H4kRT0yz: Hacking Home IoT Devices
Era Vuksani
Carnegie Mellon University, Information Networking Institute

The presence of IoT devices in the home is booming. Just between 2016 and 2017 alone, the number of home IoT devices has more than doubled from 31.2 million devices to 82.7 million devices¹. IoT devices are already present in many areas of the home. Smart locks, cameras, and security systems provide home security. Appliances are outfitted with screens and sensors that give information to users and can be remotely controlled. Children’s toys and baby monitors have cameras and microphones for parents to interact with their kids.

With the influx of IoT devices, security has taken a back seat. Vendors initially have little incentive to provide security on their devices. Consumers typically have little to no understanding of security. As such, they may unwittingly purchase devices that expose their homes’ privacy. With more IoT devices being introduced in houses, the boundary between a home’s privacy and security, and the outside world begins to break down.

Our poster focuses on finding vulnerabilities in household IoT devices. It describes our process of finding these vulnerabilities and our attempts at hacking three IoT devices: the Geeni Lux 800 Smart Light Bulb, the iBaby Monitor M6S, and the Swift Robo Buddy.

-----


(feel free to remove the reference if deemed unnecessary)