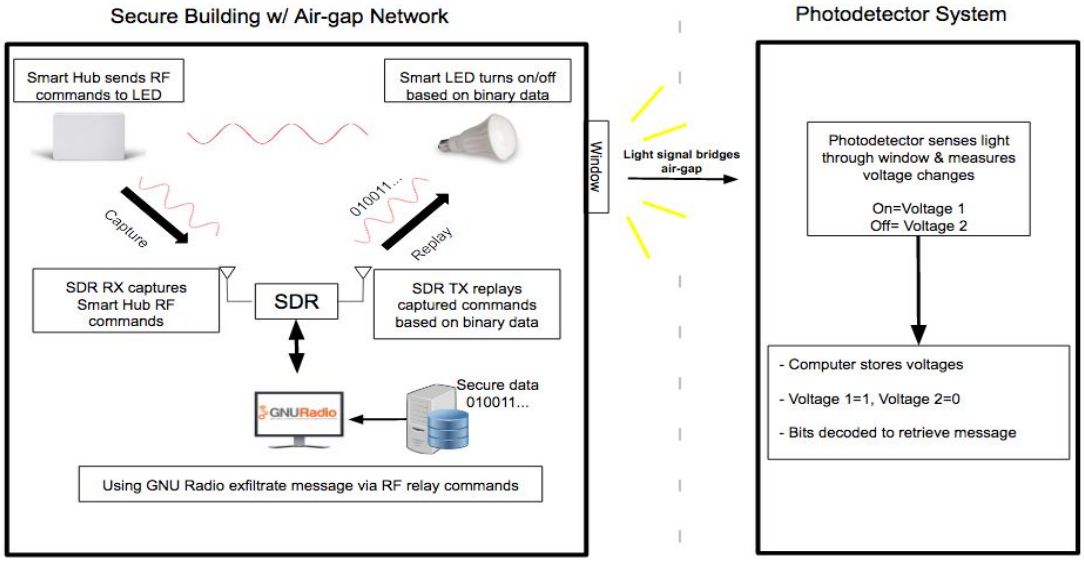
Data Exfiltration using Building Automation to Bridge Air Gapped System

Marcial Tienteu, Asia Mason, Michael Talley, Tellrell White, Edmund Ahovi, Denzel Hamilton,
Dr. Kevin Kornegay, Dr. Michel Reece, and Dr. Willie Thompson
Department of Electrical and Computer Engineering, Morgan State University

The Internet of Things (IoT) has a major impact on our daily lives. Building automation is very popular IoT application. Recently, there have been several exploits on home/building automation devices used in a secured facility that take advantage of implementation flaws in the communication protocols [1, 2]. This hardware demo will display a replay attack on a building automation system in order to transmit secure data across an airgap system. This demonstration will identify vulnerabilities in building automation systems that use the 802.15.4/ZigBee protocol and provide a countermeasure to combat the problem. The full setup for this hardware demo, as seen in the figure below, includes a commercial ZigBee Hub, an LED controller, a software defined radio (SDR), and a photodetector system.

In a typical building automation system, a Hub receives instructions from a router and then sends a command via RF link to a smart device for execution. For this hardware demo, the command sent from the Hub to an LED controller will be captured using an SDR to identify which commands control the light. Next, GNU Radio interface will be used to exfiltrate secure data in binary form via RF relay commands. The SDR transmitter then replays the captured RF commands based on the binary data switching the LED between on and off states. The light signal is sensed through a window by a photodetector, thus bridging the air gap allowing secure data to escape. The photodetector system measures voltage changes from the light switching between on and off states and converts the information back to the secure data. At the output of the system, the audience will see the actual secure data that was transmitted by modulating the LED.



References

[1] T. Zilner, “ZigBee Exploited: The good, the bad and the ugly,” Black Hat USA 2015, pp. 1-8, Las Vegas, Nevada, Aug. 2015

[2] S. Gupta, “Experimental Security Analyses of Non-networked Compact Fluorescent Lamps: A Case Study of Home Automation Security,” Proc. Learning from Authoritative Security Experiment Results, pp. 1-14, Arlington, Virginia, Oct. 2013