FLORIDA TECH
FLORIDA'S STEM UNIVERSITY™

Department of Computer Science

CSE 4820: Wireless and Mobile Security

17. Z-Wave Security

Dr. Abdullah Aydeger
Location: Harris Inst #310
Email: aaydeger@fit.edu

Outline

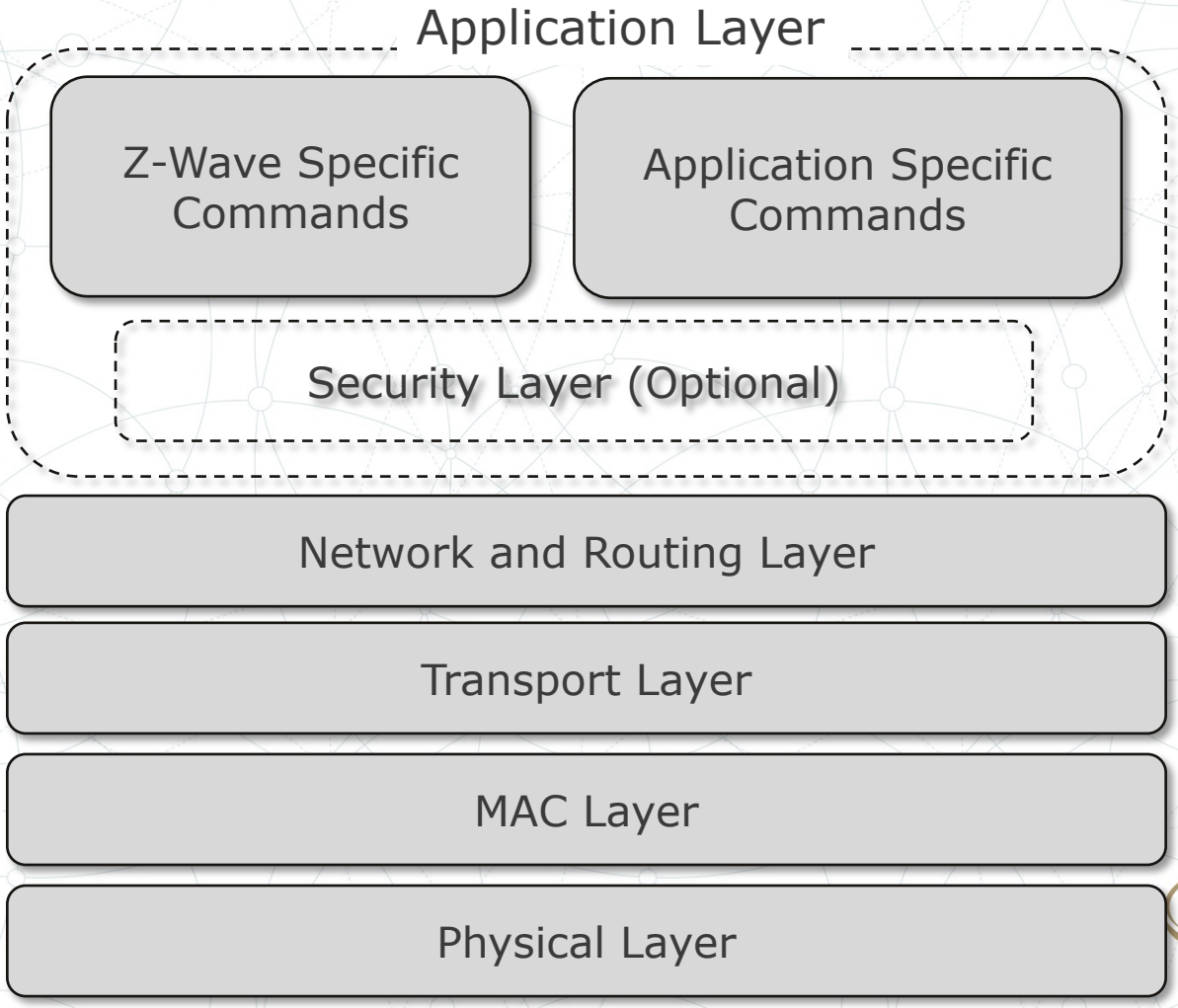
Z-wave Security

Recall: Z-Wave

- Low-energy, mesh-networking protocol
- Predominately used in home automation (locks, garage door openers, thermostats)
  - Over 100 million products in use in homes
- Proprietary design by Sigma Systems and governed by standards established by Z-Wave Alliance
  - Does not share details of protocol outside of NDA (nondisclosure agreement)
  - Controls all fabrication and delivery of Z-Wave chips to product manufacturers

Recall: Z-Wave Protocol Stack

- Uses structured protocol stack

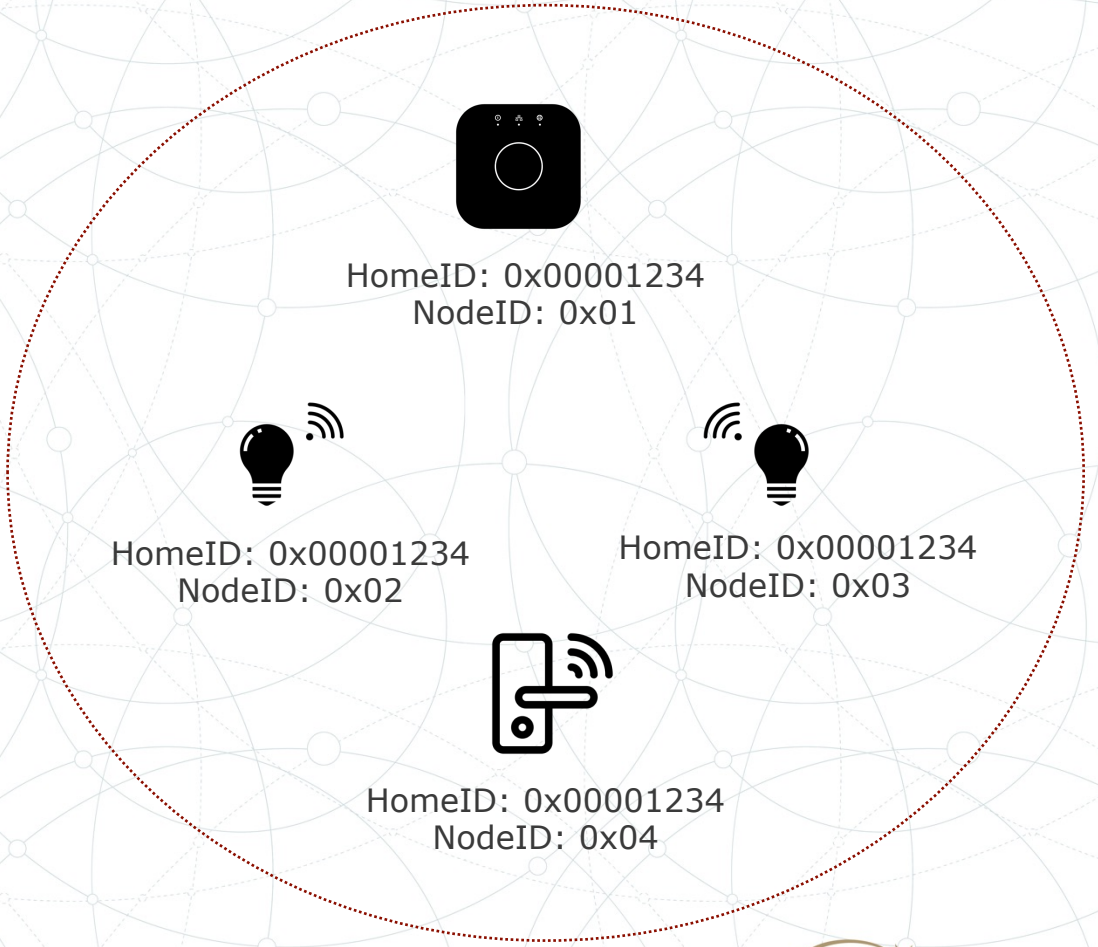


Recall: Z-Wave Network Layer: Inclusion

- Involves configuring the controller in inclusion mode (allowing it to accept new nodes) by pressing a physical button or choosing a menu item, and pressing a button on the new node to initiate an inclusion exchange
- When the new node initiates the inclusion process, it sends a Z-Wave node information frame using homeID of 0x00000000 and nodeID of 0x00 and a brodcast dest NodeID
  - Discloses the capabilities of the new device to the controller, which, in turn, allocates a NodeID to the new device for subsequent use on the network and updates routing tables to accommodate packet delivery to the new node

Z-Wave Network Topology

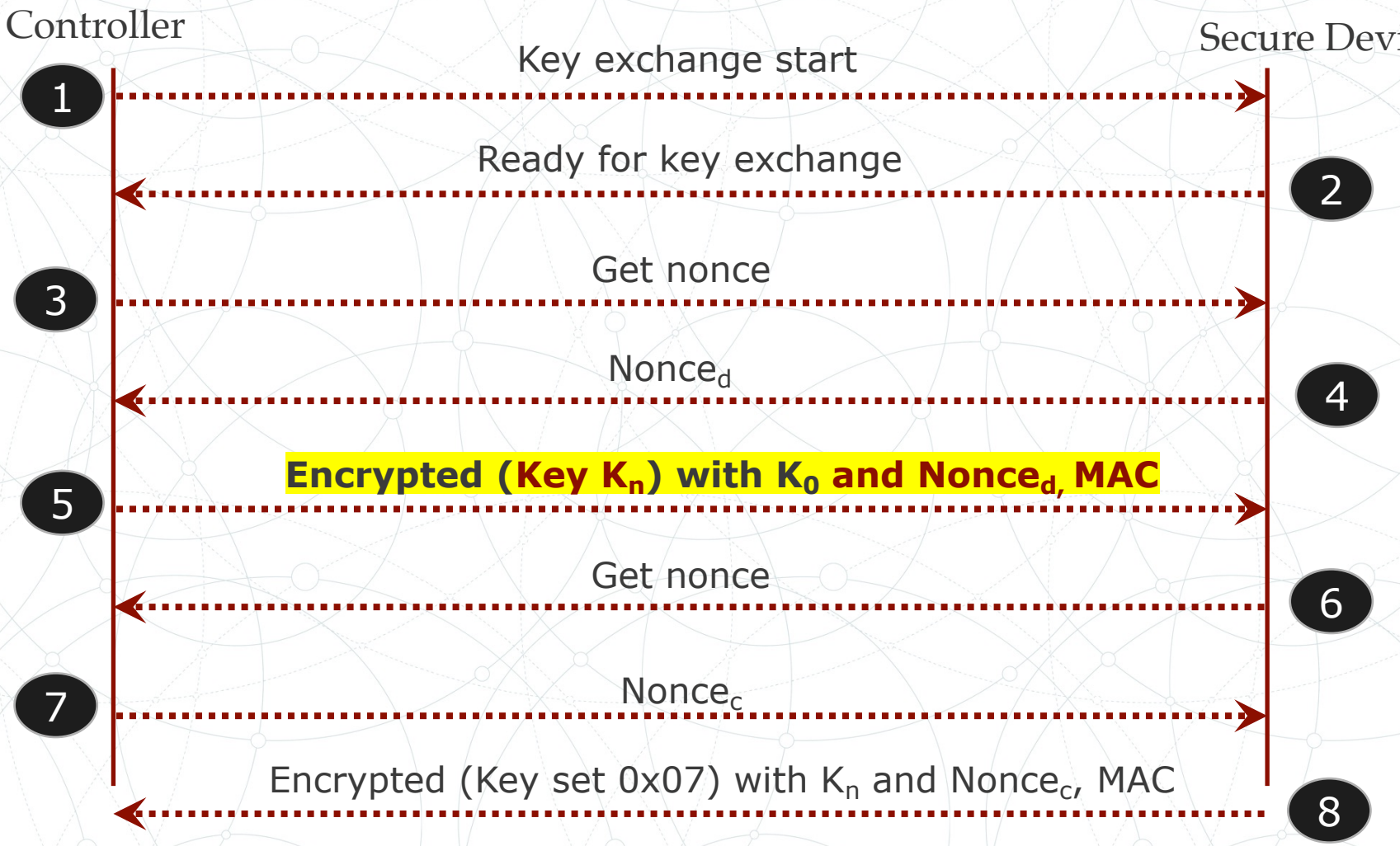
- Nodes in a Z-Wave have a 1-byte NodeID, which must be different than every other node in the network
- Nodes in a Z-Wave network have a 4-byte HomeID, assigned by the controller at the time of inclusion
- Nearby networks must have different HomeIDs



Recall: Z-Wave Security

- Uses AES-OFB (Output Feedback Mode) to provide data confidentiality on the network
  - Conserve the amount of payload content transmitted in Z-Wave frames while being NIST (National Institute of Standards and Technology) approved
- AES CBC-MAC (cipher block chaining message authentication code) for data integrity protection
- CLASS_SECURITY command; key exchange process to derive keys

Recall: Z-Wave Key Exchange Process



Temporal Key
$K_{0=}$ 16 bytes of 0x00

Network Key
$K_{n\ =}$ Chosen by controller

Recall: Z-Wave Key Exchange's Solution

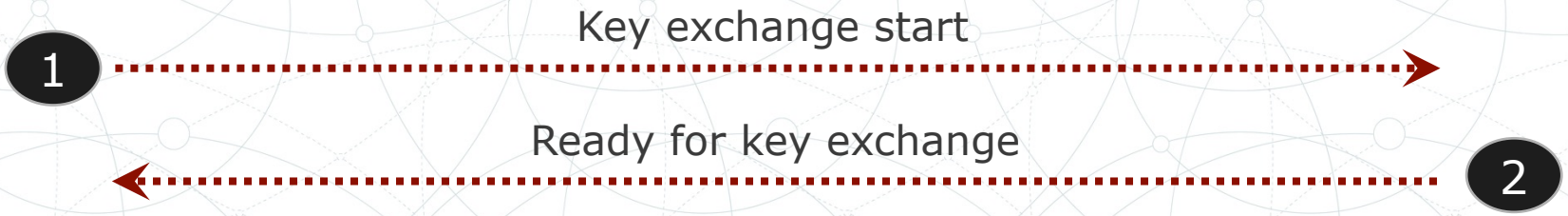
- Low power inclusion mode
  - Controller and secure device transmit using minimal power capabilities
  - Require no more than 3 feet apart to complete the process
  - Also infrequent practice of adding new devices
  - Results in less opportunity for the attacker

Z-Wave Key Derivation

- After the K_n (network key) is established, the device generates two additional keys K_c (packet encryption) and K_m (message auth key)
  - Kc (packet encryption) = AES-ECB_{kn}($Password_c$)
  - K_m (message auth key) = AES-ECB_{kn}($Password_m$)
- Where $Password_c$ and $Password_m$ are static values across all Z-Wave devices
- However, if we observe Kn and we know $Password_c$ and $Password_m$, we can compute the packet encryption and message auth keys

Z-Wave Key Establishment Attack

- We can force the key establishment process to establish a new K_n if we missed the original key establishment
  - Similar to an IEEE 802.11 Deauth

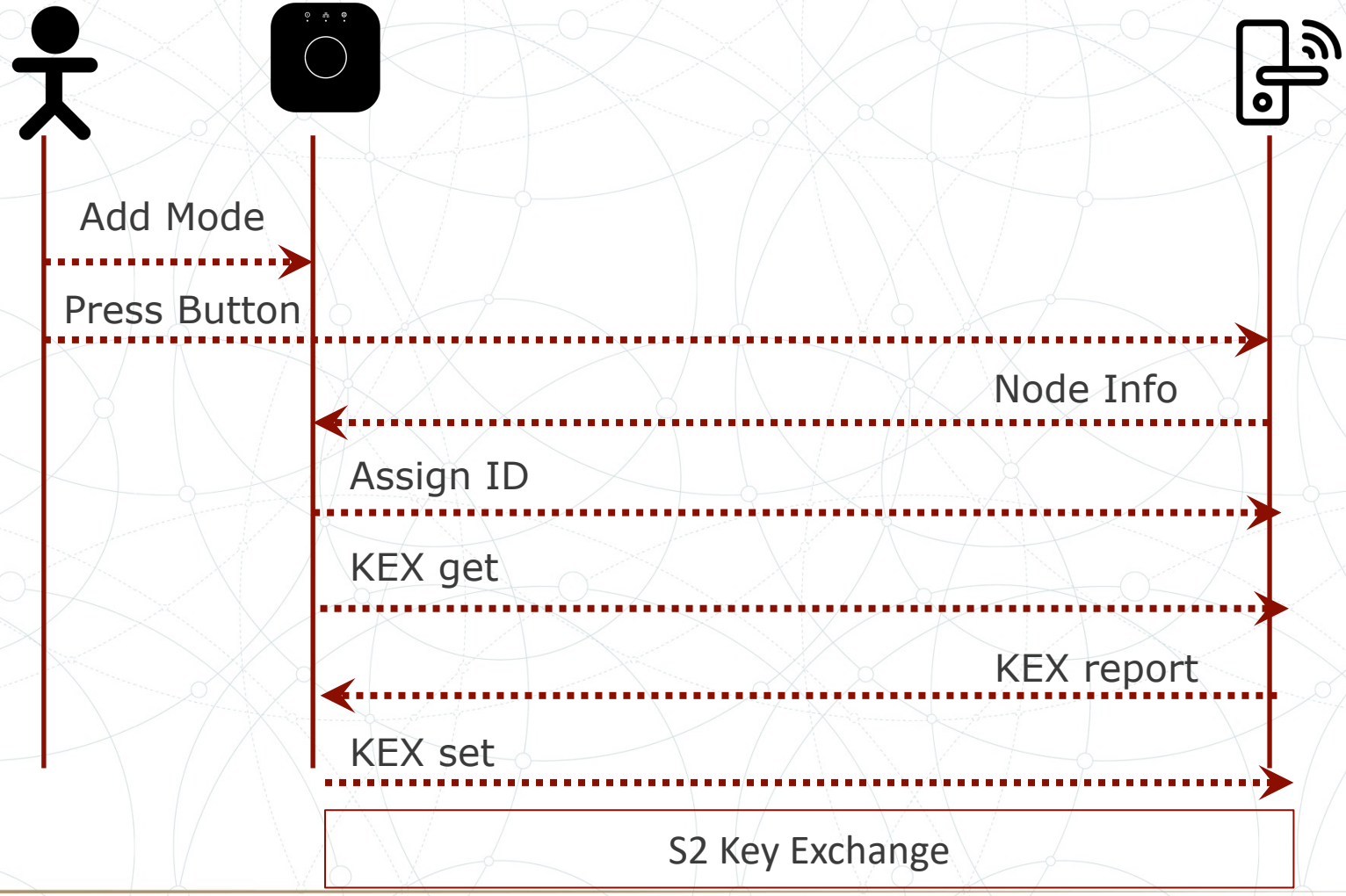


Z-Wave Key Establishment: Solution

- In response to the flawed S_0 Key Establishment and Pairing Process, SI Labs (i.e., Z-Wave Alliance) responded with a S_2 Key Establishment
- Removed the null temporal key
- Each devices has a DSK [device specific key] – 16 byte key
- Key exchanged using Diffie Hellman key exchange protocol
- Removed issues with man-in-the-middle
  - Are we safe now?

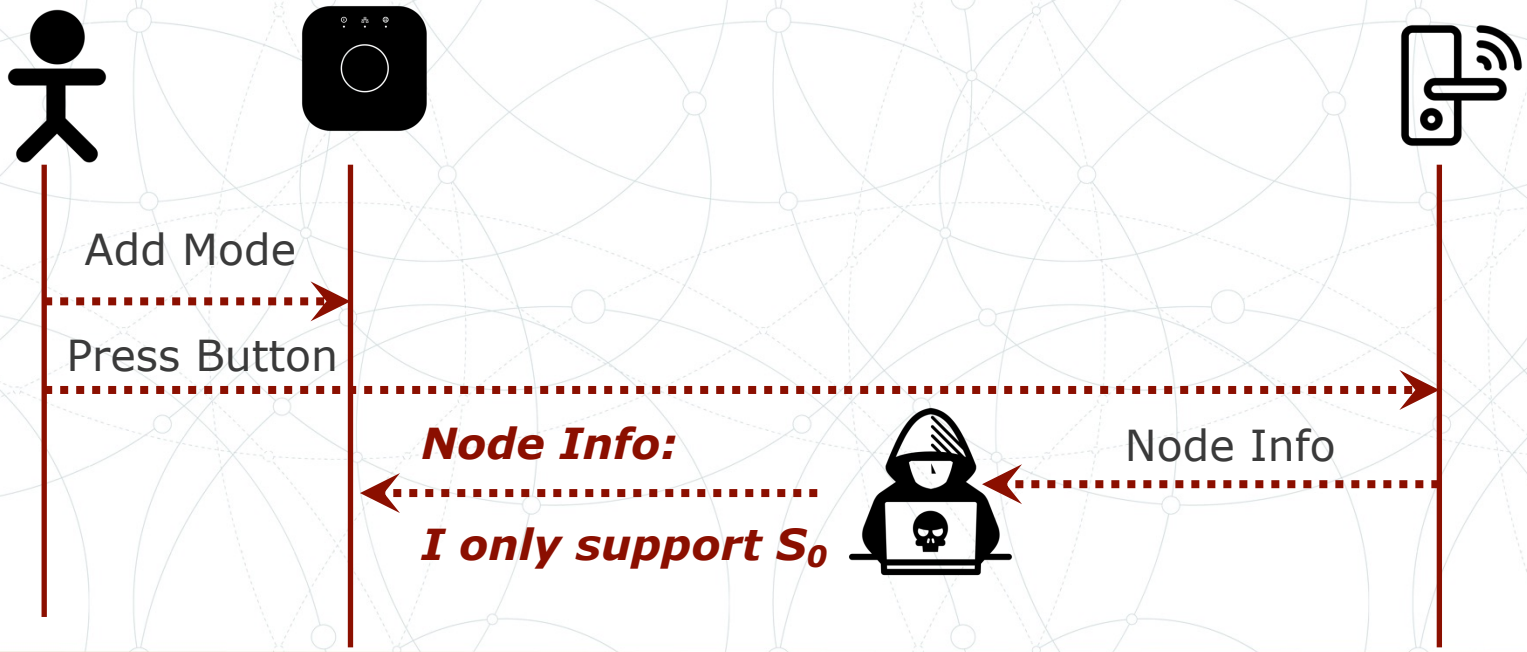
https://community.silabs.com/s/topic/0TO1M000000qHcQWAU/zwave?language=en_US&tabset-178da=2

Z-Wave Key Exchange



S2 Z-Wave Rollback Attack

- An attacker jams the node info or responds prior to the node
- Provides node info that device only supports flawed S_0 pairing mode



Mitigating Eavesdropping in Z-Wave

- As in any wireless technology, attacker can always capture the traffic (aka eavesdropping)
  - Useless if confidentiality and integrity of the data is ensured
- Unfortunately, the use of encryption in Z-Wave is optional
  - Switch to a vendor that offers network confidentiality and integrity control

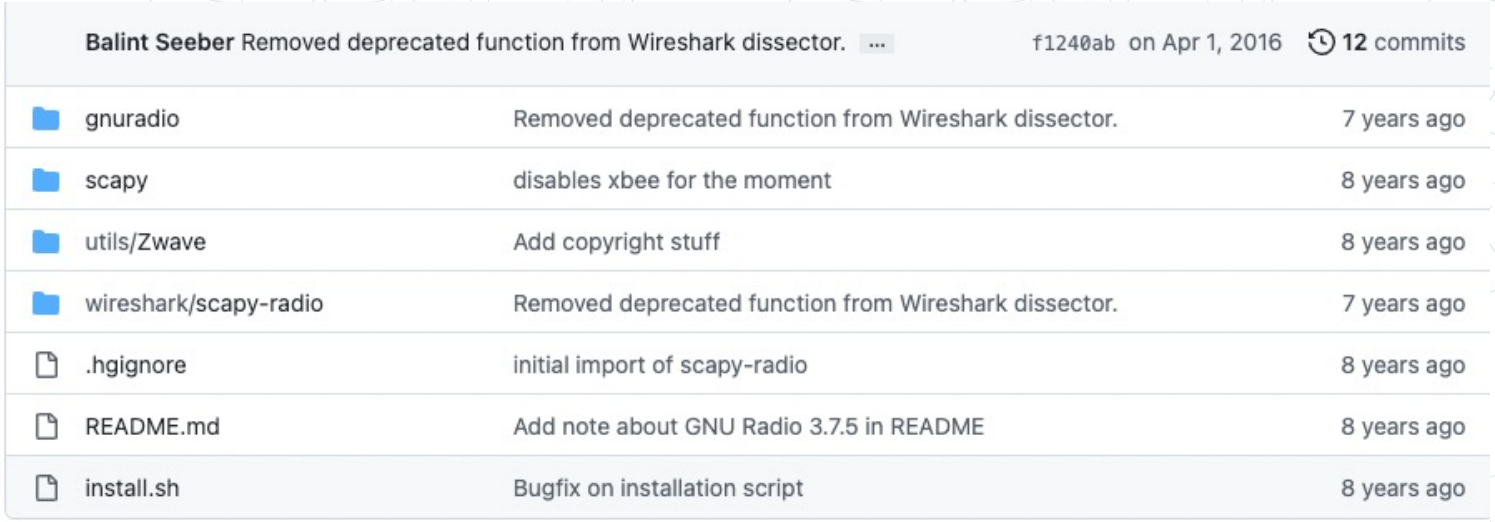
Injection Attacks in Z-Wave

- If no encryption, attacker can capture and replay the packets
- Injection is also done if the device is in the Z-Wave network
  - To be in the network, Z-Wave inclusion needed
    - Does it solve this problem?
  - Attacker can spoof the address and inject any packet

https://github.com/joswr1ght/killerzee

Scapy-Radio Framework

- Modified version of Scapy to support
  - Zwave
  - Zigbee
  - 802.15.4
- Works with software defined radios (SDR)



Balint Seeber Removed deprecated function from Wireshark dissector. ··· `f1240ab` on Apr 1, 2016 **12** commits

gnuradio	Removed deprecated function from Wireshark dissector.	7 years ago
scapy	disables xbee for the moment	8 years ago
utils/Zwave	Add copyright stuff	8 years ago
wireshark/scapy-radio	Removed deprecated function from Wireshark dissector.	7 years ago
.hgignore	initial import of scapy-radio	8 years ago
README.md	Add note about GNU Radio 3.7.5 in README	8 years ago
install.sh	Bugfix on installation script	8 years ago

README.md

Introduction

This tool is a modified version of scapy that aims at providing an quick and efficient pentest tool with RF capabilities.

It includes:

- A modified version of scapy that can leverage GNU Radio to handle a SDR card
- GNU Radio flow graphs (GRC files) we have build that allows full duplex communication
- GNU Radio blocks we have written to handle several protocols

FLORIDA TECH

FLORIDA'S STEM UNIVERSITY™

Thank you. Questions?

Dr. Abdullah Aydeger