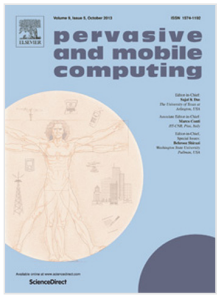
Accepted Manuscript



Anomaly detection for smartphone data streams

Yisroel Mirsky, Asaf Shabtai, Bracha Shapira, Yuval Elovici, Lior Rokach

PII: S1574-1192(16)30106-7
DOI: http://dx.doi.org/10.1016/j.pmcj.2016.07.006
Reference: PMCJ 732

To appear in: *Pervasive and Mobile Computing*

Received date: 2 December 2015
Revised date: 9 June 2016
Accepted date: 21 July 2016

Please cite this article as: Y. Mirsky, A. Shabtai, B. Shapira, Y. Elovici, L. Rokach, Anomaly detection for smartphone data streams, *Pervasive and Mobile Computing* (2016), http://dx.doi.org/10.1016/j.pmcj.2016.07.006

Anomaly Detection for Smartphone Data Streams

Yisroel Mirsky, Asaf Shabtai, Bracha Shapira
Yuval Elovici, Lior Rokach

Ben-Gurion University of the Negev, Beer Sheva, Israel
Department of Information Systems Engineering
{yisroel, shabtaia, bshapira, elovici, liorrk}@post.bgu.ac.il

Abstract

Smartphones centralize a great deal of users' private information and are thus a primary target for cyber-attack. The main goal of the attacker is to try to access and exfiltrate the private information stored in the smartphone without detection. In situations where explicit information is lacking, these attackers can still be detected in an automated way by analyzing data streams (continuously sampled information such as an application's CPU consumption, accelerometer readings, etc.). When clustered, anomaly detection techniques may be applied to the data stream in order to detect attacks in progress. In this paper we utilize an algorithm called pcStream that is well suited for detecting clusters in real world data streams and propose extensions to the pcStream algorithm designed to detect point, contextual, and collective anomalies. We provide a comprehensive evaluation that addresses mobile security issues on a unique dataset collected from 30 volunteers over eight months. Our evaluations show that the pcStream extensions can be used to effectively detect data leakage (point anomalies) and malicious activities (contextual anomalies) associated with malicious applications. Moreover, the algorithm can be used to detect when a device is being used by an unauthorized user (collective anomaly) within approximately 30 seconds with 1 false positive every two days.

Key words: Smartphone security, data streams, anomaly detection, contexts, continuous authentication

1 Introduction

In 2016, over two billion people will have a smartphone as a part of their daily lives [1]. Smartphones provide a means of communication, as well as a central location to store and organize information, a quality which makes