

# Bluetooth Security

Gustavo Padovan

<http://padovan.org>  
[gustavo@padovan.org](mailto:gustavo@padovan.org)

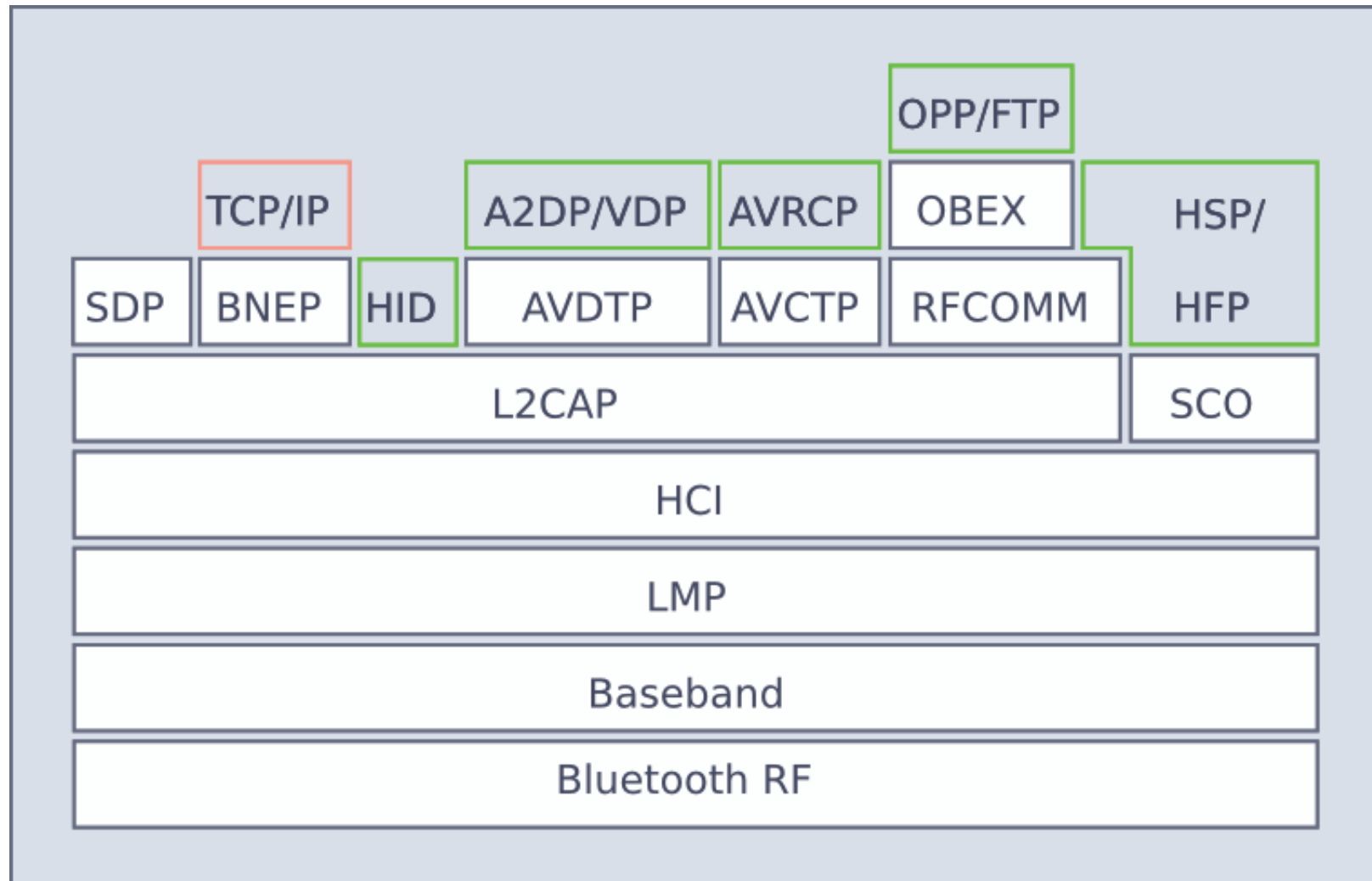
# Agenda

- What is Bluetooth?
- The Bluetooth stack
- Pairing
- The Old Way
- Secure Simple Pairing
- IO capabilities
- Bluetooth Low Energy Security
- Bluetooth High Speed Security

# What is Bluetooth?

- Use the unlicensed 2.4GHz ISM band
- Designed for short-distance data exchange
- Designed as a cable replacement
- Many use cases (profiles)
- Specified by the Bluetooth SIG
- Low Power, Low Cost
- Security based on pairing/PIN Code

# The Bluetooth Stack



# Pairing

- First Connection
  1. > HCI\_Pin\_Code\_Request
  2. < HCI\_Pin\_Code\_Request\_Reply
  3. > HCI\_Link\_Key\_Notification
- Further Connections
  1. > HCI\_Link\_Key\_Request
  2. < HCI\_Link\_Key\_Request\_Reply

# Legacy Pairing

- 3 Security Modes
- Limited resources
- Modified SAFER+ (Massey et al 1998)
- 1-16 bytes long secrets
- 128 bits authentication link keys
- Encrypted by the E0 stream cipher
- Encryption on the controller

# Legacy Pairing

- Security Mode 1
  - No security
- Security Mode 2
  - Service Level Security
  - On device level no difference to Mode 1
- Security Mode 3
  - Device Level Security
  - Encrypt all low-level connections

# Security Flaws in Legacy Pairing

- Brute-force attack for small PIN
- E0 is too weak
- No expiration date for link keys
- No protection against MITM

# Secure Simple Pairing

- Simplify and improve security
- Elliptic curves Diffie-Hellman
- Passive eavesdropping protection
- Optional MITM protection
- New concept of IO Capabilities
- Security Mode 4
- Encryption on the controller

# IO Capabilities

- Take in account input and output capabilities
- Choose the option that fits better
- Pairing Models
  - Numeric Comparison (MITM protection)
  - Just Works (No MITM protection)
  - Passkey Entry(MITM protection)
  - Out of Band (It depends)

# IO Capabilities

- Input Capabilities
  - NoInput
  - Yes/No
  - Keyboard
- Output Capabilities
  - No output
  - Numeric Output

# IO Capabilities

<b>Local Output Capacity</b> <b>Local Input Capacity</b>	<b>No Output</b>	<b>Numeric Output</b>
<b>No input</b>	NoInputNoOutput	DisplayOnly
<b>Yes / No</b>	NoInputNoOutput	DisplayYesNo
<b>Keyboard</b>	KeyboardOnly	DisplayYesNo

<b>Initiator A</b> <b>B Responder</b>	<b>Display Only</b>	<b>DisplayYesNo</b>	<b>KeyboardOnly</b>	<b>NoInputNoOutput</b>
<b>DisplayOnly</b>	Numeric Comparison with automatic confirmation on both devices.  Unauthenticated	Numeric Comparison with automatic confirmation on device B only.  Unauthenticated	Passkey Entry: Responder Display, Initiator Input.  Authenticated	Numeric Comparison with automatic confirmation on both devices.  Unauthenticated
<b>DisplayYesNo</b>	Numeric Comparison with automatic confirmation on device A only.  Unauthenticated	Numeric Comparison: Both Display, Both Confirm.  Authenticated	Passkey Entry: Responder Display, Initiator Input.  Authenticated	Numeric Comparison with automatic confirmation on device A only.  Unauthenticated
<b>Keyboard Only</b>	Passkey Entry: Initiator Display, Responder Input.  Authenticated	Passkey Entry: Initiator Display, Responder Input.  Authenticated	Passkey Entry: Initiator and Responder Input.  Authenticated	Numeric Comparison with automatic confirmation on both devices.  Unauthenticated
<b>NoInputNoOutput</b>	Numeric Comparison with automatic confirmation on both devices.  Unauthenticated	Numeric Comparison with automatic confirmation on device B only.  Unauthenticated	Numeric Comparison with automatic confirmation on both devices.  Unauthenticated	Numeric Comparison with automatic confirmation on both devices.  Unauthenticated

# Bluetooth Low Energy

- Bluetooth Core Spec v4.0
- New 2.4GHz radio
- Reduced Low Power consumption
- Very limited resources
- Use AES-CCM
- No eavesdropping protection
- Key generation in the Host
- Privacy Feature

# Bluetooth Low Energy

- Similar IO Capabilities Concept
- Have JustWorks, Passkey Entry, OOB
- But no Numeric Comparison

# Bluetooth High Speed

- Bluetooth Core Spec v3.0
- Alternate MAC/PHY (AMP)
- Support to use other radios like 802.11
- Increases transfer bandwidth

# Bluetooth High Speed Security

- Use Secure Simple Pairing
- GAMP\_LK is based on the BR/EDR link key

# Credits

- The New Security Model Of Bluetooth, Marcel Holtmann, 2007.  
<http://www.securitytube.net/video/1974>
- Chats with Vinicius Gomes
- Bluetooth Core Specification v4.0.  
[https://www.bluetooth.org/docman/handlers/downloaddoc.ashx?doc\\_id=229737](https://www.bluetooth.org/docman/handlers/downloaddoc.ashx?doc_id=229737)

# Questions?

Gustavo Padovan

<http://padovan.org>  
[gustavo@padovan.org](mailto:gustavo@padovan.org)