Infrastructure for Securing IoT

Srinivasan Seshan (srini@cs.cmu.edu)

The demands on metropolitan wireless networks is likely to change dramatically over the coming years due to the emergence of new applications and devices. The network infrastructure will need to adapt to meet these changing demands. In order to design the future infrastructure, we must first understand these workload trends and the applications that create them. In this white paper, we focus on the impact that the Internet of Things will have on our wireless networking and mobile computing infrastructure.

The Internet-of-Things (IoT) has quickly moved from hype to reality; Gartner, Inc. estimates that the number of deployed IoT devices will grow from 5 Billion in 2015 to 25 Billion in 2020. Like other disruptive technologies, such as smartphones and cloud computing, IoT holds the potential for societal scale impact by transforming many industries as well as our daily lives.

While IoT has huge potential, issues such as security remain a significant stumbling block to its wide deployment. The reason is that securing the IoT infrastructure must tackle very different issues than securing the current IT infrastructure. First, IoT device vendor priorities have been providing novel functionality, getting their products to market soon, making them easy to use, and making them very inexpensive. This combination of goals leads to software development practices that are more risky and error-prone, which, in turn, leads to devices with many security vulnerabilities. In addition, resource limitations of the resulting devices limit the range of software that can run on them. Second, IoT devices are long-lived. As a result, IoT devices are often used well after the companies that developed them provide official support. Third, IoT devices are diverse. While the IT ecosystem is dominated by just a few operating systems, the IoT environment consists of a wide range of custom developed embedded systems. The vulnerabilities exhibited by a group of IoT device is similarly larger and more diverse than a similar set of traditional IT devices. In combination, these factors suggest the flaws associated with IoT devices are inherently *unfixable* and that we cannot rely on patching and ant-virus software like we do in the traditional IT environment. In contrast, we need to rely more on the network and edge cloud services to secure our IoT systems.

Any security infrastructure design can be split up along three key dimensions: (1) abstractions for security policies; (2) mechanisms to learn attack and normal profiles; and (3) dynamic and context-aware enforcement capabilities. As we move IoT security into the edge cloud infrastructure, we will need to rethink security along all three of these dimensions. For example, IoT devices can interact with other devices via explicit channels (e.g. a single app may use multiple IoT devices) or implicitly by affecting the *physical* world around them (e.g., an IoT light bulb may trigger an IoT light sensor). Note that compromised devices can affect both applications that use them directly or indirectly. As a result, the polices that we use in IoT settings are likely to be more complex and dynamic that those in traditional settings. The diversity of IoT devices makes learning the properties of normal and anomalous behavior difficult. Traditional approaches, such as honeypots, are unlikely to scale to the diversity needed by IoT. Finally, each IoT device is likely to need a customized set of rules and this security must be enforced on all communication to the device (i.e. not just traffic through a firewall to external domains) and this enforcement should add little overhead or latency. While each part of this redesign is challenging, we believe that we can leverage a number of ideas from existing research areas, such as crowdsourcing, edge cloud computing, SDN, NFV, as a first step towards solving some of these challenges.

Testbed. A core goal of this work is to understand the types of policies, defenses and learning needed for IoT. This depends heavily on how IoT devices are used in practice by real users and applications. A city-scale testbed with actual IoT components and real users would provide valuable insight for our design and provide a desirable evaluation testbed for our system.

Brief Bio: Srini Seshan has a long history of working on various topics in wireless networking and mobile computing. This includes highly cited and award winning work developing; 1) routing and transport protocols for wireless links [Mobicom 1995], 2) privacy mechanisms for wireless links [Mobisys 2008], 3) efficient aggregate query protocols for wireless sensor networks [Sensys 2004], 4) characterization of chaotic wireless deployments [Mobicom 2005], 5) protocols for indoor directional antenna [Sigcomm 2009], 6) implementation techniques for software-defined radio MAC protocols [NSDI 2009]. He has also served as program committee chair for Mobisys and served on the Mobicom and Mobisys program committees numerous times.