VULNERABILITY TRENDS IN IOT DEVICES AND NEW SENSOR-ASSISTED SECURITY PROTECTIONS

Junia da Rocha Valente, PhD
The University of Texas at Dallas, 2018

Supervising Professor: Alvaro A. Cardenas, Chair

Internet of Things (IoT) devices are found everywhere: in our houses as voice-assistant devices, home automation smart devices, or smart appliances. As our lives become more dependent on these systems, their security has become an important growing concern. To systematically study the security and privacy issues in IoT devices, we obtained over 40 IoT devices in our Cyber-Physical Systems Security Laboratory at UTD. These devices represent a wide range of consumer products including smart children toys, consumer drones, surveillance systems, smart home devices, and voice-enabled personal assistant devices.

The first part of the dissertation summarizes security and privacy practices in these devices, deployment patterns that emerge among them, and vulnerabilities we found on them including: (1) encryption problems on smart toys; (2) filesystem misconfigurations on consumer drones; and (3) hard-coded passwords on network video recorders (NVR) firmware. We show that voice-enabled toys–targeting young children–pose new unanticipated threats. An attacker can inject malicious voice content and insult or ask young children to do unsafe things. Also, an attacker can obtain private-sensitive data (when the toy is lost or resold). Further, we tested a variety of attacks in a new family of drones (U818A) released in 2016. We conclude our discussions with considerations that vendors should take when designing their products. We also share our experience in reporting the security vulnerabilities to

CERT/CC and to affected vendors following a responsible disclosure approach. Our contributions include vulnerability disclosures published at the National Vulnerability Database (NVD) maintained by NIST: CVE-2015-8287 (on Swann NVW-470 surveillance systems); CVE-2017-3209 (on Discovery U818A consumer drones); and CVE-2017-8865, CVE-2017-8866, and CVE-2017-8867 (on CogniToys Dino smart toys).

The second part of the dissertation focuses on how IoT devices can be secured by fundamentally new security paradigms. In particular, we focus on the security of camera surveillance systems and propose a new way to verify the integrity and freshness of the video feed by sending visual challenges to the area the camera monitors. Our work illustrates the unique cyber-physical properties that sensor devices can leverage in their cyber-security defenses. At a high-level, our research is motivated by attestation and challenge-response protocols. While these traditional mechanisms exchange digital challenges between devices authenticating each other, our work instead proposes challenges that manifest physically in the field-of-view of the device. Our physical (visual challenge) and cyber (verification) mechanism can help protect systems even when the sensors (cameras) and actuators (digital signage displaying physical challenges or multi-color light bulbs that change the environment lighting color) are compromised. Our implementation results show that visual challenges are an effective method to add defense-in-depth mechanisms to improve the trustworthiness of security cameras deployed in sensitive settings.