Accepted Manuscript

Identifying cyber threats to mobile-IoT applications in edge computing paradigm

Jemal Abawajy, Shamsul Huda, Shaila Sharmeen, Mohammad Mehedi Hassan, Ahmad Almogren

PII: S0167-739X(18)30090-6
DOI: https://doi.org/10.1016/j.future.2018.06.053
Reference: FUTURE 4315

To appear in: *Future Generation Computer Systems*

Received date : 13 January 2018
Revised date : 3 June 2018
Accepted date : 27 June 2018

Please cite this article as: J. Abawajy, S. Huda, S. Sharmeen, M.M. Hassan, A. Almogren, Identifying cyber threats to mobile-IoT applications in edge computing paradigm, *Future Generation Computer Systems* (2018), https://doi.org/10.1016/j.future.2018.06.053

Identifying Cyber Threats to Mobile-IoT Applications in Edge Computing Paradigm

Jemal Abawajy[1], Shamsul Huda[1], Shaila Sharmeen[1], Mohammad Mehedi Hassan[2] and Ahmad Almogren[2]

[1]School of Information Technology, Deakin University, Burwood, Melbourne, Australia
E-mail: jemal.abawajy@deakin.edu.au, shamsul.huda@deakin.edu.au, ssharmee@deakin.edu.au

[2]College of Computer and Information Sciences, King Saud University, Riyadh 11543, Saudi Arabia.
E-mail: mmhassan@ksu.edu.sa, ahalmogren@ksu.edu.sa

Abstract: The malware has become an increasing problem for Mobile-Internet of Things applications in edge computing platform. Variants of malware can be identified once their general characteristics are known and overtly malicious behavior can be identified. Some research has been performed using static analysis in order to identify privacy violating malware for IoT in edge computing. Dynamic analysis can be easily evaded as malware can adapt to avoid detection and has performance overheads. The case where an application lies about its intention for requesting a permission or intentionally violates the user's expectation of an applications behavior is not so well researched. This research extensively explores the fundamental gap in the current literature in terms of mobile malware. We particularly focus on a greater set of permissions which may be leveraged for other purposes, for example by using sensors to record user credentials or monitoring a user's movements. This research will attempt to identify such scenarios by employing behavioral analysis to determine when and how permissions are used and static and dynamic analysis to determine the behavior of application logic yet to execute. We proposed two-layer detection engine with hybrid feature analysis. Experimental results with real mobile malware IoT data show that our proposed approach with permission related features outperforms other detection engines.

Keywords: Cyber-threat, Mobile Malware, Internet of Things, Edge Computing, Feature Analysis.

1 Introduction

The IT industry is currently progressing into a "post-pc" era. General purpose computing platforms running traditional desktop operating systems are being replaced by powerful portable platforms such as smart phones and tablets. Functionality rich applications which were once confined to use on powerful desktop and laptop systems are now available on these portable mobile platforms as their computational power increases. On the other hand, while many of our modern devices are taking benefits from cloud computing, Internet of Things (IoT) manufacturers and application developers are starting to discover the benefits of using computational power from the devices themselves. The ability to do advanced on-device processing and analytics is the core concept of edge computing. The edge computing paradigm overcomes the limitations of centralized cloud computing by taking the control of applications away from the central nodes to the edge. As the public cloud vendors introduced large scale data centres to serve large number of users, this centralization increases the network latency and jitter (Roman et. al 2018). Edge computing minimizes the dependency on core computing environment and removes the bottleneck scenario of networks. It also eliminates the possibility of single point failure. For these reasons, Edge computing paradigm is the latest option for the delay sensitive modern applications.