IoT Security

IoT: Internet of things

- Hidden Voice Commands, *Usenix Security'16*
  - *Presented by Jinli Zhong*
- FBS-Radar: Uncovering Fake Base Stations at Scale in the Wild, *NDSS'17*
  - *Presented by Jie Li*
- Protecting Privacy of BLE Device Users, *Usenix Security'16*
  - *Presented by Wei Zhang*

Protecting Privacy of BLE Device Users

Kassem Fawaz*, Kyu-Han Kim†, Kang G. Shin*

*The University of Michigan

†Hewlett Packard Labs

Presented by Wei Zhang

Outline

- Introduction
- BLE Primer
- Threats from BLE Devices
- BLE-Guardian
- Implementation and Evaluation
- Summary

Outline

- Introduction
- BLE Primer
- Threats from BLE Devices
- BLE-Guardian
- Implementation and Evaluation
- Summary

Internet of Things

What is BLE?

- BLE: Bluetooth Low Energy
  - Attractive communication protocol in IoT
    - Short range
    - Low energy footprint
    - Supported by most hosts
  - Popularity
    - Currently: 74K unique products with BLE support
    - 2013: 1.2 billion BLE products shipped
    - 2020: 2.7 billion BLE products expected

Outline

- Introduction
- BLE Primer
- Threats from BLE Devices
- BLE-Guardian
- Implementation and Evaluation
- Summary

BLE States

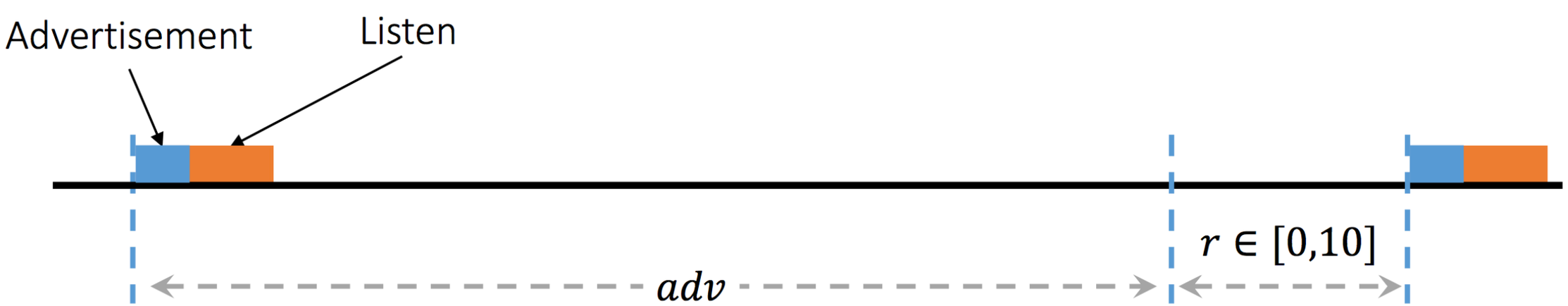
- Peripheral role
  - Sensors, fitness trackers, health monitors, etc
  - Lower capabilities: sleep for most of the time
    - With the information to advertise
- Central role
  - AP, PC or smartphone
  - Higher burden: scans for advertisement and initiates connection

BLE Advertisements

- 3 advertisement channels
  - 37 (2402MHz)
  - 38 (2426MHz)
  - 39 (2480MHz)
- 4 advertisement message types
  - ADV_DIRECT_IND
  - ADV_IND
  - ADV_NONCONN_IND
  - ADV_SCAN_IND

BLE Advertisements

Type	Description	Frequency
ADV_DIRECT_IND	Connect to a particular device only	3.75 ms, but only for 1.28 seconds
ADV_IND	General presence known + connections	20ms – 10.24s
ADV_NONCONN_IND	Don’t accept any scan or connection requests	100ms – 10.24s
ADV_SCAN_IND	Don’t accept connections but accept scan requests	100ms – 10.24s



BLE Security and Privacy

- Pairing & bonding
  - Whitelisting: only accept connections from devices it has been paired with before
  - Prevent unauthorized access to device or secured services
- Address randomization
  - Prevent user tracking
- Direct Advertisements
  - Enable fast and private reconnections.
  - Prevent user tracking and profiling

Outline

- Introduction
- BLE Primer
- Threats from BLE Devices
- BLE-Guardian
- Implementation and Evaluation
- Summary

Threats from BLE Devices

- Insight: Whether or not manufacturers properly implement BLE's privacy provisions is an entirely different story
- Passively scan for BLE advertisements
  - `<Timestamp, BT Address, advertisement content, RSSI>`
- Dataset

Site	Participants	Period
Hewlett Packard Labs	1	40 days
Ann Arbor	13	2 months
Phone LAB/ SUNY Buffalo	86	2 months

Threats from BLE Devices

- Indirect Advertisements
  - Detected 214 different unique types of devices
- Address Randomization

Name	Description
ihere	key finder
DEXCOMRX	Glucose monitor
Frances's Band ea:9d	smartband
Otbeat	heart rate monitor
JS00002074	digital pen

Revealing Names

Device	Days observed
One	37
Flex	37
Zip	37
Forerunner 920	36
Basis Peak	25

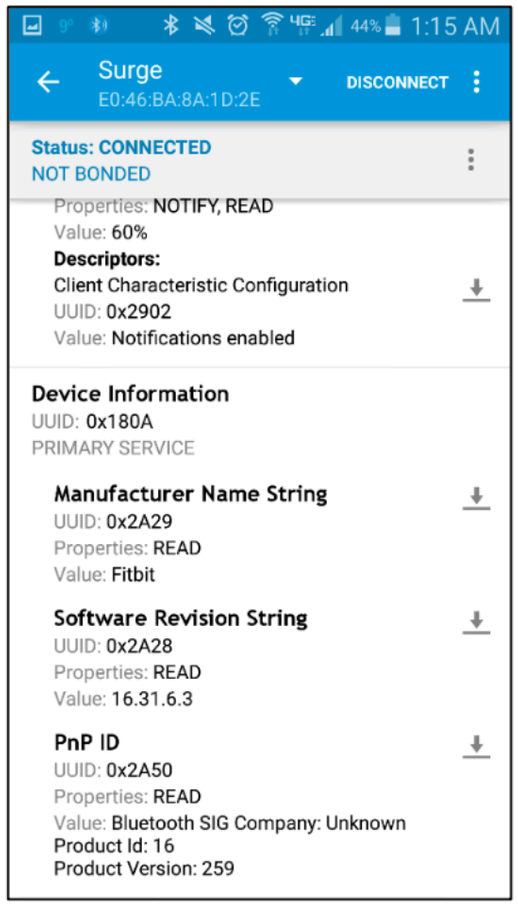
Consistent Addresses

Address
00:17:E9:CB:F3:61
00:17:E9:CB:F5:01

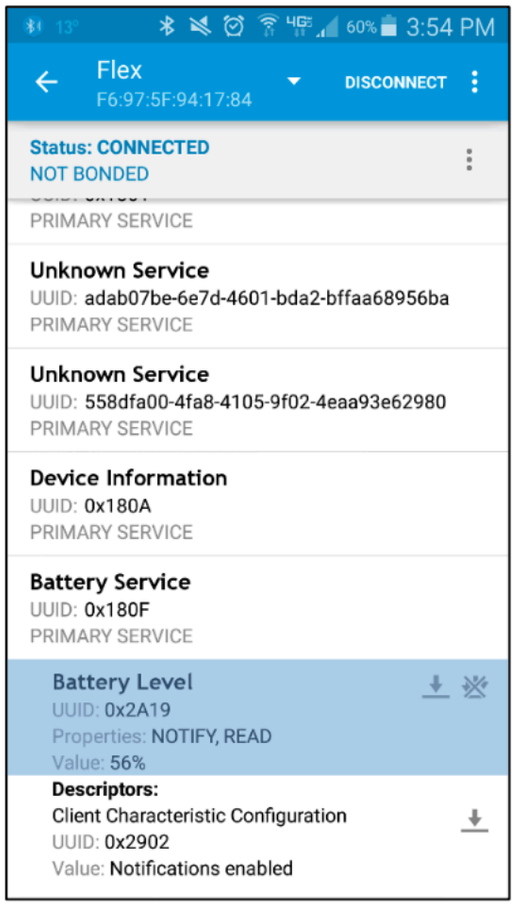
Poor Randomization

Threats from BLE Devices

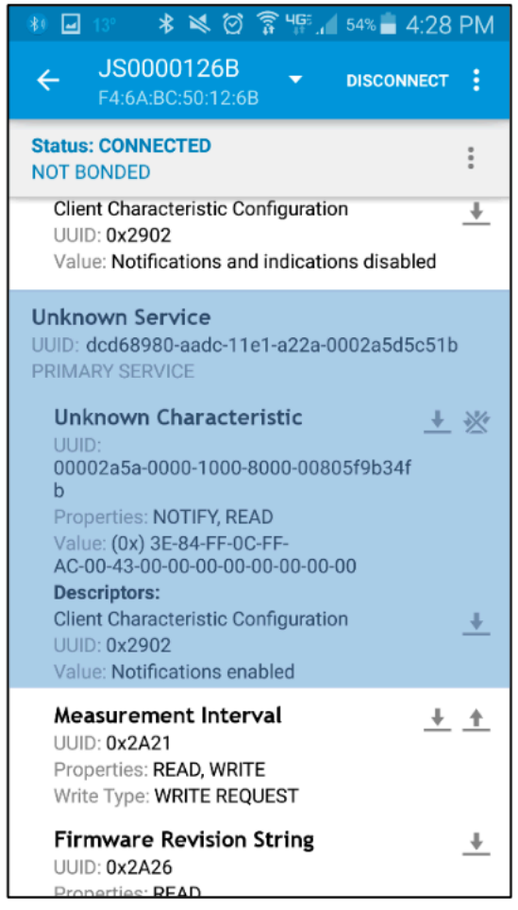
- Device pairing



Advertise and accept connections



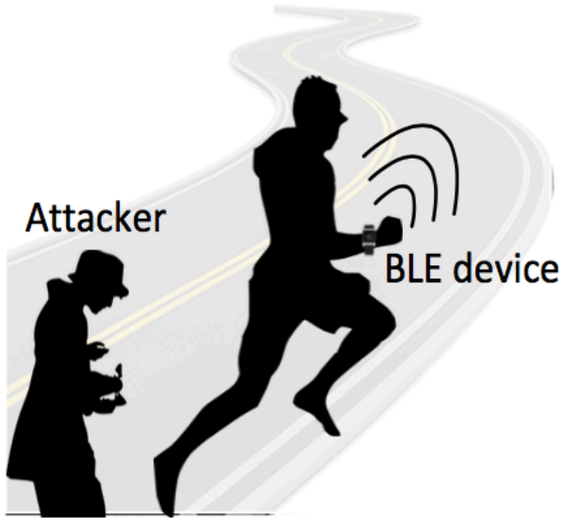
Battery level



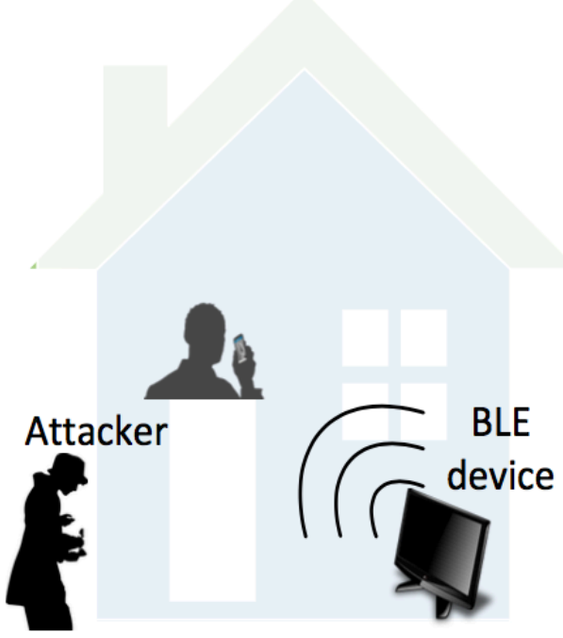
Unique identifiers

Potential Attacks

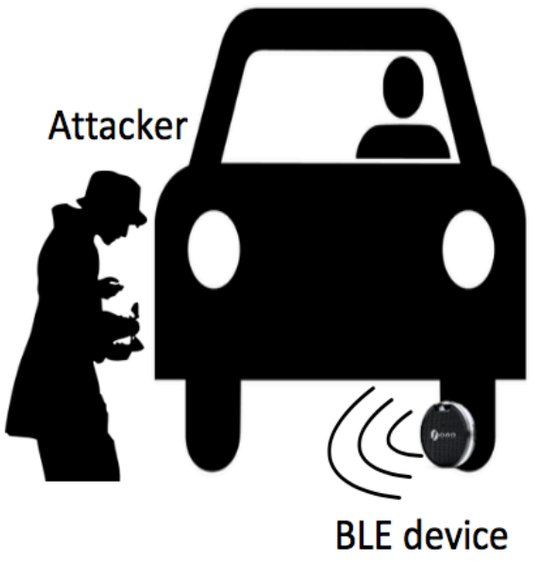
- Tracking user: consistent addresses, poor randomization, unique identifiers
- Profiling user: health situation, user's behavior, and personal interests
- Harming user: fingerprint of and unauthorized access for sensitive devices



Tracking User



Profiling User



Harming User

Research Questions

Can we effectively fend off the threats to BLE-equipped devices

(1) in a device-agnostic manner

(2) using COTS (Commercial-Off-The-Shelf) hardware only

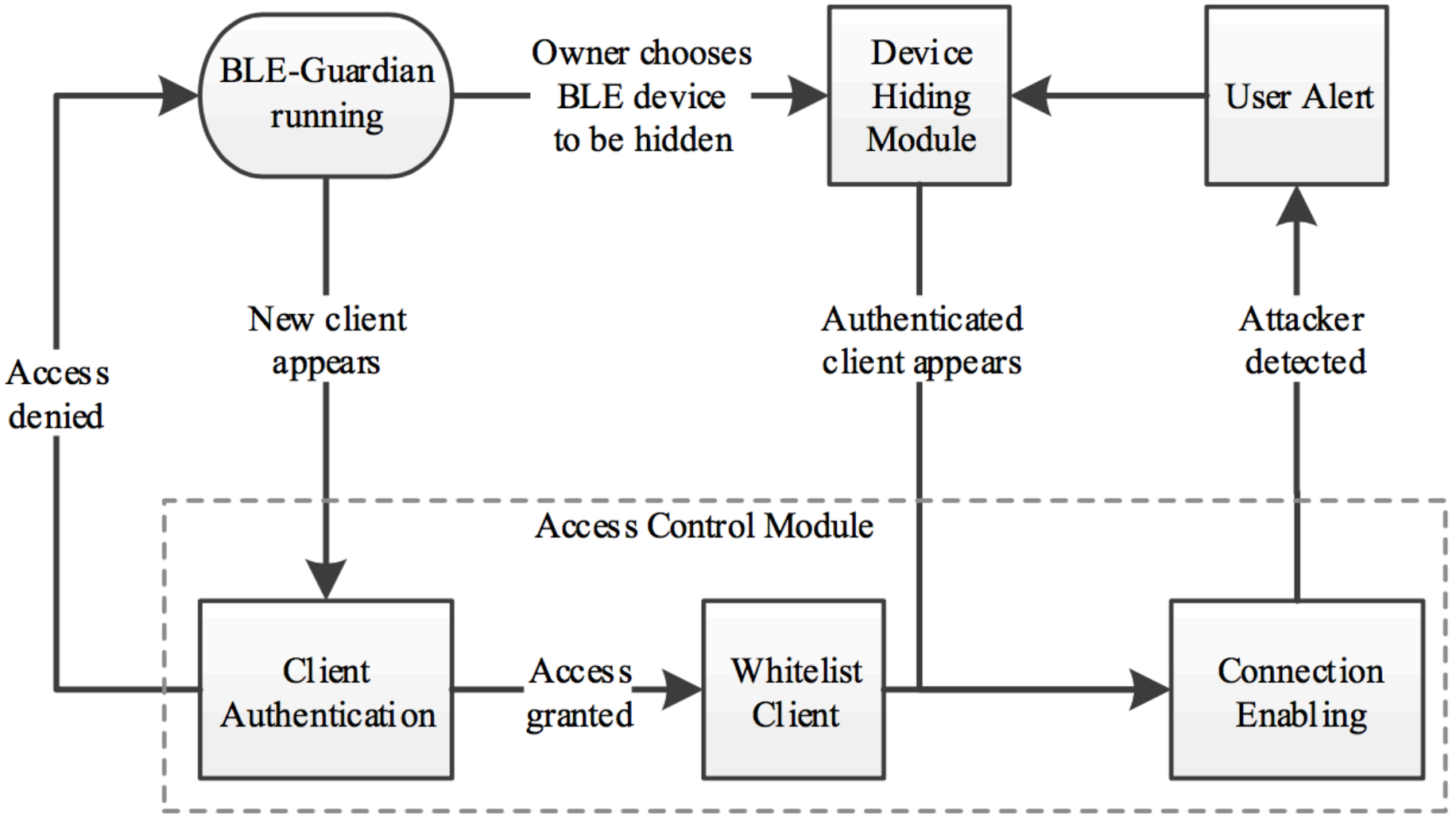
(3) with as little user intervention as possible

Outline

- Introduction
- BLE Primer
- Threats from BLE Devices
- BLE-Guardian
- Implementation and Evaluation
- Summary

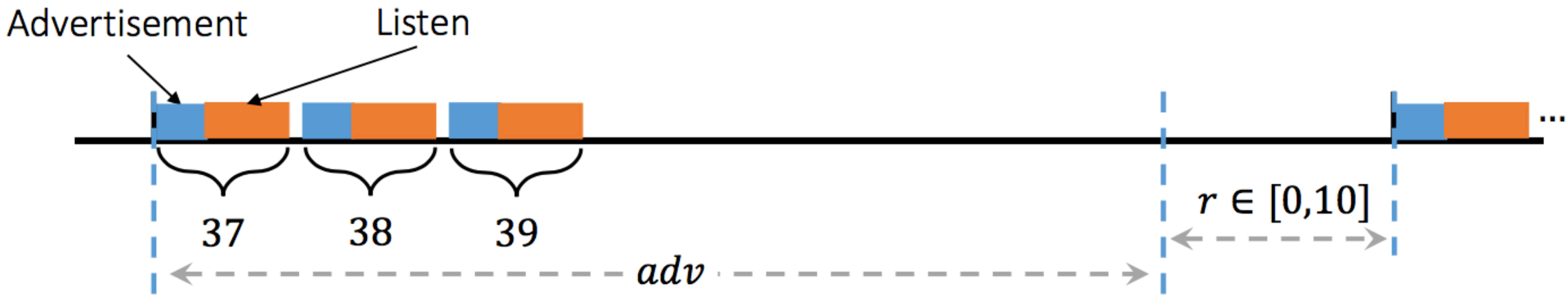
High-level Description

- Two main modules
  - Device hiding module and access control module



Device Hiding

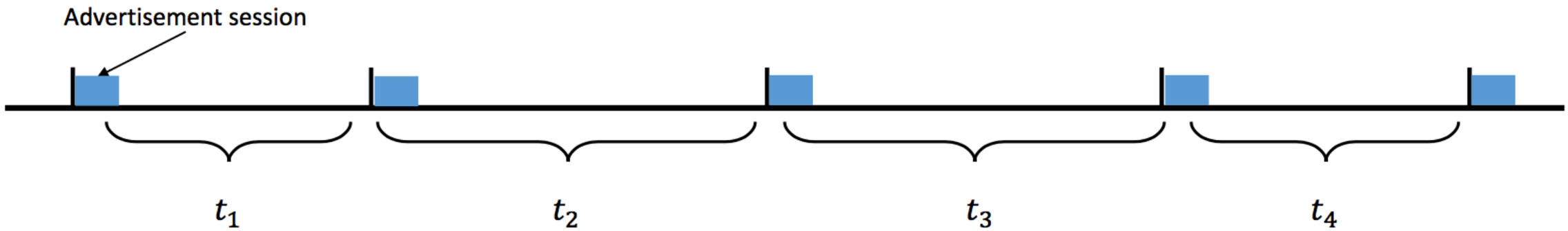
- Goal: jam BLE device advertisements to hide its existence
- Need to learn device advertising Sequence
  - Otherwise jamming will be ineffective or inefficient



Interval $t = adv + r$

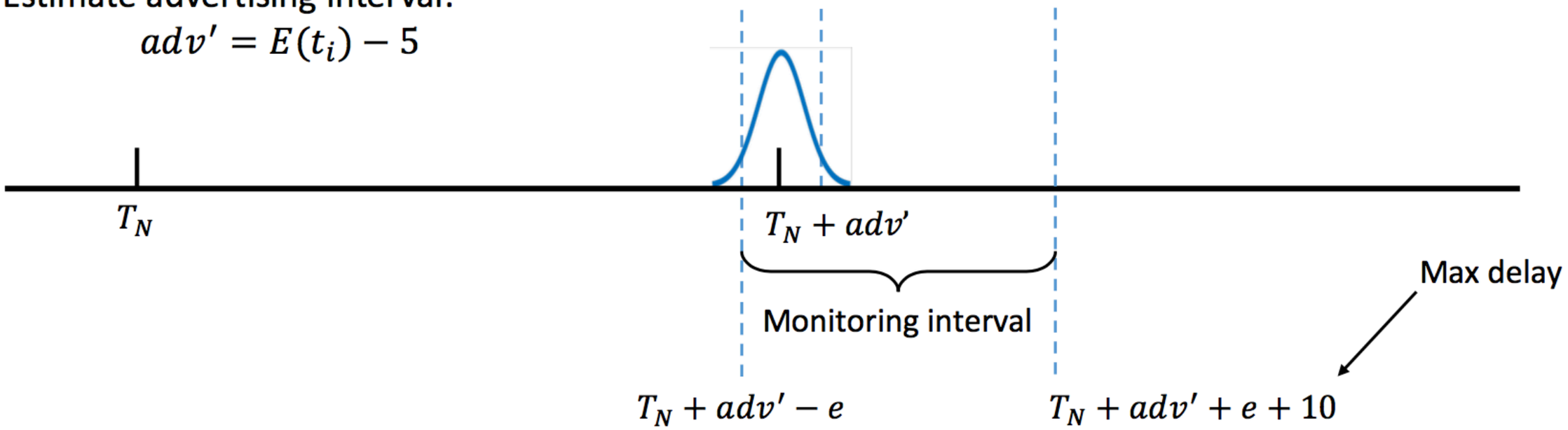
- *adv* is the actual advertisement interval as set by the device
- *r* is a random variable representing the random delay such that $r \in unif(0, 10ms)$

Device Hiding



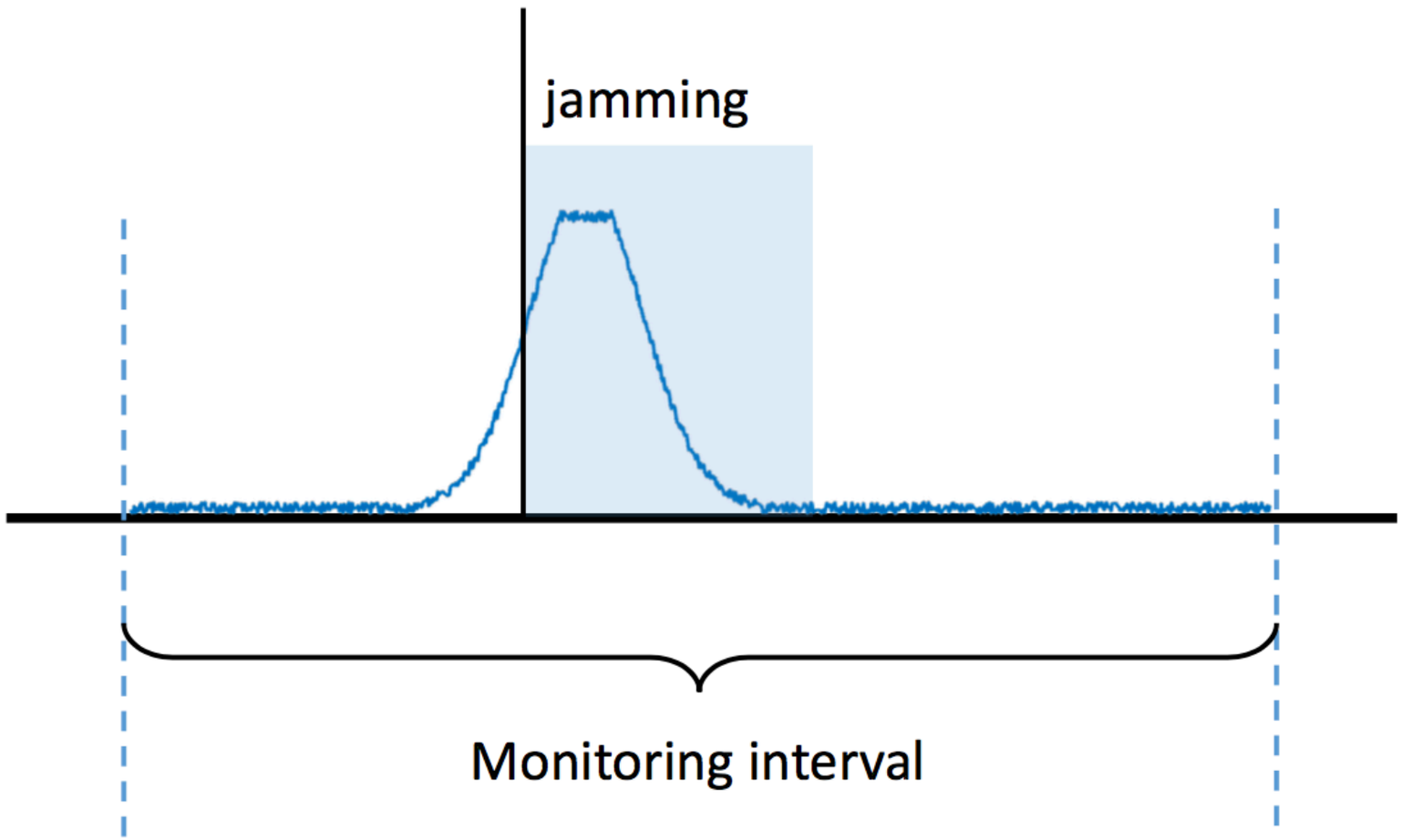
Estimate advertising interval:

$$adv' = E(t_i) - 5$$



Device Hiding

- Detect RSSI (Received Signal Strength Indication) increase
- Apply jamming and follow advertising sequence

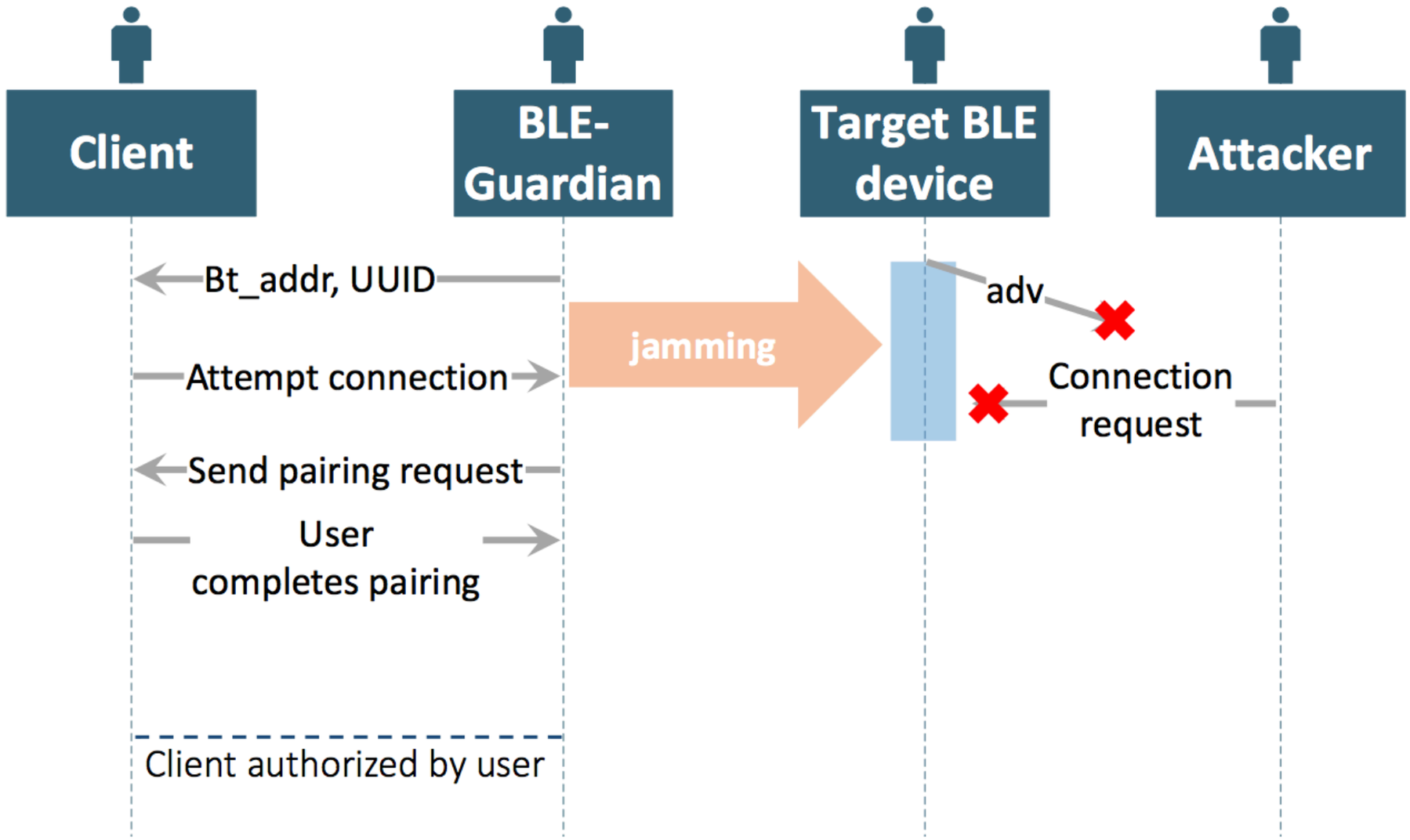


Access Control

- Goal: authorize client devices and enable their access to the BLE devices
- Device authorization
  - *BLE-Guardian* runs in server mode on the gateway waiting for incoming connections
  - Authenticating devices have *BLE-Guardian* running in client mode to initiate connections and ask for authorization
  - Authorization: the Bluetooth address of the user's gateway as well as the UUID of the authentication service
- Connection enabling
  - *BLE-Guardian* advertises on behalf of the target BLE device on the same channel
  - *BLE-Guardian*'s app running on the client device uses the address and the parameters to initiate a connection to the BLE device

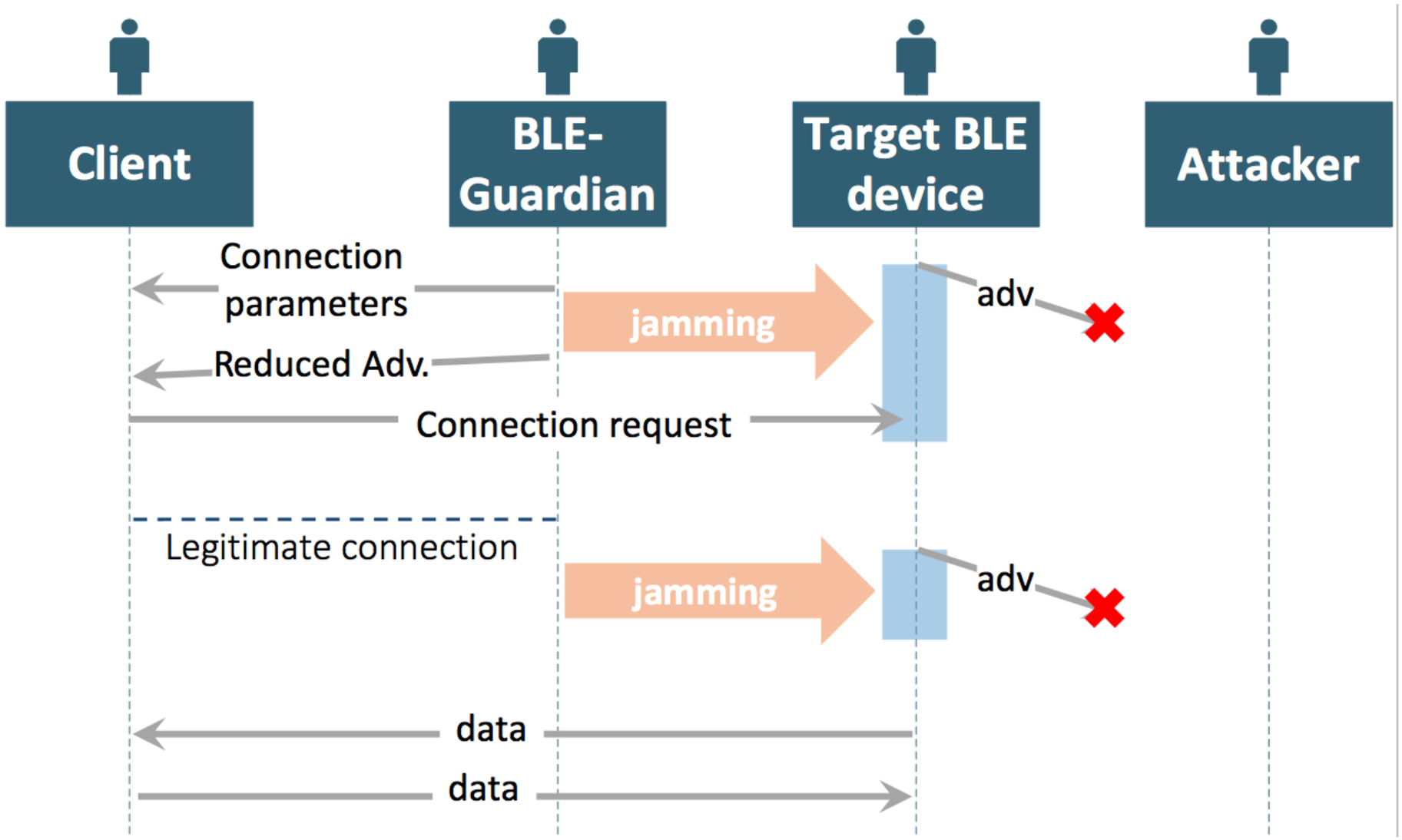
Access Control

- Authorization: bluetooth classic as an OOB channel



Access Control

- Connection Enabling: connection parameters to distinguish legitimate connection request

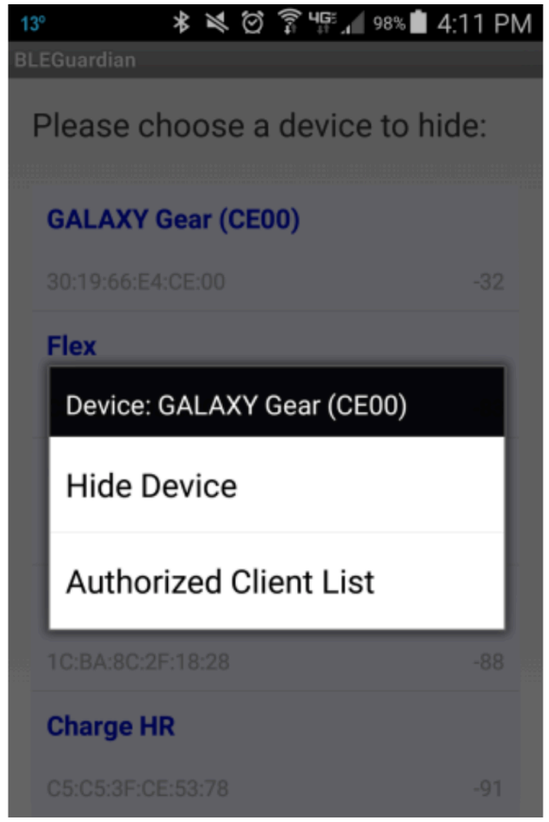


Outline

- Introduction
- BLE Primer
- Threats from BLE Devices
- BLE-Guardian
- Implementation and Evaluation
- Summary

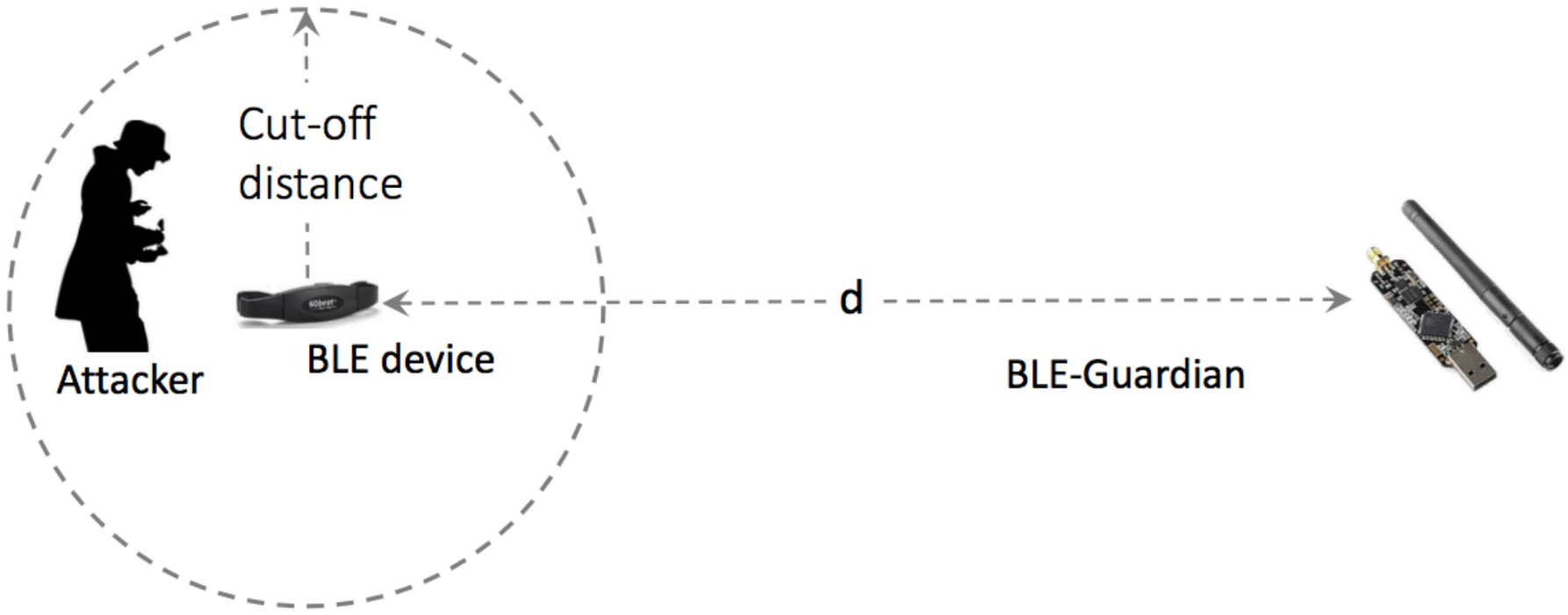
Implementation

- Hardware: Ubertooth One
  - Programmable BT radio
  - Open source firmware
    - Rx/Tx on each BT channel
- Software: user-level app
  - Control BLE-Guardian
  - Update firmware seamlessly



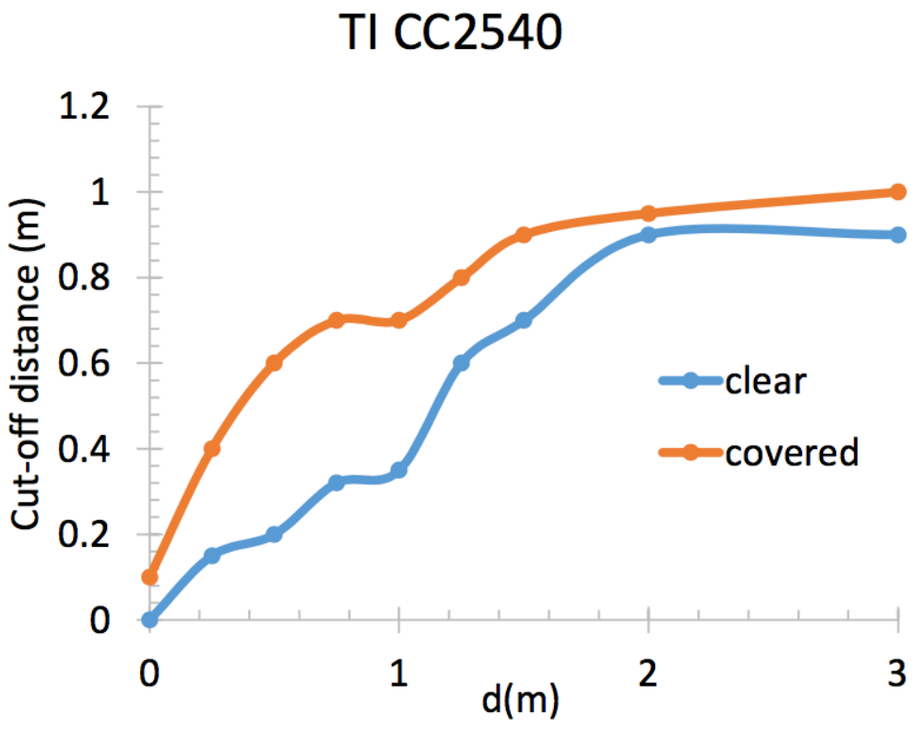
Evaluation

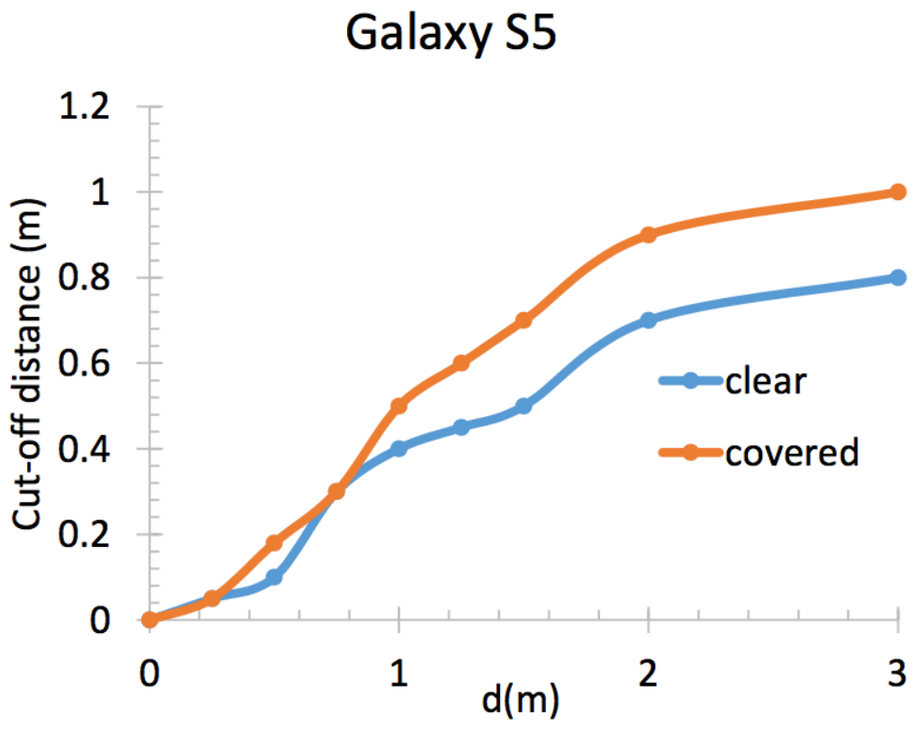
- Cutoff distance
  - Due to transmission power limitations, there would always be a small area around the target BLE device where privacy protection can not be enacted
  - Beyond it the adversary can’t scan and connect to the target BLE device



Evaluation

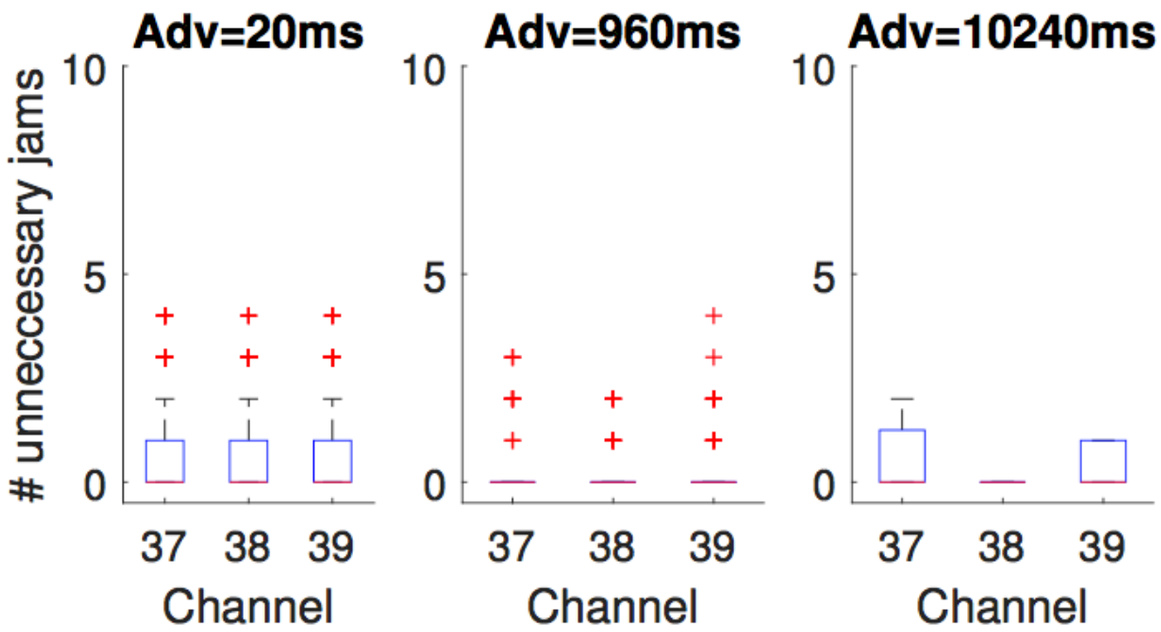
- Cutoff distance
  - Adversary has to be within 1 m of BLE device to read its advertisements





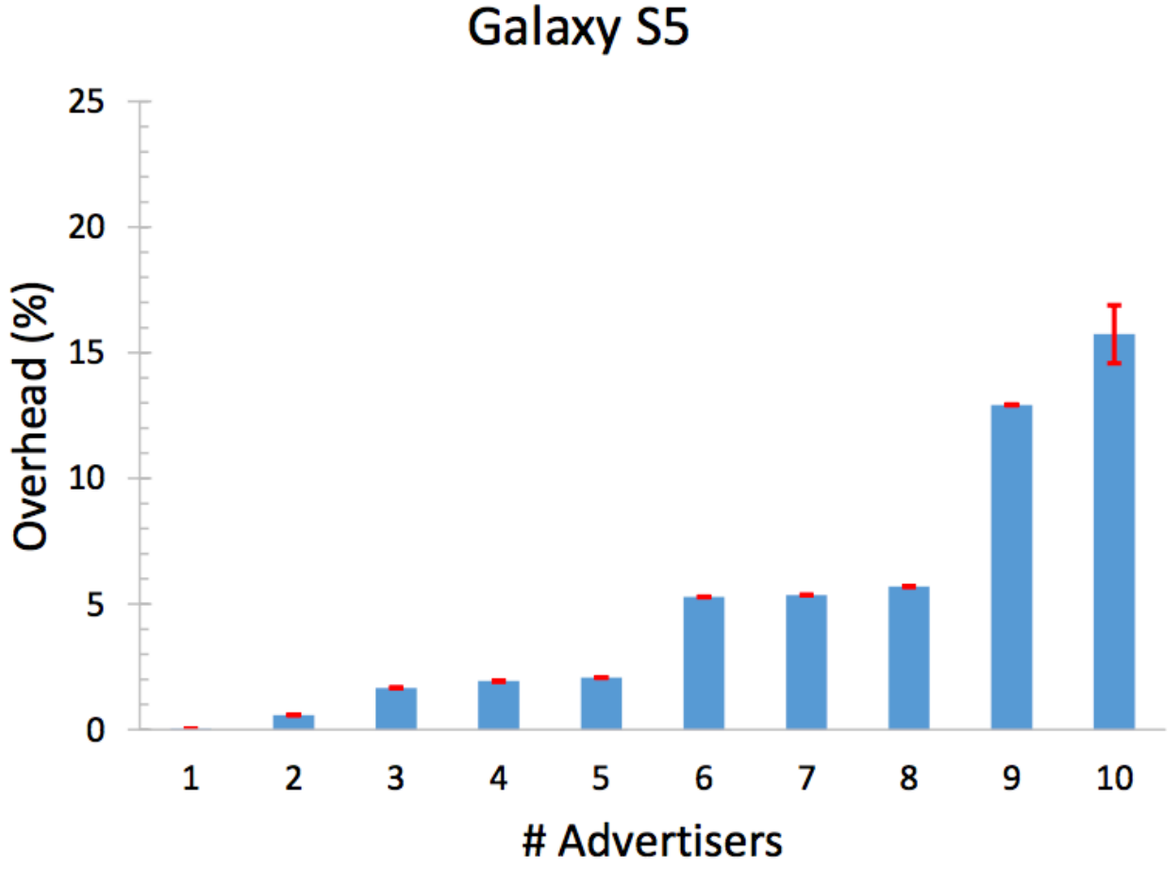
Evaluation

- Advertisement Hiding
  - Impact on Advertising Channels
    1. Protect single device at advertising intervals: 20 ms, 960 ms, and 10.24 sec
    2. Two devices advertising at 20 ms
    3. 15 other devices: with varying advertising frequencies
- The number of unnecessary jamming instance is minimal



Evaluation

- Energy Overhead
  - BLE-device and authorized clients
    - No overhead
  - Smartphone as a gateway
    - Idle power: 1370mW
    - Overhead: less than 16%



Outline

- Introduction
- BLE Primer
- Threats from BLE Devices
- BLE-Guardian
- Implementation and Evaluation
- Summary

Summary

- BLE-Guardian
  - Privacy protection for BLE device users
  - Device agnostic and relies on COTS hardware
  - Low overhead on advertisement channels
- Future work
  - Explore other M2M protocols such Zigbee
  - Implement without needing external hardware (need firmware access)

Thanks!