Efficient Intrusion Detection for Mobile Devices Using Spatio-temporal Mobility Patterns

Sausan Yazji[1], Robert P. Dick[2], Peter Scheuermann[1], and Goce Trajcevski[1]

[1] EECS Dept., Northwestern University, Evanston, IL. 60208
[2] EECS Dept., University of Michigan, Ann Arbor, MI. 48109

Introduction

Mobile phones are ubiquitous and are used for email, text messages, navigation, education, and as a pyment tool (e.g., Mobile Money – extensively used in China and Japan [1]). Consequently, mobile devices carry a lot of personal data and, if stolen, that data can be more important than the loss of the device.

Most of the works on mobile devices security have focused on physical aspects and/or access control, which do not protect the private data on a stolen device that is in the post authentication state. However, some existing works, e.g. Laptop Cop [2] aim to protect data on stolen devices by remotely and manually deleting it, which requires user intervention. It may take hours before the user notices the loss of his device.

The main goal of this work is to efficiently detect a theft of a mobile device based on the intruder's anomalous behavior. In a previous study [3], we used network access and file system activities to build a behavioral model and were able to detect attacks on portable devices within 5 minutes with 90% accuracy. In this study, we use spatio-temporal information and trajectory analysis for modelling user behavior and anomaly detection.

While some works [4,5,6] have proposed mobility-based intrusion detection, to the best of our knowledge, this is the first mobile intrusion detection solution that is based on spatio-temporal information and trajectory analysis enabling a detection of an attack in 15 minutes with 81% accuracy. The simple data structure used to represent user model (2- and 3-dimension matrix), allows efficient lookup-based attack detection.

System Architecture

Our main objectives are to: (1) develop an efficient algorithm to derive a user model based on spatio-temporal information and trajectory analysis; (2) determine the accuracy of distinguishing individual users based on their motions patterns, and (3) provide high detection accuracy with the smallest possible delay at low energy cost. Our methodology is based on the following observations:

- most mobile systems have GPS receivers and can gather location traces.
- individuals tend to have small set of locations that they visit every day [7].
- individuals tend to take the same path when moving between the same locations [7].

P. Sénac, M. Ott, and A. Seneviratne (Eds.): MobiQuitous 2010, LNICST 73, pp. 342–343, 2012.

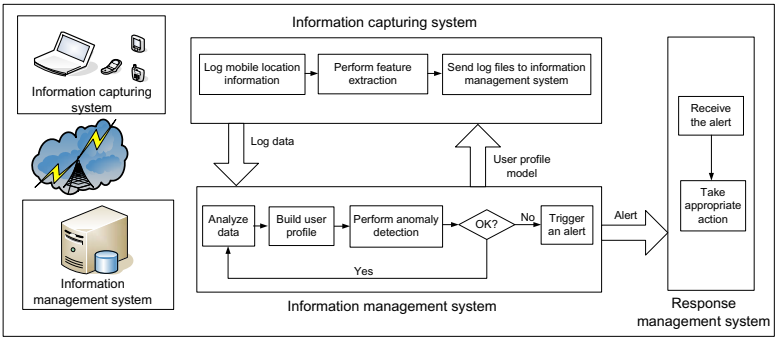

Fig. 1. System architecture

To achieve our objectives, we developed a system to automatically generate mobility models and detect behavioral anomalies. Figure 1 illustrates the system architecture which consists of: (ICS) – the *information capturing system*, residing on the mobile device, with a custom-developed application to track the device location; register it continuously in a new log every T minutes. It also contains the feature extraction module. (IMS) – the *information management system*, which collects the log-files from the ICS and resides on a computer with higher performance and much looser power consumption constraints than the mobile device. It is responsible for building mobility models and performing anomaly detection. Upon building the user model, the IMS sends it to the mobile device allowing it to detect attacks in the absence of wireless connection at some power consumption penalty. (RMS) – the *response management system* resides on both the mobile device and the remote server that hosts the IMS. Upon receiving an alert, the IMS identifies the appropriate action to be taken to protect data on the mobile device. These actions could be a notification to the device owner, locking device, or deleting data automatically.

References

1. Chen, L.-D.: A Model of Consumer Acceptance of Mobile Payment. J. IJMC 6(1), 32–52 (2008)
2. Laptop COP Software, `http://www.laptopcopsoftware.com/index.html`
3. Yazji, S., Chen, X., Dick, R.P., Scheuermann, P.: Implicit User Re-authentication for Mobile Devices. In: Zhang, D., Portmann, M., Tan, A.-H., Indulska, J. (eds.) UIC 2009. LNCS, vol. 5585, pp. 325–339. Springer, Heidelberg (2009)
4. Sun, B., Yu, F., Wu, K., Xiao, Y., Leung, V.: Enhancing Security Using Mobility-Based Anomaly Detection in Cellular Mobile Networks. IEEE Trans. Vehicular Technology (2007)
5. Hall, J., Barbeau, M., Kranakis, E.: Anomaly-Based Intrusion Detection Using Mobility Profiles of Public Transportation Users. In: Proc. WiMob (2005)
6. Yan, G., Eidenbenz, S., Sun, B.: Mobi-Watchdog: You Can Steal, But You Can't Run! In: Proc. WiSec (2009)
7. Gonzalez, M.C., Hidalgo, C.A., Barabasi, A.L.: Understanding Individual Human Mobility Patterns. J. Nature 453 (2008)