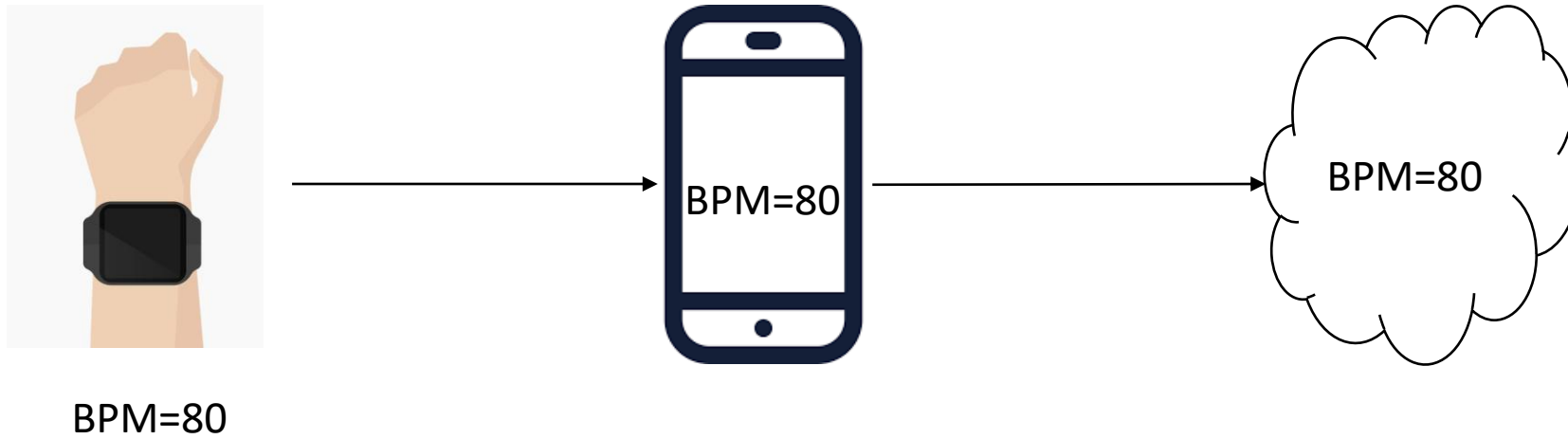
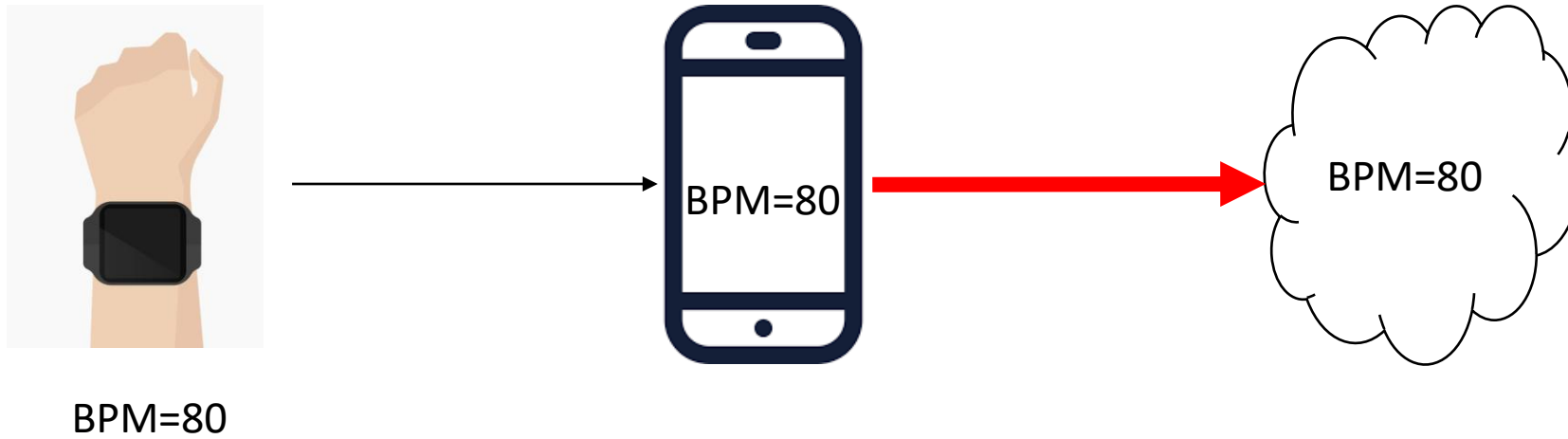


Data Leaks in health data transition

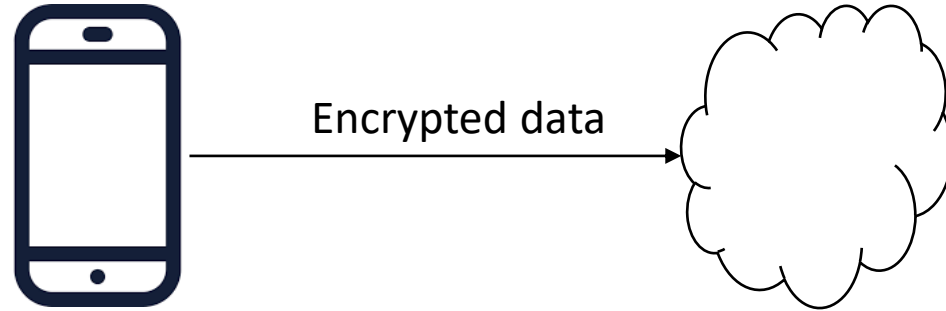
Where data can be attacked?



Between phone and cloud!



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



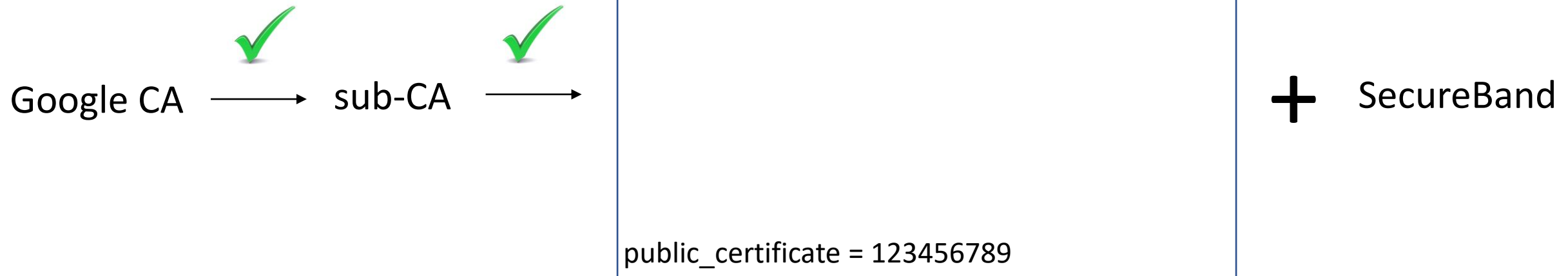
`https://:www.secureband.com`

`public_certificate = 123456789`

+

SecureBand

CA and certification

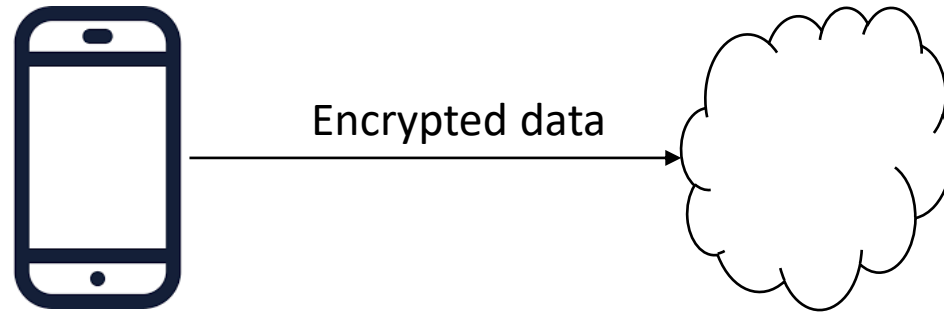


What doesn't TLS conceal?

- 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

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

Dashboard Target Proxy Intruder Repeater Sequencer Decoder Comparer Extender Project options User options

Intercept HTTP history WebSockets history Options

Filter: Hiding CSS, image and general binary content

#	Host	Method	URL	Params	Edited	Status	Length	MIME type	Extension	Title	Comment	TLS	IP	Cookies
103	https://app-analytics-us.huami.c...	POST	/api/v3/app/collect/android			201	114					✓	34.208.199.39	
104	https://api-mifit-us2.huami.com	POST	/v1/data/band_data.json?r=1abac8fe-3...	✓		200	482	JSON	json			✓	44.241.171.66	
105	https://api-mifit-us2.huami.com	POST	/v1/data/heart_rate.json?r=1abac8fe-3...	✓		200	482	JSON	json			✓	44.241.171.66	

Request Response

Raw Params Headers Hex

```

1 POST /v1/data/heart_rate.json?r=1abac8fe-39d3-46f4-8eb3-5deb87da205f&t=1602684559364 HTTP/1.1
2 hm-privacy-diagnostics: false
3 country: US
4 cv: 50362_4.6.1
5 appplatform: android_phone
6 appname: com.xiaomi.hm.health
7 hm-privacy-ceip: true
8 X-Request-Id: 04469d97-1c9f-48a8-9bc0-58f8acee187d
9 v: 2.0
10 timezone: Europe/Athens
11 channel: play
12 apptoken:
  UQVBQFJyQktGH1p6QkpbR1SLR1Sgex4uXAQABAAAAKJ-BqcYmzp34yDJ8zfv0f3whnHH4GE0hVuVTzpeMMBczdjgJFrL1HjZtwKokAtxdmxx9xRO6cwOp8GLXziOCaMWN_h4J6oxWR_R3eshSucYf67D24-qUU2qUCiZuvVcG4Fhc_eH0XL_V1j-vK0a
  XxfpI1JfOsRkDLDx2RYFpA
13 lang: en_US
14 Content-Length: 345
15 Content-Type: application/x-www-form-urlencoded
16 Host: api-mifit-us2.huami.com
17 Connection: close
18 Accept-Encoding: gzip, deflate
19
20 userid=3035982506&appid=428135909242707968&callid=1602684559362&channel=play&country=US&cv=50362_4.6.1&device=android_28&device_type=android_phone&heart_rate=
  %5B%7B%22time%22%3A1602684553%2C%22rate%22%3A%22SQ%3D%3D%22%2C%22type%22%3A%2C%22device_id%22%3A%22EE2871FFFEBB8084%22%2C%22source%22%3A%22%3D%5D%lang=en_US&timezone=Europe%2FAthens&v=2.0

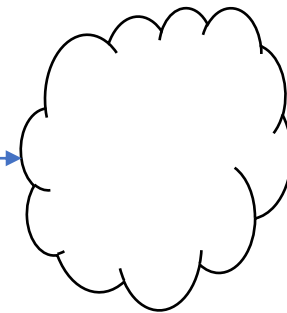
```

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

MITM and certificates

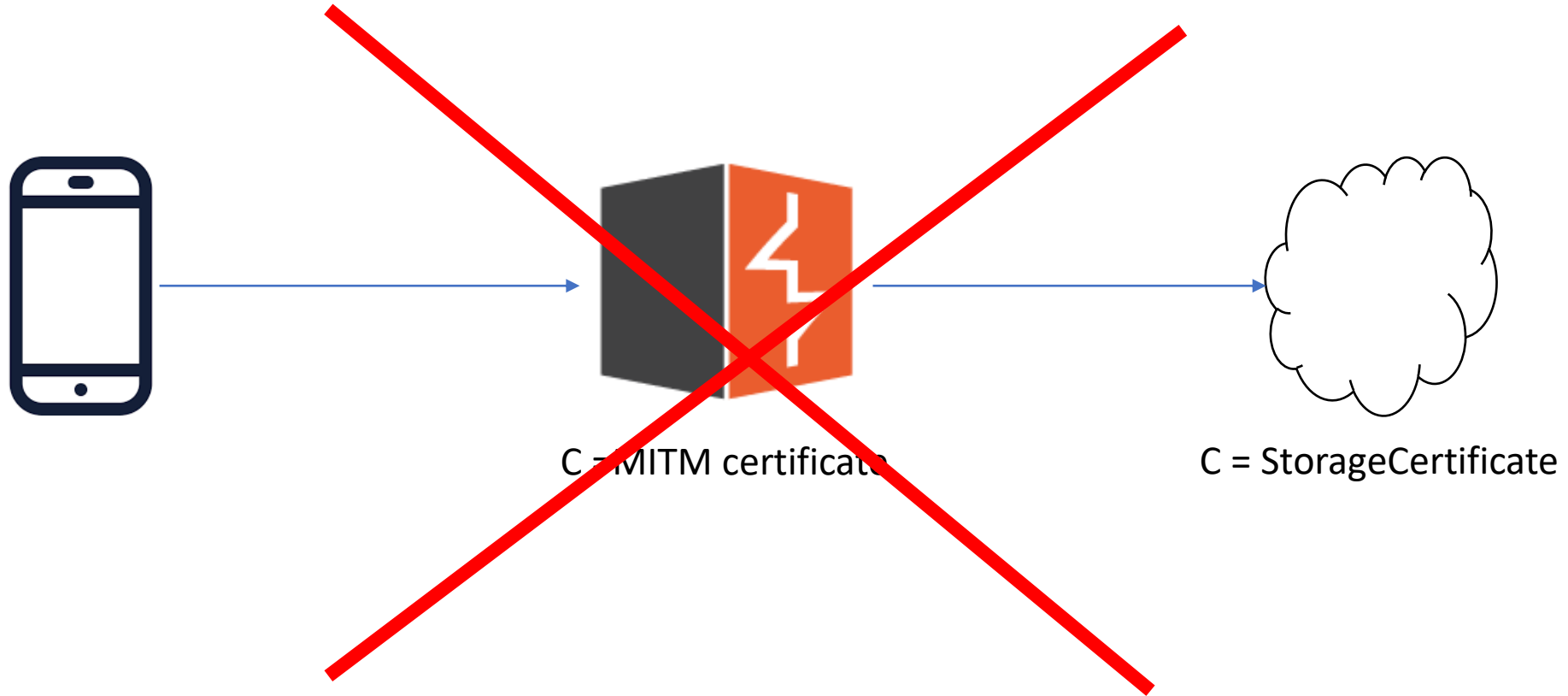


C = MITM certificate



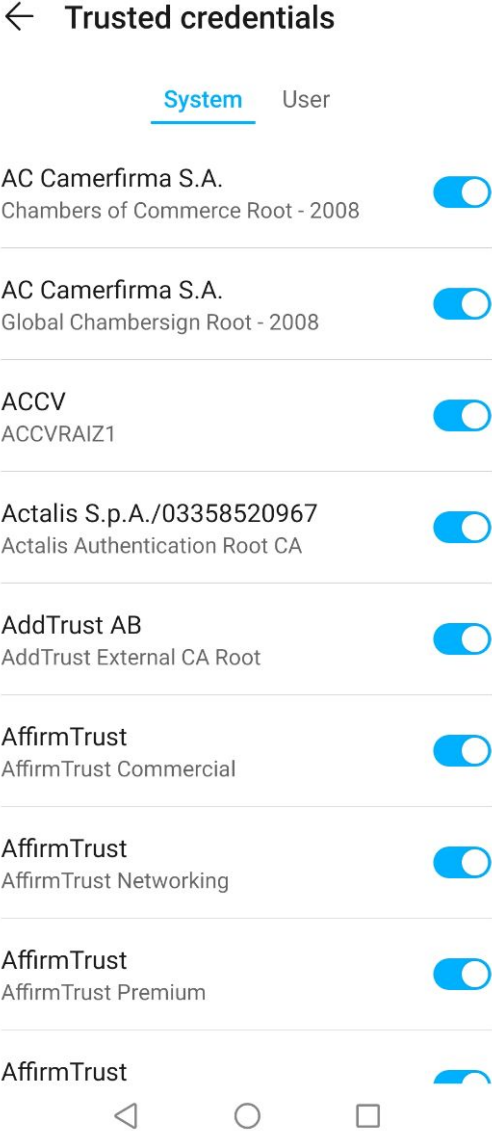
C = StorageCertificate

MITM and certificates

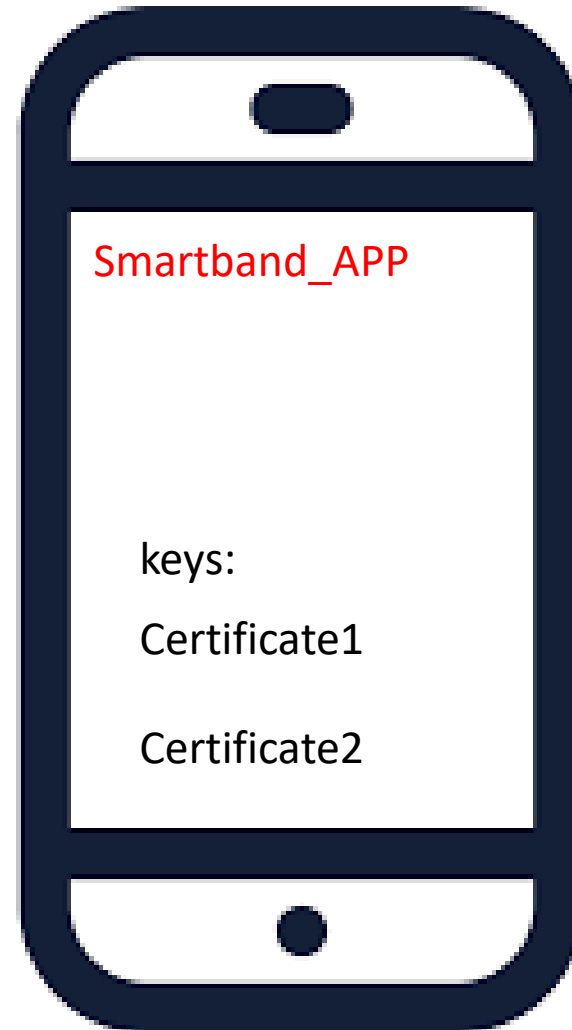


Trusted certificates

Need to install MITM certificate



Certificate pinning

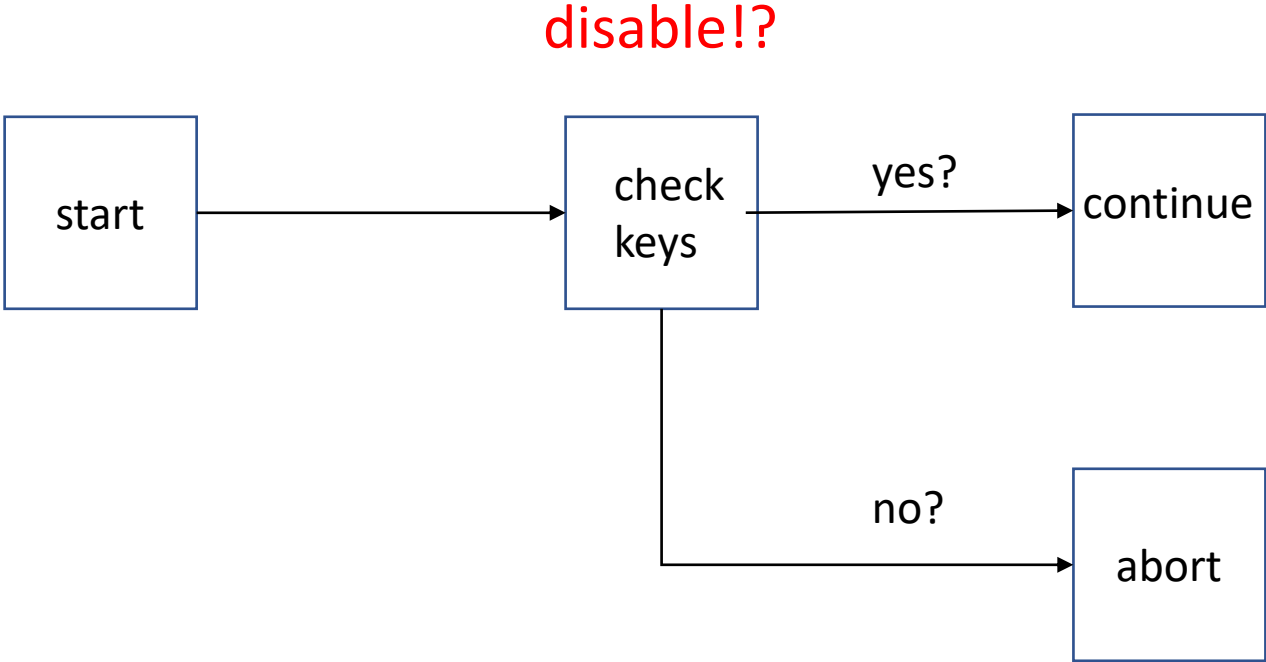


Disabling pinning

reverse-engineering toolkits

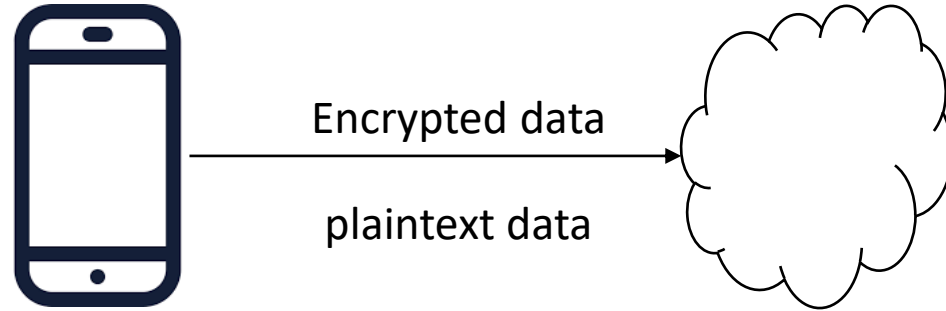
- Frida
- Xposed framework

App structure



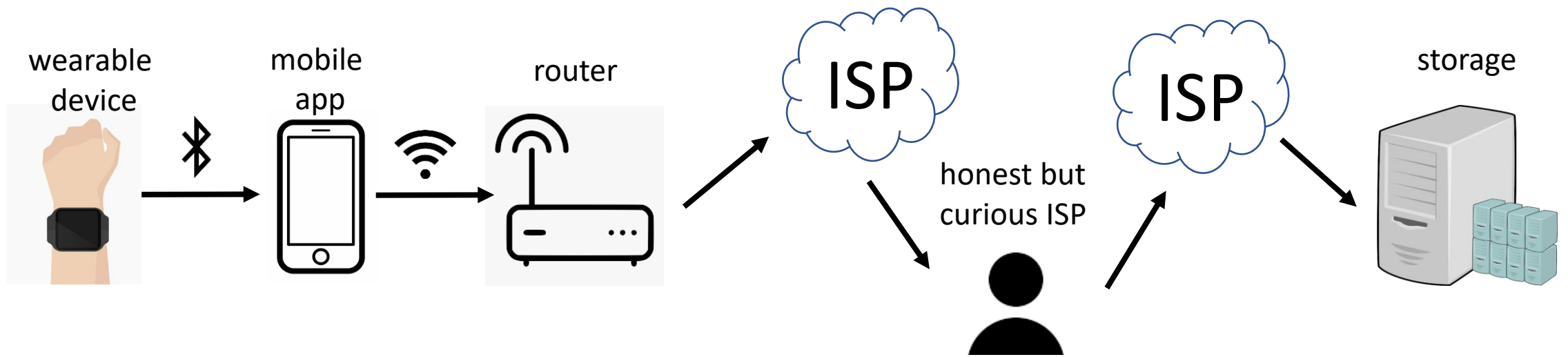
Data leaks

Data leaks



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

Attack



Attack

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

Dashboard Target Proxy Intruder Repeater Sequencer Decoder Comparer Extender Project options User options

Intercept HTTP history WebSockets history Options

Filter: Hiding CSS, image and general binary content

#	Host	Method	URL	Params	Edited	Status	Length	MIME type	Extension	Title	Comment	TLS	IP	Cookies
103	https://app-analytics-us.huami.c...	POST	/api/v3/app/collect/android			201	114					✓	34.208.199.39	
104	https://api-mifit-us2.huami.com	POST	/v1/data/band_data.json?r=1abac8fe-3...	✓		200	482	JSON	json			✓	44.241.171.66	
105	https://api-mifit-us2.huami.com	POST	/v1/data/heart_rate.json?r=1abac8fe-3...	✓		200	482	JSON	json			✓	44.241.171.66	

Request Response

Raw Params Headers Hex

```

1 POST /v1/data/heart_rate.json?r=1abac8fe-39d3-46f4-8eb3-5deb87da205f&t=1602684559364 HTTP/1.1
2 hm-privacy-diagnostics: false
3 country: US
4 cv: 50362_4.6.1
5 appplatform: android_phone
6 appname: com.xiaomi.hm.health
7 hm-privacy-ceip: true
8 X-Request-Id: 04469d97-1c9f-48a8-9bc0-58f8acee187d
9 v: 2.0
10 timezone: Europe/Athens
11 channel: play
12 aptoken:
  UQVBQFJyQktGH1p6QkpbR1SLR1Sgex4uXAQABAAAAKJ-BqcYmsp34yDJ8zfv0f3whnHH4GE0hVuVTzpeMMBczdjgJFrL1HjZtwKokAtxdmxx9xRO6cwOp8GLXziOCaMWN_h4J6oxWR_R3eshSucYf67D24-qUU2qUCiZuvVcG4Fhc_eH0XL_V1j-vK0a
  XxfpI1JfOsRkDLDx2RYFpA
13 lang: en_US
14 Content-Length: 345
15 Content-Type: application/x-www-form-urlencoded
16 Host: api-mifit-us2.huami.com
17 Connection: close
18 Accept-Encoding: gzip, deflate
19
20 userid=3035982506&appid=428135909242707968&callid=1602684559362&channel=play&country=US&cv=50362_4.6.1&device=android_28&device_type=android_phone&heart_rate=
  %5B%7B%22time%22%3A1602684553%2C%22rate%22%3A%22SQ%3D%3D%22%2C%22type%22%3A%2C%22device_id%22%3A%22EE2871FFFEBB8084%22%2C%22source%22%3A%22%3D%5D%lang=en_US&timezone=Europe%2FAthens&v=2.0

```

[{"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