ELL365: Embedded Systems

Lecture on Introduction to Embedded System Security

Vireshwar Kumar
CSE@IITD

February 12, 2024

Semester II
2023-2024

Agenda

- Cryptographic Operation Costs
- Fundamental Challenge in Embedded System Security
- Example of a Security Protocol in Conventional Computer Network
  - Transport Layer Security (TLS)
- Example of a Security Protocol in Embedded System
  - Bluetooth Security
- Explanation of an Attack on Bluetooth

Cryptography Overview

	Symmetric Key Setting	Asymmetric Key Setting
Secrecy / Confidentiality	Block Cipher	Public Key Encryption
Authenticity / Integrity	Hash-Based Message Authentication Code	Digital Signature

Overhead (9^{th} Gen i7 Processor, 16 GB RAM)

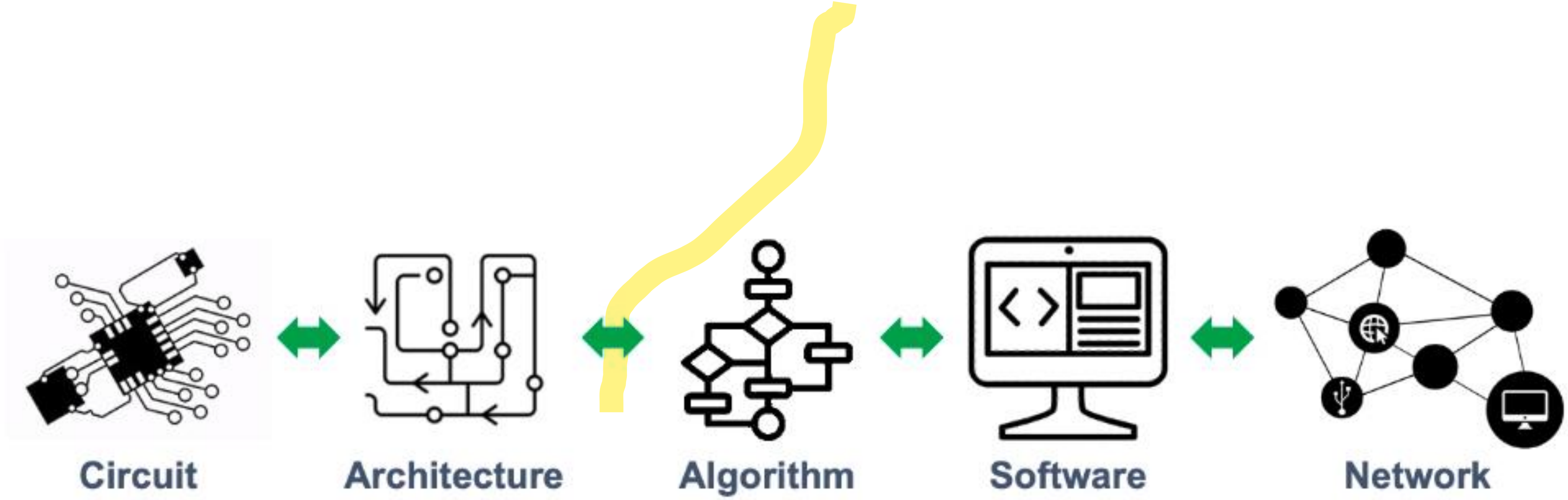
Encryption Algorithm	Key Length (bits)	Execution Time (ms)	Block Length (bits)
Symmetric Key Encryption AES-CBC	128	0.5	128
Public Key Encryption RSA	2048	5.0	2048

Authentication Algorithm	Key Length (bits)	Execution Time (ms)	Tag Length (bits)
Symmetric Key Authentication SHA3-HMAC	128	0.1	256
Digital Signature RSA-SHA3	2048	50.0	2048

Resource-Constraints in Embedded Devices

	Typical Desktop	Typical IoT Device
Computation (Clock Frequency)	2 GHz	20 MHz
Communication (Packet Length)	16 KB	16 B
Storage (RAM)	16 GB	2 KB

Embedded System Security



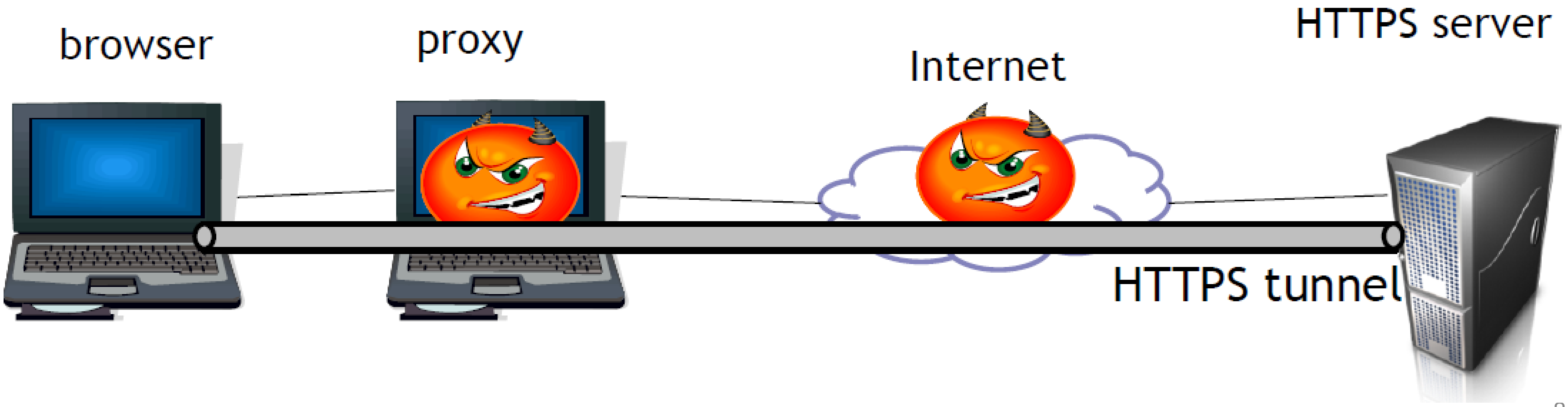
Transport Layer Security (TLS)

- Secure communications in the presence of an attacker who can
  - own the network
  - control Wi-Fi, DNS, routers
  - can listen to any packet
  - modify packets in transit
  - inject packets into the network

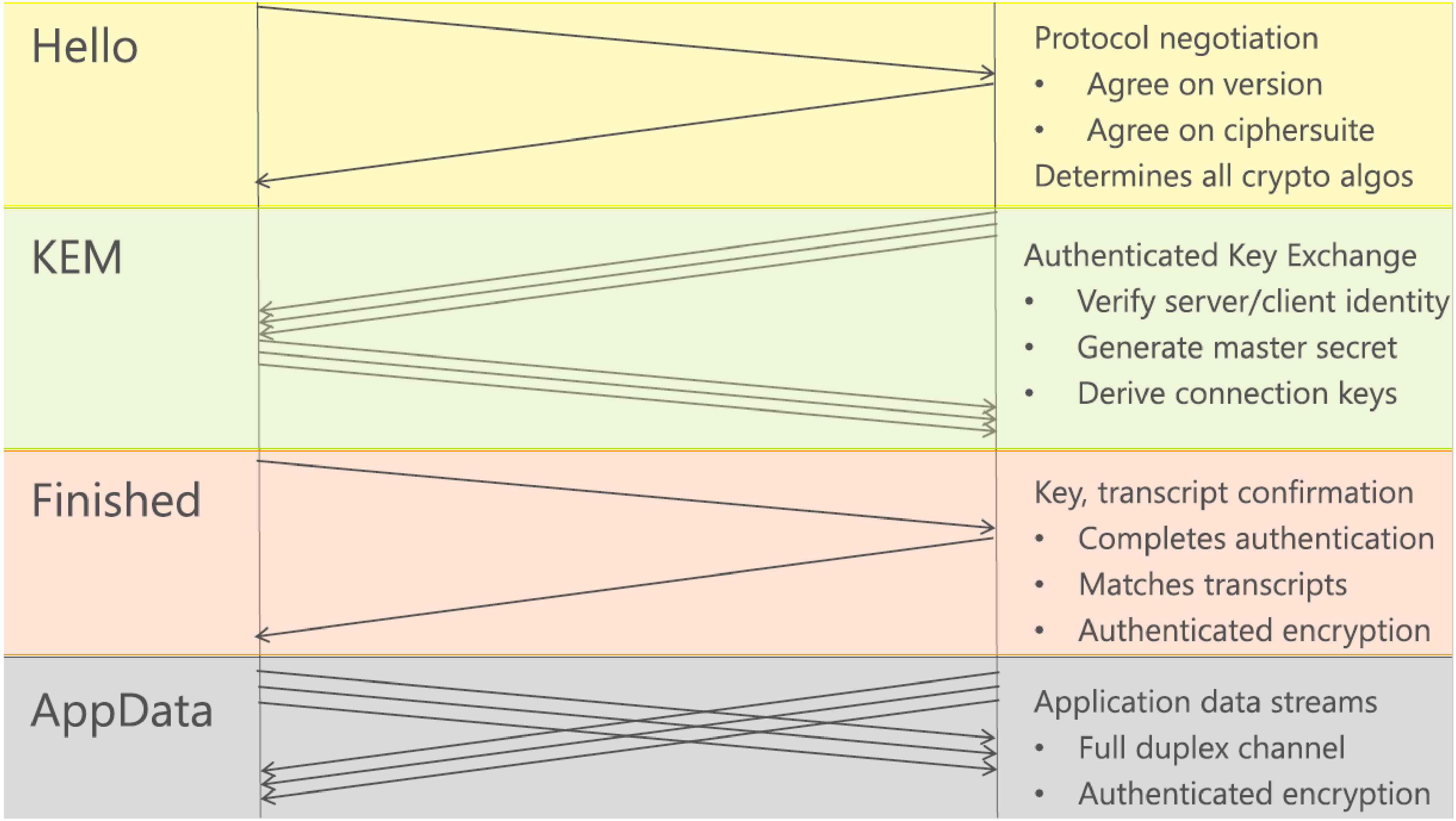
- Scenario: Internet Success Story using TLS
  - You are reading your email from an Internet cafe connected via a Wi-Fi access point to a sketchy ISP in a hostile authoritarian country

HTTPS (HTTP over SSL/TLS)

- HTTPS: end-to-end secure protocol for Web (Hypertext Transfer Protocol)
  - Encryption
  - Authentication (usually for server only)
  - Integrity protection

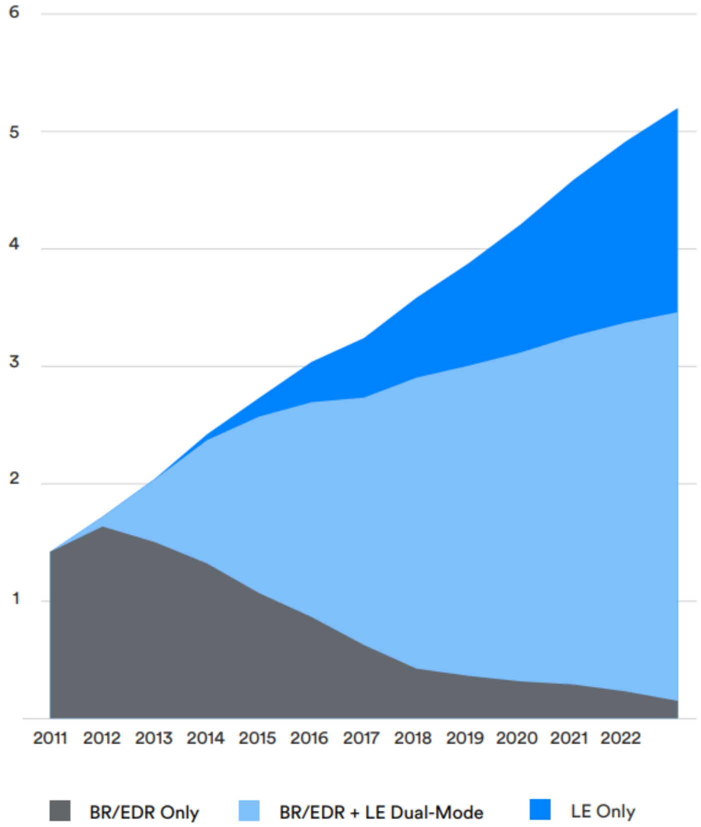


TLS Message Exchange



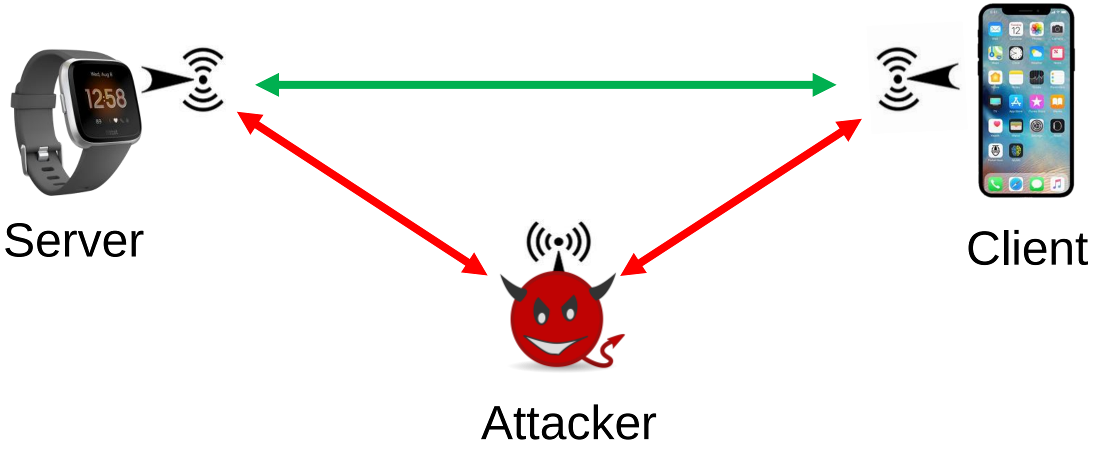
Bluetooth Low Energy (BLE)

- Number of devices: 4 billion
  - Smart home
    - Smart bulb
  - Wearable
    - Smart watch
  - Health care
    - Smart glucose monitor
    - Aarogya Setu



Number of Bluetooth equipped devices

Wireless Medium: Threat Model



- *Client* and *Server*: communicate messages on a wireless channel
- *Attacker*: eavesdrop, intercept, and modify legitimate messages

BLE Link-Layer Security Mechanism

- Defined: Security Level
  - Level 1: No security
  - Level 2: Encryption
  - Level 3: Encryption and authentication
  - Level 4: New encryption and authentication

Device
without I/O

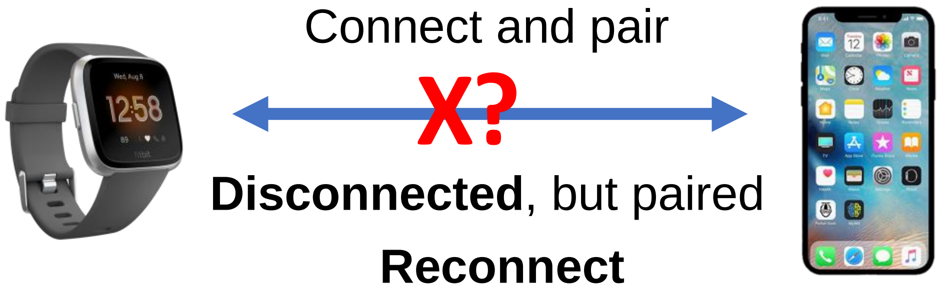
- Real-World: Security Level
  - Without I/O: Level 2 (no authentication)
  - With I/O: Level 3 and 4

Device
with I/O

- Level in Aarogya Setu?

Attack Surface Investigation

- Prior Work
  - Target the pairing procedure during the initial connection
  - Malicious software on the client
- Reconnection procedure: Unexplored



Discovered Vulnerabilities and Attack

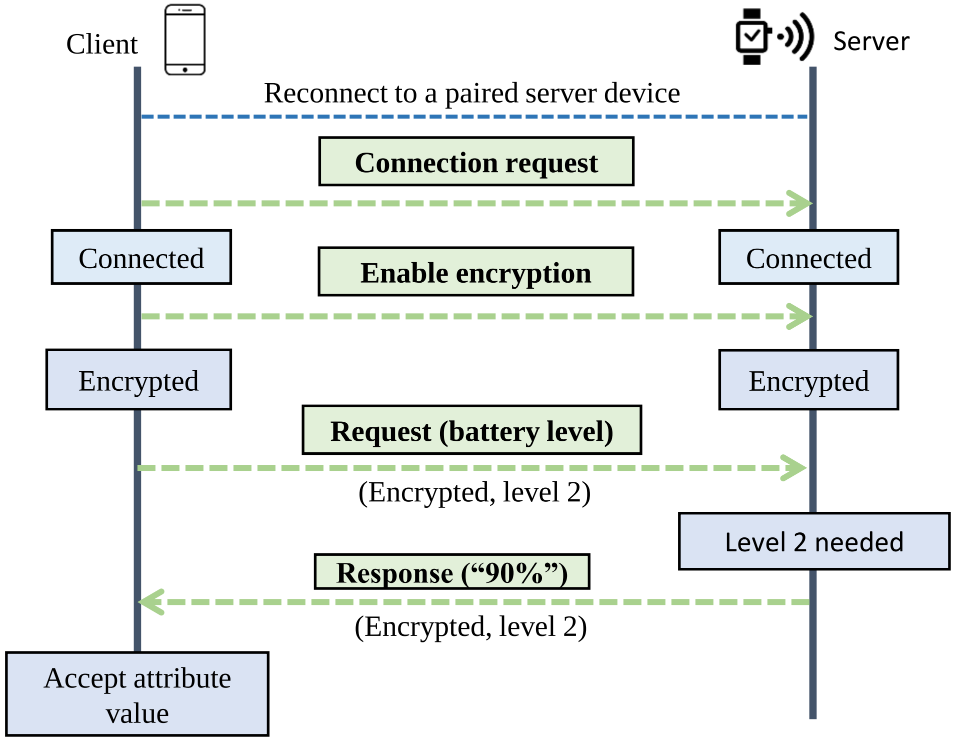
- Two **design** vulnerabilities - lack of authentication
  - Formal analysis of BLE connection procedure

- One **implementation** vulnerability - bypass authentication
  - Examination of real-world BLE devices

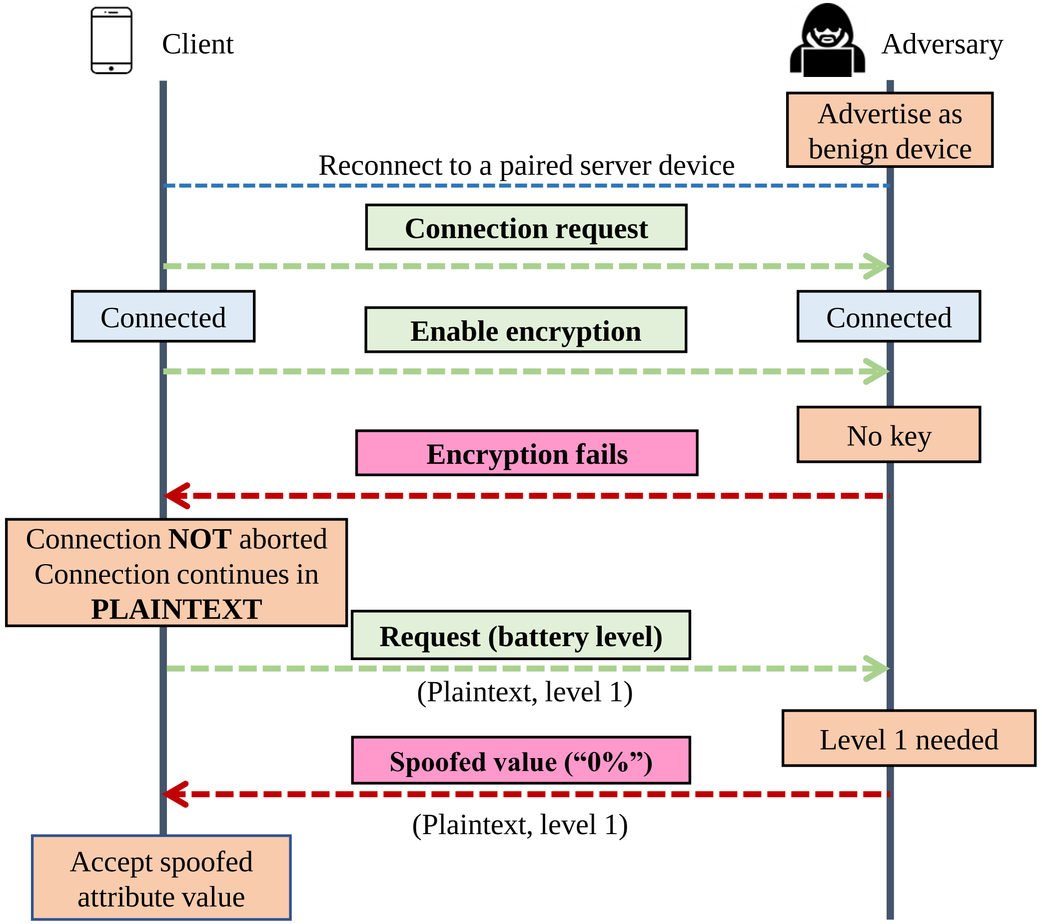
- Vulnerabilities >>> BLE Spoofing Attack (**BLESA**)

BLESA: Step by Step

Benign Scenario



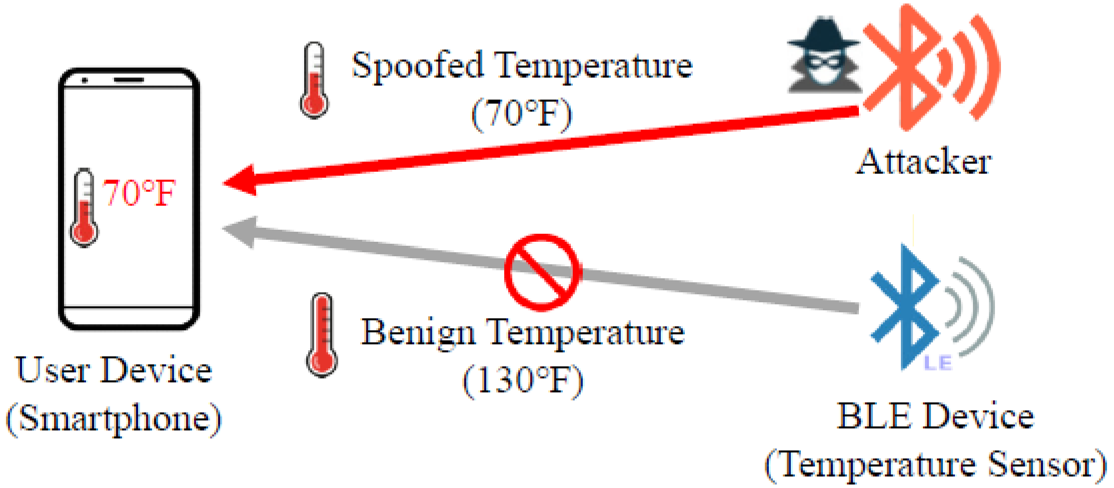
BLESA



Formal Analysis and Findings

- Formal model
  - Modeling BLE reconnection procedure using **ProVerif**
  - Verifying security properties
    - Confidentiality, Integrity, and Authenticity

- Identified Weaknesses
  - Optional authentication
  - Circumventing authentication
    - Design issue
    - *Potential* for Implementation issue



Design Vulnerability

- Whether the BLE apps use authentication during reconnection?
  - No authentication: **86/127 (67.7%)**

- Whether the real-world server BLE devices use authentication during reconnection?
  - No authentication: **10/12**

Device Name	Auth.
Nest Protect Smoke Detector	×
Nest Cam Indoor Camera	×
SensorPush Temperature Sensor	×
Tahmo Tempi Temperature Sensor	×
August Smart Lock	×
Eve Door & Window Sensor	×
Eve Button Remote Control	×
Eve Energy Socket	×
Ilumi Smart Light Bulb	×
Polar H7 Heart Rate Sensor	×
Fitbit Versa Smartwatch	√
Oura Smart Ring	√

Implementation Vulnerability

- Can we circumvent the authentication procedure?

Platform	OS	BLE Stack	Vulnerable
Linux Laptop	Ubuntu 18.04	BlueZ 5.48	**Yes**
Google Pixel XL	Android 8.1, 9, 10	Fluoride	**Yes**
iPhone 8	iOS 12.1, 12.4, 13.3.1	iOS BLE stack	**Yes**
Thinkpad X1 Yoga	Windows 10 V. 1809	Windows stack	No

Thanks!