Cyber-Assurance for Internet of Things and Fog Computing Architectures

Tyson Brooks
U.S. DoD/Syracuse University
ttbrooks@syr.edu

Shiu-Kai Chin
Syracuse University
skchin@syr.edu

Erich Devendorf
U.S. Air Force
erich.devendorf.1@us.af.mil

Col William 'Dollar' Young
U.S. Air Force
william.young.3@us.af.mil

Abstract

Cyber-Assurance theory, application and embedded security for the Internet of Things (IoT)/Fog Computing architectures is based on theoretical aspects and studies of practical applications. The objective of this minitrack is to increase the visibility of current research and emergent trends in the area of Cyber-Assurance for IoT and Fog computing architectures. Cyber-Assurance is the justified confidence that networked systems are adequately secure to meet operational needs, even in the presence of attacks, failures, accidents and unexpected events. The Internet of Things (IoT) is the network of physical devices, vehicles, and other items embedded with electronics, software, sensors, actuators, and network connectivity which enable these objects to collect and exchange data. Fog computing refers to extending cloud computing to the edge of an enterprise's network. Cyber-assurance means that IoT/Fog Computing smart internet connected devices (ICD) and networks provide the opportunity of automatically securing themselves against cyber-attacks while addressing cybersecurity concerns.

1. Introduction

IoT/Fog Computing devices, systems and networks should be able to resist the various security cyber-attacks such as hacking of networks, devices, theft of information, disruption, etc. and be able to continue performing under severe environmental conditions. Through embedded processors and algorithms over the transmitted information, the miscoding and leaking of information during transmission channels has to monitor any loss, miscoding and leaking of data. Timely adjustments of information with falling quality and automatic switching to the best routing IoT/Fog Computing system by making uses of multi-directional routing is also warranted. Cyber-assurance will need to provide the principles and technologies to unify these systems to deliver the end-state goal of secure IoT/Fog Computing systems for greatly enhanced interoperability, scalability, performance, and agility.

The target audience of this minitrack will be composed of researchers, professionals and students working in the field of cyber-security, wireless technologies, information system theory, systems engineering, information security architecture and security system design along with university professors and researchers involved in IA, IoT and Fog Computing related networking. Through the research identified for this track, graduate students, researchers and academics who want to improve contribute their understanding of the latest security developments for the IoT and Fog Computing. This minitrack will focus on the security needs of the IoT/Fog Computing environment, highlighting key issues and identifying the associated security implications so that the general participates can readily grasp the core ideas in this area of research.

The following articles will be included in this minitrack:

2. Minitrack Articles.

Securing Wearables through the Creation of a Personal Fog Formatting

Abstract:
Increased reliance on wearables using Bluetooth requires additional security and privacy measures to protect these devices and personal data, regardless of device vendor. Most wearables lack the ability to monitor their communication connections and protect personal data without assistance. Attackers can force wearables to disconnect from base stations. When a wearable loses its connection to its base station, an attacker can connect to the wearable to steal stored personal data or await reconnection to the base station to eavesdrop on communications. If the base station inadvertently disconnects from the cloud serving a security-aware app, it would be unable to respond to a

URI: http://hdl.handle.net/10125/50581
ISBN: 978-0-9981331-1-9

rapid change in the security of its current environment. We design a personal fog incorporating wearables, base station, and cloud that allows the wearable to be situationally aware and manage inter- and intra-fog communications, given local personal fogs with the same app.

Addressing Operator Privacy in Automatic Dependent Surveillance – Broadcast (ADS-B)

Abstract:
Automatic Dependent Surveillance-Broadcast (ADS-B) is planned to be one of the pillars of the Next Generation Air Transportation System (NextGen). ADS-B lacks some capabilities that are essential for addressing cybersecurity concerns. We investigate security of ADS-B system and propose a framework composed of two solutions that would require minimal change to the existing system. The investigation focuses on providing an encrypted ADS-B system that provides confidentiality, availability, and integrity while requiring minimal changes to the existing ADS-B specification. The proposed framework consisting of two solutions is envisioned to be implemented through software updates while providing backwards compatibility. The biggest challenge during this study was to work within the constraints of the existing ADS-B system.