Behavioural Profiling In Wireless Networks

I. Zincir, S. M. Furnell, A. D. Phippen
Network Research Group, University of Plymouth
Plymouth, Devon PL4 8AA
izincir@plymouth.ac.uk, sfurnell@network-research-group.org,
andrew.phippen@staff.plymouth.ac.uk

***Abstract*-In the last 10 years, mobile devices have become an important part of daily life of everyone. We use them in a wide variety of applications from basic phone telephony through to a variety of m-commerce scenarios. Not only they provide mobile communication at anytime anywhere, they also enable us to browse the net, to use it like a credit card, etc. Since the information is transmitted through radio frequencies instead of cables, they require much more protection than the wired ones. This paper presents a different solution to this problem: behavioural profiling. We believe creating user profiles and then comparing them with the real-time ones will help us to detect malicious activity in wireless networks. The paper proposes a basic architecture to support profiling approach.**

I. Introduction

Wireless networks have gained an increasingly important role in our daily lives. Wireless WANs provide data transmission over wide area coverage, while Wireless PANs provide data transmission over limited area coverage and Wireless LANs provide data transmission inside local area networks [1, 2, 3]. They give us the much needed flexibility and mobility with one major concern, security.

Security methods such as user authentication and authorization, encryption, and defensive programming, can make it a little more difficult to hack the wireless systems, but they still do not provide a complete protection against a really dedicated snoop [4]. Once the sniffer cracks the password it is very easy for him to impersonate the registered user. One solution to this is behavioural profiling of the registered users of the network. To this end, historical user profiles of normal usage are generated and are then compared to the current usage to monitor the differences [5]. A historical user profile is built over a time period and may consist of applications being run, usage times, types and combination of tasks, process durations, types of files used and etc. A user who changes his behaviour such as using different application programmes or calling different files can be a malicious user/behaviour that results in alerting the system [6].

In this paper, the aim is to define how a mobile user's behavioural profile can be used in order to detect malicious users. We believe that this will assist us to design and implement an Intrusion Detection System for a safer environment in wireless networks.

II. Security requirements in wireless environments

Wireless technology is changing the IT world enormously, creating new opportunities for everyone but increasing the security risks. Since they use radio frequencies to transmit data from one node to another, the hacker does not have to gain physical access to the network wires and to pass through firewalls and gateways. The attacks can come from any direction and any node. Hence, they introduce a number of critical security challenges such as [7]:

i. Insufficient policies, training and awareness
ii. Access constraints
iii. Rogue access points
iv. Traffic analysis and eavesdropping
v. Insufficient network performance
vi. Hacker attacks
vii. Spoofing/session hijacking
viii. Physical security deficiencies

Installing antivirus programmes into the PCs does not provide protection against multiple types of attacks. In a survey made by the NTHCU (National High Tech Crime Unit), in 2003, 83% of medium and large enterprises were the victims of cyberspace crimes such as denial of service attacks, virus, fraud, and information theft [8]. According to Symantec, malicious code exposing confidential data increased significantly in 2003. Still, there are only a few downloadable third-party applications for handheld mobile devices and hence, malicious code threats that can be directed at the devices are minimal. However, this will not continue forever. Devices which will be on the market at the fourth quarter of 2004, such as Nokia 9500 Communicator, will support Wireless LAN access (IEEE 802.11b) as well as working with the GSM. Capabilities such as instant messaging and push-to-talk will be used as much as SMS [9]. In addition, there will be issues related to 3G (Third Generation) systems. The main difference between GSM and 3G services is 3G supports a faster data transmission providing new windows for mobile communications. The major concern for 3G is the complexity of its architecture.

According to Cerebrus Solutions, this will give many opportunities to hackers to commit frauds since an average 3G subscriber will generate 10 times more transactions than a 2G subscriber [10]. Hence, the potential number of threats for the mobile networking is expected to increase rapidly in the following years.

As the threats are envisaged to come from multiple angles with a variety of different platforms, traditional security methods such as user authentication and authorization, encryption, and defensive programming, will not provide sufficient protection against security challenges that is governed in mobile networks [8]. Once the hacker will gain access to the environment it will be very easy for him to impersonate the registered user. Thus, more powerful solutions will be needed. We believe that using behavioural profiling such as an Intrusion Detection System (IDS) to detect the malicious user/behaviour will help us to improve the security regarding to wireless networks.

III. Intrusion detection using behavioural profile

A. User Authentication

In a network system the first step of the security begins with the confirmation of a person who has the ability to access sensitive, confidential or classified information [11]. There are 3 types of user authentication: something the user knows (e.g. password), something the user has (e.g. smart card) and something the user is (e.g. biometrics). The problems with the passwords are most of the time they can easily be cracked by a dedicated hacker [18]. The smart cards improve security but with the right tools they can be imitated [17]. Biometrics, though, are mostly costly but better solutions since they add extra authentication procedures such as keystroke analysis, face recognition, voice verification, iris scanning that will not be easy to be altered with.

Many organizations are already using these procedures together in order to create a safer environment for their networks. In our Network Research Group, research has already been done on authenticating users in wireless networks by using biometrics [12,13,14,15]. Therefore, our project will not require this part, but will take it further in improving the security.

B. User Profiling In Behaviour Based IDS

An IDS is the first line of defence of a computer network which detects unauthorized access attempts. A good IDS must provide successful visibility and control of the network. The visibility of the network depends on the ability to understand the nature and the procedures of the network while the control of the network depends on the ability to affect the traffic inside the network [4].

The main aim of IDS is to identify the intruder who has attempted to gain or has gained unauthorized access to the network. This intruder can be either external or internal. An external intruder is a person who does not have any authority to gain access to the network. An internal intruder is a person who has authority but tries to gain extra ability illegally. The IDS provides a view into the traffic inside the network to the security administrator. There are two types of IDS: Network-Based IDS and Host-Based IDS. Network-Based IDS analyze the data packets continuously to identify unauthorized users, threats and attacks towards the network, working like a real time monitoring system. It captures, stores, and reports the signatures without altering them by using TCP or UDP protocols. On the other hand, Host-Based IDS analyze the key system logs, firewall logs, router logs, application logs and performance logs to catch the suspicious access to the network in real time. Although Network-Based IDS gives the administrator a rich view of the traffic there is always a new way of attack to the system. Thus involving Host-Based IDS is a must. A successful Host-Based IDS must react not only after attacks but should also anticipate potential threats [5].

There are two types of intrusion detection techniques: anomaly detection and misuse detection. While both detection systems sustain important roles individually in IDS, in some cases, they can also be combined together as a hybrid solution [6].

In anomaly detection, the intrusions are detected by looking for activity that is different from a user's or system's normal behaviour. The system creates a normal activity profile and then compares this profile with the ones that are connected to the network in real time. There are two types of anomaly detection: static and dynamic. A static anomaly detection system is designed to think that a portion of the system being monitored remains constant. A dynamic anomaly detection is designed to think that there is a system behaviour defined as a sequence. The major problem for this system is it may misjudge the normal activities as intrusive, and the intrusive activities as normal. Thus, the profiling must be done with great accuracy and detection criteria have to be made carefully [5,6].

In misuse detection, the monitoring system looks for an activity that corresponds to known intrusion signatures or system vulnerabilities. Misuse detector monitors for explicit patterns. Since the attacks are described by using these historical signatures, this system is not prepared against an unknown attack. The major problem for this method is how to differ the intrusive signatures from the right ones and how to include all variations of attacks into a signature [4,5,6].

Behaviour-based intrusion detection techniques detect an intrusion by observing a deviation from the expected behaviour of the user. The model of a valid behaviour is

extracted from the collected information. User profiling means developing a profile for a user of a network. The profile is built by using history of events and actions. The detection system first monitors and records the user's behaviour. Then by examining these files it creates a specific profile for that specific user. Whenever the user connects to the network the system then compares in order to check whether the user is who he claims to be. The intrusion detection system later compares this profile with the current one. When a deviation is observed, an alarm is generated. In other words, anything that does not match to the expected behaviour is considered potentially intrusive. Therefore, the intrusion detection system may be much powerful, but its accuracy will be a question mark since there will be a lot of false alarms.

The advantages of behaviour based IDS are that they can detect attacks to new vulnerabilities and they are not dependent on operating systems and they can also detect misuse. The problem with this system is anything that has not been met previously is accepted as intrusive. Hence, it gives a lot of false alarms which in turn causes a drawback of behaviour based IDS. A profile is not that easy to create. The entire characteristics of a user cannot be learned during a limited period of time. Also, behaviour can easily change by time, and the user can gain new habits. This creates another challenge since the system has to update itself from time to time to learn the new user profile, and between these periods more false alarms and vulnerabilities occur since an attack during the learning procedure may create more headaches.

There are two types of error as a result of the comparison of the profiles: false positives and false negatives. False positive means a registered user is identified as malicious user after the process of matching the profiles. False negative means a malicious user is identified as a registered one after the process of matching the profiles. To have a successful IDS both of the rates have to be lower. Especially the false negative has to be 0 since no access is wanted for a malicious user. To solve these problems, the IDS must be designed to have the ability to change itself periodically regarding to environment since the behaviour profile of a user may change over time. Otherwise, the system will lose its credibility and instead of protecting the network, it will damage the system. Thus, the IDS has to continue to obtain real time data to update the user profiles. A major concern in this approach is how the mechanism will work when a change in a profile happens. When will it reject and when will it accept it? It cannot continuously update itself with every new activity of the user. How much will be the learning period? When it is too long, the network will be vulnerable to attacks and will not record every action but instead will record the most common ones. When it is too short, then it will miss some long-term differences. Another problem is how the system will defy against a potential attacker who will gradually train the system by time to accept malicious behaviour as normal. If he continuously connects to the network during a period of time and creates only small differences then the normal behaviour in order to adapt it to himself, how will the system react to this?

In short, there are many important issues in designing behaviour based IDS:

- How can we define the main parameters of the behavioural characteristics of a registered user?
- How can we define the main parameters of the potential behavioural characteristics of a malicious user?
- Which machine learning techniques do we use to monitor the usage of a network to decide whether or not the user is a registered or malicious user?
- How do we profile sample users by using the information obtained through the monitoring system to describe the different user classes?
- What will be the necessary period needed to update the profiles?
- What will be the mechanism to update the changing profiles?

C. How To Employ An IDS In Mobile Networks

The mobile telecommunication companies carefully watch the quickly changing trends of the consumers and adapt themselves to them accordingly. To achieve these objectives, cellular service providers keep records of their customers' behaviours. In 2001 Ericsson conducted research similar to this trying to detect fraud use of the network by creating user behavioural profiles. The system uses pattern recognition software built into intelligent agents-called sentinels-that assign behavioural profiles of subscribers on a network. If the software detects unusual activity on an account, it will send a text message to the mobile phone, the user will then have to punch in a PIN to identify themselves, if they fail to do so, the phone will be cut off [16].

In our project, we will first design the specifications for creating behavioural profiles that will tell us what information is going to be collected. Then, the network provider will install a program into the mobile phones that will log the user's activities. The program will record the data regarding to the specifications. These will be the activities such as: how the user reacts with his phone, what does he do first in the morning, whether he uses his phone like a PDA, if he does so on what occasions, how does he use its radio, camera or MP3 player, does he watch movies installed on the memory card (if it contains these specifications), and so on. The service provider will also record activities such as: who does he calls first, which web sites he browses, which numbers he calls, what is the general time he spends on calls,

how often does he use SMS and MMS and to whom does he send, whether he uses his phone like a PDA, if he does so on what occasions, when and how, how much does he spend for his calls, SMS, browsing the net, watching videos, sending MMS, using his voice mail, does he download anything from anywhere, transactions regarding to m-commerce and m-banking, and etc., inside its system. In addition, increasingly common smart phone devices will add extra challenges. When the phone uses its Wi-Fi abilities to connect to a computer network, the installed programme is going to record again some transactions such as which network it is connected, does it have an internet access, the IP address of the servers, what is the reason for the connection; downloading or uploading files, pictures or documents, how long does the connection to the network take place. If Bluetooth technology is used, the programme will react to the case as in the same manner. Then, all of this data will be sent to the mobile service provider through the network if the device is on the coverage area of the provider or by using Internet access from the network connection if there is any. In the end, the service provider will combine the information that is collected both from the device and network. After this, the provider will create a user profile for that specific user. This user profile will be updated regularly in order to adapt itself to the changing behaviour of the user. Fig. 1 gives a brief explanation of how this will work.

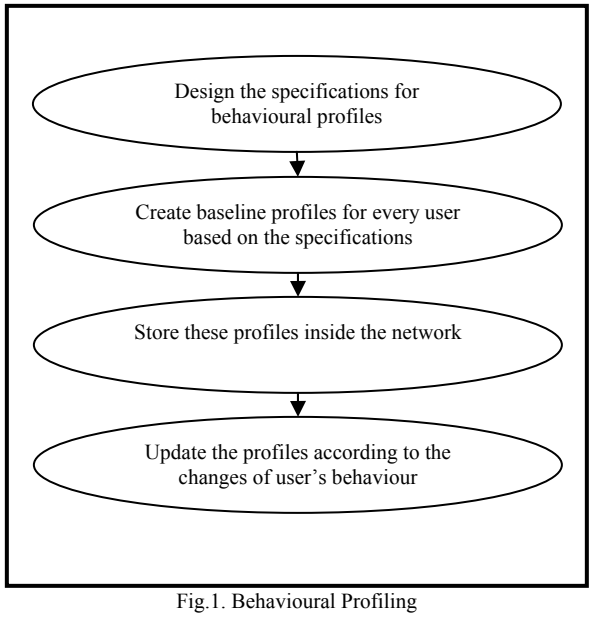

Fig.1. Behavioural Profiling

The IDS that is going to be designed, will store the collected information inside the service provider's network and will monitor continuously, hence decisions will be made much more quickly and accurately. The IDS will learn to predict the next action of the user by comparing the historical profile (that consists of applications being run, usage times, types and combination of tasks, process durations, types of files used and etc. for a given time period) of the same specific user. The system will constantly observe the new trend and will update the user behaviour over time. The main problems will be how to react to a rapidly changing behaviour and how to decide the 'normal' behaviour. To build a stable system one has to decide which data to collect and how to use it. The IDS will carry out the following steps in order to identify the malicious activities:

i. When the mobile device is connected to the network the system will begin to collect real-time information inside the network
ii. This real-time profile will then be compared to the historical profile
iii. If the two profiles will match then the user will be accepted as legitimate and the system will continue to monitor at specific time intervals
iv. If the two profiles do not match then the user will be regarded as suspicious and the IDS will ask the device to send the data that it is collected
v. Then this data will be compared with the baseline profile
vi. If the two profiles will match then the user will be accepted as a legitimate and the system will continue to monitor at specific time intervals
vii. If the two profiles will not match then the user will be accepted as malicious and it will alert the system to make the appropriate response

In our project, the profiles are compared using the artificial intelligence methods to catch the malicious activity inside the network. Then, once the user is identified as suspicious, the system can begin to watch the activities closer and then by again making comparisons, it can alert the system in case of need. It can then respond according to the decision of the service provider. However, it should be noted here that there is a trade-off between false negatives and false positives. When one goes down, the other usually goes up!

Fig. 2 shows the structure of the Intrusion Detection System based on behavioural profiling.

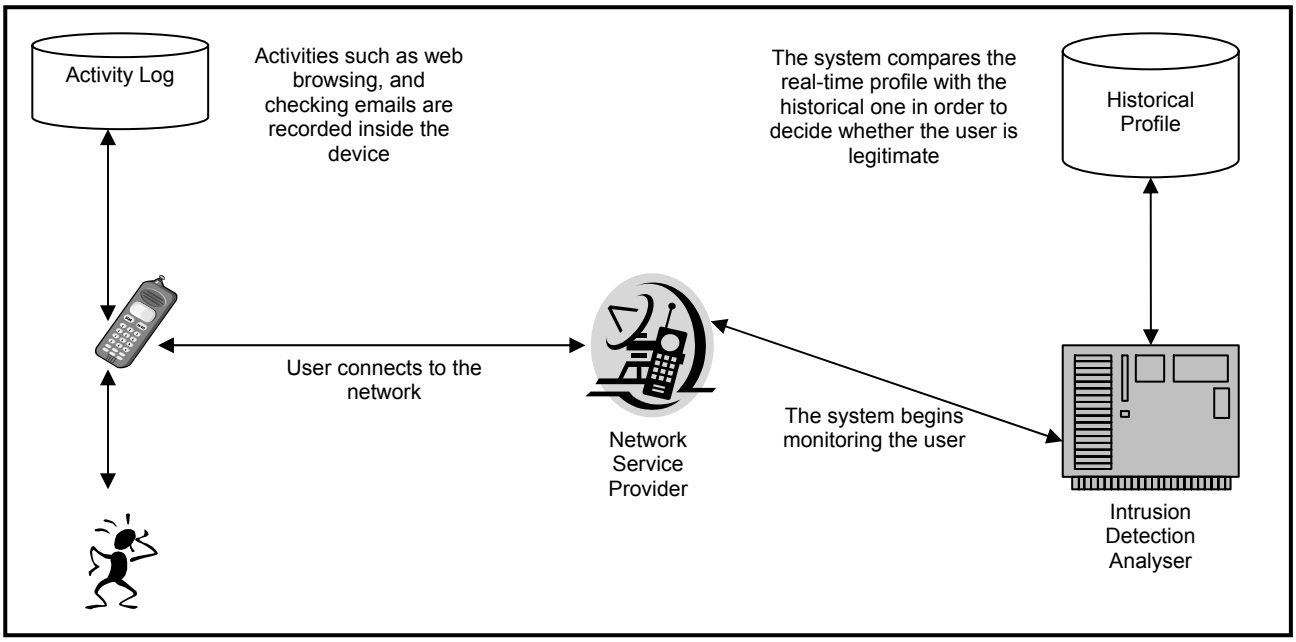

Fig. 2. A Behavioural Profiling Based Intrusion Detection System

IV. Conclusion

Behaviour based IDS for wireless networks help the clients to live in a much more secure environment. They use a reference rule of normal behaviour and make decisions from this model as intrusive or legitimate. Any activity that does not match the historical profile is considered as dangerous. The advantage of this model is it provides better protection against new attacks that are not known or met. Since a lot of activities can be recorded in order to create a much healthier behavioural profile it is not very easy for any hacker to guess which ones are important. By updating the profiles regularly in large time intervals such as 3 months, it would not be easy for a malicious user to train the system by time.

The aim of the project, as explained, is the design of a stable, durable and trustable Intrusion Detection System that has the ability to adapt itself into new challenges and attacks supporting minimum false positive alerts. The IDS will use artificial intelligence methods through the matching process of the profiles. The authors are currently trying to identify the specifications of the behavioural profiles in order to decide which ones we will choose as the most distinctive ones. After this step, we will create the novel architecture that will then be followed by the design of the prototype.

Dynamic profiling will be used and the host and the network systems will act together in order to catch intrusive behaviours.

References

[1] G. Held, *Deploying Wireless LANs*, McGraw-Hill, USA, 2002.

[2] R. D. Vines, *Wireless Security Essentials*, Wiley, USA, 2002.

[3] K. Chaplin, "Wireless LANs vs. Wireless WANs", *Sierra Wireless White Paper*, USA, November 2002.

[4] J. McHugh, A. Christie, J. Allen, "Defending Yourself: The Role Of Intrusion Detection Systems", *IEEE Software*, USA, September/October 2000, pp. 42-51.

[5] A. Brox, "Signature Based or Anomaly Based Intrusion Detection: The Practice and Pitfalls", *http://www.itsecurity.com/papers/proseq1.htm*, February 2002.

[6] O. Babaoglu, "IDS: Intrusion Detection Systems", *http://www.cs.unibo.it/babaoglu/courses/security/lucidi/IDS.pdf*, January 2003.

[7] S. Kennedy, "Best Practices For Wireless Network Security", *http://www.computerworld.com/printthis/2003/0,4814,86951,00.html*, November 24, 2003.

[8] "Keeping Out The Bad Guys", *IEE Information Professional*, UK, April/May 2004, pp. 28-29.

[9] "Symantec Internet Security Threat Report 2003", *http://www.symantec.com*, January 2004.

[10] "Fraud Visions From Cerebrus Solutions", *http://www.cerebrussolutions.com/newsletter-pdf/FraudVision_Autumn-2002.pdf*, Autumn 2002.

[11] M. Zimmerman, "Biometrics And User Authentication", *www.sans.org/rr/papers/6/122.pdf*, SANS Institute, 2002.

[12] N. Clarke, J. Lecomte, & S. Furnell, "Artificial Imposter Profiling For Keystroke Analysis On A Mobile Handset", *Advances in Network & Communication Engineering*, pp. 55-62, 2004.

[13] N. Clarke, S. Furnell, P. Reynolds & B. Lines, "Application Of Keystroke Analysis To Mobile Text Messaging", *Proceedings of the 3rd Security Conference, Las Vegas, USA*, 2004.

[14] N. Clarke, S. Furnell, & P. Reynolds, "Biometric Authentication For Mobile Devices", *Proceedings of the 3rd Australian Information Warfare and Security Conference, Perth, Western Australia, 28-29 November 2002*, pp. 61-69, 2002.

[15] N. Clarke, S. Furnell, P. Reynolds & B. Lines, "Keystroke Dynamics On A Mobile Handset: A Feasibility Study", *Information Management and Computer Security*, vol. 11, no. 4, pp 161-166, August 27, 2003.

[16] G. Rowe, "Something In The Way She Phones", *http://www.newscientist.com/hottopics/ai/somethingintheway.jsp*, New Scientist, February 2001.

[17] Semiconductor Insights Inc. “Tamper Resistance – A Second Opinion”, http://www.smartcard.co.uk/resources/articles/tamper-res.html, Accessed, April 2004.

[18] Rosencrance, "Survey: Insecure passwords can be costly for companies," *ComputerWorld.* August 8, 2003.