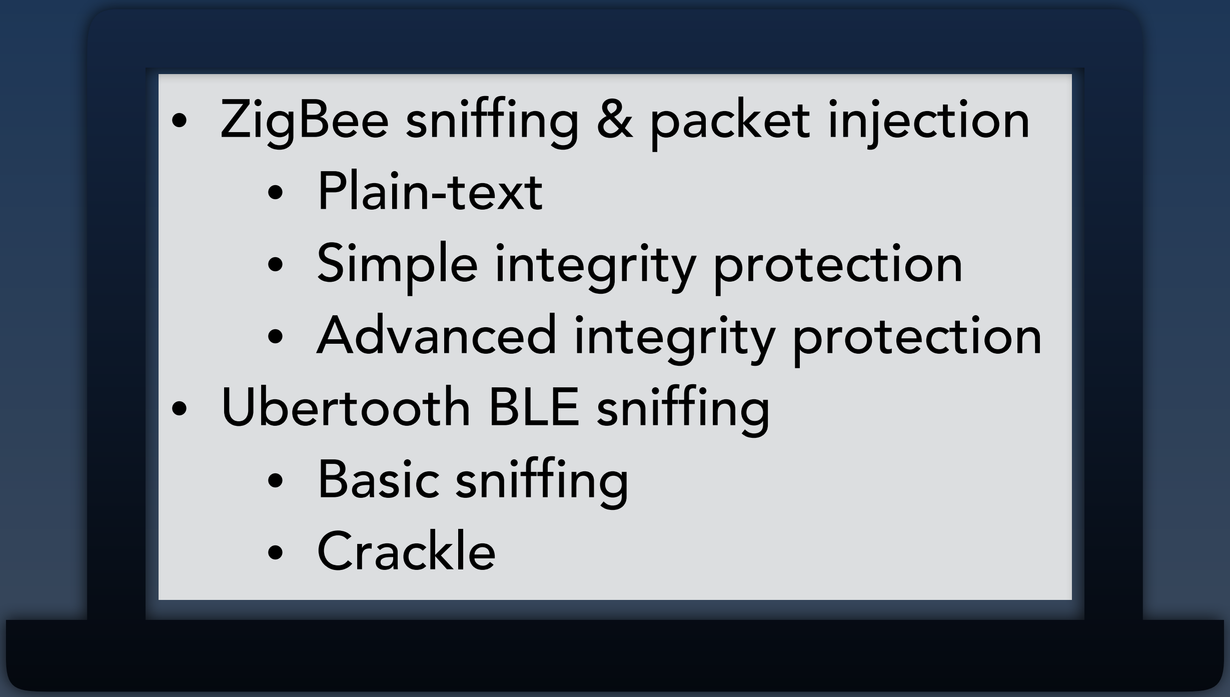
DEEP
ARMOR

Hands-on Exploitation & Hardening of Wearable and IoT Platforms

Sumanth Naropanth & Sunil Kumar

Agenda

- Technical overview of an IoT/wearable ecosystem
- Building blocks
- Communication Protocols
- Case Studies
  - IEEE 802.15.4/ZigBee
  - Bluetooth and BLE
- **Hands-on exercises**
- Privacy for next generation IoT/wearable platforms
- Security development lifecycle (SDL) overview



- ZigBee sniffing & packet injection
  - Plain-text
  - Simple integrity protection
  - Advanced integrity protection
- Ubertooth BLE sniffing
  - Basic sniffing
  - Crackle

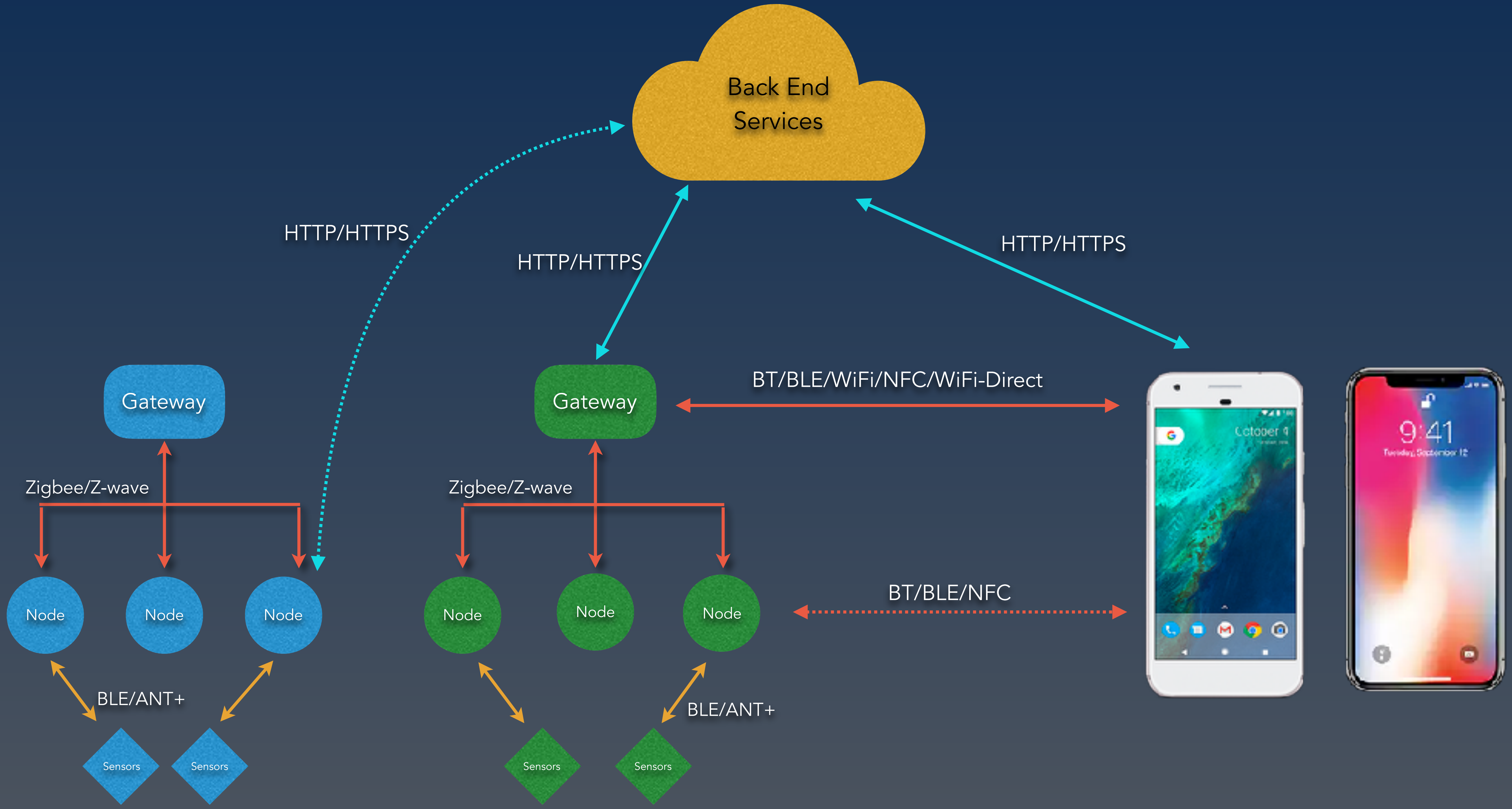
Instructors

- Sunil Kumar
  - Security Analyst — Deep Armor
  - Ola Security, Aricent/Intel

- Sumanth Naropanth
  - Founder and CEO — Deep Armor
  - Intel, Palm/HP, Sun Microsystems

- Security consulting, vulnerability testing, SDL and training services for emerging technologies
- www.deeparmor.com | @deep_armor

IoT/Wearable Ecosystem



Building Blocks

Device	Mobile	Cloud
• Hardware • Firmware/OS/RTOS • Crypto Device • Communication interfaces • Communication protocols • Device Software SDK • Remote device management • Third party libraries	• iOS and Android apps • Unity/VR apps • SDK for third party apps and services	• User & Admin portals • Micro-services • Databases • Web applications • Storage solutions • SDK for third party services • Analytics • Data sharing

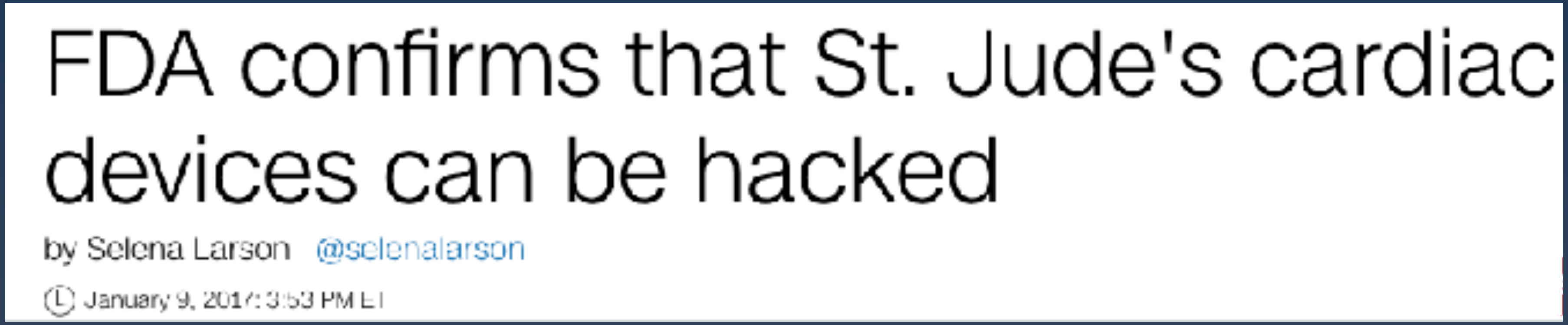
Security for IoT

- Why?
  - Personal and PII data
  - Healthcare, Payment, Critical Infrastructure, …
- Messy
  - Defensive Security Measures
  - Plethora of protocols and standards
- Process & Technical challenges

Attacking IoT

New Car Hacking Research: 2017, Remote Attack Tesla Motors Again

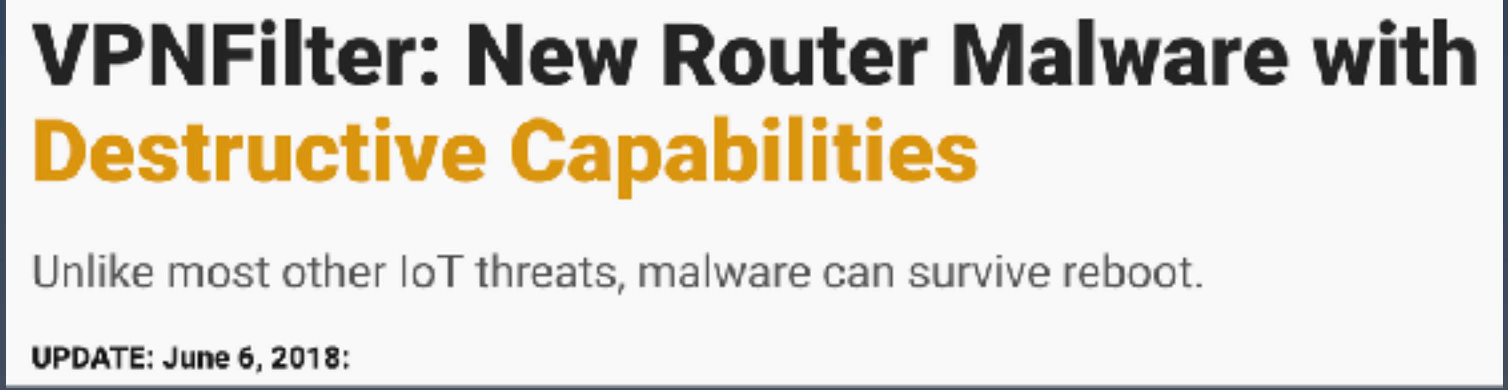
by Keen Security Lab of Tencent



FDA confirms that St. Jude's cardiac devices can be hacked

by Selena Larson @selenalarson

January 9, 2017: 3:53 PM ET



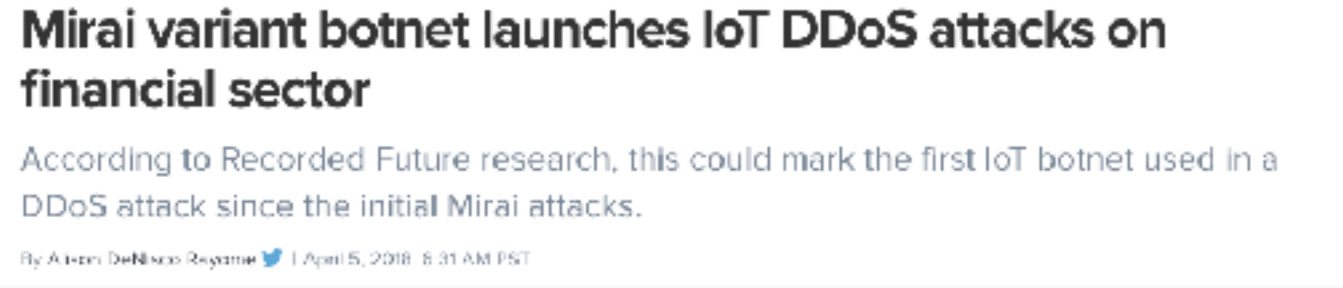
VPNFilter: New Router Malware with Destructive Capabilities

Unlike most other IoT threats, malware can survive reboot.

UPDATE: June 6, 2018:

ANDY GREENBERG SECURITY 07.29.15 07:00 AM

HACKERS CAN DISABLE A SNIPER RIFLE—OR CHANGE ITS TARGET



Mirai variant botnet launches IoT DDoS attacks on financial sector

According to Recorded Future research, this could mark the first IoT botnet used in a DDoS attack since the initial Mirai attacks.

By Alison DeNisco Rayome | April 5, 2018, 6:31 AM PST

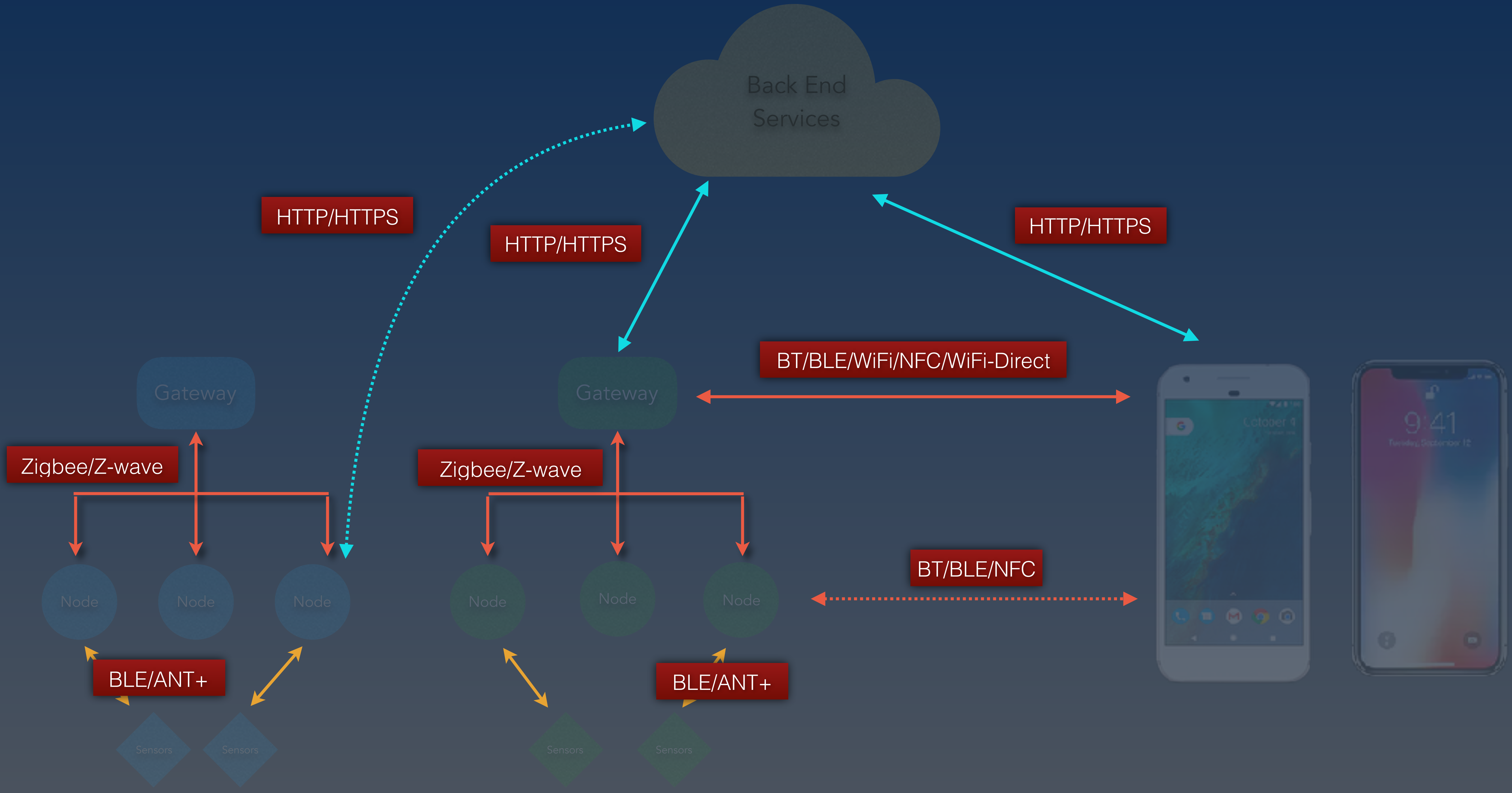
Weak Links?

Device	Mobile	Cloud
• Hardware • Firmware/OS/RTOS • Crypto Device • Communication interfaces • Communication protocols • Device Software SDK • Remote device management • Third party libraries	• iOS and Android apps • Unity/VR apps • SDK for third party apps and services	• User & Admin portals • Micro-services • Databases • Web applications • Storage solutions • SDK for third party services • Analytics • Data sharing

Weak Links

Device	Mobile	Cloud
• Hardware • Firmware/OS/RTOS • Crypto Device • Communication interfaces • Communication protocols • Device Software SDK • Remote Device management • Third party libraries	• iOS and Android apps • Unity/VR apps • SDK for third party apps and services	• User & Admin portals • Micro-services • Databases • Web applications • Storage solutions • SDK for third party services • Analytics • Data sharing

Communication Channels



Back End Services

HTTP/HTTPS

HTTP/HTTPS

HTTP/HTTPS

BT/BLE/WiFi/NFC/WiFi-Direct

Gateway

Gateway

Zigbee/Z-wave

Zigbee/Z-wave

BT/BLE/NFC

Node

Node

Node

Node

Node

Node

BLE/ANT+

BLE/ANT+

Sensors

Sensors

Sensors

Sensors

IoT Protocols

SigFox

MQTT

nWave

RFID

Bluetooth

DASH

LTE

DSMx

Zigbee

Thread

NFC

ANT+

Z-Wave

6LoWPAN

CoAP

4G

Cellular

Wi-Fi

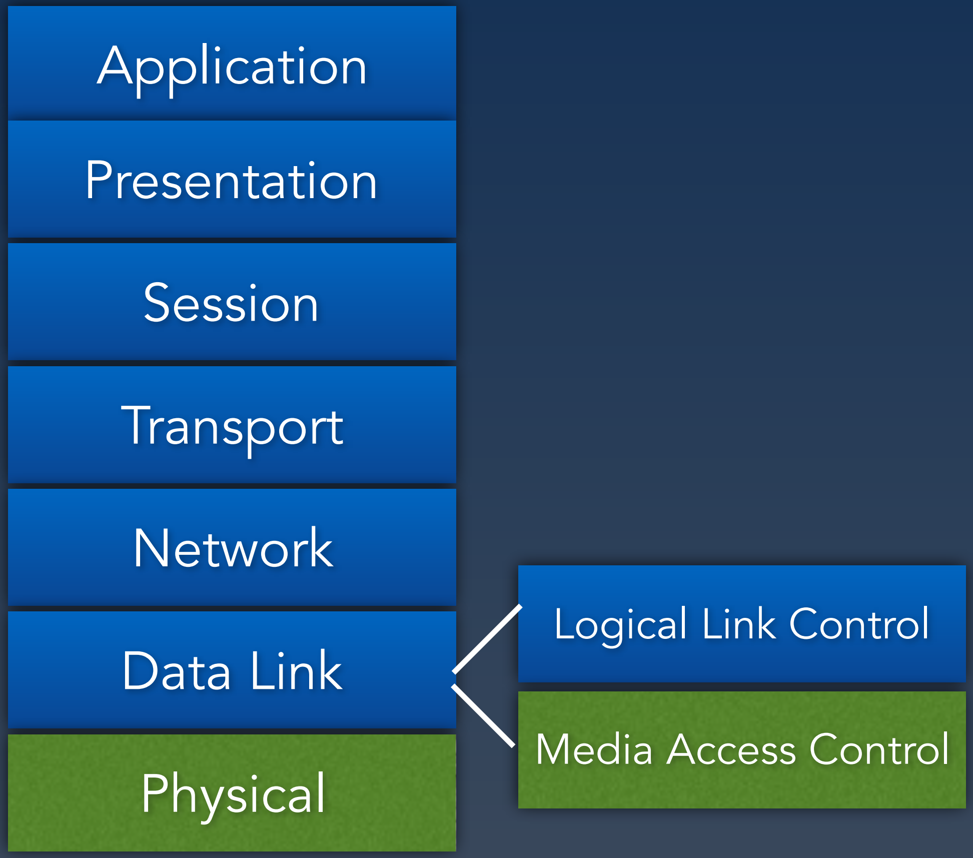
BLE

Zigbee

802.15.4

802.15.4

- IEEE standard for low-rate wireless personal area networks (LR-WPANs)
- 6LoWPAN for IPv6 over WPANs
- Zigbee extends 802.15.4 (wrapper services)



Zigbee

- Low data rate wireless applications
- Smart energy, medical, home automation, IIoT
- Two bands of operation: 868/915MHz and 2450MHz
- Simpler & less expensive than Bluetooth
- 10-100m range
- Zigbee Alliance

Zigbee Security Model

- Open Trust model (Device Trust Boundary)
- Crypto protection
  - Network Key
  - Link Key (App Support Sublayer)
- Secure key storage assumptions
- *Transmission of network key for new nodes*
- *Hard-coded Trust Center Link Keys*

Exercise 1

Sniffing and Packet Injection in an 802.15.4 network

Overview

- IoT product simulator
- Zigbee-like 802.15.4 based communication protocol
- Packet sniffing, capture and injection
- Goals:
  - Basic packet header formats
  - Security models for protecting comms
  - Hardware and software tools for packet sniffing & injection

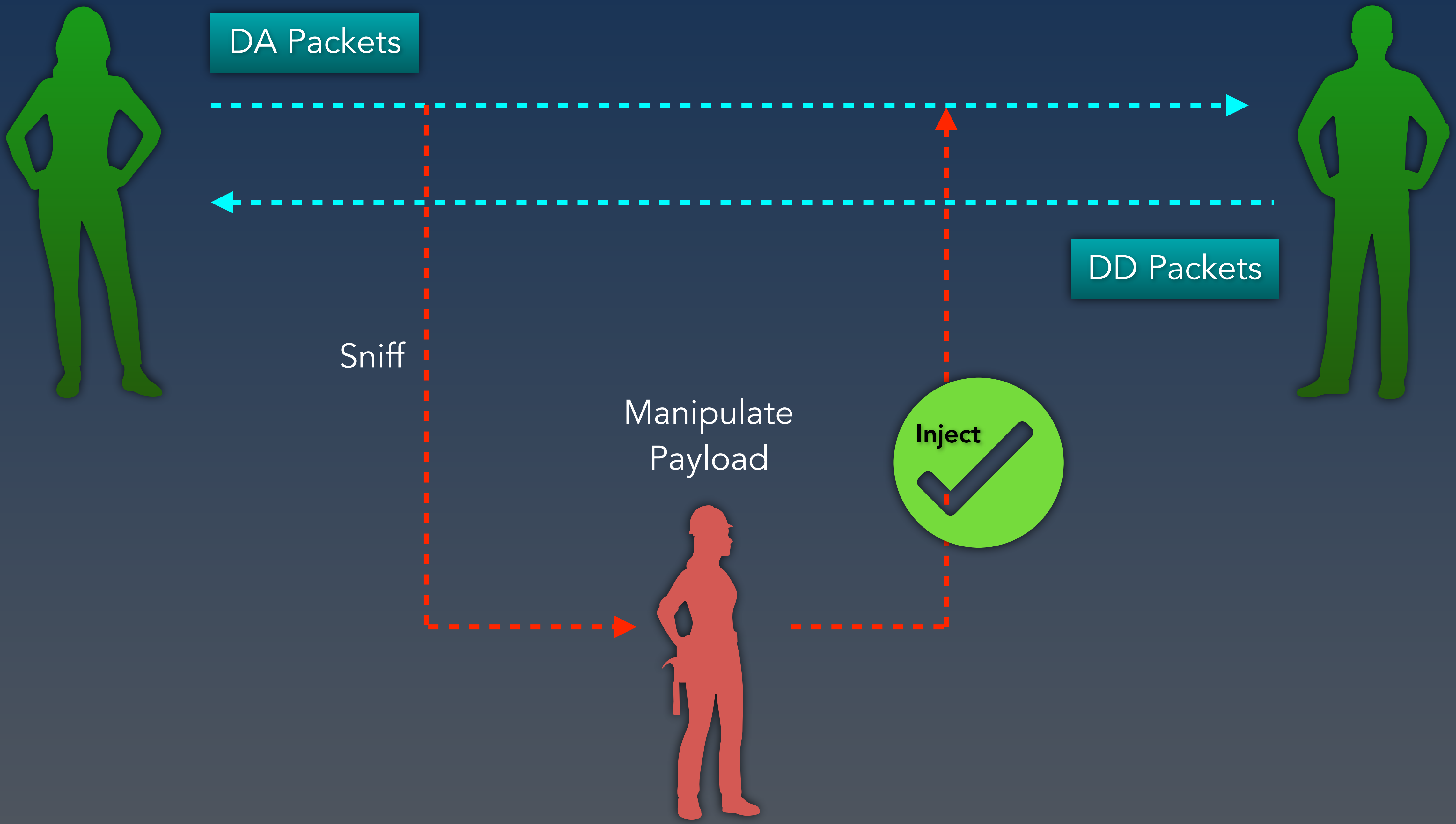
Tools

- Microchip’s RZUSBStick
  (2 “Victims” and 1 “attacker”)
- KillerBee firmware
  - IEEE 802.15.4/ZigBee Security Research Toolkit
  - River Loop Security
- KillerBee tools
  - ~17 tools
  - zbwireshark and zbreplay
- Scapy

Scenario 1

Packet sniffing & Injection

Outline

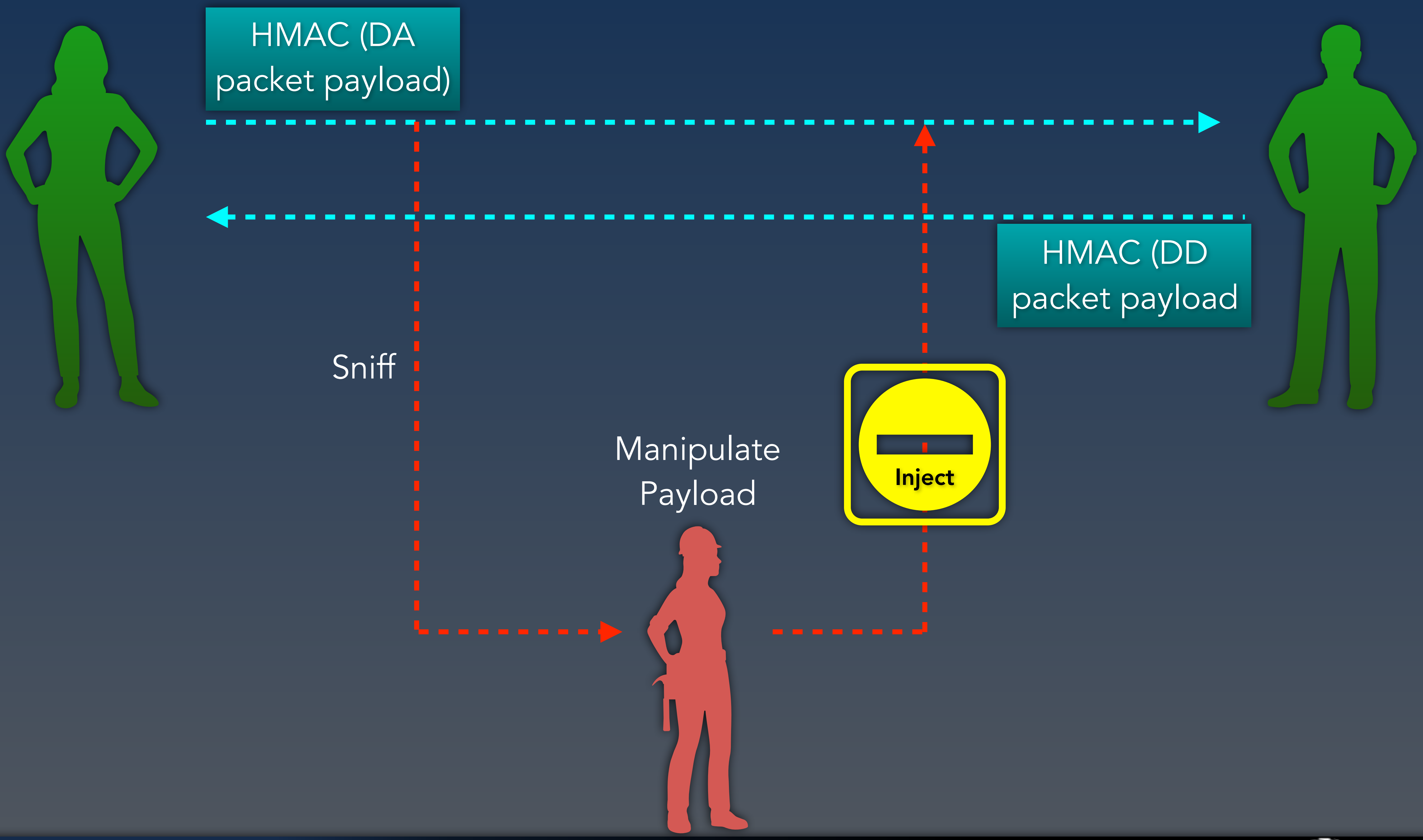


Demo

Scenario 2a

(Some Security)

Outline


HMAC (DA
packet payload)
HMAC (DD
packet payload
Sniff
Manipulate
Payload
Inject

Demo

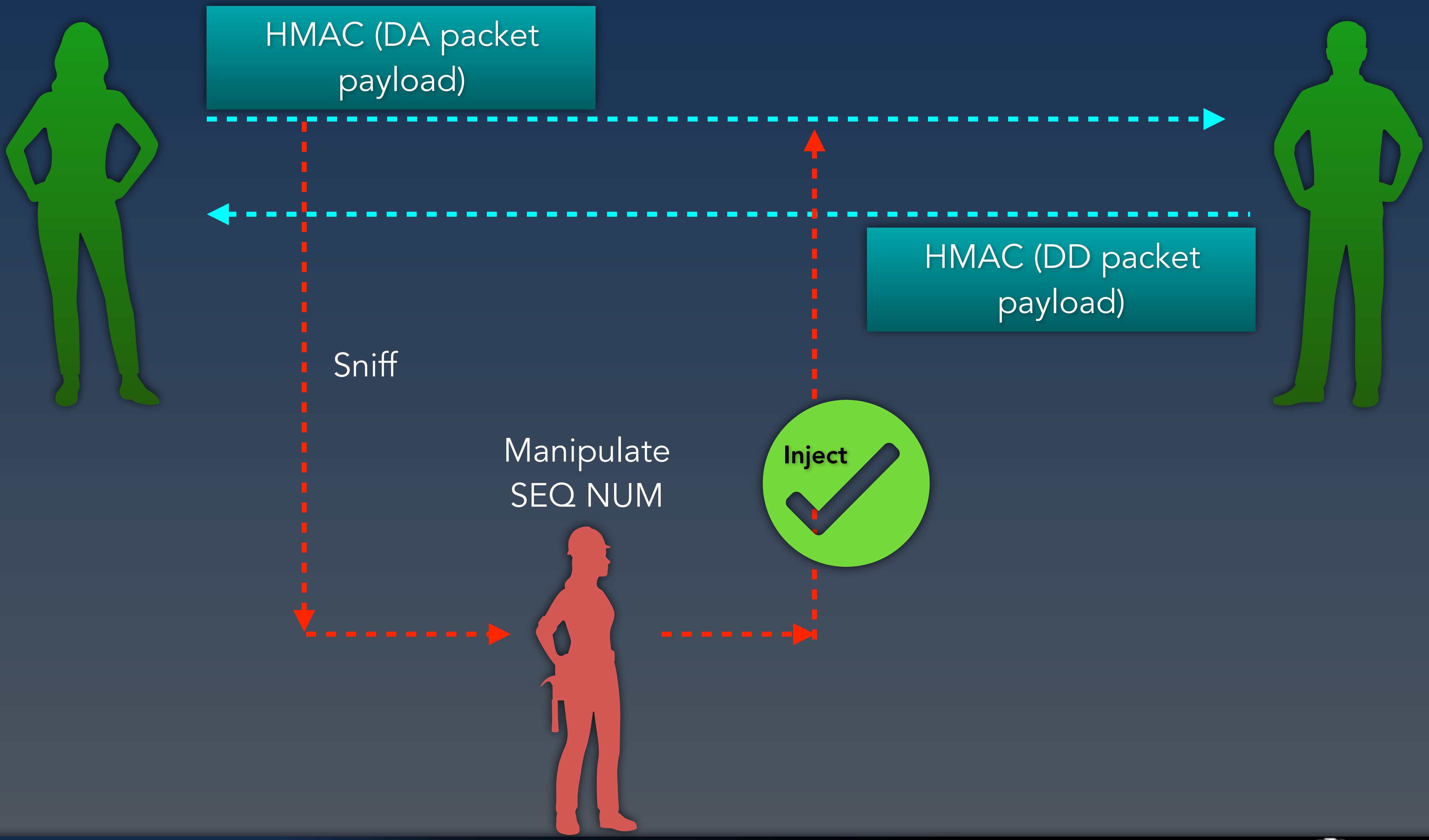
Scenario 2b

☠

(Some Security)

Demo (first)

Outline



HMAC (DA packet payload)

HMAC (DD packet payload)

Sniff

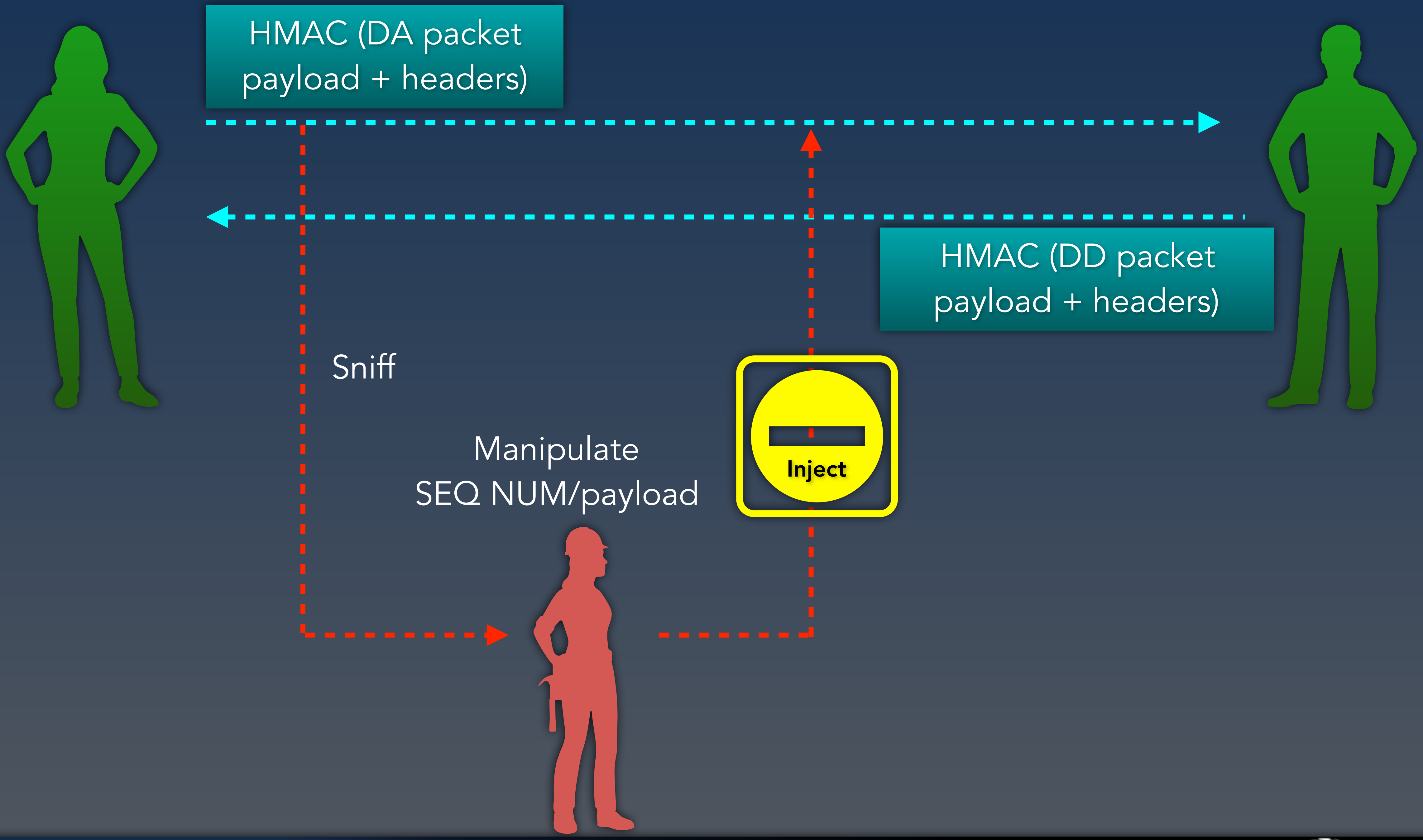
Manipulate SEQ NUM

Inject

Scenario 3

(Full Security)

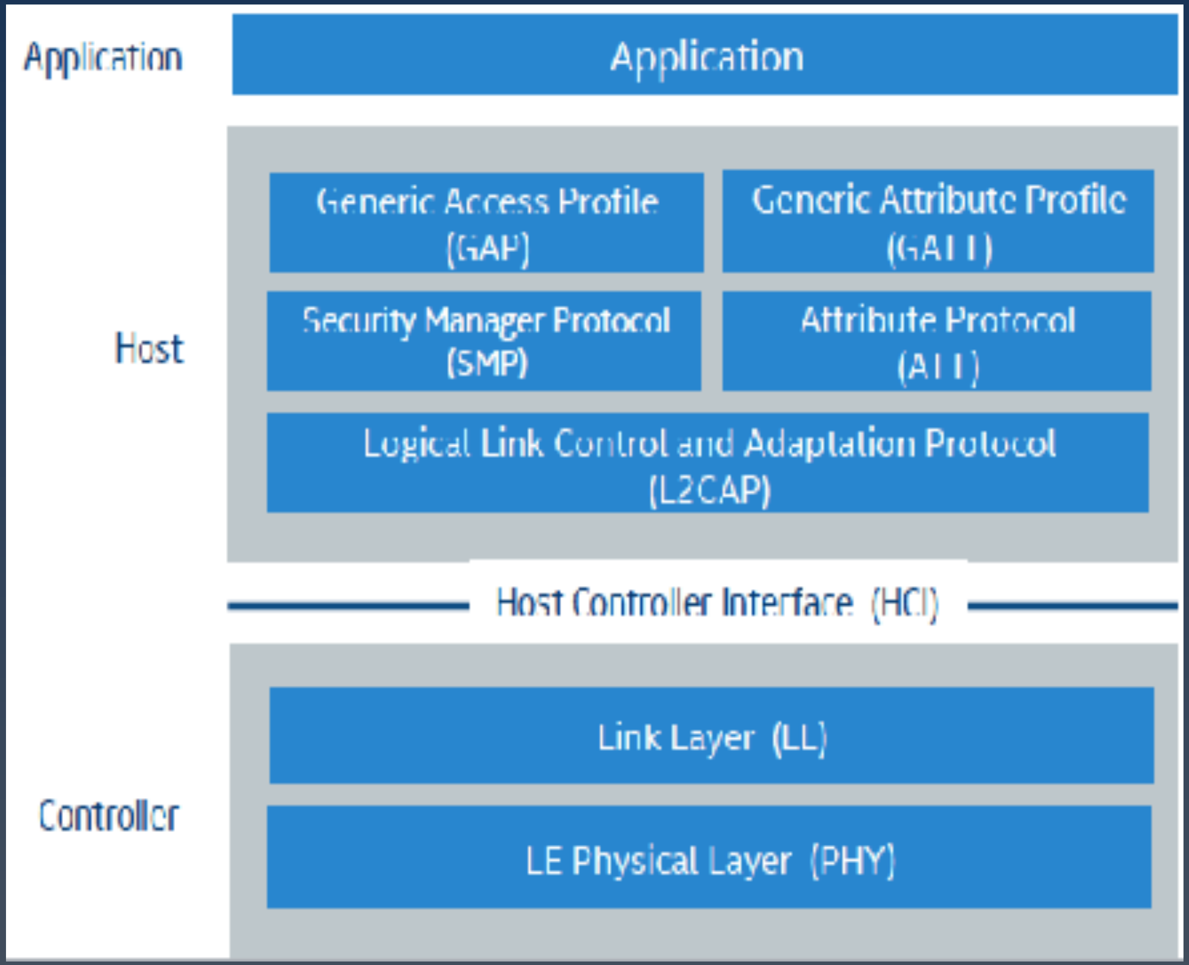
Outline


HMAC (DA packet payload + headers)
HMAC (DD packet payload + headers)
Sniff
Manipulate SEQ NUM/payload
Inject

Demo

Bluetooth and Bluetooth Low Energy (BLE)

Overview: Bluetooth Stack


Application
Application
Host
Generic Access Profile (GAP)
Generic Attribute Profile (GATT)
Security Manager Protocol (SMP)
Attribute Protocol (ATT)
Logical Link Control and Adaptation Protocol (L2CAP)
Host Controller Interface (HCI)
Controller
Link Layer (LL)
LE Physical Layer (PHY)

GAP
Defines how devices discover, connect and create bonding between them

GATT
Describes characteristics, services and type of attributes/ their usage

SMP
Protocol for pairing and key distribution and authenticating other device
Shared secrets can be managed and hence speed-up the reconnection process

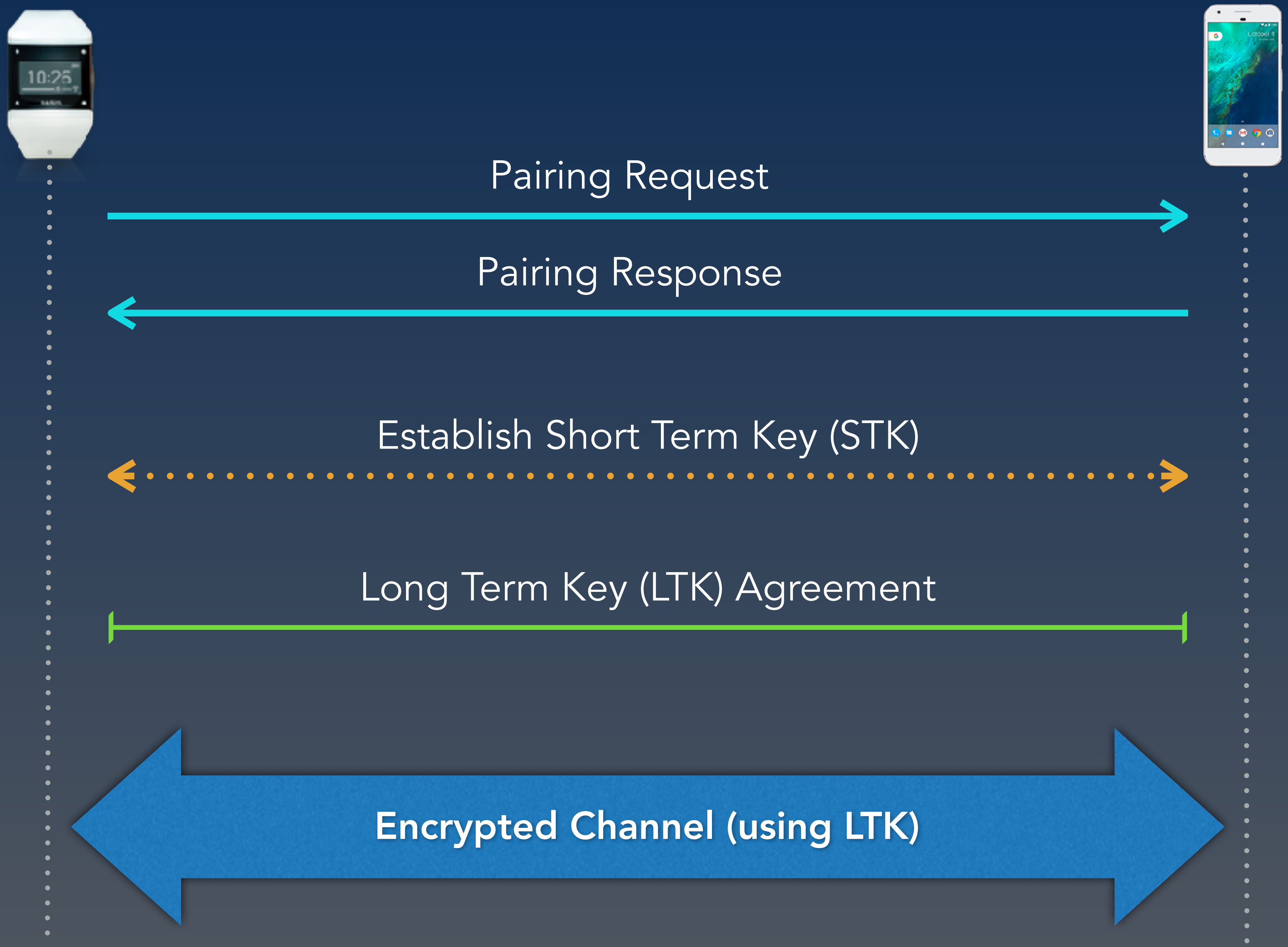
ATT
Simple Client/ Server stateless protocol with rules for accessing data on a peer device

L2CAP
Multiplexing layer for BLE

Intro to BLE

- Wireless protocol for short range data exchange (~10 to 100 m)
- Light-weight subset of classic Bluetooth with low power consumption
- Operates in radio frequencies between 2.4 to 2.485 GHz
- Managed by the Bluetooth Special Interest Group (SIG)
- Use cases include wearable devices, smart pay systems, smart security systems etc

BLE Security



Pairing Request

Pairing Response

Establish Short Term Key (STK)

Long Term Key (LTK) Agreement

Encrypted Channel (using LTK)

Pairing Algorithms

Secure Simple Pairing

- Just Works: very limited/ no user interface
- Numeric Comparison: devices with display plus yes/ no button
- Passkey Entry: 6 digit pin as the pass key
- Out Of Band: Use of an out of the band channel against MITM attacks

Security weaknesses in BT/BLE

- Security of the communication link depends on pairing algorithm
- Eavesdropping on pairing mechanism compromises encryption keys
- ‘Just works’ mode prone to MITM attacks
- Apps (on the same phone as the companion app) snooping on encrypted BLE traffic
    - Our talk yesterday

BT/BLE Security - Tools

- Ubertooth
- Bluefruit LE sniffer
- NRFsniffer (Nordic BLE sniffer)
- Ellisys sniffer

Exercise 2

BLE packet eavesdropping with Ubertooth

Overview

- Market products for fitness tracking
- Use Bluetooth Low Energy
- Packet sniffing, capture and cracking LE encryption
- Goals:
    - BLE traffic eavesdropping
    - Tools to crack the basic security offered by BLE spec

Tools

- Ubertooth One
  - Great Scott Gadgets
  - 2.4 GHz wireless deployment platform for BT experimentation
- Wireshark
- “Malware” Android app and logcat
- Mike Ryan’s crackle

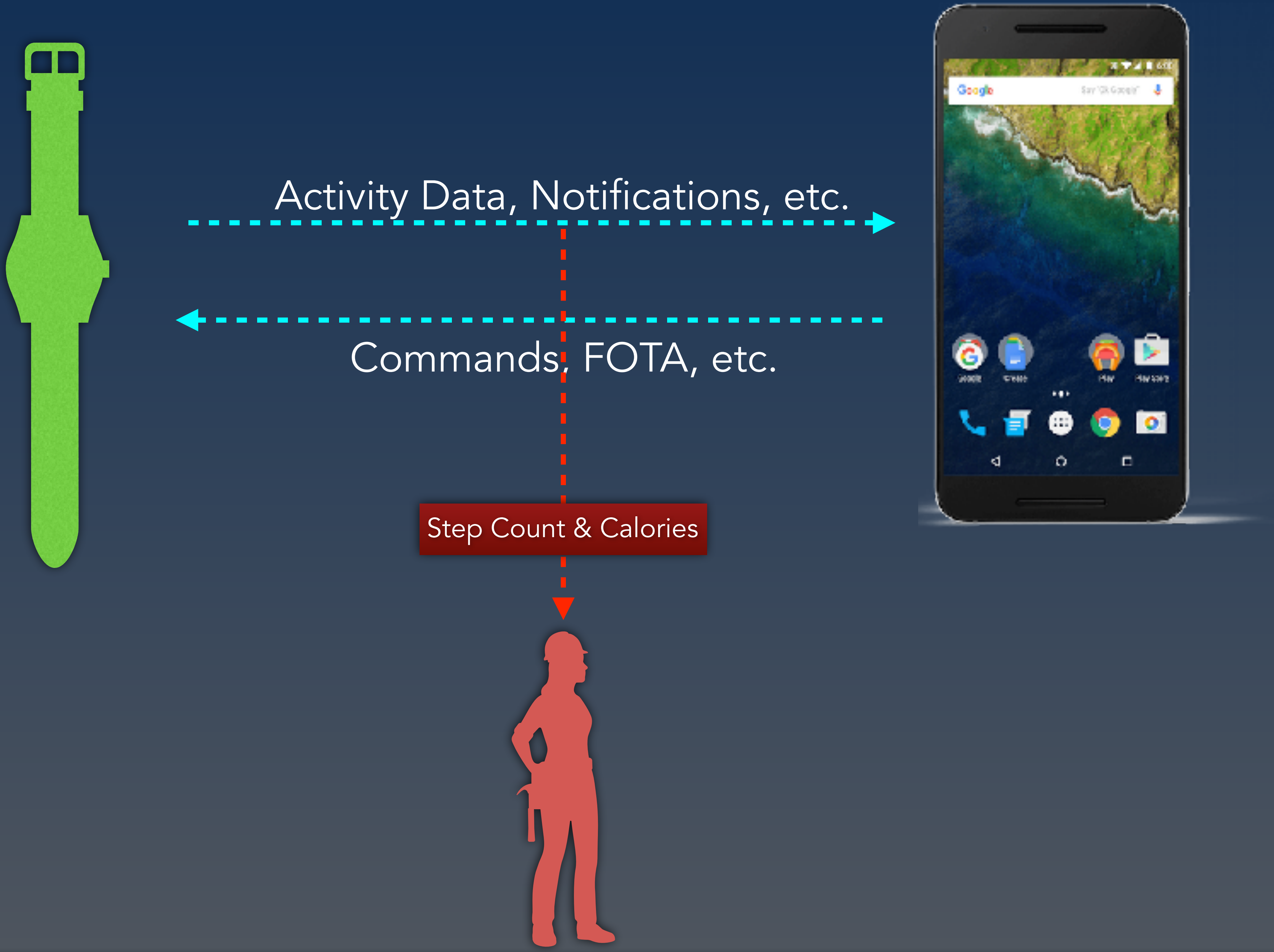
Problems & Packet Injection

- Multiple advertising channels (37, 38, 39)
- Uncertainty —> 3 Ubertooths are better than 1
- Custom FW for packet injection

Scenario 1

Packet sniffing — ‘X’ Fitness Band

Outline

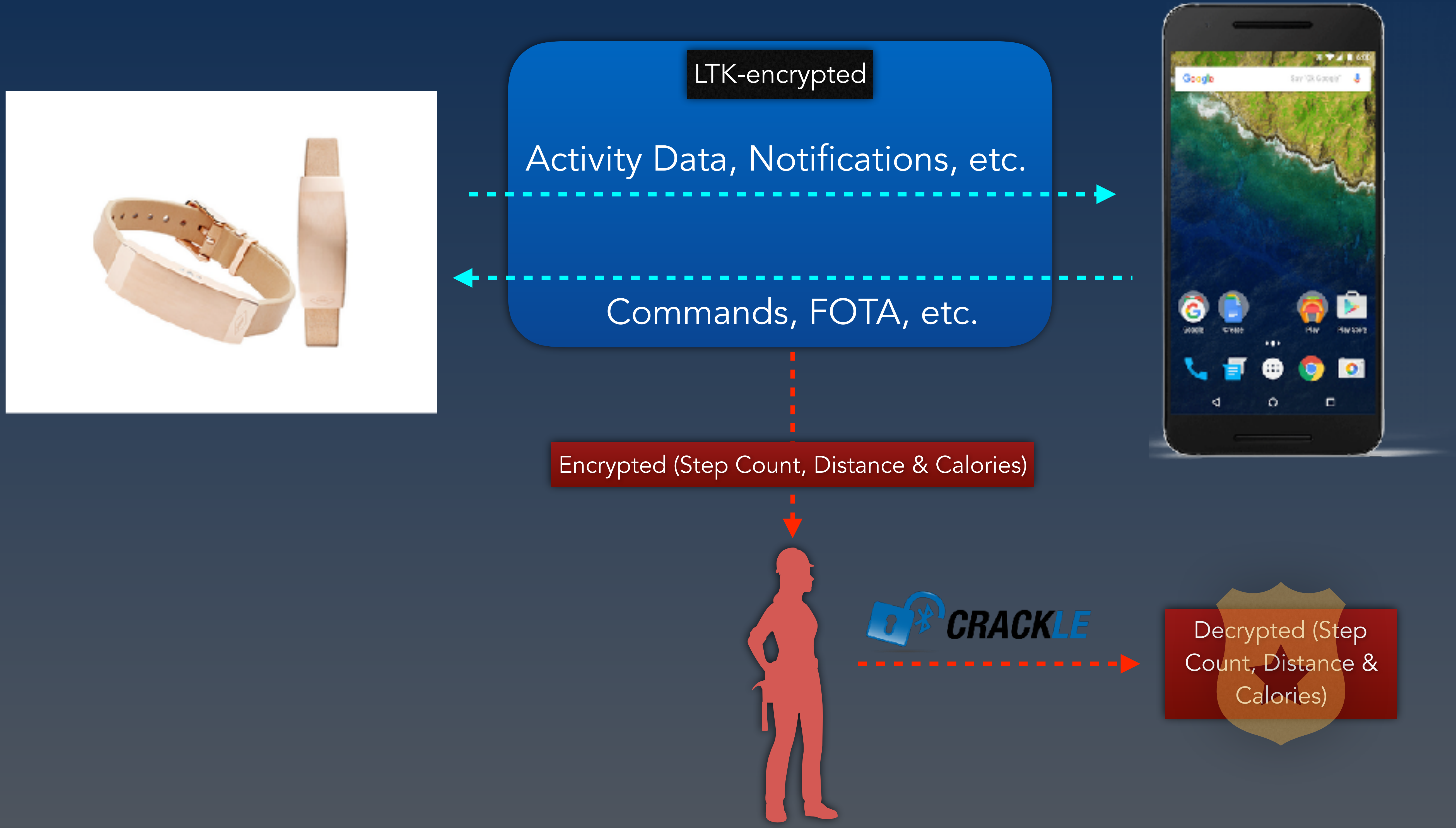

Activity Data, Notifications, etc.
Commands, FOTA, etc.
Step Count & Calories

Demo

Scenario 2

Packet sniffing & LE Encryption cracking — Fossil Q

Outline



LTK-encrypted

Activity Data, Notifications, etc.

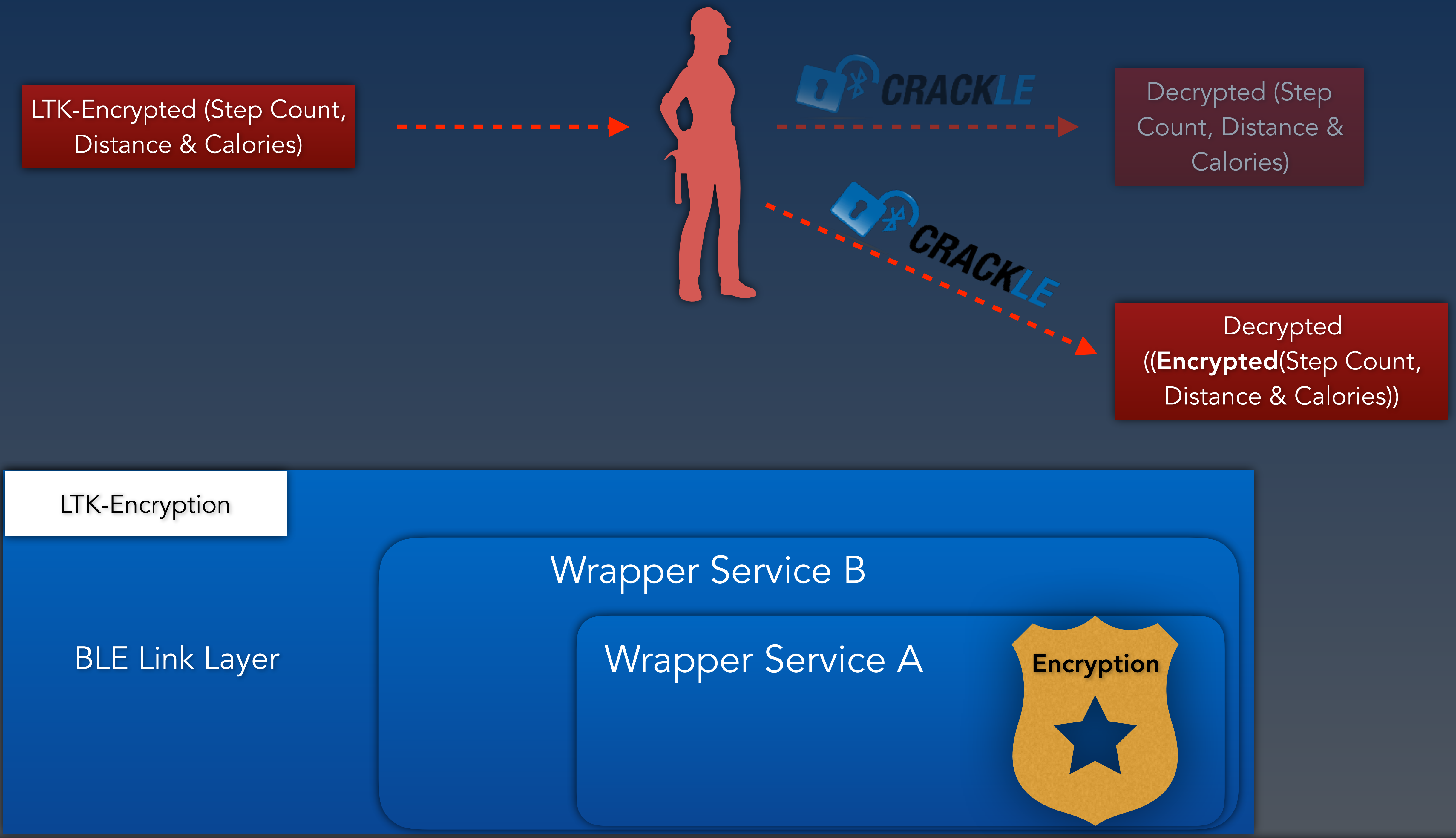
Commands, FOTA, etc.

Encrypted (Step Count, Distance & Calories)

Decrypted (Step Count, Distance & Calories)

Demo

What happened there?



LTK-Encrypted (Step Count, Distance & Calories)

Decrypted (Step Count, Distance & Calories)

Decrypted ((**Encrypted**(Step Count, Distance & Calories))

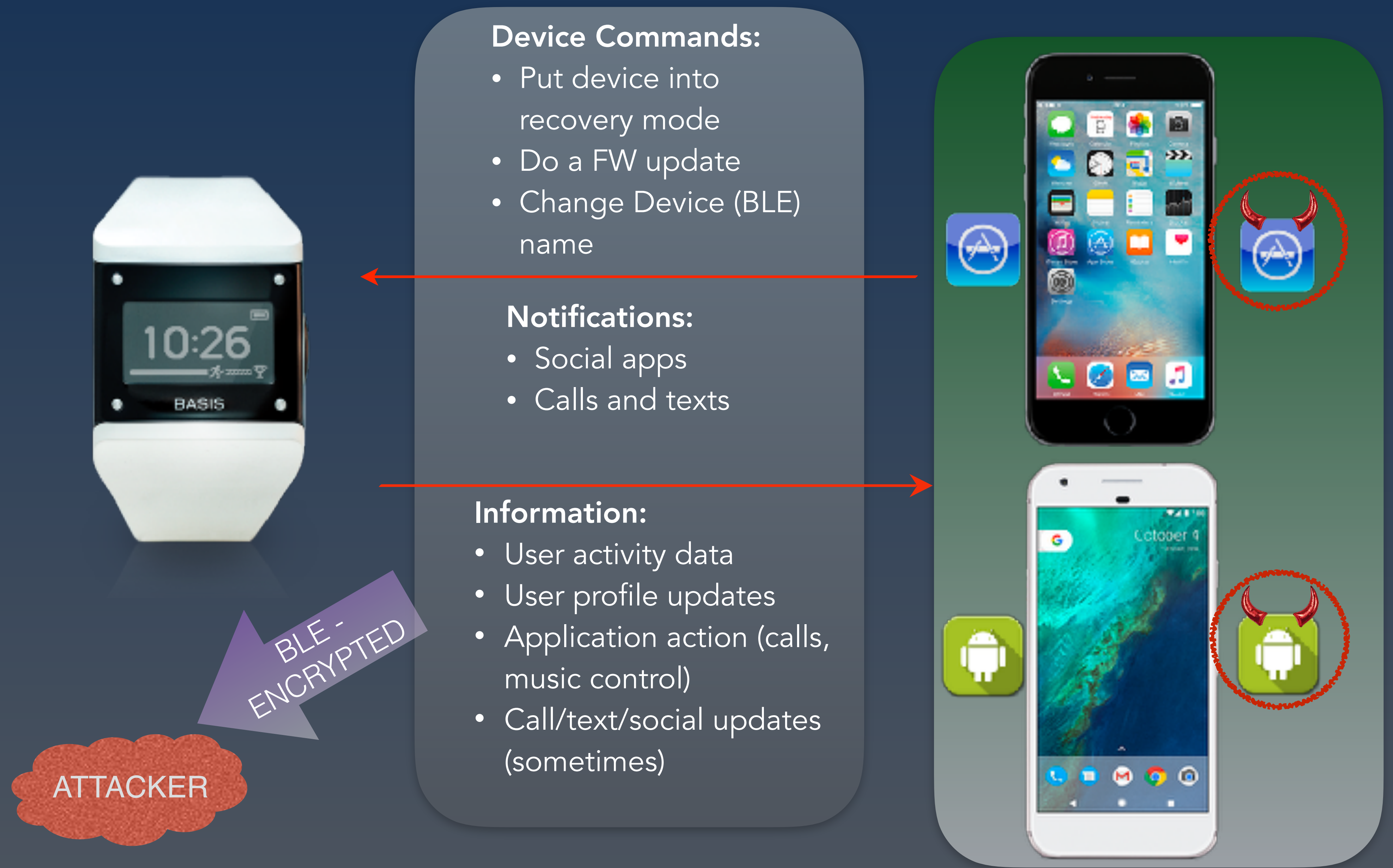
LTK-Encryption

BLE Link Layer

Wrapper Service B

Wrapper Service A

BT/BLE problems with Android and iOS



Device Commands:

- Put device into recovery mode
- Do a FW update
- Change Device (BLE) name

Notifications:

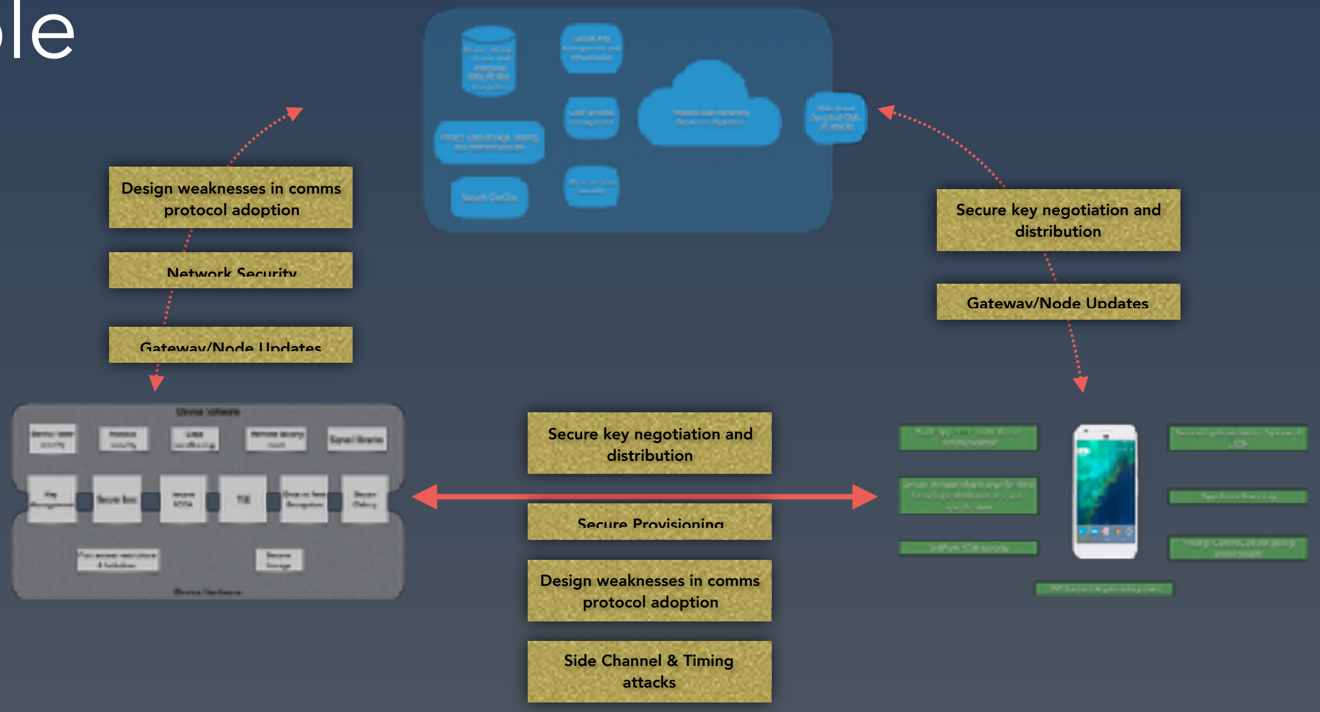
- Social apps
- Calls and texts

Information:

- User activity data
- User profile updates
- Application action (calls, music control)
- Call/text/social updates (sometimes)

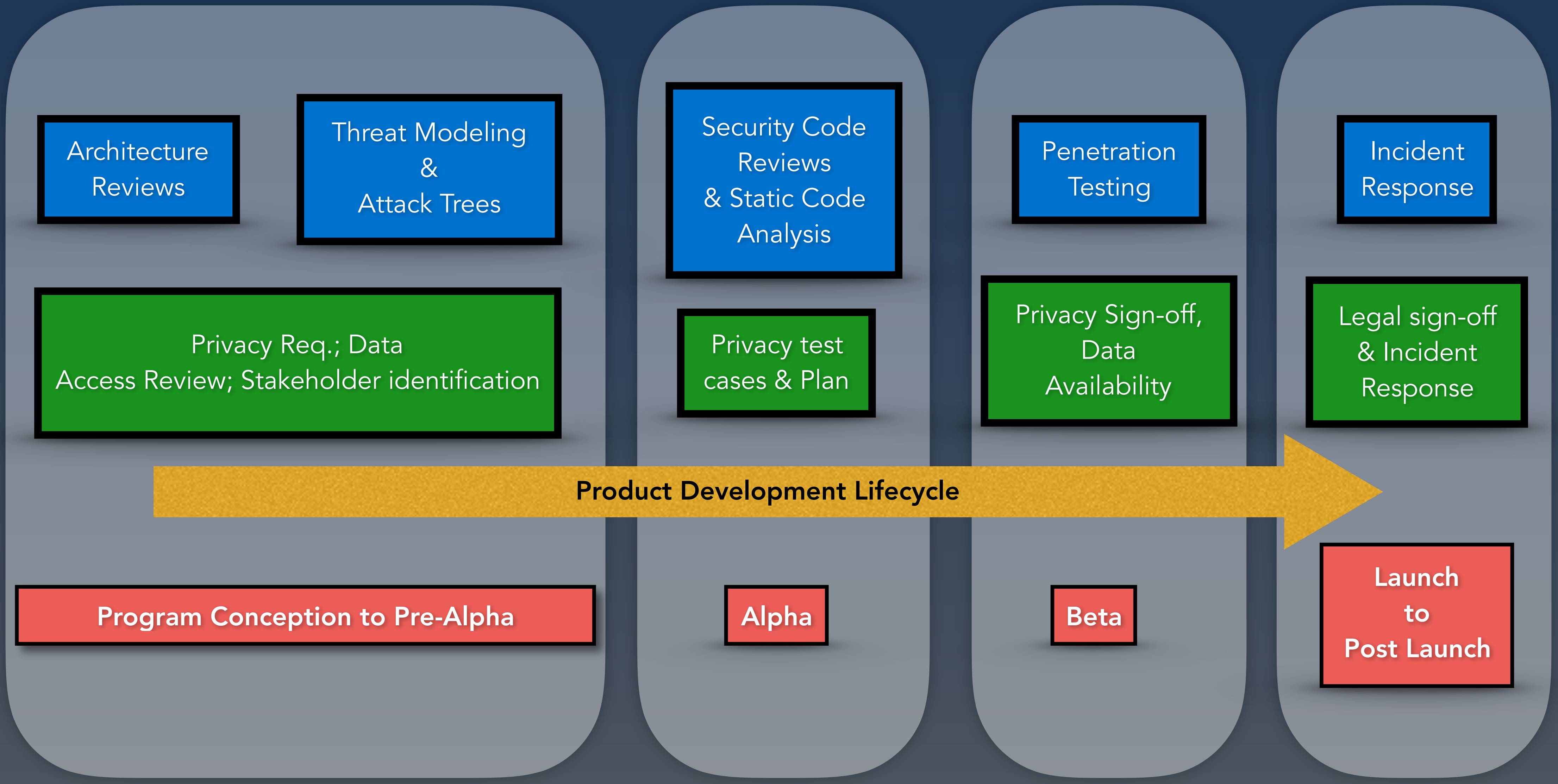
Secure by Design for IoT

- Starts with architecture and product design
  - Multi-device crypto flows
  - In-field read/write disable
- Shift-left
- Ecosystem security


Design weaknesses in comms protocol adoption
Network Security
Gateway/Node Updates
Secure key negotiation and distribution
Gateway/Node Updates
Secure key negotiation and distribution
Secure Provisioning
Design weaknesses in comms protocol adoption
Side Channel & Timing attacks

Unshackling from traditional SDL

Security & Privacy Development Lifecycle



Architecture Reviews

Threat Modeling & Attack Trees

Privacy Req.; Data Access Review; Stakeholder identification

Program Conception to Pre-Alpha

Security Code Reviews & Static Code Analysis

Privacy test cases & Plan

Alpha

Penetration Testing

Privacy Sign-off, Data Availability

Beta

Incident Response

Legal sign-off & Incident Response

Launch to Post Launch

Product Development Lifecycle

Privacy

- Why worry?
  - Global Markets
  - Country-specific guidelines
  - Ecosystems and overlapping policies

Quantifying Privacy Vulnerabilities

- <quote>*Common Vulnerability Scoring System (CVSS) is a free and open industry standard for assessing the severity of computer system security vulnerabilities* </quote>

- Privacy vulnerabilities?

- CVSS Extensions Framework
  - Allowing CVSS to be extensible by third parties

Summary

- Plethora of protocols (and standards)
- Custom hardware & software for IoT comms penetration testing
- RZUSBStick works great. Also, APImote
  - Not much else
- BT/BLE sniffing is still sketchy
- SDL/SPDL and Shift-left

DEEP ARMOR

SDL

Vulnerability Assessments

Security Consulting

Trainings

www.deeparmor.com | @deep_armor | services@deeparmor.com