Security Vulnerabilities in Children's Toys

Ali Ahmed
Dakota State University
Ali.Ahmed@trojans.dsu.edu

Ashley Podhradsky
Dakota State University
Ashley.Podhradsky@dsu.edu

Abstract

The internet of things has advanced the way people communicate with devices, other people, our appliances and even children's toys. The "smart" movement has impacted phones, homes, cars, now toys. Children toys are becoming "smart" and with the integration of technology toy manufacturing companies are incorporating Wi-Fi, cameras, radio-frequencies and other communication devices in the toys. This has created a security vulnerability for children as well as for parents. There is a need for children, parents and toy manufacturers to understand the potential cyber threats associated with these high-tech "smart" toys. In this study, we have analyzed the available toys which can have potential cyber security vulnerabilities. These toys include, Mattel's Hello Barbie Doll, VTech Learning Tablet and Smart Watch, Smart Toy Bear from Fisher – Price, I-Que Intelligent Robot and long range Walkie-Talkies. We have reviewed the available literature on the topic and currently testing these toys in a security lab under various scenarios. We would like to get feedback on our research idea, get suggestions on methodology to conduct this research and what future research areas we can explore under this topic. In short, the purpose of this presentation is to present our research idea, gain feedback from other researchers and create awareness on security vulnerabilities in children toys.