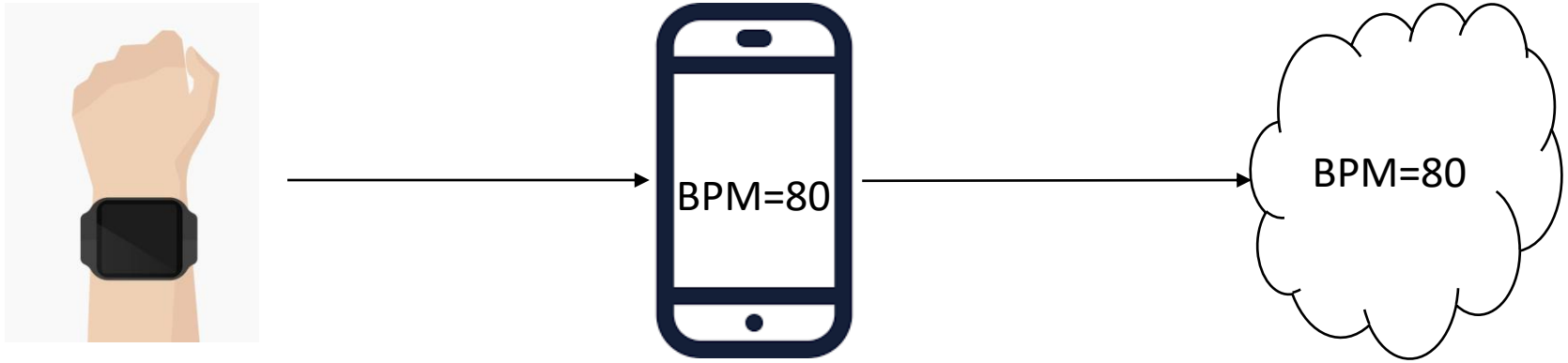
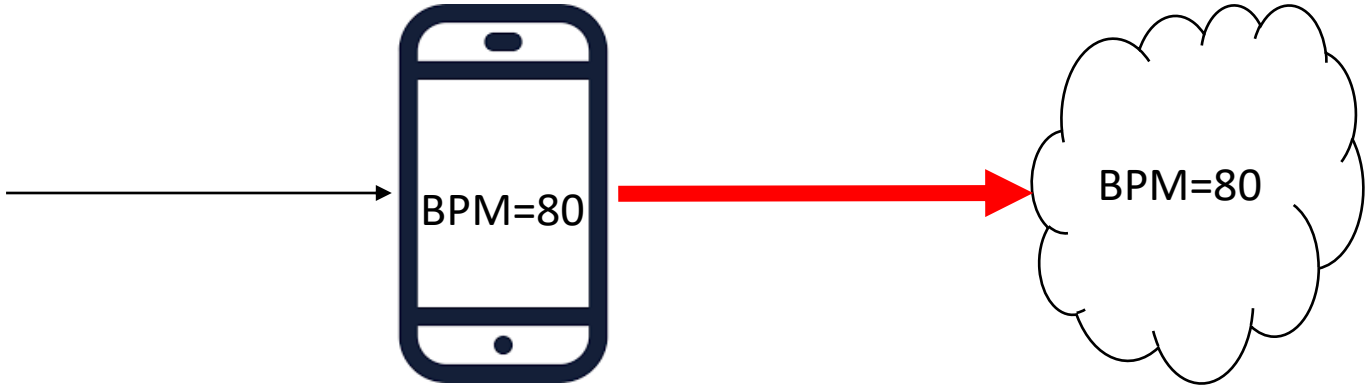
Data Leaks in health data transition

Where data can be attacked?

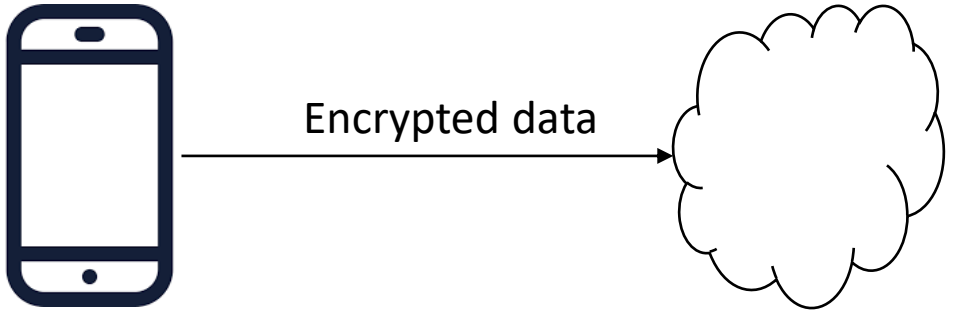


Between phone and cloud!

BPM=80



Connection between phone and storage



Why?

- Secure storage
- Legal prosecution
- Internet traversal

Internet and TLS

Secure Socket Layers (SSL) -> Transport Layer Security (TLS)

Encryption and Internet
<40% 2013 (Edward Snowden on JRE podcast)
50% Oct, 2018 (Sandvine's Global Internet)
80% Oct, 2019 (Edward Snowden on JRE podcast)
95% Oct, 2020 (“HTTPS encryption on the web” Google)

How TLS works

1. Client validates ownership of server’s public key
2. Securely generating and exchanging a session key
3. Encrypt the transmitted data

CA and certification

Google CA 

https//:www.secureband.com

public_certificate = 123456789

+ SecureBand

CA and certification

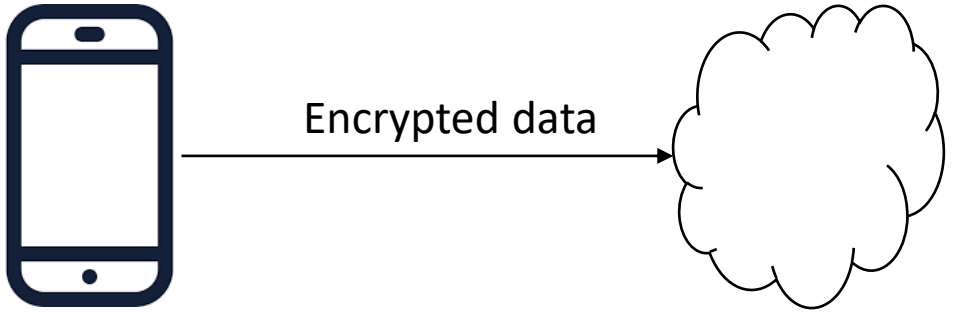
What doesn’t TLS conceal?

- the contacted site
- the length of the rest of the URL (Example.com/secreturl)
- **the length of the HTML of the visited page**
- the number of other resources (e.g., images, iframes)
- the timestamps.
- IP

Wireshark, tcpdump, snort

TLS in smartbands apps

Connection between phone and storage



Why?

- Secure storage
- Legal prosecution
- Internet traversal

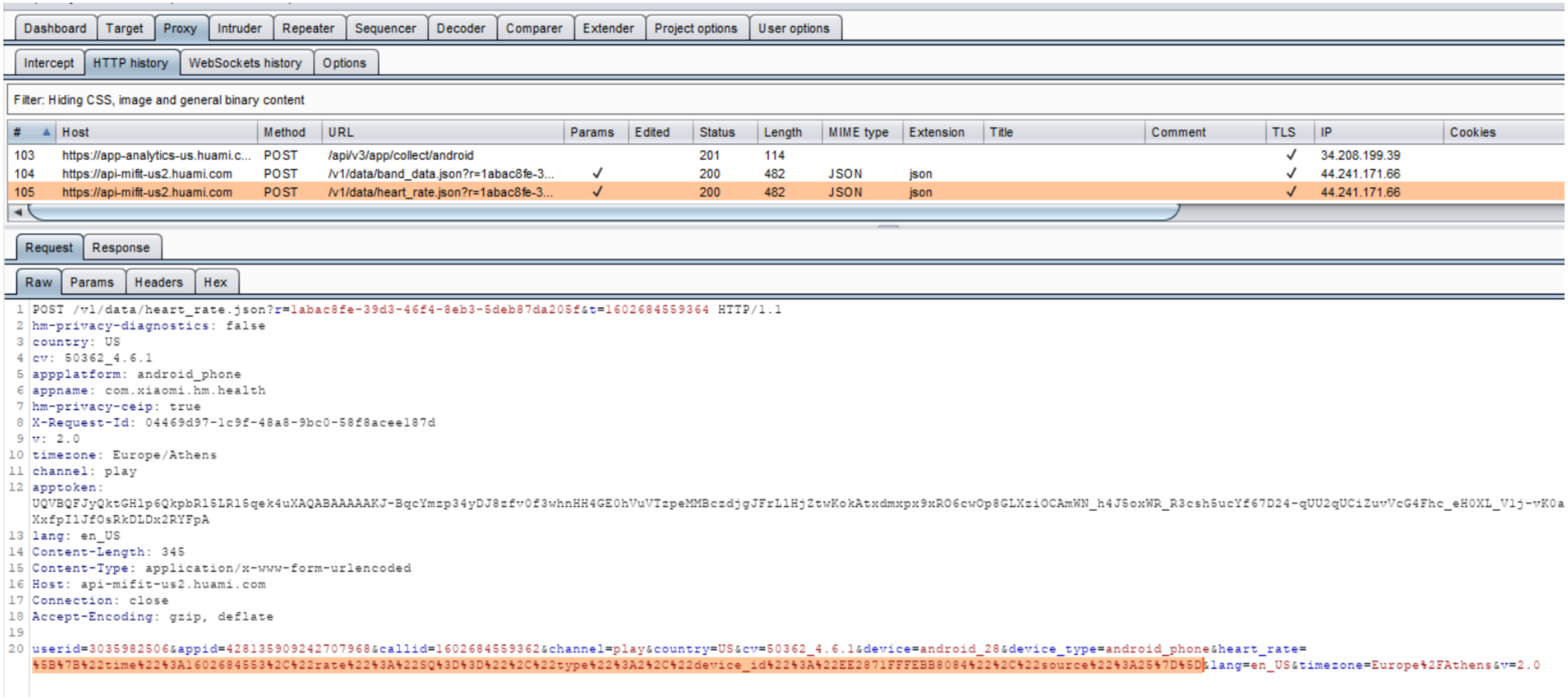
TLS shows the length of the HTML of the visited page!!

Learning the ground truth

Man in the Middle proxy

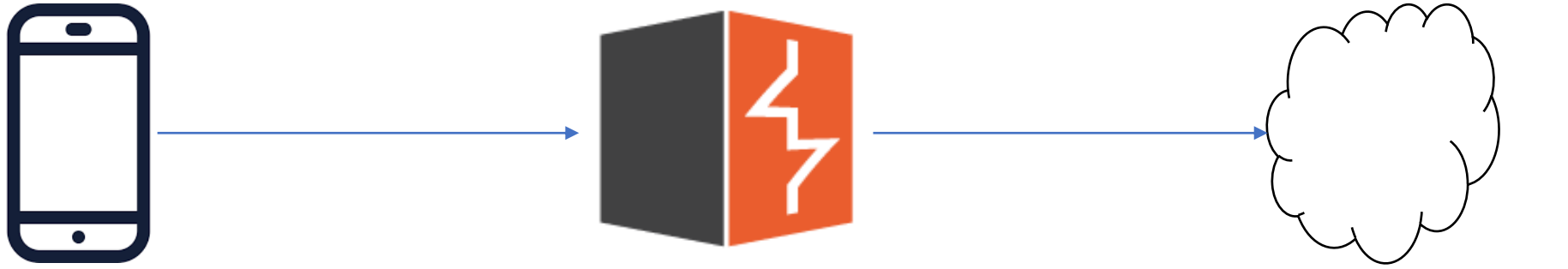
(i) decrypts the traffic
(ii) examines the packet contents
(iii) re-encrypts the traffic
(iv) sends the traffic to its destination.

Burp Suite
Fiddler

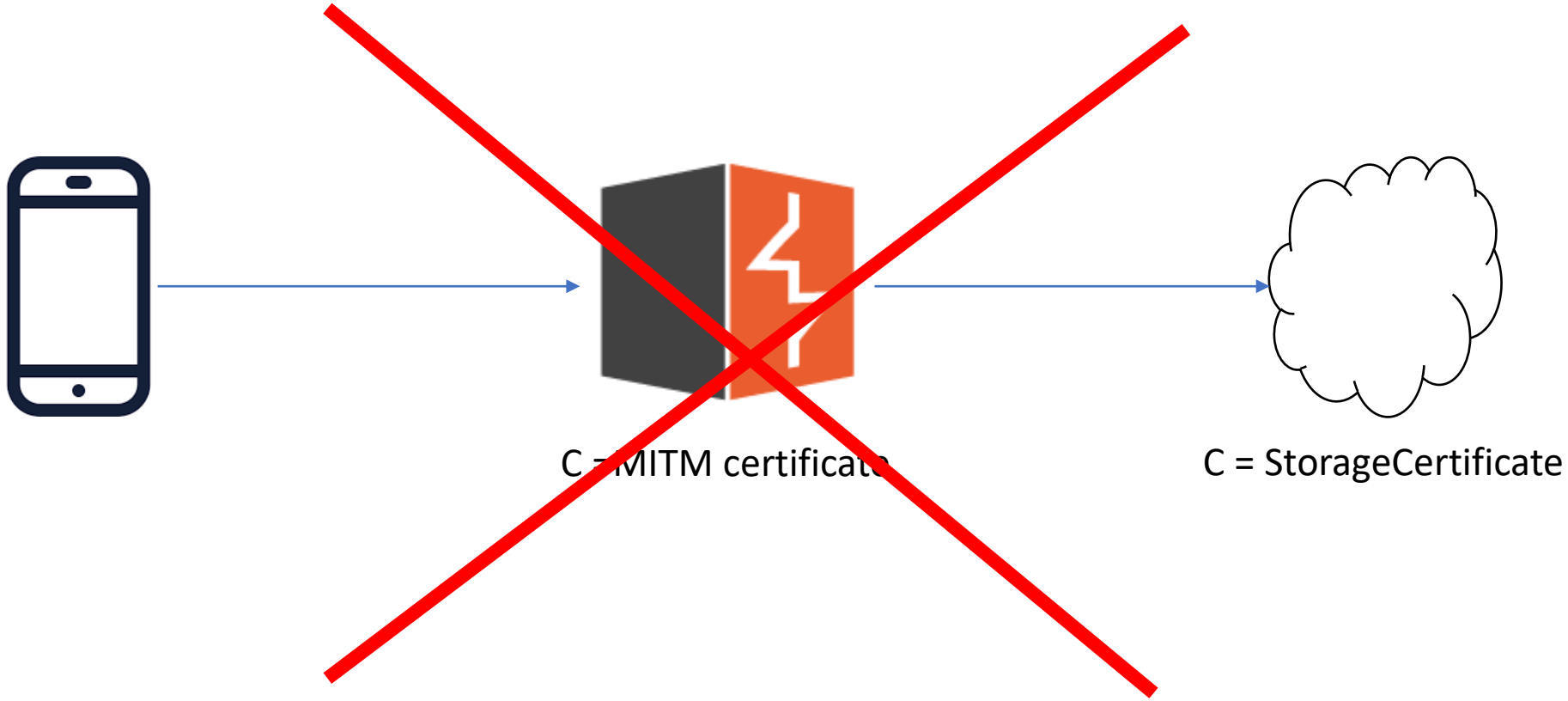


[{"time":1602684553,"rate":"SQ==","type":2,"device_id":"EE2871FFFEBB8084","source":25}]

MITM and certificates

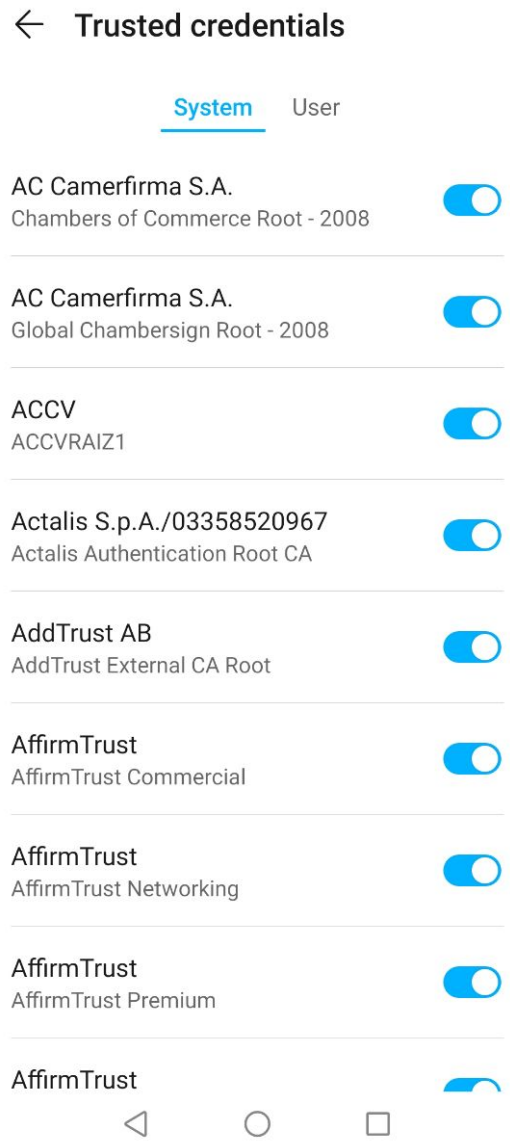


MITM and certificates

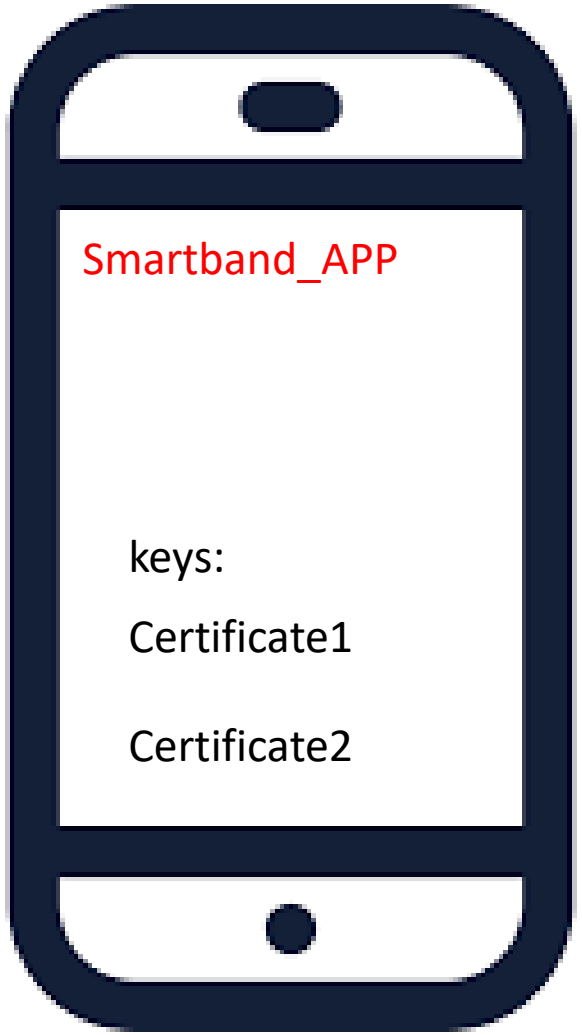


Trusted certificates

Need to install MITM certificate



Certificate pinning

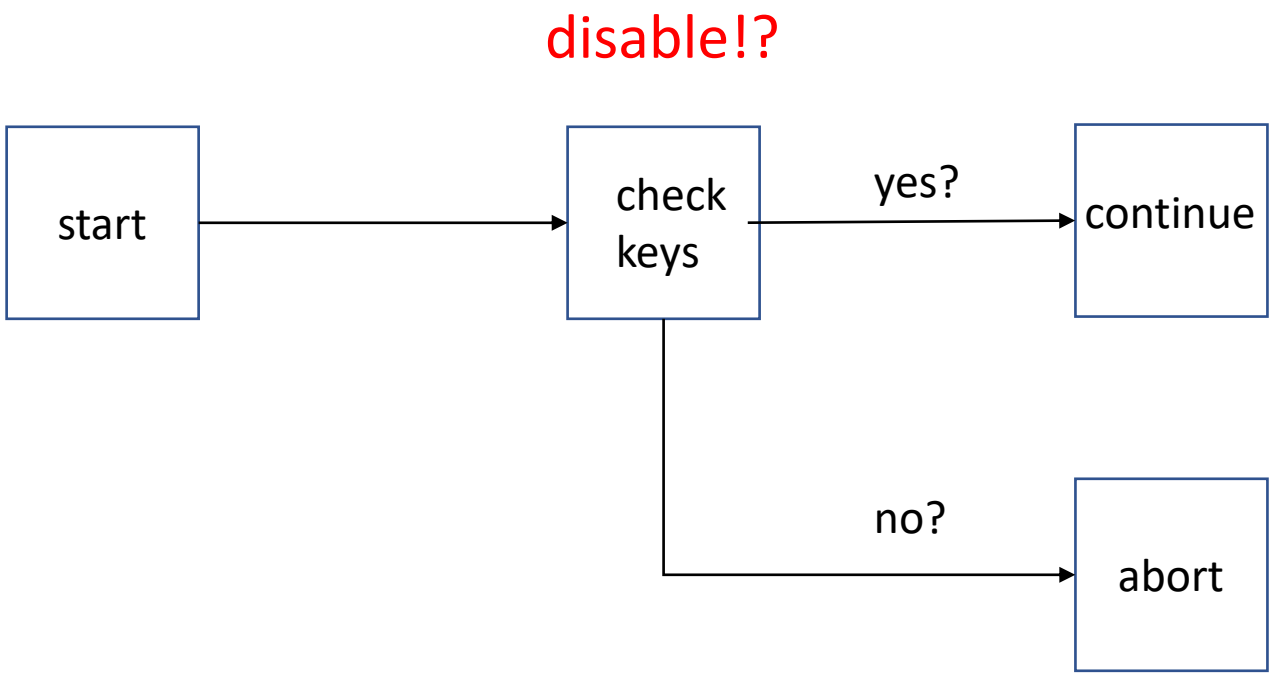


Disabling pinning

reverse-engineering toolkits

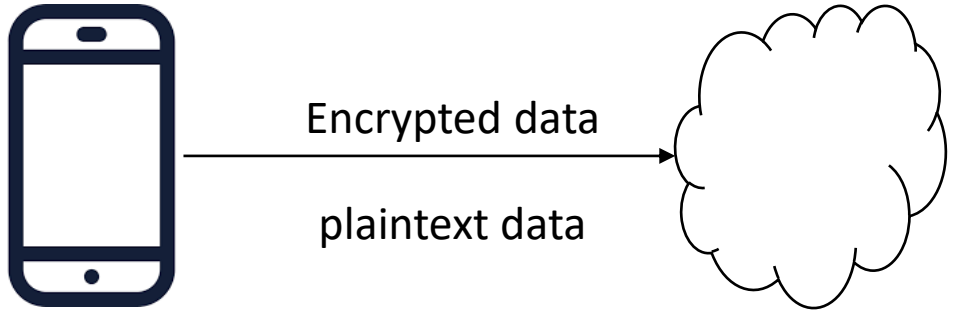
- Frida
- Xposed framework

App structure



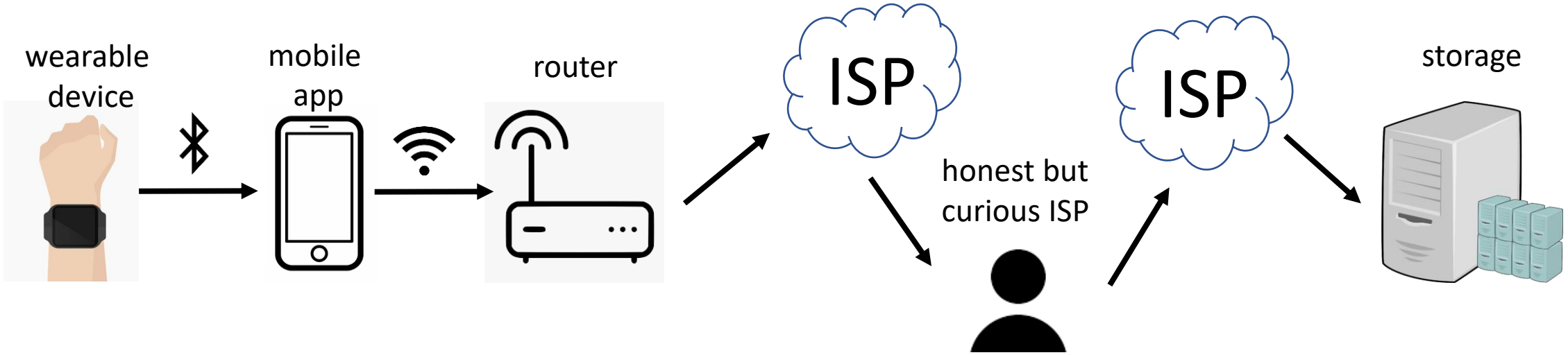
Data leaks

Data leaks



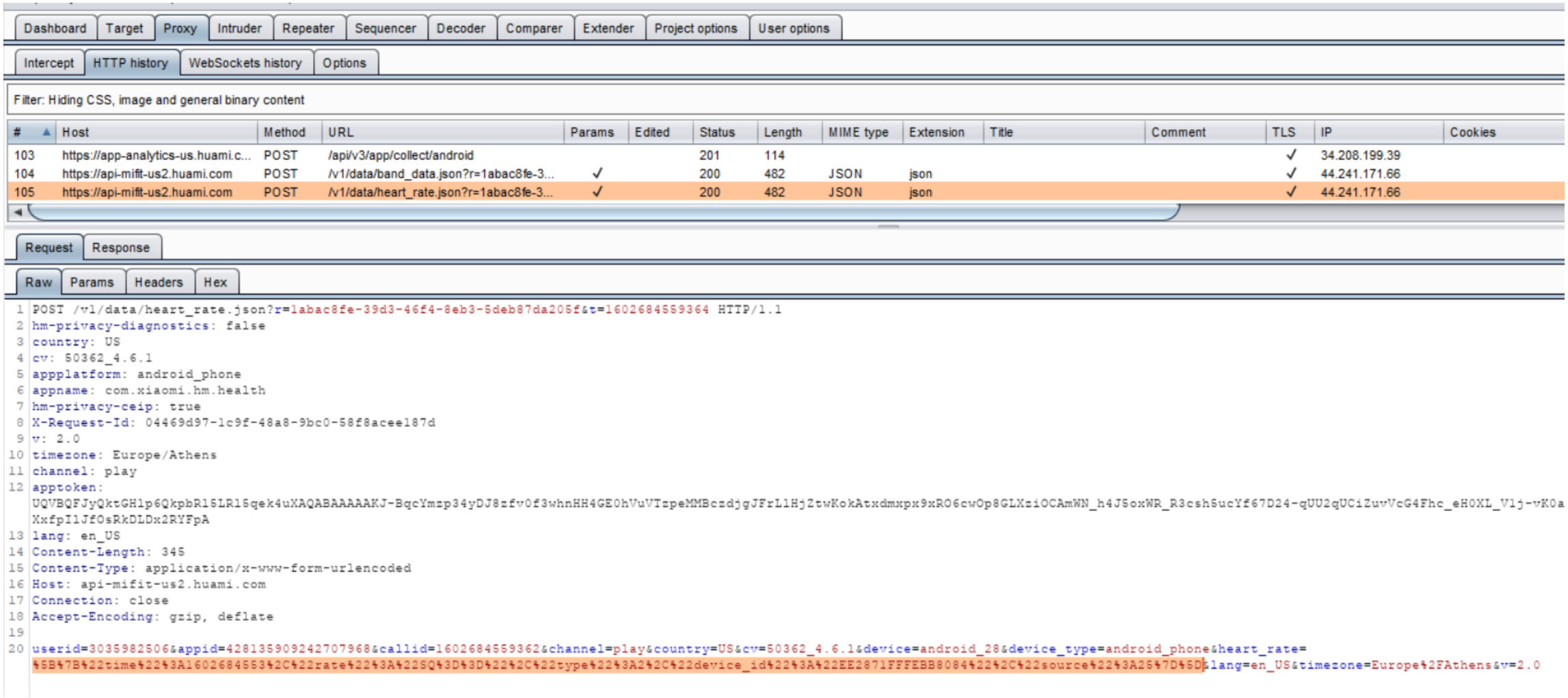
heartrate: 80 → ABCDEFGHIJKLM (13 char)
heartrate: 100 → ABCDEFGHIJKLMN (14 char)

Attack


wearable device
mobile app
router
ISP
honest but curious ISP
ISP
storage

Attack

- obtaining a copy of the smartband
- discovering the ground truth
- inferring the data leaks from encrypted traffic
- mass profiling end users of smartbands



[{"time":1602684553,"rate":"SQ==","type":2,"device_id":"EE2871FFFEBB8084","source":25}]

Mass profiling

- gathering all relevant IPs
- traffic filtering
- applying metadata rules

Why attack and smartbands?

- Controllable synchronization of activities.
- Absence of any countermeasures.
- Constant pull of possible IPs.

Detecting the adversary

- ISP?
- Country?
- Legislations?

Possible countermeasures

- Modifying plain text → cipher text size ratio
- Concealing frequency of packets transmission
- Introducing randomness for order of packets