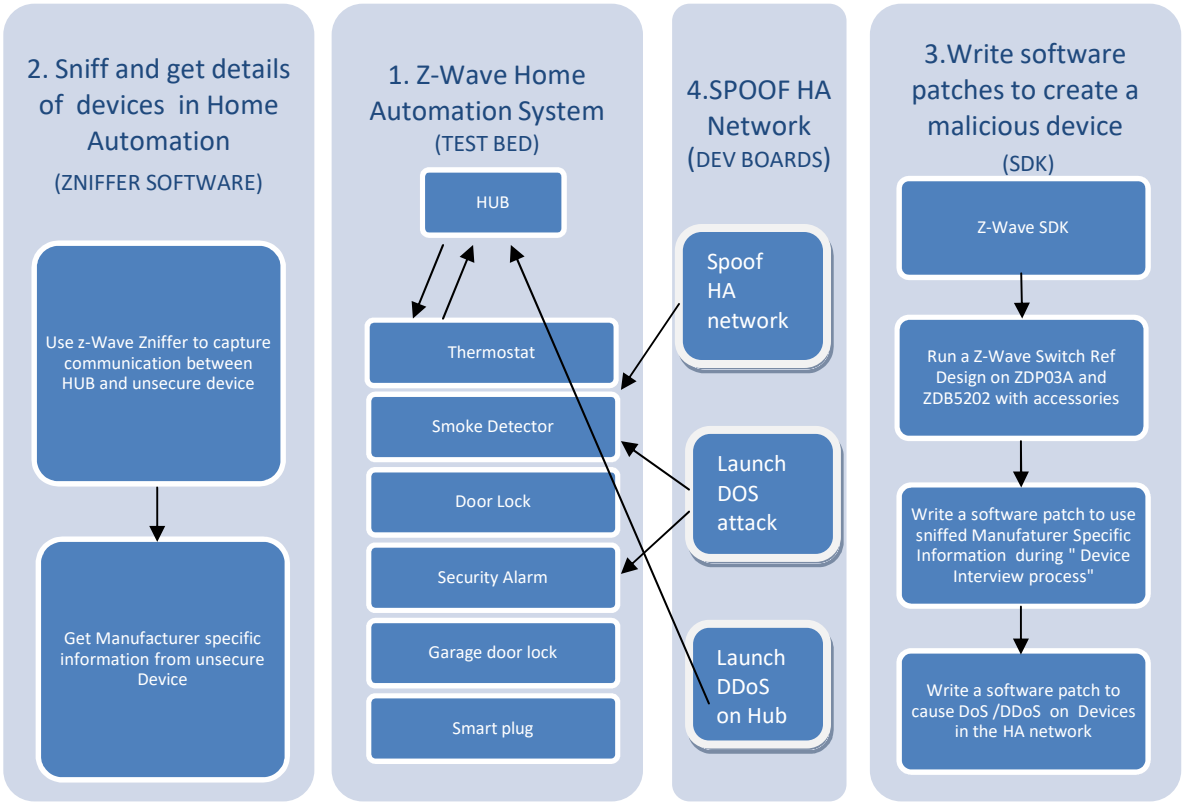
Authors: Latha Suryavanshi Mahadeva Rao, Khir Henderson, Tsion Yimer, Aaron Edmund,
Dr. Kevin Kornegay, Dr. Jumoke Ladeji-Osias
Affiliation: ECE Department, Morgan State University, Baltimore, MD United States

Home automation is an IoT application area that uses sensors for data collection and protocols like Zigbee and/or Z-Wave for communication. The proliferation of Z-Wave devices poses information security challenges such as a hacked z-wave door lock, due to a protocol implementation error [1]. To support our IoT device vulnerability research, a Z-Wave home automation test bed has been created that includes a Z-Wave controller (HUB), thermostat, smoke detector, door lock and security alarm, garage door lock and smart plug. The home automation test bed presents a great demonstration platform for attacks. For the hardware demo, we propose to spoof a commercial home automation system using Z-Wave development boards and associated software, launch a DoS attack on the unsecure devices like smoke detector and security alarm. A DDoS attack will be performed on the controller. Malicious software patches are written and programmed into the development board which spoofs the home automation system. The steps and equipment used for the demo are presented in the figure below. The observables for the demonstraton include the following:

- Spoofing Z-wave Home Automation network
- DoS attack on smoke detector and security alarm
- DDoS attack on the Z-Wave controller using unsecure Z-wave devices



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] 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