications can provide a basic level of information on how the mobile user utilises the device. Such basic information could be the name of the application, time, and location of usage. Given the hypothesis that mobile users utilise their mobile applications differently (i.e. two users utilise different applications in different time periods and at different locations), an experiment was devised to explore the possibility of utilising application-level information for discriminating mobile device users.

3.1.2 Application-specific analysis

The second experiment focussed upon utilising further information about the applications. Within many applications the user connects to data that could provide additional discriminatory information. For instance, when surfing the Internet, the Internet browser can capture all the URLs an individual accesses. Unfortunately, due to limitations on the dataset (collected prior to data-based applications becoming prevalent), the range of application-specific analysis that could be undertaken were limited to telephony and text messaging.

The prior literature shows that calling behaviour has been studied several times in a network-based environment with results demonstrating the ability to discriminate mobile phone users. Within a mobile host environment, the availability of calling features does change slightly – for example, the IMSI (International Mobile Subscriber Identity) is not a useful feature in a host-based solution. Furthermore, although several studies suggested utilising a user's location information, it was never been treated as a calling feature. Therefore, it was interesting to identify the effectiveness of a new set of calling features, which included the user's location information.

Due to the enormous use of text messaging, with the UK alone sending more than 100 billion text messages in 2010 (Ofcom 2010), the application is amongst the most widely used application on a mobile device. Despite the high volume of text message usage, little research has been undertaken to show how text messages may be used to detect abnormal usage in the mobile environment. Hence, it was also deemed important to discover the possibility and usefulness of employing text messaging to detect anomalous mobile user's behaviours.

For methodological reasons: to maximise the number of participants within a reasonable timeframe, the experiment employed 76 participants whose activities occurred during the period of 24/10/2004-20/11/2004. As not all participants started or finished the experiment at the same time, it was imperative to isolate a sub-section of the dataset that maximised the number of participants and available data. The methodology employed two types of profile techniques: static and dynamic. For the static profiling, each individual dataset was divided into two halves: the first half was used for building the profile, and the other half was utilised for testing. For the dynamic profiling, the profile contained 7/10/14 days of the user's most recent activities; the evaluation process was carried out on the same sub-dataset as for the static experiment in order to provide a meaningful comparison. Given the highly variable nature of the input data a smoothing function was applied. Rather than taking each individual result, the smoothing function permitted the system to make a decision after a number of results were present (similar to a winner-takes-all decision-based biometric fusion model). The basis for this approach was derived from the descriptive statistics produced when analysing the data and the large variances observed. A dynamic approach therefore seemed sensible to cope with the changing nature of the profile. Based on the premise that the historical profile can be used to predict the probability of a current event, the following formula illustrated in Equation 1 was devised. The equation also includes a weighting factor to allow for more discriminative features to have a greater contribution (W_i) within the resulting score than less discriminative features. Moreover, the equation also provides a mechanism to ensure all outputs are bounded between 0 and 1 to assist in defining an appropriate threshold.

Equation 1: Alarm if: $1 - \frac{\sum_{i=1}^{N}\left(\frac{\text{Occurannce of Feature}_{ix}}{\sum_{x=1}^{M}\text{Occurannce of Feature}_{ix}} \times W_i\right)}{N}$ ≥threshold

Where:

i=The features of one chosen application (i.e. dialled number for telephony application) x=The value of Feature_i (i.e. office telephone number and home telephone number)

M=Total number of values for Feature_i

N=Total number of features

W_i=The weighting factor associated with Feature_i ($0 < W_i \leq 1$)

Threshold= A predefined value according to each individual user

4. Experimental results

4.1 Application-level profiling

For the general applications, the following features were extracted from the dataset: application name, date of initiation, and location of usage. As a total of 101 individual applications were used among the chosen 76 users during the chosen period, a final sub-dataset for application-level applications with 30,428 entry logs was formed. Among these 101 applications, the phonebook, call logs and camera were used by all participants. By using the proposed mathematical equation, a final set of EER's (Equal Error Rate) for users' application-level usage is presented in Table 2. The best EER is 13.5% and it was obtained by using the dynamic profile technique with 14 days of user activity with 6 log entries. In comparison, the worst performance was achieved by using the dynamic profile technique with 7 days of user activities with 1 log entry.

Table 2: Experimental results for application-level applications

		Number of log entries					
		1	2	3	4	5	6
Profile technique	Static 14 days	21.1%	17.4%	16.3%	14.9%	14.2%	13.6%
	Dynamic 14 days	21.1%	17.3%	16.0%	14.5%	13.9%	13.5%
	Dynamic 10 days	22.1%	17.8%	16.2%	14.6%	14.4%	13.7%
	Dynamic 7 days	24.0%	19.4%	17.6%	15.9%	15.3%	14.4%

Selected experimental results for the best configuration of application-level usage are shown in Table 3. The top 3 and bottom 3 users' EERs represent the best and worst performance respectively. Further analyses of the results show that 84% of all users have an EER less than 20%.

Table 3: Selected users' performance for application-level applications with dynamic 14 days and 6 log entries

User_ID	EER
71	0%
46	0%
12	0.5%
66	37.5%
2	39.3%
68	51.6%%

4.2 Application-specific profiling

4.2.1 Telephony

For the telephone call application, a subset of 71 users from the 76 participants used the application during the aforementioned chosen period. During the same period, 2,317 unique telephone numbers were dialled and the total number of calls made was 13,719. From iteration and optimisation, the following features were chosen for each log: the telephone number, date and location of call. By using the aforementioned mathematical formula with the selected features (all features were given the same weighting factor), a final set of experiment results is shown in Table 4. The best result is an EER of 5.4% and it was achieved by using the dynamic profile technique with user's most recent 14 days activity and 6 log entries.

Table 4: Experimental results for telephone call application

		Number of log entries					
		1	2	3	4	5	6
Profile technique	Static 14 days	9.6%	9.1%	7.9%	7.2%	4.3%	6.4%
	Dynamic 14 days	8.8%	8.1%	6.4%	6.4%	6.3%	5.4%
	Dynamic 10 days	9.6%	8.6%	8.1%	7.2%	6.9%	6.0%
	Dynamic 7 days	10.4%	8.8%	8.5%	7.3%	7.0%	6.2%

A selection of experimental results for the best set up of the telephone call application is presented in Table 5. The best and worst performances for selected users are the top 3 and bottom 3 users accordingly. Furthermore, 81.7% of users have an EER less than 10%.

Table 5: Selected users' performance for telephone call application with Dynamic 14 days and 6 log entries

User_ID	Performance
23	0%
43	0%
61	0%
64	20.6%
50	23.1%
8	39.5%

4.2.2 Text messaging

For the text messaging experiment, 22 users' text messaging activities were available from the 76 participants, during the chosen period. The text messaging dataset contains 1,382 logs and 258 unique texting numbers. For each text log, the following features were extracted: receiver's telephone number, date and location of texting. Due to certain participants having limited numbers of text messaging logs; a maximum of 3 log entries were treated as one incident. By employing the aforementioned mathematical formula and all text message's features (all features were given the same weighting factor), the final result for user's text messaging application is shown in Table 6. The best result was an EER of 2.2% and it was acquired by utilising the dynamic profile method with 14 days of user's activities and 3 log entries. Also, the performance improves considerably from 1 log entry to 2 log entries across all profiling techniques.

Table 6: Experimental results for text messaging application

		Number of log entries		
		1	2	3
Profile technique	Static 14 days	7.0%	4.3%	3.6%
	Dynamic 14 days	5.7%	2.6%	2.2%
	Dynamic 10 days	8.3%	4.1%	3.7%
	Dynamic 7 days	10.7%	5.7%	3.8%

Table 7 shows a group of users' performance for the best configuration of the text messaging application. The top 3 and bottom 3 users' EERs represent the best and worst performance respectively. In addition, 95.5% of all users have an EER smaller than 10%.

Table 7: Selected users' performance for text messaging application with Dynamic 14 days and 6 log entries

User_ID	Performance
13	0%
14	0%
18	0.2%
4	5.3%
2	8.4%
17	13.1%

5. Discussion

The application name and location have proved valuable features that can provide sufficient discriminatory information to prove useful in authentication. However, whilst this might identify many misuse scenarios, it would not necessary identify all cases of misuse – particular those where a colleague might temporarily misuse your device as the location information is likely to fall within the same profile as the authorised user. So care is required in interrupting these results. The intra-application approach should also help to specifically identify this type of misuse.

In general, dynamic profiling achieved a slightly better performance than the static profiling did. This is reasonable as a dynamic profile contains a user's most recent activities; hence it obtains a more accurate detection. Furthermore, with a longer training set period, the performance is also improved. Hence, an increased number of days (i.e. 18/22 days) of user activities as the training set should be examined to find the optimum solution. Nonetheless, literature suggests users do change their usage pattern over a long period of. A study by Flurry (2009) states that users only keep 67% of the applications over a 30 days period. Moreover, storage and processing issues should also be taken into consideration with larger training. While a smoothing function treated more log entries as one incident, the performance also improved accordingly. The smoothing function reduces the impact any single event might have and seeks to take a more holistic approach to monitoring for misuse. The disadvantage of this approach is that it takes a longer time for the system to make a decision; hence, an intruder could have more opportunities to abuse a system and a certain amount of abuse could be missed by the security control.

Limitations in the dataset are also likely to have created certain difficulties. As the dataset was collected in 2004, the number of mobile applications available for users to choose was limited; this resulted in a large similarity of application-level application usage between mobile users and difficulty for any classification methods. In contrast, in the early part of 2010, there were around 200,000 mobile applications available (Distimo 2010). As mobile users have more options, their application-level usage would arguably differ larger. Therefore, it would be easier to discriminate mobile users through their application-level usage.

As shown by Table 4, the performance of the telephony application is very good – more than twice that of the application-level profiling. This reinforces the hypothesis that knowing both the application and what the user does with it, improves the chance of identifying individual users significantly. Moreover, mobile users had a far larger set of telephone contacts (the numbers they can dial) compared with the number of applications they had also makes the classification process easier because there are more identifiable data points from which to discriminate. In comparison with other biometric authentication techniques such as keystroke analysis, which has an average EER of 8%, the telephone experiment is within that category of performance (Clarke and Furnell 2006).

As presented in Table 6, the results from the text messaging application were even better than those achieved by the telephone call application, albeit with a smaller dataset. This may be caused by people only sending text messages to very close contacts. Although only 30% of the participants used the text messaging application in 2004, the situation has changed considerably: for UK alone, the volume of text messaging traffic has increased by 290% since 2004 (Ofcom 2010). This indicates that the text messaging based authentication method could serve a good proportion of the mobile users' population.

From the results presented in this paper, it can be shown that both application-level and application-specific information can be used to authenticate mobile users. In addition, although it is more difficult to profile certain users, more than 81% of all users' performance was within the bounds of a behaviour-based biometric. Dynamic-based profiling technique provides the opportunity to develop a more meaningful profile of user activities. This does however raise issues with regards to template aging and ensuring the samples utilised in creating the template are all legitimate that will need to be addressed. Furthermore, in comparison with previous research, which used computationally complicated neural networks as the classification method (Li *et al* 2009; Li *et al* 2010), this approach employed a light weight mathematical formula which saves a significant amount of processing power and storage space; this is essential for handheld mobile devices as they have limited processing power and storage space.

6. Conclusions

The experiment shows that with an EER of 5.4%, 2.2% and 13.5% for the telephony, text messaging and general application usage respectively, and these techniques are viable for a behaviour-based authentication mechanism within the mobile environment. The authentication process could be carried in the background while mobile users utilise their applications; if several abnormal activities occurred within a fixed time frame, further security methods would be initiated according to the level of the incident.

Future work will focus upon designing an authentication architecture that could accommodate the aforementioned behaviour based authentication techniques. As the architecture works behind the scene, little attention would be required from the mobile user and an intervention would only be needed when anomalous application usage occurs. Hence, such an architecture would provide a transparent and continuous protection for users. Furthermore, an operational system, which supports identity verification, will be developed for the purpose of evaluation.

References

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, Issue 9, pp. 1476-1490, Academic Press, Inc. Orlando, FL, USA

Boyd, J.E., and Little, J.J. (2005) “Biometric gait recognition”, Advanced Studies in Biometrics: Summer School on Biometrics, pp19-42, 2005, LCNS

Buchoux A, Clarke NL (2008) Deployment of Keystroke Analysis on a Smartphone, Proceedings of the 6th Australian Information Security & Management Conference, 1-3 December, Perth, Australia

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. 3-12. IEEE Computer Society, Washington, DC, USA

Campisi, P., Maiorana, E., Bosco, M.L., Neri, A. (2009) "User authentication using keystroke dynamics for cellular phones", IET Signal Processing, Vol.3 No.4 pp333-41

Clarke, N.L. and Furnell, S.M. (2005) “Authentication of users on Mobile Telephones – A Survey of Attitudes and Practices”, Computer & Security, 24(7), pp.519-527

Clarke, N.L. and Furnell, S.M. (2006) “Authenticating Mobile Phone Users Using Keystroke Analysis”, International Journal of Information Security, ISSN:1615-5262, pp.1-14

Derawi, M.O., Nickel, C., Bours, P., and Busch, C. (2010) "Unobtrusive User-Authentication on Mobile Phones Using Biometric Gait Recognition," Sixth International Conference on Intelligent Information Hiding and Multimedia Signal Processing, 2010

Distimo, (2010) “Our Presentation From Mobile World Congres 2010 – Mobile Application Stores State Of Play”, [online], http://blog.distimo.com/2010_02_our-presentation-from-mobile-world-congres-2010-mobile-application-stores-state-of-play/, date accessed: 17 January 2011Eagle, N., Pentland, A. and Lazer, D. (2009) “Inferring Social Network Structure using Mobile Phone Data”, Proceedings of the National Academy of Sciences (PNAS), vol 106, pp.15274-15278.

FBI (2010) “Smishing and Vishing”, [online], http://www.fbi.gov/news/stories/2010/november/ cyber_112410/cyber_112410, date of access: 02/12/2010

Flurry (2009) “Mobile Apps: Models, Money and Loyalty”, [online], http://blog.flurry.com/bid/26376/ Mobile-Apps-Models-Money-and-Loyalty, date accessed: 26 January 2011

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

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.

Kurkovsky, S. and Syta, E. (2010) “Digital natives and mobile phones: A survey of practices and attitudes about privacy and security”, In Proceedings of the 2010 IEEE International Symposium on Technology and Society (ISTAS), pp. 441-449

Li, F., Clarke, N.L. and Papadaki, M. (2009) “Intrusion DetectionSystem for Mobile Devices: Investigation on Calling Activity”, Proceedings of the 8th Security Conference, April, Las Vegas, USA

Li, F., Clarke, N.L., Papadaki, M. and Dowland, P.S. (2010) “Behaviour Profiling on Mobile Devices”, International Conference on Emerging Security Technologies, 6-8 September, Canterbury, UK, pp.77-82

Miettinen, M., Halonen, P., and Hatonen, K. (2006) “Host-based intrusion detection for advanced mobile devices”, Proceedings of the 20th International Conference on Advanced Information Networking and Applications (AINA’ 06), pp 72-76

Ofcom, (2010) “Communications Market Report, 2010”, [online], http://stakeholders.ofcom.org.uk/binaries/research/cmr/753567/CMR_2010_FINAL.pdf, date accessed: 20 December 2010

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

Securelist, (2010) “Mobile Malware Evolution: An Overview, Part 3”, [online], http://www.securelist.com/en/analysis?pubid=204792080, date of access: 03/12/2010

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