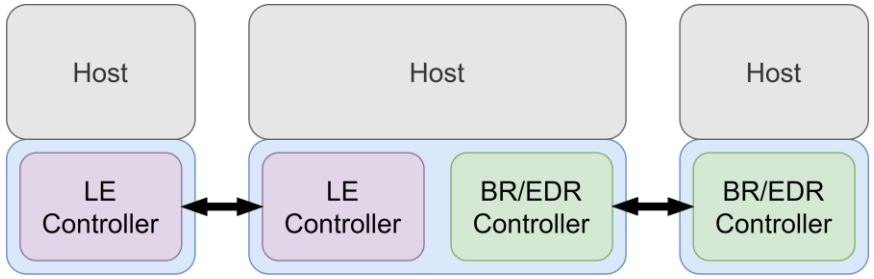
Bluetooth Low Energy (BLE) Security & Threat Modeling

by Silvia Schmidt & Christopher Skallak

BLE Basics

One Specification two Communication Protocols

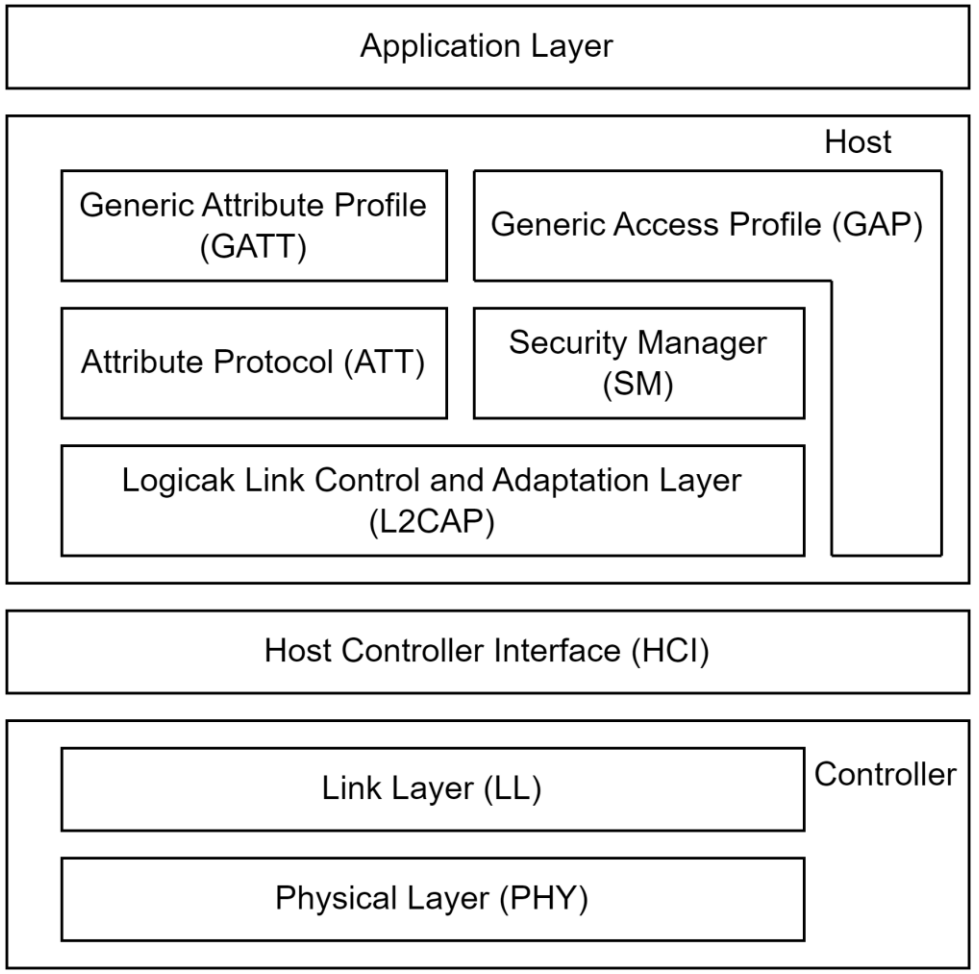
- **Bluetooth Classic (BR/EDR)**
  - Since Version 1 (1999)
  - Up to 2.1 Mb/s
  - 2,4 GHz ISM Band
  - 79 Channels
  - Use Cases:
    - Data Transfers
    - Audio Streaming
      - e.g., car hands-free phone system
    - PC Peripherals



c.f. [Spec v5.3, p. 188 fig 1.1]

- **Bluetooth Low Energy (BLE)**
  - Since Version 4.0 (2010)
  - Up to 2 Mb/s
  - 2,4 GHz ISM Band
  - 40 Channels:
    - 3 Advertising
    - 37 General Purpose
  - Use Cases:
    - Sensor Networks
    - Smart Home
    - Wearables
    - PC Peripherals

BLE Stack



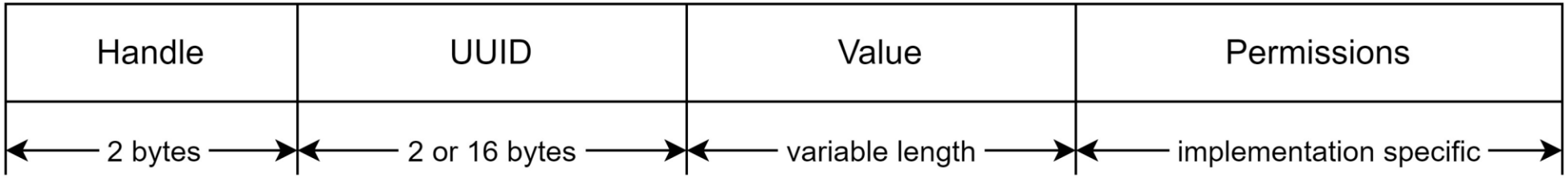
c.f. [Spec v5.3, p. 1245, fig. 2.1]

Device Roles & Communication Types

- **Connectionless Communication (Broadcast):**
  - Broadcaster
  - Observer
    - e.g. Sensor networks, Apple iTag
- **Connection-oriented Communication:**
  - Central (Client)
  - Peripheral (Server)
    - e.g. Smart Home, End-user Devices

BLE Stack: Attribute Protocol (ATT)

- Attribute Protocol (ATT):
  - Specifies a Datatype:
    - Handle
      - 16-bit Identifier unique inside of device
    - UUID
      - 128-bit unique Identifier
      - Defines Type
    - Attribute Value
    - Attribute Permissions



c.f. [Spec v5.3, p. 1473, fig. 2.4]

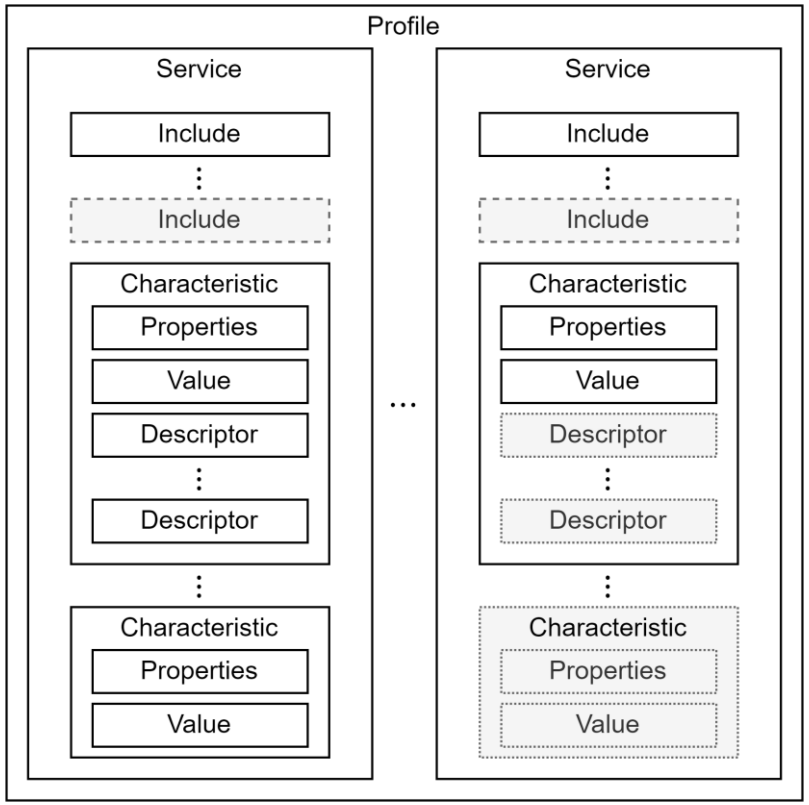
BLE Stack: Generic Attribute Protocol

- Generic Attribute Protocol (GATT):

  Defines Structure with Attributes:

  - Profile
  - Includes
  - Service
  - Characteristic
    - Data Storage
  - Descriptors

  - Security Features on a per Characteristic Basis
    - Common Chars e.g., Device Name
    - Protected Chars e.g., HID



c.f. [Spec v5.3, p. 1280, fig. 2.8]

Handles	Service > Characteristics	Properties	Data
0001 -> 0007	Generic Access (1800)		
0003	Device Name (2a00)	READ	PocketPi
0005	Appearance (2a01)	READ	Unknown
0007	2aa6	READ	01
0008 -> 0011	Generic Attribute (1801)		
000a	Service Changed (2a05)	INDICATE	
000d	2b29	READ, WRITE	00
000f	2b2a	READ	9cÞÚ0eS8dº9cÂ1fÒ9cqæÅØ
0011	2b3a	READ	01
0012 -> 0014	Device Information (180a)		
0014	PnP ID (2a50)	READ	Vendor ID: 0x1d6b (USB Implementer’s Forum assigned Vendor ID value) Product ID: 0x0246 Product Version: 0x0542
0015 -> 001b	e95dd91d251d470aa062fa1922dfa9a0		
0017	e95d93ee251d470aa062fa1922dfa9a1	READ, WRITE	ÿÿÿ1f
0019	e95d93ee251d470aa062fa1922dfa9a2	READ, WRITE	ÿÿÿ1f
001b	e95d93ee251d470aa062fa1922dfa9a3	READ, WRITE	insufficient encryption

[src: author]

BLE Security

Security Features

- Pairing
  - Key Exchange
- Bonding
  - Key Storage
- Device Authentication
- Encryption
- Message Integrity

Pairing

Legacy Pairing:

- 6-digit Temporal Key
  - 20-bit entropy
- Pairing Methods:
  - Just Works
  - Passkey Entry
  - Out of Band

Secure Connections Pairing:

- Elliptic Curve Diffie-Hellman (ECDH)
  - P-256
- Pairing Methods:
  - Just Works
  - Numeric Comparison
  - Passkey Entry
  - Out of Band

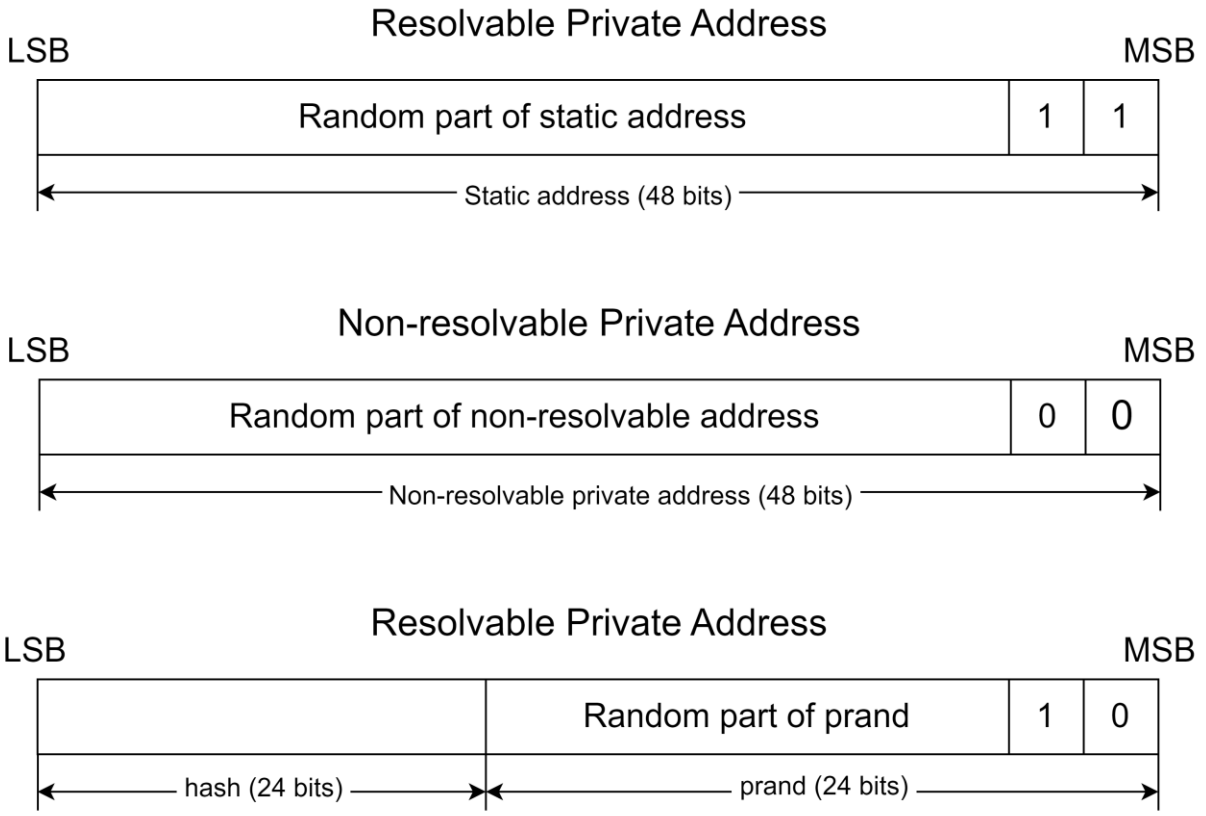
Encryption

- Session Key derived from
  - Short Term Key (STK)
  - Long Term Key (LTK)

- AES Cipher Block Chaining Message Authentication Code (CCM)
  - Stream Cipher
  - Message Integrity Check (MIC)

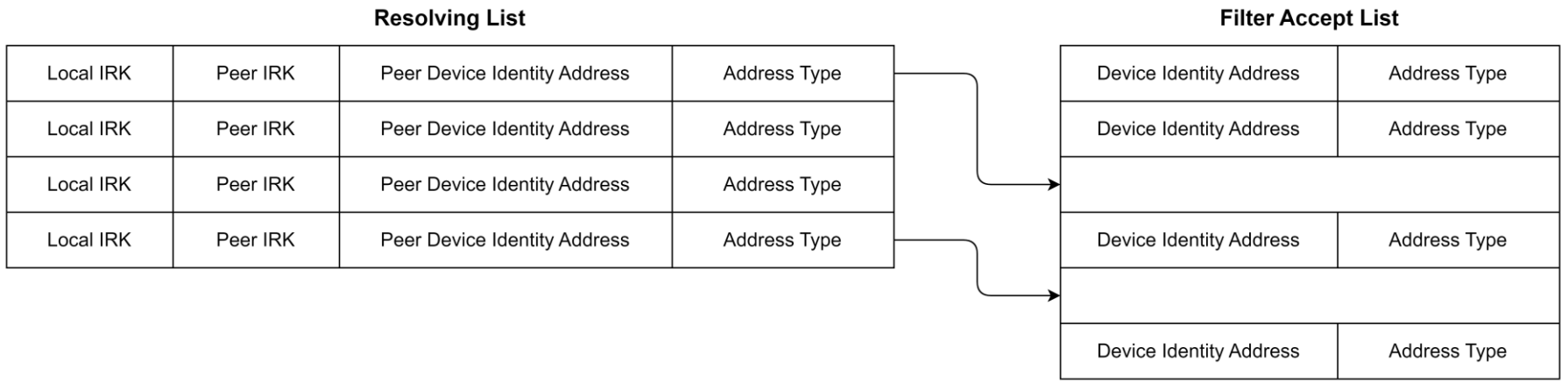
Address Types

- Public Device Address
  - 48-bit Extended Unique Identifier (EUI-48)
    e.g., Ethernet MAC address
- Random Device Address
  - Static Device Address
  - Non-resolvable Private Address
  - Resolvable Private Address (Identity Resolving Key (IRK))



c.f. [Spec v5.3, p. 2667-2668, fig. 1.2-1.4]

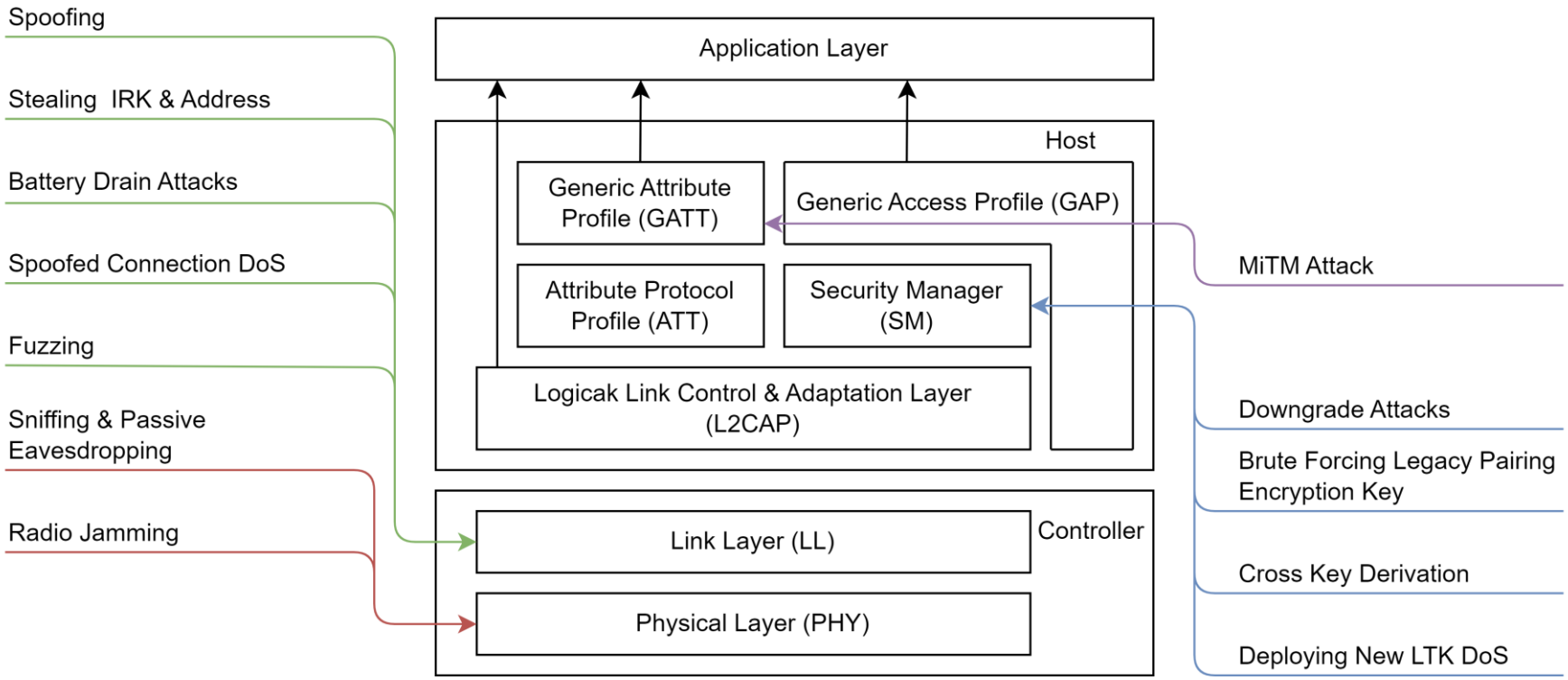
Address Filtering



c.f. [Spec v5.3, p. 276, fig. 5.6]

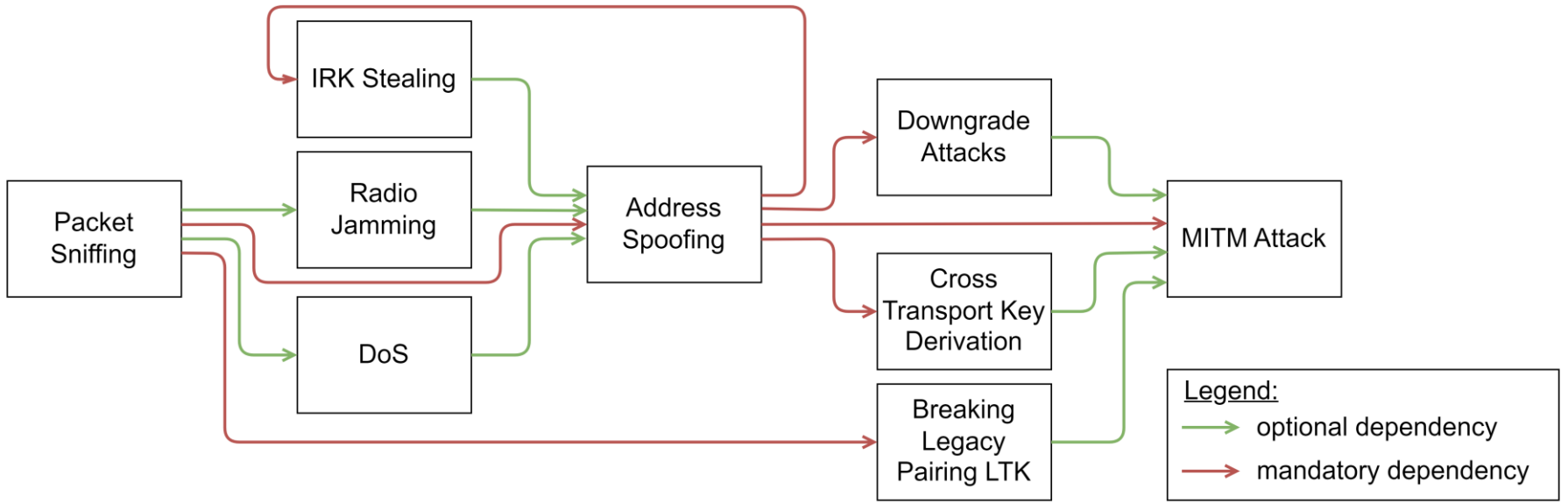
Threat Model

Threat Model



c.f. [Spec v5.3, p. 1245, fig. 2.1]

Threat Model Dependencies



[src: author]

Layer	Attack Vector	S	T	R	I	D	E
PHY	Sniffing			S	M		
PHY	Radio Jamming			I		M	
LL	Spoofing [S]	M	S	S	I		I
LL	[S] Advertisement Spoofing	M	S	S			
LL	[S] GATT Peripheral Spoofing	M	S	S	S		
LL	[S] GATT Central Spoofing	M	S	S			I
LL	Stealing the BD_Address and IRK	M	S	S	S		
LL	Demail of Service Attacks [DoS]		I			M	
LL	[DoS] Connection/Pairing request flooding					M	
LL	[DoS] Battery drain Attacks		I			M	
LL	[DoS] Spoofed connection					M	
LL	Fuzzing				I	I	
SMP	Downgrade Attacks [DA]	S	M	S	I		
SMP	[DA] Pairing Downgrade Attack	S	M	S			
SMP	[DA] Downgrade attack to Just Works	S	M	S			
SMP	[DA] Encryption Key entropy downgrade attack	S	M	S			
SMP	[DA] Downgrade Attack to plain text	S	M	S	S		
SMP	Brute Forcing Legacy Pairing Encryption Key			S	M		S
SMP	Cross Key Derivation (CTKD)	S	M	S		S	S
SMP	Deploying new LTK DoS				M		
GATT	MitM Attack	S	M	S	I		I

[src: author]

Legend:

M: Main STRIDE category of threat

S: Substitute STRIDE category of threat

I: STRIDE category applies in some specific threat implementations

Biggest Threats

- Sniffing
  - Hardware based (USB Devices) e.g.,
    - Ubertooth One[1] [8]
    - Adafruit LE Sniffer[2] [9]
    - nRF Sniffer[3] [10]
  - Software Defined Radio (SDR)
  - Jamming:
    - Types:
      - Full or Selective
      - Flooding or Reactive
    - 3 Advertisement Channels of Interest

[src: author]

Spoofing

- Changing the Device Address
  - Manufacturer HCI Commands
  - Bluez bdaddr.c [11]
    - e.g Raspberry Pi
- Types:
  - Advertisement Spoofing
    - Connection Establishment & Broadcast Messages
  - Peripheral Spoofing
    - GATT Profile Clone
  - Central Spoofing
    - MitM & Whitelist Bypass

MitM Attack

- Based on:
  - Spoofing Attack
  - Downgrade Attack

Association Model	MitM Protection	Passive eavesdropping Protection
Legacy Pairing		
Just Works	No	No
Passkey Entry	Yes	No
Out of Band	Yes/No	Yes/No
Secure Connections		
Just Works	No	Yes
Passkey Entry	Yes	Yes
Numeric Comparison	Yes	Yes
Out of Band	Yes/No	Yes

c.f. [Spec v5.3, pp. 1575-1585]

- Open Source MitM Tools
  - Btlejuice
    - Noble & Bleno (node.js)
  - Mirage
    - Security Audit Framework for IoT:
      - Zigbee
      - Wifi
      - BLE

How to Secure Connections

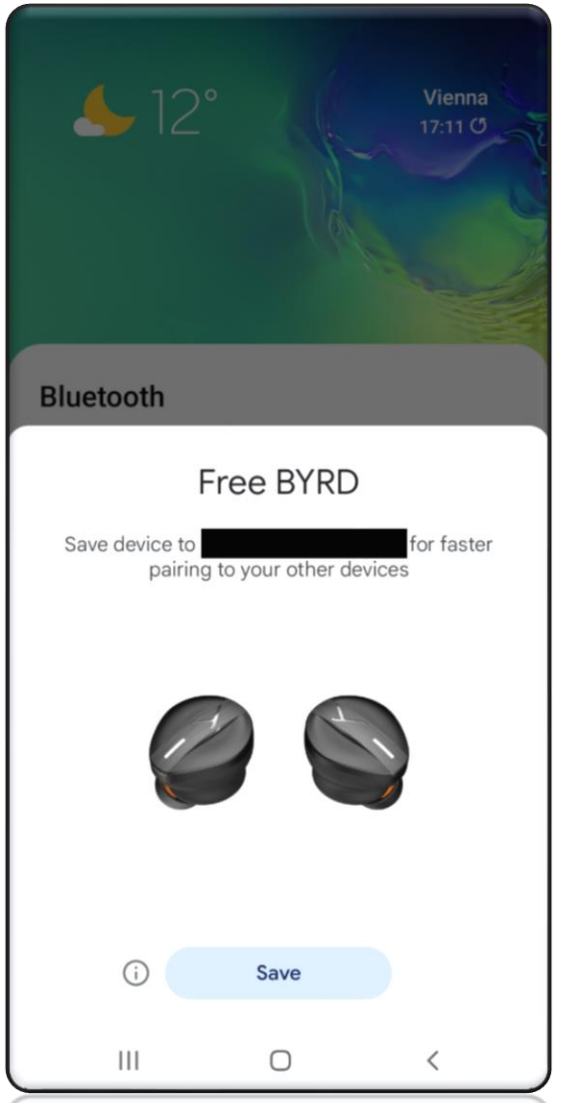
- Securing Devices:
  - Using The Security Features (Encryption)
    - or Application Layer Security
  - Chips with v4.2 or Higher
  - Secure Connections Only Mode (if possible)

Latest Threat

Apple Notification Spam

- Attack:
  - Malicious Device sends Spoofed Advertisements
    - Spoofed as Apple TV, Headphones …
  - User Devices show popups and Interrupts the usage

- Development
  - First occurrence at Def Con by Jae Bochs as prank (June 2023)
  - Techryptic ports exploit to custom Flipper Zero firmware (Sep 2023)
  - Flipper Zero XFW-Xtreme Firmware in dev build (current)
    - Advanced version of attack:
      - Works on Android
      - Crashes Apple Phones



[src: author]

Most Exotic Threat

Cross Transport Key Derivation (CTKD)

- Cross Transport Key Derivation
  - Derives BT Key from BLE key
  - Derives BLE Key from BT key

- Design Issues:
  - Dual Pairing
  - Asymmetric Role Systems
  - Replacing Keys
  - Manipulation of the Association Model

Thank You For Your Attention

ITS - NOW

June 6th and 7th 2024
Call for Participation:
https://its-now.science/?participation