WISA 2015

BurnFit: Analyzing and Exploiting Wearable Devices

2015. 08. 21.

Dongkwan Kim, Suwan Park, Kibum Choi, and Yongdae Kim

Korea Advanced Institute of Science and Technology

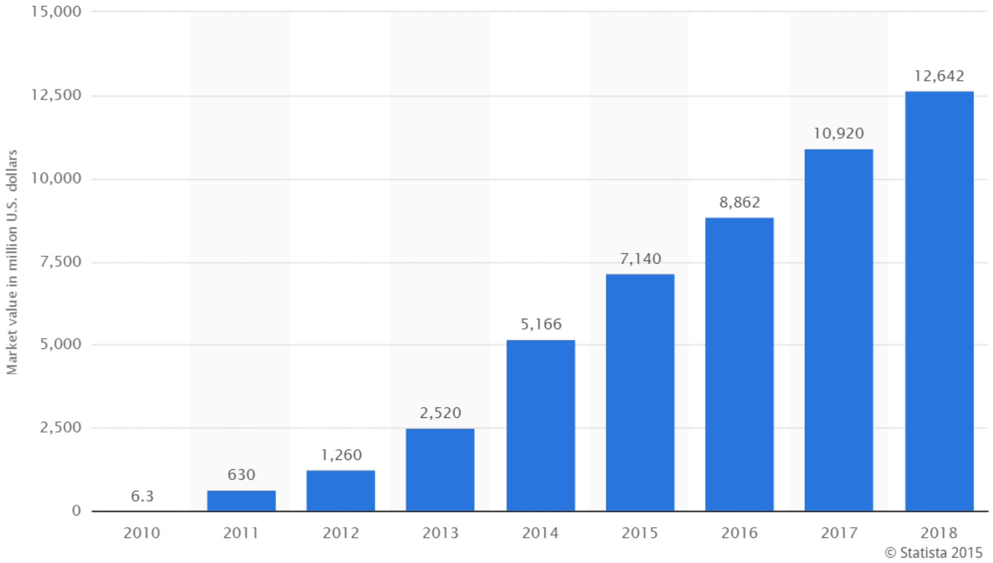
System Security Lab.

KAIST

SysSec
System Security Lab

Wearable Devices, a New Threat

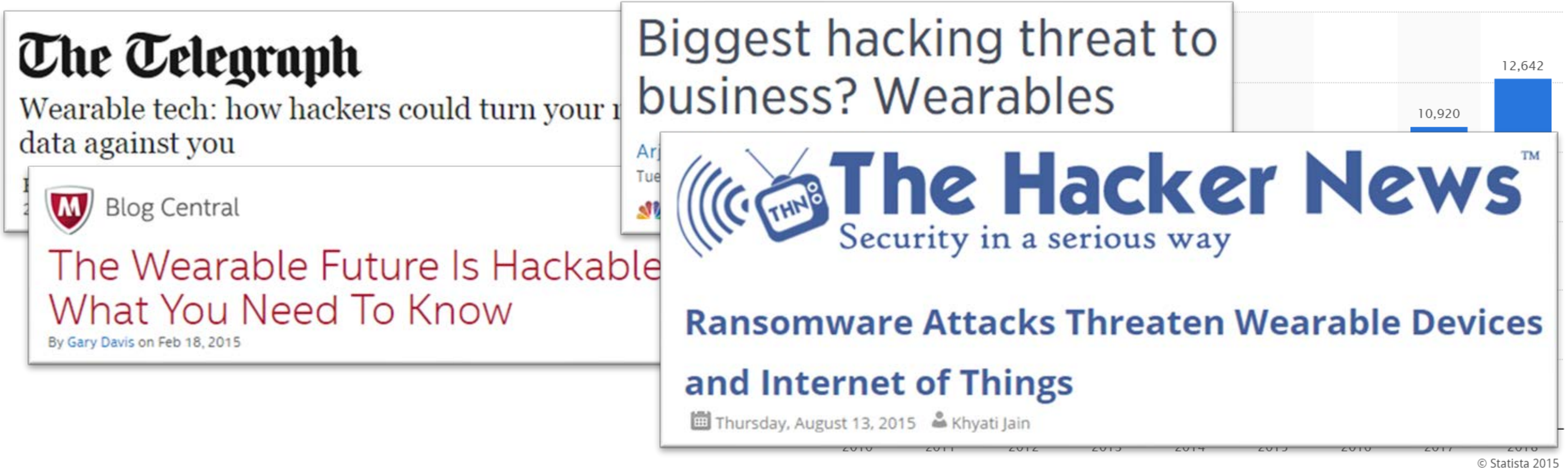
- Increasing demands for wearable devices
  - Experts are expecting market share reach $13 billion by 2018



© Statista 2015

Wearable Devices, a New Threat

- ❖ Increasing demands for wearable devices
  - Experts are expecting market share reach $13 billion by 2018
- ❖ **Hacking attempts are increasing!**



The Telegraph

Wearable tech: how hackers could turn your r
data against you

Biggest hacking threat to business? Wearables

Ar
Tue

Blog Central

The Wearable Future Is Hackable
What You Need To Know

By Gary Davis on Feb 18, 2015

The Hacker News™

Security in a serious way

Ransomware Attacks Threaten Wearable Devices and Internet of Things

Thursday, August 13, 2015 Khyati Jain

Wearable Devices, for What?

- On the rise in personal and business use,

Wearable Devices, for What?

- On the rise in personal and business use,
  - Healthcare & Medical purpose
    - Detecting health disorders

Wearable Devices, for What?

- On the rise in personal and business use,
  - Healthcare & Medical purpose
    - Detecting health disorders
  - Professional sports
    - Monitoring activity results
    - Receiving real-time feedback

Wearable Devices, for What?

- On the rise in personal and business use,
  - Healthcare & Medical purpose
    - Detecting health disorders
  - Professional sports
    - Monitoring activity results
    - Receiving real-time feedback
  - Convenience (Watch)

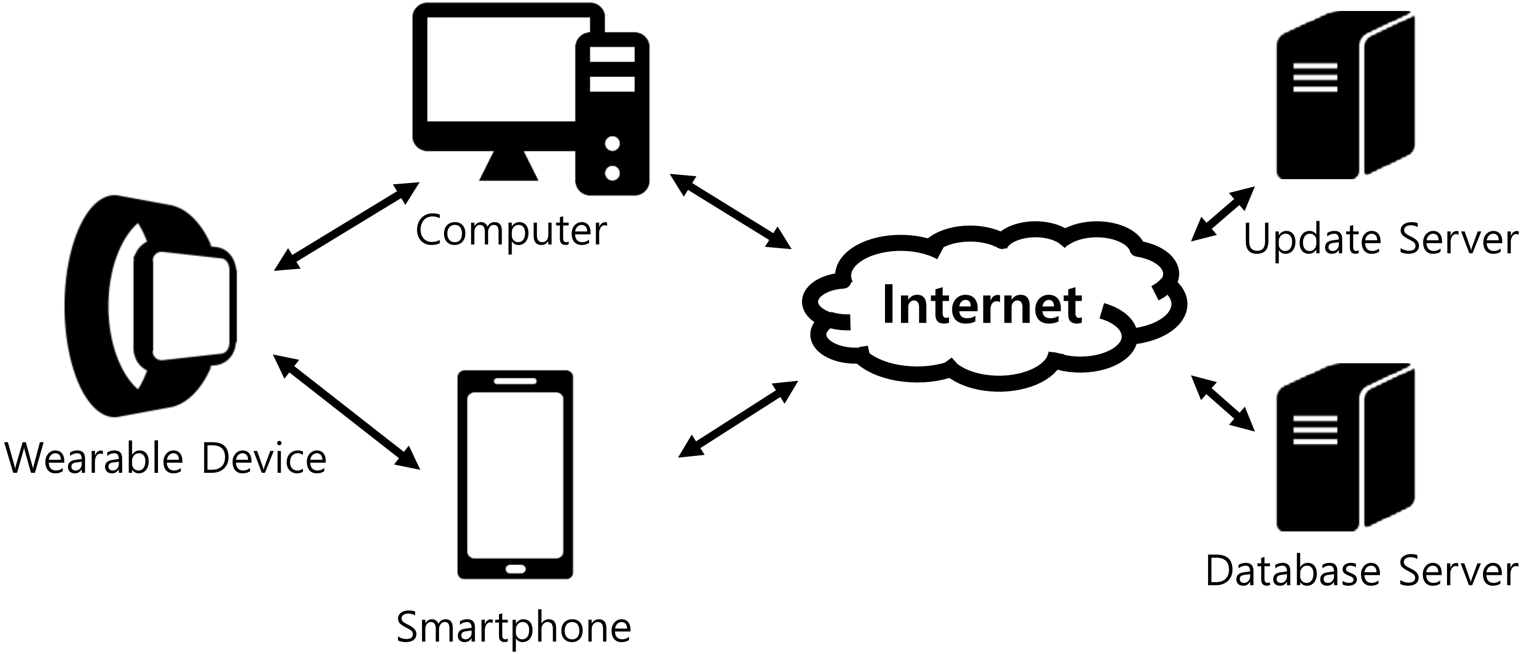
© 2013 CBS Interactive

Wearable Devices, for What?

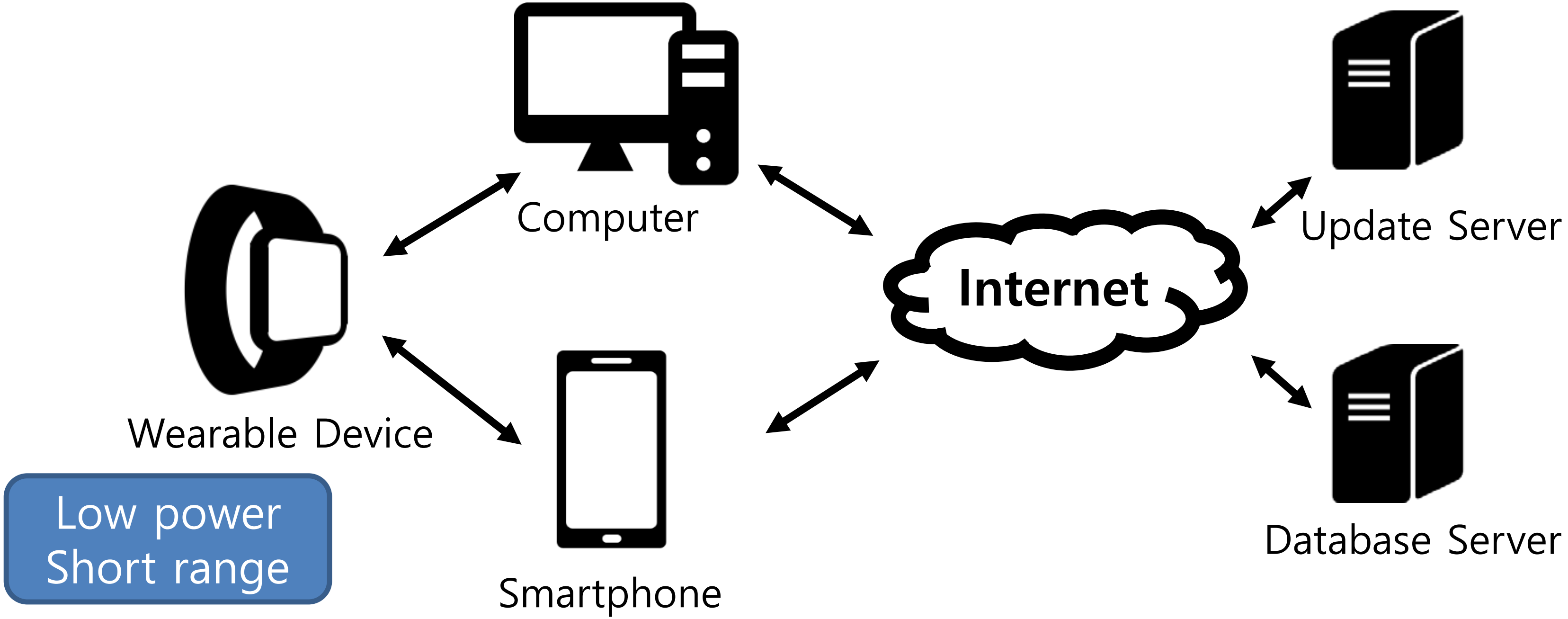
- On the rise in personal and business use,
  - Healthcare & Medical purpose
    - Detecting health disorders
  - Professional sports
    - Monitoring activity results
    - Receiving real-time feedback
  - Convenience (Watch)
  - Fashion or Show-off

© 2013 CBS Interactive

Communication Overview

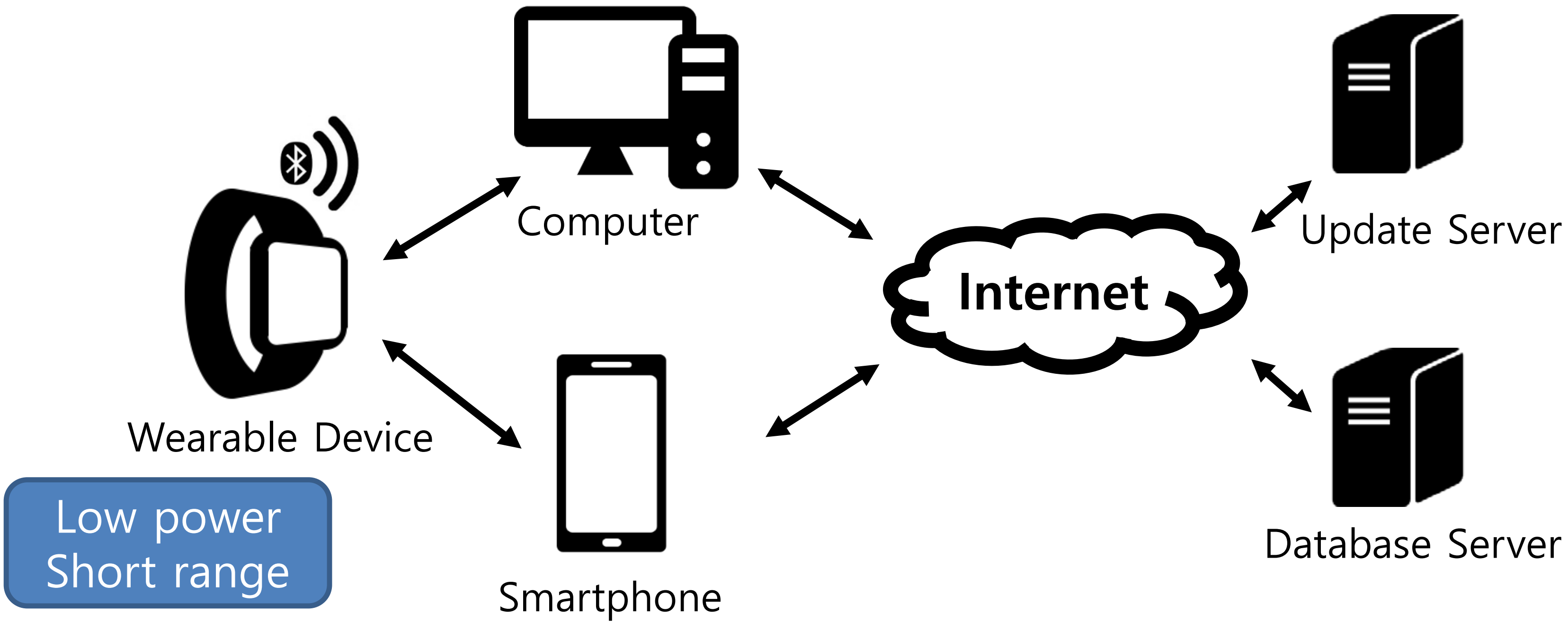


Communication Overview



Low power
Short range

Communication Overview



Computer

Wearable Device

Smartphone

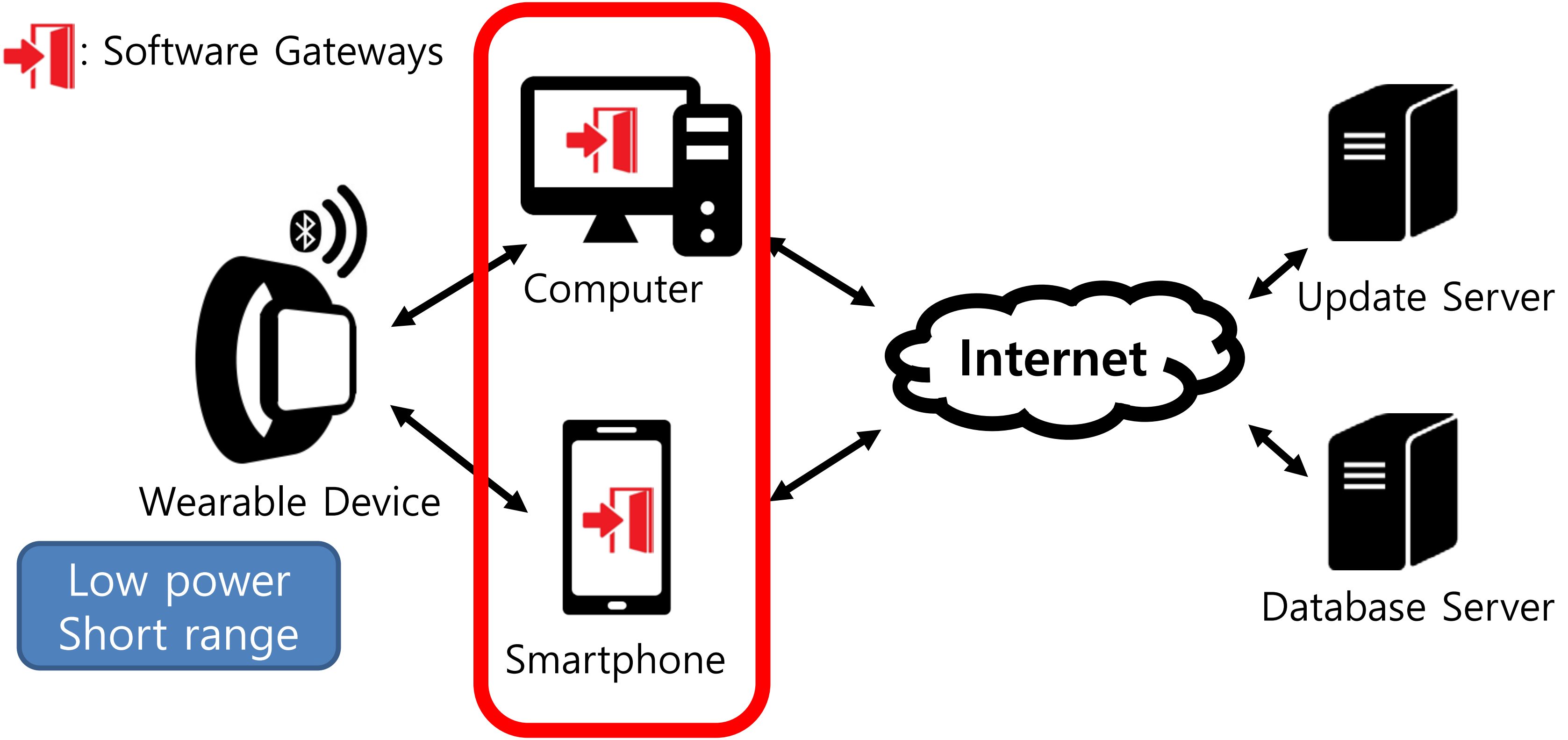
Internet

Update Server

Database Server

Low power
Short range

Communication Overview



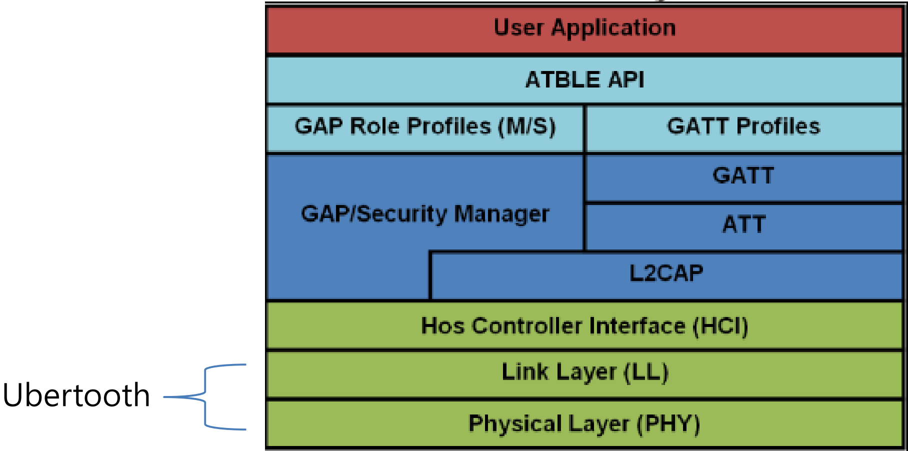
: Software Gateways

Low power
Short range

Bluetooth Low Energy (BLE)

- Bluetooth 4.0, Bluetooth Smart
- Features
  - New PHY and Link layer (for low power)
  - Same high-level protocols (L2CAP, ATT)
  - 40 channels in 2.4 GHz
  - Smartphones, medical/sports/fitness devices

- How to exploit
  - Ubertooth (Ossmann, M., 2012)
  - Recover hop interval
    - Sit on data channel and wait
  - 6-digit temporary key (TK)
    - takes < 1 sec to crack



User Application

ATBLE API

GAP Role Profiles (M/S)

GATT Profiles

GATT

GAP/Security Manager

ATT

L2CAP

Hos Controller Interface (HCI)

Link Layer (LL)

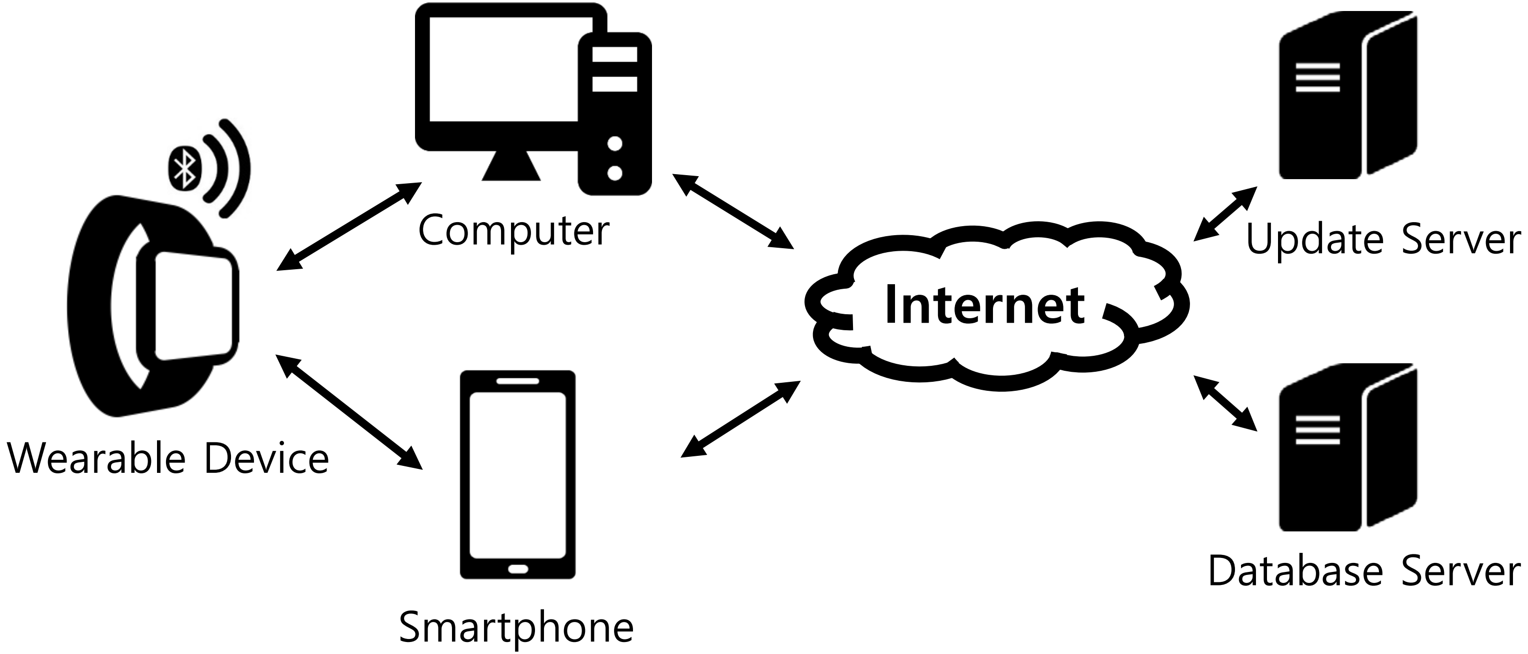
Physical Layer (PHY)

Ubertooth

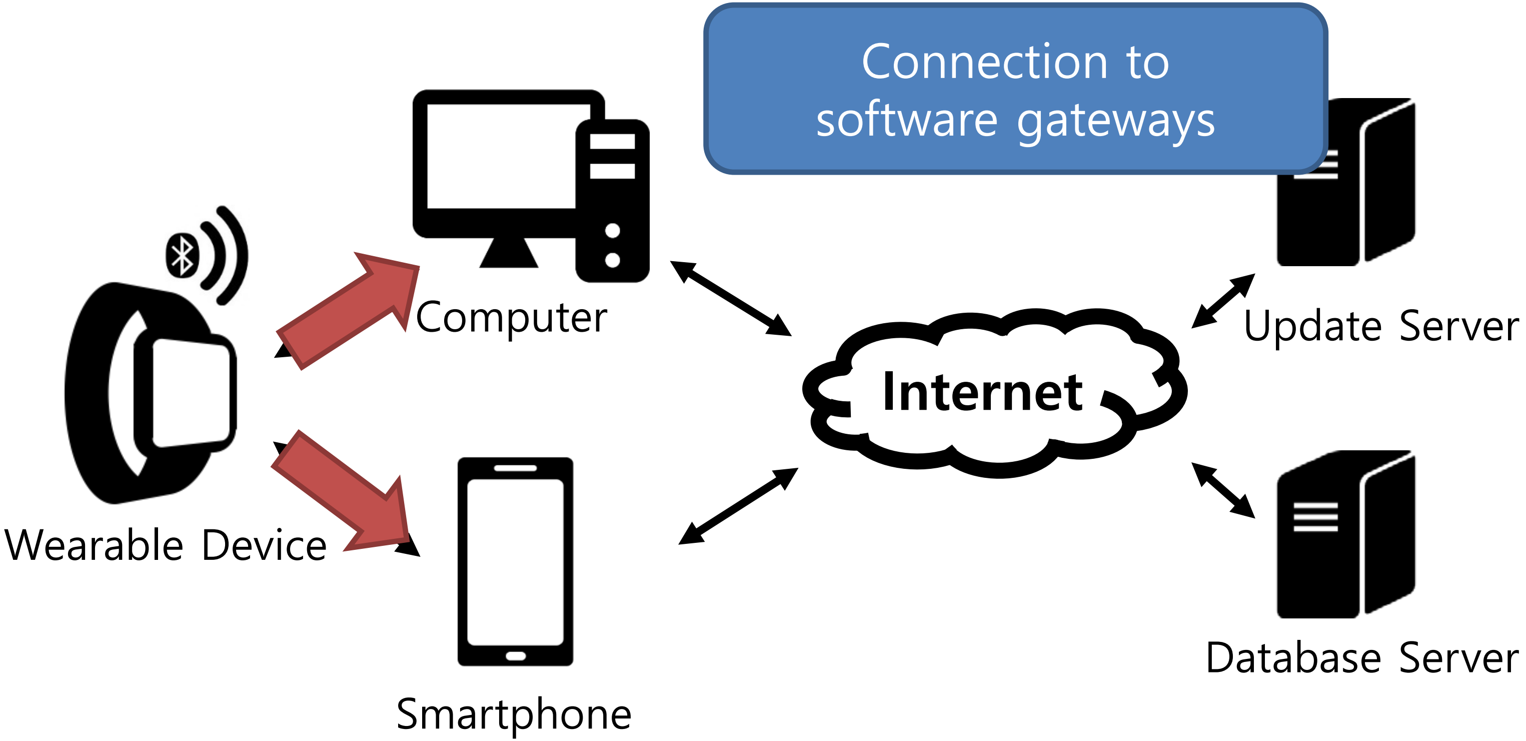
Ryan, M., Bluetooth: With low energy comes low security, WOOT 2013

http://www.blueradios.com/hardware_LE4.0-S2.htm

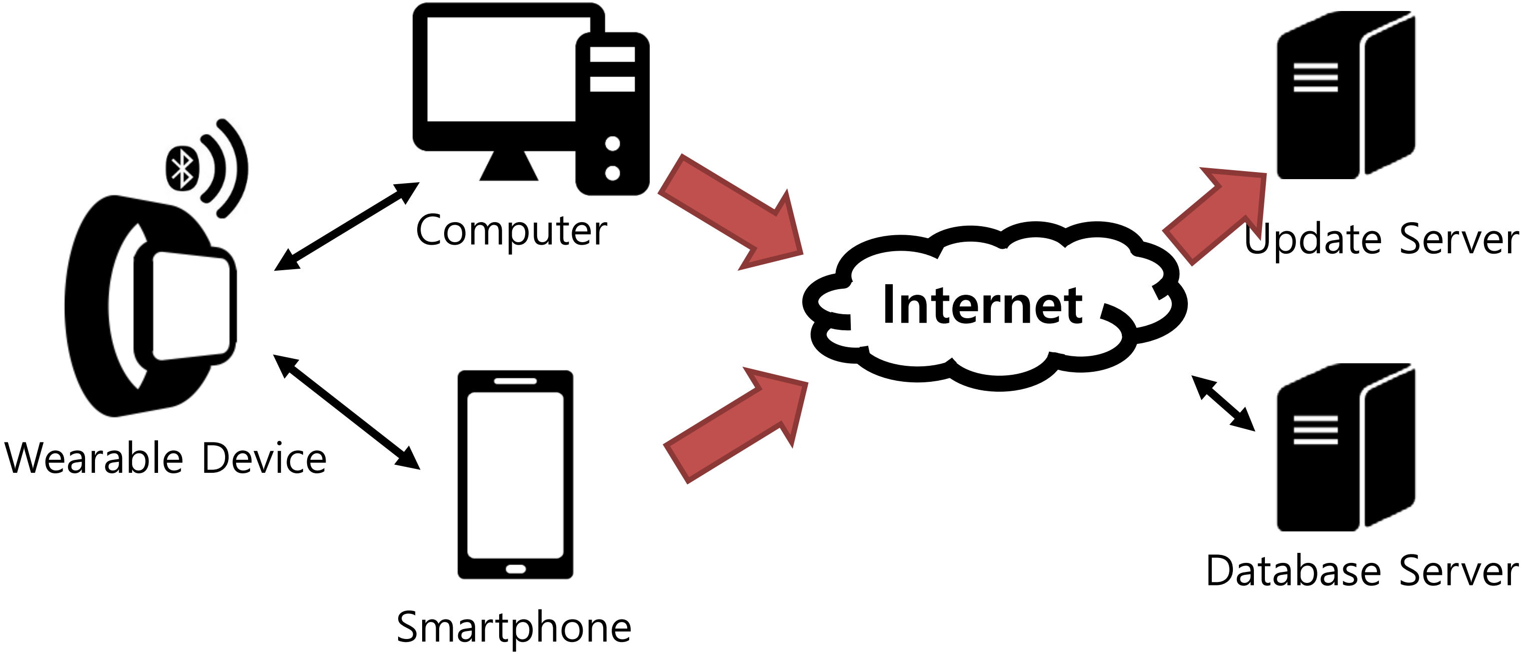
Communication Overview



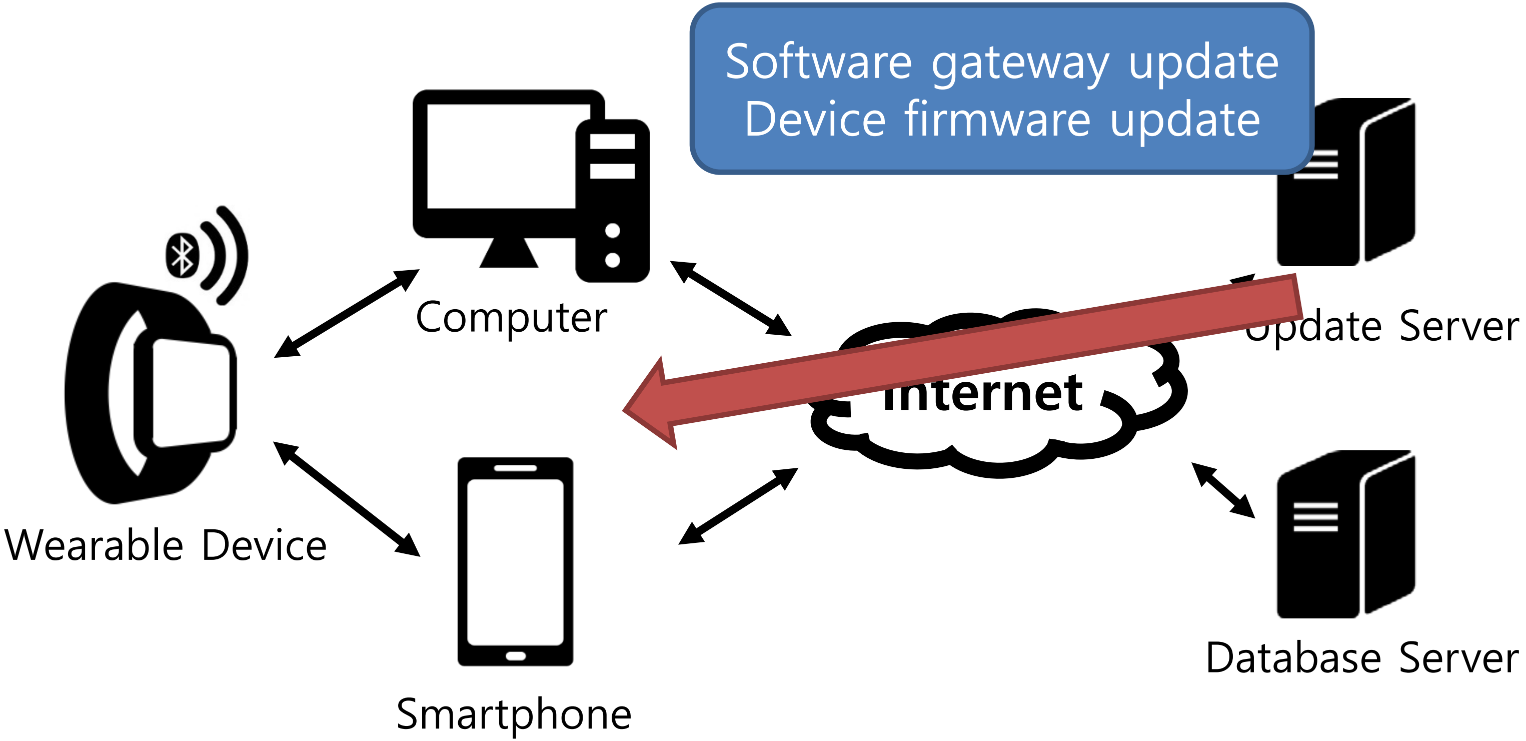
Communication Overview



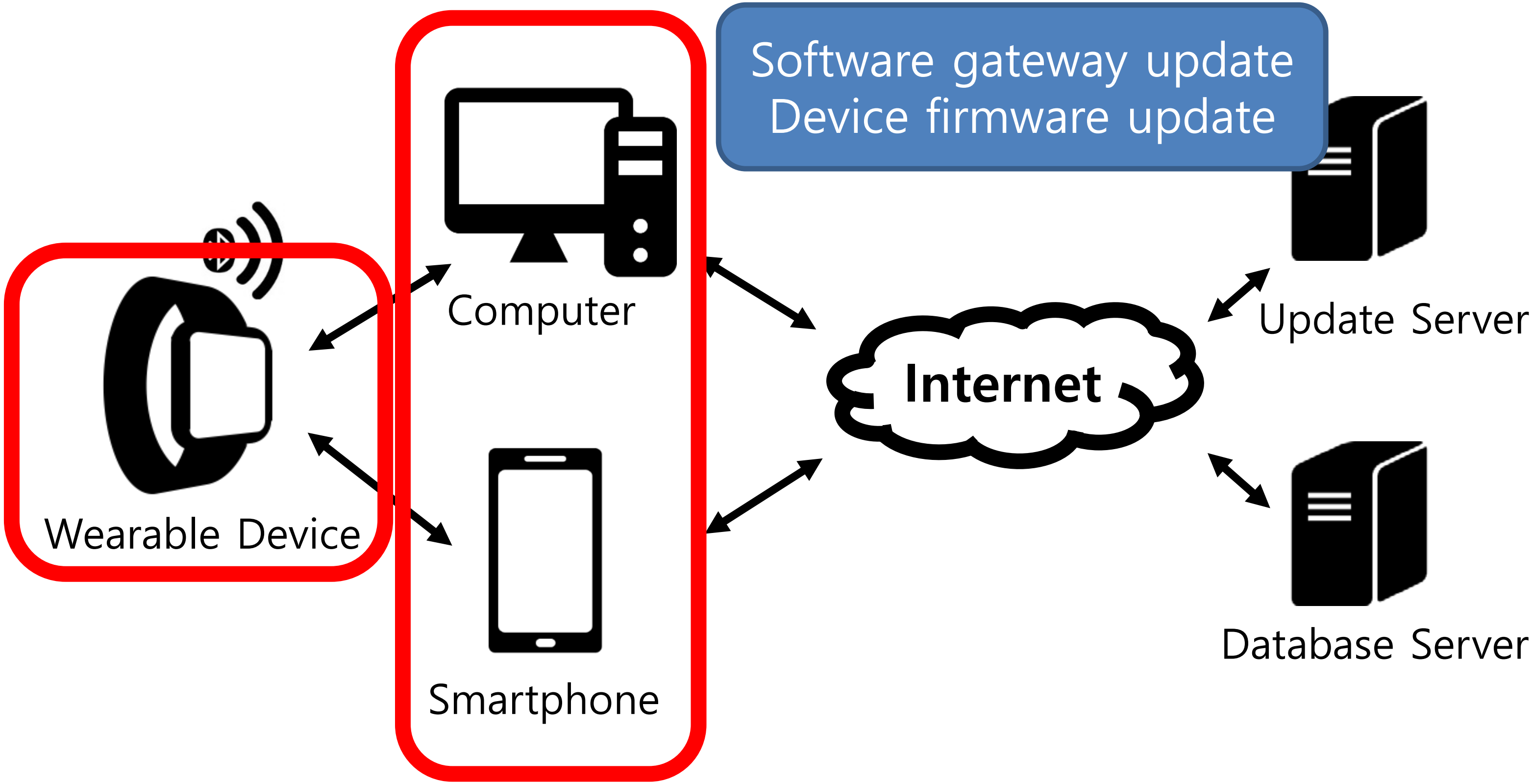
Communication Overview



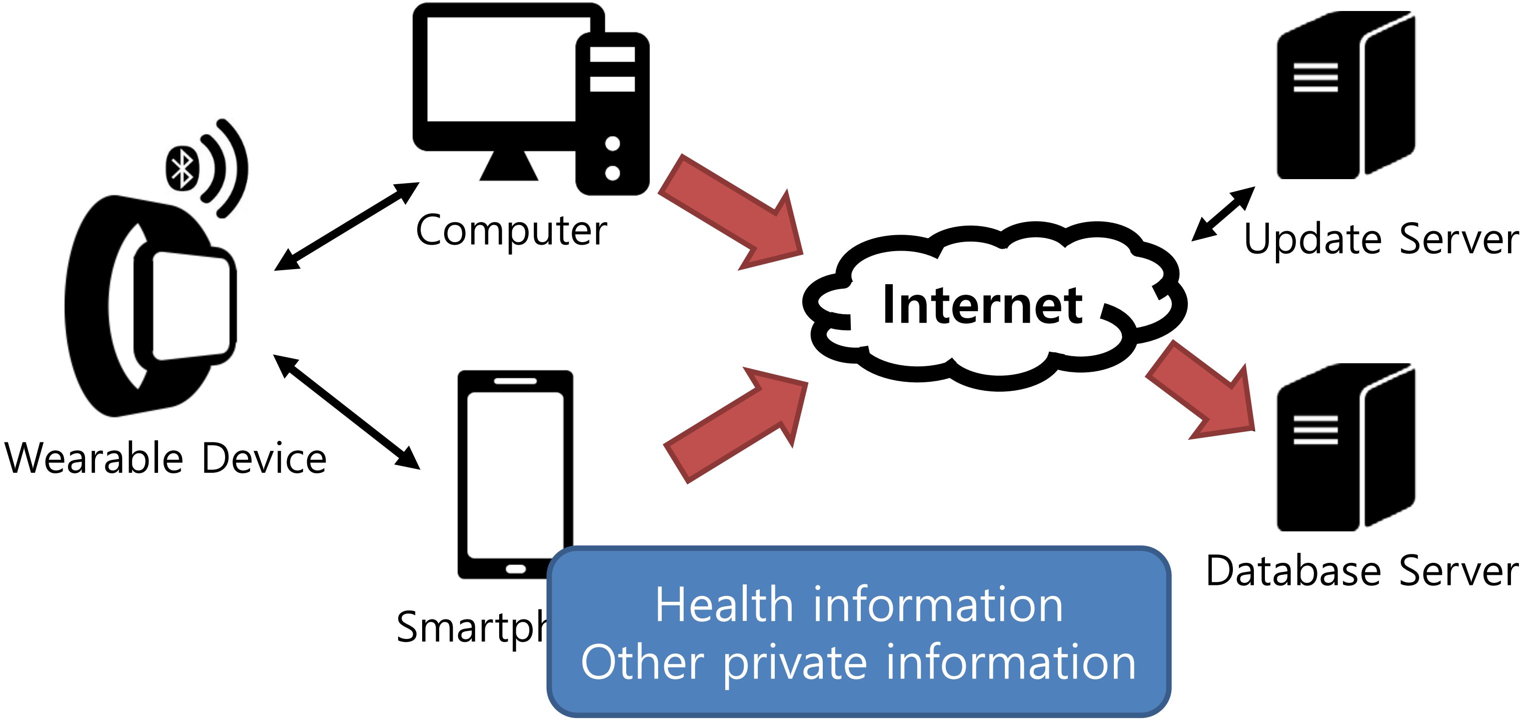
Communication Overview



Communication Overview

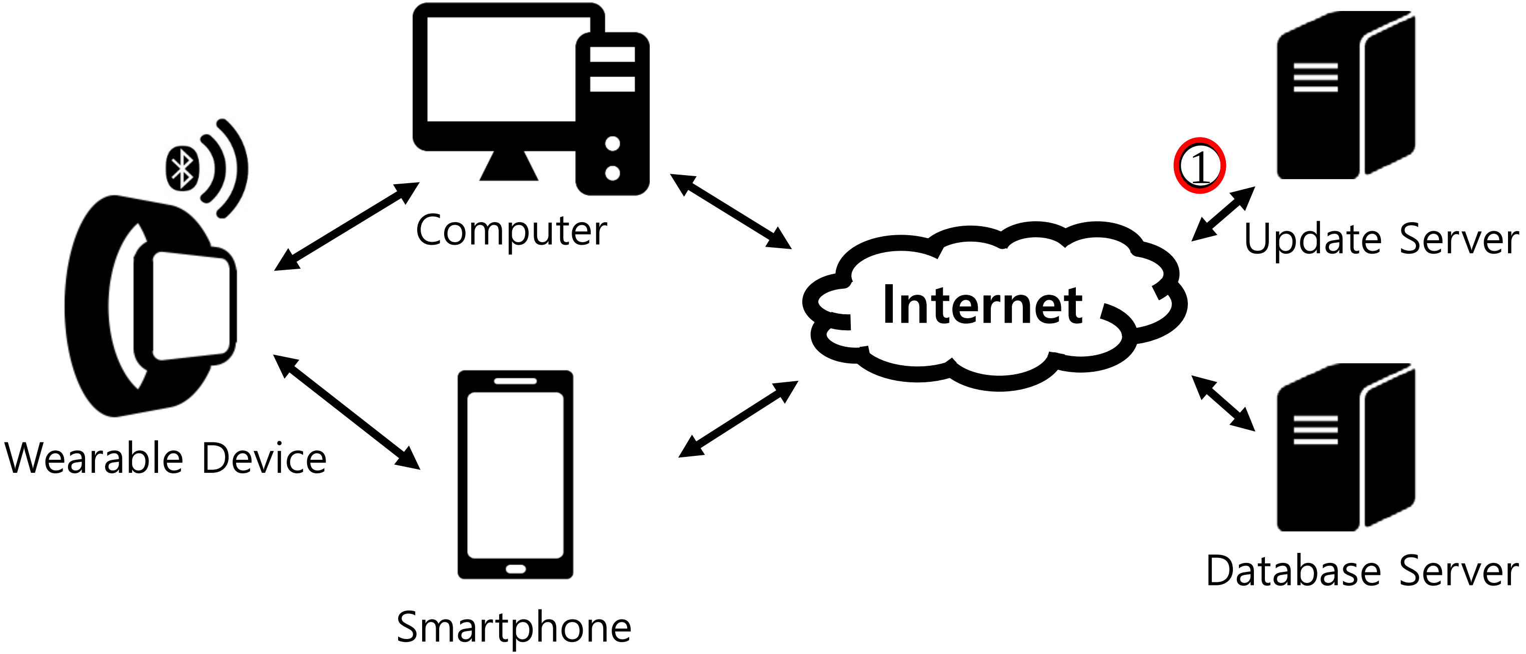


Communication Overview

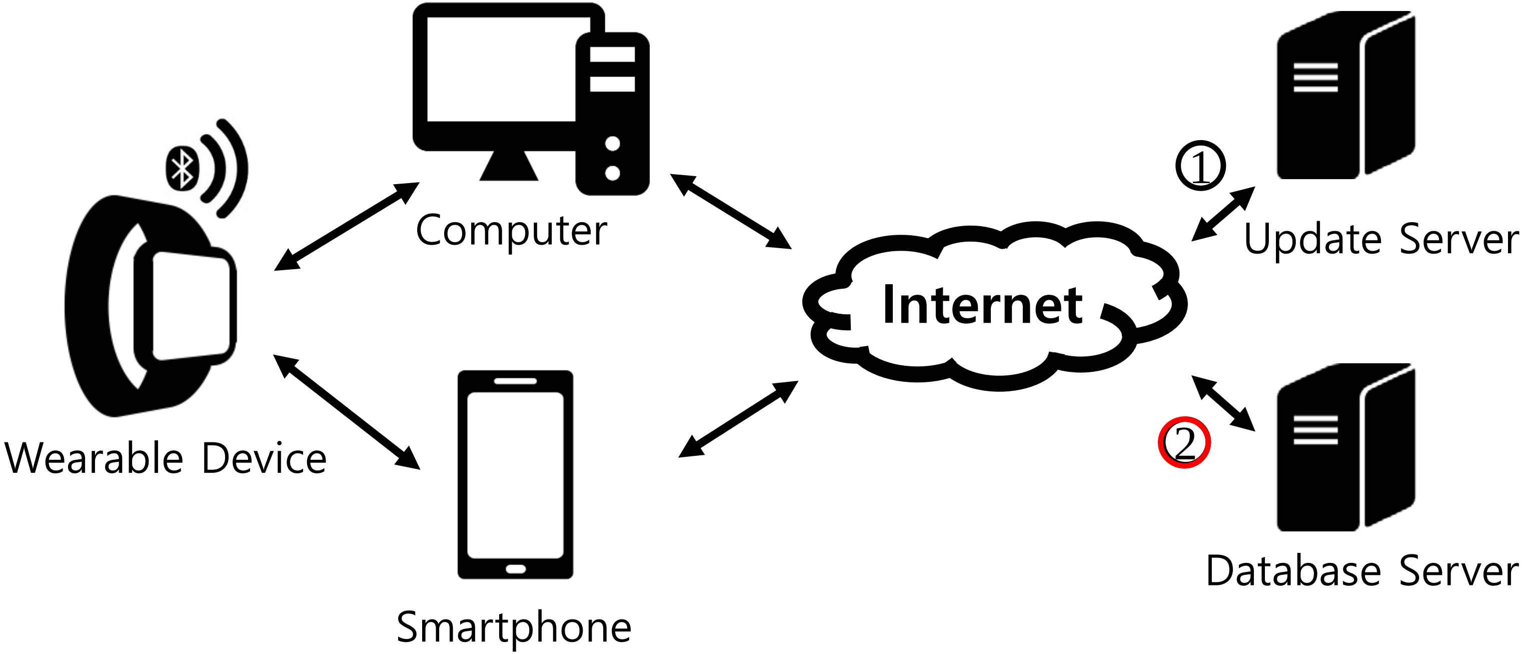


Health information
Other private information

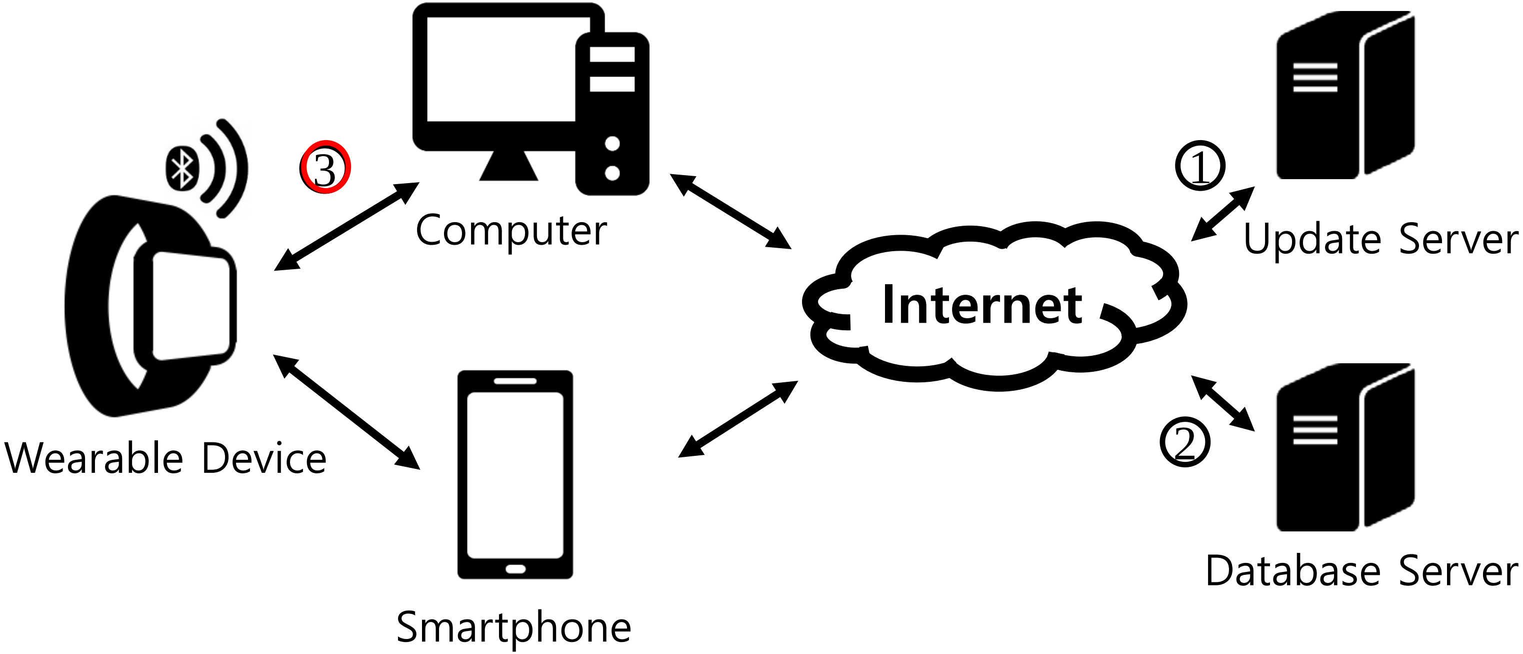
Communication Overview



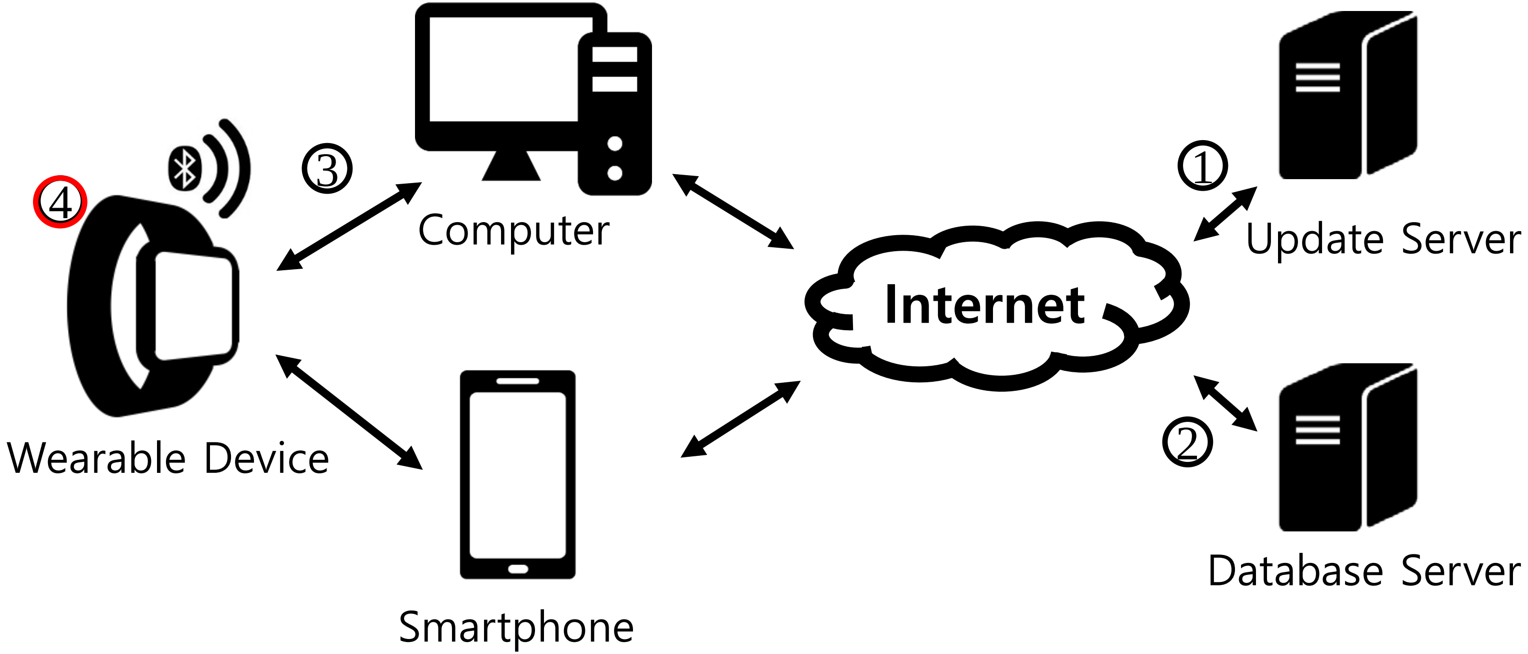
Communication Overview



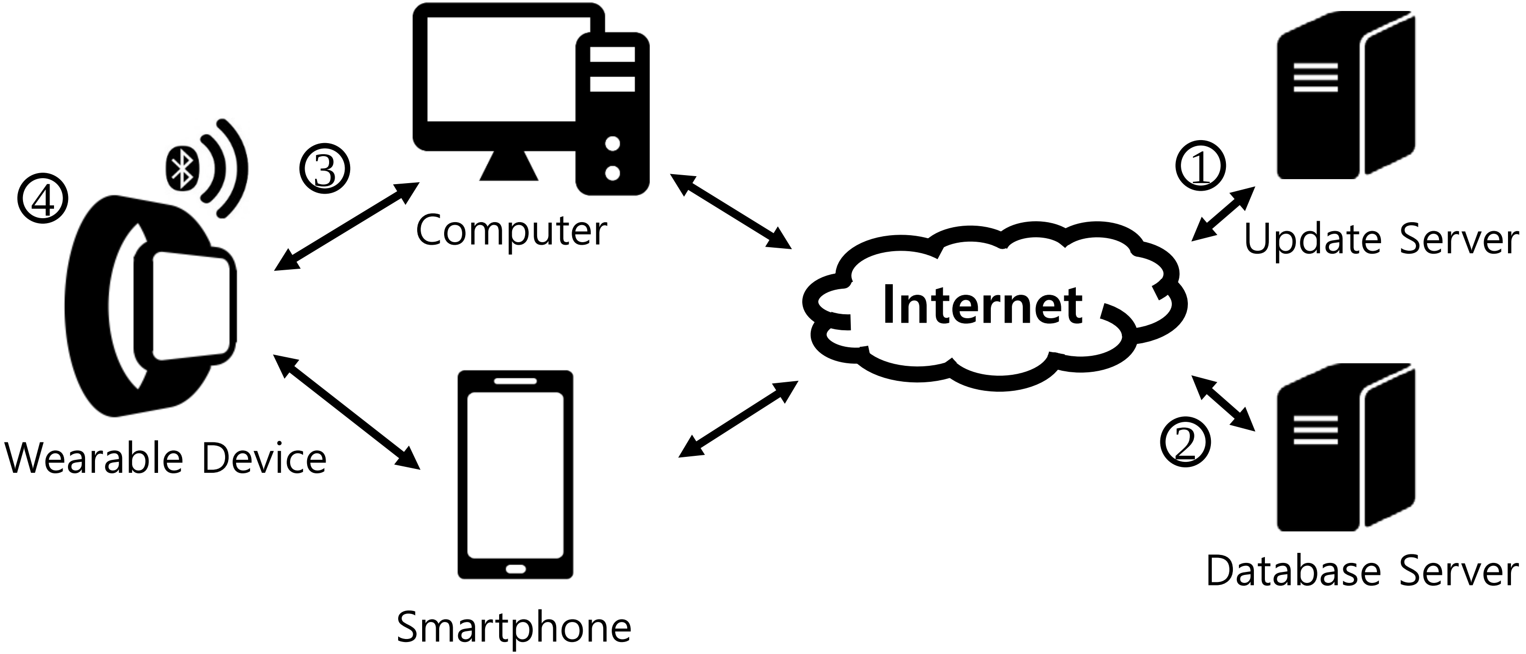
Communication Overview



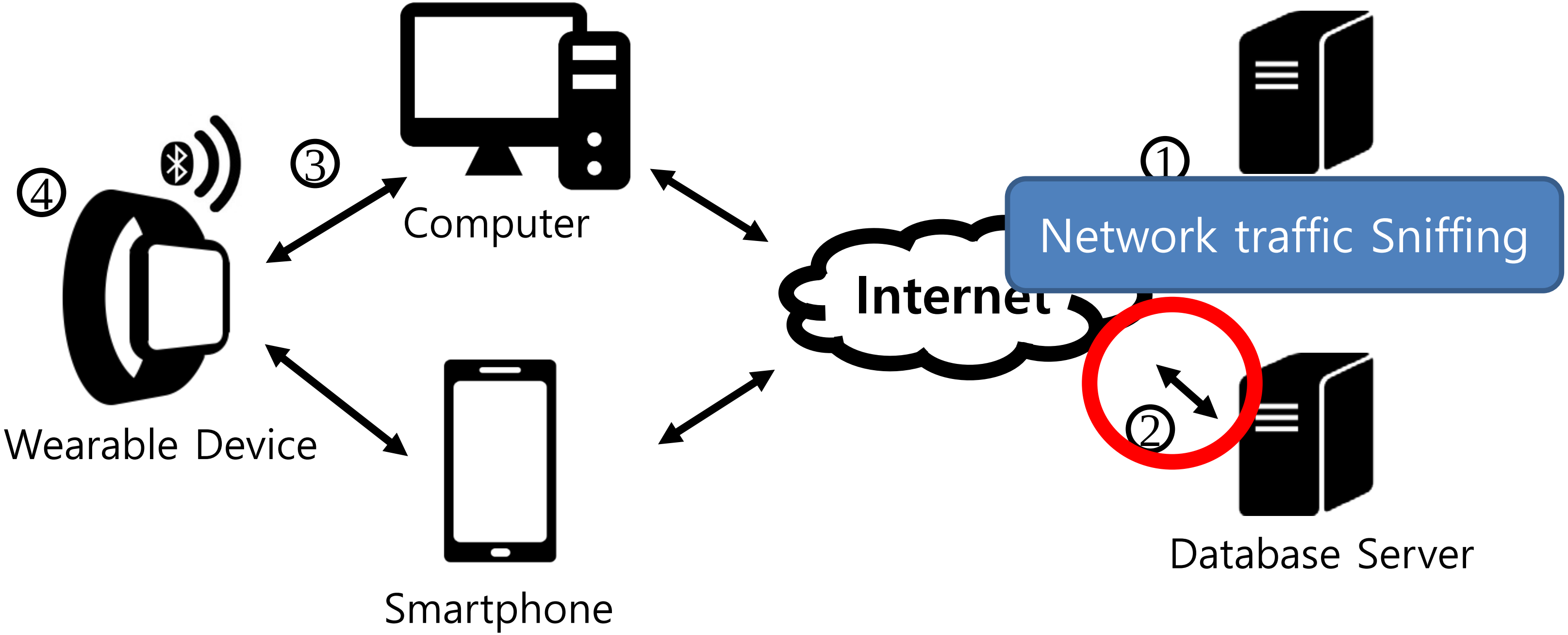
Communication Overview



Previous Studies

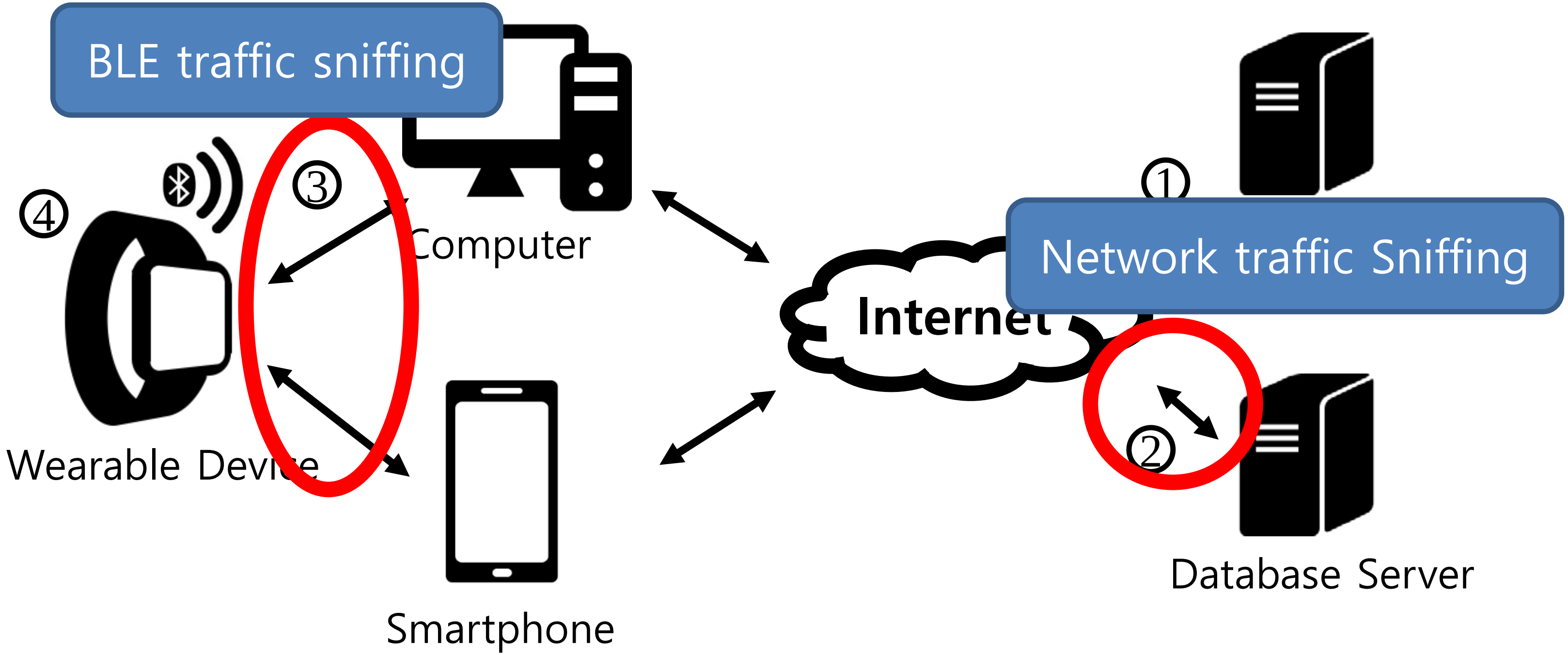


Previous Studies

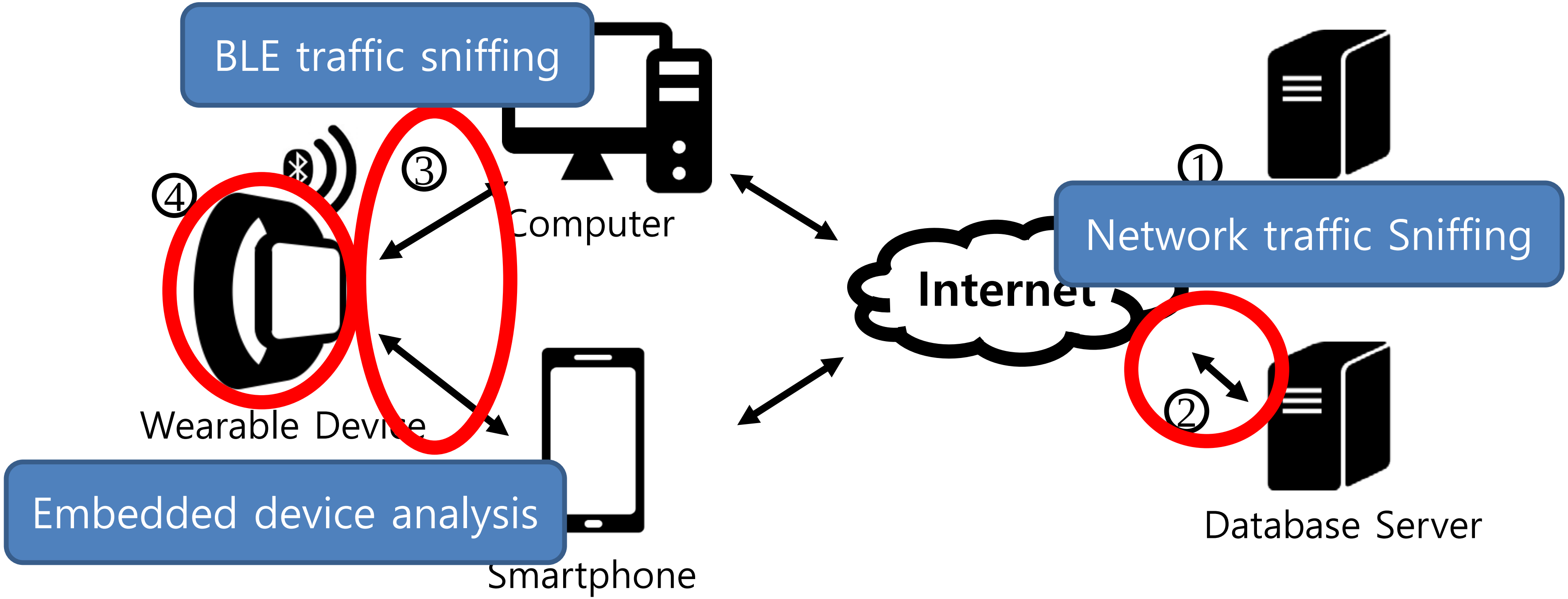


Network traffic Sniffing

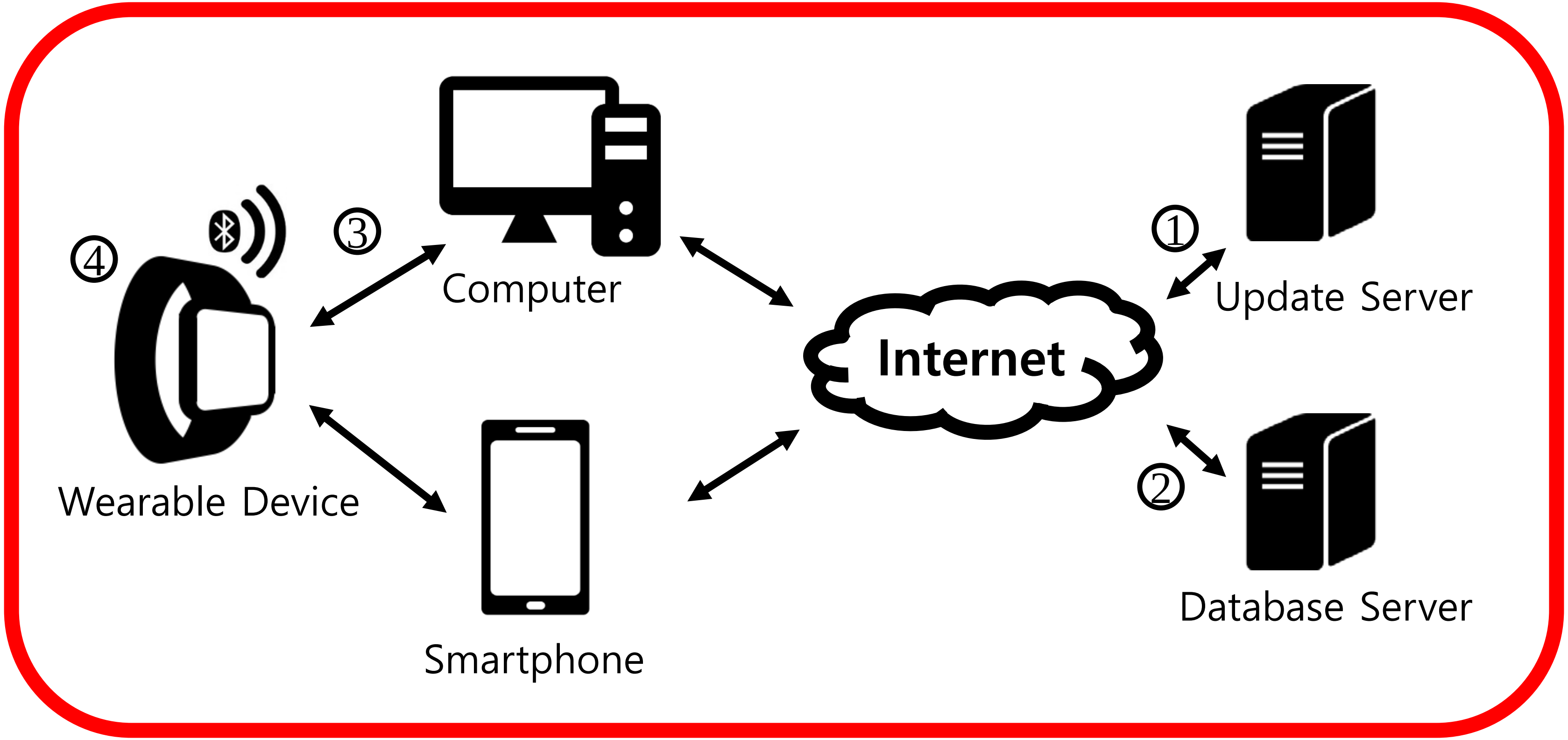
Previous Studies



Previous Studies



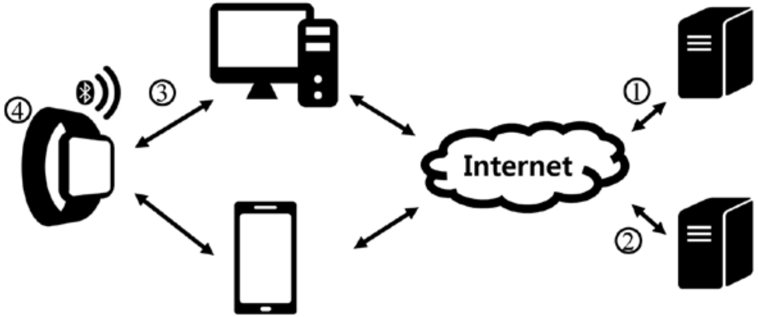
Previous Studies



Threats & Methodology

① Update Channel

– **Malicious software gateway app, device firmware** can be installed.



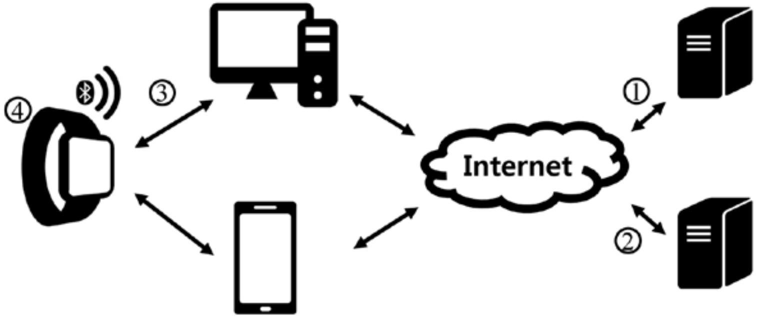
Threats & Methodology

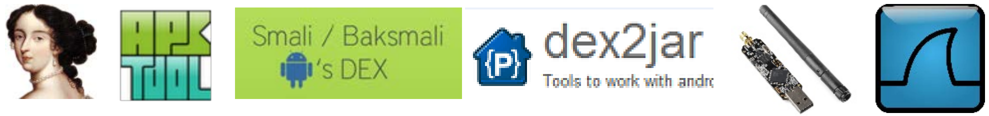
① Update Channel

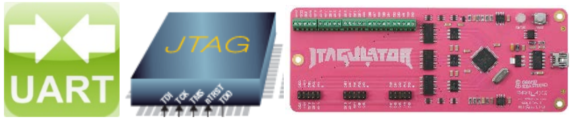
- **Malicious software gateway app, device firmware** can be installed.

② Data Channel

- User's **private information** can be exposed.
- **Malicious messages** can be injected.







Threats & Methodology

① Update Channel

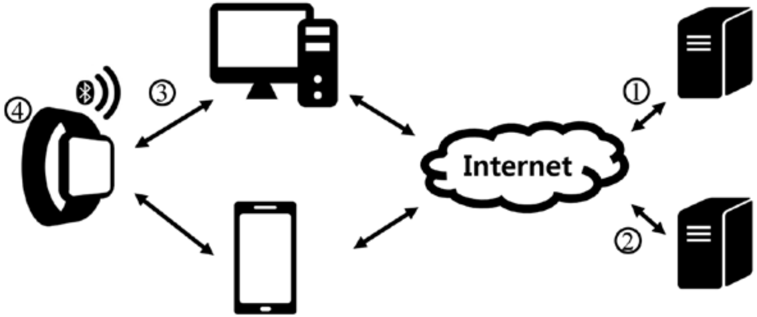
- **Malicious software gateway app, device firmware** can be installed.

② Data Channel

- User's **private information** can be exposed.
- **Malicious messages** can be injected.

③ BLE Channel

- **Health information** can be leaked.
- **Malicious input** can disable the device.



Threats & Methodology

① Update Channel

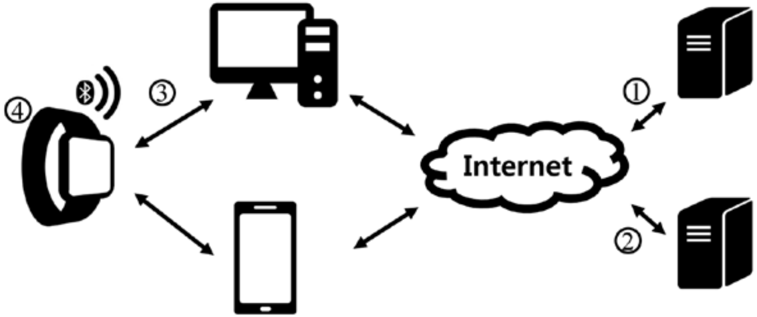
- **Malicious software gateway app, device firmware** can be installed.

② Data Channel

- User's **private information** can be exposed.
- **Malicious messages** can be injected.

③ BLE Channel

- **Health information** can be leaked.
- **Malicious input** can disable the device.



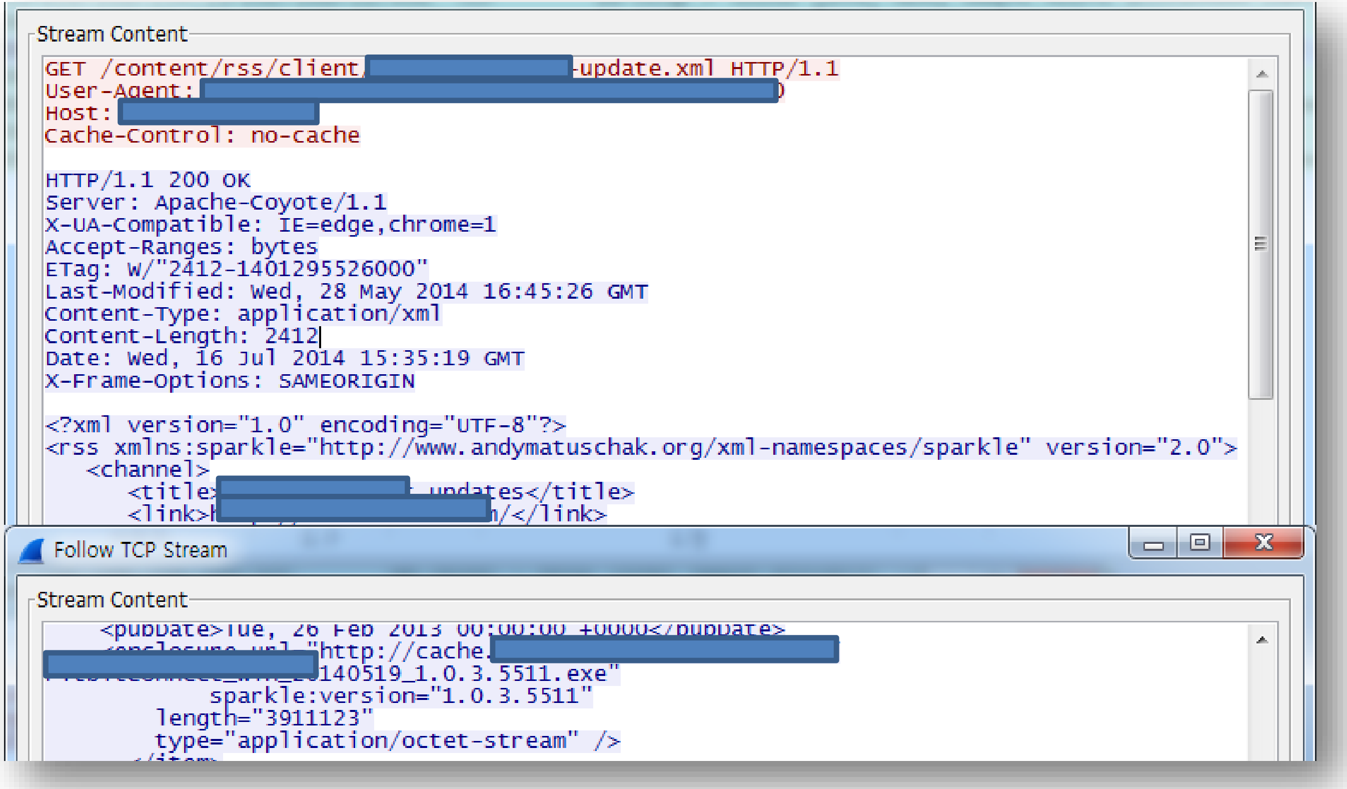
④ Device Analysis

- An adversary can take over the **control of the device**.

Analysis Result

Channel	Attacks	A-fit	B-fit	C-fit
Update Channel	No obfuscation on app	●	▲	●
	DNS spoofing	●	●	●
	App substitution	●	X	●
	Firmware substitution	X	X	●
Data Channel	Plaintext data transfer	●	X	X
BLE Channel	Sniffing	●	●	-
	Plaintext data transfer	●	●	-
Device Analysis	No obfuscation on firmware	X	X	●
	Hidden function	X	X	●
	Hidden protocol	X	X	●
	Hardare debug point	X	X	X

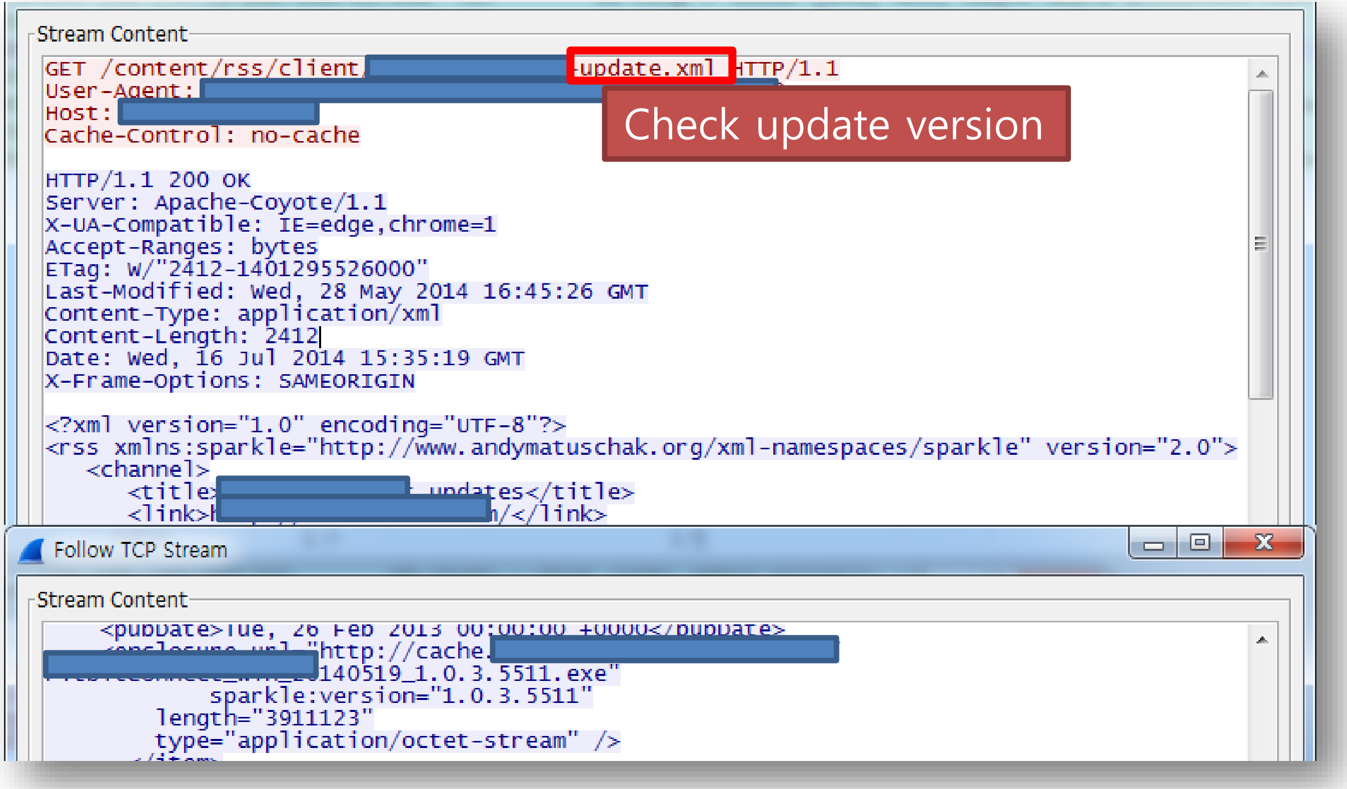
Update Channel – A-Fit



```
GET /content/rss/client[redacted]-update.xml HTTP/1.1
User-Agent: [redacted]
Host: [redacted]
Cache-Control: no-cache

HTTP/1.1 200 OK
Server: Apache-Coyote/1.1
X-UA-Compatible: IE=edge,chrome=1
Accept-Ranges: bytes
ETag: W/"2412-1401295526000"
Last-Modified: Wed, 28 May 2014 16:45:26 GMT
Content-Type: application/xml
Content-Length: 2412
Date: Wed, 16 Jul 2014 15:35:19 GMT
X-Frame-Options: SAMEORIGIN

<?xml version="1.0" encoding="UTF-8"?>
<rss xmlns:sparkle="http://www.andymatuschak.org/xml-namespaces/sparkle" version="2.0">
   <channel>
      <title[redacted]updates</title>
      <link>[redacted]/</link>
```

```
    <pubDate>Tue, 26 Feb 2013 00:00:00 +0000</pubDate>
[redacted]"http://cache.[redacted]
140519_1.0.3.5511.exe"
            sparkle:version="1.0.3.5511"
        length="3911123"
        type="application/octet-stream" />
```

Update Channel – A-Fit

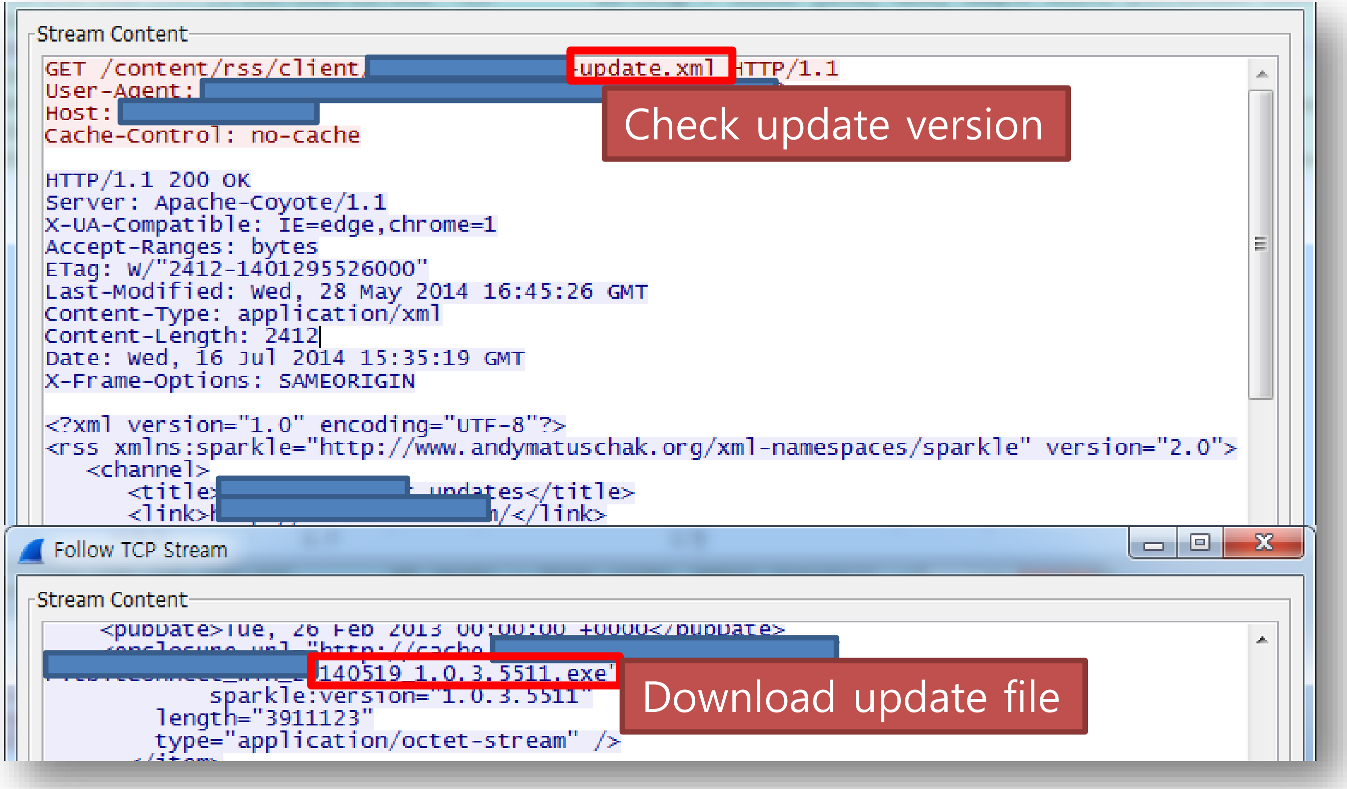


```
GET /content/rss/client/[redacted]-update.xml HTTP/1.1
User-Agent: [redacted]
Host: [redacted]
Cache-Control: no-cache

HTTP/1.1 200 OK
Server: Apache-Coyote/1.1
X-UA-Compatible: IE=edge,chrome=1
Accept-Ranges: bytes
ETag: W/"2412-1401295526000"
Last-Modified: Wed, 28 May 2014 16:45:26 GMT
Content-Type: application/xml
Content-Length: 2412
Date: Wed, 16 Jul 2014 15:35:19 GMT
X-Frame-Options: SAMEORIGIN

<?xml version="1.0" encoding="UTF-8"?>
<rss xmlns:sparkle="http://www.andymatuschak.org/xml-namespaces/sparkle" version="2.0">
    <channel>
        <title>[redacted] updates</title>
        <link>[redacted]/</link>
```

```
    <pubDate>Tue, 26 Feb 2013 00:00:00 +0000</pubDate>
[redacted]"http://cache.[redacted]
[redacted]140519_1.0.3.5511.exe"
            sparkle:version="1.0.3.5511"
        length="3911123"
        type="application/octet-stream" />
```

Check update version

Update Channel – A-Fit



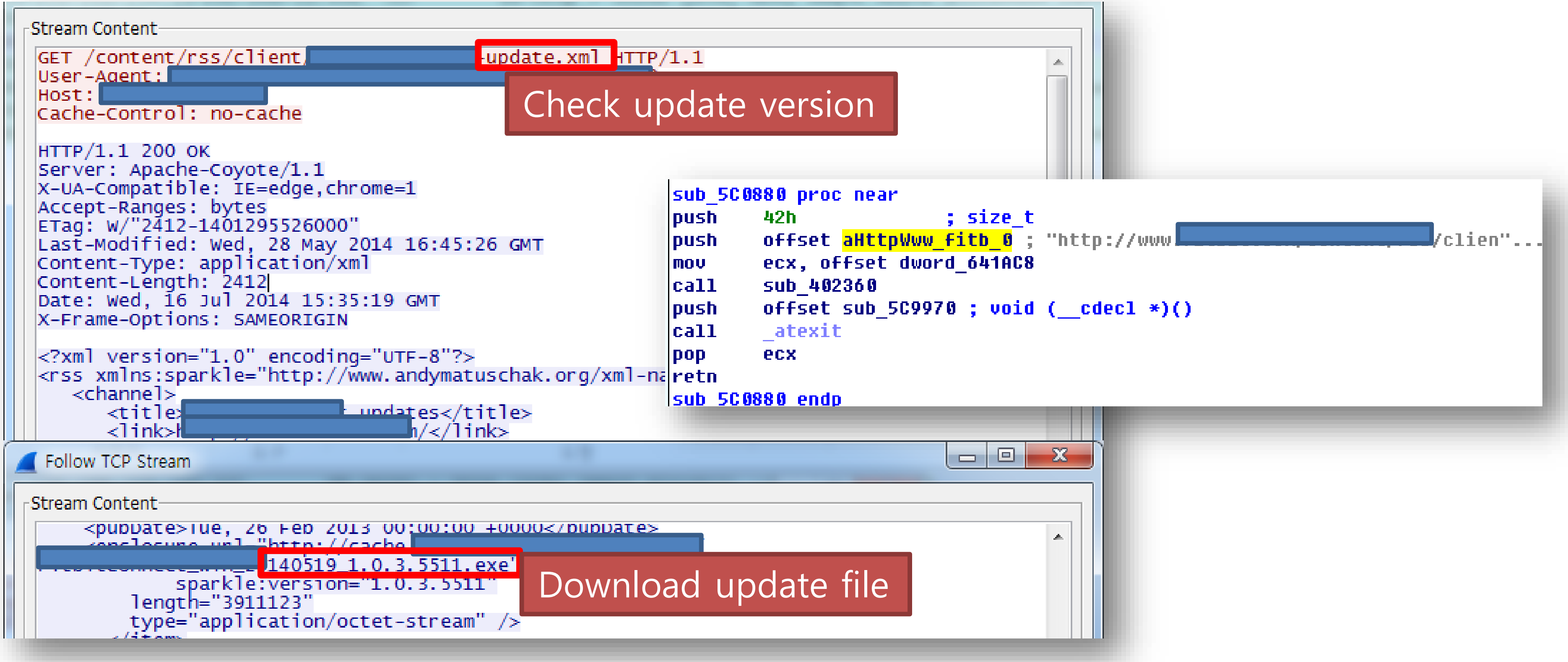
```
GET /content/rss/client[redacted]update.xml HTTP/1.1
User-Agent: [redacted]
Host: [redacted]
Cache-Control: no-cache

HTTP/1.1 200 OK
Server: Apache-Coyote/1.1
X-UA-Compatible: IE=edge,chrome=1
Accept-Ranges: bytes
ETag: W/"2412-1401295526000"
Last-Modified: Wed, 28 May 2014 16:45:26 GMT
Content-Type: application/xml
Content-Length: 2412
Date: Wed, 16 Jul 2014 15:35:19 GMT
X-Frame-Options: SAMEORIGIN

<?xml version="1.0" encoding="UTF-8"?>
<rss xmlns:sparkle="http://www.andymatuschak.org/xml-namespaces/sparkle" version="2.0">
    <channel>
        <title>[redacted] updates</title>
        <link>[redacted]/</link>
```

```
    <pubDate>Tue, 26 Feb 2013 00:00:00 +0000</pubDate>
    <enclosure url="http://cache[redacted]
[redacted]140519_1.0.3.5511.exe"
            sparkle:version="1.0.3.5511"
        length="3911123"
        type="application/octet-stream" />
```

Check update version

Download update file

Update Channel – A-Fit



```
GET /content/rss/client[redacted]update.xml HTTP/1.1
User-Agent: [redacted]
Host: [redacted]
Cache-Control: no-cache

HTTP/1.1 200 OK
Server: Apache-Coyote/1.1
X-UA-Compatible: IE=edge,chrome=1
Accept-Ranges: bytes
ETag: W/"2412-1401295526000"
Last-Modified: Wed, 28 May 2014 16:45:26 GMT
Content-Type: application/xml
Content-Length: 2412
Date: Wed, 16 Jul 2014 15:35:19 GMT
X-Frame-Options: SAMEORIGIN

<?xml version="1.0" encoding="UTF-8"?>
<rss xmlns:sparkle="http://www.andymatuschak.org/xml-na
    <channel>
        <title>[redacted] updates</title>
        <link>[redacted]/</link>
```

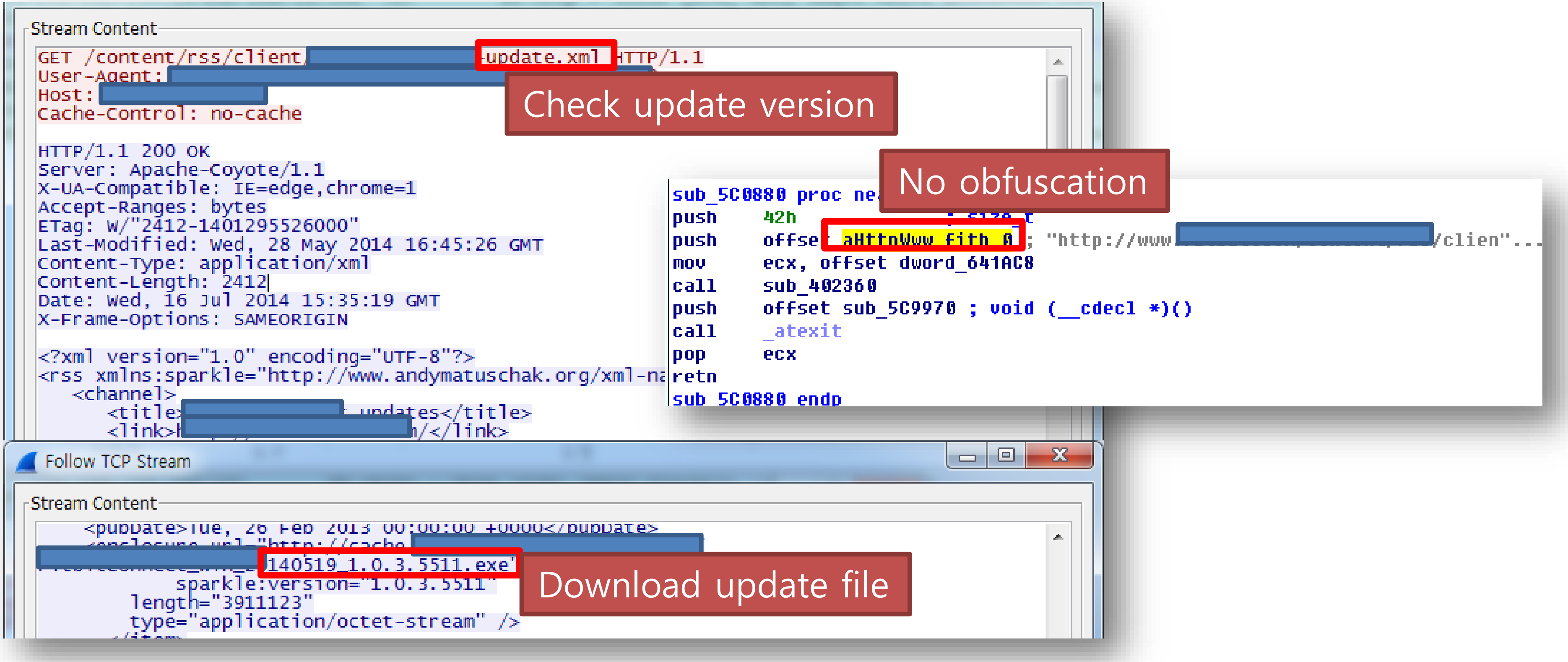
Check update version

```
sub_5C0880 proc near
push     42h              ; size_t
push     offset aHttpWww_fitb_0 ; "http://www[redacted]/clien"...
mov      ecx, offset dword_641AC8
call     sub_402360
push     offset sub_5C9970 ; void (__cdecl *)()
call     _atexit
pop      ecx
retn
sub_5C0880 endp
```

```
    <pubDate>Tue, 26 Feb 2013 00:00:00 +0000</pubDate>
    <enclosure url="http://cache[redacted]
[redacted]140519_1.0.3.5511.exe"
         sparkle:version="1.0.3.5511"
      length="3911123"
      type="application/octet-stream" />
    </item>
```

Download update file

Update Channel – A-Fit



Stream Content

```
GET /content/rss/client[redacted]update.xml HTTP/1.1
User-Agent: [redacted]
Host: [redacted]
Cache-Control: no-cache

HTTP/1.1 200 OK
Server: Apache-Coyote/1.1
X-UA-Compatible: IE=edge,chrome=1
Accept-Ranges: bytes
ETag: W/"2412-1401295526000"
Last-Modified: Wed, 28 May 2014 16:45:26 GMT
Content-Type: application/xml
Content-Length: 2412
Date: Wed, 16 Jul 2014 15:35:19 GMT
X-Frame-Options: SAMEORIGIN

<?xml version="1.0" encoding="UTF-8"?>
<rss xmlns:sparkle="http://www.andymatuschak.org/xml-na
    <channel>
        <title>[redacted] updates</title>
        <link>[redacted]/</link>
```

Check update version

No obfuscation

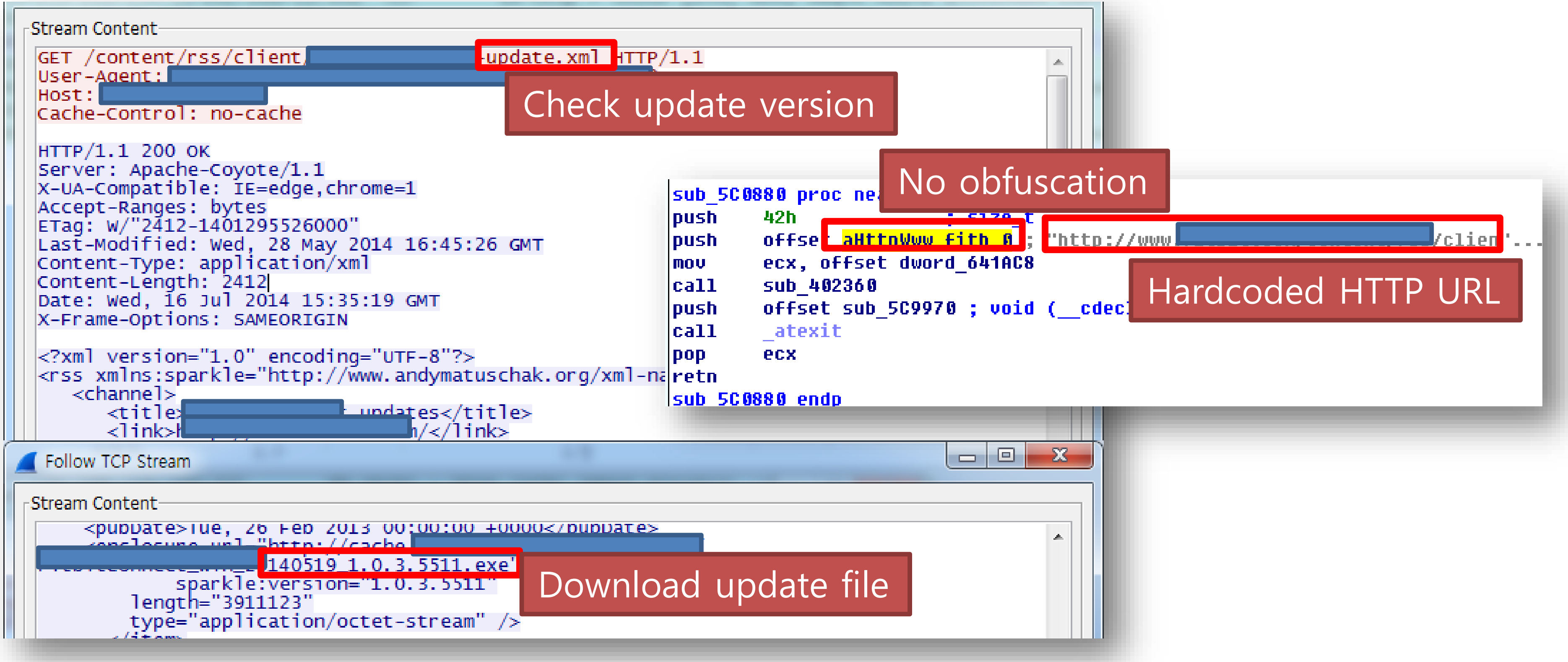
```
sub_5C0880 proc ne
push     42h
push     offset aHttpWww_fith_0 ; "http://www[redacted]/clien"...
mov      ecx, offset dword_641AC8
call     sub_402360
push     offset sub_5C9970 ; void (__cdecl *)()
call     _atexit
pop      ecx
retn
sub_5C0880 endp
```

Stream Content

```
    <pubDate>Tue, 26 Feb 2013 00:00:00 +0000</pubDate>
    <enclosure url="http://cache[redacted]
[redacted]140519_1.0.3.5511.exe"
        sparkle:version="1.0.3.5511"
      length="3911123"
      type="application/octet-stream" />
```

Download update file

Update Channel – A-Fit



Stream Content

```
GET /content/rss/client[redacted]update.xml HTTP/1.1
User-Agent:[redacted]
Host:[redacted]
Cache-Control: no-cache

HTTP/1.1 200 OK
Server: Apache-Coyote/1.1
X-UA-Compatible: IE=edge,chrome=1
Accept-Ranges: bytes
ETag: W/"2412-1401295526000"
Last-Modified: Wed, 28 May 2014 16:45:26 GMT
Content-Type: application/xml
Content-Length: 2412
Date: Wed, 16 Jul 2014 15:35:19 GMT
X-Frame-Options: SAMEORIGIN

<?xml version="1.0" encoding="UTF-8"?>
<rss xmlns:sparkle="http://www.andymatuschak.org/xml-na
    <channel>
        <title>[redacted] updates</title>
        <link>[redacted]/</link>
```

Check update version

```
sub_5C0880 proc ne
push    42h             ; size_t
push    offset aHttpWww_fith_0 ; "http://www[redacted]/clien"...
mov     ecx, offset dword_641AC8
call    sub_402360
push    offset sub_5C9970 ; void (__cdec
call    _atexit
pop     ecx
retn
sub_5C0880 endp
```

No obfuscation

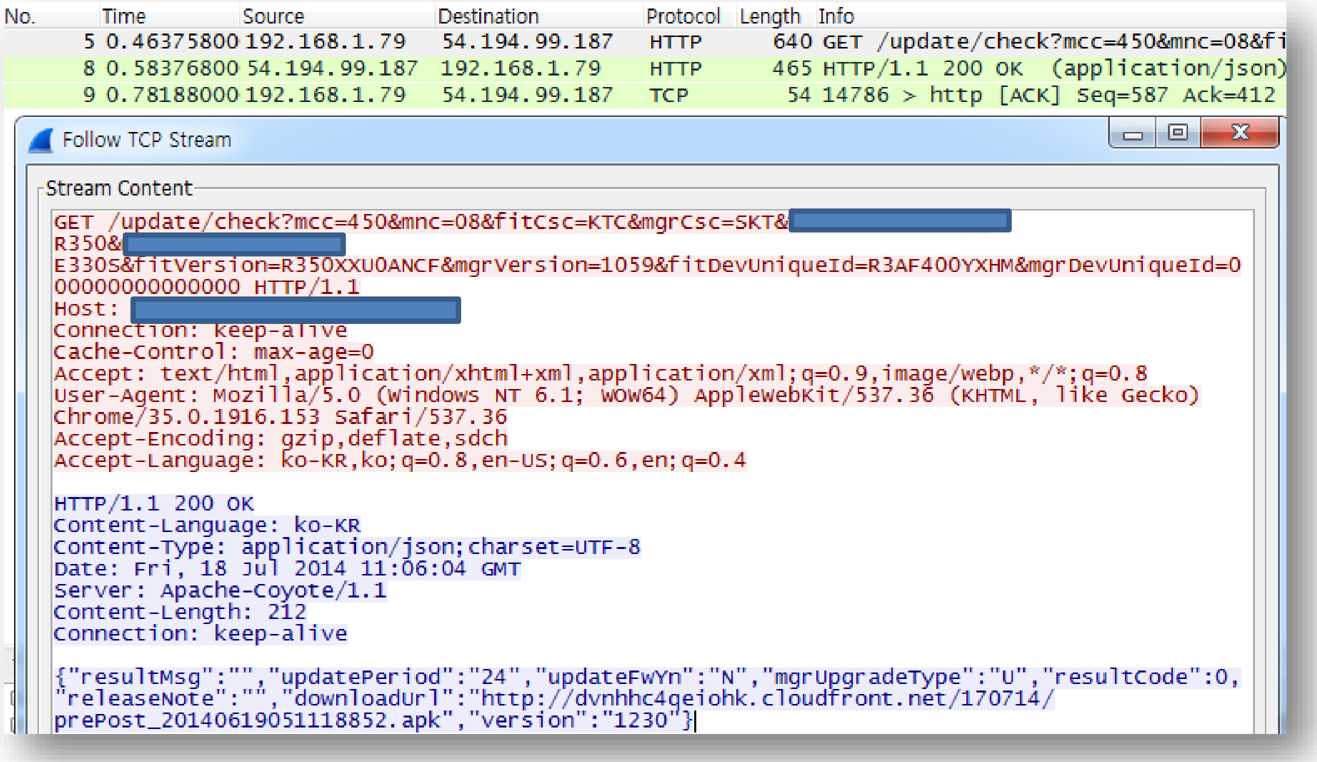
Hardcoded HTTP URL

Stream Content

```
      <pubDate>Tue, 26 Feb 2013 00:00:00 +0000</pubDate>
      <enclosure url="http://cache[redacted]
[redacted]140519_1.0.3.5511.exe"
            sparkle:version="1.0.3.5511"
          length="3911123"
          type="application/octet-stream" />
      </item>
```

Download update file

Update Channel – C-Fit

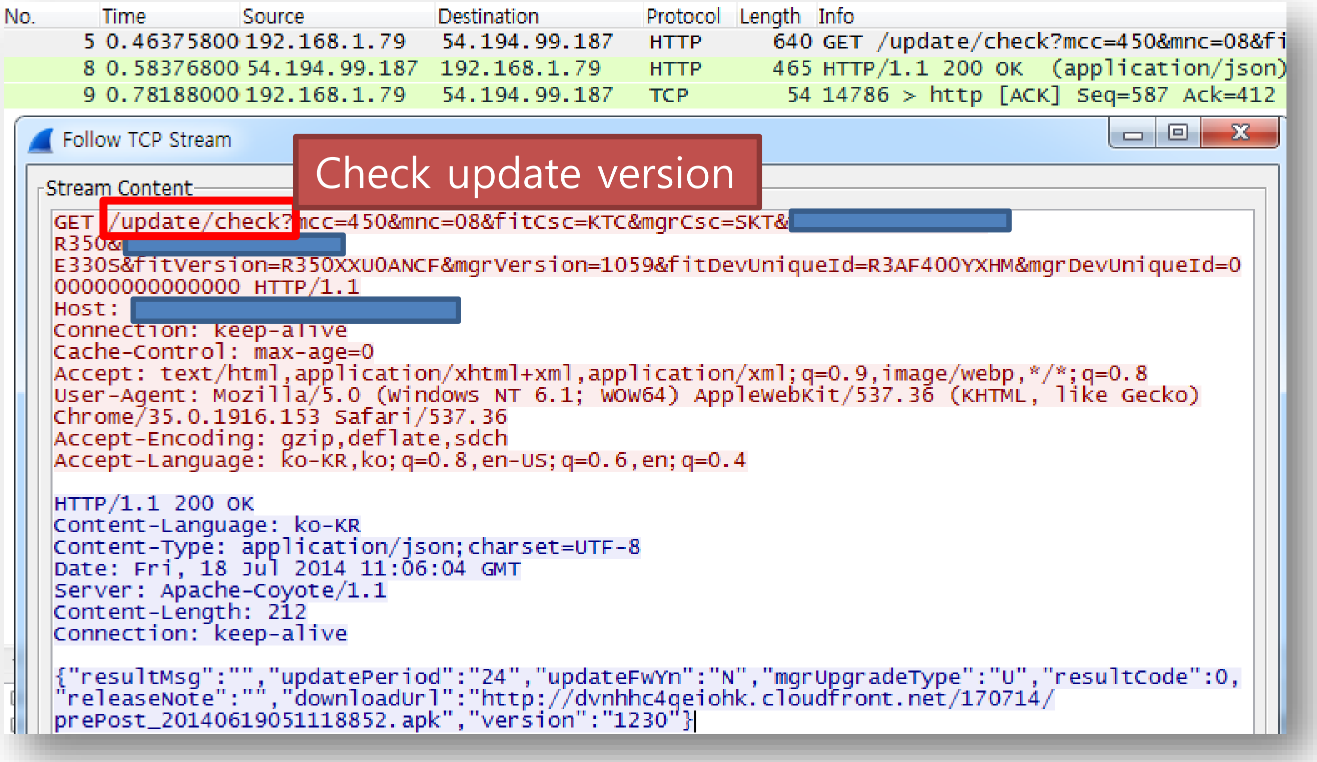


```
No.   Time        Source         Destination    Protocol  Length  Info
    5 0.46375800  192.168.1.79   54.194.99.187  HTTP         640  GET /update/check?mcc=450&mnc=08&fi
    8 0.58376800  54.194.99.187  192.168.1.79   HTTP         465  HTTP/1.1 200 OK  (application/json)
    9 0.78188000  192.168.1.79   54.194.99.187  TCP           54  14786 > http [ACK] Seq=587 Ack=412
```

Stream Content

```
GET /update/check?mcc=450&mnc=08&fitCsc=KTC&mgrCsc=SKT&[redacted]
R350&[redacted]
E330S&fitVersion=R350XXU0ANCF&mgrVersion=1059&fitDevUniqueId=R3AF400YXHM&mgrDevUniqueId=0
00000000000000 HTTP/1.1
Host: [redacted]
Connection: keep-alive
Cache-Control: max-age=0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,*/*;q=0.8
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/35.0.1916.153 Safari/537.36
Accept-Encoding: gzip,deflate,sdch
Accept-Language: ko-KR,ko;q=0.8,en-US;q=0.6,en;q=0.4

HTTP/1.1 200 OK
Content-Language: ko-KR
Content-Type: application/json;charset=UTF-8
Date: Fri, 18 Jul 2014 11:06:04 GMT
Server: Apache-Coyote/1.1
Content-Length: 212
Connection: keep-alive

{"resultMsg":"","updatePeriod":"24","updateFwYn":"N","mgrUpgradeType":"U","resultCode":0,
"releaseNote":"","downloadUrl":"http://dvnhhc4qeiohk.cloudfront.net/170714/
prePost_20140619051118852.apk","version":"1230"}
```

Update Channel – C-Fit

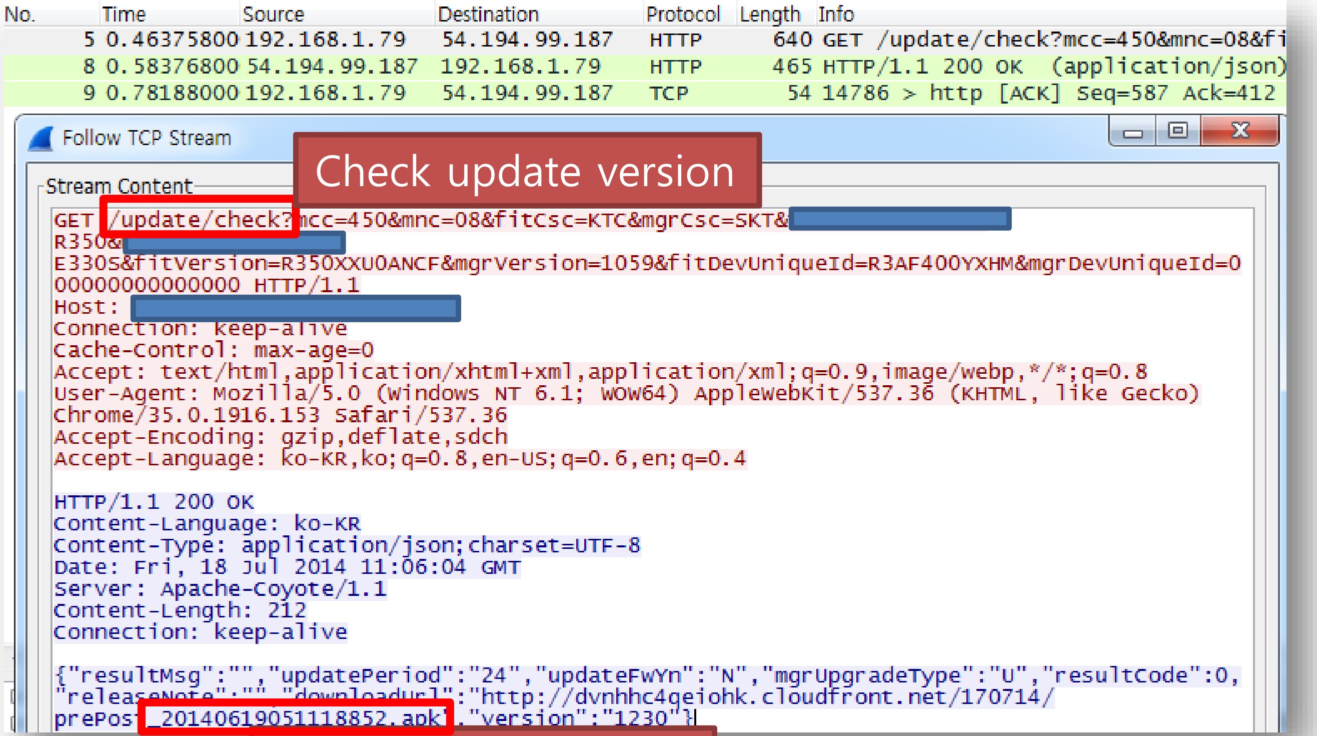


```
No.   Time        Source          Destination     Protocol  Length  Info
    5 0.46375800  192.168.1.79    54.194.99.187   HTTP         640  GET /update/check?mcc=450&mnc=08&fi
    8 0.58376800  54.194.99.187   192.168.1.79    HTTP         465  HTTP/1.1 200 OK  (application/json)
    9 0.78188000  192.168.1.79    54.194.99.187   TCP           54  14786 > http [ACK] Seq=587 Ack=412
```

Check update version

```
GET /update/check?mcc=450&mnc=08&fitCsc=KTC&mgrCsc=SKT&[redacted]
R350&[redacted]
E330S&fitVersion=R350XXU0ANCF&mgrVersion=1059&fitDevUniqueId=R3AF400YXHM&mgrDevUniqueId=0
000000000000000 HTTP/1.1
Host: [redacted]
Connection: keep-alive
Cache-Control: max-age=0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,*/*;q=0.8
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/35.0.1916.153 Safari/537.36
Accept-Encoding: gzip,deflate,sdch
Accept-Language: ko-KR,ko;q=0.8,en-US;q=0.6,en;q=0.4

HTTP/1.1 200 OK
Content-Language: ko-KR
Content-Type: application/json;charset=UTF-8
Date: Fri, 18 Jul 2014 11:06:04 GMT
Server: Apache-Coyote/1.1
Content-Length: 212
Connection: keep-alive

{"resultMsg":"","updatePeriod":"24","updateFwYn":"N","mgrUpgradeType":"U","resultCode":0,
"releaseNote":"","downloadUrl":"http://dvnhhc4qeiohk.cloudfront.net/170714/
prePost_20140619051118852.apk","version":"1230"}
```

Update Channel – C-Fit



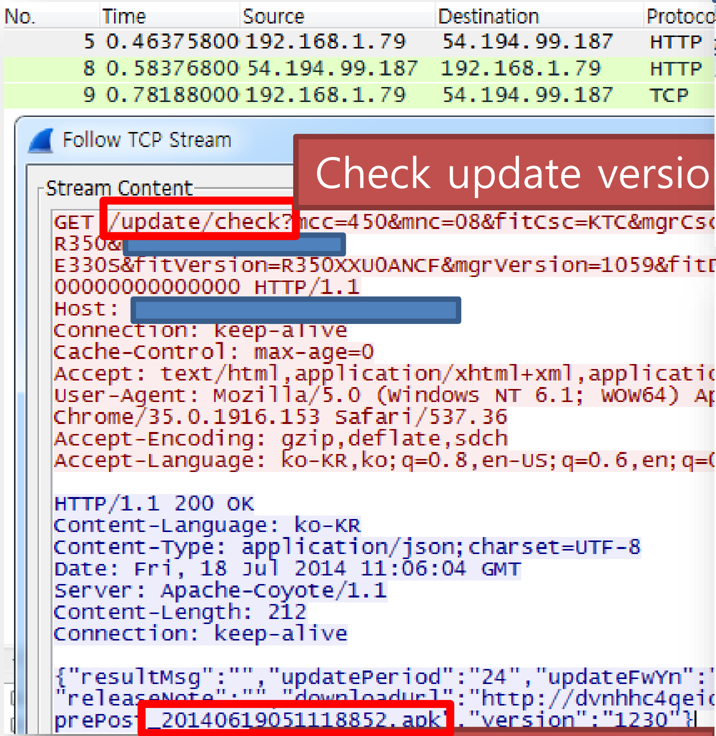
```
No.     Time        Source          Destination     Protocol  Length  Info
      5 0.46375800  192.168.1.79    54.194.99.187   HTTP         640  GET /update/check?mcc=450&mnc=08&fi
      8 0.58376800  54.194.99.187   192.168.1.79    HTTP         465  HTTP/1.1 200 OK  (application/json)
      9 0.78188000  192.168.1.79    54.194.99.187   TCP           54  14786 > http [ACK] Seq=587 Ack=412
```

```
GET /update/check?mcc=450&mnc=08&fitCsc=KTC&mgrCsc=SKT&[redacted]
R350&[redacted]
E330S&fitVersion=R350XXU0ANCF&mgrVersion=1059&fitDevUniqueId=R3AF400YXHM&mgrDevUniqueId=0
00000000000000 HTTP/1.1
Host: [redacted]
Connection: keep-alive
Cache-Control: max-age=0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,*/*;q=0.8
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/35.0.1916.153 Safari/537.36
Accept-Encoding: gzip,deflate,sdch
Accept-Language: ko-KR,ko;q=0.8,en-US;q=0.6,en;q=0.4

HTTP/1.1 200 OK
Content-Language: ko-KR
Content-Type: application/json;charset=UTF-8
Date: Fri, 18 Jul 2014 11:06:04 GMT
Server: Apache-Coyote/1.1
Content-Length: 212
Connection: keep-alive

{"resultMsg":"","updatePeriod":"24","updateFwYn":"N","mgrUpgradeType":"U","resultCode":0,
"releaseNote":"","downloadUrl":"http://dvnhhc4qeiohk.cloudfront.net/170714/
prePost_20140619051118852.apk","version":"1230"}
```

Check update version

Download update file

Update Channel – C-Fit



```
No.   Time        Source          Destination     Protocol
    5 0.46375800  192.168.1.79    54.194.99.187   HTTP
    8 0.58376800  54.194.99.187   192.168.1.79    HTTP
    9 0.78188000  192.168.1.79    54.194.99.187   TCP
```

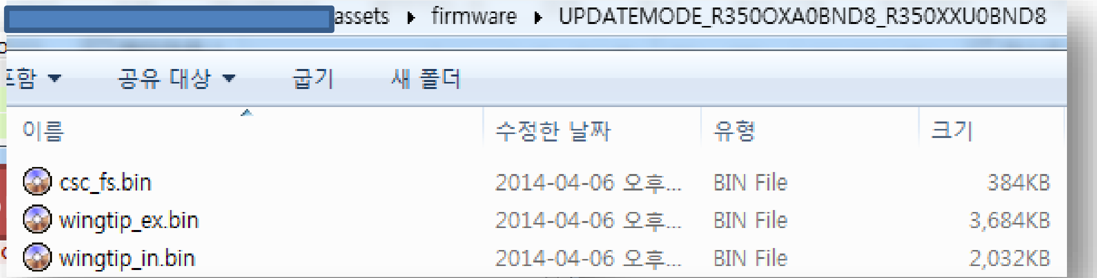
Follow TCP Stream

Stream Content

```
GET /update/check?mcc=450&mnc=08&fitCsc=KTC&mgrCsc
R350&[redacted]
E330S&fitVersion=R350XXU0ANCF&mgrVersion=1059&fitDevUniqueId=R3AF400XXHM&mgrDevUniqueId=0
000000000000000 HTTP/1.1
Host: [redacted]
Connection: keep-alive
Cache-Control: max-age=0
Accept: text/html,application/xhtml+xml,applicatio
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64) Ap
Chrome/35.0.1916.153 Safari/537.36
Accept-Encoding: gzip,deflate,sdch
Accept-Language: ko-KR,ko;q=0.8,en-US;q=0.6,en;q=(

HTTP/1.1 200 OK
Content-Language: ko-KR
Content-Type: application/json;charset=UTF-8
Date: Fri, 18 Jul 2014 11:06:04 GMT
Server: Apache-Coyote/1.1
Content-Length: 212
Connection: keep-alive

{"resultMsg":"","updatePeriod":"24","updateFwYn":'
"releaseNote":"","downloadUrl":"http://dvnhhc4qeic
prePos_20140619051118852.apk","version":"1230"}
```

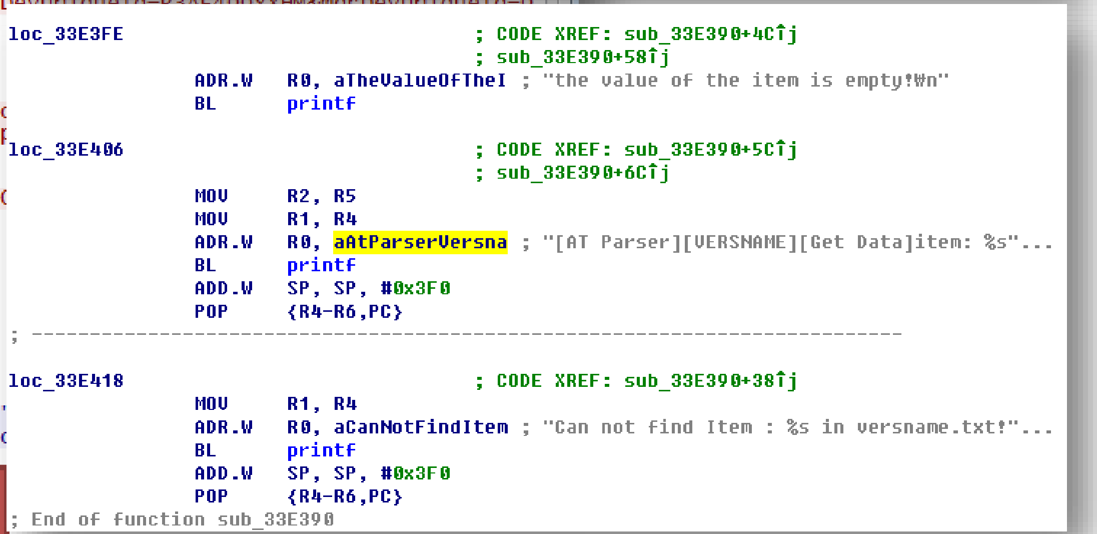
Check update versio

Download update file



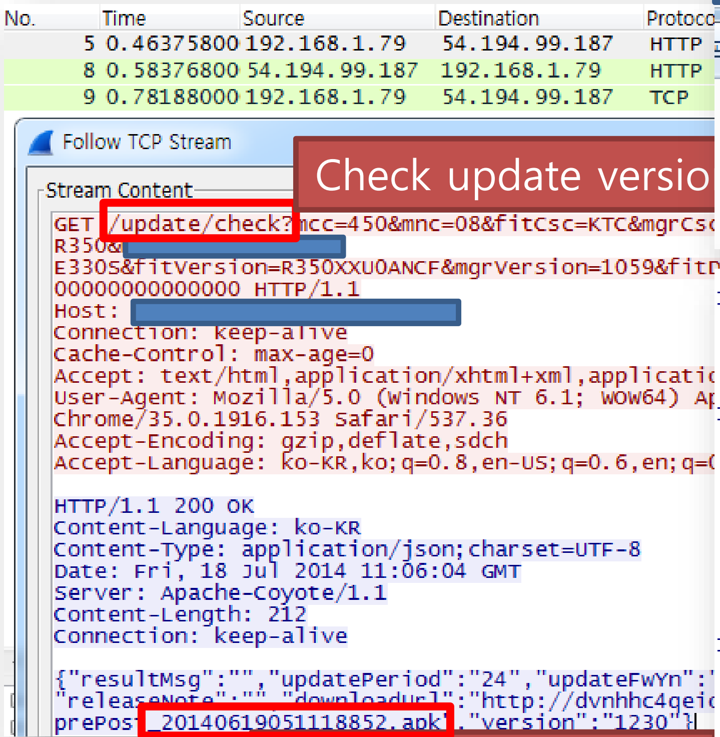
[redacted] assets ▸ firmware ▸ UPDATEMODE_R350OXA0BND8_R350XXU0BND8

이름	수정한 날짜	유형	크기
csc_fs.bin	2014-04-06 오후...	BIN File	384KB
wingtip_ex.bin	2014-04-06 오후...	BIN File	3,684KB
wingtip_in.bin	2014-04-06 오후...	BIN File	2,032KB



```
loc_33E3FE                              ; CODE XREF: sub_33E390+4C↑j
                                        ; sub_33E390+58↑j
                ADR.W   R0, aTheValueOfTheI ; "the value of the item is empty!₩n"
                BL      printf

loc_33E406                              ; CODE XREF: sub_33E390+5C↑j
                                        ; sub_33E390+6C↑j
                MOV     R2, R5
                MOV     R1, R4
                ADR.W   R0, aAtParserVersna ; "[AT Parser][VERSNAME][Get Data]item: %s"...
                BL      printf
                ADD.W   SP, SP, #0x3F0
                POP     {R4-R6,PC}
; ---------------------------------------------------------------------------

loc_33E418                              ; CODE XREF: sub_33E390+38↑j
                MOV     R1, R4
                ADR.W   R0, aCanNotFindItem ; "Can not find Item : %s in versname.txt!"...
                BL      printf
                ADD.W   SP, SP, #0x3F0
                POP     {R4-R6,PC}
; End of function sub_33E390
```

Update Channel – C-Fit

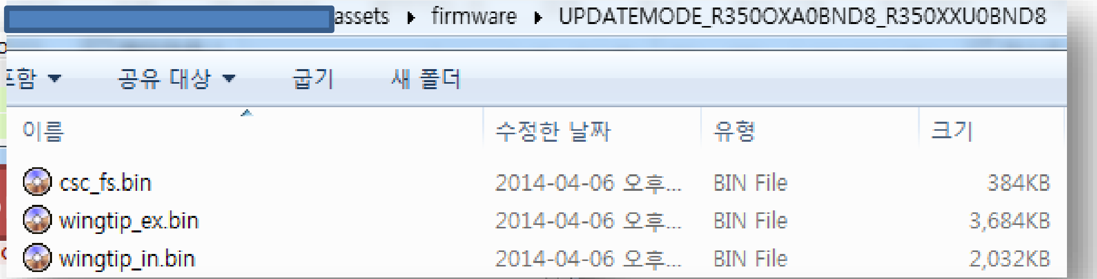


No.	Time	Source	Destination	Protoco
5	0.46375800	192.168.1.79	54.194.99.187	HTTP
8	0.58376800	54.194.99.187	192.168.1.79	HTTP
9	0.78188000	192.168.1.79	54.194.99.187	TCP

```
GET /update/check?mcc=450&mnc=08&fitCsc=KTC&mgrCsc
R350&[redacted]
E330S&fitVersion=R350XXUOANCF&mgrVersion=1059&fitDevUniqueId=R3AF400XXHM&mgrDevUniqueId=0
000000000000000 HTTP/1.1
Host: [redacted]
Connection: keep-alive
Cache-Control: max-age=0
Accept: text/html,application/xhtml+xml,applicatio
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64) Ap
Chrome/35.0.1916.153 Safari/537.36
Accept-Encoding: gzip,deflate,sdch
Accept-Language: ko-KR,ko;q=0.8,en-US;q=0.6,en;q=0

HTTP/1.1 200 OK
Content-Language: ko-KR
Content-Type: application/json;charset=UTF-8
Date: Fri, 18 Jul 2014 11:06:04 GMT
Server: Apache-Coyote/1.1
Content-Length: 212
Connection: keep-alive

{"resultMsg":"","updatePeriod":"24","updateFwYn":
"releaseNote":"","downloadUrl":"http://dvnhhc4qeic
prePost_20140619051118852.apk","version":"1230"}
```

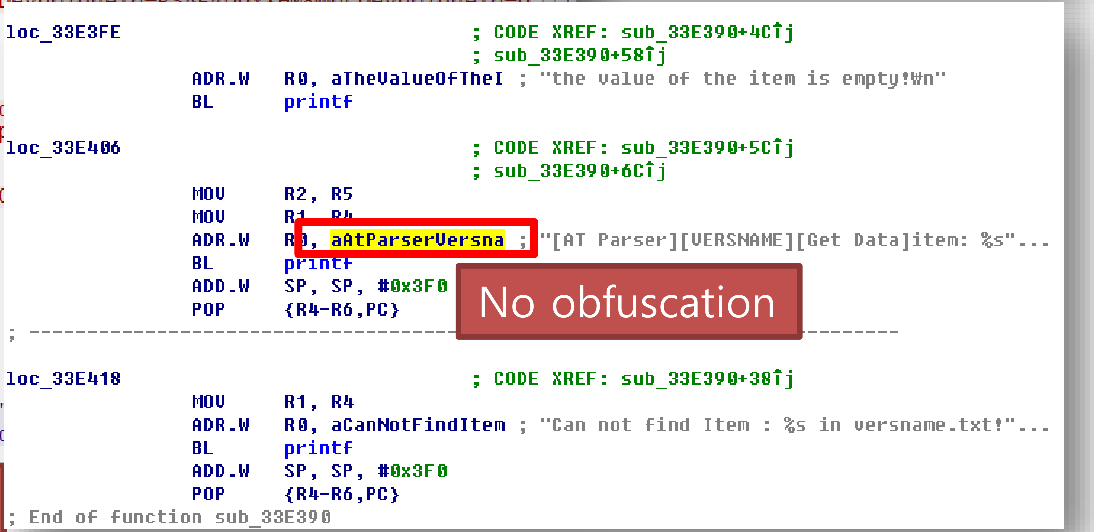
Check update versio

Download update file



[redacted] assets ▸ firmware ▸ UPDATEMODE_R350OXA0BND8_R350XXU0BND8

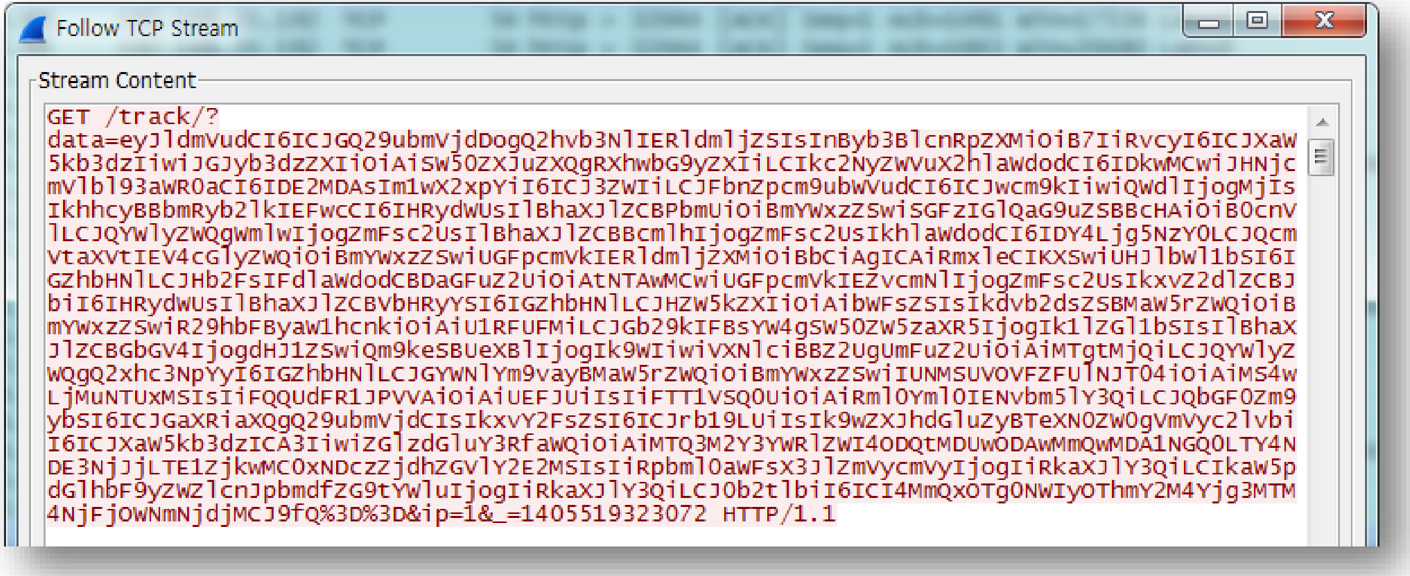
이름	수정한 날짜	유형	크기
csc_fs.bin	2014-04-06 오후...	BIN File	384KB
wingtip_ex.bin	2014-04-06 오후...	BIN File	3,684KB
wingtip_in.bin	2014-04-06 오후...	BIN File	2,032KB



```
loc_33E3FE                              ; CODE XREF: sub_33E390+4C↑j
                                        ; sub_33E390+58↑j
                ADR.W   R0, aTheValueOfTheI ; "the value of the item is empty!₩n"
                BL      printf

loc_33E406                              ; CODE XREF: sub_33E390+5C↑j
                                        ; sub_33E390+6C↑j
                MOV     R2, R5
                MOV     R1, R4
                ADR.W   R0, aAtParserVersna ; "[AT Parser][VERSNAME][Get Data]item: %s"...
                BL      printf
                ADD.W   SP, SP, #0x3F0
                POP     {R4-R6,PC}
; ---------------------------------------------------------------------------

loc_33E418                              ; CODE XREF: sub_33E390+38↑j
                MOV     R1, R4
                ADR.W   R0, aCanNotFindItem ; "Can not find Item : %s in versname.txt!"...
                BL      printf
                ADD.W   SP, SP, #0x3F0
                POP     {R4-R6,PC}
; End of function sub_33E390
```

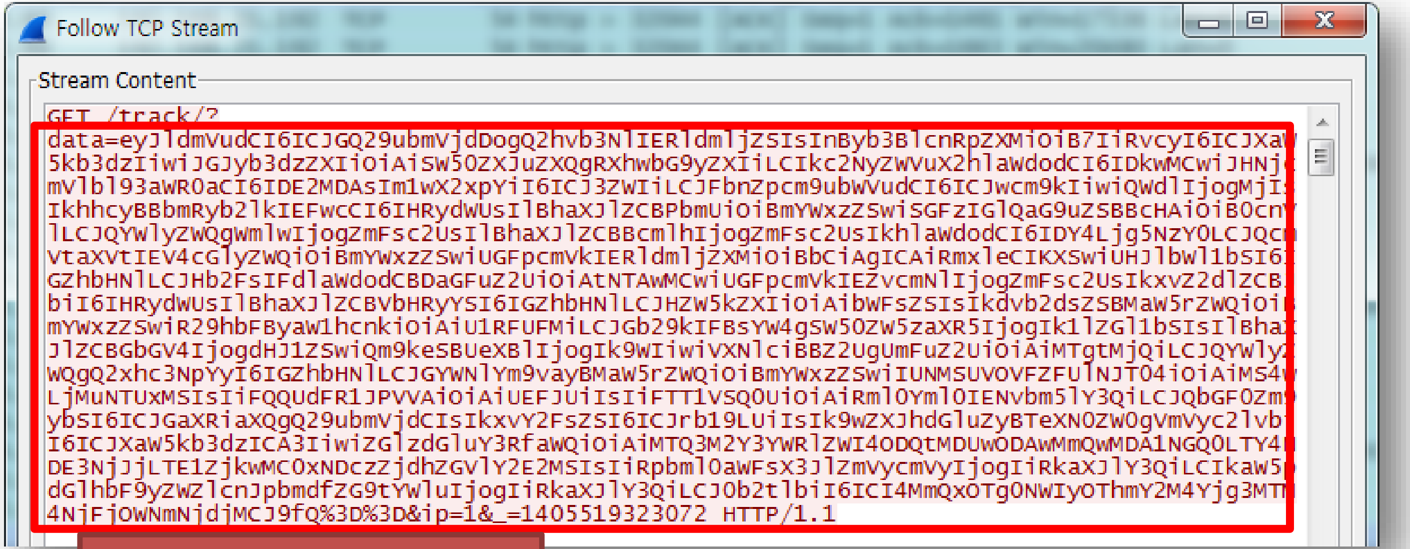
No obfuscation

Data Channel Analysis



```
GET /track/?
data=eyJldmVudCI6ICJGQ29ubmVjdDogQ2hvb3NlIERldmljZSIsInByb3BlcnRpZXMiOiB7IiRvcyI6ICJXaW
5kb3dzIiwiJGJyb3dzZXIiOiAiSW50ZXJuZXQgRXhwbG9yZXIiLCIkc2NyZWVuX2hlaWdodCI6IDkwMCwiJHNjc
mVlbl93aWR0aCI6IDE2MDAsIm1wX2xpYiI6ICJ3ZWIiLCJFbnZpcm9ubWVudCI6ICJwcm9kIiwiQWdlIjogMjIs
IkhhcyBBbmRyb2lkIEFwcCI6IHRydWUsIlBhaXJlZCBPbmUiOiBmYWxzZSwiSGFzIGlQaG9uZSBBcHAiOiB0cnV
lLCJQYWlyZWQgWmlwIjogZmFsc2UsIlBhaXJlZCBBcmlhIjogZmFsc2UsIkhlaWdodCI6IDY4Ljg5NzY0LCJQcm
VtaXVtIEV4cGlyZWQiOiBmYWxzZSwiUGFpcmVkIERldmljZXMiOiBbCiAgICAiRmxleCIKXSwiUHJlbWl1bSI6I
GZhbHNlLCJHb2FsIFdlaWdodCBDaGFuZ2UiOiAtNTAwMCwiUGFpcmVkIEZvcmNlIjogZmFsc2UsIkxvZ2dlZCBJ
biI6IHRydWUsIlBhaXJlZCBVbHRyYSI6IGZhbHNlLCJHZW5kZXIiOiAibWFsZSIsIkdvb2dsZSBMaW5rZWQiOiB
mYWxzZSwiR29hbFByaW1hcnkiOiAiU1RFUFMiLCJGb29kIFBsYW4gSW50ZW5zaXR5IjogIk1lZGl1bSIsIlBhaX
JlZCBGbGV4IjogdHJ1ZSwiQm9keSBUeXBlIjogIk9WIiwiVXNlciBBZ2UgUmFuZ2UiOiAiMTgtMjQiLCJQYWlyZ
WQgQ2xhc3NpYyI6IGZhbHNlLCJGYWNlYm9vayBMaW5rZWQiOiBmYWxzZSwiIUNMSUVOVFZFUlNJT04iOiAiMS4w
LjMuNTUxMSIsIiFQQUdFR1JPVVAiOiAiUEFJUiIsIiFTT1VSQ0UiOiAiRml0Yml0IENvbm5lY3QiLCJQbGF0Zm9
ybSI6ICJGaXRiaXQgQ29ubmVjdCIsIkxvY2FsZSI6ICJrb19LUiIsIk9wZXJhdGluZyBTeXN0ZW0gVmVyc2lvbi
I6ICJXaW5kb3dzICA3IiwiZGlzdGluY3RfaWQiOiAiMTQ3M2Y3YWRlZWI4ODQtMDUwODAwMmQwMDA1NGQ0LTY4N
DE3NjJjLTE1ZjkwMC0xNDczZjdhZGVlY2E2MSIsIiRpbml0aWFsX3JlZmVycmVyIjogIiRkaXJlY3QiLCIkaW5p
dGlhbF9yZWZlcnJpbmdfZG9tYWluIjogIiRkaXJlY3QiLCJ0b2tlbiI6ICI4MmQxOTg0NWIyOThmY2M4Yjg3MTM
4NjFjOWNmNjdjMCJ9fQ%3D%3D&ip=1&_=1405519323072 HTTP/1.1
```

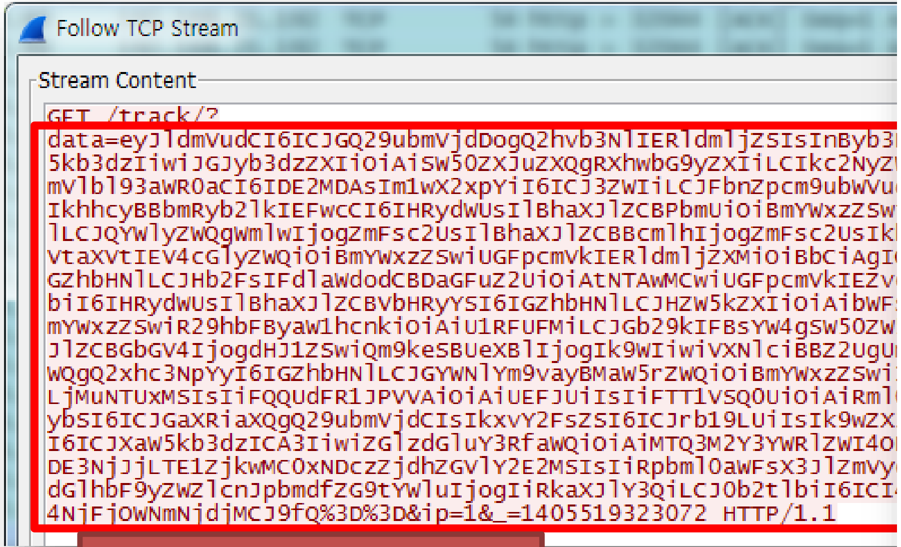
Data Channel Analysis



```
GET /track/?
data=eyJldmVudCI6ICJGQ29ubmVjdDogQ2hvb3NlIERldmljZSIsInByb3BlcnRpZXMiOiB7IiRvcyI6ICJXa
5kb3dzIiwiJGJyb3dzZXIiOiAiSW50ZXJuZXQgRXhwbG9yZXIiLCIkc2NyZWVuX2hlaWdodCI6IDkwMCwiJHNj
mVlbl93aWR0aCI6IDE2MDAsIm1wX2xpYiI6ICJ3ZWIiLCJFbnZpcm9ubWVudCI6ICJwcm9kIiwiQWdlIjogMjI
IkhhcyBBbmRyb2lkIEFwcCI6IHRydWUsIlBhaXJlZCBPbmUiOiBmYWxzZSwiSGFzIGlQaG9uZSBBcHAiOiB0cn
lLCJQYWlyZWQgWmlwIjogZmFsc2UsIlBhaXJlZCBBcmlhIjogZmFsc2UsIkhlaWdodCI6IDY4Ljg5NzY0LCJQc
VtaXVtIEV4cGlyZWQiOiBmYWxzZSwiUGFpcmVkIERldmljZXMiOiBbCiAgICAiRmxleCIKXSwiUHJlbWl1bSI6
GZhbHNlLCJHb2FsIFdlaWdodCBDaGFuZ2UiOiAtNTAwMCwiUGFpcmVkIEZvcmNlIjogZmFsc2UsIkxvZ2dlZCB
biI6IHRydWUsIlBhaXJlZCBVbHRyYSI6IGZhbHNlLCJHZW5kZXIiOiAibWFsZSIsIkdvb2dsZSBMaW5rZWQiOi
mYWxzZSwiR29hbFByaW1hcnkiOiAiU1RFUFMiLCJGb29kIFBsYW4gSW50ZW5zaXR5IjogIk1lZGl1bSIsIlBha
JlZCBGbGV4IjogdHJ1ZSwiQm9keSBUeXBlIjogIk9WIiwiVXNlciBBZ2UgUmFuZ2UiOiAiMTgtMjQiLCJQYWly
WQgQ2xhc3NpYyI6IGZhbHNlLCJGYWNlYm9vayBMaW5rZWQiOiBmYWxzZSwiIUNMSUVOVFZFUlNJT04iOiAiMS4
LjMuNTUxMSIsIiFQQUdFR1JPVVAiOiAiUEFJUiIsIiFTT1VSQ0UiOiAiRml0Yml0IENvbm5lY3QiLCJQbGF0Zm
ybSI6ICJGaXRiaXQgQ29ubmVjdCIsIkxvY2FsZSI6ICJrb19LUiIsIk9wZXJhdGluZyBTeXN0ZW0gVmVyc2lvb
I6ICJXaW5kb3dzICA3IiwiZGlzdGluY3RfaWQiOiAiMTQ3M2Y3YWRlZWI4ODQtMDUwODAwMmQwMDA1NGQ0LTY4
DE3NjJjLTE1ZjkwMC0xNDczZjdhZGVlY2E2MSIsIiRpbml0aWFsX3JlZmVycmVyIjogIiRkaXJlY3QiLCIkaW5
dGlhbF9yZWZlcnJpbmdfZG9tYWluIjogIiRkaXJlY3QiLCJ0b2tlbiI6ICI4MmQxOTg0NWIyOThmY2M4Yjg3MT
4NjFjOWNmNjdjMCJ9fQ%3D%3D&ip=1&_=1405519323072 HTTP/1.1
```

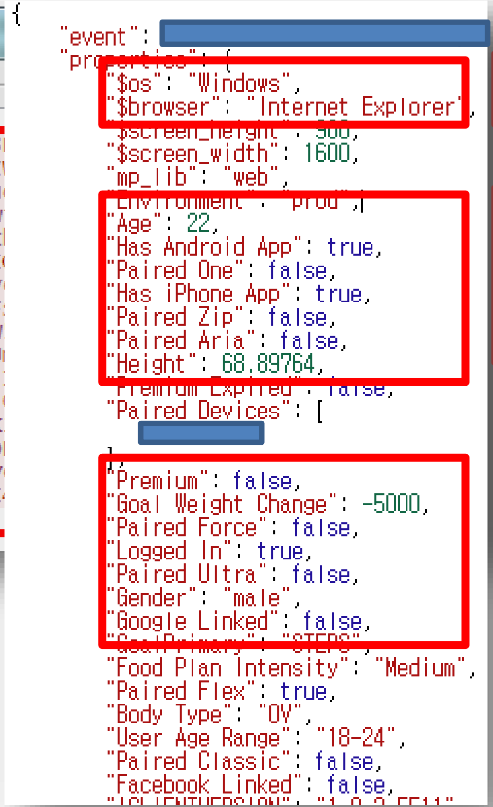
Base64 encoded data

Data Channel Analysis



```
GET /track/?
data=eyJldmVudCI6ICJGQ29ubmVjdDogQ2hvb3NlIERldmljZSIsInByb3
5kb3dzIiwiJGJyb3dzZXIiOiAiSW50ZXJuZXQgRXhwbG9yZXIiLCIkc2NyZ
mVlbl93aWR0aCI6IDE2MDAsIm1wX2xpYiI6ICJ3ZWIiLCJFbnZpcm9ubWVu
IkhhcyBBbmRyb2lkIEFwcCI6IHRydWUsIlBhaXJlZCBPbmUiOiBmYWxzZSw
lLCJQYWlyZWQgWmlwIjogZmFsc2UsIlBhaXJlZCBBcmlhIjogZmFsc2UsIk
VtaXVtIEV4cGlyZWQiOiBmYWxzZSwiUGFpcmVkIERldmljZXMiOiBbciAgI
GZhbHNlLCJHb2FsIFdlaWdodCBDaGFuZ2UiOiAtNTAwMCwiUGFpcmVkIEZv
biI6IHRydWUsIlBhaXJlZCBVbHRyYSI6IGZhbHNlLCJHZW5kZXIiOiAibWF
mYWxzZSwiR29hbFByaW1hcnkiOiAiU1RFUFMiLCJGb29kIFBsYW4gSW50ZW
JlZCBGbGV4IjogdHJ1ZSwiQm9keSBUeXBlIjogIk9WIiwiVXNlciBBZ2UgU
WQgQ2xhc3NpYyI6IGZhbHNlLCJGYWNlYm9vayBMaW5rZWQiOiBmYWxzZSwi
LjMuNTUxMSIsIiFQQUdFR1JPVVAiOiAiUEFJUiIsIiFTT1VSQ0UiOiAiRml
ybSI6ICJGaXRiaXQgQ29ubmVjdCIsIkxvY2FsZSI6ICJrb19LUiIsIk9wZX
I6ICJXaW5kb3dzICA3IiwiZGlzdGluY3RfaWQiOiAiMTQ3M2Y3YWRlZWI4O
DE3NjJjLTE1ZjkwMC0xNDczZjdhZGVlY2E2MSIsIiRpbml0aWFsX3JlZmVy
dGlhbF9yZWZlcnJpbmdfZG9tYWluIjogIiRkaXJlY3QiLCJ0b2tlbiI6ICI
4NjFjOWNmNjdjMCJ9fQ%3D%3D&ip=1&_=1405519323072 HTTP/1.1
```

Base64 encoded data



```
{
    "event": [redacted]
    "properties": {
        "$os": "Windows",
        "$browser": "Internet Explorer",
        "$screen_height": 900,
        "$screen_width": 1600,
        "mp_lib": "web",
        "Environment": "prod",
        "Age": 22,
        "Has Android App": true,
        "Paired One": false,
        "Has iPhone App": true,
        "Paired Zip": false,
        "Paired Aria": false,
        "Height": 68.89764,
        "Premium Expired": false,
        "Paired Devices": [
            [redacted]
        ],
        "Premium": false,
        "Goal Weight Change": -5000,
        "Paired Force": false,
        "Logged In": true,
        "Paired Ultra": false,
        "Gender": "male",
        "Google Linked": false,
        "GoalPrimary": "STEPS",
        "Food Plan Intensity": "Medium",
        "Paired Flex": true,
        "Body Type": "OV",
        "User Age Range": "18-24",
        "Paired Classic": false,
        "Facebook Linked": false,
        "JCLIENTVERSION": "1.0.2 FF11"
```

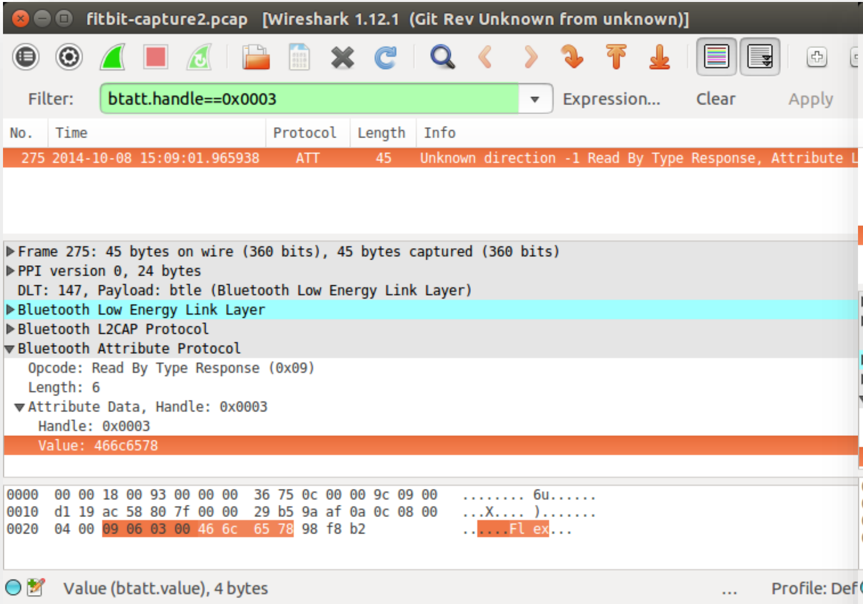
OS, browser

Age
Phone type
Height

Gender
Goal weight

BLE Channel Analysis

- BLE key brute force attack
  - Successfully received BLE packets
  - No encryption -> possible to map meaning of each byte



fitbit-capture2.pcap [Wireshark 1.12.1 (Git Rev Unknown from unknown)]

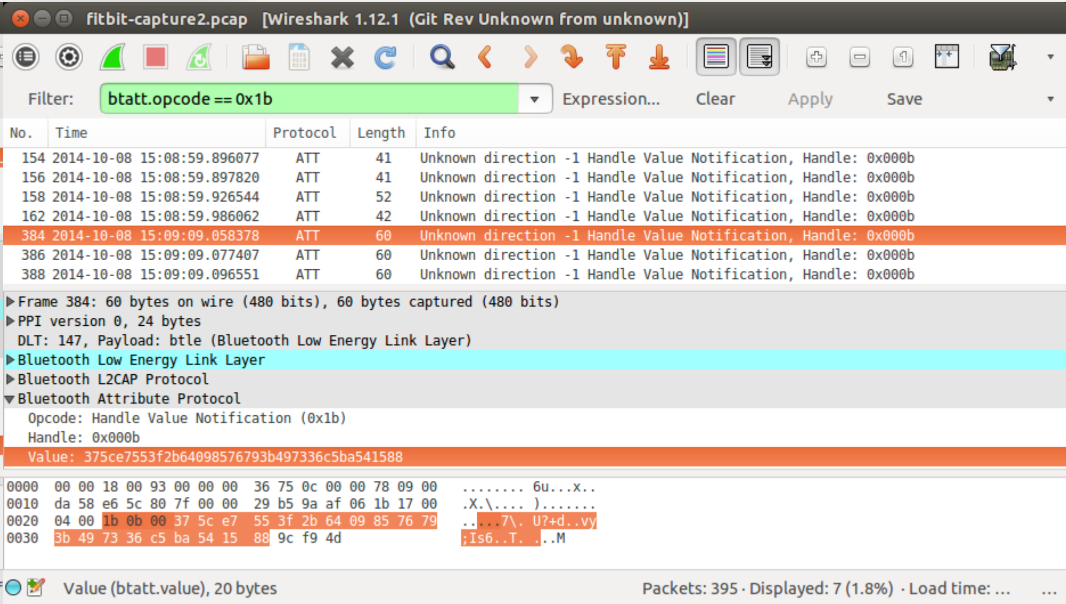
Filter: btatt.handle==0x0003

```
No.  Time                        Protocol  Length  Info
275 2014-10-08 15:09:01.965938    ATT        45    Unknown direction -1 Read By Type Response, Attribute L
```

```
▶Frame 275: 45 bytes on wire (360 bits), 45 bytes captured (360 bits)
▶PPI version 0, 24 bytes
  DLT: 147, Payload: btle (Bluetooth Low Energy Link Layer)
▶Bluetooth Low Energy Link Layer
▶Bluetooth L2CAP Protocol
▼Bluetooth Attribute Protocol
   Opcode: Read By Type Response (0x09)
   Length: 6
  ▼Attribute Data, Handle: 0x0003
     Handle: 0x0003
     Value: 466c6578
```

```
0000  00 00 18 00 93 00 00 00  36 75 0c 00 00 9c 09 00   ........ 6u......
0010  d1 19 ac 58 80 7f 00 00  29 b5 9a af 0a 0c 08 00   ...X.... ).......
0020  04 00 09 06 03 00 46 6c  65 78 98 f8 b2            ......Fl ex...
```

Value (btatt.value), 4 bytes ... Profile: Def



fitbit-capture2.pcap [Wireshark 1.12.1 (Git Rev Unknown from unknown)]

Filter: btatt.opcode == 0x1b

```
No.  Time                        Protocol  Length  Info
154 2014-10-08 15:08:59.896077    ATT        41    Unknown direction -1 Handle Value Notification, Handle: 0x000b
156 2014-10-08 15:08:59.897820    ATT        41    Unknown direction -1 Handle Value Notification, Handle: 0x000b
158 2014-10-08 15:08:59.926544    ATT        52    Unknown direction -1 Handle Value Notification, Handle: 0x000b
162 2014-10-08 15:08:59.986062    ATT        42    Unknown direction -1 Handle Value Notification, Handle: 0x000b
384 2014-10-08 15:09:09.058378    ATT        60    Unknown direction -1 Handle Value Notification, Handle: 0x000b
386 2014-10-08 15:09:09.077407    ATT        60    Unknown direction -1 Handle Value Notification, Handle: 0x000b
388 2014-10-08 15:09:09.096551    ATT        60    Unknown direction -1 Handle Value Notification, Handle: 0x000b
```

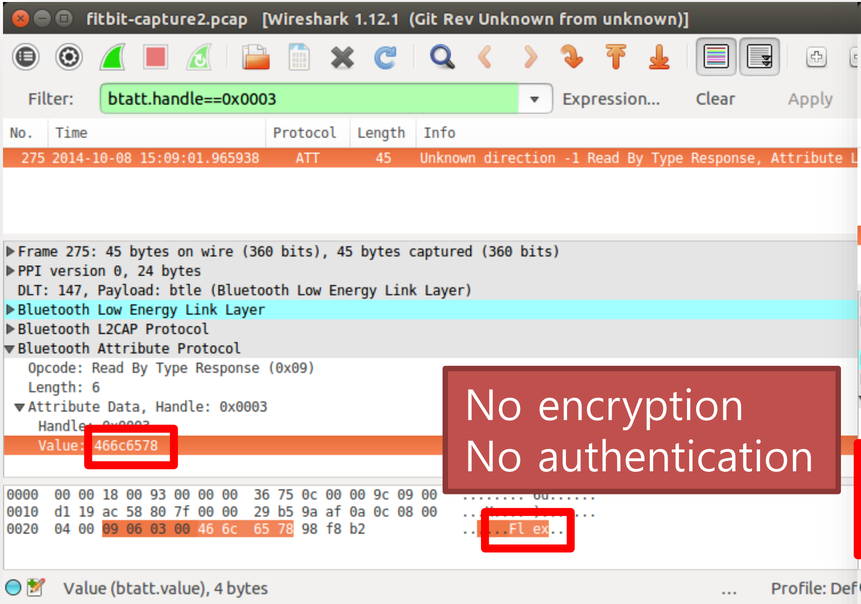
```
▶Frame 384: 60 bytes on wire (480 bits), 60 bytes captured (480 bits)
▶PPI version 0, 24 bytes
  DLT: 147, Payload: btle (Bluetooth Low Energy Link Layer)
▶Bluetooth Low Energy Link Layer
▶Bluetooth L2CAP Protocol
▼Bluetooth Attribute Protocol
   Opcode: Handle Value Notification (0x1b)
   Handle: 0x000b
   Value: 375ce7553f2b64098576793b497336c5ba541588
```

```
0000  00 00 18 00 93 00 00 00  36 75 0c 00 00 78 09 00   ........ 6u...x..
0010  da 58 e6 5c 80 7f 00 00  29 b5 9a af 06 1b 17 00   .X.\.... ).......
0020  04 00 1b 0b 00 37 5c e7  55 3f 2b 64 09 85 76 79   .....7\. U?+d..vy
0030  3b 49 73 36 c5 ba 54 15  88 9c f9 4d               ;Is6..T. ...M
```

Value (btatt.value), 20 bytes   Packets: 395 · Displayed: 7 (1.8%) · Load time: ...

BLE Channel Analysis

- BLE key brute force attack
  - Successfully received BLE packets
  - No encryption -> possible to map meaning of each byte

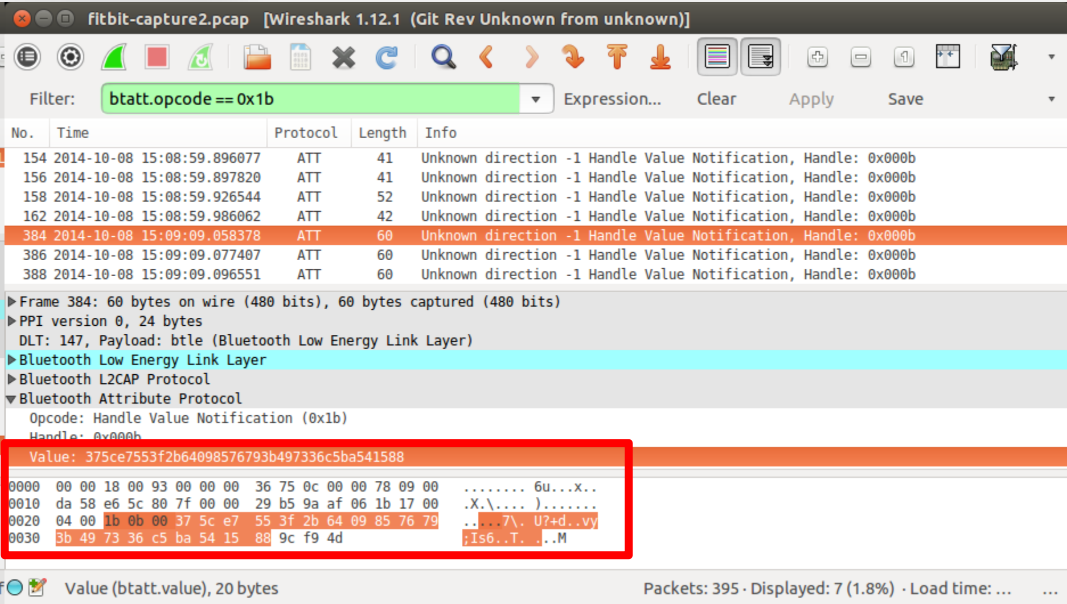

fitbit-capture2.pcap [Wireshark 1.12.1 (Git Rev Unknown from unknown)]
Expression...
Clear
Apply
Profile: Def

Filter: btatt.handle==0x0003

```
No.  Time                          Protocol  Length  Info
 275 2014-10-08 15:09:01.965938    ATT       45      Unknown direction -1 Read By Type Response, Attribute L

▶Frame 275: 45 bytes on wire (360 bits), 45 bytes captured (360 bits)
▶PPI version 0, 24 bytes
  DLT: 147, Payload: btle (Bluetooth Low Energy Link Layer)
▶Bluetooth Low Energy Link Layer
▶Bluetooth L2CAP Protocol
▼Bluetooth Attribute Protocol
   Opcode: Read By Type Response (0x09)
   Length: 6
  ▼Attribute Data, Handle: 0x0003
     Handle: 0x0003
     Value: 466c6578

0000  00 00 18 00 93 00 00 00  36 75 0c 00 00 9c 09 00   ........ 6u......
0010  d1 19 ac 58 80 7f 00 00  29 b5 9a af 0a 0c 08 00   ...X.... ).......
0020  04 00 09 06 03 00 46 6c  65 78 98 f8 b2            ......Fl ex...
```

Value (btatt.value), 4 bytes

No encryption
No authentication


fitbit-capture2.pcap [Wireshark 1.12.1 (Git Rev Unknown from unknown)]
Expression...
Clear
Apply
Save

Filter: btatt.opcode == 0x1b

```
No.  Time                          Protocol  Length  Info
 154 2014-10-08 15:08:59.896077    ATT       41      Unknown direction -1 Handle Value Notification, Handle: 0x000b
 156 2014-10-08 15:08:59.897820    ATT       41      Unknown direction -1 Handle Value Notification, Handle: 0x000b
 158 2014-10-08 15:08:59.926544    ATT       52      Unknown direction -1 Handle Value Notification, Handle: 0x000b
 162 2014-10-08 15:08:59.986062    ATT       42      Unknown direction -1 Handle Value Notification, Handle: 0x000b
 384 2014-10-08 15:09:09.058378    ATT       60      Unknown direction -1 Handle Value Notification, Handle: 0x000b
 386 2014-10-08 15:09:09.077407    ATT       60      Unknown direction -1 Handle Value Notification, Handle: 0x000b
 388 2014-10-08 15:09:09.096551    ATT       60      Unknown direction -1 Handle Value Notification, Handle: 0x000b

▶Frame 384: 60 bytes on wire (480 bits), 60 bytes captured (480 bits)
▶PPI version 0, 24 bytes
  DLT: 147, Payload: btle (Bluetooth Low Energy Link Layer)
▶Bluetooth Low Energy Link Layer
▶Bluetooth L2CAP Protocol
▼Bluetooth Attribute Protocol
   Opcode: Handle Value Notification (0x1b)
   Handle: 0x000b
   Value: 375ce7553f2b64098576793b497336c5ba541588

0000  00 00 18 00 93 00 00 00  36 75 0c 00 00 78 09 00   ........ 6u...x..
0010  da 58 e6 5c 80 7f 00 00  29 b5 9a af 06 1b 17 00   .X.\.... ).......
0020  04 00 1b 0b 00 37 5c e7  55 3f 2b 64 09 85 76 79   .....7\. U?+d..vy
0030  3b 49 73 36 c5 ba 54 15  88 9c f9 4d               ;Is6..T. ...M
```

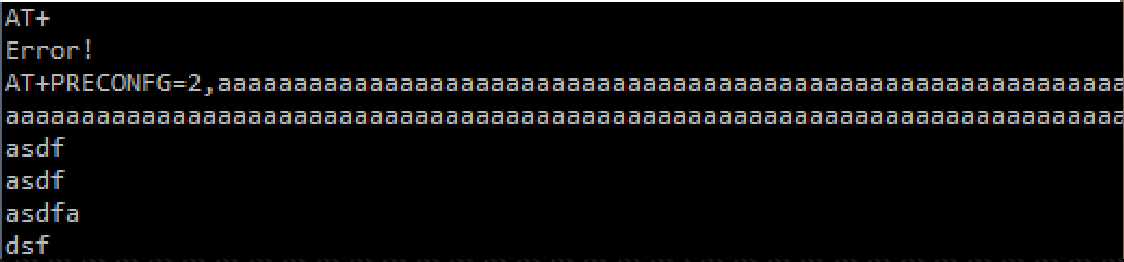
Value (btatt.value), 20 bytes

Packets: 395 · Displayed: 7 (1.8%) · Load time: ...

Device Analysis

- Hidden function
  - Device configuration
  - Firmware update

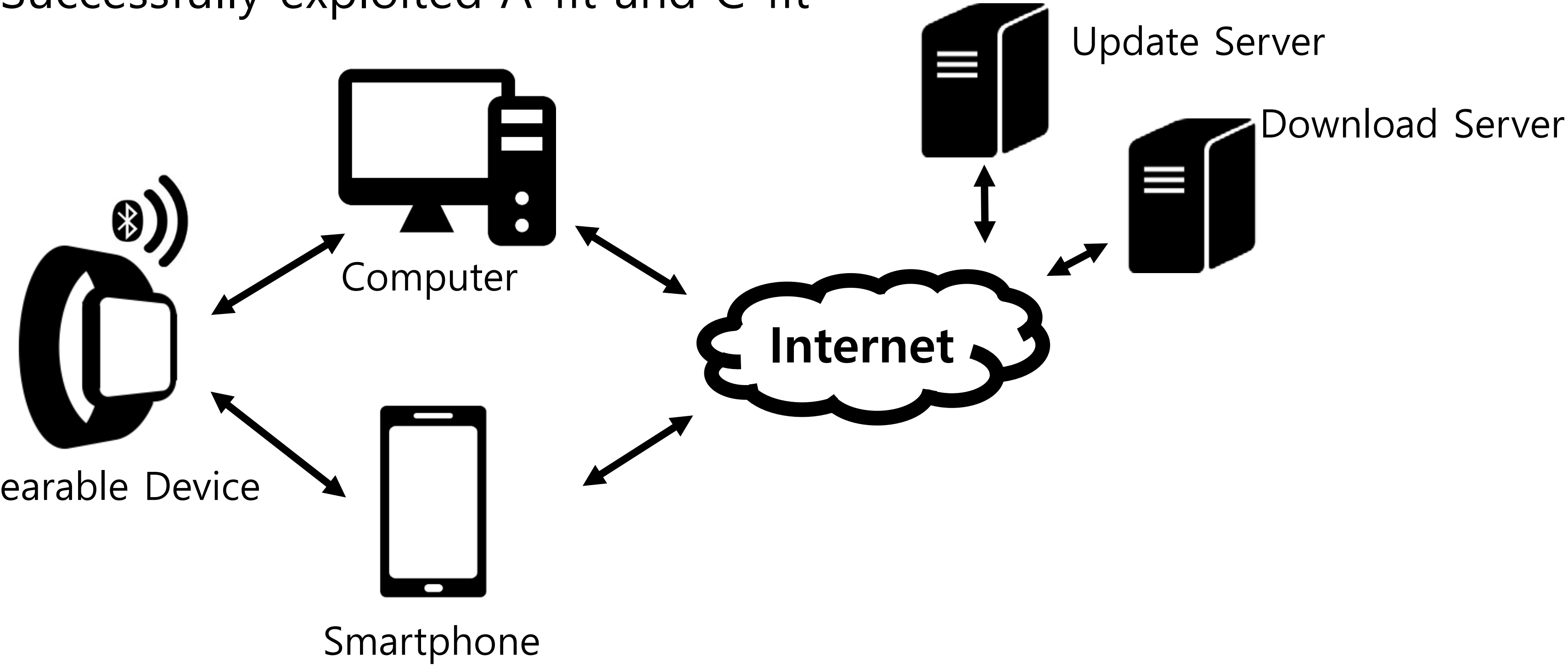
- Hidden protocol
  - AT command
  - Found BOF vuln.
  - **Crashed with ‘Hardware Fault’ message**



```
AT+
Error!
AT+PRECONFG=2,aaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaa
aaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaa
asdf
asdf
asdfa
dsf
```

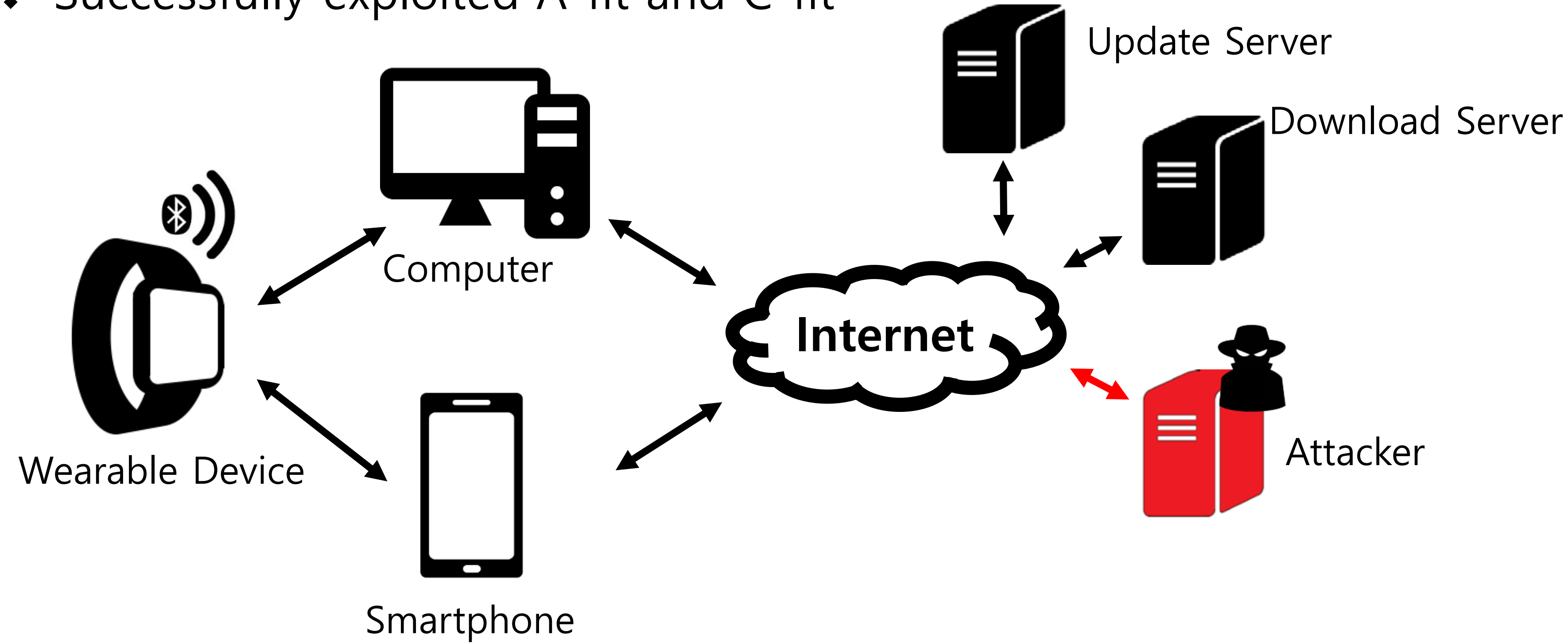
Exploitation

- Successfully exploited A-fit and C-fit



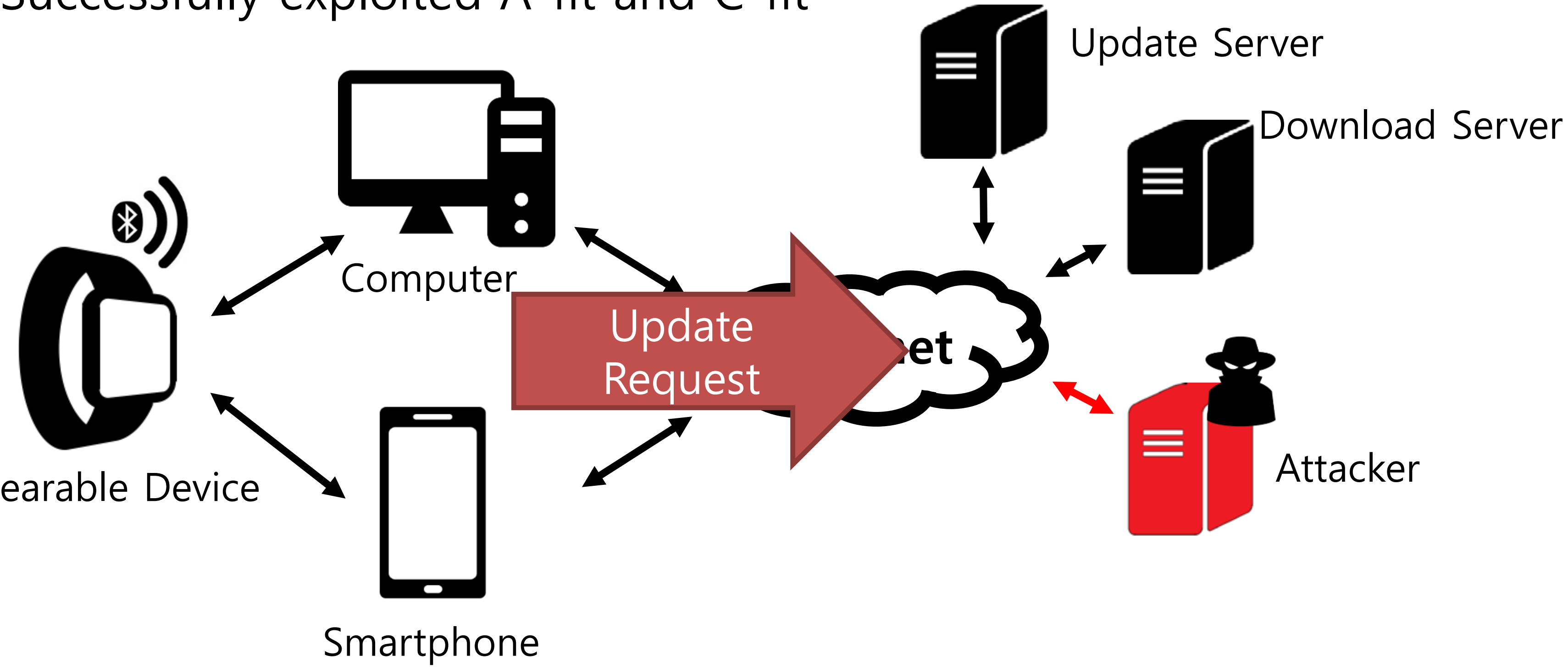
Exploitation

- Successfully exploited A-fit and C-fit



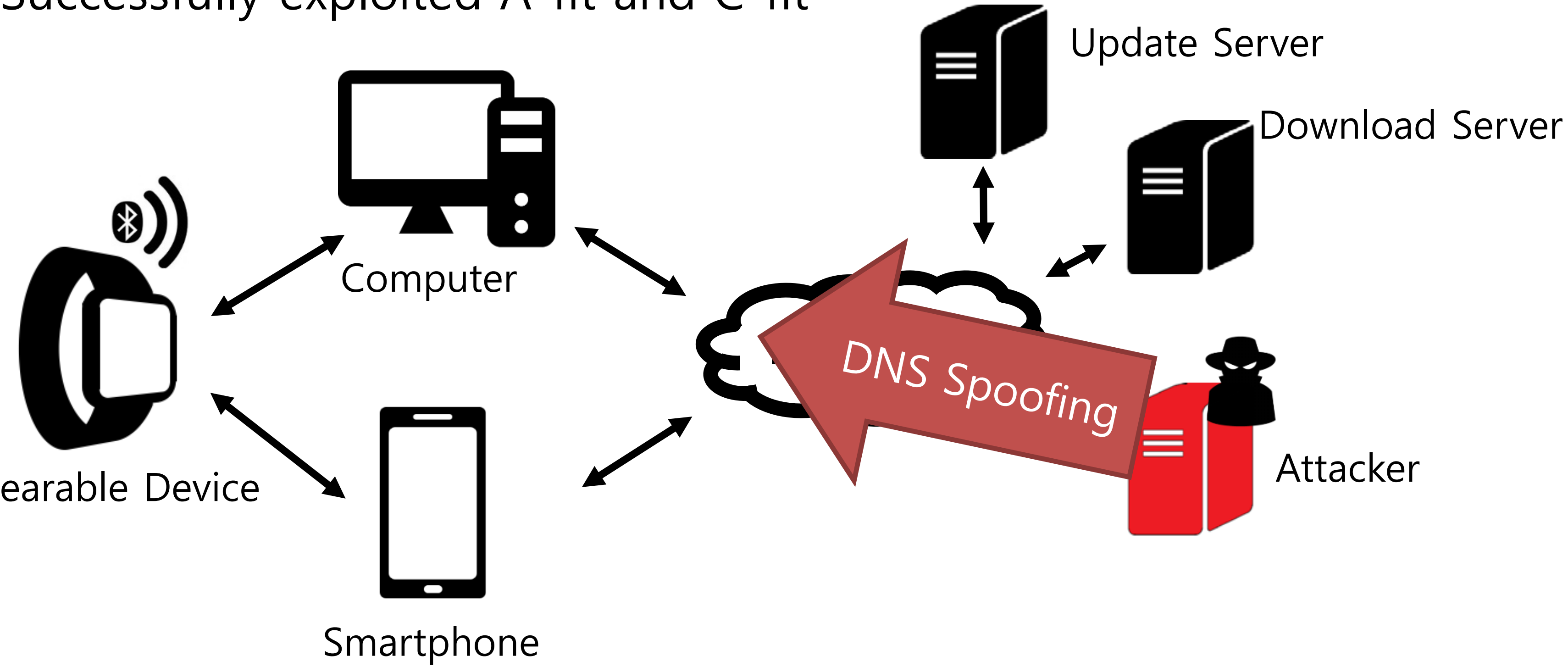
Exploitation

❖ Successfully exploited A-fit and C-fit



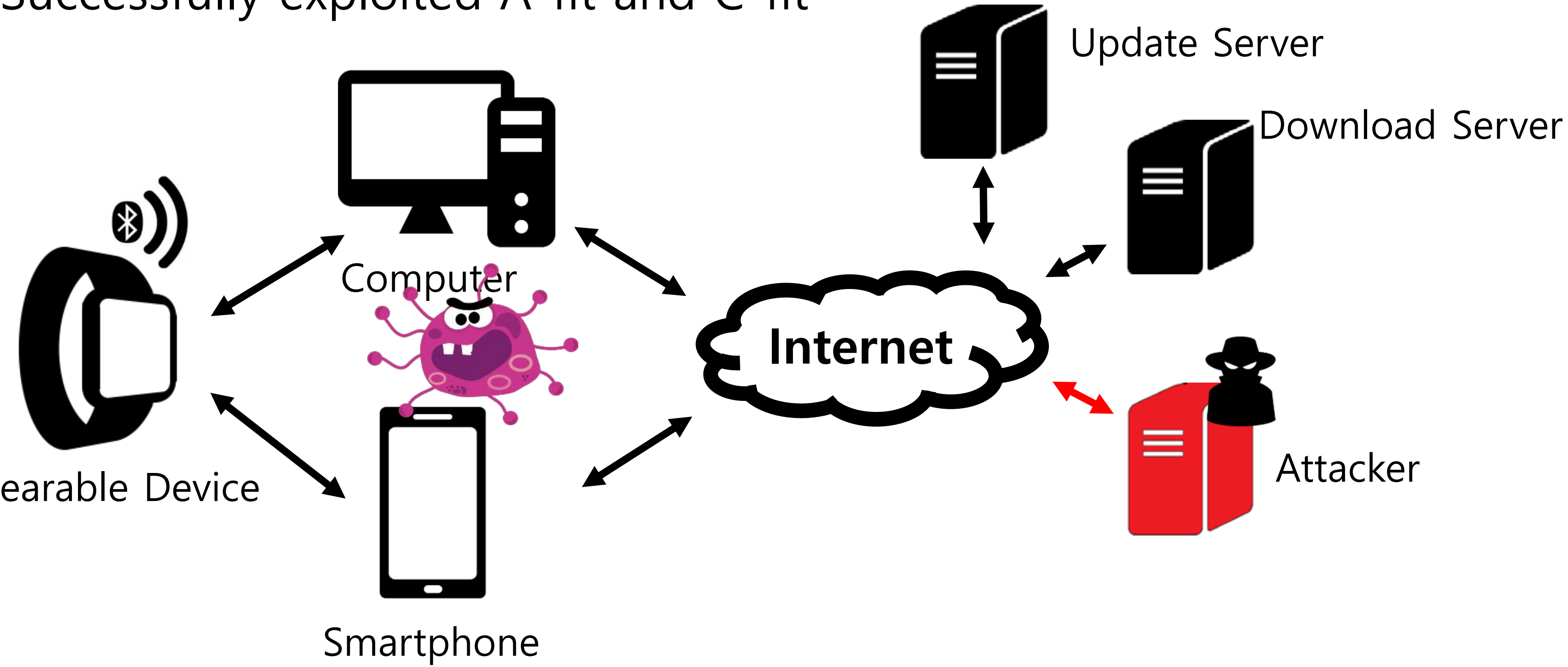
Exploitation

- Successfully exploited A-fit and C-fit



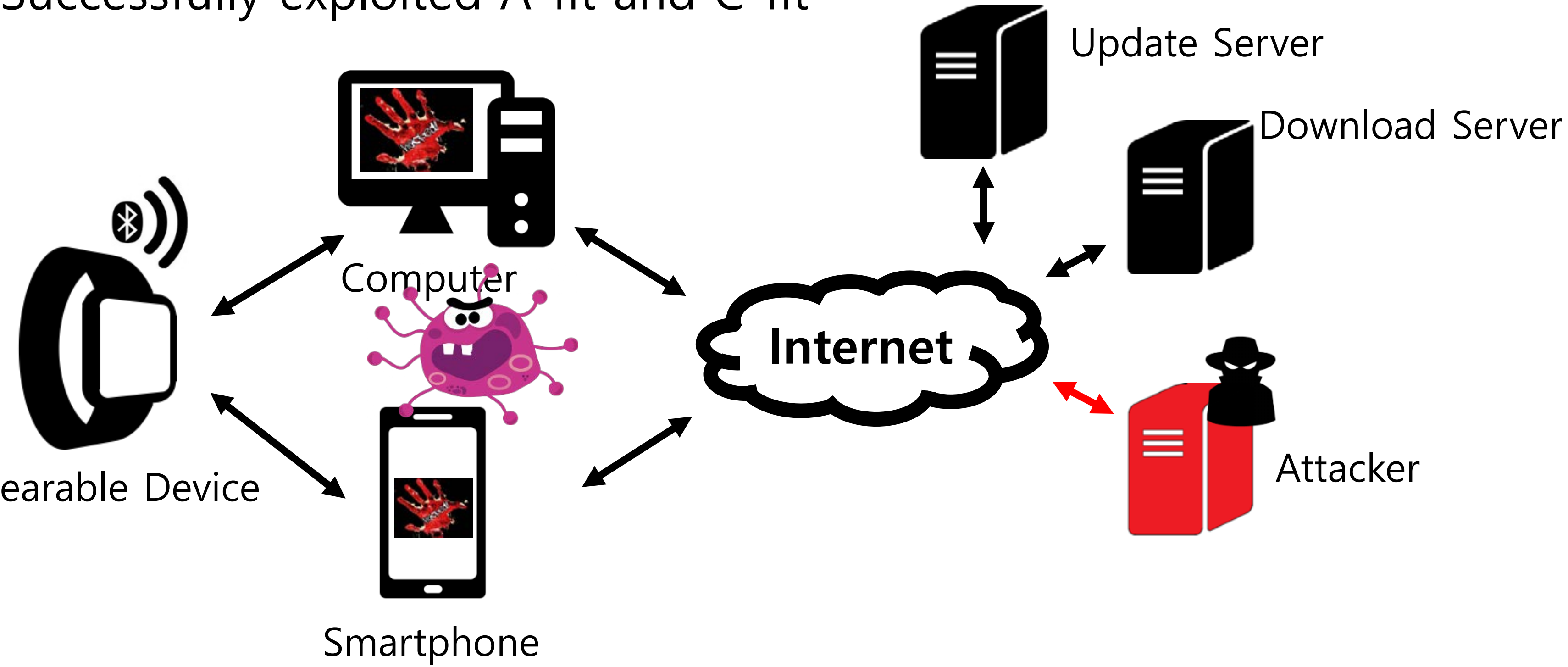
Exploitation

- Successfully exploited A-fit and C-fit



Exploitation

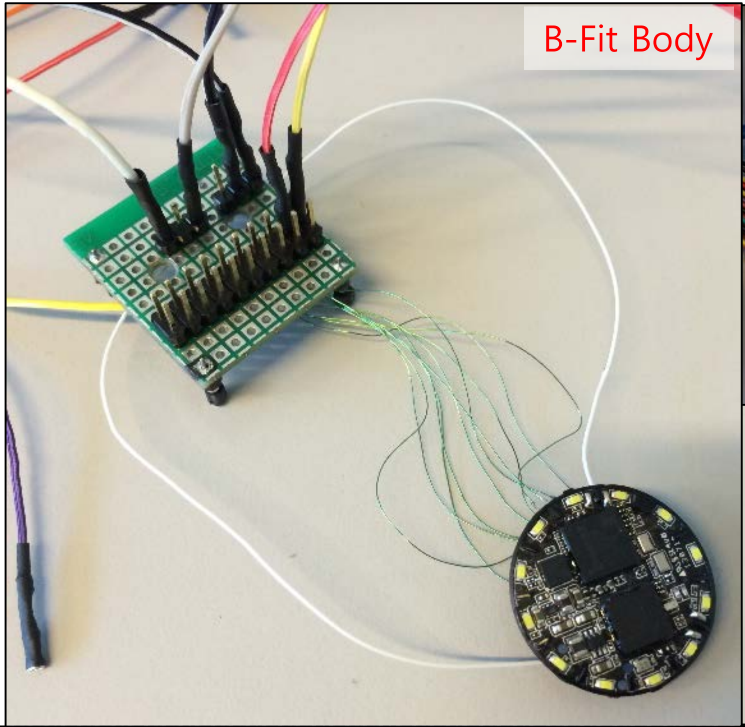
- Successfully exploited A-fit and C-fit



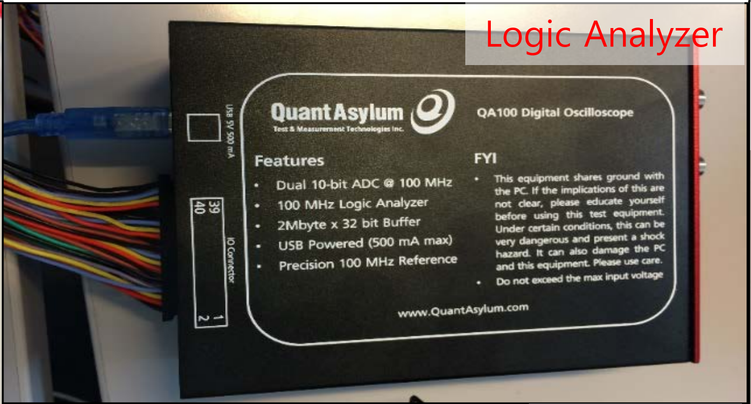
Demo

Failure to Debug Hardware

- Tried to find hardware debug points, but,

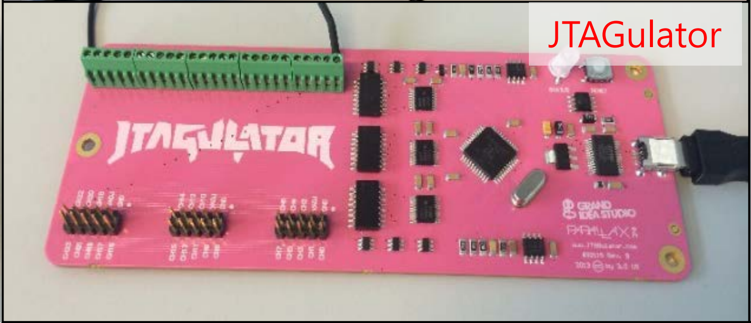


B-Fit Body



Logic Analyzer

Quant Asylum
Test & Measurement Technologies Inc.
QA100 Digital Oscilloscope
Features
Dual 10-bit ADC @ 100 MHz
100 MHz Logic Analyzer
2Mbyte x 32 bit Buffer
USB Powered (500 mA max)
Precision 100 MHz Reference
FYI
This equipment shares ground with the PC. If the implications of this are not clear, please educate yourself before using this test equipment. Under certain conditions, this can be very dangerous and present a shock hazard. It can also damage the PC and this equipment. Please use care.
Do not exceed the max input voltage
www.QuantAsylum.com
IO Connector

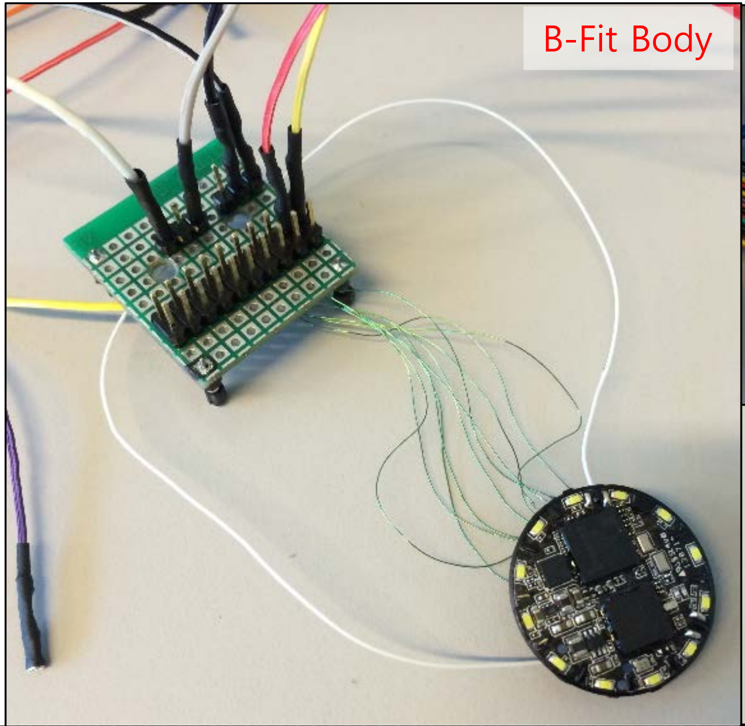


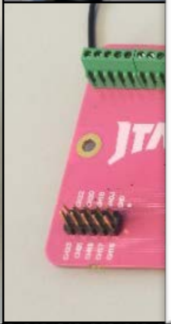
JTAGulator

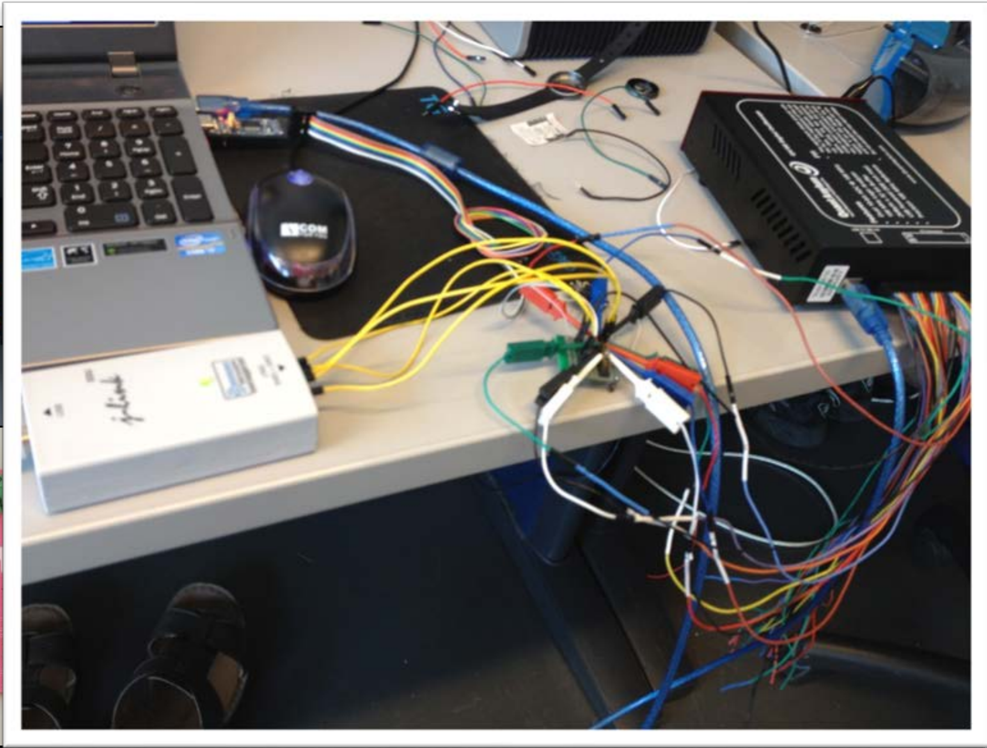
J-link
- JTAG
- SWD

Failure to Debug Hardware

❖ Tried to find hardware debug points, but,

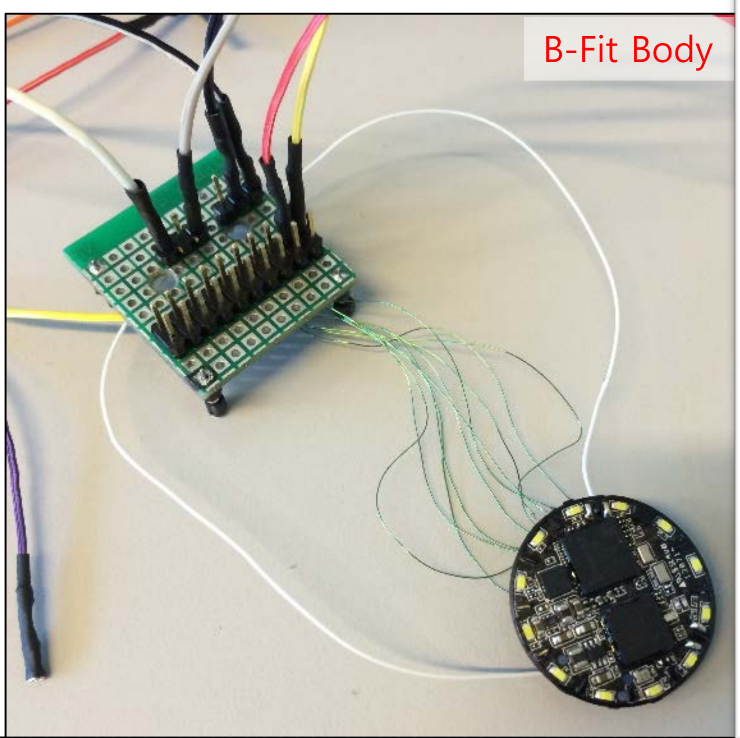


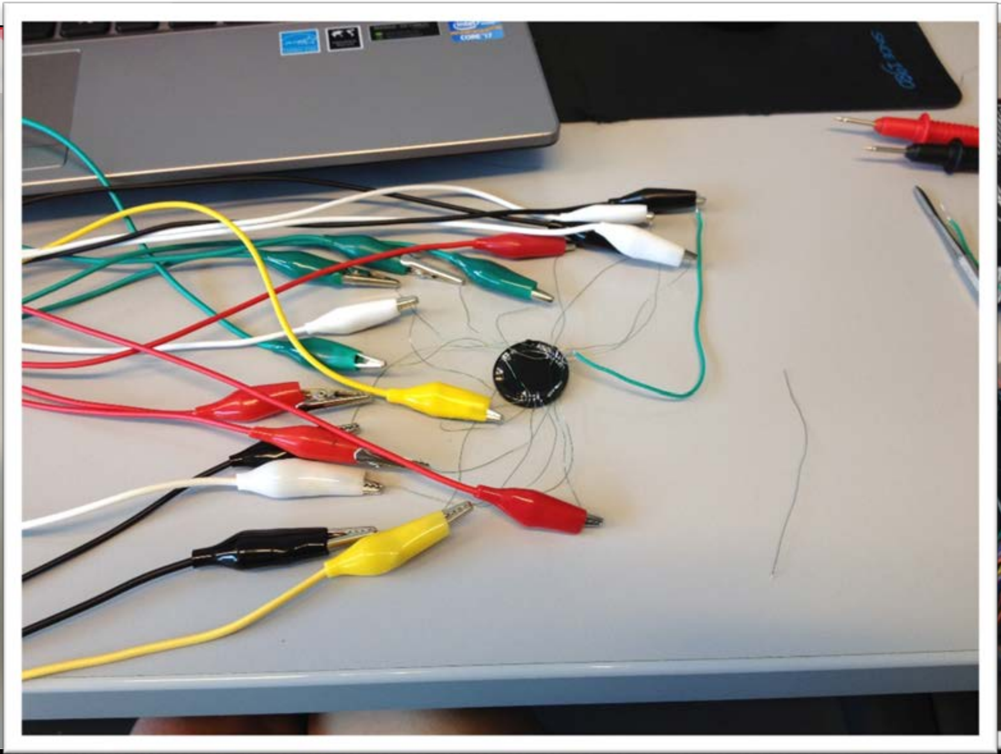




Failure to Debug Hardware

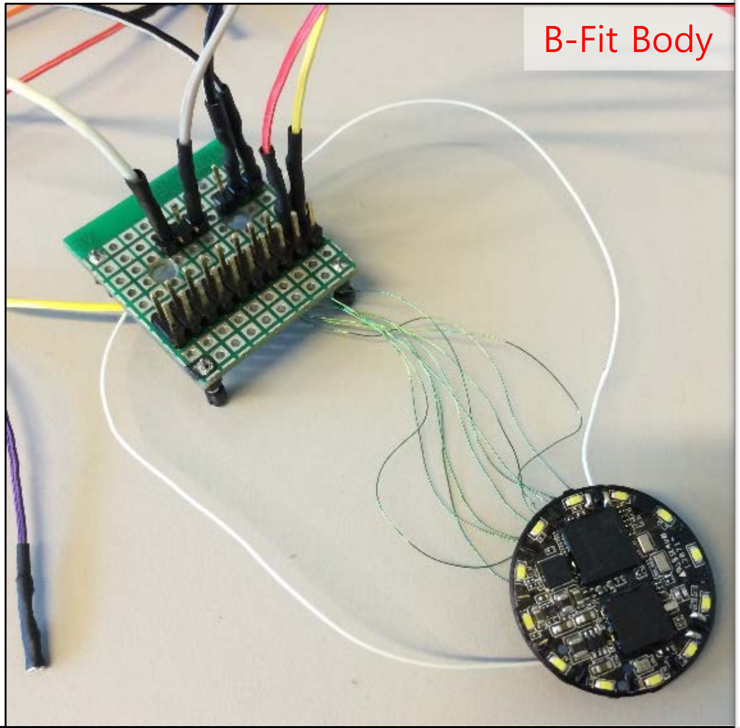
❖ Tried to find hardware debug points, but,

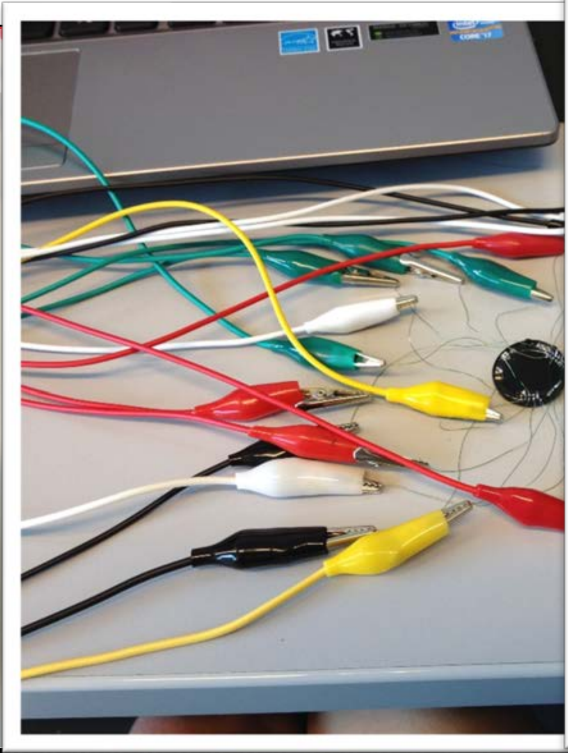


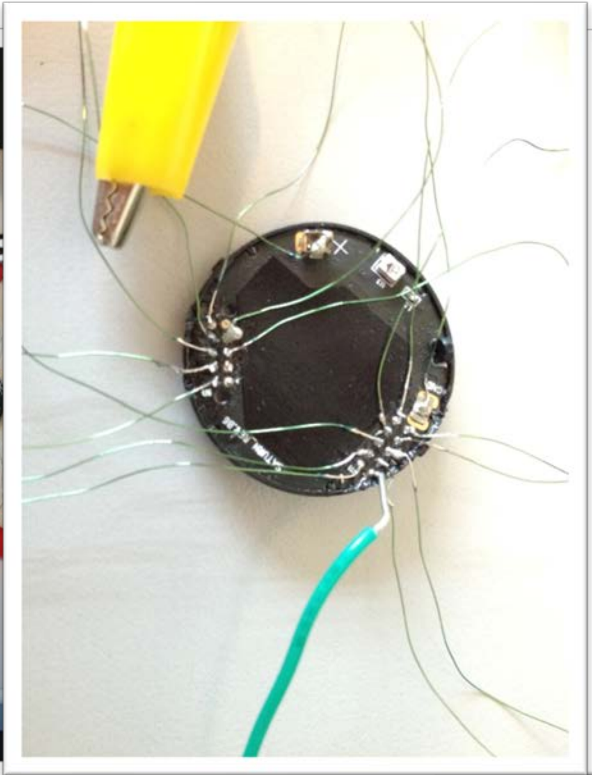


Failure to Debug Hardware

❖ Tried to find hardware debug points, but,

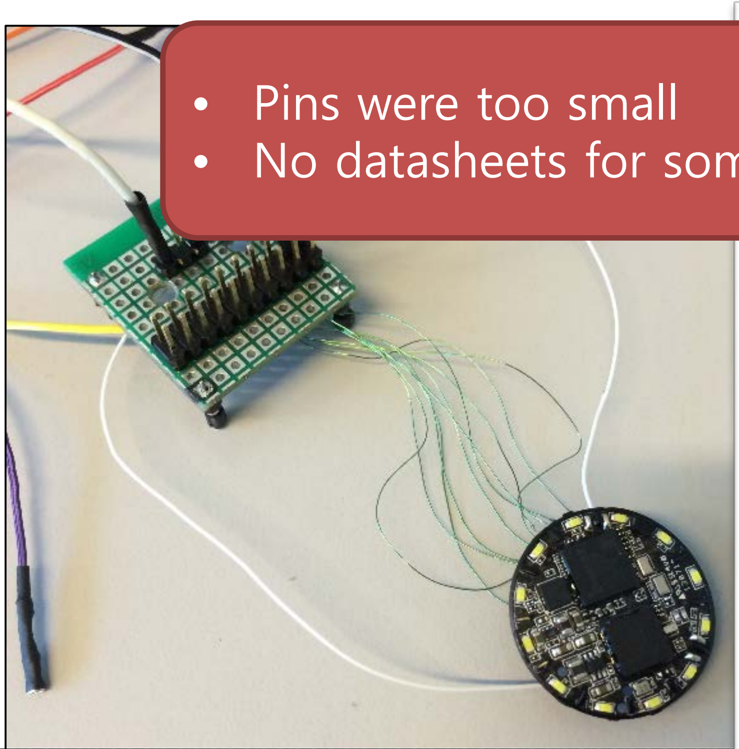


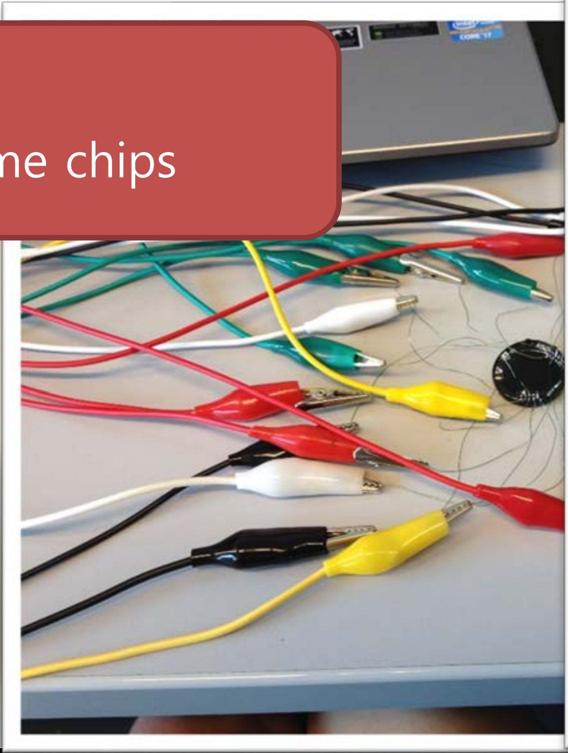


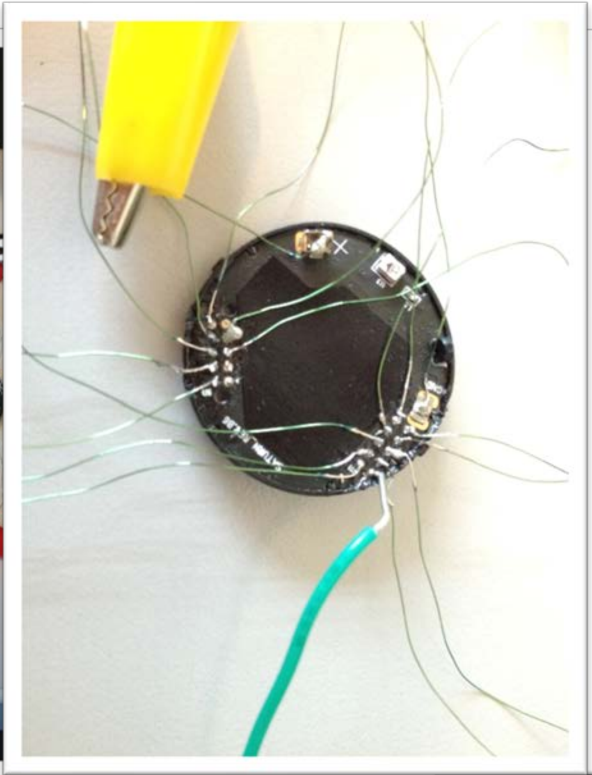


Failure to Debug Hardware

❖ Tried to find hardware debug points, but,

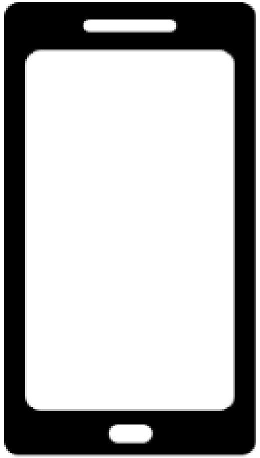






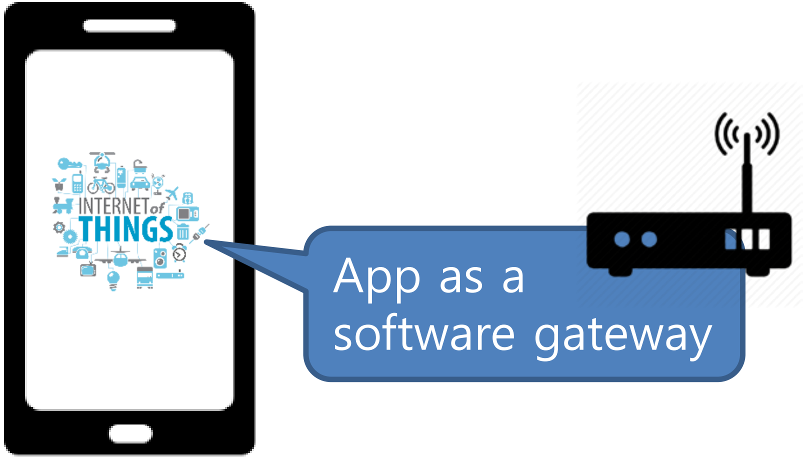
- Pins were too small
- No datasheets for some chips

Secure Device for IoT Devices



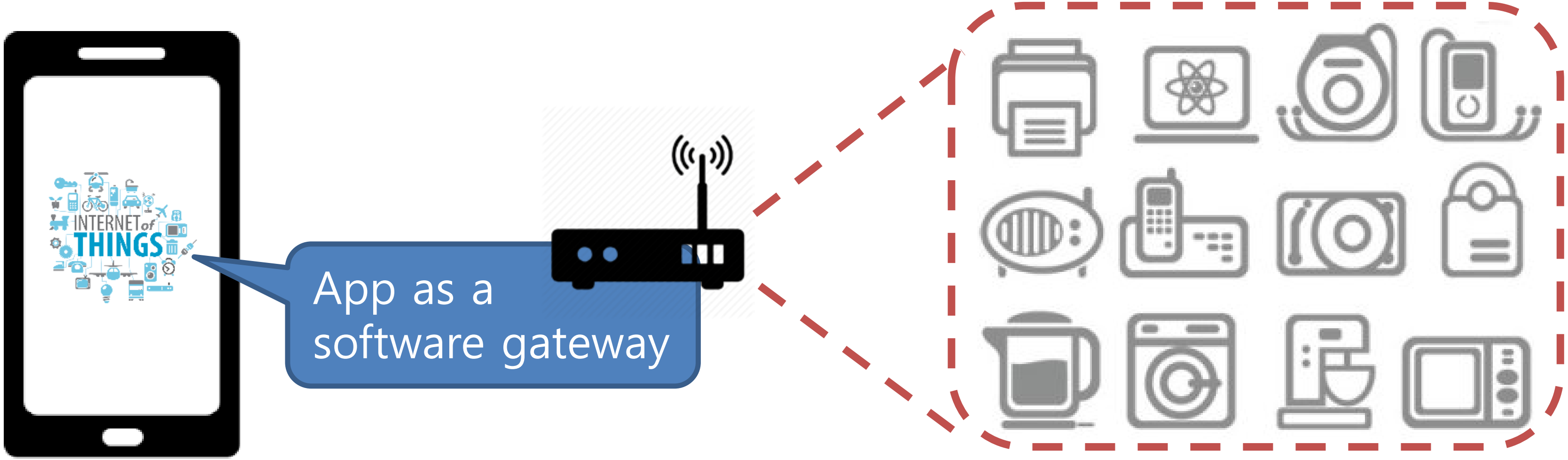
Secure Device for IoT Devices

Secure Device for IoT Devices



App as a software gateway

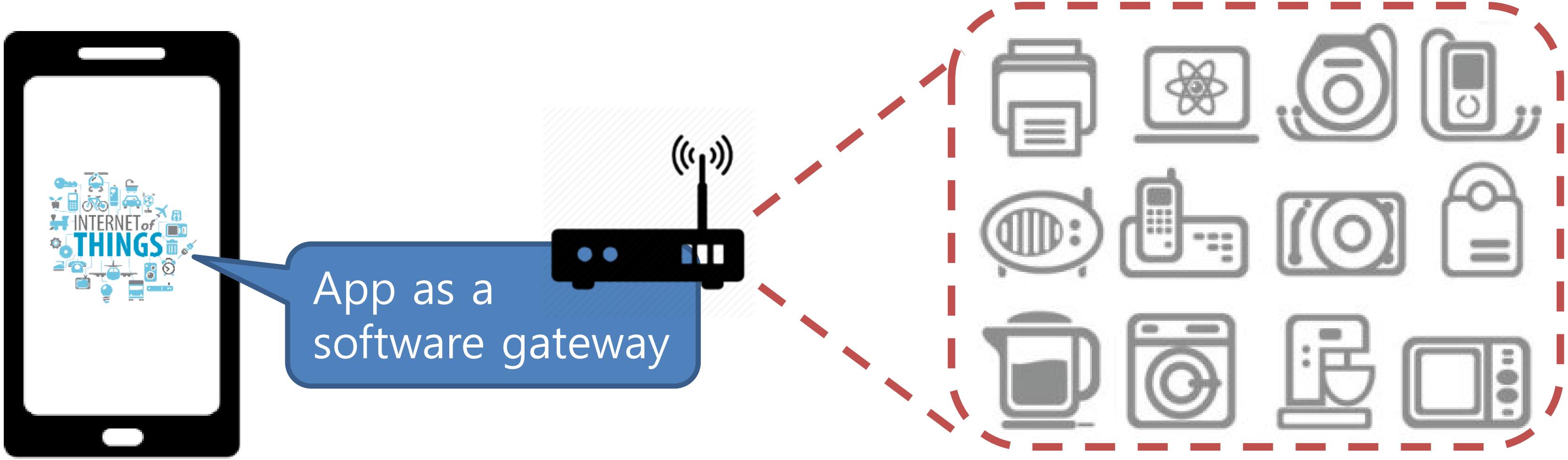
Secure Device for IoT Devices



App as a software gateway

Secure Device for IoT Devices

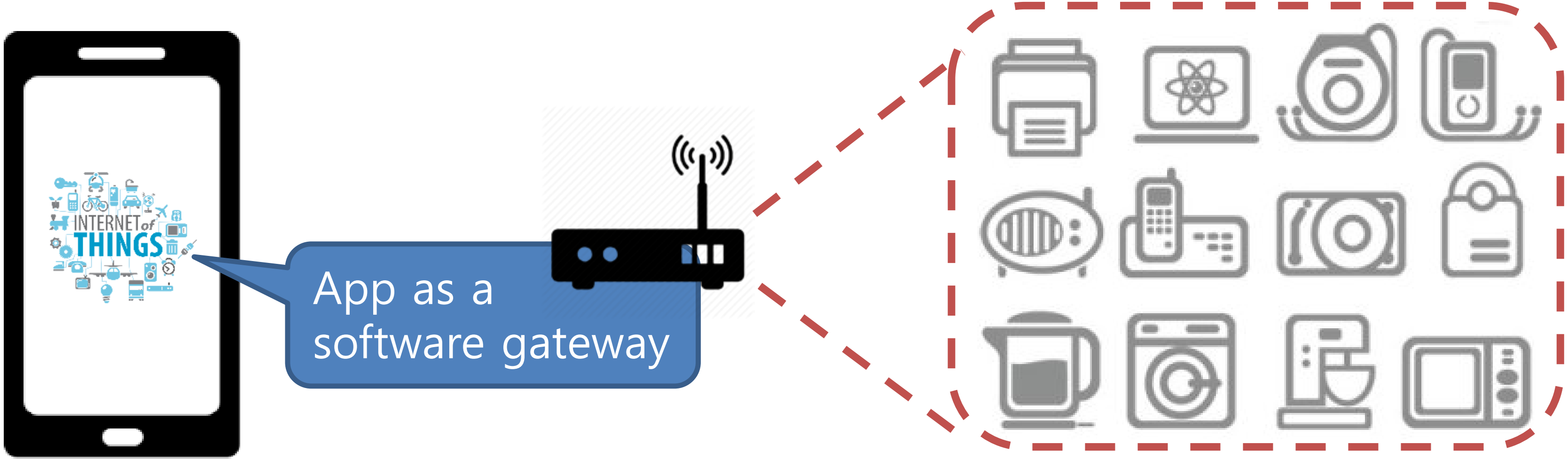
- If software gateway is compromised, all other IoT devices are in danger.
  - **Modifying or stealing user data** are possible.
  - Adversaries can **send malicious commands**.



App as a software gateway

Secure Device for IoT Devices

- ❖ If software gateway is compromised, all other IoT devices are in danger.
  - – **Modifying or stealing user data** are possible.
  - – Adversaries can **send malicious commands**.
- ❖ Even, smartphone itself have multiple vulnerabilities.
  - – Compromised smartphone can **manipulate all IoT devices**.



App as a software gateway

Countermeasure

- For communication
  - Use **SSL/TLS** with proper **certificate verification**
  - **Encryption** before data transmission

Countermeasure

- For communication
  - Use **SSL/TLS** with proper **certificate verification**
  - **Encryption** before data transmission

- For software gateways/devices,
  - Server **authentication**
  - **Integrity check** before app/firmware update
  - Use **TruztZone/secure-boot** for tamper-proof integrity check

Countermeasure

- For communication
  - Use **SSL/TLS** with proper **certificate verification**
  - **Encryption** before data transmission

- For software gateways/devices,
  - Server **authentication**
  - **Integrity check** before app/firmware update
  - Use **TruztZone/secure-boot** for tamper-proof integrity check

- For BLE,
  - Bluetooth 4.2 support **secure simple pairing (SSP)** to prevent MitM
  - Need **low-power yet continuous update** technique
  - Make devices **up-to-date**

Conclusion

- ❖ Analyzing rising wearable devices,
  - Classified possible attack vectors
  - Found 17 vulnerabilities from three popular fitness trackers
  - Successfully exploited two of them

- ❖ Future work
  - Designing a secure IoT communication paltform
  - Implementing automatic vulnerability analysis framework for embedded devices

Conclusion

- Analyzing rising wearable devices,
  - Classified possible attack vectors
  - Found 17 vulnerabilities from three popular fitness trackers
  - Successfully exploited two of them
  - **Emphasized the necessity for secure design of IoT devices**

- Future work
  - Designing a secure IoT communication paltform
  - Implementing automatic vulnerability analysis framework for embedded devices

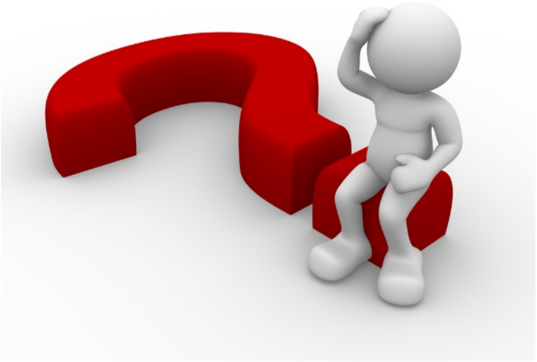
Conclusion

- ❖ Analyzing rising wearable devices,
  - Classified possible attack vectors
  - Found 17 vulnerabilities from three popular fitness trackers
  - Successfully exploited two of them

Software gateways should be investigated seriously
(Not only its usability, but also its security)

  - Implementing automatic vulnerability analysis framework for embedded devices

Thank You



dkay@kaist.ac.kr