Security in the Internet of Things: How to Patch Disposable Items
Shing Han-Chin, Khanh Nguyen, Kristine Rogers

The decreasing size of computer processors has created an opportunity to add a technological component to everyday things. Lightbulbs, water filters, and refrigerators are just a few of the many items that are receiving a wireless makeover in the “Internet of Things” (IoT). Juniper Research estimated that 13.4 billion IoT devices existed as of 2015; this number is expected to grow to more than 38 billion devices in 2020 [1]. As with many inventions, the creators of these new wireless-enabled devices tend to focus first on what is possible, and later look at issues like device security. What are the security implications of introducing small, disposable, Internet-connected products that are intended to last only a short period of time?

Summary
The focus of this research project is to evaluate security in the IoT—specifically, looking at Internet-connected items that could be considered “disposable”—in other words, they are designed to be used for a short duration (for instance, less than one year). Developers might be thinking through the security attached to a larger Internet-connected appliance, such as a refrigerator, but what about something that is only intended for a few months of use? Do companies think of computer security for throwaway devices as cost prohibitive?

Our research team proposes a research effort with three phases: first, we will perform a survey of existing “disposable” IoT products, to understand their security and logging capabilities. Second, we will compare these with existing computer security research, to determine whether these devices introduce types of threats or vulnerabilities that did not exist with other types of Internet-connected devices. Finally, we will identify methods and approaches for patching these devices—or protecting against vulnerabilities they create.

Intellectual Merit
The security of IoT devices remains an emerging area for research. While there has been some research on the security and privacy implications of adding connectivity to certain devices, we see a need for further research into disposable IoT devices, to ensure that they do not introduce new types of vulnerabilities to consumers.

Broader Impact
We believe this will lead to a new branch of research within the IoT community, and generate discussion on broader security approaches in the IoT. Longer term, this effort will result in scalable patching capabilities that companies can more easily apply to disposable devices before they hit the market.

Time and Cost
We believe this project will take 3 years to complete, with six graduate students. The estimated costs for this project will be $200,000 per year. The costs of this project include the purchase of Internet-connected disposable devices, computer equipment to test the log output and other security features of the devices, and data analysis capabilities. Additional costs include salaries of participants during the course of this project.
References