

REFERANSE:
[Skriv inn referanse]

DATO:
08.08.2017

VERSJON:
1.0

ANSVARLIG:
Martin Gravråk

Report

Investigation of privacy and security issues with internet connected health gadgets

Preface

This report has been written by Bouvet on behalf of the Norwegian Consumer Council. The report is about security and privacy issues regarding internet connected health gadgets.

Bouvet is a Scandinavian consultancy which works for players in all major sectors who are important for society. Bouvet provide services in information, technology, digital communication and enterprise management and have 1 100 employees at 15 offices in Norway and Sweden.

Summary

Privacy and security regarding internet connected blood pressure and blood sugar measuring devices have been investigated in this report. The 7 devices that have been tested are:

- Andersson BDR 1.0
- Apple QardioArm
- iHealth BP7
- Withings WPMo2
- 2in1 Smart
- Bayer Contour Next One
- iHealth BG5

All of them are connected to the internet through a mobile phone and an app. Two of them can be used without the app, 5 of them require the app to work, and 4 of them cannot be used without creating an account.

Most of the apps use various 3. Party logging services to monitor usage and errors in the app. In many cases this can reveal that a measurement is done, and there is a danger that this information can be used to conjecture health information about the user.

Contents

Preface.....	2
Summary	3
1 Introduction	5
2 Test devices	6
2.1 Devices	6
2.1.1 Blood pressure	6
2.1.2 Blood sugar	6
3 What was tested	8
3.1 Internet communication.....	8
3.1.1 Encryption of data.....	8
3.1.2 Cloud.....	8
3.1.3 Email.....	8
3.1.4 3. Parties	8
3.1.5 Accounts.....	9
3.2 Bluetooth.....	9
3.3 Hardware	9
4 Testing setup	10
4.1 Man-in-the-middle.....	10
4.2 Internet Communication	10
5 Results.....	11
5.1 Andersson BDR 1.0	11
5.1.1 Summary.....	11
5.2 QardioArm	12
5.2.1 Mixpanel.com.....	13
5.2.2 Segment	14
5.2.3 Google-analytics.....	14
5.3 iHealth BP7	15
5.3.1 data.mistat.com.....	17
5.3.2 data.flurry.com.....	18
5.3.3 Summary.....	18
5.4 Withings WPMo2.....	19
5.4.1 Amplitude	20
5.4.2 Google-analytics.com	21
5.4.3 Summary.....	21
5.5 2ini Smart	22
5.5.1 Summary.....	23
5.6 Bayer Contour Next One	24
5.6.1 Summary.....	24
5.7 iHealthBG5.....	25
5.7.1 Built in web view	26
6 Location of servers	27
6.1 api.ihealthlabs.com	27
6.2 api.ihealthlabs.eu	27
6.3 ios.bugly.qq.com	27
6.4 pingma.qq.com.....	28
6.5 xiaomi.com.....	28
6.6 flurry.com.....	28
6.7 data.flurry.com.....	28
6.8 api.segment.io	29
6.9 api.mixpanel.com	29
6.10 fusion.qq.com.....	29
6.11 data.mistat.xiaomi.com	30
6.12 api.amplitude.com.....	30

1 Introduction

This report concerns itself with the information security of internet connected health devices. These devices collect health information like blood pressure and glucose levels. This obviously makes for some safety concerns, as it might be possible for unauthorized people to obtain health information about the users, which potentially could be abused in a number of ways.

The information these devices collect is also classified as medical information and therefore subject to strict regulations on where it can be stored and transmitted.

How sensitive information is stored and processed server-side is outside the scope of this report because we do not have access to the manufactures or the third-party's servers. The focus has instead been on what kind of information that is sent, how information is sent, where it is sent and how difficult it would be for an unauthorized user to connect to the devices and use it to gather information.

In addition, we have looked into if it is possible to use the devices without storing medical information in the cloud as we could not see much benefit for the users in doing this.

2 Test devices

2.1 Devices

2.1.1 Blood pressure

2.1.1.1 Quardio Arm

Android:	Quardio Heart Health (1.16.2)
Apple:	Quardio Heart Health (1.65.1)

2.1.1.2 iHealth BP7

Android:	iHealth MyVitals (3.5.0)
Apple:	iHealth MyVitals (3.5.1)

2.1.1.3 Andersson BDR 1.0

Android:	MedM Health (2.0.170)
Apple:	MedM Health (2.0.102)

2.1.1.4 Withings WPMo2

Android:	Withings Health Mate (2.21)
Apple:	Withings Health Mate (2.18.3)

2.1.2 Blood sugar

2.1.2.1 iHealth BG5

Android:	iHealth MyVitals (3.5.0)
----------	--------------------------

Apple:	iHealth Gluco-Smart (4.1.1)
--------	-----------------------------

2.1.2.2 2in1 Smart

Android:	2in1 Smart(2.1)
Apple:	2in1 SMART (3.6.0)

2.1.2.3 Bayer Contour Next One

Android:	Contour Diabetes app(1.2.55)
Apple:	CONTOUR DIABETES app (NO) 1.2.55

.

3 What was tested

3.1 Internet communication

The tests were limited to what we considered “normal usage” of the apps devices. For each app/device the following tests (if applicable) on both iOS and Android were executed:

- Do a measurement without the app (if possible)
- Install the app
- Start the app
- Connect the device
- Do a measurement without an account (if possible)
- Create an Account
- Do a measurement with an account
- Explore the various functions in the app

Each app was only tested for a limited amount of time, meaning that the apps could be transmitting more information than we were able to uncover. Our main focus has been encryption, where the data was sent and what kind of information that has been sent directly to third parties.

3.1.1 Encryption of data

We used Fiddler to check if the data transmitted from the devices was properly encrypted.

3.1.2 Cloud

Despite no apparent benefit for the user most of the apps chose to store and process health information in the cloud. We did not see any features that could not have been implemented just as well locally where the user would have had much more control over their own data.

We checked if the measurements were stored in the cloud, if it was possible to choose not to store your health information in the cloud and where the servers the information was sent to was physically located.

3.1.3 Email

Some of the apps had a feature to export data from the app and send them by email. While the possibility to export data out of the app is a very important feature email is often a very unsecure way of transmitting information and should probably not be used for transferring sensitive health information.

3.1.4 3. Parties

Most of the devices in the test use logging services such as mixpanel¹, Crashlytics² and segment³ to log usage and crashes in the apps. These services are used in large number of apps, but they can be problematic if health information is sent to them. We checked what 3. parties' data was sent to, and where their servers were located.

¹ <https://mixpanel.com/>

² <http://crashlytics.com/>

³ <https://segment.com>

3.1.5 Accounts

We checked if you had to create an account to use the product. And what information the user had to provide.

3.1.5.1 Passwords

When storing sensitive information in the cloud strong passwords is important. We therefore checked if the apps would allow users to use passwords like 'password' or if they required a stronger password.

3.2 Bluetooth

All the devices except 2in1 Smart use Bluetooth to communicate with the smart phone or tablet it is connected to. We did not do any test to verify the authentication and encryption of the Bluetooth communication.

3.3 Hardware

We checked if it was possible to use the product without using the app.

4 Testing setup

4.1 Man-in-the-middle

To monitor the communication between the app and its web-services a man-in-the-middle approach was taken. This was achieved by routing all of the Internet traffic between the phone/tablets through our computer, making it what is known as a proxy-server. This made it possible to see what information was transmitted between the app and the various Internet servers and how often the communication occurred. Fiddler⁴ was used to monitor the Internet Traffic and to create the proxy server.

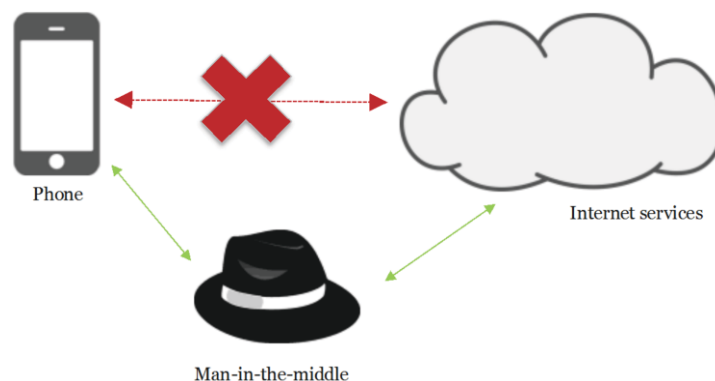


Figure 1: Overview of a man-in-the-middle attack

All of the apps uses SSL encryption on most of the Internet traffic. This is an added security layer to the unsecure HTTP message protocol, and is known as HTTPS. To break this encryption a custom root-certificate, provided by Fiddler, was installed on the phones/tablets. A root-certificate tells the phone which servers it can trust on the Internet, and the certificate provided by Fiddler makes the phones/tablets trust our proxy-server, enabling us to decrypt the traffic. This is not regarded as a security flaw as 1) it requires physical access to the phone/tablet and the knowledge of how to unlock it.

There is however possible for the app to detect this kind of monitoring and use this information to hide information from us. If the manufacturer does a thorough and deliberate effort to hide certain parts of communication it can be very hard to detect without a much more extensive testing. Except some SSL-Pinning we did not observe any indications on this.

4.2 Internet Communication

All the apps use HTTPS (encryption) when utilizing network communication, except for 2in1 witch does not use network communication except optional email.

⁴ [More information about Fiddler](#)

5 Results

5.1 Andersson BDR 1.0

About the app	
Name of app	MedM Health
Version tested (Android)	2.0.170
Version tested (iOS)	2.0.102
Security	
Is data encrypted in app?	Yes
Is data flow encrypted?	Yes
Data collection/Privacy	
Does the service include privacy settings?	No
Do the privacy settings have any actual effect?	n/a
Is data stored locally or in the cloud?	Cloud, if using account.
Is it possible to opt out of using cloud storage?	Yes
Is data sent to third parties?	No
Is there a function to share health data by e-mail?	No
Third parties	
What third parties is data sent to?	Could not detect any data sent to third parties
Data that identifies the user?	No
Data that identifies that the user is using the device?	No
Data that identifies when the user is taking measurements?	No
Data including the measurement values?	No
Where is data transmitted?	No
Permissions	
Which permissions are asked for?	Camera, location, storage, draw over other apps, control near-field communication, pair with bluetooth, run at startup...
Does the user have to accept all permissions?	No, turned off by default
Registration and deletion	
Is there an account system?	Yes
Is it necessary to create an account?	No
What information is mandatory when creating account?	e-mail, name, date of birth, height, weight
Does the service require a secure password?	6+ letters, accepts "password"

5.1.1 Summary

We could not detect any data sent to 3. parties

5.2 QardioArm

About the app	
Name of app	Qardio Heart Health
Version tested (Android)	1.16.2
Version tested (iOS)	1.65.1
Security	
Is data encrypted in app?	Yes
Is data flow encrypted?	Yes
Data collection/Privacy	
Does the service include privacy settings?	Visitor mode
Do the privacy settings have any actual effect?	Yes. Data is not transmitted while in visitor mode
Is data stored locally or in the cloud?	Cloud
Is it possible to opt out of using cloud storage?	Yes, but then data is not stored at all
Is data sent to third parties?	Yes
Is there a function to share health data by e-mail?	Yes
Third parties	
What third parties is data sent to?	Mixpanel, segment, google-analytics, app-measurement.com, crashlytics.com, Oneskyapp.com
Data that identifies the user?	Sends advertising ID at startup
Data that identifies that the user is using the device?	Yes, sent to MixPanel and Segment
Data that identifies when the user is taking measurements?	Yes, Mixpanel and google-analytics
Data including the measurement values?	Yes, irregular heartbeat (GetQardio, Segment, Mixpanel)
Where is data transmitted?	United States
Permissions	
Which permissions are asked for?	Contacts, Location, storage, collect diagnostic information, read google service configuration, pair with bluetooth devices, run at startup...
Does the user have to accept all permissions?	No, but location is needed to connect to Bluetooth
Registration and deletion	
Is there an account system?	Yes
Is it necessary to create an account?	Yes
What information is mandatory when creating account?	Name, e-mail
Does the service require a secure password?	6+ letters, accepts "password"

5.2.1 Mixpanel.com

```
{
  "event": "set up profile",
  "properties": {
    "mp_lib": "iphone",
    "time": 1502450068,
    "enabled places": "yes",
    "$app_version": "1572",
    "$screen_width": 375,
    "$model": "iPhone9,3",
    "enabled body comp": "no",
    "$app_build_number": "1572",
    "QA measurement pause": 0,
    "$carrier": "Telenor",
    "distinct_id": "896e9e96f3ae03b10ea958fe71ffc02a",
    "$wifi": true,
    "enabled photo slideshow": "no",
    "QA measurement count setting": 1,
    "entered doc info": "no",
    "mp_device_model": "iPhone9,3",
    "token": "8c1b99c8c8478122625acf27e65d0442",
    "step goal": 10000,
    "$app_release": "1.73",
    "$screen_height": 667,
    "enabled apple health": "no",
    ..
  }
}
```

#32

A detailed log of what you are doing in the app is sent to mixpanel.com, each event includes a distinct id to identify your phone.

```
{
  "event": "Loaded a Screen",
  "properties": {
    "mp_lib": "iphone",
    "time": 1494328362,
    "enabled places": "yes",
    "$app_version": "1487",
    "$screen_width": 375,
    "$model": "iPhone9,3",
    "enabled body comp": "no",
    "$app_build_number": "1487",
    "QA measurement pause": "0",
    "$carrier": "Telenor",
    "distinct_id": "28d73507b1305667ac88255ccc60b4e1",
    "$wifi": true,
    "name": "QA measurement results IHB",
    "enabled photo slideshow": "no",
    "QA measurement count setting": 1,
    "entered doc info": "no",
    "mp_device_model": "iPhone9,3",
    "token": "8c1b99c8c8478122625acf27e65d0442",
    "$app_release": "1.65.1",
    "$screen_height": 667,
    "enabled apple health": "no",
    "$radio": "None",
    "$ios_ifa": "3159C19D-8160-4CA7-811C-2E6E8EBCA44E",
    "$os_version": "10.2.1",
    "$manufacturer": "Apple",
    "$app_version_string": "1.65.1",
    "$lib_version": "3.0.4",
    "enabled haptic": "no",
    "$os": "iOS"
  }
}
```

When irregular heartbeats are detected this is also logged to Mixpanel.com. These are identified by "QA measurement results IHB"

5.2.2 Segment



The same ID is sent to api.segment.io

5.2.3 Google-analytics

an	Qardio
dm	iPhone9,3
a	1273034528
idfa	2E5A85BC-4144-417C-91E1-1404530BC760
_s	12
ds	app
aid	com.getqardio.Qardio
sr	750x1334
t	screenview
tid	UA-41096274-3
cd	MeasurementStartViewController
v	1
cid	40809b98-71e1-452f-bedf-566aaa678d69
_u	.oK-L
av	1.73
_crc	1
ht	1502452139446
qt	20004

Logs that you enter the measurement screen to google-analytics.

5.3 iHealth BP7

About the app	
Name of app	iHealth MyVitals
Version tested (Android)	3.5.0
Version tested (iOS)	3.5.1
Security	
Is data encrypted in app?	Yes
Is data flow encrypted?	Yes
Data collection/Privacy	
Does the service include privacy settings?	No
Do the privacy settings have any actual effect?	n/a
Is data stored locally or in the cloud?	Cloud
Is it possible to opt out of using cloud storage?	No
Is data sent to third parties?	Yes
Is there a function to share health data by e-mail?	Yes
Third parties	
What third parties is data sent to?	QQ, Flurry, Xiaomi
Data that identifies the user?	Not determined
Data that identifies that the user is using the device?	Yes
Data that identifies when the user is taking measurements?	Yes
Data including the measurement values?	No
Where is data transmitted?	USA, France, China, UK, Singapore
Permissions	
Which permissions are asked for?	Device & app history, location, photos/media/files, camera, wi-fi connection information, Bluetooth connection information, device ID, android.permission.CHANGE_CONFIGURATION, close other apps, run at startup...
Does the user have to accept all permissions?	Camera, location, storage and phone are automatically turned on. The app functions if you turn them off
Registration and deletion	
Is there an account system?	Yes
Is it necessary to create an account?	Yes
What information is mandatory when creating account?	Full name, gender, date of birth, height, weight, country, e-mail, are you an athlete? level of activity
Does the service require a secure password?	6+ letters, accepts "password"

Log from Fiddler.

(Overview)

Telerik Fiddler Web Debugger				
File Edit Rules Tools View Help GET /book GeoEdge				
Replay X Go Stream Decode Keep: All sessions Any Process Find Save Browse				
#	Result	Protocol	Host	URL
1	200	HTTP	Tunnel to	ios.bugly.qq.com:443
2	200	HTTP	pingma.qq.com	/mstat/report
3	200	HTTP	cgi.connect.qq.com	/qqconnectopen/openapi/policy_conf?format=json&status_version=
4	200	HTTP	fusion.qq.com	/cgi-bin/qconn_share/check_app_limit.cgi?format=json&status_vers
5	200	HTTP	Tunnel to	requestcert.ihealthlabs.eu:443
7	200	HTTP	data.flurry.com	/aas.do
8	200	HTTP	data.flurry.com	/aas.do
9	200	HTTP	Tunnel to	api.ihealthlabs.com:443
10	200	HTTP	Tunnel to	data.mistat.xiaomi.com:443
11	200	HTTPS	requestcert.ihealthlabs.eu	/api5/FirstConnection.asmx/FirstConnection
12	200	HTTPS	api.ihealthlabs.com:443	/api5/productsale_get.htm
13	200	HTTPS	data.mistat.xiaomi.com	/mistats
14	200	HTTPS	ios.bugly.qq.com	/rqd/sync?aid=FA906DEF-DD19-4D9F-932C-ED730B25B7B0
15	200	HTTP	Tunnel to	data.mistat.xiaomi.com:443
16	200	HTTPS	data.mistat.xiaomi.com	/mistats
17	200	HTTP	Tunnel to	api.ihealthlabs.eu:443
18	200	HTTP	Tunnel to	data.mistat.xiaomi.com:443
19	200	HTTPS	data.mistat.xiaomi.com	/mistats
20	200	HTTP	Tunnel to	data.mistat.xiaomi.com:443
21	200	HTTPS	data.mistat.xiaomi.com	/mistats
22	200	HTTP	data.flurry.com	/aas.do
23	200	HTTP	Tunnel to	data.mistat.xiaomi.com:443
24	200	HTTP	pingma.qq.com	/mstat/report
25	200	HTTPS	data.mistat.xiaomi.com	/mistats

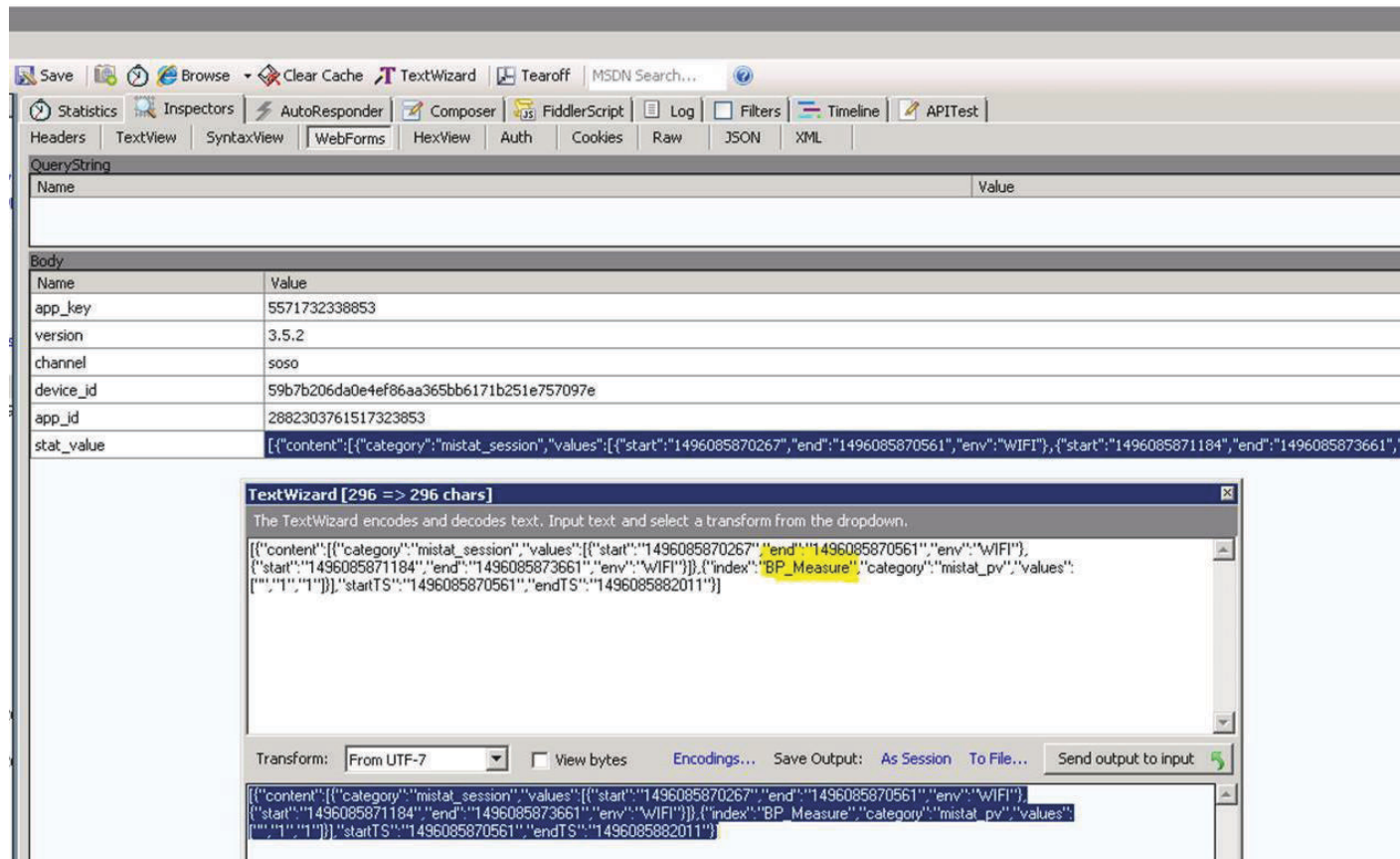
Start App

Measure

Exit App

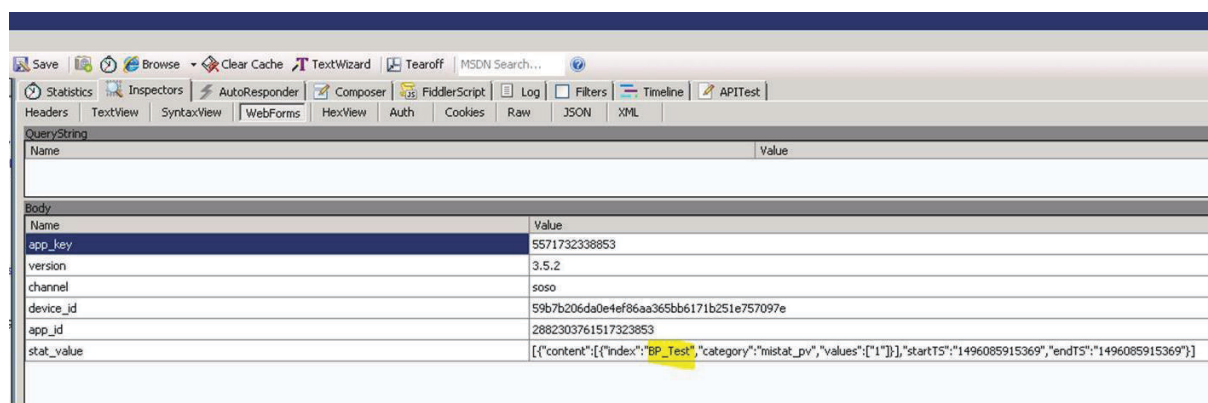
5.3.1 data.mistat.com

#16



It sends **BP_Measure** to dat <https://data.mistat.xiaomi.com/mistats>

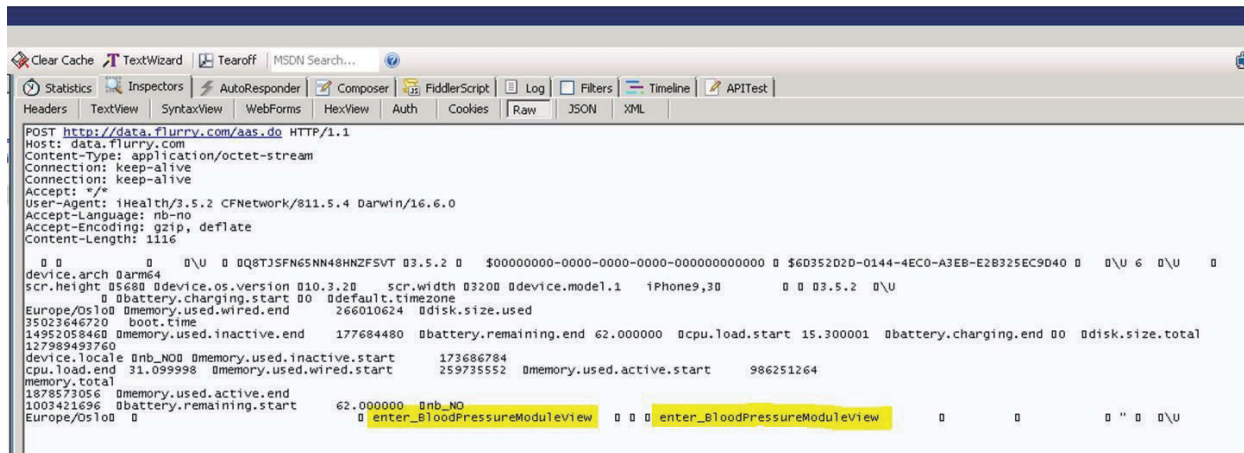
#21



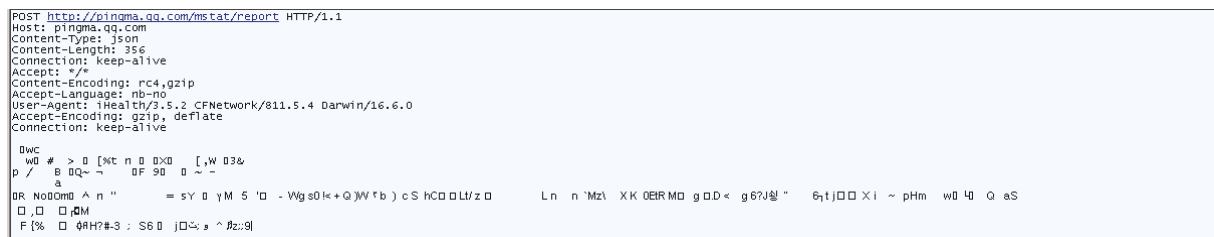
When the messurement takes place **BP_Test** til <https://data.mistat.xiaomi.com/mistats>

5.3.2 data.flurry.com

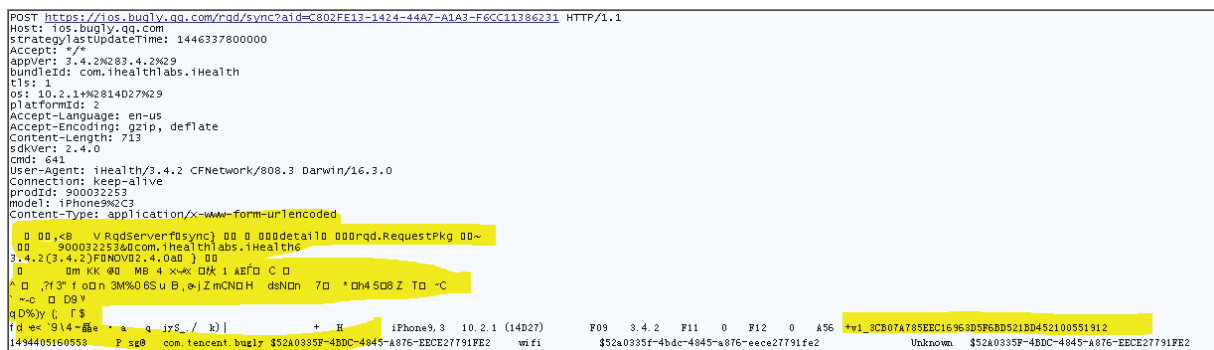
#22



The app sends data to data.flurry.com which reveals that the user enters the screen for of blood pressure measurement.



We have been unable to decode what is transmitted in #24 to <http://pingma.qq.com/mstat/report>



And #14 to <https://ios.bugly.qq.com>

5.3.3 Summary

In the data we are able to decode, there is nothing to indicate that measurement results/values are sent to third parties, but there is little doubt that it tells xiaomi.com, and indirectly* also flurry.com when you are doing a blood pressure measurement.

* The data sent flurry.com is transmitted when user enters the screen to make a measurement, not when he/she actually perform it.

5.4 Withings WPMo2

About the app	
Name of app	Withings Health Mate
Version tested (Android)	2.21
Version tested (iOS)	2.18.3
Security	
Is data encrypted in app?	yes
Is data flow encrypted?	yes
Data collection/Privacy	
Does the service include privacy settings?	No
Do the privacy settings have any actual effect?	n/a
Is data stored locally or in the cloud?	Cloud
Is it possible to opt out of using cloud storage?	No
Is data sent to third parties?	yes
Is there a function to share health data by e-mail?	Yes
Third parties	
What third parties is data sent to?	Amplitude, doubleclick, google
Data that identifies the user?	Not observed
Data that identifies that the user is using the device?	Yes (Amplitude)
Data that identifies when the user is taking measurements?	Yes (Amplitude)
Data including the measurement values?	No
Where is data transmitted?	United States
Permissions	
Which permissions are asked for?	Calendar, Camera, Contacts, Location, Telephone, SMS, Storage, diagnostic information, flashlight and Bluetooth
Does the user have to accept all permissions?	No, they are off by default
Registration and deletion	
Is there an account system?	Yes
Is it necessary to create an account?	Yes
What information is mandatory when creating account?	e-mail, full name, date of birth, height, weight, gender
Does the service require a secure password?	6+ letters, accepts "password"

5.4.1 Amplitude

```

    },
    {
      "session_id": 1494336645831,
      "user_properties": {

      },
      "language": "English",
      "event_type": "[SCREEN] Timeline",
      "sequence_number": 223,
      "user_id": "3069828b8c2cc1fe89964f53f6660f03",
      "country": "Norway",
      "api_properties": {
        "ios_idfv": "E7C39065-E53B-4DF7-9E8B-D185A145CCDE"
      },
      "device_id": "E7C39065-E53B-4DF7-9E8B-D185A145CCDE",
      "event_properties": {
        "previousScreen1": "[SCREEN] bpmaddmeasure",
        "previousEvent2": "[EVENT] manualMeasureMenuOpen",
        "interactions": "Tap (338, 27)",
        "platform": "iOS",
        "scroll": 0,
        "previousScreen2": "[SCREEN] Timeline",
        "previousEvent4": "[SCREEN] Timeline",
        "button": 0,
        "eventName": "[SCREEN] Timeline",
        "isMainUser": "yes",
        "previousEvent1": "[SCREEN] Timeline",
        "timefromLastEvent": 10,
        "orientationChanged": 0,
        "priority": 2,
        "previousScreen3": "[SCREEN] webView",
        "unknownTouch": 0,
        "taggingVersion": 1.4,
        "previousEvent3": "[SCREEN] webView",
        "previousScreen4": "[SCREEN] Timeline",
        "previousEvent0": "[SCREEN] bpmaddmeasure",
        "switch": 0,
        "previousScreen0": "[SCREEN] Timeline",
        "timeViewController": 10,
        "touch": 1
      },
      "uuid": "37726D8D-5307-4C08-B016-D645923AEFC9".
    }
  ]
}

```

Sends a device id and data revealing that the user is doing a blood pressure measurement to Amplitude.

5.4.2 Google-analytics.com

body	
Name	Value
sr	750x1334
cd12	Not determined
cd5	NO
t	screenview
cd3	NO
tid	UA-6686090-30
cd	BloodPressureController2
v	1
_u	.oKo9L
_crc	0
av	2.18.3
cd10	Not determined
ht	1494336739134
qt	32073
z	18343377015955466725%@ dm=iPhone9,3
ea	Use the BPM - Normal Mode
cid	72471d77-ef9e-433c-992f-3d6f307a8601
cd9	NO
_u	.yoL
cd5	NO
cd1	NO
_v	mi3.1.5
a	381305880
cd	BloodPressureController2
sr	750x1334
ec	Use the BPM
cd6	NO

Sends data that is a strong indication that you are doing a blood pressure measurement to google analytics

5.4.3 Summary

The app sends very detailed logs about how the app is used to both google-analytics and amplitude, this includes when the user is doing measurements. We have no indication that actual measurement results were sent to these servers.

5.5 2in1 Smart

About the app	
Name of app	2in1 Smart
Version tested (Android)	2.1
Version tested (iOS)	3.6.0
Security	
Is data encrypted in app?	n/a
Is data flow encrypted?	n/a
Data collection/Privacy	
Does the service include privacy settings?	No
Do the privacy settings have any actual effect?	n/a
Is data stored locally or in the cloud?	Locally
Is it possible to opt out of using cloud storage?	n/a
Is data sent to third parties?	No
Is there a function to share health data by e-mail?	Yes
Third parties	
What third parties is data sent to?	None
Data that identifies the user?	No
Data that identifies that the user is using the device?	No
Data that identifies when the user is taking measurements?	No
Data including the measurement values?	No
Where is data transmitted?	n/a
Permissions	
Which permissions are asked for?	Device & app history, contacts, sms (send and view), photos/media/files, microphone, device id, android.permission.CHANGE_CONFIGURATION, android.permission.SET_DEBUG_APP
Does the user have to accept all permissions?	Everything is on by default, seems to function if turned off
Registration and deletion	
Is there an account system?	No
Is it necessary to create an account?	No
What information is mandatory when creating account?	None
Does the service require a secure password?	n/a

5.5.1 Summary

The app stores data locally rather than in the cloud, and we could not detect that any third party services are used. However, it has an option to export measurements to email which is not a very safe way to transmit medical information.

5.6 Bayer Contour Next One

About the app	
Name of app	Contour Diabetes app (NO)
Version tested (Android)	1.2.55
Version tested (iOS)	1.2.55
Security	
Is data encrypted in app?	Yes
Is data flow encrypted?	Yes
Data collection/Privacy	
Does the service include privacy settings?	Guest mode
Do the privacy settings have any actual effect?	Yes. Data is not transmitted while in visitor mode
Is data stored locally or in the cloud?	
Is it possible to opt out of using cloud storage?	Yes
Is data sent to third parties?	No
Is there a function to share health data by e-mail?	Yes
Third parties	
What third parties is data sent to?	Could not detect any data sent to third parties
Data that identifies the user?	No
Data that identifies that the user is using the device?	No
Data that identifies when the user is taking measurements?	No
Data including the measurement values?	No
Where is data transmitted?	
Permissions	
Which permissions are asked for?	Contacts, location, phone (calls), photos/media/files, camera, wifi, Bluetooth, device id, read Google service configuration, run at startup
Does the user have to accept all permissions?	Everything turned on by default
Registration and deletion	
Is there an account system?	Yes
Is it necessary to create an account?	No, but guest mode disappears after logging in once
What information is mandatory when creating account?	Date of birth, e-mail
Does the service require a secure password?	8+ letters, numbers and letters required

5.6.1 Summary

We could not detect data being sent to third parties, and all communication with contour's cloud server was encrypted and SSL pinned.

5.7 iHealthBG5

About the app	
Name of app	iHealth-Gluco-Smart
Version tested (Android)	4.2.1
Version tested (iOS)	4.1.1
Security	
Is data encrypted in app?	Yes
Is data flow encrypted?	Yes
Data collection/Privacy	
Does the service include privacy settings?	No
Do the privacy settings have any actual effect?	n/a
Is data stored locally or in the cloud?	Cloud
Is it possible to opt out of using cloud storage?	No
Is data sent to third parties?	Yes. The iOS-version sends data to a lot of trackers. The Android version doesn't.
Is there a function to share health data by e-mail?	Yes
Third parties	
What third parties is data sent to?	DoubleClick, adfarm, ehealthcaresolutions, krux, etc (iOS version, integrated through http://www.diabetesforecast.org)
Data that identifies the user?	Not determined
Data that identifies that the user is using the device?	Indirectly in IOS version by launching website in app
Data that identifies when the user is taking measurements?	No
Data including the measurement values?	No
Where is data transmitted?	Not determined (built in dynamic website)
Permissions	
Which permissions are asked for?	Camera. Contacts, location, microphone, storage, flashlight, Bluetooth settings, retrieve running apps, change network connectivity, change audio settings...
Does the user have to accept all permissions?	Everything off by default. Asks for permission to storage when logging in
Registration and deletion	
Is there an account system?	Yes, same account as iHealth MyVitals
Is it necessary to create an account?	Yes
What information is mandatory when creating account?	Name, e-mail
Does the service require a secure password?	6+ letters, accepts "password"

5.7.1 Built in web view


The IOS version of this app has a built in web-view that automatically opens diabetesforecast.org inside the app. This site includes a lot of ad trackers including facebook, googletagservices, dubleclick witch among other things are designed to track the user across multiple sites. This can potentially reveal your medical condition to a lot of advertisement networks.

6 Location of servers

The physical location of third party servers was obtained from <https://www.iplocation.net/> 06.07.2017


6.1 api.ihealthlabs.com

Geolocation data from ipinfo.io (Product: API, real-time)


Domain Name	Country	Region	City
api.ihealthlabs.com	United States 	California	San Jose
ISP	Organization	Latitude	Longitude
Amazon.com, Inc.	Amazon.com, Inc.	37.3388	-121.8914

6.2 api.ihealthlabs.eu

Geolocation data from ipinfo.io (Product: API, real-time)


Domain Name	Country	Region	City
api.ihealthlabs.eu	France 	Not Available	Not Available
ISP	Organization	Latitude	Longitude
INFORMATIQUE DE SECURITE (IDS), SAS	INFORMATIQUE DE SECURITE (IDS)	48.8582	2.3387

6.3 ios.bugly.qq.com

Domain Name	Country	Region	City
ios.bugly.qq.com	China 	Beijing	Beijing
ISP	Organization	Latitude	Longitude
Tencent Building, Kejizhongyi Avenue	Shenzhen Tencent Computer Systems Company Limited	39.9289	116.3883

6.4 pingma.qq.com

Geolocation data from [EurekAPI](#) (Product: API, real-time)

Domain Name	Country	Region	City
pingma.qq.com	China 	Guangdong	Shenzhen
ISP	Organization	Latitude	Longitude
Tencent cloud computing	Tencent Building, Kejizhongyi Avenue	22.5333	114.1333


6.5 xiaomi.com

Geolocation data from [ipinfo.io](#) (Product: API, real-time)

Domain Name	Country	Region	City
xiaomi.com	China 	Beijing	Beijing
ISP	Organization	Latitude	Longitude
China Telecom (Group)	21ViaNet(China),Inc.	39.9289	116.3883


6.6 flurry.com

Geolocation data from [ipinfo.io](#) (Product: API, real-time)

Domain Name	Country	Region	City
flurry.com	United Kingdom 	Not Available	Not Available
ISP	Organization	Latitude	Longitude
Yahoo! UK Services Limited	Yahoo! Europe	51.4964	-0.1224


6.7 data.flurry.com

Geolocation data from [ipinfo.io](#) (Product: API, real-time)

Domain Name	Country	Region	City
data.flurry.com	United States 	California	Sunnyvale
ISP	Organization	Latitude	Longitude
Yahoo	Inktomi Corporation	37.4249	-122.0074


6.8 api.segment.io

Geolocation data from [ipinfo.io](#) (Product: API, real-time)

Domain Name	Country	Region	City
API.SEGMENT.IO	United States 	Oregon	Boardman
ISP	Organization	Latitude	Longitude
Amazon.com, Inc.	Amazon Technologies Inc.	45.8696	-119.6880


6.9 api.mixpanel.com

Geolocation data from [ipinfo.io](#) (Product: API, real-time)


Domain Name	Country	Region	City
api.mixpanel.com	United States 	Not Available	Not Available
ISP	Organization	Latitude	Longitude
SoftLayer Technologies Inc.	Mixpanel, Inc.	37.7510	-97.8220

6.10 fusion.qq.com

Geolocation data from [ipinfo.io](#) (Product: API, real-time)


Domain Name	Country	Region	City
fusion.qq.com	China 	Guangdong	Shenzhen
ISP	Organization	Latitude	Longitude
Tencent Building, Kejizhongyi Avenue	Shenzhen Tencent Computer Systems Company Limited	22.5333	114.1333

Geolocation data from ipinfo.io (Product: API, real-time)

Domain Name	Country	Region	City
api.amplitude.com	United States 	Oregon	Boardman
ISP	Organization	Latitude	Longitude
Amazon.com, Inc.	Amazon.com, Inc.	45.8696	-119.6880

6.11 data.mistat.xiaomi.com


Geolocation data from ipinfo.io (Product: API, real-time)

Domain Name	Country	Region	City
data.mistat.xiaomi.com	Singapore 	Central Singapore Community Development Council	Singapore
ISP	Organization	Latitude	Longitude
Amazon.com, Inc.	Amazon Technologies Inc.	1.2855	103.8565

6.12 api.amplitude.com

Location of servers was obtained from <https://www.iplocation.net/> 06.07.2017

Geolocation data from ipinfo.io (Product: API, real-time)

Domain Name	Country	Region	City
api.amplitude.com	United States 	Oregon	Boardman
ISP	Organization	Latitude	Longitude
Amazon.com, Inc.	Amazon.com, Inc.	45.8696	-119.6880