Chapter 53
Exploring Secure Computing for the Internet of Things, Internet of Everything, Web of Things, and Hyperconnectivity

Maurice Dawson
University of Missouri – St. Louis, USA

ABSTRACT

Secure computing is essential as environments continue to become intertwined and hyperconnected. As the Internet of Things (IoT), Web of Things (WoT), and the Internet of Everything (IoE) dominate the landscape of technological platforms, protection these complicated networks is important. The everyday person who wishes to have more devices that allow the ability to be connected needs to be aware of what threats they could be potentially exposing themselves to. Additionally, for the unknowing consumer of everyday products needs to be aware of what it means to have sensors, Radio Frequency IDentification (RFID), Bluetooth, and WiFi enabled products. This submission explores how Availability, Integrity, and Confidentiality (AIC) can be applied to IoT, WoT, and IoE with consideration for the application of these architectures in the defense sector.

INTRODUCTION

The next era of computing will be outside of the traditional desktop (Gubbi, Buyya, Marusic, & Palaniwami, 2013). When you consider Bring Your Own Device (BYOD) as a radical step imagine using devices such as a refrigerator that contain an embedded computing device to track the quantity of groceries within. This embedded device would allow access to email, weather, and other devices that allow connectivity through WiFi, or some Application Programming Interface (API) to a web based application. Thus, the data collected would be weather, thermostat cooling patterns, foods purchased, the cost of items per month, average consumption, and more. This massive amount of data that can also be collected means

there has to be the large place that this data is stored. At the moment organizations such as Cisco Systems and others are pushing for IoT, and IoT but none has a plan for ensuring Information Assurance (IA) posture is maintained during various modes of operation.

HYPERCONNECTIVITY

Hyperconnectivity is a growing trend that is driving cyber security experts to develop new security architectures for multiple platforms such as mobile devices, laptops, and even wearable displays (Dawson, Omar, Abramson, & Bessette, 2014). The futures of both national and international security rely on complex countermeasures to ensure that a proper security posture is maintained during this state of hyperconnectivity. To protect these systems from the exploitation of vulnerabilities, it is essential to understand current and future threats to include the instructions, laws, policies, mandates, and directives that drive their need to be secured. It is imperative to understand the potential security-related threats with the use of social media, mobile devices, virtual worlds, augmented reality, and mixed reality.

In an article published by Forbes, a contributor describes the concept of hyperconnectivity in six different scenarios (Ranadivé, 2013). These events range from energy to hospitality. In health-care there would be real time monitoring through wrist monitors that the medical staff could monitor to get instantaneous feeds on patients that are real time. They would be able to foresee problems before they occur or receive alerts during various events. Imagine a pregnant woman that is having early complications could be monitored first through a wristband that delivers real-time patient information wirelessly.

When discussing hyperconnectivity, it is necessary to examine systems of systems concepts. Systems of systems is a collection of systems tied together to create a more complex system (Popper, Bankes, Callaway, & DeLaurentis, 2004). When thinking about the possibilities of hyperconnectivity the Personal Area Network (PAN) is an excellent example as it allows multiple technologies to be interconnected with soil ware applications. The Google Glass has the potential to all Global Positioning System (GPS), social media, digital terrain overlays, and synchronization with other devices. This increases the complexity of the system as it becomes part of larger systems which multiplies the number of potential vulnerabilities.

INTERNET OF THINGS

IoT is a global infrastructure for information society enabling services by interconnecting physical and virtual things based on existing and evolving interoperable Information Communication Technologies (ICT) (International Telecommunication Union, 2012). Gartner has developed a figure which displays the hype cycle of emerging technologies. This hype circle shows the expectations on the y-axis where on the x-axis time is displayed [See Figure 1]. The time shown is the innovation trigger, the peak of inflated expectations, the trough of disillusionment, slope of enlightenment, and plateau of productivity (Gartner, 2014). What the figure fails to provide is anything associated with security about the technologies identified. The figure simply shows the cycle of emerging technologies with time corresponding to expectations.

8 more pages are available in the full version of this document, which may be purchased using the "Add to Cart" button on the publisher's webpage: www.igi-global.com/chapter/exploring-secure-computing-for-the-internet-of-things-internet-of-everything-web-of-things-and-hyperconnectivity/234988

Related Content

Design of a Home Automation App to Assist Elderly and Limited Mobility People
Bianca Stephanie Guimarães Morais, Álvaro Sobrinho, Helder Oliveira, Lenardo Chaves e Silvaand Robson Locatelli Macedo (2019). *The IoT and the Next Revolutions Automating the World (pp. 66-83).*
www.irma-international.org/chapter/design-of-a-home-automation-app-to-assist-elderly-and-limited-mobility-people/234023

Data Caching in Web Applications
Tony C. Shanand Winnie W. Hua (2008). *Encyclopedia of Internet Technologies and Applications (pp. 132-141).*
www.irma-international.org/chapter/data-caching-web-applications/16845

Multimedia Internet Applications over WiMAX Networks: State-of-the-Art and Research Challenges
Nicola Scalabrino, Daniele Miorandi, Enrico Gregoriand Imrich Chlamtac (2008). *Encyclopedia of Internet Technologies and Applications (pp. 331-338).*
www.irma-international.org/chapter/multimedia-internet-applications-over-wimax/16872

Edge Computing in Intelligent IoT
Rajarajeswari S.and Hema N. (2023). *Convergence of Deep Learning and Internet of Things: Computing and Technology (pp. 157-181).*
www.irma-international.org/chapter/edge-computing-in-intelligent-iot/316019

Open Source Software in the Arab World: A Literature Survey
Manar Abu Talib (2020). *Securing the Internet of Things: Concepts, Methodologies, Tools, and Applications (pp. 1646-1663).*
www.irma-international.org/chapter/open-source-software-in-the-arab-world/235014