Semjon Kerner
Fachbereich Mathematik und Informatik

Freie Universität Berlin

Comparison of Bluetooth Low Energy and IEEE 802.15.4 and known attacks

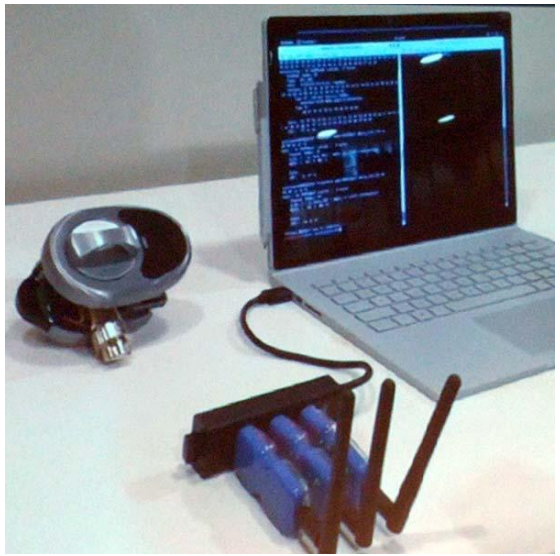
Seminar IoT & Security

2019-01-24

Attacks on IoT Devices

Attack Reasons

- Hacked devices used for Distributed Denial of Service Attacks
- Steal money / open „smart“ doors
- Malconfiguration of devices for life support
- Control cars



Attack Surface: Radio

- Jamming
- Eavesdropping
- Packet Injection
- Man in the Middle

Freie Universität Berlin

Table of Content

Bluetooth Low Energy

- Controller
  - Physical Layer
  - Link Layer
- Host
  - L2CAP / GATT / ATT
  - SMP

IEEE 802.15.4

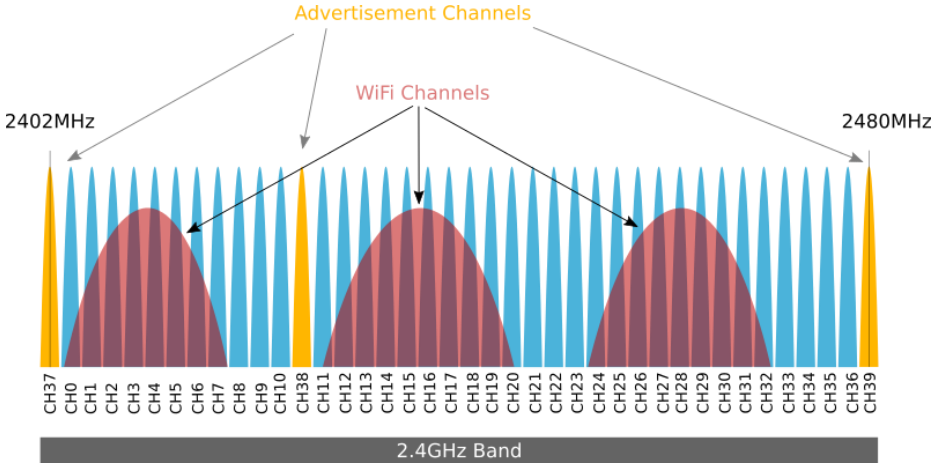
- Network Architecture
- Physical Layer
- Security Mechanisms

Known Attacks

- Denial of Service
- Eavesdropping
- Packet Injection
- Man in the Middle

BLE - Physical Layer

- Operates in 2,4 GHz ISM-Band
- Radio Modulation:
  - Gaussian Frequency Shift Keying (distinguish symbols)
  - Time Division Multiple Access (timeslots)
  - Frequency Hopping Spread Spectrum
- Bandwidth 1 Msym/s
  - Without coding: 1 Mb/s (less complex, no FEC)
  - 500 kb/s payload with coding
  - 125 kb/s header (optional payload)
- 40 Channels
  - 2 MHz wide
  - 37 dedicated channels + 3 advertising channels



BLE - Link Layer

- Statemachine for communication states
- Device Adresses
  - Public device adresses
  - Random device adresses
  - Private device adresses
- Provides Logical Channels
  - Synchronize to timing, hopping sequence, access adress

BLE Packet

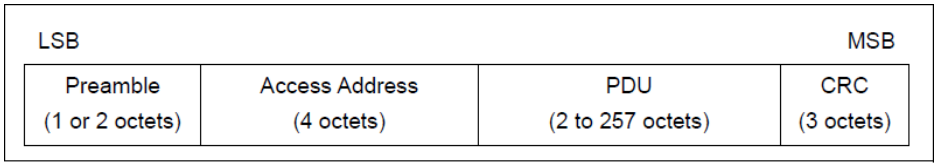
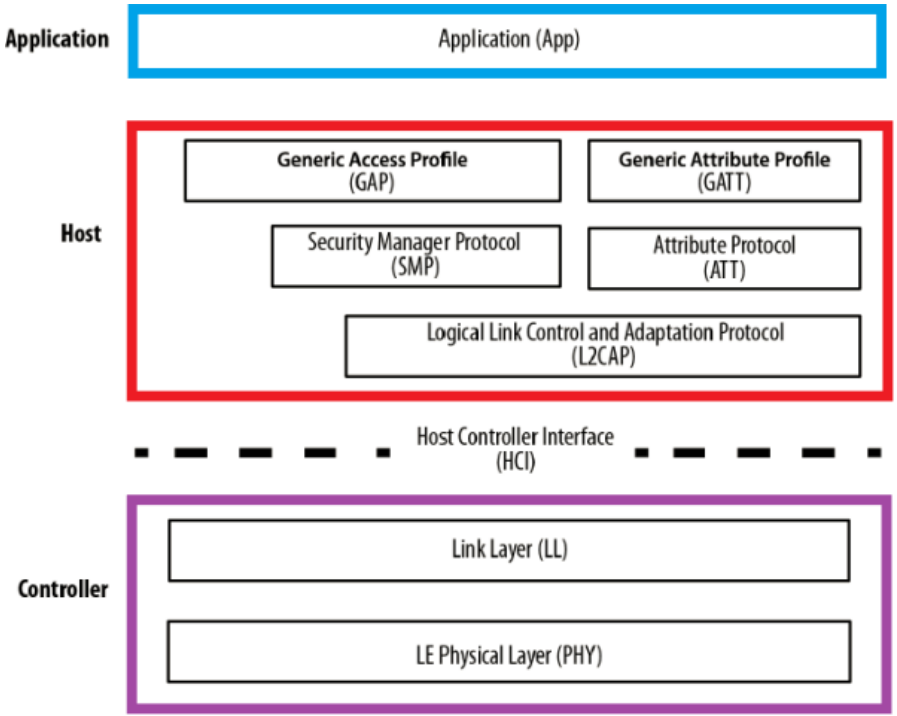


Figure 2.1: Link Layer packet format for the LE Uncoded PHYs

- Preamble: (10101010: LSB 1, 01010101: LSB 0)
- Access Adress: unique adress for each link layer connection
- Protocol Data Unit (PDU): payload
- 24 bit Cyclic Redundancy Check (CRC)

Freie Universität Berlin

BLE – Host profiles



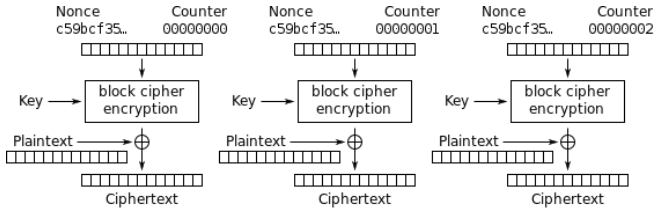
- L2CAP
  - Provide connectionless and connection-oriented Services to upper layers
  - Multiplexing data between profiles
  - Segmentation and assembly of packets
- ATT & GATT
  - Discover, Read, Write Services / Data and Attributes
- GAP
  - Standby State, Advertising State, Scanning State, Initiating State, Connection State
  - Roles: Master (Initiator), Slave (Advertiser), Scanner

Freie Universität Berlin

BLE – Security

Security Manager Protocol

- Pairing / Bonding
  1. Numeric comparison
  2. Passkey entry
  3. Out of band
  4. Just works
- 128 bit AES-CCM
  - Cypherblock Chaining with Counter



Counter (CTR) mode encryption

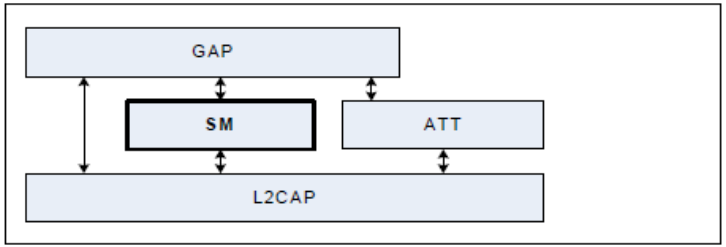


Figure 1.1: Relationship of the Security Manager to the rest of the LE Bluetooth architecture

Privacy

- Prevent tracking
- Devices may change private adresses
- Paired devices have tesolving zable

Authentication

- Approach without encryption
- Signing PDU in a trusted communication

IEEE 802.15.4

- IEEE 802.15.4 specifies PHY and MAC
- PAN Coordinators organize WPANs
  - Only Full Function Devices
  - Center in Star-Topology
  - Coordinate Beaconframes
  - Cluster Tree meshing networks between PAN Coordinators
- Beaconframes
  - Contention Access Period
  - Contention Free Period (Guaranteed Time Slots)

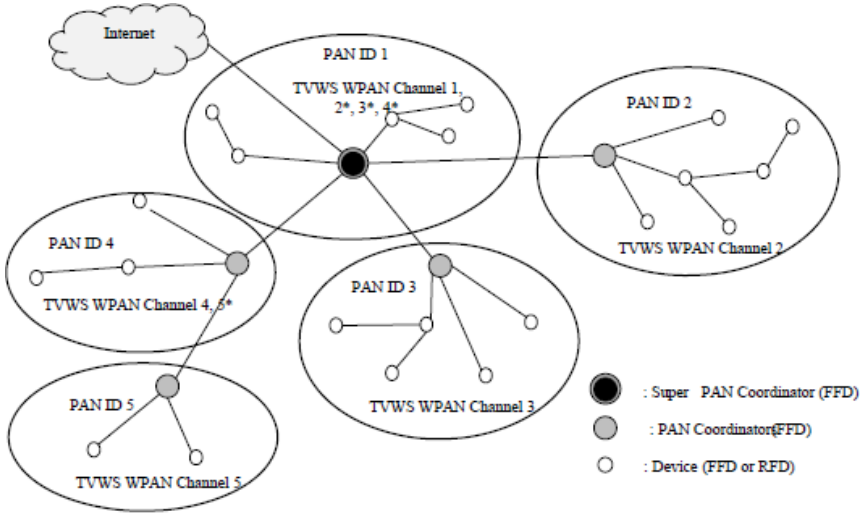
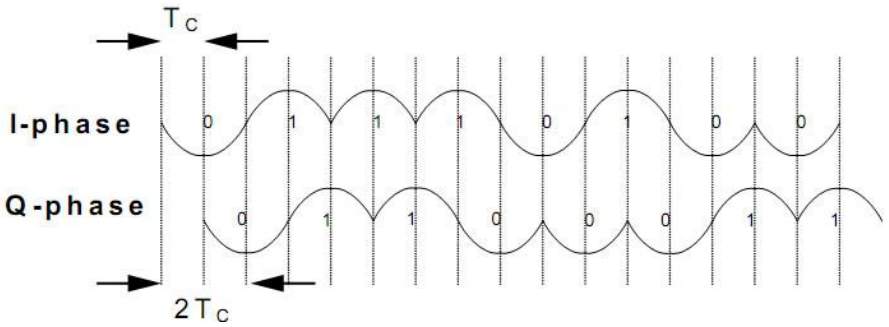


Figure 5-3—Example of TVWS multichannel cluster tree PAN

Freie Universität Berlin

IEEE 802.15.4 – Physical Layer

- Modulation:
  - Quadrature Phase Shift Keying (2 bit per Symbol)
  - Direct Sequence Spread Spectrum
  - Carrier Sense Multiple Acces / Collision Avoidance
- 2,4 GHz ISM-Band:
  - 16 Channels, 2 MHz wide, 5 MHz spacing
  - 250 kb/s



Freie Universität Berlin

IEEE 802.15.4 – Above the Physical Layer

- Link Layer
  - Acknowledgement
  - 2 Byte CRC
  - Short Adresses
  - Frame Counter (against replay attacks)
  - Slotted Mode with Superframes (Beaconframes)
  - Additional Low Energy States
- Additional Stacks, e.g.
  - Zigbee
  - 6LoWPAN
  - Provide Internet Protocols and Translation
    - IPv6, CoAP, RPL, …

IEEE 802.15.4 – Security

- Implementation of security is optional
- Establishment and maintenance of cryptographic keys is outside of the scope of the standard
- Keys are shared between two peers or among a group of devices
- Keys are adapted on a frame-by-frame basis with encryption and decryption functions

- 8 Security Levels are referred, composed of:
  - [unsecured]
  - 128 bit AES
  - Cipher Block Chaining
  - Counter
  - Truncation of Message Integrity Code

- IEEE 802.15.4 Security provides:
  - Data confidentiality
  - Data authenticity
  - Replay protection

Denial of Service

Jamming - Attacks

- Network configuration is unknown

continuous, random and deceptive jamming

- High rate of packetloss
- High power consumption

- Strategical jamming

reactive (interruptive) jamming

- Hard to detect
- Energy efficient

Network shapping jamming

- Jam all channels except some/one
- Force defenders into one channel

Defenses

- Channel hopping
- Segmentation
- Secret chipping sequences
- Secret preambles
- Forward Error Correction (FEC)

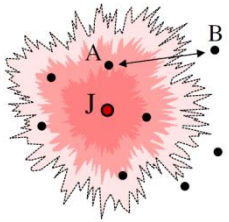


Fig. 1. Node J jams reception at neighbor A.

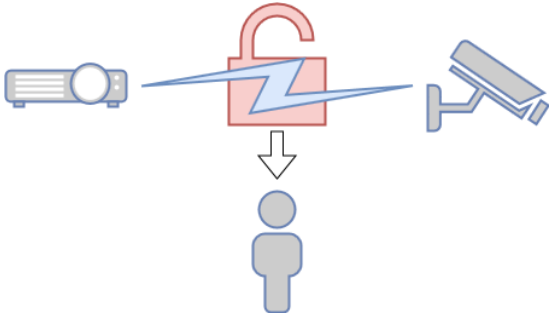
Most of these defenses are provided in BLE by default

Eavesdropping

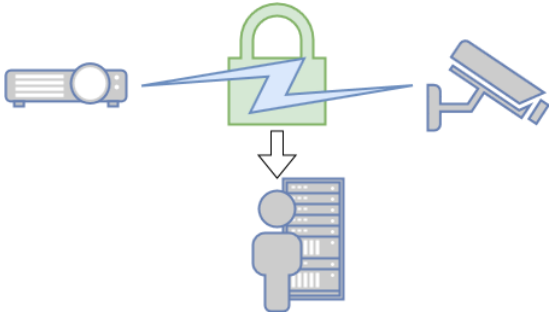
- Intercepting communication
- Only correct implemented and carried out cryptographie can prevent eavesdropping

- No encryption or special modulation in IEEE 802.15.4

- Information is needed to eavesdrop on BLE connections:
  - Slot length
  - Hopping sequence
  - Access addresses
  - CRC with unique seed



Attacker listens to unencrypted communication



Attacker uses tool (crackle) to decrypt communication

Packet Injection

Overshadowing

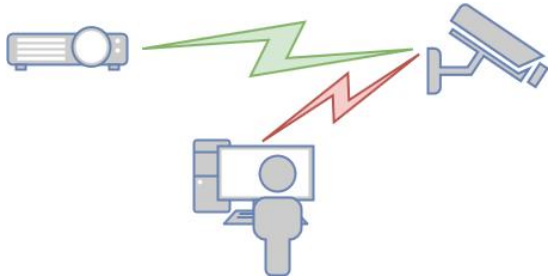
- Modify packets with interference signals
- If the receiver accepts the packet – attack is not tracked
- specific knowledge, special hard- and software needed

Packet-in-Packet Spoofing

- Encapsule a malicious packet within a higher level packet
- Typically an attacker must physically place or hijack a device to access the area of attack
- Symbol errors in the network are exploited

BLE Cloning (Evil Twin)

- In depth knowledge of the infrastructure is necessary
- A device clones services and tracks connection



Attacker overshadowing a transmission

Man in the Middle

- Feasible when communication is not encrypted, keys are tapped or guessed
- Multiple radio Interfaces are needed (e.g. interconnect via Websockets)

Attack on encrypted BLE:

- guessing the key (e.g. social engineering, reuse due to limited resources)
- cracking the key with crackle
- force reconnection by jamming

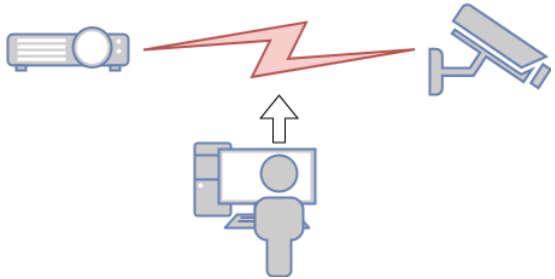
Established Tools:

- GATTacker

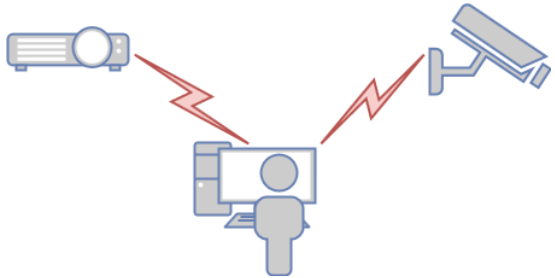
https://github.com/securing/gattacker

- Btlejuice

https://github.com/DigitalSecurity/btlejuice



Attacker forces a reconnection by e.g jamming



Attacker relays the reinitiated connection

7h4nk y0u f0r y0ur 4773n710n!