Intrusion Detection System for mobile devices

D.S.Michalopoulos and N.L.Clarke

Network Research Group, University of Plymouth, Plymouth, United Kingdom
e-mail: info@network-research-group.org

Abstract

Mobile devices are getting very popular these days. Most of people use mobile phones and now, as the new generation of smartphones, the capabilities that are included in a portable palmtop device are amazing. However, single user authentication is not enough as their compact size makes them easy to be stolen. The variety of frauds on these devices has lead to the development of an intrusion detection system, that acts as a constant and transparent authentication mechanism.In this paper an algorithm for host based intrusion detection in mobile devices has is developed. Normal Intrusion Detection Systems use signature checking algorithms, something that can not be implemented easily on a mobile device. This system is based on statistical models that try to identify anomalies in users' attitude by utilizing a profiling procedure and then requires a second layer of authentication from the user, where at the same time network administrator is warned about possible abuse.

Keywords

Mobile, Security, Fraud, IDS, Wireless

1. Introduction

The main aim of this project is to develop an intrusion detection system (IDS) for mobile devices. Single authentication mechanisms are not enough and many frauds take place (Clarke&Furnell, 2005). As a result our thought is the development of a continuous and transparent authentication system capable of identifying any possible abnormal attitude. Before we analyze the designing plans of our system, some basic principles of the intrusion detection have to be understood. First of all the idea of intrusion detection is taken from desktop and laptop computers as they are developed before the mobile devices and there are many problems in terms of information security. The evolution of the mobile devices was very fast and started during the previous decade. The first of them were capable to perform phone calls through the GSM network, store names and numbers, provide calendar services like date reminding etc, storing notes etc (Mobitedia, 2006).

The last generations of these devices are far more developed. The definition of palmtop computers is precise enough. Having a processor, memory, operating system and many other computer infrastructure they can support many type of applications and of course at the same time to be normal cell phones. As an example for their evolution we can give Microsoft's windows mobile operating system, specially designed for mobile devices.

What is in our minds is to create a system, capable to identify frauds and misuses at the mobile device (Lundin&Jonsson, 2000). In order to achieve that, we install multiple sensors on the device that monitor user's attitude and keep records of it. Then, as the device is in operation, the captured traffic is compared with what was kept and a threshold. In case there is enough aberration the IDS is activated, warning the user and the network about the potential danger.

In section 2 literature review is analyzed providing information about the sources and the references of this project. In addition the research method that has been followed is analyzed giving details on the aspects on where the author was focused on. In section 3 the main framework of the IDS is presented analytically providing all the necessary details. In section 4 some advantages and disadvantages of the framework are discussed

2. Literature review

Our aim is to develop a system that is capable to protect all kind of mobile devices. However, not all of them have the same capabilities. What is more, data connections for these devices are many, for example Bluetooth, GPRS, UMTS, infrared etc. Now, in order to develop this project, we need to research in depth existing vulnerabilities and further security aspects in this area.

As the project is more focused on the development of a host based anomaly detection IDS research is needed on these fields. In (Lundin&Jonsson, 2000) some effective strategies for intrusion detection are presented, like the mobile agents one. In addition in (Farshchi&Jamil, 2006) useful ideas about wireless intrusion detection are presented. What is more, in (McGraw, 2005) some interesting thoughts are presented about the necessity of effective security mechanisms on mobile devices and mainly for intrusion detection systems. Furthermore, in (Kemp, 2005) some interesting thoughts about effective tactic on intrusion detection are presented, some of them useful for our research. Besides, in (Elison, 2006) there is a very good discussion about potential problems in general for intrusion detection.

The system that it is designed, acts like a constant transparent authentication system. As a result, before the designing attempt of the IDS, a research for authentication methods is needed. What is more, a research for biometric authentication mechanisms is also suggested, as the method with the threshold, where the system decides whether the user is authenticated or not, can be used with a similar to the IDS identifying whether an activity is normal or not (Clarke&Furnell, 2005).

In a recent survey presented in (Clarke et al 2002) we can see that PIN is the only authentication procedure that is used. Indeed, sometimes it is not used properly and as a result frauds occur. Another interesting point is the concern that users express for security aspects. This is certainly an optimistic message to continue our work and achieve our goals.

2.1 Statistical analysis

Mobile devices are mobile phones as well and one of their basic functions is telephony. As mentioned above, by the increasing processing power and storage capability of a device like these, statistical data about the calling activities and the user's roaming can be kept in the device and be analyzed. In case new data get over some specific limits, a warning signal may be sent. A very good algorithm is IDAMN, developed by (Samfat&Molva, 1997). Although it is a bit complicated, a very good point is the user classification they use: Domestic, Business, Corporate and Roamer according their usage. However, the complicity of the statistical data makes me think that it requires a lot of processing power where at the same time the percentage of false alarms may be high. On the other hand, a similar, simpler, algorithm can be used gathering and analyzing data, giving warnings when something unusual is happening. Finally, one more disadvantage may be the possible leak of personal data that may occur from gathering all these personal data of calls and roaming (Clarke et al 2002; Clarke and Furnell, 2005)

3. IDS framework for mobile devices

Now, all parts of the system need to be implemented at the mobile device.

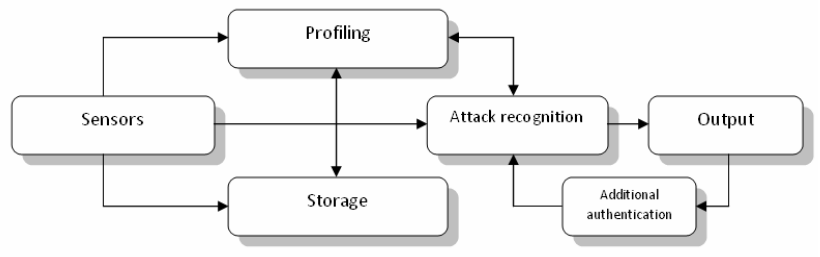

Figure 1: The plan of the IDS

Sensors are implemented at the mobile device monitoring all the network activities. Parts for monitoring telephony, user's roaming, exchanged SMS/MMS, wireless network activity, e-mail activity, file accessing applications, Internet activity, Bluetooth connections, Infrared activity, web browser activity, new applications installation. What is in common in all the above sensors is the common way an attack is recognized. By having kept a statistical amount of previous activity, which is hypothesized as normal, it is comparing with the received data and a threshold. In case the difference is higher than the allowed then the IDS is activated (Samfat&Molva, 1997).

Data are collected from sensors and then they are forwarded to storage and profiling session. At the second one, user's profile is created based on the data collected from the training period. This time is approximately one month but it is variable and it depends on the time that the device is used on daily basis. In other words the training period lasts as time as it is needed for enough data to be captured for profile creation. An alternative solution, more efficient for powerful devices as it requires more resources is when the profile is created from the activities of the last time interval, large enough in order to calculate users profile, average one month.

Indeed, when the users starts his/hers device for first time some brief questions are asked in order to be categorized in one of the default profiles. These are:

- Student
- Domestic
- Business
- Roaming

The categorization in these profiles except from providing data for protection during training period, it gives the opportunity for variable thresholds in attack recognitions. Different users do not have the same security expectations and for example thresholds in business profile can be tighter than the home one. This categorization gives the opportunity to the system to treat each user with a different way, more suitable to his/hers needs.

3.1 Hardware capability

This project is designed to be implemented to a wide range of devices. This of course is not possible as not all devices have the same capabilities. For example is there is no need to implement Bluetooth sensor in a device that does not support this protocol.

Group	1	2	3	4	5
Sensors	Telephony, Roaming, Exchanged SMS/MMS	All the previous plus Bluetooth, Infrared	All the previous plus Wifi connections, Internet activity	All the previous plus Web browser, E-mail activity	All the previous plus monitoring new applications installation

Table 1: Groups and sensors

Now, the mobile devices have to be categorized into these five groups according to their hardware capabilities. However, this is not simple as many vendors do not publish any details about their products. Actually, devices are categorized basically according to their CPU speed or memory. Table 1 presents a proposed categorization of the sensors into 5 groups. Of course this is not a necessity a device may be very powerful to have all sensors however some of them may be useless and not implemented. On the other hand, in case a devices performance is slowed down, some of the installed sensors can be removed. What is achieved with this method is that the designed IDS can be implemented to a wide range of devices.

3.2 Output

When a potential threat is recognized from the IDS then there are two levels, the warning and the alarm one. By the first time something unusual is recognized, the first (warning) level warns the users about potential abnormal activity. Then, he/she has the opportunity to authenticate again his/her self to continue that activity. In case this goes on, then the IDS is activated at the second layer, the alarm one. Then the network administrator is informed that a continuous abnormal activity takes place at the specific device. Now, additional authentication is mandatory, not optional as it was at the first layer. What is proposed for this a biometric authentication algorithm.

That on (Lodi et al 2002) is a very good one for voice recognition, not only by requiring low system resources, but also by its very effective results.

4 Discussion

This system is developed in order to recognize and identify abnormal activity on a mobile device. This recognition however, is based on the way user behaves with his/hers mobile. A potential vulnerability of the system is the fact that in case of an emergency, when user performs more calls and generally the whole activity of the system is increasing, the system is activated by false. Indeed, this reduces the reliability of the system and makes it more irritating for the user. This is the reason the optional additional authentication process is added at the first warning level.

What is more, the system needs a reset function/button. In case the device is sold again as second hand, all the previous settings in the IDS (profiles etc) need to be deleted and the training period needs to be started again for the new user. However, lots of care has to be given at this point as an attacker may be capable of resetting the IDS and perform his/hers malicious acts without a problem.

In general, it can be argued that the system is not able to follow any changes at user's attitude. For example, if someone changes his/hers job, then possibly the way he/she is using the device is changed as well. This of course is not similar with the attitude at the training time and consequently the IDS starts generating false alarms, something irritating. Once more, a reset function is necessary but with paying lots of attention at the authentication process of the person that performs the reset.

Furthermore, this system acts by capturing data from all kind of activities of the device. This however may be irritating for the user. Many people may feel that they are monitored from their own device, that their actions are captured. As a result, lots of care has to be given in order the system in not used for malefic purposes. For example, it can be modified and used by a company manager, to watch and monitor employees' activities, especially by monitoring their roaming.

In addition, the system is not capable of protecting the owner from attackers that know users attitude. For example, when an attacker knows the way that the victims uses his/hers device and the fact that this IDS model is implemented, then he/she is capable of stealing it and not be identified just by using it as its owner used it.

5. Conclusion

This framework is developed in 2006. As it can be argued that the area of mobile devices is a rapid developing are, the current situation is possible to be changed in a sort time. A future work can update this project by recategorizing them to new groups according to device resources of the exiting time. As devices are getting more powerful new sensors can be added and of course new groups covering all kind of activities. The author would be grateful to see this work updated and developed in future.

6. References

Barber, R. (2001). “Security in a mobile world – Is Bluetooth the answer?” Computers and Security, v 20, n 5, 2001, p 374-379

Clarke, N.L, Furnell, S.M., Rodwell, P.M., Reynolds, P.L. (2002). “Acceptance of subscriber authentication methods for mobile telephony devices” Computers and Security, v 21, n 3, 2002, p 220-228

Clarke, N.L, Furnell, S.M.(2005). “Authentication of users on mobile telephones - A survey of attitudes and practices” Computers and Security, v 24, n 7, October, 2005, p 519-527

Clarke, NL., Furnell, SM. (2005). “Biometrics - The promise versus the practice Source: Computer Fraud and Security”, v 2005, n 9, September, 2005, p 12-16

Elison, D. (2006). “Intrusion Detection, Theory and Practice” http://www.securityfocus.com/print/infocus/1203 accessed 1/2006

Farshchi, J. (2006). “Wireless Intrusion Detection Systems” http://www.securityfocus.com/print/infocus/1742 accessed 1/2006

Furnell, S. (2005). “Handheld hazards: The rise of malware on mobile devices” Computer Fraud and Security, v 2005, n 5, May, 2005, p 4-8

Hager, C., Midkiff, S. (2003). “Demonstrating Vulnerabilities in Bluetooth Security” Conference Record / IEEE Global Telecommunications Conference, v 3, 2003, p 1420-1424

Innella,P. (2006). “The evolution of Intrusion Detection Systems, Tetrad Digital Integrity”, LLC, 16 November 2001, http://www.securityfocus.com/print/infocus/1514 accessed 1/2006

Ivo, P. (2003). “Bluetooth and security” Proceedings of SPIE - The International Society for Optical Engineering, v 5445, Microwave and Optical Technology *2003*, 2004, p 55-59

Hynninen, J. (2006). “Experiences in Mobile Phone fraud” Helsinki University of Technology http://www.niksula.hut.fi/~jthynnin/mobfra.html accessed 7/2006

Kachirski, G. (2006). “Effective intrusion detection using multiple sensors” http://doi.ieeecomputersociety.org/10.1109/PDCAT.2005.34 accessed 1/2006

Kafi H., Conner, M. (2003). “Identifying security threats in ad hoc wireless network” Proceedings of the International Conference on Security and Management, v 1, Proceedings of the International Conference on Security and Management, SAM *2003*, 2003, p 34-38

Kemp, M. (2005). “For whom the bells toll: Effective IDS deployment strategies” Network Security, v 2005, n 5, May, 2005, p 16-18

Kitsos, P., Sklavos, N., Papadomanolakis, K., Koufopavlou, O. (2003) “Hardware Implementation of Bluetooth Security” IEEE Pervasive Computing, vol. 02, no. 1, pp. 21-29, January-March, 2003

Krugel, C, Toth, T. (2006). Applying Mobile Agent Technology. To Intrusion Detection. www.infosys.tuwien.ac.at/Staff/tt/publications/Applying_Mobile_agent_Technology_to_Intrusion_Detection.pdf accessed 1/2006

Lodi, A.; Toma, M.; Guerrieri, R (2002). "Very low complexity prompted speaker verification system based on HMM-modeling Acoustics, Speech, and Signal Processing" Proceedings. (ICASSP '02). IEEE International Conference on Volume 4, 13-17 May 2002 Page(s):IV-3912 - IV-3915 vol.4

Lundin, E., Jonsson, E. (2000). "Anomaly-based intrusion detection: Privacy concerns and other problems" Computer Networks, v 34, n 4, Oct, 2000, p 623-640

McGraw, G. (2005). "Are cell phones the next target?" Network Magazine, v 20, n 6, 2005, p 82

Mell, P., McLarnon, M. (2006). "Mobile Agent Attack Resistant Distributed. Hierarchical Intrusion Detection Systems" www.raid-symposium.org/raid99/PAPERS/Mell.pdf accessed 1/2006

Mobitedia. (2006). "Cell phones – Features Specs and user Reviews" http://www.mobiledia.com/phones/ accessed 7/2006

Papadaki, M., Furnell, S. (2004). "IDS or IPS: What is best?" Network Security, v 2004, n 7, July, 2004, p 15-19

Rawat, S., Gulati, V., Pujari, A. (2004). "Frequency- and ordering-based similarity measure for host-based intrusion detection" Information Management and Computer Security, v 12, n 5, 2004, p 411-421

Samfat, D., Molva, Refik. (1997). "IDAMN: An intrusion detection architecture for mobile networks" IEEE Journal on Selected Areas in Communications, v 15, n 7, Sep, 1997, p 1373-1380

Stamouli, I., Argyroudis, P., Tewari, H. (2006). "Real-time Intrusion Detection for Ad hoc Networks" https://www.cs.tcd.ie/~htewari/papers/wowmom05.pdf accessed 1/2006

Telecommunications magazine (2006). "Bluetooth still needs security bite", July 1, 2004, http://telecomtest.bvdep.com/International/article.asp?HH_ID=AR_646 accessed 1/2006

Teresa, L. (2006). "Detecting Intruders In Computer Systems" ,Computer Scince laboratory SRI International Menlo Park California http://citeseer.ist.psu.edu/lunt93detecting.html accessed 1/2006

The Register. (2006a). "Mobile Devices and Users Quocirca Insight Report" www.theregister.co.uk/2005/06/29/mobile_management_report.pdf accessed 1/2006

The Register (2006b). "Mobile web access on the up" http://www.theregister.co.uk/2006/04/19/mobile_ipsos/ accessed 8/2006

Westhoff, K., Paul, D. (2006). "Context Aware Detection of Selfish Nodes in DSR based Ad-hoc Networks" http://www.iponair.de/publications/Paul_Globecom02.pdf accessed 1/2006

Wiens, R. (2001). "Realistic Expectations for Intrusion Detection Systems" 19 March 2001, http://www.securityfocus.com/print/infocus/1206 accessed 1/2006

Yap, T., Ewe, H. (2005). "A mobile phone malicious software detection model with behavior checker" Lecture Notes in Computer Science, v 3597, Web and Communication Technologies and Internet-Related Social Issues - HSI 2005: 3rd International Conference on Human.Society@Internet. Proceedings, 2005, p 57-65

Yongguang Z., Wenke L. (2006). “Intrusion Detection in Wireless Ad-Hoc Networks” ACM MobiCom'2000 http://citeseer.ist.psu.edu/zhang00intrusion.html accessed 1/2006