3-21-2016

Detecting And Tracking Attacks in Mobile Edge Computing Platforms

Abderrahmen Mtibaa
University of Missouri-St. Louis, amtibaa@umsl.edu

Khaled A. Harras

Hussein Alnuweiri

ARC '16

مؤتمر مؤسسة قطر
السنوي للبحوث
QATAR FOUNDATION
ANNUAL RESEARCH
CONFERENCE

Towards World-class
Research and Innovation

مؤسسة قطر
Qatar Foundation
لإطلاق قدرات الإنسان
Unlocking human potential

Information Communications Technology Pillar

http://dx.doi.org/10.5339/qfarc.2016.ICTPP2011

Detecting And Tracking Attacks in Mobile Edge Computing Platforms

Abderrahmen Mtibaa[1], Khaled A. Harras[2], Hussein Alnuweiri[1]

[1]Texas A&M University in Qatar, QA
[2]Carnegie Mellon University, QA

Email: amtibaa@cmu.edu

Device-to-device (d2d) communication has emerged as a solution that promises high bit rates, low delay and low energy consumption which represents the key for novel technologies such as Google Glass, S Beam, and LTE-Direct. Such d2d communication has enabled computational offloading among collaborative mobile devices for a multitude of purposes such as reducing the overall energy, ensuring resource balancing across device, reducing the execution time, or simply executing applications whose computing requirements transcend what can be accomplished on a single device. While this novel computation platform has offered convenience and multiple other advantages, it obviously enables new security challenges and mobile network vulnerabilities. We anticipate challenging future security attacks resulting from the adoption of collaborative mobile edge cloud computing platforms, such as MDCs and FemtoClouds. In typical botnet attacks, "vertical communication" between a botmaster and infected bots, enables attacks that originate from outside the network. While intrusion detection systems typically analyze network traffic to detect anomalies, honeypots are used to attract and detect attackers, and firewalls are placed at the network periphery to filter undesired traffic. However, these traditional security measures are not as effective in protecting networks from insider attacks such as MobiBots, a mobile-to-mobile distributed botnet. This shortcoming is due to the mobility of bots and the distributed coordination that takes place in MobiBot attacks. In contrast to classical network attacks, these attacks are difficult to detect because MobiBots adopt "horizontal communication" that leverages frequent contacts amongst entities capable of exchanging data/code. In addition, this architecture does not provide any pre-established command and control channels (C&C) between a botmaster and its bots. Overall, such mobile device infections will circumvent classical security measures, ultimately enabling more sophisticated and dangerous attacks from within the network. We propose HoneyBot, a defense technique that detects, tracks, and isolates malicious device-to-device communication insider attacks. HoneyBots operate in three phases: detection, tracking, and isolation. In the detection phase, the HoneyBot operates in a vulnerable mode in order to detect lower layer and service-based malicious communication. We adopt a data driven approach, using real

Cite this article as: Mtibaa A, Harras KA, Alnuweiri H. (2016). Detecting And Tracking Attacks in Mobile Edge Computing Platforms. Qatar Foundation Annual Research Conference Proceedings 2016: ICTPP2011 http://dx.doi.org/10.5339/qfarc.2016.ICTPP2011.

world indoor mobility traces, to evaluate the impact of the number of HoneyBots deployed and their placement on the detection delay performance. Our results show that utilizing only a few HoneyBot nodes helps detect malicious infection in no more than 15 minutes. Once the HoneyBot detects malicious communication, it initiates the tracking phase which consists of disseminating control messages to help “cure” the infected nodes and trace back the infection paths used by the malicious nodes. We show that HoneyBots are able to accurately track the source(s) of the attack in less than 20 minutes. Once the source(s) of the attack is/are identified, the HoneyBot activates the isolation phase that aims at locating the suspected node. We assume that the suspect node is not a cooperative device that aims at hiding its identity by ignoring all the Honeybot messages. Therefore, the HoneyBot requests wireless fingerprints from all nodes that have encountered this suspect nodes at a given time period. These fingerprints are used to locate these nodes and narrow down the suspect’s location. To evaluate our localization accuracy, we first deploy an experimental testbed where we show that HoneyBots accurately localize the suspect node within 4 to 6 m^2. HoneyBots can operate efficiently in small numbers, as few as 2 or 3 nodes while improving the detection, tracking, and the isolation by a factor of 2 to 3. We also assess the scalability of HoneyBots using a large scale mobility trace with more than 500 nodes. We consider, in the attached Figure, a scenario of a corporate network consisting of 9 vulnerable devices labeled 1 to 9. Such network is attacked by one or many botmaster nodes using d2d MobiBot communication. We notice that attacks are propagated horizontally, bypassing all Firewall and intrusion detection techniques deployed by the corporate network administrators. In this scenario, we identify 3 main actors; the botmaster (red hexagon), the HoneyBot (green circle), the infected bot (red circle), and the cured or clear node (blue circle). We assume that the 9 nodes shown in the figure only represent the vulnerable d2d nodes in this corporate networks. We propose detection, tracking and isolation technique that aim at accurately and efficiently defend networks from insider d2d malicious communication.