C23 An Efficient and Effective Forensic Analysis Approach for the Internet of Things (IoT)

Anthony Skjellum, PhD, Auburn University, Dept of Computer Science and Software Eng, 345 W Magnolia, 3101 Shelby Center, Auburn, AL 36849-5347; Ankit Kumar Singh*, Auburn University, Dept of Comp, Sci and Software Engineering, 3101 Shelby Center, Auburn, AL 36849; and Janice Canedo*, Auburn University, 3101 Shelby Center, Auburn, AL 36849-5347*

After attending this presentation, attendees will better understand an IoT Forensics Framework that consists of both device and network-level forensics.

This presentation will affect the forensic science community by providing direction toward addressing changes in digital forensics with the introduction of IoT devices. Identification of the limitations of existing, early models for IoT Forensics with a new, resource-conscious paradigm offered for IoT Forensics combines concepts from continuous monitoring (network forensics) and computer forensics.

The IoT is an emerging distributed network of billions of smart devices ("things") that possess the ability to communicate and exchange data. The number of such devices is expected to increase rapidly, resulting in generating massive amounts of data. Considering these factors, Digital Forensic (DF) investigations will face new challenges arising from the ubiquitous use of the IoT in society. DF investigation processes including identification, collection, organization, and presentation in the context of the IoT devices must be understood, planned-for, and recognized as significantly different than the processes for common devices such as smart phones, tablets, servers, and Personal Computers (PCs).

Existing procedures used for handling DF investigations aren't sufficient for the IoT. Some investigators have already recognized this. For example, one recent model for the IoT-related crime investigations, Forensic Aware IoT (FAIoT) described by Hasan et al., requires that all registered IoT devices be monitored and that they store potential evidence in a shared repository.[1] A second model, the Forensic Edge Management System (FEMS) advanced by Oriwoh et al., proposes the use of a smart device that would be used for real-time monitoring and forensic services within a Smart Home IoT environment.[2]

While current models focus only on a device-driven architecture, this study's strategy is to create an IoT Forensics Framework that includes device and network forensics. The IoT devices will be connected and communicate through a network; therefore, identifying forensic elements and retrieving relevant evidence from the network is vital. To group similar events efficiently, investigative techniques are covered using data mining techniques including Bayesian Classification.

Overall, a systematic analysis approach geared toward handling IoT-related forensic investigations is needed. An IoT Forensics Framework is proposed that will impact all stages of forensic investigations and make the IoT domain more forensic-ready. Systematic trade-offs of static and dynamic resource overheads will be shown in order to achieve sufficient degrees of forensic fidelity. An argument that all IoT Forensics is best implemented as continuous monitoring, includes forensics for devices as well as the associated networks, uses secure protocols for communication between FEMS smart devices and other devices, and has small events grouped as super events shall be made clear to the attendees.

Reference(s):

1. Hasan R., Zawoad S. (2015) FAIoT: Towards Building a Forensics Aware Eco System for the Internet of Things. IEEE 12th International Conference on Services Computing. 279-284.
2. Oriwoh, E., Sant P. (2013) **The Forensics Edge Management System: A Concept and Design.** UIC-ATC '13 Proceedings of the 2013 IEEE 10th International Conference on Ubiquitous Intelligence & Computing and 2013 IEEE 10th International Conference on Autonomic & Trusted Computing. 544-550.

Internet of Things, Forensics, Framework