Security Vulnerabilities in Networked E-Health Devices

Ratinder Kaur, Hugo Gonzalez, Ghazale Amel Zendehdel, Alina Matyukhina, Natalia Stakhanova

Canadian Institute for Cybersecurity (CIC), University of New Brunswick (UNB)

CIC

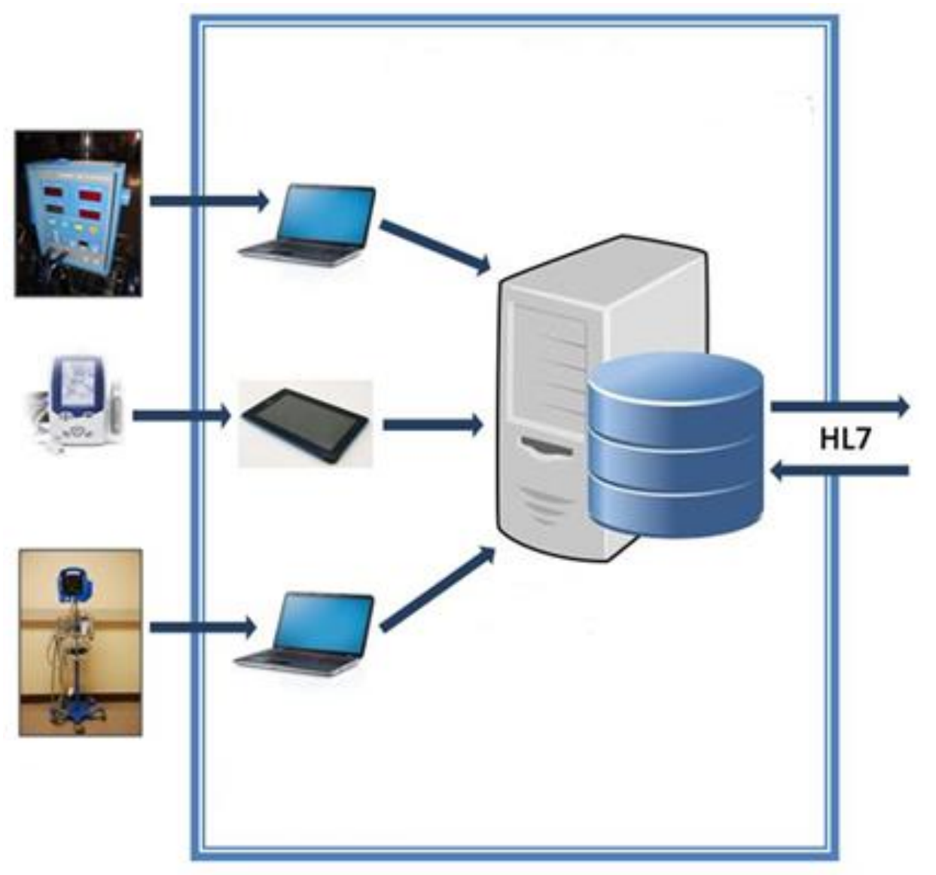
UNB

Abstract

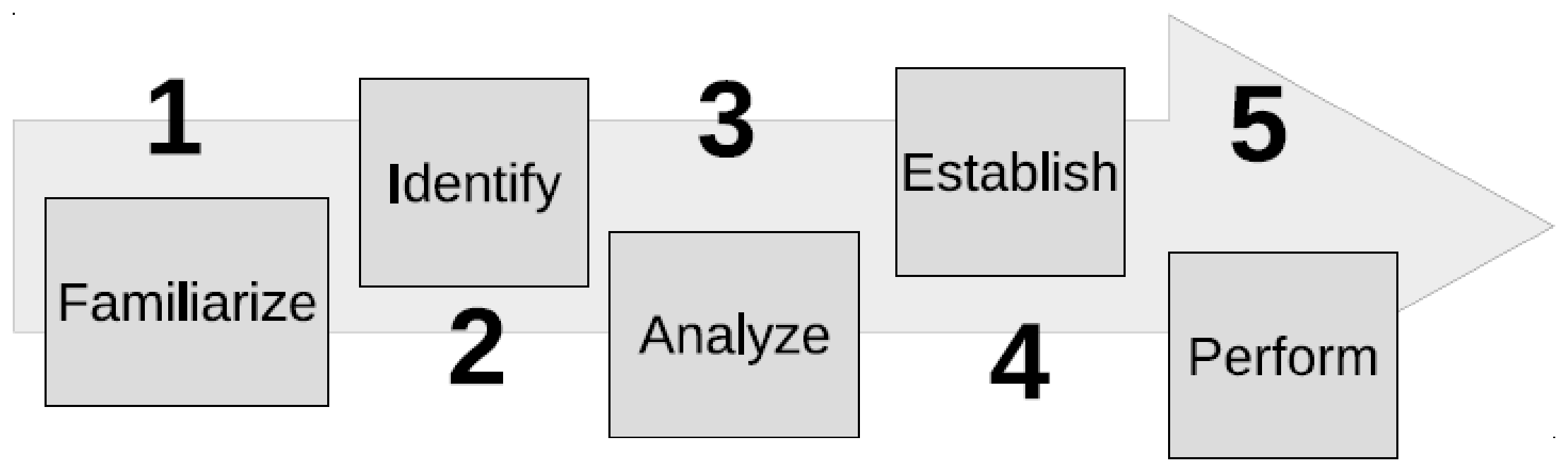
Poor design and implementation of security in e-health devices leaves patient and their data vulnerable to different threats. These vulnerable devices can expose the entire digital healthcare infrastructure where they belong to the same security threats. Further, the defences of e-health devices and the entire healthcare network are not fully developed nor accomplished. With the motivation to protect patient's personal information and sensitive e-health data, in this work we performed in-depth security analysis of some well-known e-health devices. We also proposed an attack methodology to assess the security of any networked e-health device in general. As a case study we assessed the security of a CloudDX Pulsewave Monitor, Athos Wearable Fitness Apparel, Withings Wireless Blood Pressure Monitor.

Networked E-health Devices

- Any e-health device that has capability of connecting to the Internet.
- Collects data from the sensors, converts into digital format, display results and / or transmits data directly or indirectly to the server.
- Vulnerable Software components include - Web server, database server, application running on e-health devices and servers, communication links (USB, Bluetooth, Wireless).

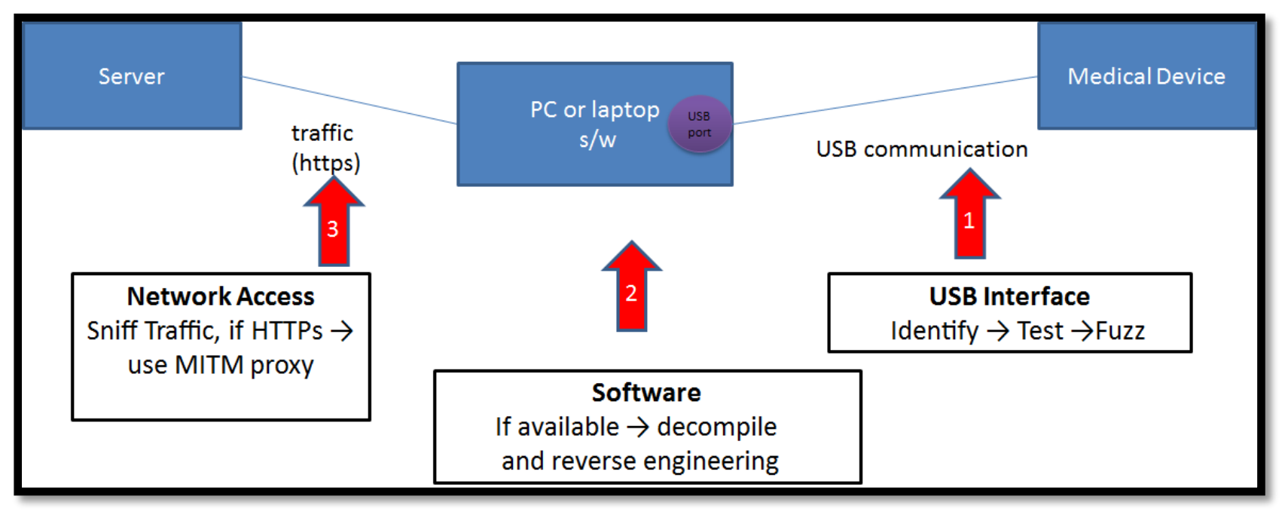


Attack Methodology

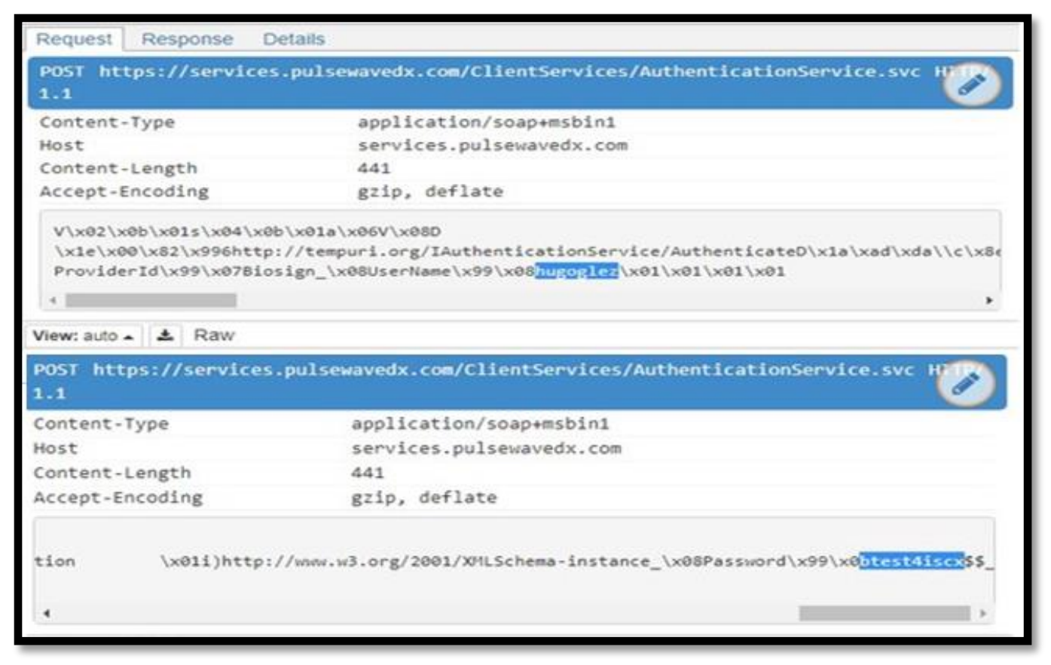


1. Familiarize on how the device works.
2. Identify software components and type of communication links.
3. Analyze potential attack surfaces.
4. Establish a test environment and define attack scenarios
5. Perform the security testing

CloudDX Pulsewave Monitor



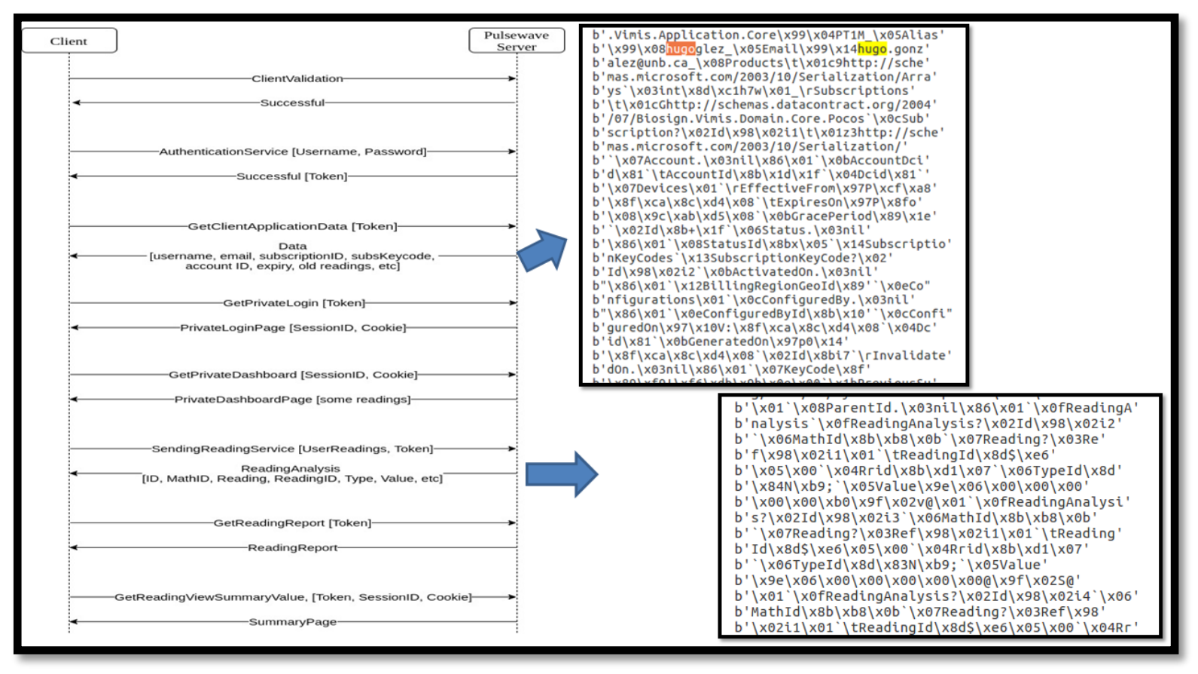
(a) Attack surfaces identified



```
POST https://services.pulsewavedx.com/ClientServices/AuthenticationService.svc HTTP/
1.1
Content-Type            application/soap+msbin1
Host                    services.pulsewavedx.com
Content-Length          441
Accept-Encoding         gzip, deflate

V\x02\x0b\x01s\x04\x0b\x01a\x06V\x08D
\x1e\x00\x82\x996http://tempuri.org/IAuthenticationService/AuthenticateD\x1a\xad\xda\\c\x8
ProviderId\x99\x07Biosign_\x08UserName\x99\x08hugoglez\x01\x01\x01\x01

POST https://services.pulsewavedx.com/ClientServices/AuthenticationService.svc HTTP/
1.1
Content-Type            application/soap+msbin1
Host                    services.pulsewavedx.com
Content-Length          441
Accept-Encoding         gzip, deflate

tion        \x01i)http://www.w3.org/2001/XMLSchema-instance_\x08Password\x99\x0btest4iscx$$_
```

(c) Man-in-the-middle attack leaks login credential login

(b) Controlling device with custom code


Client
Pulsewave Server
ClientValidation
Successful
AuthenticationService [Username, Password]
Successful [Token]
GetClientApplicationData [Token]
Data [username, email, subscriptionID, subsKeycode, account ID, expiry, old readings, etc]
GetPrivateLogin [Token]
PrivateLoginPage [SessionID, Cookie]
GetPrivateDashboard [SessionID, Cookie]
PrivateDashboardPage [some readings]
SendingReadingService [UserReadings, Token]
ReadingAnalysis [ID, MathID, Reading, ReadingID, Type, Value, etc]
GetReadingReport [Token]
ReadingReport
GetReadingViewSummaryValue, [Token, SessionID, Cookie]
SummaryPage

```
b'.Vimis.Application.Core\x99\x04PT1M_\x05Alias'
b'\x99\x08hugoglez_\x05Email\x99\x14hugo.gonz'
b'alez@unb.ca_\x08Products\t\x01c9http://sche'
b'mas.microsoft.com/2003/10/Serialization/Arra'
b'ys`\x03int\x8d\xc1h7w\x01_\rSubscriptions'
b'\t\x01cGhttp://schemas.datacontract.org/2004'
b'/07/Biosign.Vimis.Domain.Core.Pocos`\x0cSub'
b'scription?\x02Id\x98\x02i1\t\x01z3http://sche'
b'mas.microsoft.com/2003/10/Serialization/'
b'`\x07Account.\x03nil\x86\x01`\x0bAccountDci'
b'd\x81`\tAccountId\x8b\x1d\x1f`\x04Dcid\x81``'
b'\x07Devices\x01`\rEffectiveFrom\x97P\xcf\xa8'
b'\x8f\xca\x8c\xd4\x08`\tExpiresOn\x97P\x8fo'
b'\x08\x9c\xab\xd5\x08`\x0bGracePeriod\x89\x1e'
b'`\x02Id\x8b+\x1f`\x06Status.\x03nil'
b'\x86\x01`\x08StatusId\x8bx\x05`\x14Subscriptio'
b'nKeyCodes`\x13SubscriptionKeyCode?\x02'
b'Id\x98\x02i2`\x0bActivatedOn.\x03nil'
b"\x86\x01`\x12BillingRegionGeoId\x89'`\x0eCo"
b'nfigurations\x01`\x0cConfiguredBy.\x03nil'
b"\x86\x01`\x0eConfiguredById\x8b\x10'`\x0cConfi"
b'guredOn\x97\x10V:\x8f\xca\x8c\xd4\x08`\x04Dc'
b'id\x81`\x0bGeneratedOn\x97p0\x14'
b'\x8f\xca\x8c\xd4\x08`\x02Id\x8bi7`\rInvalidate'
b'dOn.\x03nil\x86\x01`\x07KeyCode\x8f'
```

```
b'\x01`\x08ParentId.\x03nil\x86\x01`\x0fReadingA'
b'nalysis`\x0fReadingAnalysis?\x02Id\x98\x02i2'
b'`\x06MathId\x8b\xb8\x0b`\x07Reading?\x03Re'
b'f\x98\x02i1\x01`\tReadingId\x8d$\xe6'
b'\x05\x00`\x04Rrid\x8b\xd1\x07`\x06TypeId\x8d'
b'\x84N\xb9;`\x05Value\x9e\x06\x00\x00\x00'
b'\x00\x00\xb0\x9f\x02v@\x01`\x0fReadingAnalysi'
b's?\x02Id\x98\x02i3`\x06MathId\x8b\xb8\x0b'
b'`\x07Reading?\x03Ref\x98\x02i1\x01`\tReading'
b'Id\x8d$\xe6\x05\x00`\x04Rrid\x8b\xd1\x07'
b'`\x06TypeId\x8d\x83N\xb9;`\x05Value'
b'\x9e\x06\x00\x00\x00\x00\x00@\x9f\x02S@'
b'\x01`\x0fReadingAnalysis?\x02Id\x98\x02i4`\x06'
b'MathId\x8b\xb8\x0b`\x07Reading?\x03Ref\x98'
b'\x02i1\x01`\tReadingId\x8d$\xe6\x05\x00`\x04Rr'
```

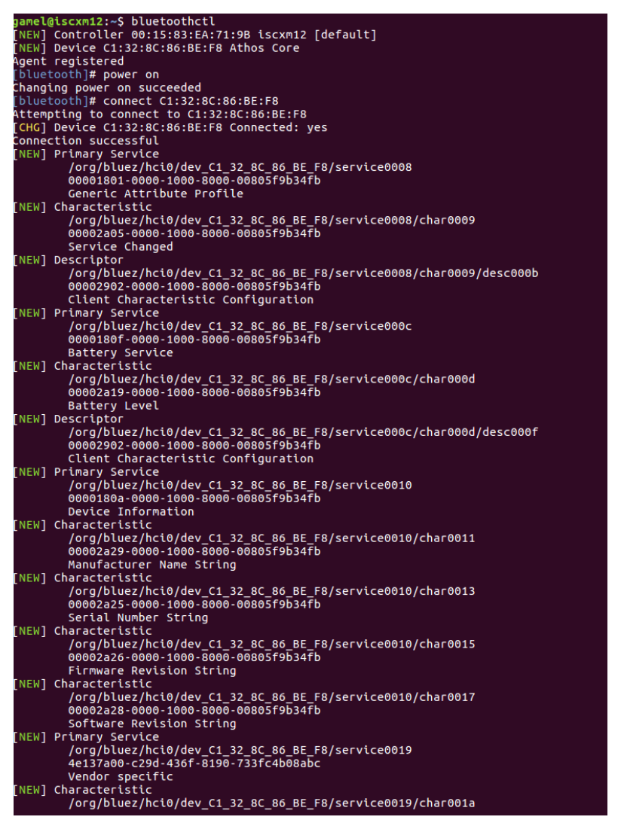
(d) Leaked readings in the network flow

Withings BPM

- Pre-static analysis of Withings BPM's mobile app:
  - App seems obfuscated with Dexguard
  - Some of the plist files are encrypted
  - Insecure Http urls
  - Found hardcoded key used for certificate pinning
  - Third party integrations also use hardcoded keys to connect to the server.

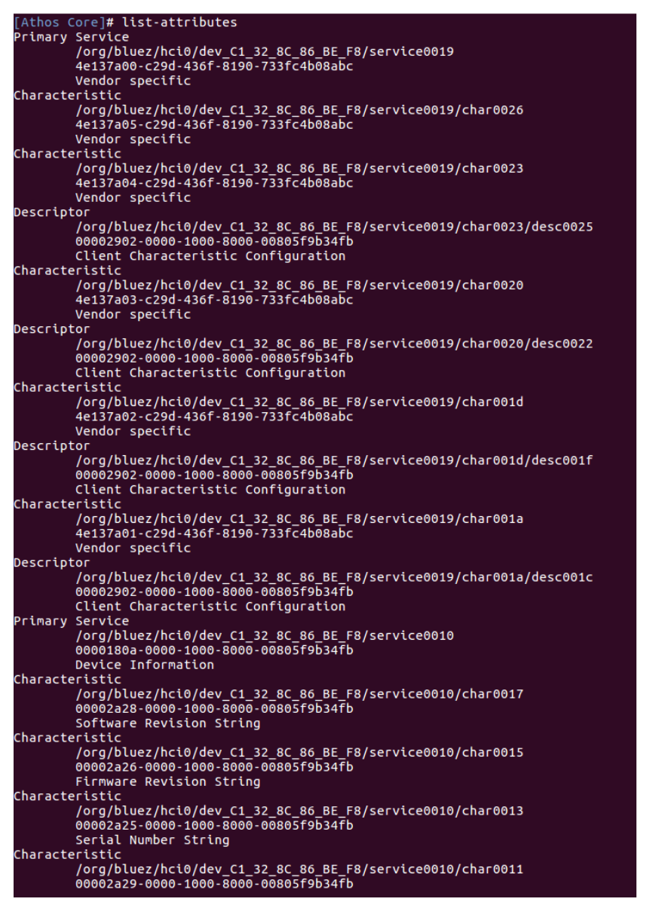
Athos Apparel

(a) Working of Athos Apparel



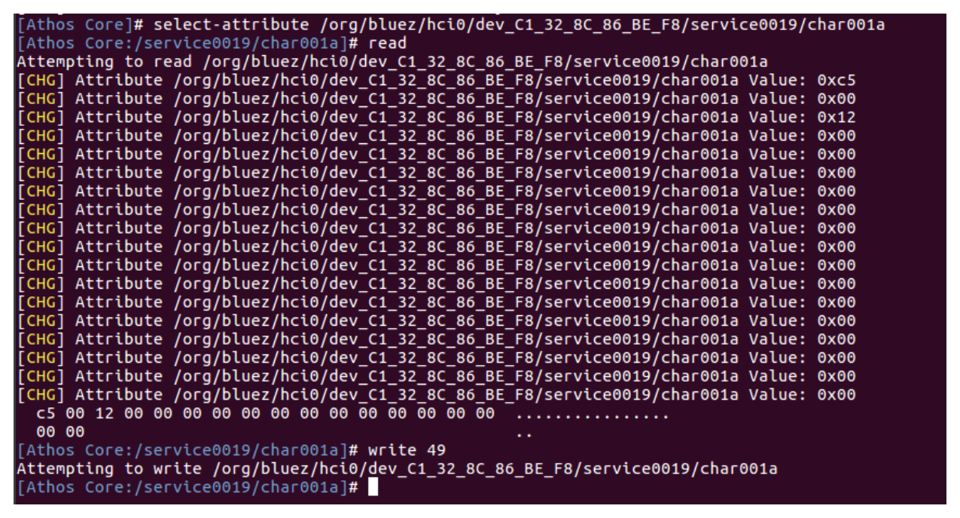
```
gamel@iscxm12:~$ bluetoothctl
[NEW] Controller 00:15:83:EA:71:9B iscxm12 [default]
[NEW] Device C1:32:8C:86:BE:F8 Athos Core
Agent registered
[bluetooth]# power on
Changing power on succeeded
[bluetooth]# connect C1:32:8C:86:BE:F8
Attempting to connect to C1:32:8C:86:BE:F8
[CHG] Device C1:32:8C:86:BE:F8 Connected: yes
Connection successful
[NEW] Primary Service
        /org/bluez/hci0/dev_C1_32_8C_86_BE_F8/service0008
        00001801-0000-1000-8000-00805f9b34fb
        Generic Attribute Profile
[NEW] Characteristic
        /org/bluez/hci0/dev_C1_32_8C_86_BE_F8/service0008/char0009
        00002a05-0000-1000-8000-00805f9b34fb
        Service Changed
[NEW] Descriptor
        /org/bluez/hci0/dev_C1_32_8C_86_BE_F8/service0008/char0009/desc000b
        00002902-0000-1000-8000-00805f9b34fb
        Client Characteristic Configuration
[NEW] Primary Service
        /org/bluez/hci0/dev_C1_32_8C_86_BE_F8/service000c
        0000180f-0000-1000-8000-00805f9b34fb
        Battery Service
[NEW] Characteristic
        /org/bluez/hci0/dev_C1_32_8C_86_BE_F8/service000c/char000d
        00002a19-0000-1000-8000-00805f9b34fb
        Battery Level
[NEW] Descriptor
        /org/bluez/hci0/dev_C1_32_8C_86_BE_F8/service000c/char000d/desc000f
        00002902-0000-1000-8000-00805f9b34fb
        Client Characteristic Configuration
[NEW] Primary Service
        /org/bluez/hci0/dev_C1_32_8C_86_BE_F8/service0010
        0000180a-0000-1000-8000-00805f9b34fb
        Device Information
[NEW] Characteristic
        /org/bluez/hci0/dev_C1_32_8C_86_BE_F8/service0010/char0011
        00002a29-0000-1000-8000-00805f9b34fb
        Manufacturer Name String
[NEW] Characteristic
        /org/bluez/hci0/dev_C1_32_8C_86_BE_F8/service0010/char0013
        00002a25-0000-1000-8000-00805f9b34fb
        Serial Number String
[NEW] Characteristic
        /org/bluez/hci0/dev_C1_32_8C_86_BE_F8/service0010/char0015
        00002a26-0000-1000-8000-00805f9b34fb
        Firmware Revision String
[NEW] Characteristic
        /org/bluez/hci0/dev_C1_32_8C_86_BE_F8/service0010/char0017
        00002a28-0000-1000-8000-00805f9b34fb
        Software Revision String
[NEW] Primary Service
        /org/bluez/hci0/dev_C1_32_8C_86_BE_F8/service0019
        4e137a00-c29d-436f-8190-733fc4b08abc
        Vendor specific
[NEW] Characteristic
        /org/bluez/hci0/dev_C1_32_8C_86_BE_F8/service0019/char001a
```

(a) Connecting to athos core



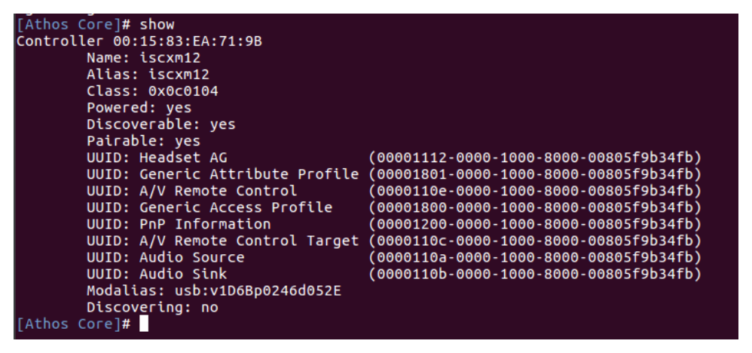
```
[Athos Core]# list-attributes
Primary Service
        /org/bluez/hci0/dev_C1_32_8C_86_BE_F8/service0019
        4e137a00-c29d-436f-8190-733fc4b08abc
        Vendor specific
Characteristic
        /org/bluez/hci0/dev_C1_32_8C_86_BE_F8/service0019/char0026
        4e137a05-c29d-436f-8190-733fc4b08abc
        Vendor specific
Characteristic
        /org/bluez/hci0/dev_C1_32_8C_86_BE_F8/service0019/char0023
        4e137a04-c29d-436f-8190-733fc4b08abc
        Vendor specific
Descriptor
        /org/bluez/hci0/dev_C1_32_8C_86_BE_F8/service0019/char0023/desc0025
        00002902-0000-1000-8000-00805f9b34fb
        Client Characteristic Configuration
Characteristic
        /org/bluez/hci0/dev_C1_32_8C_86_BE_F8/service0019/char0020
        4e137a03-c29d-436f-8190-733fc4b08abc
        Vendor specific
Descriptor
        /org/bluez/hci0/dev_C1_32_8C_86_BE_F8/service0019/char0020/desc0022
        00002902-0000-1000-8000-00805f9b34fb
        Client Characteristic Configuration
Characteristic
        /org/bluez/hci0/dev_C1_32_8C_86_BE_F8/service0019/char001d
        4e137a02-c29d-436f-8190-733fc4b08abc
        Vendor specific
Descriptor
        /org/bluez/hci0/dev_C1_32_8C_86_BE_F8/service0019/char001d/desc001f
        00002902-0000-1000-8000-00805f9b34fb
        Client Characteristic Configuration
Characteristic
        /org/bluez/hci0/dev_C1_32_8C_86_BE_F8/service0019/char001a
        4e137a01-c29d-436f-8190-733fc4b08abc
        Vendor specific
Descriptor
        /org/bluez/hci0/dev_C1_32_8C_86_BE_F8/service0019/char001a/desc001c
        00002902-0000-1000-8000-00805f9b34fb
        Client Characteristic Configuration
Primary Service
        /org/bluez/hci0/dev_C1_32_8C_86_BE_F8/service0010
        0000180a-0000-1000-8000-00805f9b34fb
        Device Information
Characteristic
        /org/bluez/hci0/dev_C1_32_8C_86_BE_F8/service0010/char0017
        00002a28-0000-1000-8000-00805f9b34fb
        Software Revision String
Characteristic
        /org/bluez/hci0/dev_C1_32_8C_86_BE_F8/service0010/char0015
        00002a26-0000-1000-8000-00805f9b34fb
        Firmware Revision String
Characteristic
        /org/bluez/hci0/dev_C1_32_8C_86_BE_F8/service0010/char0013
        00002a25-0000-1000-8000-00805f9b34fb
        Serial Number String
Characteristic
        /org/bluez/hci0/dev_C1_32_8C_86_BE_F8/service0010/char0011
        00002a29-0000-1000-8000-00805f9b34fb
```

(c) Listing of Attributes



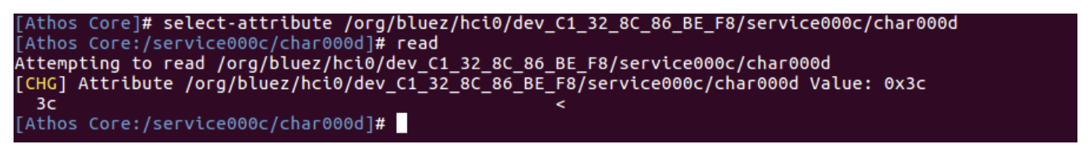
```
[Athos Core]# select-attribute /org/bluez/hci0/dev_C1_32_8C_86_BE_F8/service0019/char001a
[Athos Core:/service0019/char001a]# read
Attempting to read /org/bluez/hci0/dev_C1_32_8C_86_BE_F8/service0019/char001a
[CHG] Attribute /org/bluez/hci0/dev_C1_32_8C_86_BE_F8/service0019/char001a Value: 0xc5
[CHG] Attribute /org/bluez/hci0/dev_C1_32_8C_86_BE_F8/service0019/char001a Value: 0x00
[CHG] Attribute /org/bluez/hci0/dev_C1_32_8C_86_BE_F8/service0019/char001a Value: 0x12
[CHG] Attribute /org/bluez/hci0/dev_C1_32_8C_86_BE_F8/service0019/char001a Value: 0x00
[CHG] Attribute /org/bluez/hci0/dev_C1_32_8C_86_BE_F8/service0019/char001a Value: 0x00
[CHG] Attribute /org/bluez/hci0/dev_C1_32_8C_86_BE_F8/service0019/char001a Value: 0x00
[CHG] Attribute /org/bluez/hci0/dev_C1_32_8C_86_BE_F8/service0019/char001a Value: 0x00
[CHG] Attribute /org/bluez/hci0/dev_C1_32_8C_86_BE_F8/service0019/char001a Value: 0x00
[CHG] Attribute /org/bluez/hci0/dev_C1_32_8C_86_BE_F8/service0019/char001a Value: 0x00
[CHG] Attribute /org/bluez/hci0/dev_C1_32_8C_86_BE_F8/service0019/char001a Value: 0x00
[CHG] Attribute /org/bluez/hci0/dev_C1_32_8C_86_BE_F8/service0019/char001a Value: 0x00
[CHG] Attribute /org/bluez/hci0/dev_C1_32_8C_86_BE_F8/service0019/char001a Value: 0x00
[CHG] Attribute /org/bluez/hci0/dev_C1_32_8C_86_BE_F8/service0019/char001a Value: 0x00
[CHG] Attribute /org/bluez/hci0/dev_C1_32_8C_86_BE_F8/service0019/char001a Value: 0x00
[CHG] Attribute /org/bluez/hci0/dev_C1_32_8C_86_BE_F8/service0019/char001a Value: 0x00
[CHG] Attribute /org/bluez/hci0/dev_C1_32_8C_86_BE_F8/service0019/char001a Value: 0x00
[CHG] Attribute /org/bluez/hci0/dev_C1_32_8C_86_BE_F8/service0019/char001a Value: 0x00
[CHG] Attribute /org/bluez/hci0/dev_C1_32_8C_86_BE_F8/service0019/char001a Value: 0x00
  c5 00 12 00 00 00 00 00 00 00 00 00 00 00 00 00  ................
  00 00                                            ..
[Athos Core:/service0019/char001a]# write 49
Attempting to write /org/bluez/hci0/dev_C1_32_8C_86_BE_F8/service0019/char001a
[Athos Core:/service0019/char001a]#
```

(e) Writing random value to core



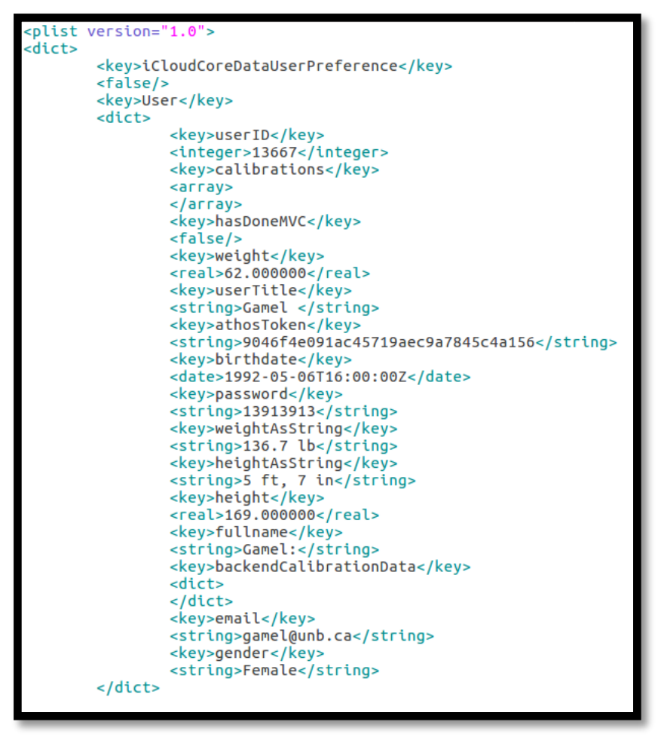
```
[Athos Core]# show
Controller 00:15:83:EA:71:9B
        Name: iscxm12
        Alias: iscxm12
        Class: 0x0c0104
        Powered: yes
        Discoverable: yes
        Pairable: yes
        UUID: Headset AG                (00001112-0000-1000-8000-00805f9b34fb)
        UUID: Generic Attribute Profile (00001801-0000-1000-8000-00805f9b34fb)
        UUID: A/V Remote Control        (0000110e-0000-1000-8000-00805f9b34fb)
        UUID: Generic Access Profile    (00001800-0000-1000-8000-00805f9b34fb)
        UUID: PnP Information           (00001200-0000-1000-8000-00805f9b34fb)
        UUID: A/V Remote Control Target (0000110c-0000-1000-8000-00805f9b34fb)
        UUID: Audio Source              (0000110a-0000-1000-8000-00805f9b34fb)
        UUID: Audio Sink                (0000110b-0000-1000-8000-00805f9b34fb)
        Modalias: usb:v1D6Bp0246d052E
        Discovering: no
[Athos Core]#
```

(b) Leaked athos information



```
[Athos Core]# select-attribute /org/bluez/hci0/dev_C1_32_8C_86_BE_F8/service000c/char000d
[Athos Core:/service000c/char000d]# read
Attempting to read /org/bluez/hci0/dev_C1_32_8C_86_BE_F8/service000c/char000d
[CHG] Attribute /org/bluez/hci0/dev_C1_32_8C_86_BE_F8/service000c/char000d Value: 0x3c
  3c                                               <
[Athos Core:/service000c/char000d]#
```

(d) Reading battery information



```
<plist version="1.0">
<dict>
        <key>iCloudCoreDataUserPreference</key>
        <false/>
        <key>User</key>
        <dict>
                <key>userID</key>
                <integer>13667</integer>
                <key>calibrations</key>
                <array>
                </array>
                <key>hasDoneMVC</key>
                <false/>
                <key>weight</key>
                <real>62.000000</real>
                <key>userTitle</key>
                <string>Gamel </string>
                <key>athosToken</key>
                <string>9046f4e091ac45719aec9a7845c4a156</string>
                <key>birthdate</key>
                <date>1992-05-06T16:00:00Z</date>
                <key>password</key>
                <string>13913913</string>
                <key>weightAsString</key>
                <string>136.7 lb</string>
                <key>heightAsString</key>
                <string>5 ft, 7 in</string>
                <key>height</key>
                <real>169.000000</real>
                <key>fullname</key>
                <string>Gamel:</string>
                <key>backendCalibrationData</key>
                <dict>
                </dict>
                <key>email</key>
                <string>gamel@unb.ca</string>
                <key>gender</key>
                <string>Female</string>
        </dict>
```

(f) Data leak in plist

Conclusions and Future Work:

- The findings confirm that the tested devices are not developed with sufficient security in mind.
- Future works involves:
  - Thorough testing of mobile apps that are provided with e-health devices.
  - Designing automatic security assessment framework to test e-health devices.