INTRUSION DETECTION VIA BEHAVIOURAL PROFILING ON MOBILE AND WIRELESS NETWORKED DEVICES

Ibrahim Zincir, Steven Furnell and Andrew Phippen
University Of Plymouth
Portland Square A304
Plymouth, PL4 8AA, UK
E-mail: izincir@plymouth.ac.uk, sfurnell@plymouth.ac.uk,
andy@jack.see.plymouth.ac.uk

KEYWORDS
Wireless, Behaviour, Profile, Security, IDS.

ABSTRACT

Wireless networks have gained an increasingly important role in our daily lives. They give us the much needed flexibility and mobility with one major concern, security. 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. As the threats are coming from multiple angles with a variety of different platforms, traditional security methods do not provide sufficient protection. Hence, more powerful solutions are needed. It is considered that using Behavioural-Based Intrusion Detection System (IDS) will assist the identification of malicious user activity, and help to improve the resulting security of wireless networks.

INTRODUCTION

The world has changed a lot since Marconi made a long trip from Italy to England to present his magic box to the British Telegraph authorities he developed to be used as a wireless telegraph system. One hundred years later, digital satellites broadcasting HD TV channels, mobile phones are connecting us to each other for any type of purpose a man could not even imagine a century ago, laptops surfing the Internet via hot spots, and PDAs checking emails at the airports are common scenes that we are all used to seeing. Today wireless is the shining star. The idea of connecting everything, anywhere at anytime pushes enterprises to pour more money than ever into wireless technologies. There are 1.5 billion cell phones in the world today, 3 times more than the number of computers and these mobile phones provides the equal amount of processor power to the desktops of 1990's (Newsweek 2004). Wireless technology is everywhere.

The major problem with them is as the information between the information is transmitted between the nodes through radio frequencies instead of cables, and the threats are envisaged to come from multiple angles with a variety of different platforms, traditional security methods will not provide sufficient protection against security challenges that is governed in wireless networks. We believe that using behavioural profiling as an Intrusion Detection System (IDS) to detect the malicious user/behaviour will help us to improve the security of wireless networks. In this system, historical user profiles are created and then compared with real-time activity in order to detect malicious behaviour.

BEHAVIOUR PROFILING

A behaviour profile is a collection of information that can be used to describe basic characteristics of an individual defined under the rules created by the system administrator. These specifications are designed depending on for when, where and how the profile will be used. In a way a profile can be seen as a business card as it contains some basic definitions such as name, location, and phone number of the user. In order to create stable profiles one must not include every bit of information but must use sensible specifications to enable a common way of defining the behaviour.

One of the biggest problems of modern IDSs is that they try to catch the malicious activity by analysing the user signatures and/or detecting the misuse. In misuse detection, the monitoring system looks for an activity that corresponds to known intrusion signatures or system vulnerabilities; it monitors for explicit patterns and diagnoses the specific attacks from the signatures. 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. Moreover, this type of a technique explicitly works on known attack patterns. This results in the IDS remaining vulnerable to unknown attack patterns (McHugh et al. 2000, Brox 2002, Babaoglu 2003). In order to detect novel and unknown attacks a Behaviour Based IDS implements not only misuse tools but also an anomaly detection approach. Anomaly means something that is not nominal or normal. In anomaly detection, the intrusions are detected by looking for an 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. As a result, it has the ability to detect symptoms of new kinds of threats. 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 (McHugh et al. 2000, Brox 2002,Babaoglu 2003). In addition, during the process, the system has to work as fast as possible since the malicious activity has to be detected as quickly as possible once it occurs.

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 numerous (Lawrence Livermore National Laboratory 1996); they can detect attacks to new vulnerabilities and they are not dependent upon operating systems and they can also detect misuse. However, there are also several challenges to overcome before implementing such a system. Wireless intrusion detection is a very new technology and hence before applying it to any network one must be very careful since there may be bugs and vulnerabilities that can create the biggest threats. Finally, an IDS is only as effective as the individuals who analyze and respond to the data collected by the system. A Behaviour-Based IDS, like a standard IDS, can require vast human resources to analyze and respond to threat detection. There are four main rules to be able to deal with these risks: know & plan, protect communications, protect wireless devices, protect airwaves and monitor 24/7.

The biggest problem with this system is anything that has not been met previously is accepted as intrusive. As a result, it causes a lot of false alarms which in turn results a drawback (Newman et al. 2002, Timm 2001). In addition, creating a profile for a user is not that easy. The whole specifications of a person cannot be learned in a 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 these rates have to be lower. Specifically the false negative has to be zero since a malicious user cannot be given access to the network. To solve these problems, the IDS must be designed to have the ability to update 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 long should the learning period be? Another problem is how the system will protect itself from a malicious user who will try to train the system by time to impersonate a registered user. How can the system react to this?

Response to the malicious activities is another important issue in Intrusion Detection Systems. Usually, system administrators prefer passive response systems as they want to see the alert and take the appropriate action by themselves, in order to prevent adverse effects upon legitimate users in the event of false alarms (Papadaki 2004). Once the administrator is convinced that there may be a malicious user inside the network, he then may ask the system to send a text or email to that user asking his specific password and/or PIN number especially created for situations like this. One last challenge for behaviour profiling is the privacy issue. As a lot personal information may be collected about the registered user, the system will be totally automated and all the log entries will be encrypted and no one will have the access to read these log entries.

In short, there are many important challenges in designing a Behaviour-Based IDS; but we believe by creating a successful profiling mechanism we will be able deal with all of these problems.

CREATING BEHAVIOUR PROFILES

There is no opposition against the idea that wireless networks are not totally secured against targeted attacks. As the sensitive information theft becomes the most growing concern for the enterprises it is inevitable that there may not be any attacks. As a result, it is important to develop effective security solutions and policies. Since the medium cannot be controlled properly, wireless networks bring big risks as much as big advantages. However, with the solutions and the policies they can still be secured. Using a successful IDS that monitors and analyze the traffic inside the network by 24/7 will help the solution to the problem. To this end, our project will create historic profiles of the clients and then compare them with the real-time ones in order to detect malicious activity. As explained above, choosing which characteristics of a registered user to audit in order to create historical profiles is a major challenge. In our project, our IDS will collect data both on the mobile device and on the network. The service provider will install a program which will log the information regarding how the device is used while it is not using the wireless network, as well as it will continuously monitor the user whenever he or she is connected to the network.

Our Behaviour Based IDS will be implemented on a mobile device (e.g. a smart phone) that will have the ability to operate under other wireless networks (WiFi, WiMax, and/or Bluetooth) as well as the network service provided by the operator (GSM, GPRS and/or 3G/4G). Mobile devices have gained an increasingly important role in our daily lives as 675 million phone sales is expected by 2006 while 30 million Personal Digital Assistants (PDAs)(Reed 2002). We use them for many different purposes as they provide flexibility and mobility. Since few individuals like to share their mobile phone with others they are very personal, and as they are regularly connected to the network they are easily traceable. As a result, the way they are used is very unique depending on the owner and there are many different characteristics that can be used to define a profile for the user.

Today, mobile telecommunication companies keep records of their customers' behaviours for many different purposes. In 2001 Ericsson conducted research similar to our project, 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 (Rowe 2001).

According to The Register, a website for latest technological inventions, American researches Nathan Eagle and Sandy Pentland from Massachusetts Institute of Technology are developing applications for mobile phones which can learn user's daily habits so that they can become mobile digital secretaries. The smart phone learns about owner's behaviour by logging calls and recording when the digital camera implemented on the phone is used. In addition, it takes note of Bluetooth pairing bonds in order to understand who the user socialise with. The software has been installed on 100 Nokia 6600 and the collected information is downloaded onto a server in MIT. The results will be used to investigate how social networks build as well as technologies (Leyden 2004). Another research is made again by Nathan Eagle and Sandy Pentland in order to explore a mobile device user's situation by recording his conversations with the individuals around him and the commands he gives to his mobile device while he is waiting in the queue in a restaurant. The device then analyse these conversations and commands in order to offer different solutions to the user (Eagle and Pentland 2003). According to Schilke et al, the biggest problem with the personalisation is there is too much information for users to be deal with, and they cannot access it at the right time and at the right place as well as at the right format. The main dimensions are time, location and interest. The time dimension is the user's repeating behaviour, the location dimension is where the user is, and the interest dimension is understanding what the user is doing and why (Schilke et al. 2004).

Other research conducted in order to understand whether the different cultures really have different ways of using mobile devices shows that approximately 35% of the users are using wireless networks only to download files and to send emails (Lee et al. 2002).

According to Donner (2004), it would not be wrong to describe the call register (the log of the incoming and outgoing calls) is a distinct characteristic of a mobile phone user. Donner's research showed that nearly 66% of the outgoing calls were made to family members and friends and 65% of incoming calls were made by the family members and friends were answered.

Another application that tries to predict user's behaviour is created by Zeynep Inanoglu and Ron Caneel of the Media Lab at the Massachusetts Institute Of Technology. It is a voicemail system called Emotive Alert that labels messages according to the caller's tone of voice in order to identify which messages are the most urgent (Biever 2005).

These findings suggest that there are many different characteristics of wireless device owner's that can be used to define as their profiles. In addition to which applications are used at when and where also how the device is used to interact with other devices and networks are going to be taken into consideration in our project. Table 1 describes the some of the basic characteristics that can be used in the behavioural profiling.

Table 1: Basic Characteristics Of Mobile Devices' Users

Outgoing Calls
Incoming Calls
Video Calls
Location
Time
SMS
MMS
Favourite Websites
Email Addresses
IP Address Of Access Points
Bluetooth ID
Digital Camera Usage
Key Stroke
Voice Commands
Opened Applications
Media Player
Downloaded Files

IMPLEMENTING A BEHAVIOUR-BASED IDS

In order to design a novel structure of a Behaviour-Based Intrusion Detection System, the first step is to choose what to log on both at the mobile device and the network. Since the IDS will be designed for a mobile device which can be active in all the known wireless networks and bandwidths, there are too many different kinds of information regarding to the user to be logged. After analysing the other behavioural profiling research summarized above, the most accepted distinctive characteristics of the users are chosen to be collected.

To prevent too much memory consumption and processor speed, the system will record only very basic processes inside the mobile device. The program installed by the network service provider will log the Bluetooth ID of the connection point when the device is connected to other networks through Bluetooth and it will log the IP address of the access point if it is connected to other networks through any IEEE 802.1X technologies. It will also record the addresses that emails are sent and the websites that are visited during the connection to these networks. When the device is connected to its registered network, all the outgoing and incoming calls, the numbers that the SMS and MMS messages are sent, all the addresses of the emails that are sent and finally all the websites that are visited will be logged by the network. Of course, all these log entries will include the time and the location dimensions. In the end, this collected data will then be combined and used to create behaviour profiles for the registered users. Table 2 shows a basic explanation of this.

Table 2: Data To Be Collected

Mobile Device		**Network**
Bluetooth	IEEE 802.1X	GSM/GPRS/3G/4G
Bluetooth ID	*IP Address*	*SMS, MMS Messages*
Email Addresses	*Email Addresses*	*Email Addresses*
Websites visited	*Websites visited*	*Websites visited*
		Call Register

In our project, we will first implement the program into a mobile device which will be used to collect information about different people who will use the device. Then the program will record the data regarding to the specifications described in the table above. We will then download this data into our server in order to analyse this information. During this analysing process we will try to understand and create characteristics for each user such as: who does he calls first, which web sites he browses most, which numbers he calls most and at what time, 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, when and how, to whom he sends SMS and/MMS messages, does he make any video calls and if so to whom, does he use internet from the service operators or does he use his own wireless connections such as Bluetooth, or WiFi to browse the net, and if he does surf the Internet which web sites does he prefer to visit most. When the device uses its WiFi abilities to connect to a computer network, what is the IP address of the servers, how long does the connection to the network take place? If Bluetooth technology is used, what is the Bluetooth ID? In the end, we will create a user profile for each of the specific user of the system. This user profile will be updated regularly in order to adapt itself to the changing behaviour of the user.

The IDS that is going to be designed, as explained, will store the collected information inside the service provider's network and will monitor the traffic continuously. There will not be any analyse on the user side and hence the 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) with the real-time one of the same specific user. The system will constantly observe the new trend and will update the user behaviour over time. This update will be made regularly by a time basis of 3 months. The main problems will be how to react to a rapidly changing behaviour and how to decide the 'normal' behaviour. In order to have a standard the system will carry out the following steps in order to identify the malicious activities:

1) When the mobile device is activated inside the network the system will begin to collect real-time data in order to create a real-time profile
2) This real-time profile will then be compared to the historical profile in order to catch malicious activity
3) If the two profiles (historical & real-time) will match then the user will be accepted as legitimate and the system will continue to monitor the user in specific time intervals
4) If the two profiles (historical & real-time) do not match then the user will be regarded as suspicious and the system will ask the device to send the data that it is collected
5) Then this data will be compared with the baseline profile created as a safeguard
6) If the two profiles (baseline & real-time) will match then the user will be accepted as a legitimate and the system will continue to monitor the at specific time intervals
7) If the two profiles (baseline & real-time) do not match then the user will be regarded as malicious and it will alert the system administrator to make the appropriate response

Figure 1 gives a brief explanation of how this will work:

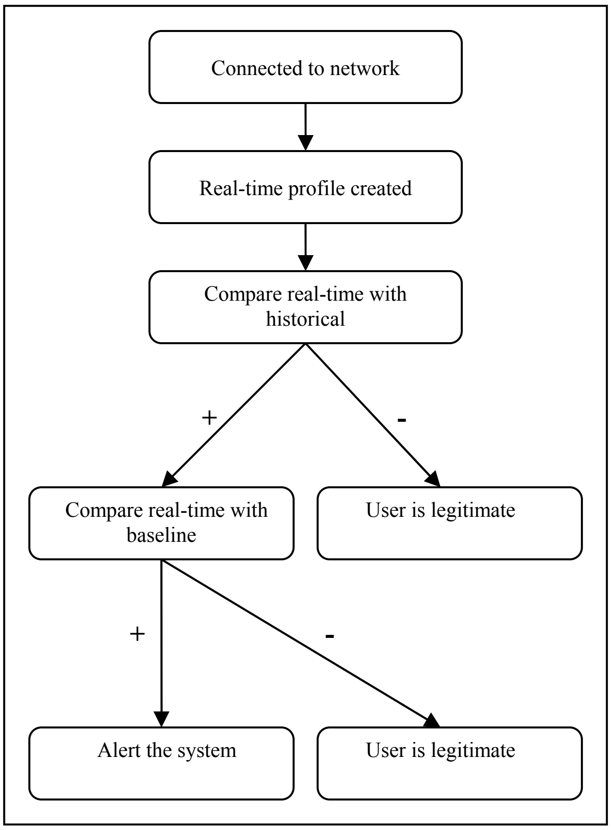
Connected to network
Real-time profile created
Compare real-time with historical
+
-
Compare real-time with baseline
User is legitimate
+
-
Alert the system
User is legitimate

Figure 1: Architecture Of Behaviour-Based IDS

In our project, the profiles will be compared by 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. The IDS will use dynamic profiling and the host and the network systems will act together in order to catch intrusive behaviours.

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

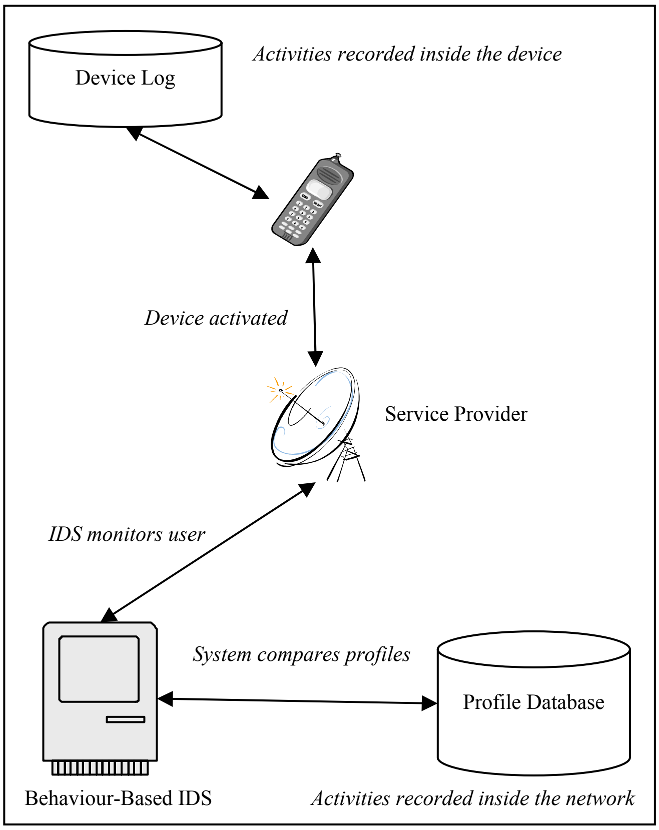

Figure 2: Behaviour-Based IDS

CONCLUSION

In our project, the profiles will be compared using a neural network technique 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. The advantage of behaviour based IDS is it provides better protection against new attacks that are not known or met. Since many 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. Also, by updating the profiles regularly in large time intervals such as three 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 authors are currently trying to implement a program into the mobile devices in order to collect data to be able to create profiles. After this step, we will create the novel architecture that will then be followed by the design of the prototype.

REFERENCES

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

Biever C., 2005, "Voicemail Software Recognises Callers' Emotions", *New Scientist*, 8 January 2005. http://www.newscientist.com/article.ns?id=mg18524813.100

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

Donner J., 2004, "The Mobile Behaviours", *The Global and The Local In Mobile Communication Conference*, Hungary, June 2004, http://www.columbia.edu/~jd2210/whowhy.pdf

Eagle N. and Pentland S., 2003, "Handhelds That Listen And Learn", *IEEE Computer Magazine, Special Issue on Handheld Computing.* September 2003.

Lawrence Livermore National Laboratory, 1996, "Intrusion Detection And Response", *National Info-Sec Technical Baseline*, http://all.net/journal/ntb/ids.html

Lee Y., Lee I., Kim J. and Kim H., 2002, "A Cross-Cultural Study On The Value Structure Of Mobile Internet Usage", *Journal Of Electronic Commerce Research*, vol. 3, no. 4.

Leyden J., 2004, "Smart Phone Predicts Owner's Behaviour", *The Register*, 25 November 2004, http://www.theregister.co.uk/2004/11/25/super_smart_phone

McHugh J., Christie A. and Allen J., 2000, "Defending Yourself: The Role Of Intrusion Detection Systems", *IEEE Software,* September 2000, pp. 42-51.

Newman D., Snyder J. and Thayer R., 2002, "Crying Wolf: False Alarms Hide Attacks", *Network World*, 24 June 2002, http://www.nwfusion.com/cgi-bin/mailto/x.cgi

Newsweek, 2004, "Wireless Is Everywhere", *Newsweek Magazine*, 7 June 2004, pp. 68.

Papadaki, M. 2004. *Classifying and Responding to Network Intrusions*, PhD thesis, University of Plymouth, Plymouth, UK.

Reed Electronic Research, 2002, "The Mobile Industry- A Strategic Overview", October 2002, http://www.rer.co.uk

Rowe G., 2001, "Something In The Way She Phones", *New Scientist,* February 2001.

Schilke S. W., Bleimann U., Furnell S.M. and Phippen A., 2004, "Multi-Dimensional Personalisation For The Online And Offline World", *Internet Research*, vol. 14, no. 5, pp. 379-385.

Timm K., 2001, "Strategies To Reduce False Positives And False Negatives In NIDS", 11 September 2001, http://www.securityfocus.com/printable/infocus/1463