Investigating Security Attacks on Wireless Sensor Networks (WSNs) via an IoT Environmental Monitoring System

Internet of Things (IoT) has become a popular subject in the technology industry and will soon reach the popularity level of smartphones. One common branch of IoT is the notion of Wireless Sensor Networks (WSN). In our research, we focus on evaluating and improving the current security posture of a WSN environment. Many applications currently use Wireless Sensor Networks to collect and analyze data for monitoring purposes. In our work, we use an environmental monitoring system as our application, where sensor nodes are deployed to monitor certain parameters such as temperature and humidity. Due to nature of WSN applications, these sensor nodes are vulnerable to node capture attacks. We perform an attack on a WSN environment by capturing one of the nodes, hacking into that node and reverse engineering binary data found in the capture node. We also present a security flaw discovered on the password-protected firmware found in MSP430 microcontrollers. We demo that these password-protected firmware can still be read and downloaded to a computer by brute forcing methodologies. Moreover, these binaries can be reverse engineered to find secret information such as encryption/authentication keys that can be used to get into a WSN system.

To demonstrate our work, we have implemented a secure temperature monitoring system that makes use of the IEEE 802.15.4 standard, AES-128 hardware encryption and TelosB sensor nodes. In our design, we consider one of the nodes to be a coordinator node, which plays the role of a central node that establishes network association requests, listens for incoming packets, decrypts the incoming packets and forwards any received packets to the monitoring device. Three other nodes act as end-devices, which play the role of collecting temperature measurements, encrypting the collected data and sending the encrypted packets to the coordinator node. A last one acts as packet sniffer, which plays the role of listening to packets sent over the network and forwarding the capture packets to Wireshark. We study the security used in WSNs and perform hacking scenarios on our environmental monitoring system.

Our preliminary results show that the passwords used to protect the firmware found in sensor nodes are not random. The 32 bytes passwords are not unique and are predictable because the password used is the same as the interrupt vector table. We measure the time needed to perform an attack on a WSN environment and we study the overhead of our solution to randomize the password used to protect firmware. Our contributions prevent future attackers from obtaining a copy of firmware found in these sensor nodes and ultimately overall protect WSN environments.

Keywords: Wireless Sensor Networks (WSN), Internet of Things (IoT), Security Measurement, Encryption, Hacking, Reserve Engineering