Applications of Secure Location Sensing in Healthcare

Michael Rushanan, David Russell, Aviel D. Rubin
Johns Hopkins University

Introduction

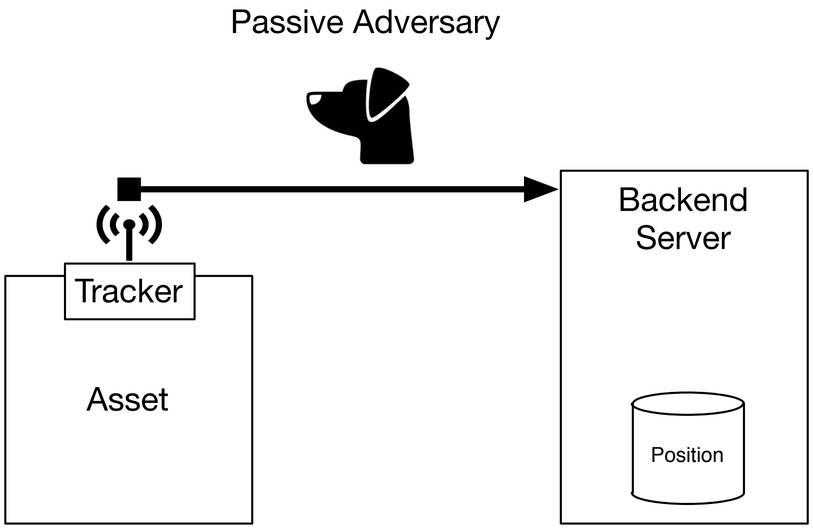
- Healthcare Application
    - Benefit patient care, delivery, and safety
    - Protect sensitive patient data
- Tracking and managing assets in real-time
- Access Control
- Barcode medication administration system

Real-time Tracking

- Tracking and managing assets in real-time
  - Hospitals
    - 1/3 Nurses spend at least 1hr/shift
    - 35,000 Units; 32-48% Being used
    - $4,000 equipment per bed

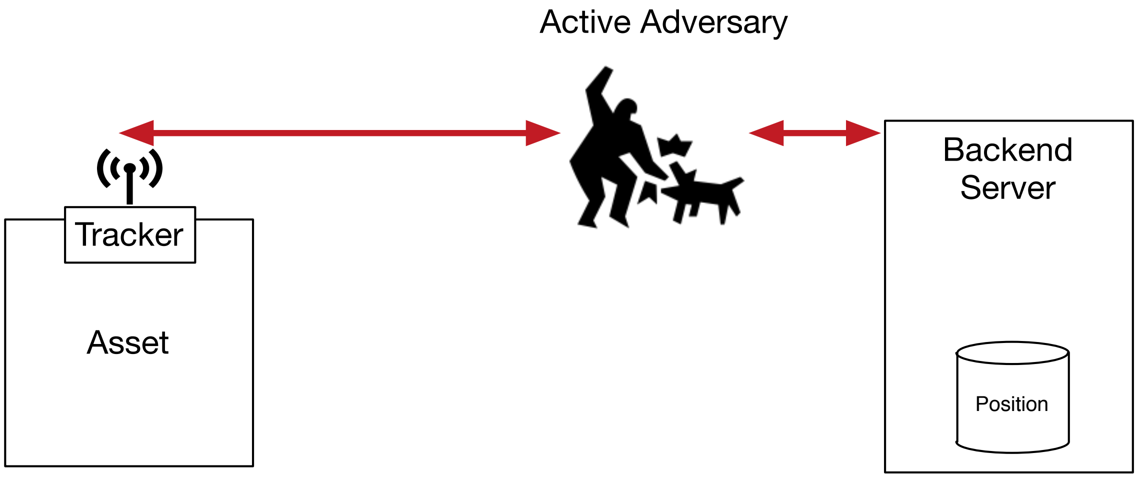
Problem

- Tracking needs to be secure
  - Resilient to *passive* and active attacks



Problem

- Tracking needs to be secure
  - Resilient to passive and *active* attacks



BCMA

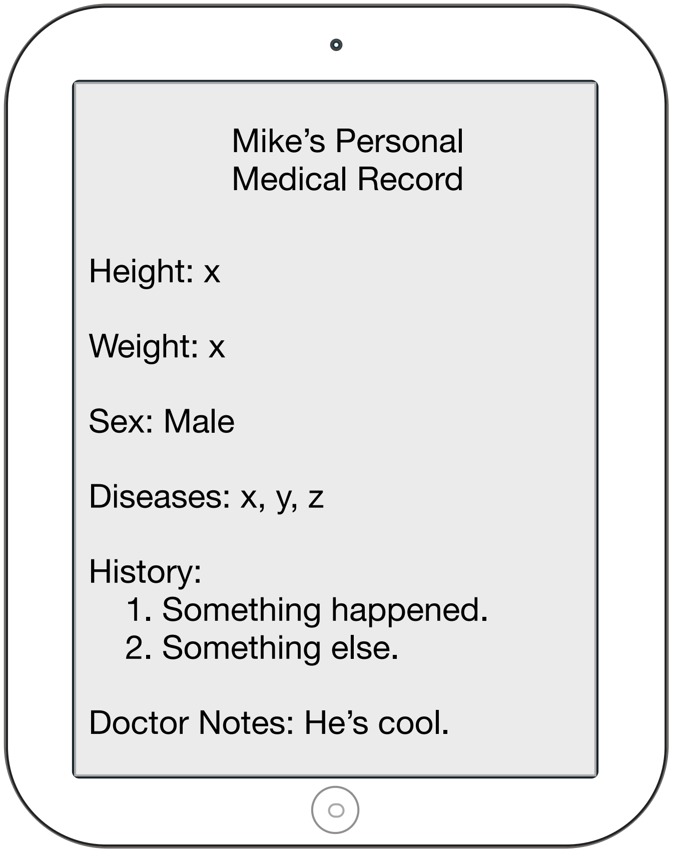
- Scan barcodes on patients and medications
    - Improve patient safety by reducing human error
- Electronic information integration
    - Interface with electronic medical records

Problem

- Scanning considered impractical
- Koppel et al. identify 31 unique causes that influence workarounds
  - Malfunctioning scanner
  - Unreadable wristbands
- Wrong administration of medication

Access Control

- Electronic medical records
  - Require access all the time
    - Mobile device
  - BYOD or Hospital asset
- Single-factor
  - Password or pin



Mike’s Personal
Medical Record

Height: x

Weight: x

Sex: Male

Diseases: x, y, z

History:

1. Something happened.
2. Something else.

Doctor Notes: He’s cool.

Problem

- Attacker can bypass this access control
- All the data stored no the device is compromised

Mike’s Personal
Medical Record

Active Adversary

Solution

- Implement secure real-time tracking system
- Secure against *active* and *passive* attacks
- Implement other applications:
  - Location-based restrictions
  - BCMA with physical proximity

Outline

- We will discuss:
  - Common architecture
  - Secure real-time tracking system
  - Location-based access restrictions

Common Architecture

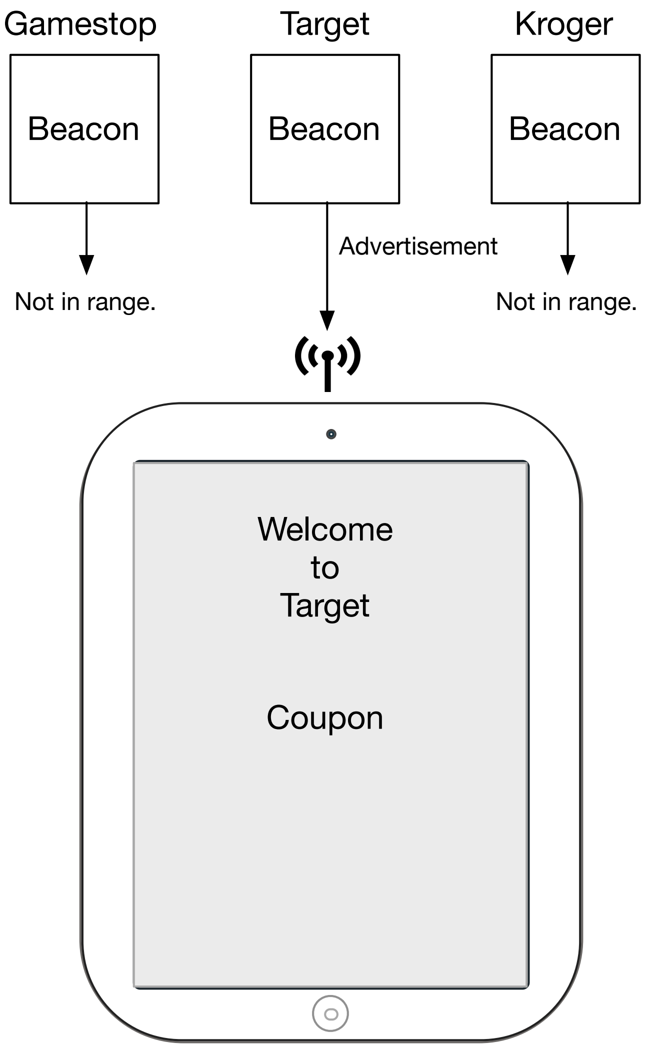
- We need a physical device that is:
  - Simple (computation, space)
  - Wireless
  - Efficient (i.e., run on battery)
  - Low-cost
- Trusted central server

BLE Beacons

Apple iBeacon

- Low-cost device
- Bluetooth Low Energy (BLE)
  - *Unidirectional*
- Computes distance via RSSI
- Intended for advertising
- “Spoofing” as a *feature*

iBeacon

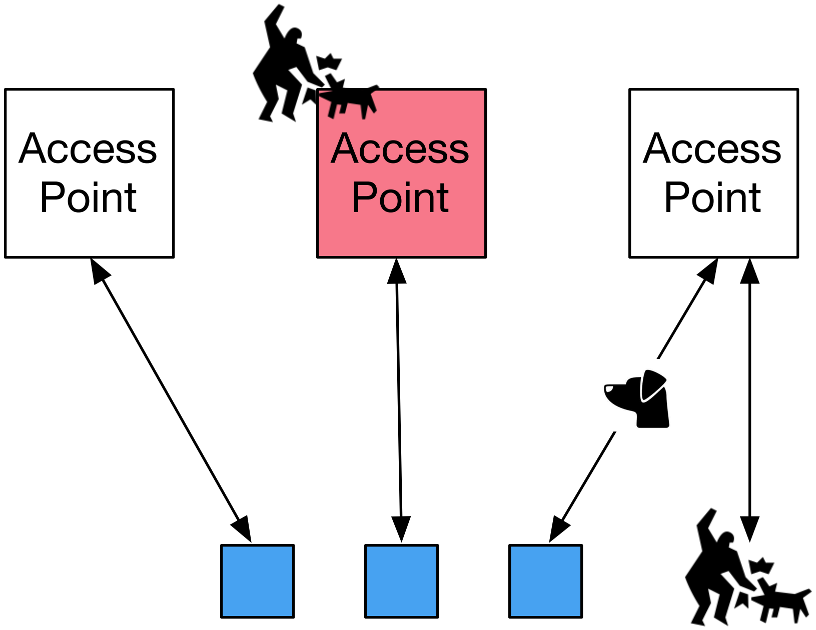

Gamestop
Target
Kroger
Beacon
Beacon
Beacon
Advertisement
Not in range.
Not in range.
Welcome
to
Target
Coupon

Other Technologies

- RFID is expensive
  - Infrastructure (i.e., ingress and egress antennas)
  - Hospital RF policies
- GPS doesn't work well indoors

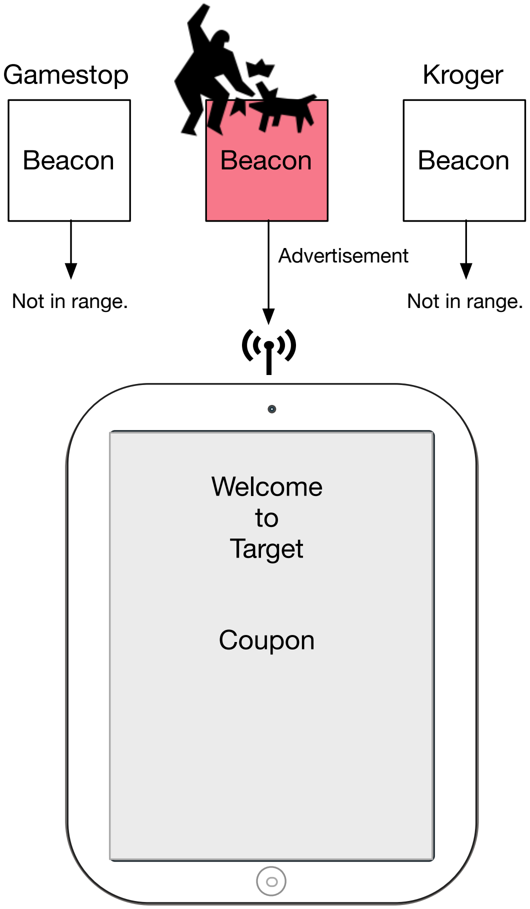
Other Technologies

- Wi-Fi is bi-directional
  - Introduces complexity
  - Consumes more power
  - Larger attack surface



iBeacon Problem

- iBeacon specification is *not secure*



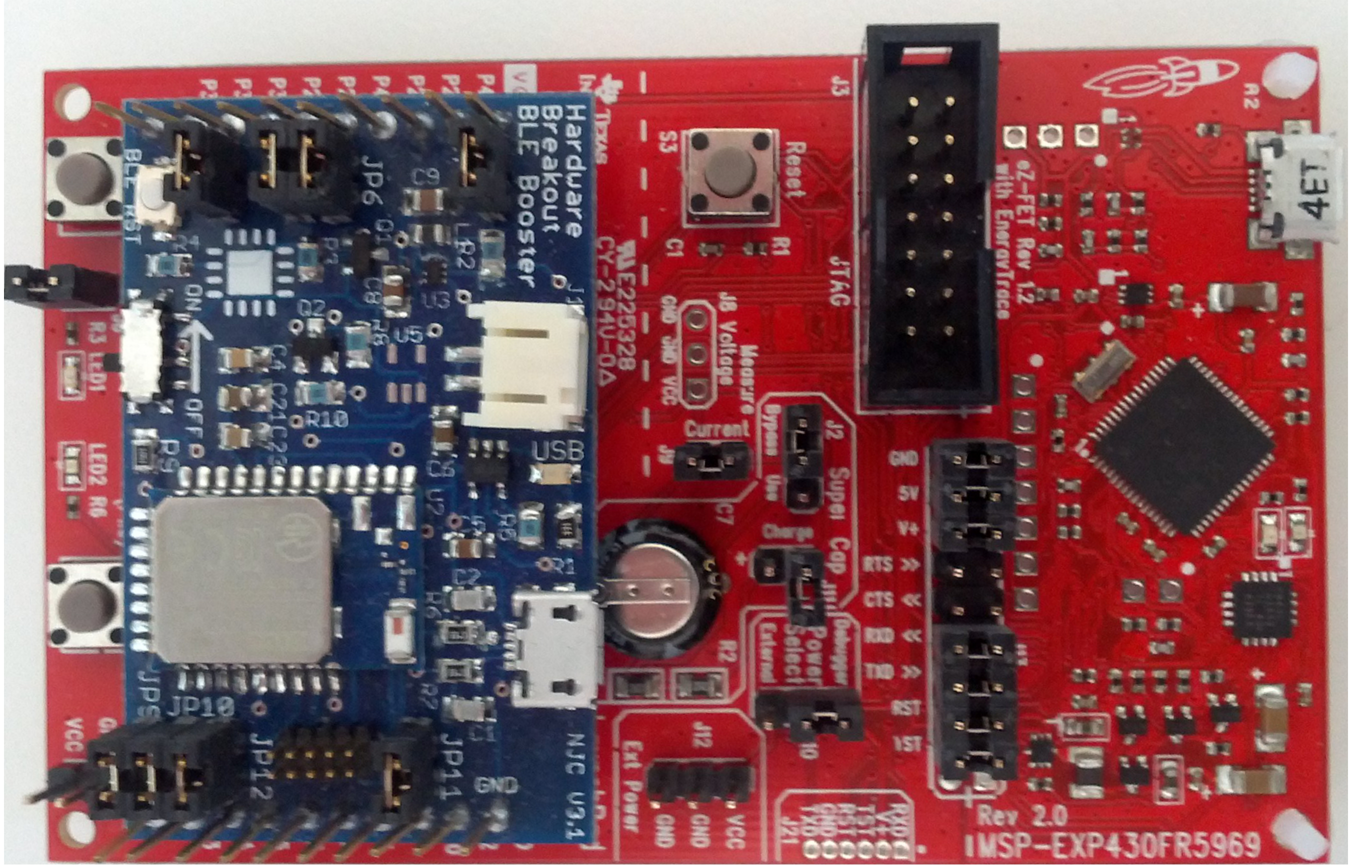
Introducing Beacon+

- Modify iBeacon specification
  - Add an AES CBC-MAC (i.e., authentication)
  - Secret key assigned *a priori* to deployment
- Monotonically increasing sequence number
  - To handle clock skew

Crypto Primer

- Message Authentication Code
    - Short piece of information
    - Authenticates a message
        - Message came from state sender
        - Has not changed
- Secret key needed to compute MAC

Beacon+


Hardware
Breakout
BLE Booster
JP6
JP10
JP11
JP12
USB
NJC V3.1
Reset
JTAG
eZ-FET Rev 1.2
with EnergyTrace
Super Cap
Power Select
Ext Power
Rev 2.0
MSP-EXP430FR5969

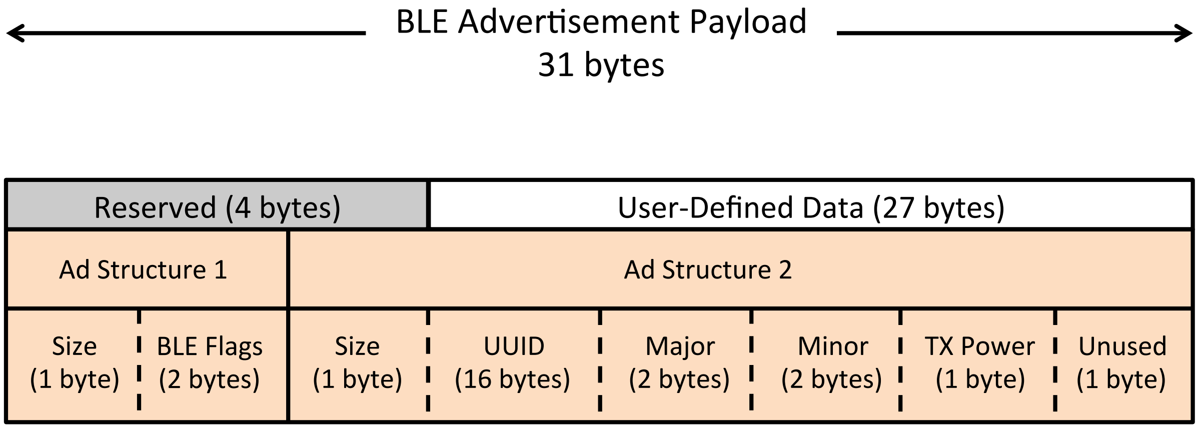
Initialization

- Beacon+ on initialization:
  - ID
  - Sequence Number
  - Secret
  - Location

Design

- Every second, Beacon+:
  - Increments sequence number
  - Computes new MAC
    - MAC sent to BLE BoosterPack via UART at a regular interval (i.e., 8x per second)
  - Replace previous advertisement

Advertisements



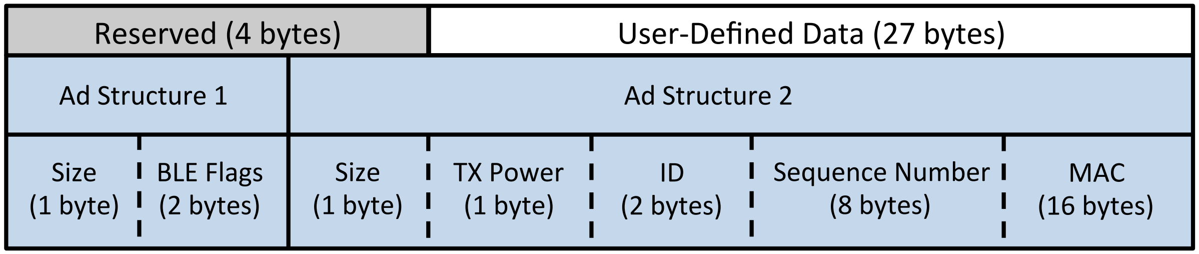
BLE Advertisement Payload
31 bytes

Reserved (4 bytes) | User-Defined Data (27 bytes)

Ad Structure 1 | Ad Structure 2

Size (1 byte) | BLE Flags (2 bytes) | Size (1 byte) | UUID (16 bytes) | Major (2 bytes) | Minor (2 bytes) | TX Power (1 byte) | Unused (1 byte)

iBeacon Advertisement



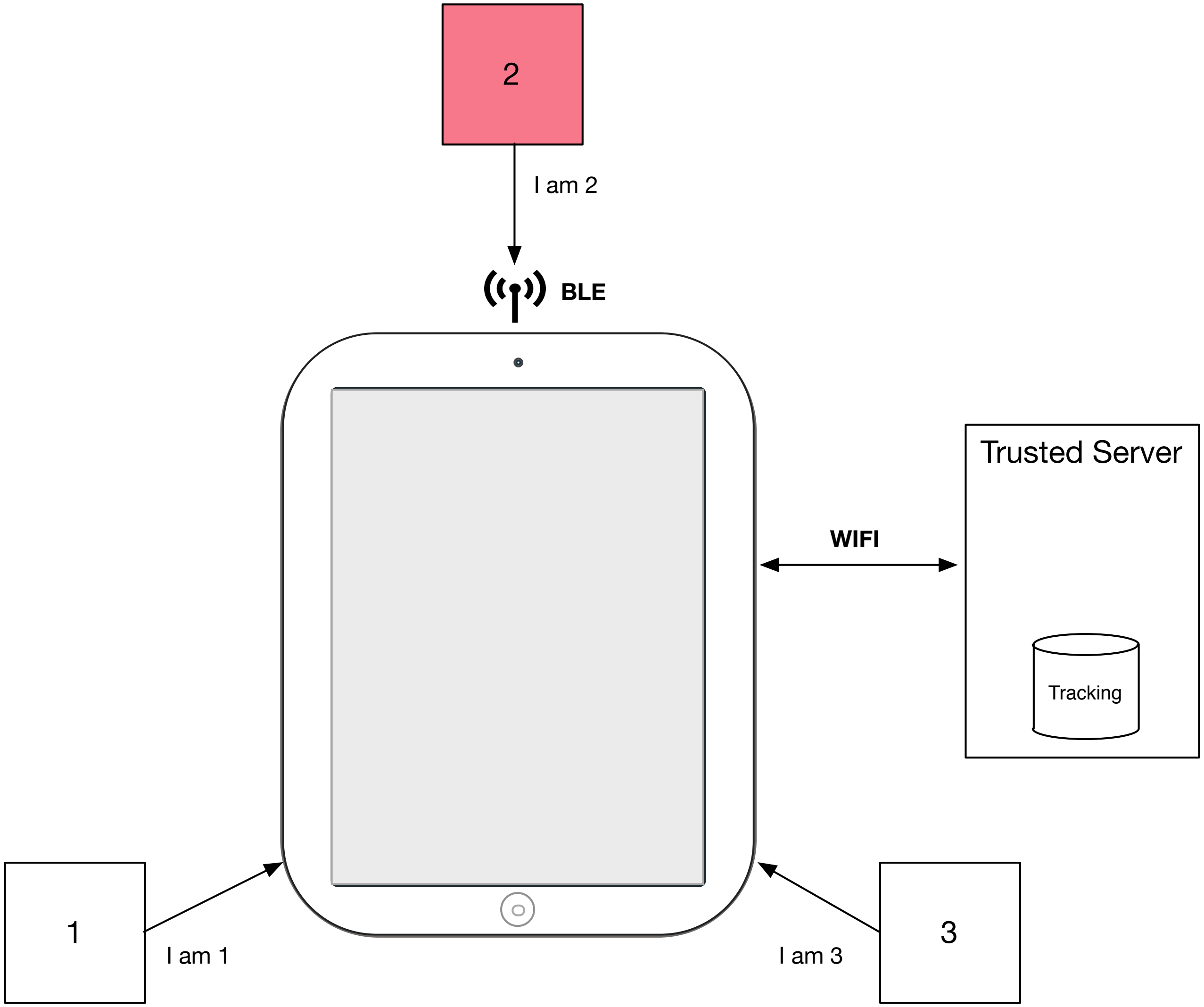
Reserved (4 bytes) | User-Defined Data (27 bytes)

Ad Structure 1 | Ad Structure 2

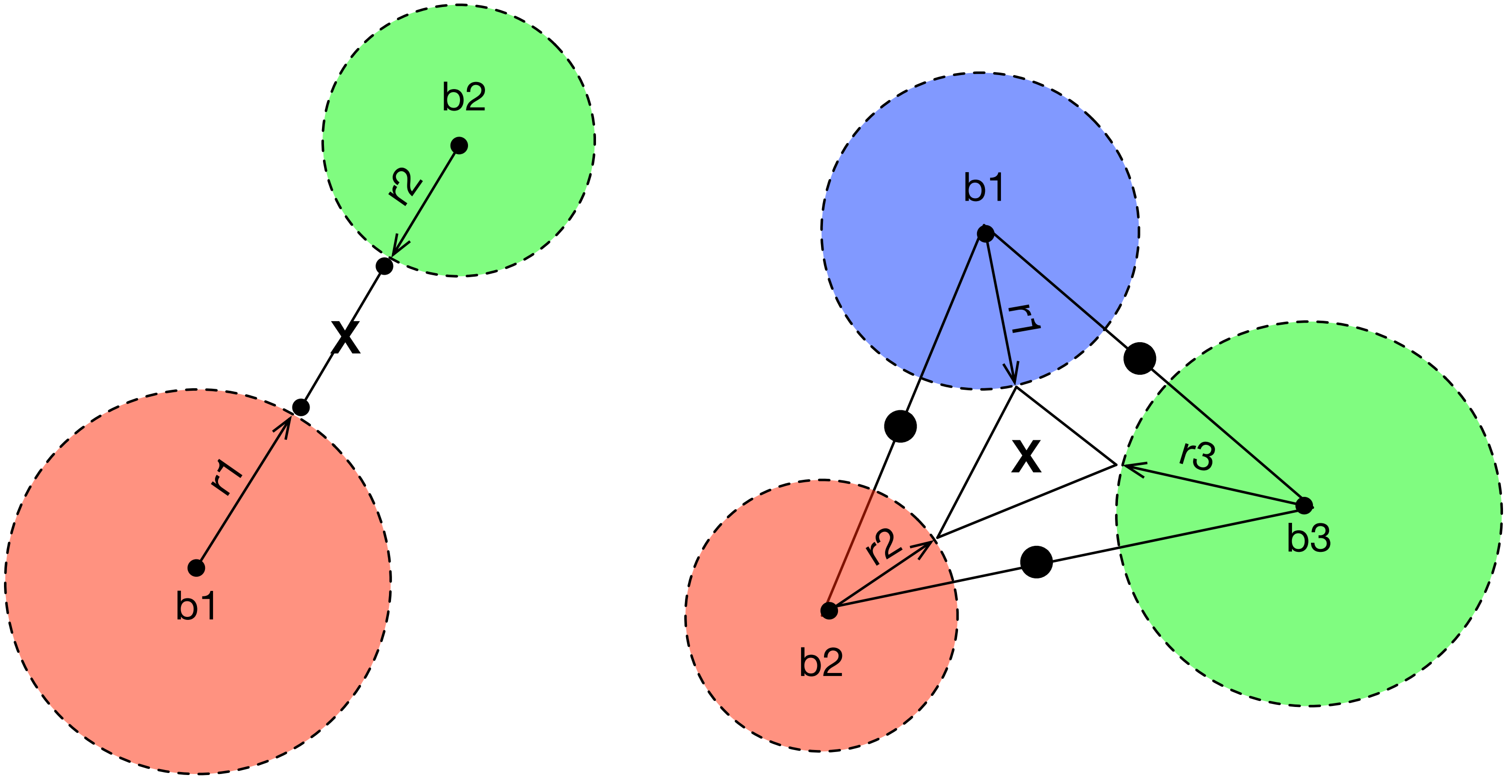
Size (1 byte) | BLE Flags (2 bytes) | Size (1 byte) | TX Power (1 byte) | ID (2 bytes) | Sequence Number (8 bytes) | MAC (16 bytes)

Beacon+ Advertisement

Communication



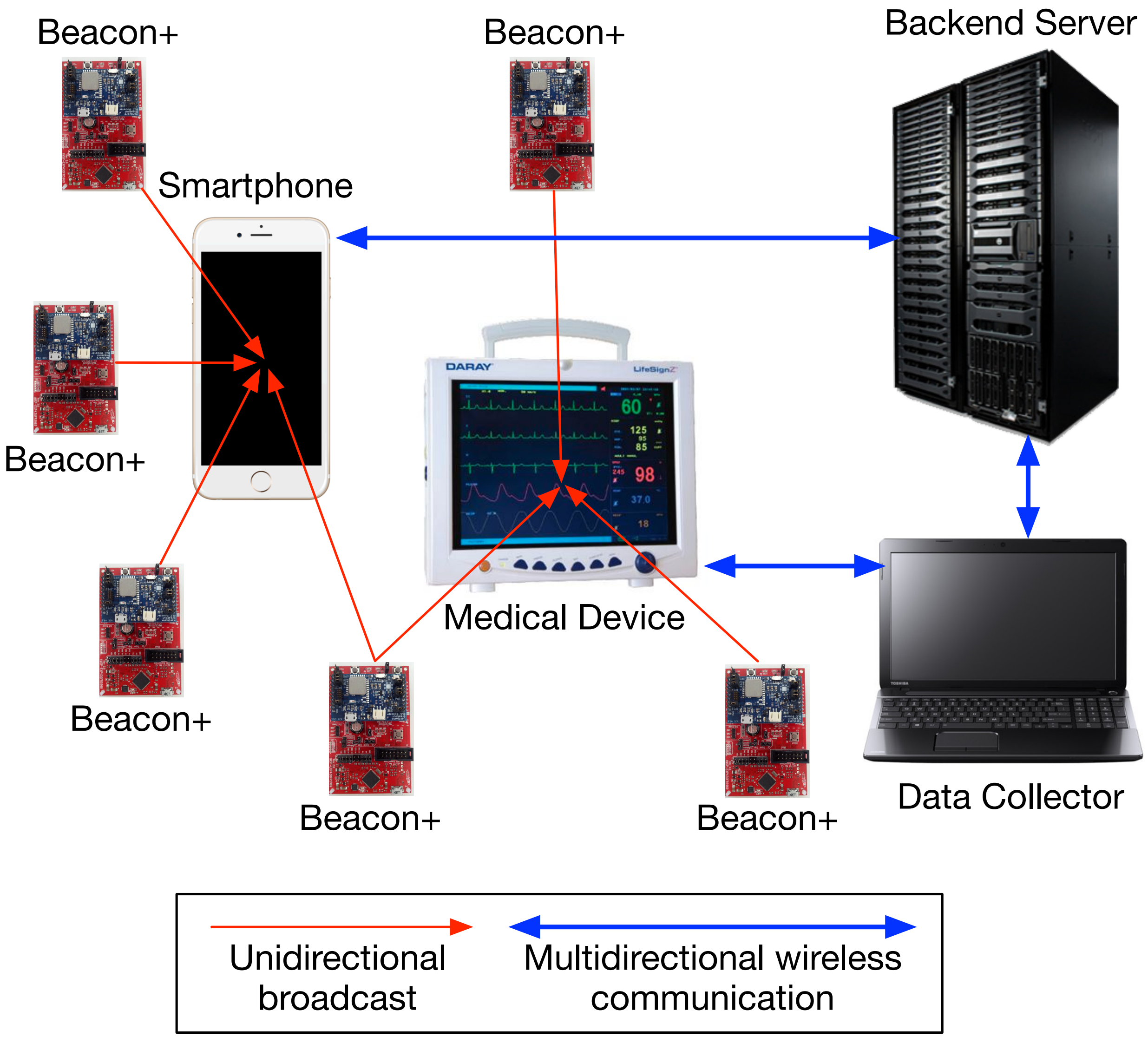
Communication



Real-time Tracking

- Beacon+'s are fixed at physical locations
- Tracked BLE-speaking devices collect
  - Authenticated advertisements
  - RSSI
- Beacon+'s data is shared with the *trusted server*

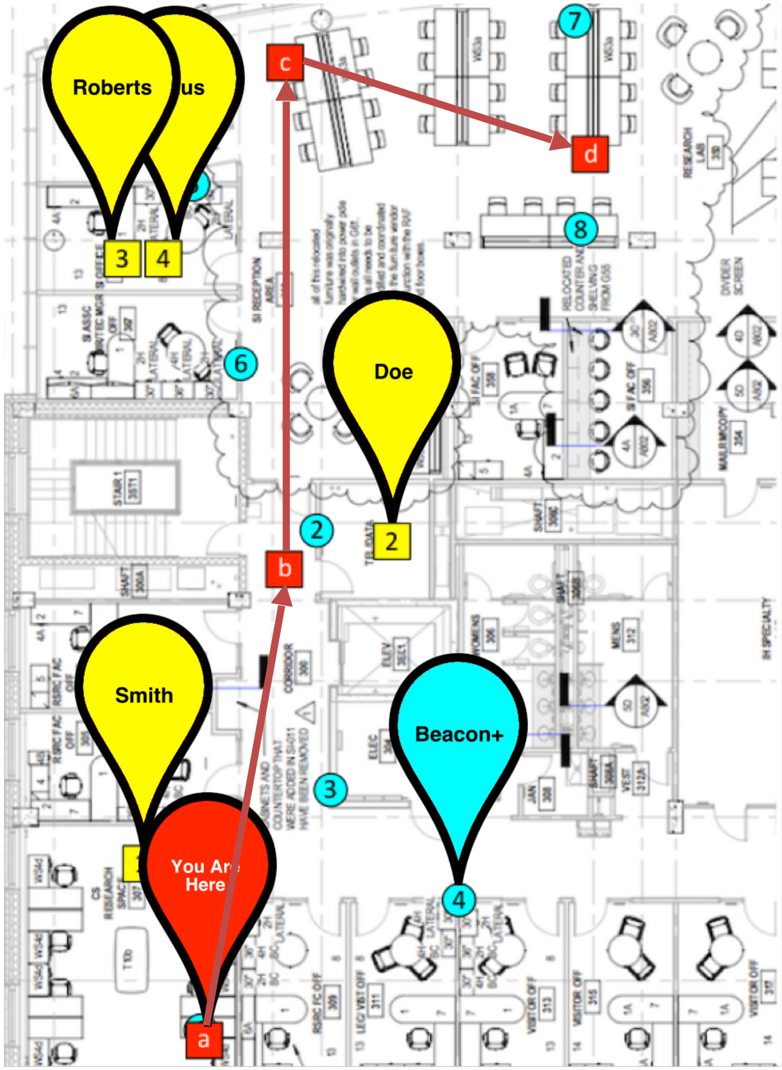
Real-time Tracking

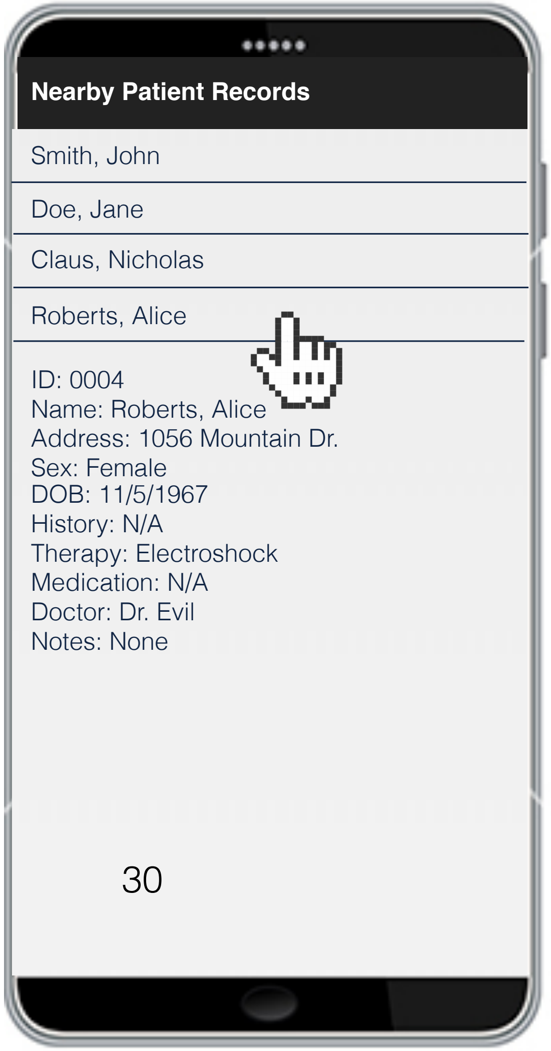


Access Control

- Bypass or breaks traditional access control
  - Password
- Location-based access restrictions
  - Restrict access to data based on location
  - Another factor of authentication

Beacon+





Nearby Patient Records

Smith, John

Doe, Jane

Claus, Nicholas

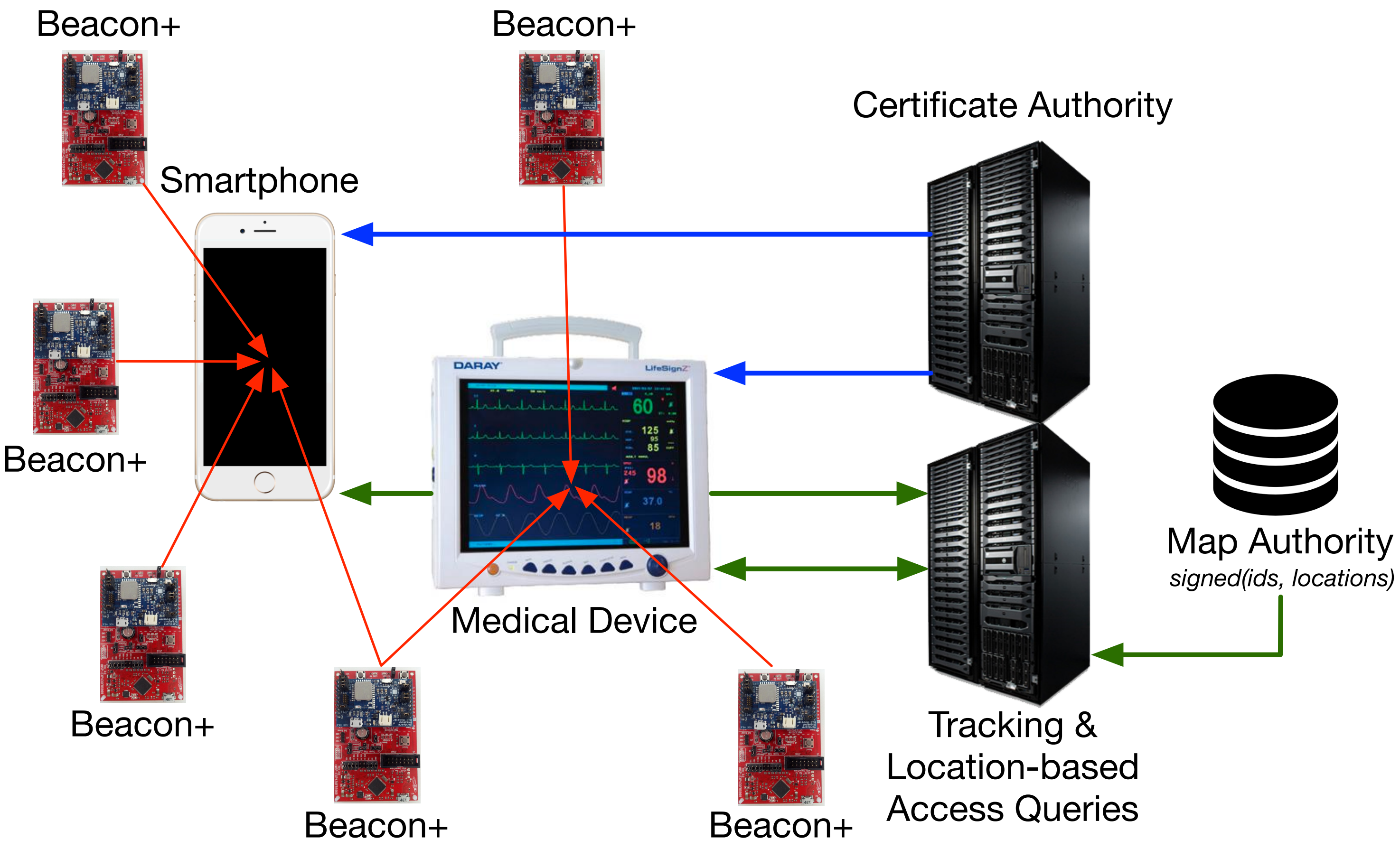
Roberts, Alice

ID: 0004
Name: Roberts, Alice
Address: 1056 Mountain Dr.
Sex: Female
DOB: 11/5/1967
History: N/A
Therapy: Electroshock
Medication: N/A
Doctor: Dr. Evil
Notes: None

Criticisms of Beacon+

- Access control
    - Need access to data immediately
- Location verification issues
    - Inside attacker can modify RSSI to fake location
    - Proxy received signals
- Trusted server

No Central Trusted Authority



Summary

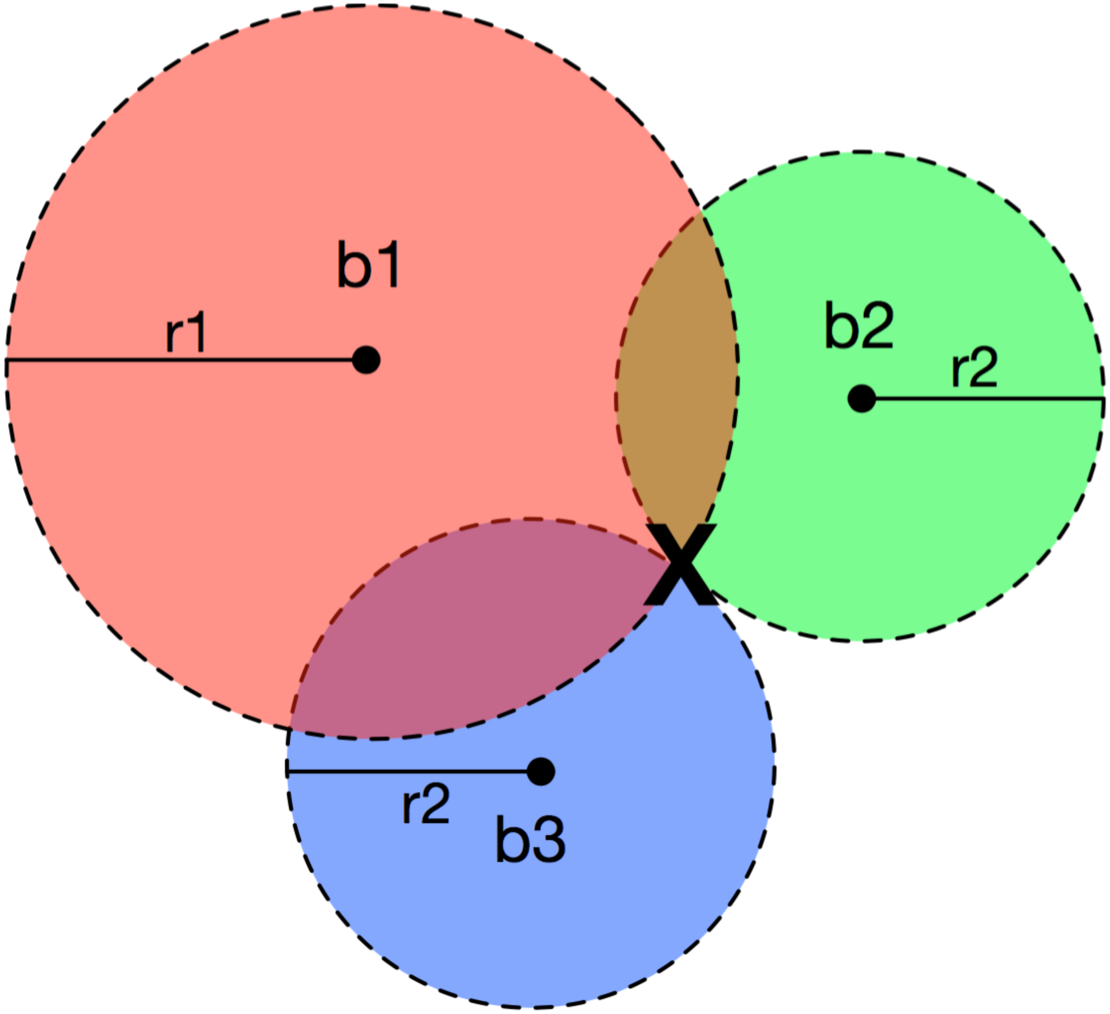
- Described common architecture
  - Beacon+
- Discussed location sensing applications
  - Benefit patient safety
- Addressed some criticisms

Questions

Thank you for attending my talk!

Backup Slides

Trilateration

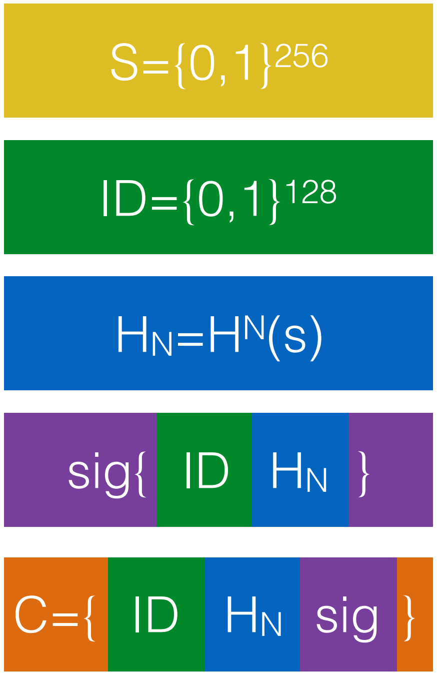


No Central Trusted Authority

Setup

A hash chain is the successive application of a hash function to a piece of data.

Its used to produce many one-time keys from a single key or password.



$S=\{0,1\}^{256}$

$ID=\{0,1\}^{128}$

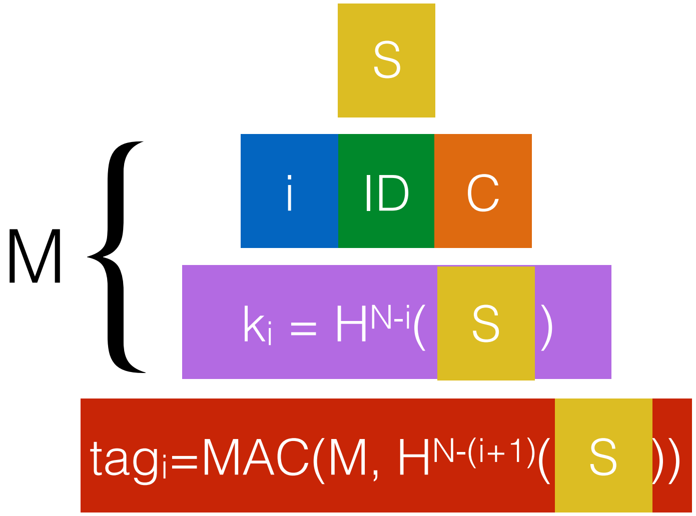
$H_N=H^N(s)$

sig{ ID H_N }

C={ ID H_N sig }

No Central Trusted Authority

[Sender] Beacon+



S

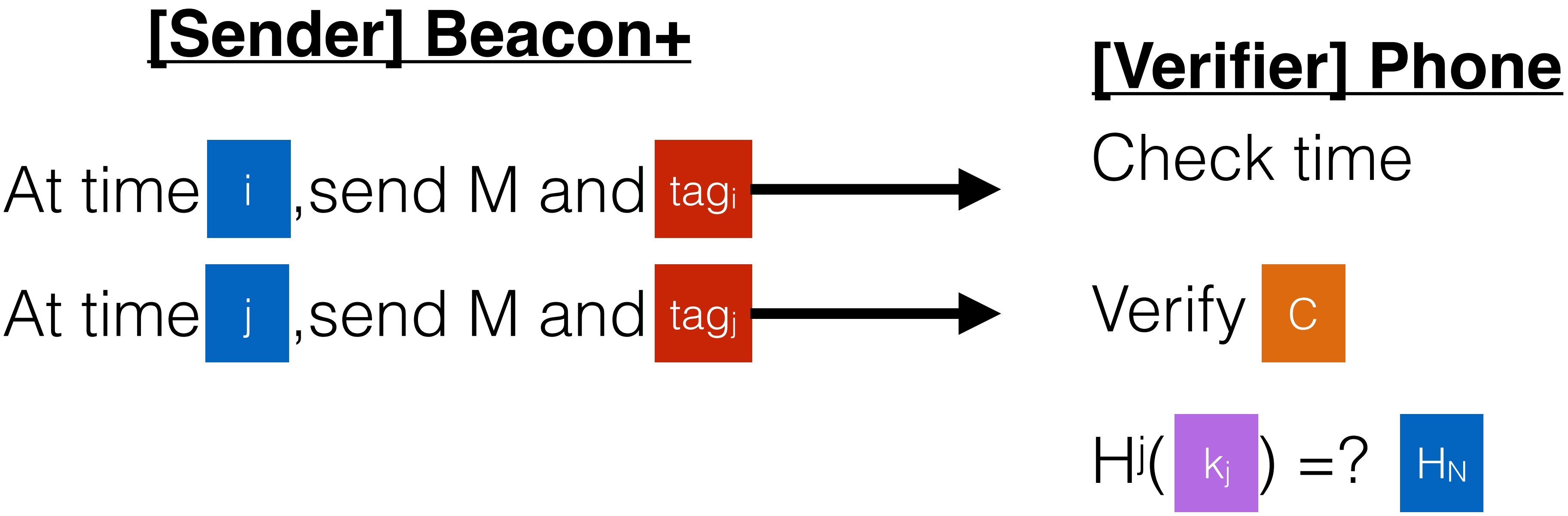
i ID C

M

$k_i = H^{N-i}($ S $)$

$tag_i=MAC(M, H^{N-(i+1)}($ S $))$

No Central Trusted Authority



[Sender] Beacon+

At time i ,send M and tag_i

At time j ,send M and tag_j

[Verifier] Phone

Check time

Verify C

$H^j(k_j) =? H_N$