The Internet of Things (IoT) extends internet connectivity to a wide range of everyday things and devices. Home automation is an IoT application area that uses sensors for data collection and protocols like Z-Wave for communication. Extensive research on Z-Wave IoT device security at application, network and perception layers reveals that Z-Wave IoT device manufacturers[3]:

1. Do not implement enough security features leaving devices vulnerable at each of the above layers.
2. Count on the security provided by the home wireless routers [4].

Successful application and network layer attacks have been demonstrated by several researchers which include exploiting both secure and unsecure Z-Wave devices [1]. Although the attack vectors remain similar, attackers have used newer techniques each time to launch the same attacks [2]. We use Z-Wave development tools including development boards to spoof the home automation network and launch attacks by exploiting vulnerabilities.

As a part of our demo, a Z-Wave home automation test bed has been created that includes a hub, thermostat, smoke detector, door lock and security alarm, garage door lock and smart plug. The home automation test bed presents numerous attack vectors and allows for attacks such as data sniffing and packet extraction attacks by using device credentials, monitoring of specific device traffic, scanning for new vulnerabilities, as well, as launching a variety of Denial of Service (DoS) attacks.

'Zniffer' along with the dongle is a smart Z-Wave network analysis tool and can be used to engage in unauthorized network reconnaissance for up to several meters of radius. Network data is reliably sniffed, data packets can be extracted and read. Software is written and programmed into the development board which acts as a malicious device to spoof the home automation network and launch DoS attacks on both secure and unsecure devices.

In this demo, we will spoof the home automation test bed using software and hardware development tools to launch a DoS attack on secure and unsecure home automation IoT devices such as the smoke detector and security alarm. The steps and equipment used for the demo are presented in the figure below. The observables include the following:

- Spoofing Z-Wave Home Automation network
- DoS attack on Z-Wave switch, thermostat, smoke detector and security alarm
- DoS attack on Z-Wave door lock

References

[1] ABehrang, Fouladi ; Ghanoun , Sahand;. (2013). Security Evaluation of the Z-wave Wireless Protocol. *ShmooCon.* UK: Sensepost.

[2] Fuller, J. D., & Ramsey, B. W. (2015). Rogue Z-Wave Controllers: Peristent attack channel. *Local Computer Networks Conference Workshops.* IEEE.

[3] R. Mahmoud, T. Yousuf, F. Aloul and I. Zualkernan , "Internet of Things (IoT) Security:Current Status, Challenges and Prospective Measures," in *Internet Technology and Secured Transactions (ICITST)*, London,UK, 2015

[4] S. Demetriou, N. Zhang, Y. Lee, X. Wang, C. Gunter, X. Zhou and M. Grace, "Guardian of the HAN: Thwarting Mobile Attacks, on Smart-Home Devices Using OS-level Situation Awareness","Cornell University Library," 2017. [Online]. Available: https://arxiv.org/. [Accessed 6 10 2017].

[5] Knight, M. (2006, Dec-Jan). How safe is Z-wave ? *Computing & Control Engineering Journal, 17*(6), 18-23. Retrieved 12 15, 2016, from http://ieeexplore.ieee.org/document/4105852/?reload=true

DOS ATTACK FLOW ON Z-WAVE HOME AUTOMATION SYSTEM