Security and Privacy by Design is Key in the Internet of Everything (IoE) Era

Saraju P. Mohanty
University of North Texas

I welcome the readers to the 2nd issue of 2020 of IEEE Consumer Electronics Magazine. The cover theme of this issue is dedicated to Security and Privacy by Design (SPbD). The cover essentially conveys the idea that Cyber-Physical Systems (CPS) such as (smart grid, smart healthcare, etc.) need to have security/privacy aspect right from the beginning of the design cycle not retrofitted. In this context several questions include the following arise:

(1) What is Security and Privacy by Design (SPbD)?
(2) What is Internet-of-Everything (IoE)?
(3) Why Security and Privacy by Design (SPbD)?

The Security by Design (SbD) and Privacy by Design (PbD) are system design paradigms to ensure security and privacy are considered right from the beginning of the design phase so that retrofitting at the later stage is not needed. These can be collectively called Security and Privacy by Design (SPbD), and Privacy and Security by Design (PSbD). Based on the 7-principles of PbD proposed by the inventor, I present the 7-principle of SPbD/PSbD as follows: (1) Security/Privacy features should be Proactive not Reactive, (2) Security/Privacy should be Default, (3) Security/Privacy should be Embedded into Design, (4) Security/Privacy should be incorporated as a Full Functionality - Positive-Sum, not Zero-Sum without trade-offs, (5) The should be End-to-End Security/Privacy for Lifecycle Protection, (6) Security/Privacy solutions should have Visibility and Transparency, and (7) Security/Privacy solutions should have Respect for Users.

We have been seeing Internet-of-Things (IoT) being deployed to ensure that smart system and smart system of systems (like smart cities) are possible with the use of right variety of connected sensors, and data analytics. IoT computing then evolved to edge computing and fog computing based on the location of computing and intelligence. Edge/fog computing advocates computation and processing close to the sensor and user so that less traffic data goes to the cloud through Internet. As a natural evolution, when and implantable or wearable is connected to the IoT, an user becomes part of the IoT as Human-in-the-Loop (HITL). At the same time humans can provide data though crowdsourcing mechanism which can be used for AI/ML modeling and data analytics and used form IoT intelligence. There are four main components to an IoE are the following: (1) People, (2) Data, (3) Process, and (4) Things. In IoE framework device, system, and data security is required. In IoE framework system, location, and data privacy is also important. The SPbD/PSbD mechanisms has the potentials to provide both security and privacy in the IoE framework to ensure the security and privacy is full proof.

FEATURE ARTICLES

PUFChain: Hardware-Assisted Blockchain for Sustainable Simultaneous Device and Data Security in Internet of Everything (IoE): This article presents the first-ever blockchain which is overhauled by hardware-assisted security (HAS) mechanism so that it can simultaneously handle device and data security, which is important for the emerging Internet-of-Everything (IoE).

Consumer IoT: Security Vulnerability Case Studies and Solutions: This article presents selected common attacks faced by consumer IoT devices and suggests potential strategies for their mitigation with intention for provide inputs for the design of consumer IoT devices.

Supporting Blockchain based Cryptocurrency Mobile Payment with Smart Devices: This article presents schemes to obtain cryptocurrency mobile payment while overcoming high storage cost and payment processing latency of the blockchains.

Design of a framework to detect device spoofing attacks using network characteristics: This article presents a mechanism for detection of device spoofing attacks based on physical characteristics of networks.

Tracking Attacks on Virtual Reality Systems: This article present attacks and possible countermeasure of the security of Virtual Reality (VR) systems.

Power Management Strategies for Medical Information Transmission in Wireless Body Sensor Networks: This article presents discussions on the impact of power management techniques on resource-constrained networks for in healthcare framework.

Autonomous Tactical Deployment of the UAV Array Using Self-Organized Swarm Intelligence: This article discussed application of swarm intelligence for the arrays of autonomous unmanned aerial vehicles (UAVs) for effective deployment in various applications.

Extending aspect-oriented programming for dynamic user's activity detection in mobile app analytics: This article analyzes the possibility of Oriented Programming for providing a mechanism for detecting activity of the users inside mobile apps.

COLUMNS

Bits Vs. Electrons -- Communities of Things: This article presents the vision of Communities of Things in which a community using a set of IoT devices can present their collective ability.

Storage -- New Electronic Architectures: This article presents perspectives of new architectures which are needed due to need for data driven processing of AI and IoT.

Energy & Security Matters -- Switch Technologies: Powering milliWatts to MegaWatts: The article presents views of electronic switch technologies used in the power supplies from a portable consumer electronics system to large power electronics systems.

SPECIAL SECTION

The cover theme articles selected by the team of guest editors are presented in the Special Section titled “Privacy and Security by Design”. I would like to thank the Guest Editors Ibrahim J. Gedeon, Pamela Snively, Carey Frey, Wahab Almuhtadi, and Saraju P. Mohanty for all their hard work for this strong special section which will be a good reading for CE community around the globe.

I would like to sincerely thank TELUS Communications for their generous support to sponsor this thematic issue on Privacy and Security by Design.

I would like to thank Xavier Fernando for his hard work for selecting articles for a Special Section on Implementable Humanitarian Technology.

LOOKING FORWARD

I hope this issue dedicated to Privacy and Security by Design 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 for our enthusiastic readers in future issues on the latest hot topics with the help of editorial board and authors around the globe.

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.