BLESA: Spoofing Attacks against Reconnections in Bluetooth Low Energy

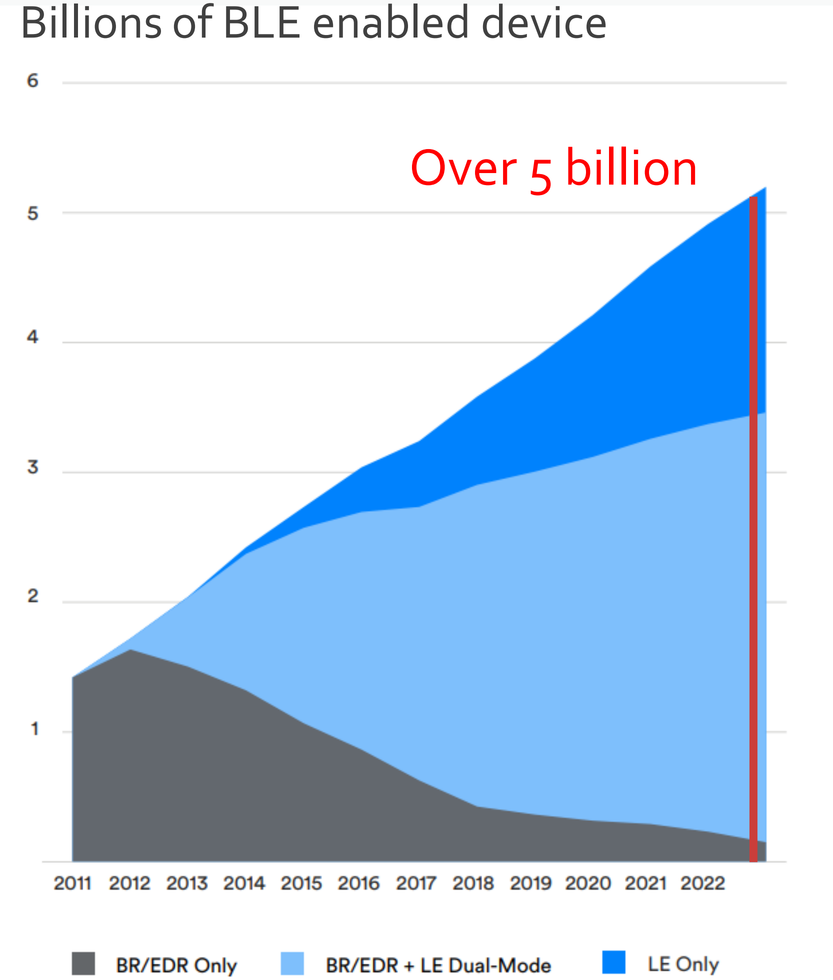
Jianliang Wu[1], Yuhong Nan[1], Vireshwar Kumar[1], Dave (Jing) Tian[1], Antonio Bianchi[1], Mathias Payer[2], Dongyan Xu[1]

[1] Purdue University [2] EPFL

Motivation

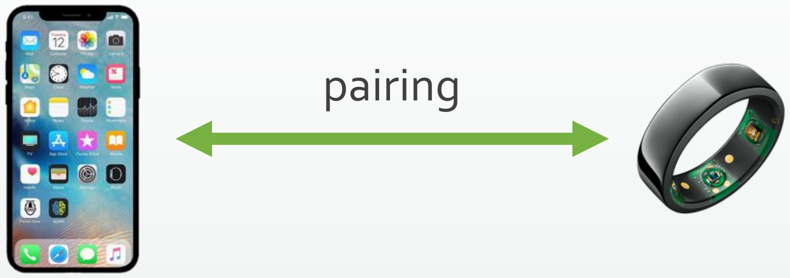
- Bluetooth Low Energy (BLE) devices are ubiquitous
  - Smart home devices
    - Smart temperature sensor

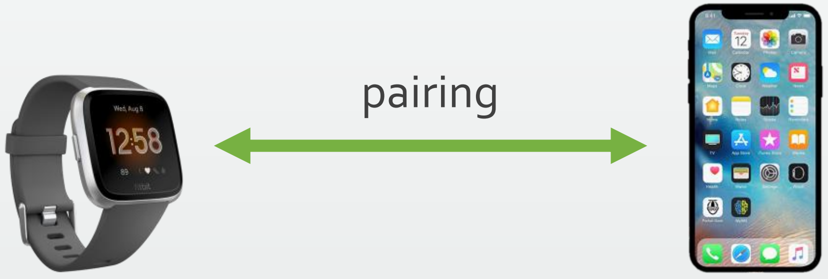
  - Health care devices
    - Smart glucose monitor

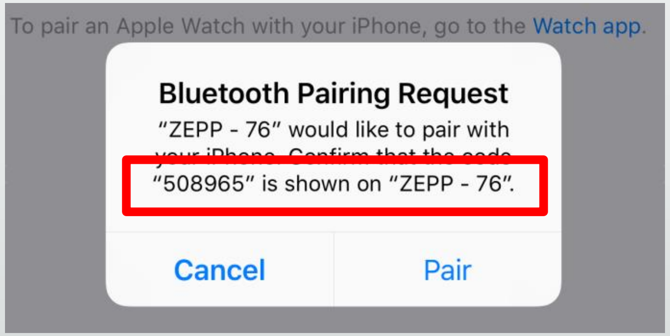


Motivation

- BLE security mechanism
  - Security level
    - Level 1
      - No security
    - Level 2
      - Encryption
    - Level 3 and 4
      - Encryption and authentication
  - Bluetooth pairing
    - No I/O interfaces
      - Level 2 (unauthenticated key)
    - With I/O interfaces
      - Level 3 and 4 (authenticated key)



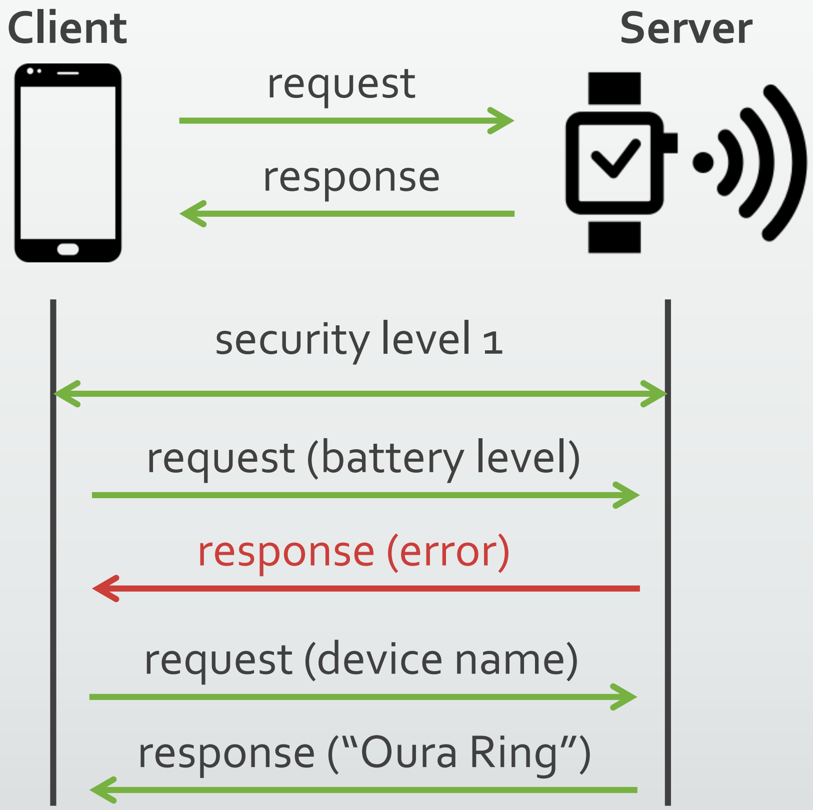




Motivation

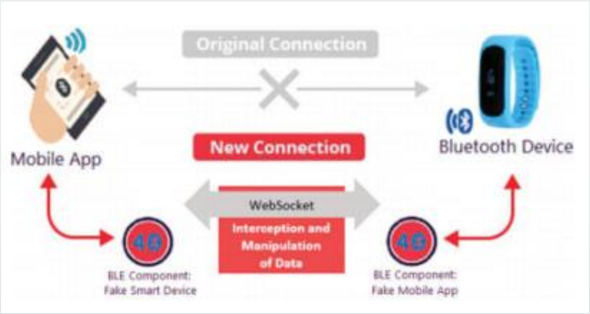
Attribute	Value	Security Requirement
Device Name	"Oura Ring"	Level 1
Battery level	"90%"	Level 2

- BLE security mechanism
  - Server-client architecture
    - BLE uses request and response scheme
    - Data is stored as attribute on server device
    - Each attribute has security requirements
  - Server-side security enforcement
    - Server checks whether the current security level match the requirement or not



Motivation

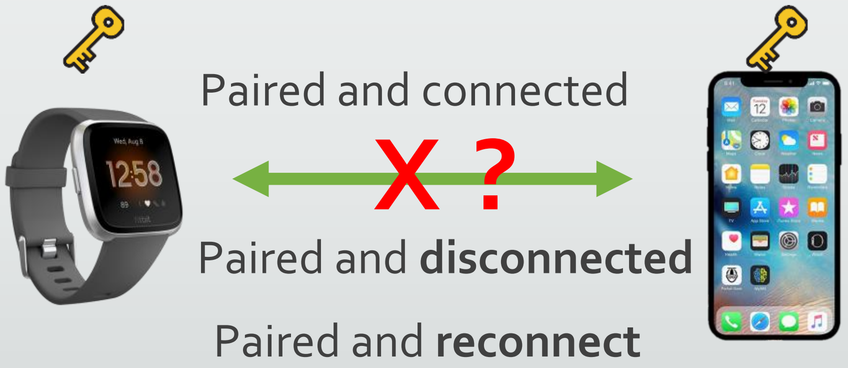
- Attacks on BLE
  - Eavesdropping[1]
  - Illegal access by compromising client BLE device [2]
    - Reading glucose level
    - Opening smart lock
  - Man-In-The-Middle Attacks against *unpaired* BLE devices[3]
    - Manipulating user data



[1]. Mike Ryan. Bluetooth: *With low energy comes low security*. In proceedings of the USENIX Workshop on Offensive Technologies (WOOT), 2013.
[2]. Pallavi Sivakumaran and Jorge Blasco. *A study of the feasibility of co-located app attacks against BLE and a largescale analysis of the current application-layer security landscape*. In Proceedings of the USENIX Security Symposium (USENIX Security) 2019
[3]. Tal Melamed. *An active man-in-the-middle attack on Bluetooth smart devices*. International Journal of Safety and Security Engineering, 8(2), 2018

Motivation

- Prior attacks on BLE
  - Some attacks target the pairing procedure for **first-connection** and **unpaired devices** [WOOT'13, blackhat'16]
  - Some other attacks need **additional assistance** [NDSS'14, SEC'19, NDSS'19]
    - Malicious app on the phone
- Unexplored reconnection procedure



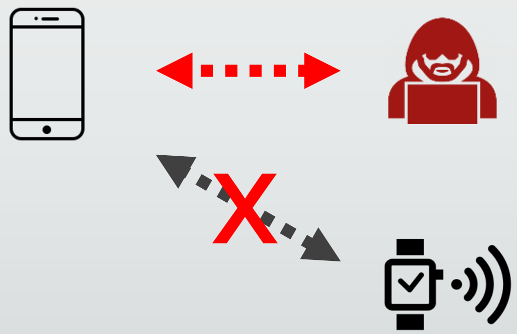
Our Work

- Formal analysis of BLE ***reconnection*** procedure
  - Two design weaknesses identified
- BLE Spoofing Attacks (BLESA) against ***paired*** devices ***without*** extra assistance
  - Do not need malicious apps
- Evaluation on real-world BLE devices
  - Affecting more than 1 billion real-world BLE devices and 16,000 BLE apps

Formal Analysis and Findings

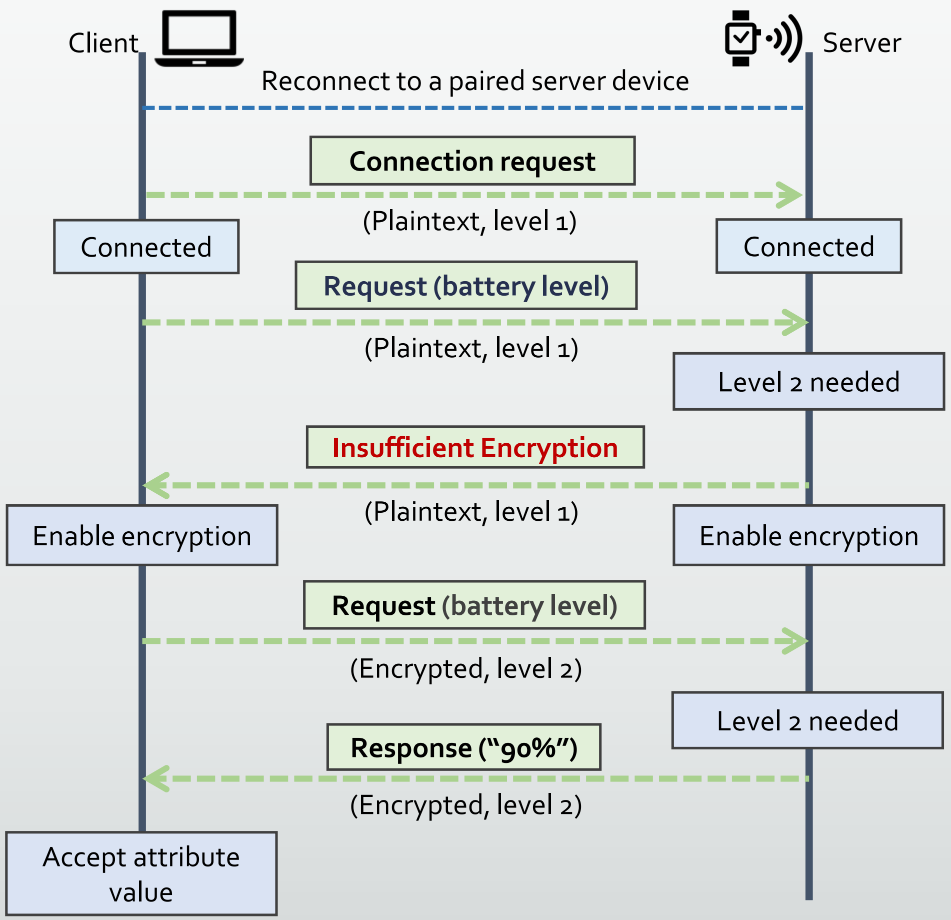
- Formal model
  - Modeling BLE reconnection procedure using ProVerif
  - Verifying security properties
    - Confidentiality, Integrity, and Authenticity
- Identified Weaknesses
  - Optional authentication
  - Circumventing authentication
    - Reactive authentication
      - Design issue
    - Proactive authentication
      - Implementation issue

BLE Spoofing Attacks (BLESA)

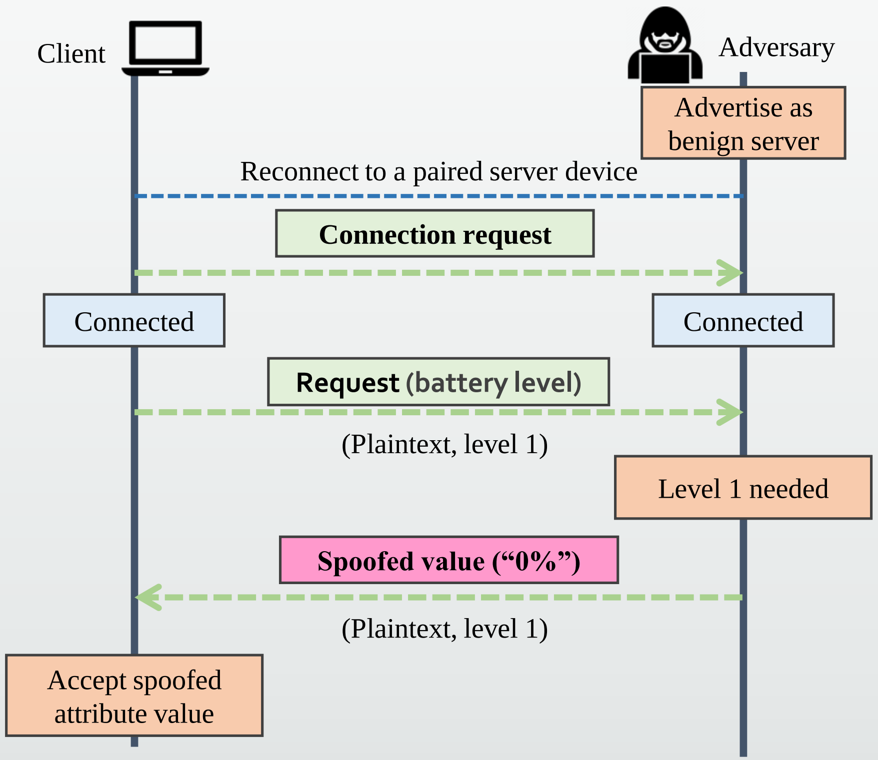


BLESA against Reactive Authentication

Reactive authentication



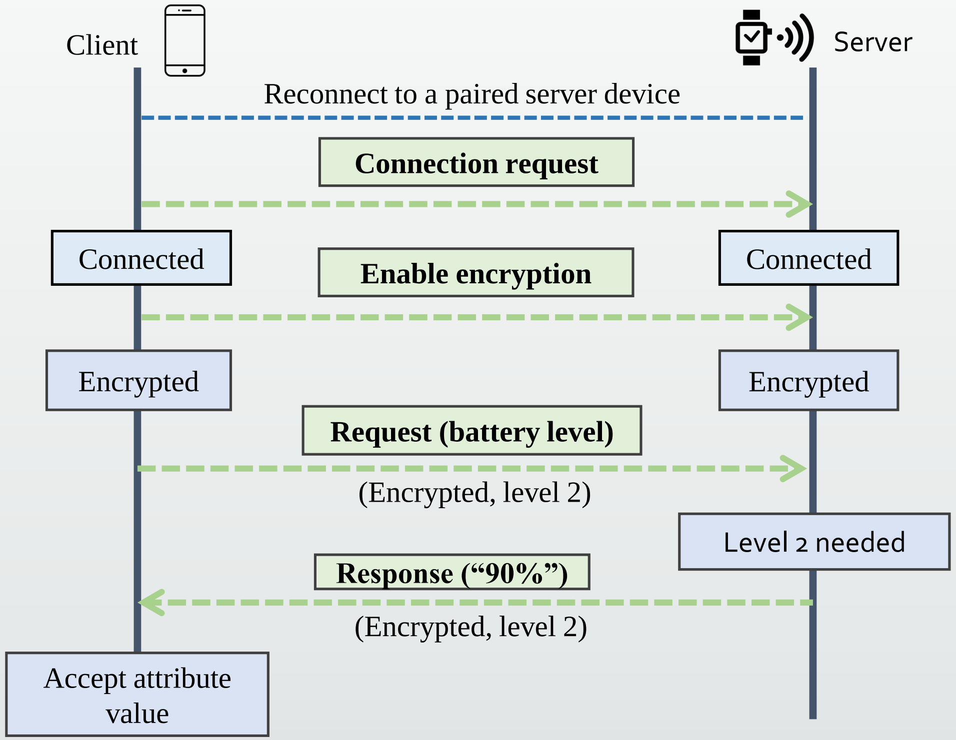
Attack reactive authentication



Attribute	Value	Security Requirement
Battery level	"90%"	Level 2

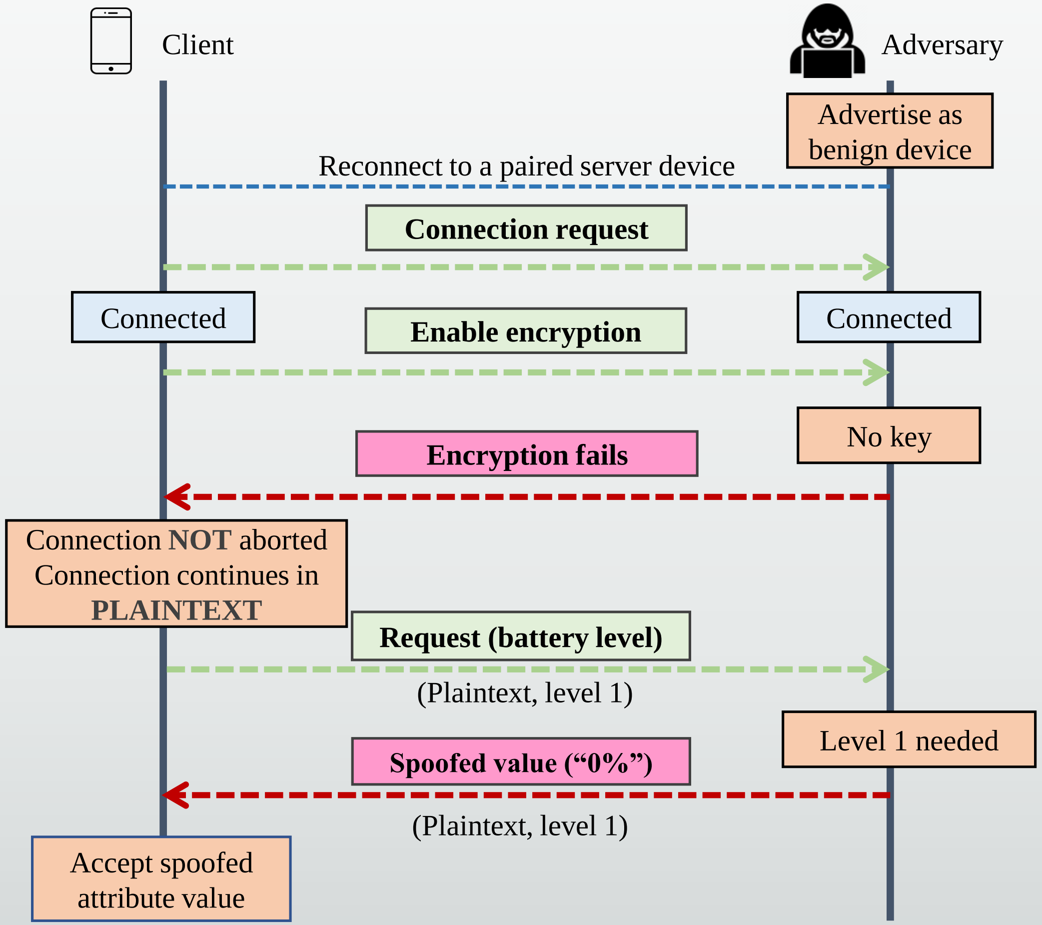
BLESA against Proactive Authentication

Proactive authentication



Attribute	Value	Security Requirement
Battery level	“90%”	Level 2

Attack proactive authentication



Evaluation and Impact

- Weakness 1 (optional authentication) examination
  - Whether the BLE apps use authentication during reconnection?
  - Whether the real-world server BLE devices use authentication during reconnection?

- Weakness 2 (circumventing authentication) examination
  - Which authentication procedure is during reconnection used by main-stream BLE stacks?
  - Whether the used authentication procedure is vulnerable to BLESA?

Evaluation and Impact

- Weakness 1 (optional authentication)
  - Whether the BLE apps use authentication during reconnection?
    - Analyzing BLE apps
    - 86/127 (67.7%) of analyzed BLE apps **do not** use authentication during reconnection
  - Whether the real-world server BLE devices use authentication during reconnection?
    - Analyzing real-world server BLE devices
    - 10/12 of analyzed BLE devices **do not** support authentication during reconnection

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	√

Evaluation and Impact

- Weakness 2 (circumventing authentication)
  - Which authentication procedure is used for main-stream BLE stacks?
  - Whether the authentication procedure is vulnerable to BLESA?
    - Analyzing main-stream BLE stacks

Platform	OS	BLE Stack	Authentication	Issue	Vulnerable
Linux Laptop	Ubuntu 18.04	BlueZ 5.48	Reactive	Design	**Yes**
Google Pixel XL	Android 8.1, 9, 10	Fluoride	Proactive	Implementation	**Yes**
iPhone 8	iOS 12.1, 12.4, 13.3.1	iOS BLE stack	Proactive	Implementation	**Yes**
Thinkpad X1 Yoga	Windows 10 V. 1809	Windows stack	Proactive	None	No

Evaluation and Impact

BLESA against Oura Ring Demo

Evaluation and Impact

- Impact
  - Affected BLE apps
    - At least 8,000 Android BLE apps with 2.38 billion installations[1]
    - Similar number may apply to iOS apps
  - Affected server BLE devices
    - More than 1 billion BLE devices[1]
  - Medeia report
    - Security Boulevard

Bluetooth Reconnection Flaw Could Lead to Spoofing Attacks

by Joan Goodchild on July 20, 2020

A group of researchers at Purdue University's Center for Education and Research in Information Assurance and Security (CERIAS)

[1]. Pallavi Sivakumaran and Jorge Blasco. *A study of the feasibility of co-located app attacks against BLE and a largescale analysis of the current application-layer security landscape*. In Proceedings of the USENIX Security Symposium (USENIX Security) 2019

Evaluation and Impact

- Responsible disclosure
  - Apple Product Security
    - CVE-2020-9770
  - Android Security Team
    - Reported on April 8, 2019

The Android Security Team believes that this is a duplicate of a report previously submitted by another external researcher on Apr 5, 2019.

The duplicate issue is being tracked by AndroidID-130833727.

Thank you,
Android Security Team

Mitigations

- Reactive authentication
  - Updating specification
    - Removing reactive authentication
    - Exchanging attributes' security requirements during pairing
- Proactive authentication
  - Fixing vulnerable implementations
    - iOS BLE stack
      - Apple issued iOS 13.4 and iPadOS 13.4 to fix the vulnerability
    - Android BLE stack (Fluoride)
    - Linux BLE stack (BlueZ)
      - Changing to proactive authentication

Summary

- Formal analysis of the BLE reconnection procedure
- BLESA against paired BLE devices
- Evaluation on real-world BLE devices

Thank you! Questions?

This work was supported in part by ONR under Grant N00014-18-1-2674.

wu1220@purdue.edu

PURDUE UNIVERSITY CERIAS