IEEE SECURITY & PRIVACY
THE IoT AND SECURITY AND PRIVACY
VOLUME 17
NUMBER 5
SEPTEMBER/OCTOBER 2019
WWW.COMPUTER.ORG/SECURITY

Cybersecurity for the Masses ■ Toward Automated Firmware Analysis ■ It Takes a Village

IEEE

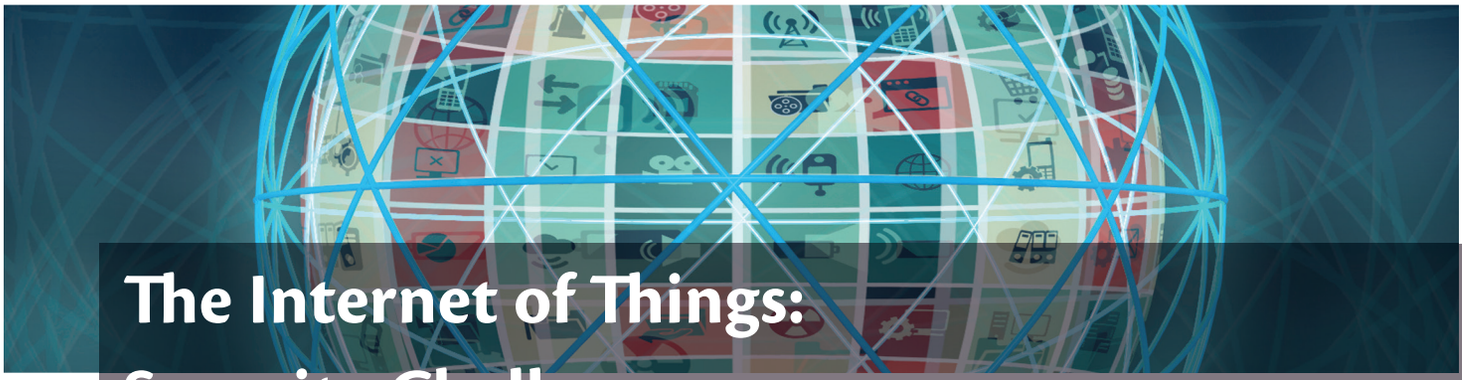
SECURITY & PRIVACY

Building Dependability, Reliability, and Trust

The IoT and Security and Privacy

Reliability Society
IEEE COMPUTER SOCIETY
IEEE

September/October 2019
Vol. 17, No. 5



The Internet of Things: Security Challenges

Paul C. van Oorschot | Carleton University
Sean W. Smith | Dartmouth College

Our special issue of *IEEE Security & Privacy* explores security and privacy issues related to the Internet of Things (IoT). But what is the IoT? A simplified description is that it involves embedding, at massive scale, processor-based systems into physical infrastructure and everyday objects, including things that neither look like computers nor communicate using the Internet Protocol. Two important elements are of note: sensors that provide an input mechanism from the real world to the digital world (essentially present in all IoT systems) and actuators that result in mechanically induced changes to the physical world (commonly a defining characteristic of cyberphysical systems).

Historically, when things went wrong in the traditional Internet, or the Internet of Computers (IoC), this caused problems in the digital world of computers—and occasionally, this would indirectly impact the physical world. For example, corrupted databases could disrupt air travel, and theft of credit card or banking information could lead to financial losses. In contrast, when things go wrong in an IoT world, there can be direct physical consequences in the real world: for example, unlocking a gate or building door, altering heating or cooling systems, affecting the steering or braking of a vehicle, even, perhaps, killing the host of an implanted medical device. In this sense, with the IoT, security-related problems in the digital world have greater direct consequences on physical-world safety and security. This changes things, increasing the risks and consequences of digital attacks.

What else is different? Embedded processors are now ubiquitous, permeating our physical environments and personal lives. Typical IoT devices have limited, often wireless-only, user interfaces and constrained resources (processing, memory, bandwidth). Even if the resources in a physically embedded system do not appear to be constrained today, by Moore's law, they almost certainly will appear to be constrained in 10 or 20 years from now, as that device still lives on. As has been discussed elsewhere, IoT properties contribute to a set of new security issues beyond those experienced in the traditional IoC. A few of those concerns include the following:

- Device-access, maintenance, and software-update issues arise, including those due to longer lifetimes (e.g., compared to smartphones and desktop computers).
- There are vastly larger numbers of manufacturers, most without traditional information technology (IT) expertise, resulting in interoperability issues and poor security hygiene.

Digital Object Identifier 10.1109/MSEC.2019.2925918
Date of publication: 3 September 2019

- This lack of IT expertise extends to end users (who are all de facto system administrators).
- Scale (number of devices) and global connectedness exacerbate all issues.

Our special issue's call for papers (CFP) solicited articles in specific areas of focus, including smart homes, consumer devices, embedded systems, and supporting infrastructures. The CFP de-emphasized some topics that have been dealt with in other venues, such as IoT issues that arise in connection with critical infrastructure, cyberphysical systems, customized industrial IoT, smart medicine, and smart automobiles. This left a wide range of IoT security and privacy topics such as

- system and software security of home IoT devices, including trust management
- lightweight cryptography, protocols, and standards for consumer IoT
- lifecycle, longevity, and aging issues, including software updates
- issues arising due to multiple IoT deployment silos within a home
- issues due to the overall architecture for consumer-targeted IoT applications
- novel privacy, liability, and legal issues raised by commodity IoT devices
- related security and privacy risks, including those due to malware.

From the submissions received, we selected a sequence of five articles that show the threats raised by individual IoT devices and larger populations of devices as well as how countermeasures may help mitigate these threats on the level of individual devices and broader populations.

The first special-issue article highlights the fact that IoT threats are real. Junia Valente, Matthew A. Wynn, and Alvaro A. Cardenas, using an explicit sequence of examples, explain how security vulnerabilities in commercial IoT (smart) products can have significant nontechnical consequences in personal lives. The attacks considered involve specific devices: consumer drones, IoT cameras, smart toys for children, and sexual toys (e.g., smart vibrators). The vulnerabilities discussed manifest at a wide range of points, from end devices to cloud services to the communication protocols connecting them. In the IoT settings considered, many of the attacks are enabled by violations of what would be considered, in the standard IoC, security best practices—for example, use of global default passwords is a clear violation. The article serves both to raise awareness of risks and bring attention to ethical and legal questions that relate IoT devices to safety, privacy, and sexual assault considerations.

Musard Balliu, Iulia Bastys, and Andrei Sabelfeld look at the larger design picture. They consider functionality and risks in two categories of IoT software applications (IoT apps): in-vehicle apps and user-programmed cloud-hosted apps. The latter run on platforms that provide IoT automation services or frameworks that take input from sensors and produce responses. As background, a general web service like If This Then That may use input from one IoT device as a trigger that sends a signal to another IoT device; in this way, a web-based code snippet may be used as part of a distributed home automation application that relates actions in the physical world—for example, a motion sensor may trigger a light to turn on as a result of a cloud-based decision. In other words, an IoT app (code snippet) runs on a user's behalf, providing user-desired functionality (involving IoT devices) to manage relationships between IoT objects and/or connect them to online services and social networks. The article helps us to understand new threats and opportunities that arise when services/apps are programmed to interact with real-world objects.

Smart devices may have functionalities and vulnerabilities whose interactions together create safety and security risks due to possible device-composition conflicts. Z. Berkay Celik, Patrick McDaniel, Gang Tan, Leonardo Babun, and A. Selcuk Uluagac discuss verification techniques to help uncover these. They note that it is insufficient to verify individual IoT devices since that does not take into account interactions between, for example, colocated devices. A suggestion is to use analysis techniques that involve state machines and model checkers.

Can we address security risks if ubiquitous IoT devices are unpatchable and an analyst has only firmware binary files available? Grant Hernandez, Farhaan Fowze, Dave (Jing) Tian, Tuba Yavuz, Patrick Traynor, and Kevin R.B. Butler survey how automated security-analysis methods apply to the particular problems of IoT firmware, which may contain malware or vulnerabilities not found as easily as in their IoC counterparts. They leverage experience in security analysis of USB and Android firmware. More generally, the article informs readers about challenges involved in the analysis of custom firmware on embedded systems, which is often closed source and proprietary, and how existing binary analysis techniques and tools cannot always be directly applied to IoT processor architectures. The authors share lessons learned.

Securing an emerging IoT real world requires characterizing what it means for IoT devices to interact securely and establishing real-world mechanisms to get

there. Hannes Tschofenig and Emmanuel Baccelli survey what the Internet Engineering Task Force (IETF) is doing on this front. They give an informed overview of current IETF activities on protocol standards for constrained IoT devices (e.g., applicable to IoT/smart-home deployments) and how these protocols address European security guidelines, such as the European Union Agency for Cybersecurity, or ENISA. This is explored in line with seven areas of IETF work: authentication and communication security (including Transmission Control Protocol versus Use Datagram Protocol considerations, i.e., TCP versus UDP); object security; authorization and access control; cryptographic algorithms; credential and key management, including secure bootstrapping; restricting communications (including use of Manufacturer Usage Descriptions files, i.e., MUD files); and software/firmware update.

A future world where small computing systems permeate physical infrastructure is coming, perhaps sooner than computer security professionals can respond to and prepare for it. We hope this special issue offers a helpful road map. ■

Paul C. van Oorschot is with Carleton University. Contact him at paulv@scs.carleton.ca.

Sean W. Smith is a professor of computer science at Dartmouth College. Contact him at sws@cs.dartmouth.edu.

Digital Object Identifier 10.1109/MSEC.2019.2933706