Security-Smart is of Paramount Importance for Autonomous Vehicles

Saraju P. Mohanty
University of North Texas

I welcome the readers to the last issue of year 2019, the November 2019 issue, of the IEEE Consumer Electronics magazine. This becomes our second issue after Consumer Electronic Society decided to move from the previous editorial service to new one called "Common Design Service" for its production. I bring an excellent news to your attention. I came to know about 2018 impact factor of CEM. It is a pleasure to learn that the Impact Factor of CEM for year 2018 is 3.273. Based on my experiences, I consider this as an extraordinary achievement for a 7-year-old magazine. This is 128.24% increase with respect to the year 2017 impact factor of 1.434. I would like to thank all the members of the editorial board and enthusiastic authors who made this possible. I am hopeful that we will maintain same quality and standards and momentum trend for future years.

The current issue of IEEE CE magazine has a theme of vehicular security. I have discussed the concept of Energy-Smart, Security-Smart, and Response-Smart (ESR-Smart) in the past in my editorials as well many keynote addresses. This is theme on vehicular security is a specific example of security-smart. Security-Smart deals with the security, privacy, or ownership-protection of electronic systems as well as that of the data that these systems capture, process, or store. In many articles and keynote addresses, I have formally defined smart cities as well as discussed the technologies and components needed for their design and operations. The smart cities use one or multiple smart components, which are essentially cyber-physical systems (CPS) built using Internet-of-Things (IoT). The components include smart healthcare, smart transportation, smart agriculture, smart infrastructure, and smart grids.

Security and privacy are important for any of these components of smart cities. However, the challenges to provide the security/privacy solutions is not same for different components and technologies deployed in the smart cities. The smart healthcare domain that uses various devices in the Internet-of-Medical-Things (IoMT) framework need to have security/privacy solutions which does not introduce much energy overheads. The IoMT devices many include medical sensors, Implantable Medical Devices (IMDs), or Wearable Medical Devices (WMDs). The IMDs which in the current generation design may have communications capabilities along with WMDs are collectively defined as Implantable and Wearable Medical Devices (IWMDs). I envision that IWMDs in the framework of IoMT may lead to realization of Internet-of-Everything (IoE) in which users are more active participants through crowdsourcing and human-in-the-loop (HITL). IWMDs are severely energy constrained and hence security solutions need to take that into account. For the smart cars, latency overhead due to security is the critical constraint with some tolerable energy overhead. The latency introduced by any security mechanisms should be less than a millisecond for smart cars to be effective. However, for battery operated electric vehicles (EV) the driving range can be affected by energy overhead. Security solutions for Unmanned Aerial Vehicle (UAV) is much more difficult due to both energy and latency constraints need to be taken into account as battery life can affect flying range and battery size can affect aerodynamics.

Due to the diverse nature of constraints involved in various applications, careful thoughts on the use of software or hardware-based security/privacy solutions is needed. Keeping these constraints in consideration I define "Hardware-Assisted Security (HAS)" as the optimal solution for energy and security trade-offs.

Hardware-Assisted Security (HAS) is the security provided by hardware for: (1) the information being processed, (2) hardwares themselves, and (3) the overall system. HAS may involve additional hardware components used for security, hardware design modifications, and/or system design modifications. The HAS methodologies need to be incorporated right during the design phase of the systems, so that no retrofitting is required after the system is built. This is the essence of emerging concepts of Security-by-Design (SbD) and Privacy-by-Design (PbD) which can be together called Security and Privacy and by Design (SPbD).

Vehicular security is a specific subset of the security/privacy problems associated with connected and/or smart vehicles. Smart/connected cars can have 100 Electronic Control Units (ECUs) and 100 million lines of code, each from different vendors which makes these target of massive security issues. With the ambition of having autonomous or driver-less vehicles in future, this problem of security/privacy is only going to be worse. Imagine the traffic jam, the fatal accidents if the signal between sensors and actuators are tampered. The various forms of security attacks on smart/connected vehicles include eavesdropping, data tampering, impersonation/forgery, man-in-the-middle, and denial of service (DoS)/jamming. The privacy issues in connected, smart automotive may involve system privacy, location privacy, and privacy of the driver and passengers. System privacy involves learning details of the insides/components of the vehicle other than the owner so that attackers can exploit them for security breaches. Location privacy reveals location of the vehicles through some form of tracking due to cellular as well as GPS connectivity. The current issue includes several articles addressing many aspects of vehicular security.

FEATURE ARTICLES

Early Detection of Cardiovascular Diseases Using Wearable Ultrasound Device: This article presents an ultrasound based wearable device for early detection of cardiovascular disease.

Blockchain-enabled Smart Contracts for Enhancing Distributor-to-Consumer Transactions: This article presents a smart contract-based Distributor-to-Consumer (D2C) transaction mechanism to improve efficiency and prevent counterfeits in the consumer electronics (CE) industry.

Finger-vein as a Biometric based Authentication: This article presents finger-vein based biometric authentication method.

Tree-based Attack-Defense Model for Risk Assessment in Multi-UAV Networks: This article presents an attack-defense model for security analysis of multi-UAV networks (or Internet of drones).

An Efficient Anti-Phishing Method to Secure eConsume: This article presents a method called Resource Request based Phishing Discovery (RRPD) to provide security against phishing.

Security Vulnerabilities in Raspberry Pi: This article presents anysis of different hardware and software vulnerabilities of widely used single-board computing devices Raspberry Pi.

MultiScan - A Private Online Virus Detection System: This article presents a virus detection system useful for operating systems of tablets and smart phones.

Evaluating Technologies for Reliable Software in Consumer Electronics: This article presents reliability models of softwares of consumer electronics which is increasing along with their hardware components.

Broadcast-Based Hybrid Wired-Wireless Network-on-Chip for GPGPUs: This article presents a Network-on-Chips (NoC) based method for efficient data transfer in the Graphical Processing Units (GPUs).

Energy-Aware Core Switching for Mobile Devices with a Heterogeneous Multicore Processor: This article discusses the core assignment problem for mobile devices with a heterogeneous multicore processor for energy consumption and performance trade-offs.

COLUMNS

Bits Vs. Electrons -- Connecting: This article titled "Connecting" by Bob Frankston presents is perspective on the growth of connecting technology over the time.

The Art of Storage -- Immersive Storage: This article discusses digital storage trends in the wearable devices that support virtual reality (VR), augmented reality (AR) and light field imaging.

SPECIAL SECTION

This special section titled "Emerging Paradigms in Vehicular Cybersecurity" presents selected articles which discuss various advances in research related security and privacy of smart and connected vehicles. I would like to thank the Guest Editors Himanshu Thapliyal and Stacy Prowell, for all their hard work for this strong special section which will be a good reading for CE community around the globe who are specifically engaged in research and development of smart cars, smart automotive, and smart transportation.

LOOKING FORWARD

I hope this issue dedicated to vehicular security becomes a good reading for a wider set of CE community to advance their knowledge. CE magazine will continue the trend of covering more themes in future issues on the latest hot topics with the help of editorial board and authors around the globe. I hope to continue excellent quality CE magazine for our readers with the production team.

Saraju P. Mohanty is the Editor in Chief of the IEEE CONSUMER ELECTRONICS MAGAZINE and Professor in the Department of Computer Science and Engineering (CSE), University of North Texas (UNT), Denton, TX, USA. Contact him at: Saraju.Mohanty@unt.edu.