FLORIDA TECH
FLORIDA'S STEM UNIVERSITY™

Department of Computer Science

CSE 4820: Wireless and Mobile Security

15. Zigbee Security

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

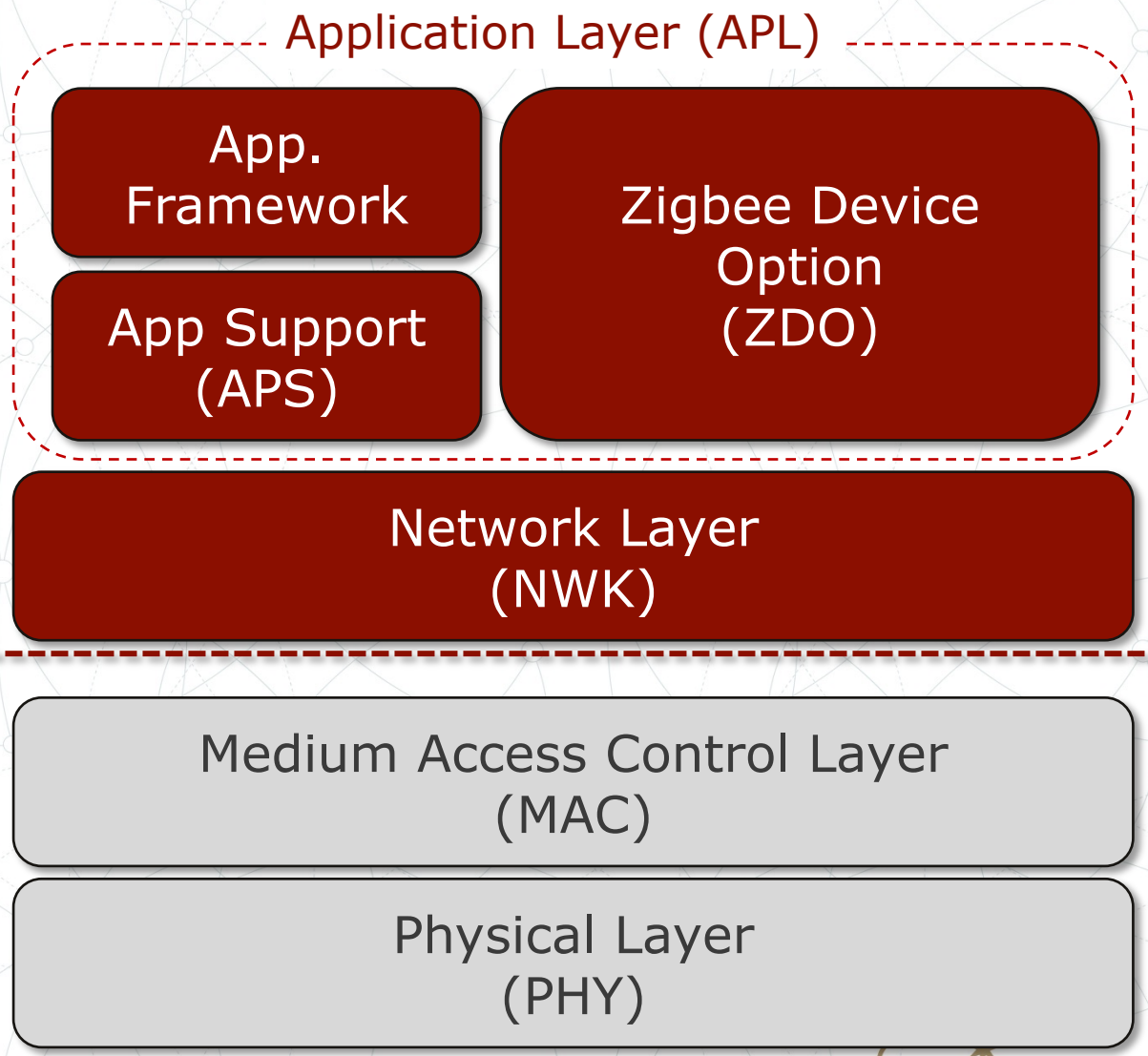
Outline

Attacking Zigbee

Recall: Zigbee Overview

Solution	Description
Network Protocol	Zigbee PRO 2015 (or newer)
Network Topology	Self-Forming, Self-Healing MESH
Network Device Types	Coordinator (routing capable), Router, End Device, Zigbee Green Power Device
Net. Size (theoretical # of nodes)	Up to 65,000
Radio Technology	IEEE 802.15.4-2011
Frequency Band / Channels	2.4 GHz (ISM band) 16-channels (2 MHz wide)
Data Rate	250 Kbits/sec
Security Models	Centralized (with Install Codes support) Distributed
Encryption Support	AES-128 at Network Layer AES-128 available at Application Layer
Communication Range (Avg)	Up to 300+ meters (line of sight) Up to 75-100 meter indoor
Low Power Support	Sleeping End Devices Zigbee Green Power Devices (energy harvesting)
Legacy Profile Support	Zigbee 3 devices can join legacy Zigbee profile networks. Legacy devices may join Zigbee 3 networks (based on network's security policy)
Logical device support	Each physical device may support up to 240 end-points (logical devices)

Recall: ZigBee Layers



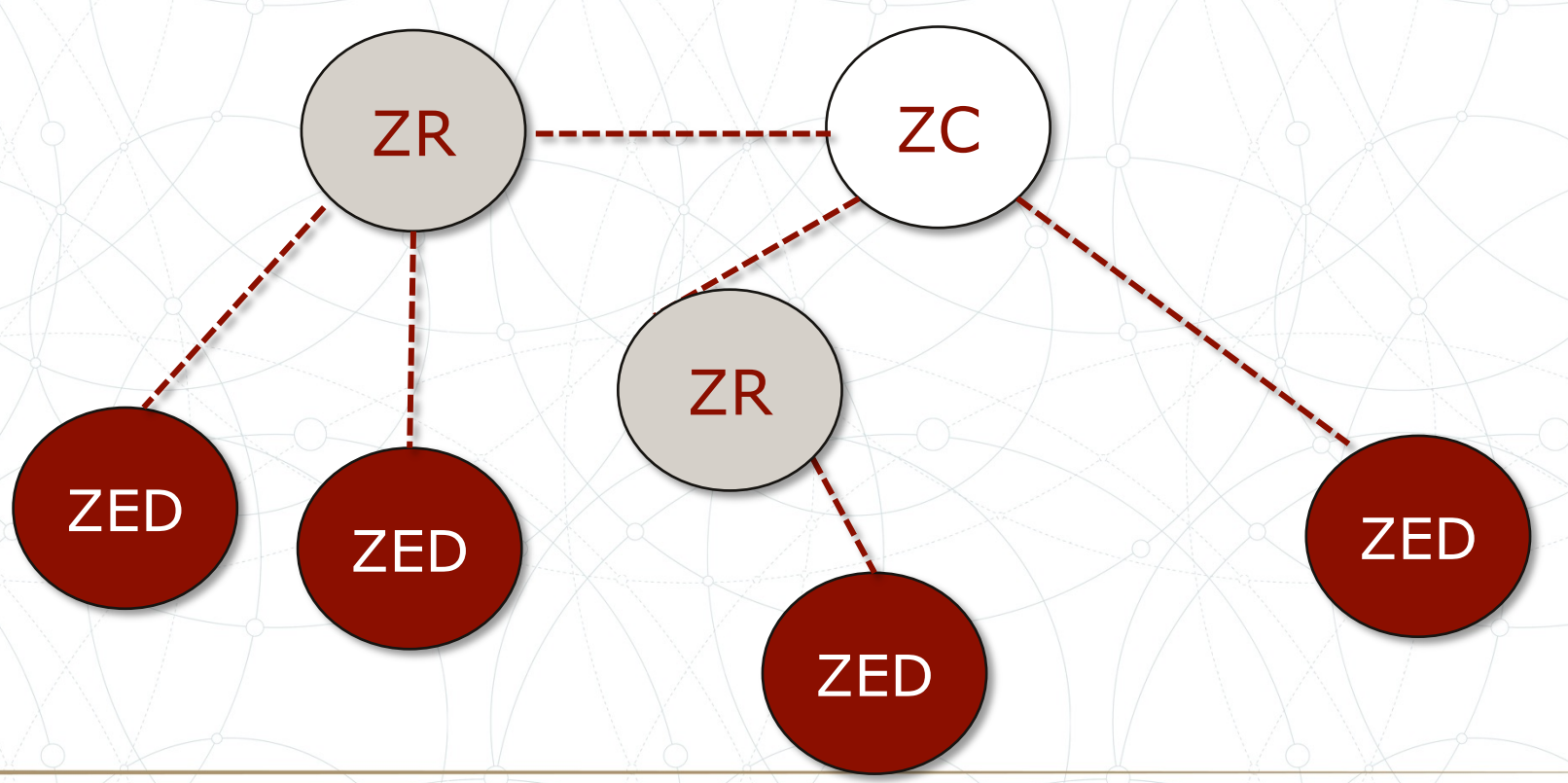
Defined by Zigbee Alliance

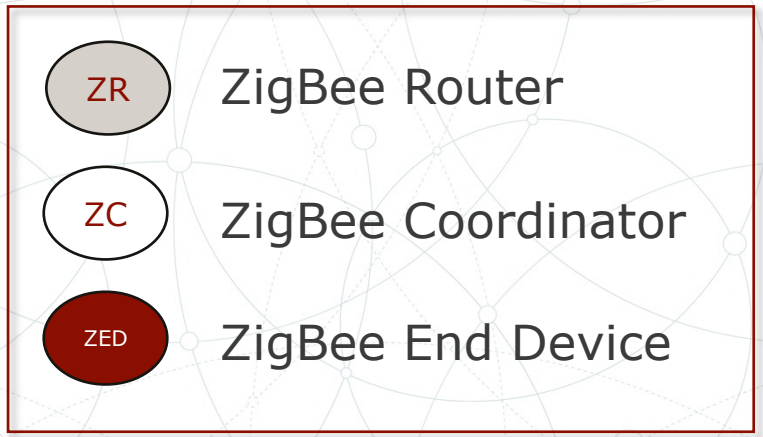
Defined in IEEE 802.15.4 (Low-rate wireless personal area network)

https://csa-iot.org/all-solutions/zigbee/

Recall: Example Zigbee Network

- One ZC for the network, additional ZRs



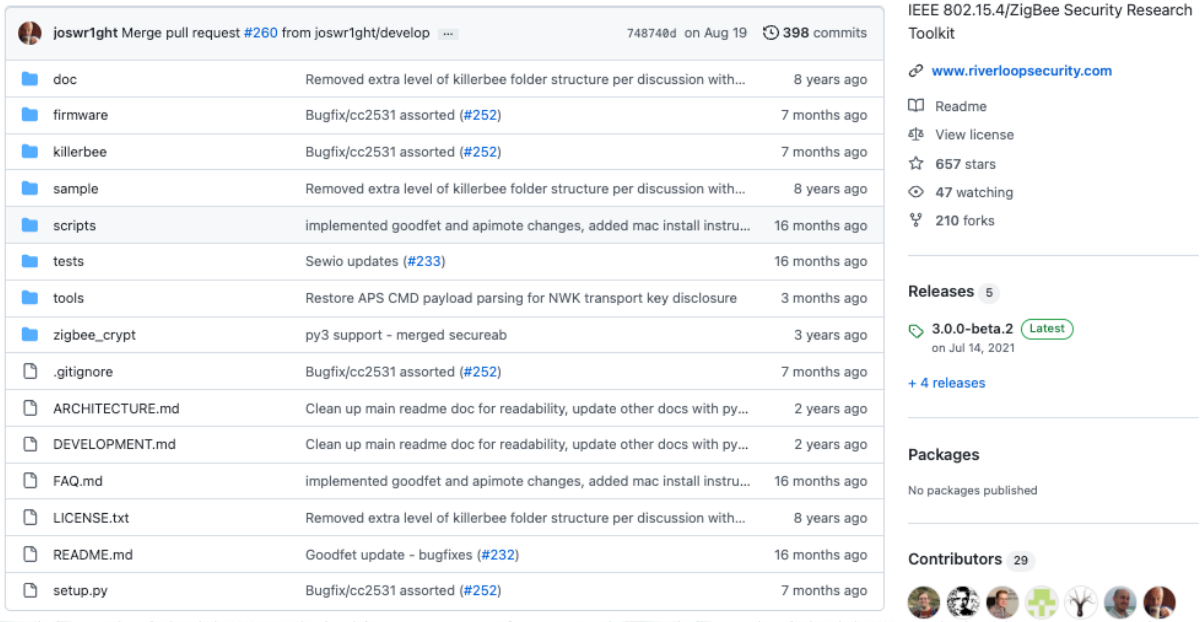


Recall: Zigbee: Key Provisioning

- Significant challenge; process of provisioning, rotating, and revoking keys on devices
- Zigbee Pro; Administrator can use the SKKE method to derive the network and link keys on devices
  - Requires devices to have master key provisioned on the TC and device joining the network

Recall: Zigbee Attacks

- KillerBee:
  - Python-based framework for manipulating and penetration testing Zigbee and IEEE 802.15.4 networks
  - Written and tested on Linux, free and open-source
  - Includes support for Scapy
  - Includes a variety of tools including zbwireshark, zbdump, and zbreplay



https://github.com/riverloopsec/killerbee

Zigbee: Network Discovery

- First assessment is to discover networks within range and enumerate the configuration of devices
  - Simple way; mimic Zigbee network discovery process with Killerbee
- Part of network discovery process in Zigbee Standard, ZDEs transmit beacon request on a given channel
  - All ZR and ZCs receiving beacon -> respond by sending a beacon frame
    - Disclose PAN ID, ZC or ZR source address, stack profile/version, extended IEEE address information
- Using same technique to actively scan for the presence of Zigbee network

Zigbee: Network Discovery

- Killerbee tool zbstumbler (similar to Wifi discovery tool Netstumbler):
  - Channel hops and transmits beacon request frames
    - Every two seconds hopping to a new channel
  - Display useful information from response beacon frames

```
test@test-HP-EliteBook-840-G3:~/killerbee$ sudo zbstumbler
[sudo] password for test:
Warning: You are using pyUSB 1.x, support is in beta.
zbstumbler: Transmitting and receiving on interface '1:11'
New Network: PANID 0xC762  Source 0xE2DA
        Ext PANID: 79:21:70:53:a3:d7:fc:34      Stack Profile: ZigBee Enterprise
        Stack Version: ZigBee 2006/2007
        Channel: 11
New Network: PANID 0xC762  Source 0xFF4F
        Ext PANID: 79:21:70:53:a3:d7:fc:34      Stack Profile: ZigBee Enterprise
        Stack Version: ZigBee 2006/2007
        Channel: 11
```

Zigbee Network Scanning Countermeasure

- Beacon request mechanism is integral to Zigbee
  - Cannot be disabled
  - Attacker can use it freely
- Best countermeasure is to understand the impact and evaluate your own networks to identify the information attacker can gain

Eavesdropping Attacks

- Zigbee networks are mostly

not encrypted

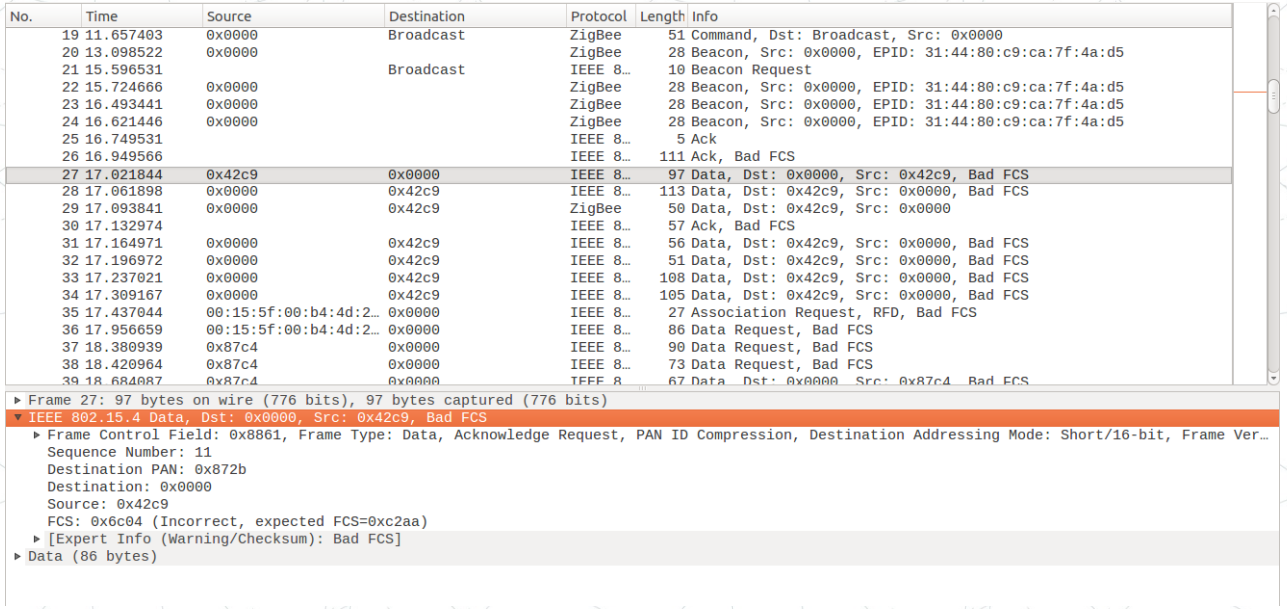
  - Extremely easy to eavesdrop

- Even if it uses encryption

  - Many unencrypted fields useful; MAC header, config of network, node address and PAN ID

  - Might substitute network discovery?

- Killerbee zbdump -> similar to tcpdump



DoS Zigbee

- Silva/Nunes attack exploits a flaw in how recipients process inbound packets with regard to the IEEE 802.15.4 frame counter (FC) value
- When a transmitting node sends a secure packet, it includes a sequential frame counter value in each frame with a range of 0 to 0xffffffff-1
  - FC value is not encrypted but it is included in the calculation of MIC (Message Integrity Check) for a packet

DoS Zigbee

- A receiving node remembers the last observed FC value for all of the nodes on the network
- To defeat replay attacks and avoid reprocessing packet retransmissions, receiving node only accepts packets with greater FC than last observed
- FC is also used to make the 'nonce' unique for each packet transmitted by a specific node

DoS Zigbee

- The unique nonce is important for AES-CTR to avoid initialization vector collision
  - Attacker can use plaintext/ciphertext data to get the key, if collision
- IEEE 802.15.4 specifies that when FC is equal to 0xffffffff, receiving node must stop processing all further data from the device
  - Add the transmitter to a device blacklist
  - Only way to recover, administrator updating the network key on all devices (firmware update)

DoS Zigbee

- Under intended use circumstances in IEEE 802.15.4, devices are not likely to reach max FC value
  - 1 packet per second, a node will need 136 years to reach
- If node receives packet with increasing FC, it will accept and update FC value prior to validating the encrypted packet
  - Attacker forges 0xffffffff-1 and blacklist the legitimate transmitter

Zbscapy

```
$ sudo zbscapy                                  # start killerbee framework

>>> kb = KillerBee()                            # acquire killerbee-enabled device

>>> conf.killerbee_channel = 15                 # set to channel #15

>>> f = Dot15d4()/Dot15d4Cmd(cmd_id=7)          # craft a IEEE 802.15.4 Command Frame
                                                # with the CMD_ID = 7 (Beacon Req)

>>>kbsendp(f,iface=kb)                         # send the frame
```

FLORIDA TECH

FLORIDA'S STEM UNIVERSITY™

Thank you. Questions?

Dr. Abdullah Aydeger