Abstract

Internet-of-Things (IoT) Security Threats: Attacks on Communication Interface

by

Mohammad Mezanur Rahman Monjur

University of New Hampshire

Internet of Things (IoT) devices collect and process information from remote places and have significantly increased the productivity of distributed systems or individuals. Due to the limited budget on power consumption, IoT devices typically do not include security features such as advanced data encryption and device authentication. In general, the hardware components deployed in IoT devices are not from high end markets. As a result, the integrity and security assurance of most IoT devices are questionable. For example, adversary can implement a Hardware Trojan (HT) in the fabrication process for the IoT hardware devices to cause information leak or malfunctions. In this work, we investigate the security threats on IoT with a special emphasis on the attacks that aim for compromising the communication interface between IoT devices and their main processing host. First, we analyze the security threats on low-energy smart light bulbs, and then we exploit the limitation of Bluetooth protocols to monitor the unencrypted data packet from the air-gapped network. Second, we examine the security vulnerabilities of single-wire serial communication protocol used in data exchange between a sensor and a microcontroller. Third, we implement a Man-in-the-Middle (MITM) attack on a master-slave communication protocol adopted in Inter-integrated Circuit (I^2C) interface. Our MITM attack is executed by an analog hardware Trojan, which crosses the boundary between digital and analog worlds. Furthermore, an obfuscated Trojan detection method