Securing the Internet of Things (IoT)

Joseph Rossi

September 19, 2021

The Rise of IoT

Over the past decade, the Internet of Things (IoT) has transformed from a start-up buzzword into becoming an integral part of everyday life. The ubiquity and low cost of smartphones and the cloud have significantly lowered the bar to entry for new and existing businesses to deliver these Internet connected "smart" devices into the hands of consumers. Many of these products integrate with cloud services require barely any software engineering to get up and running. Don't have a free hand to start the coffee machine while making breakfast? "Alexa, turn on my coffee machine". Reading on the couch while it's getting dark outside? "Alexa, turn on the living-room lamp." Cars, toasters, refrigerators. . . they're all (not so slowly) joining the IoT.

While IoT devices continue to overtake the home, industrial systems are utiliting IoT to increase manufacturing efficiency, enable smarter facilities management[1], and to provide scalable cost-efficient access to once costly services. In medicine, there are products that allow diabetes patients to monitor and manage their own insulin[2] without incurring the cost of frequent doctor visits. In civil infrastructure, IoT solutions are starting to enable smart stormwater management[3]. The IDC predicts that by 2025 that 55% of all data will be generated by the IoT, 43% of AI tasks will run their computation on edge devices, and 70% of enterprises will have incorporated IoT edge computing into their operations by 2023.[4]

What about security?

With IoT rapidly integrating into every aspect of business and society, it is becoming more essential than ever that these devices are secure from cyberattacks. Nowadays it is rare to go a week without hearing of a new vulnerability, data leak, or ransomware attack that compromises the data of hundreds or thousands of people. While the risk are already uncomfortable with exposing personal data, they become unacceptable when a compromised insulin pump can kill you[1], or foreign hackers are looking to gain control of a country's power grid.[5] The extreme hazards of cyberattacks escalate from financial hardships and identity theft to hazards that could inflict instant physical harm on individuals or communities. Developing and deploy safe and secure systems becomes of paramount importance.

Security on the Internet has historically been a bit of an afterthought. The original technology and protocols powering the Internet (ARPANET, UDP, TCP, HTTP, etc) were not developed with security in mind. As more and more people put their data personal and financial data online in the 1990s and 2000s, the need for secure communication started taking center stage. Even today, simple web services attempting to follow mondern best practices suffer from security breaches, DDoS, and randomware. For IoT system, the challenge to running secure systesm becomes even trickier.

One of the features IoT that makes security challenging is the many layers involved in the end-to-end system[6]. These layers include everything from the small edge devices up through the applications running in the cloud that constantly analyzing and making predictions based on data from the devices. Security vulnerabilities exist and can be exploited in any (and multiple) layers. Adding to the complication, each tier uses different types of computing resources and different connectivity technology, and there are different protocols to exploit at every layer. Edge devices may communicate over Bluetooth LE, WiFi (and all its security protocols), Zibgee, etc, while more application servers are setup in the clound, sharing hardware with hundreds of other companies. Securing every layer in these systems becomes a daunting challenge.

Ok, security is important and tricky. How do we do it?

Research has been primary driver for the advancement of security on the Internet. There is a culture among the security community that encourages open publication of cryptographic protocols and implementations of security. After the standards are published, other researchers try to break them! So when organizations like the NSA develop and publish cryptograph standards like SHA1, the research community can expose security failures so other professionals know to move away from them.[7]

The culture of testing device security has evovled with the rise of the IoT to focus less on cryptographic robustness and more towards uncovering software vulnerabilities. With the proliferation of cheap microprocessors making there was into every eletronic device, vulnerabilities in the software stack (due to implementation bugs), especially in then vendor written firmware could leave hundres or thousands of devices vulnerable to exploit. Researchers in Singapore recently found a variety of vulnerability in the Bluetooth stacks of multiple SoCs.

[1] This example in no way reflects that the referenced Tandem product poses any such risk. It's simply to illustrate the risk of insecure IoT medical products. According to the website, t:slim X2 Insulin Pump is being developed in accordance with FDA guidelines.

Garbelini et al. showed that with cheap commodity hardware, an attacker can exploit vulnerabilities in these chipsets to render the device non-functional.[8] Remember, some of these chips could be preventing your city's streets from flooding when it rains. Crashing these devices is could prevent them from functioning properly when they're needed most.

While many researchers (and the media) focus finding vulnerabilities in IoT systems, others focus on defining practices that IoT vendors and system designers could adopt for their own networks. For example, Bonetto et al.[9] proposed an architecture that details the different layer of IoT applications and specifically dives into each one, incorporating details such as how security keys are managed, how new edge devices securely join a network, and where to draw the boundaries between differnet parts of the network to minimize the attack surface. They focus primarily the protocols used the differnet application layers, but also factor in the resource contrained nature edge devices by introducing a gateway between the "constrained" (i.e. isolated) and "unconstrained" networks.

Where do we go from here?

While there seems to be a plethora of research on

Citations

[1] Microsoft, "What is IoT?" Sep. 2021. https://azure.microsoft.com/en-us/overview/internet-of-things-iot/what-is-the-internet-of-things/

[2] Tandem, "T:slim X2 insulin pump," Sep. 2021. https://www.tandemdiabetes.com/products/t-slim-x2-insulin-pump

[3] OptiRTC, "Optimizing stormwater management," Sep. 2021. https://optirtc.com/

[4] J. R. Reinsel Danel; Gantz, "The digitization of the world, from edge to core," IDC, 2018.

[5] L. H. Newman, "Russian hackers havne't stopped probing the US power grid," Nov. 2018. https://www.wired.com/story/russian-hackers-us-power-grid-attacks/

[6] IoTSense, "The layers of IoT," Jun. 2018. https://medium.com/@iotsense/the-layers-of-iot-a9daf122acc9

[7] G. L. T. Peyrin, "SHA-1 is a shambles: First chosen-prefix collision on SHA-1and application to the PGP web of trust," 2020.

[8] M. E. G. S. C. V. B. S. S. E. Kurniawan, "BRAKTOOTH: Causing havoc on bluetooth link manager," Sep. 2021.

[9] R. Bonetto, N. Bui, V. Lakkundi, A. Olivereau, A. Serbanati, and M. Rossi, "Secure communication for smart IoT objects: Protocol stacks, use cases and practical examples," in *2012 IEEE international symposium on a world of wireless, mobile and multimedia networks (WoWMoM)*, 2012, pp. 1–7. doi: 10.1109/WoWMoM.2012.6263790.