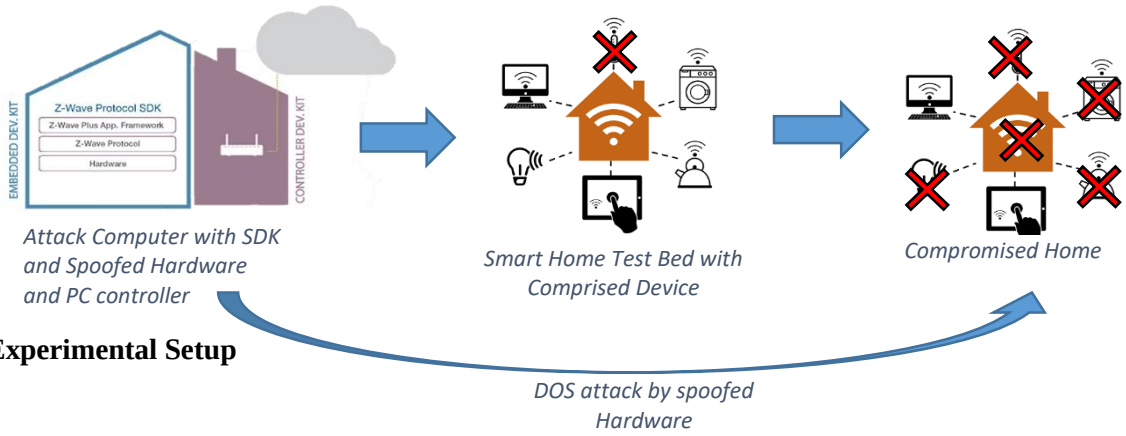
# Hardware Demo: Hacking Z-Wave using Insider Tools

Aaron Edmond [3], Khir Henderson [1], Latha Suryavanshi [1], Tsion Yimer [2]

*Morgan State University, Baltimore, Maryland,*
*Department of Electrical and Computer Engineering, [1] D. Eng. ,[2] M.S., [3] B.S.*

## Proposal

This hardware demonstration will display vulnerabilities through an attack on the Z-Wave communication protocol in a smart home environment using insider proprietary tools. This attack scenario "flips the script" and exposes new vulnerabilities and openings that aren't available using open source tools. This demonstration is from the stand point of a malicious person either with stolen credentials or insider information that is given license access to exclusive proprietary tools, protocols, and processes. The use of inside development tools makes these attacks faster, more reliable and generally easier. Wireless attacks such as; man in the middle, packet injection, spoofing, evil twin attacks, denial-of-service, data sniffing and extraction are all possible. This hardware demonstration results in a complete denial-of-service attack on a Z-Wave smart home network. Beginning on a prebuilt smart home testbed consisting of commercial Z-wave devices; a hub, smart thermostat, garage door opener, motion detector, and motion sensor. A computer using proprietary commercial software IDE's and hardware with restricted license access will scan the network for insecure and vulnerable devices. Once a device is found, the specific manufacturing information and ID are used to spoof and impersonate the already established device circumventing any security protocols and connecting to the Z-Wave hub. A software patch is written for the spoofed device to overload the hub with instructions denying service and proper function of the smart home.




## Experimental Setup

The observable demonstration will provide a pre-configured computer, along with Zniffer and PC controller dongles, and ZDP03A embedded development platform. On a monitor, reviewers will be able to see the program code, as well as the software used to view packet information, and write to the embedded system. Lastly the reviewer can test the functionality of the home network with a mobile phone connected to the IRIS Hub that is used to control the system.

## References

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

[2] Series G: Transmission Systems and Media, Digital Systems and Networks, ITU-T G.9959, 2012.

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