Forensic investigation of Chinese smartwatches

Renee Witsenburg & Kasper van Brakel

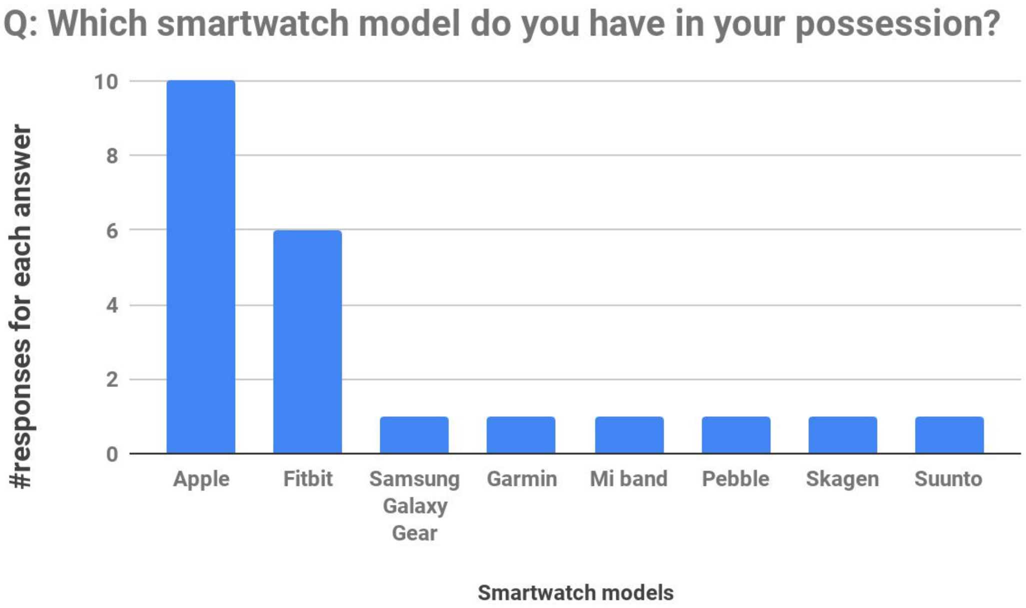
A smartwatch is a wristband with sensors. Sensor information from the wristband is send to a mobile telephone. Furthermore, notifications from the mobile telephone are sent to the wristband.

Research questions

When smartwatches are used in a business organisation environment, what potential information leakage risks are encountered?

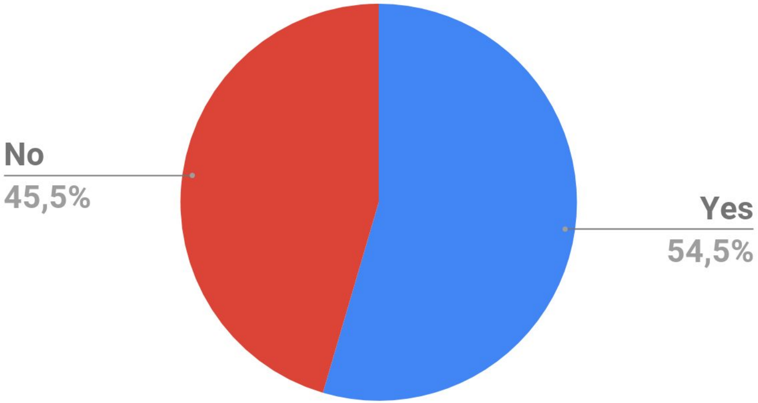
- For which purposes are smartwatches used in a business environment?
- Which connections can be made with the smartwatch?
- Which security measures are in place?
- Which data is stored on the smartwatch?
- Is it possible to tamper with, read or intercept this data?

Smartwatches in a business environment

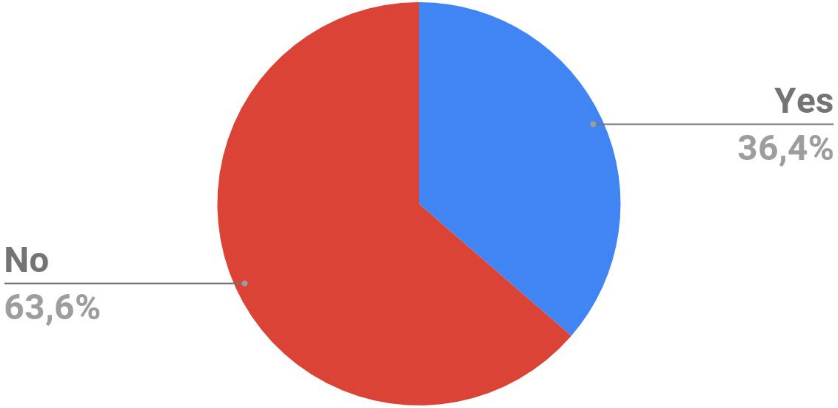


Smartwatches in a business environment (1)

Q: Do you have a pincode on your watch?



Q: Have you taken any precautions in case you lose your smartwatch or when it gets stolen?



Watches

Amazfit Bip

Kingwear KW18

Lemfo LEM8

Attack scenarios

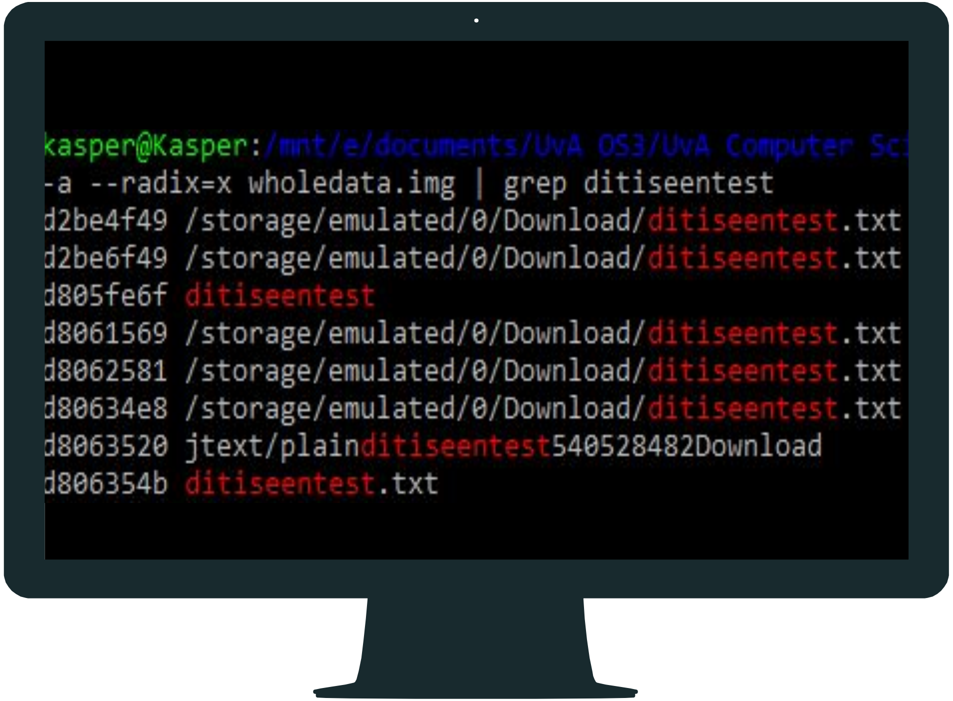
Lost or theft

USB

Bluetooth

Results

- Basic data retrieval and encryption test



```
kasper@Kasper:/mnt/e/documents/UvA OS3/UvA Computer Sci
-a --radix=x wholedata.img | grep ditiseentest
d2be4f49 /storage/emulated/0/Download/ditiseentest.txt
d2be6f49 /storage/emulated/0/Download/ditiseentest.txt
d805fe6f ditiseentest
d8061569 /storage/emulated/0/Download/ditiseentest.txt
d8062581 /storage/emulated/0/Download/ditiseentest.txt
d80634e8 /storage/emulated/0/Download/ditiseentest.txt
d8063520 jtext/plainditiseentest540528482Download
d806354b ditiseentest.txt
```

Results

Major	Device
259	blkext
7	loop
134	sd
135	sd
179	mmc
253	device-mapper
254	zram

Partial output of /proc/devices

Major	Minor	Name	#Blocks
179	0	mmcblk0	15267840
179	1	mmcblk0p1	1024
179	2	mmcblk0p2	24576
179	3	mmcblk0p3	512
179	4	mmcblk0p4	20480
179	31	mmcblk0p31	11859951

Partial output of /proc/partitions

Name	Path
Whole disk	mmcblk0
boot_para	mmcblk0p1
recovery	mmcblk0p2
para	mmcblk0p3
expdb	mmcblk0p4
userdata	mmcblk0p31

Partial output ls -la /dev/block/platform/*/by-name

Results

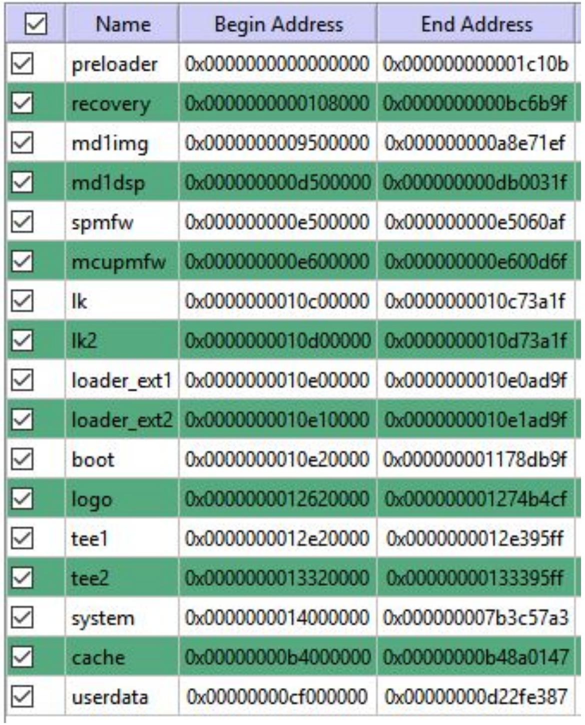
Composing the scatter-file

Major	Minor	#Blocks	Device	Name	Start addr	Length
179	1	1024	mmclk0p1	boot_para	8000	100000
179	2	24576	mmclk0p2	expd	1800000	108000
179	3	512	mmclk0p3	para	1908000	80000
179	31	11859951	mmclk0p31	userdata	2D3DFBC00	CF000000

Results

- Filling in the values in Flash tool

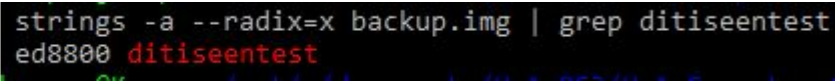
- Ext4 partitions



☑	Name	Begin Address	End Address
☑	preloader	0x0000000000000000	0x000000000001c10b
☑	recovery	0x0000000000108000	0x0000000000bc6b9f
☑	md1img	0x0000000009500000	0x000000000a8e71ef
☑	md1dsp	0x000000000d500000	0x000000000db0031f
☑	spmfw	0x000000000e500000	0x000000000e5060af
☑	mcupmfw	0x000000000e600000	0x000000000e600d6f
☑	lk	0x0000000010c00000	0x0000000010c73a1f
☑	lk2	0x0000000010d00000	0x0000000010d73a1f
☑	loader_ext1	0x0000000010e00000	0x0000000010e0ad9f
☑	loader_ext2	0x0000000010e10000	0x0000000010e1ad9f
☑	boot	0x0000000010e20000	0x000000001178db9f
☑	logo	0x0000000012620000	0x000000001274b4cf
☑	tee1	0x0000000012e20000	0x0000000012e395ff
☑	tee2	0x0000000013320000	0x00000000133395ff
☑	system	0x0000000014000000	0x000000007b3c57a3
☑	cache	0x00000000b4000000	0x00000000b48a0147
☑	userdata	0x00000000cf000000	0x00000000d22fe387

Results

- Unencrypted
- Data structure KW18



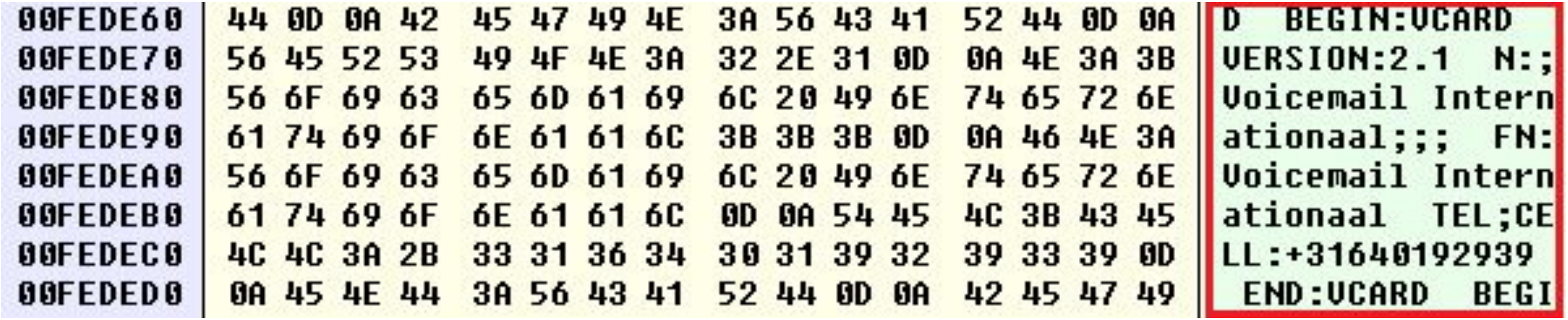
```
strings -a --radix=x backup.img | grep ditiseentest
ed8800 ditiseentest
```

Part	Start addr	End addr
SF_boot	00000000	000001F0
BRLYT	00000200	000007F0
int_bootloader	00000800	000028C0
padding	000028D0	00005FF0
ext_bootloader	00006000	0000FB90
padding	0000FBA0	0001FFF0
FILE_01_mtk	00020000	00BE5000
User data	00BE5010	00FFFFF0

Overview over the data structure that was identified

Results

- Contact details in the form of vCards.

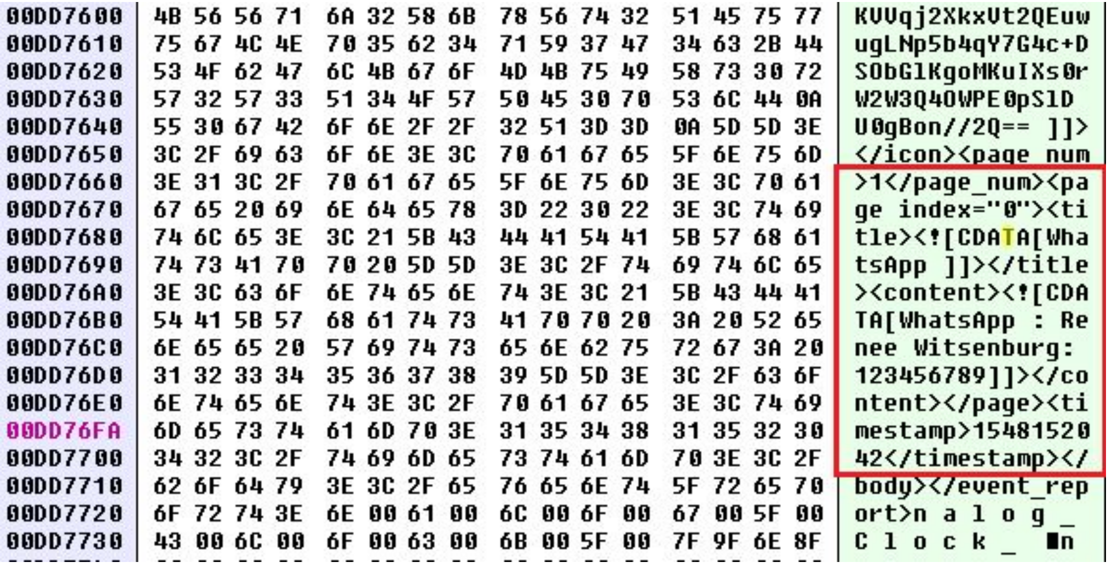


```
00FEDE60  44 0D 0A 42  45 47 49 4E  3A 56 43 41  52 44 0D 0A  D  BEGIN:VCARD
00FEDE70  56 45 52 53  49 4F 4E 3A  32 2E 31 0D  0A 4E 3A 3B  VERSION:2.1  N:;
00FEDE80  56 6F 69 63  65 6D 61 69  6C 20 49 6E  74 65 72 6E  Voicemail Intern
00FEDE90  61 74 69 6F  6E 61 61 6C  3B 3B 3B 0D  0A 46 4E 3A  ationaal;;;  FN:
00FEDEA0  56 6F 69 63  65 6D 61 69  6C 20 49 6E  74 65 72 6E  Voicemail Intern
00FEDEB0  61 74 69 6F  6E 61 61 6C  0D 0A 54 45  4C 3B 43 45  ationaal  TEL;CE
00FEDEC0  4C 4C 3A 2B  33 31 36 34  30 31 39 32  39 33 39 0D  LL:+31640192939
00FEDED0  0A 45 4E 44  3A 56 43 41  52 44 0D 0A  42 45 47 49   END:VCARD  BEGI
```

Results

- Whatsapp notifications in plaintext

- Possibility to Simulate a notification



```
00DD7600  4B 56 56 71  6A 32 58 6B  78 56 74 32  51 45 75 77  KVVqj2XkxVt2QEuw
00DD7610  75 67 4C 4E  70 35 62 34  71 59 37 47  34 63 2B 44  ugLNp5b4qY7G4c+D
00DD7620  53 4F 62 47  6C 4B 67 6F  4D 4B 75 49  58 73 30 72  SObGlKgoMKuIXs0r
00DD7630  57 32 57 33  51 34 4F 57  50 45 30 70  53 6C 44 0A  W2W3Q4OWPE0pSlD
00DD7640  55 30 67 42  6F 6E 2F 2F  32 51 3D 3D  0A 5D 5D 3E  U0gBon//2Q== ]]>
00DD7650  3C 2F 69 63  6F 6E 3E 3C  70 61 67 65  5F 6E 75 6D  </icon><page_num
00DD7660  3E 31 3C 2F  70 61 67 65  5F 6E 75 6D  3E 3C 70 61  >1</page_num><pa
00DD7670  67 65 20 69  6E 64 65 78  3D 22 30 22  3E 3C 74 69  ge index="0"><ti
00DD7680  74 6C 65 3E  3C 21 5B 43  44 41 54 41  5B 57 68 61  tle><![CDATA[Wha
00DD7690  74 73 41 70  70 20 5D 5D  3E 3C 2F 74  69 74 6C 65  tsApp ]]></title
00DD76A0  3E 3C 63 6F  6E 74 65 6E  74 3E 3C 21  5B 43 44 41  ><content><![CDA
00DD76B0  54 41 5B 57  68 61 74 73  41 70 70 20  3A 20 52 65  TA[WhatsApp : Re
00DD76C0  6E 65 65 20  57 69 74 73  65 6E 62 75  72 67 3A 20  nee Witsenburg: 
00DD76D0  31 32 33 34  35 36 37 38  39 5D 5D 3E  3C 2F 63 6F  123456789]]></co
00DD76E0  6E 74 65 6E  74 3E 3C 2F  70 61 67 65  3E 3C 74 69  ntent></page><ti
00DD76FA  6D 65 73 74  61 6D 70 3E  31 35 34 38  31 35 32 30  mestamp>15481520
00DD7700  34 32 3C 2F  74 69 6D 65  73 74 61 6D  70 3E 3C 2F  42</timestamp></
00DD7710  62 6F 64 79  3E 3C 2F 65  76 65 6E 74  5F 72 65 70  body></event_rep
00DD7720  6F 72 74 3E  6E 00 61 00  6C 00 6F 00  67 00 5F 00  ort>n a l o g _
00DD7730  43 00 6C 00  6F 00 63 00  6B 00 5F 00  7F 9F 6E 8F  C l o c k _  ■n
```

Understanding BLE devices

Services

Characteristics

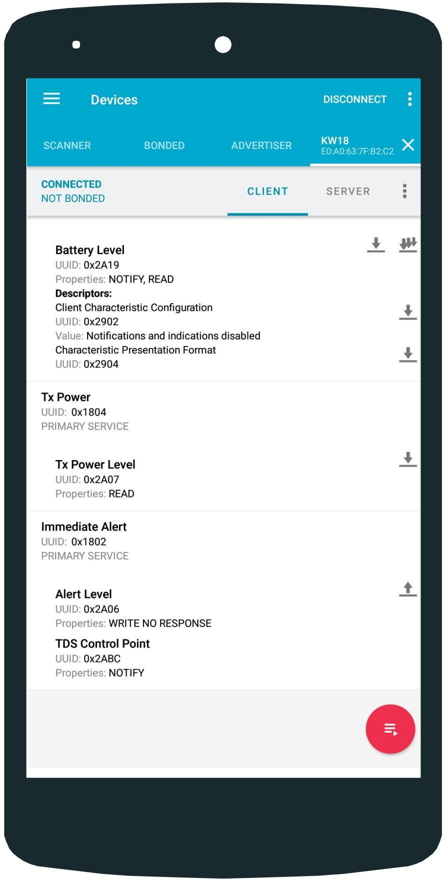
Descriptors

Read/write access

Request/notification

nRF connect

Unpair device and connect in mobile app. nRF Connect displays UUID’s of services



Battery Level
UUID: 0x2A19
Properties: NOTIFY, READ
Descriptors:
Client Characteristic Configuration
UUID: 0x2902
Value: Notifications and indications disabled
Characteristic Presentation Format
UUID: 0x2904

Tx Power
UUID: 0x1804
PRIMARY SERVICE

Tx Power Level
UUID: 0x2A07
Properties: READ

Immediate Alert
UUID: 0x1802
PRIMARY SERVICE

Alert Level
UUID: 0x2A06
Properties: WRITE NO RESPONSE

TDS Control Point
UUID: 0x2ABC
Properties: NOTIFY

Results (Amazfit)

With nRF Connect it is possible to generate fake notifications (sms, mail, calendar, call)

With the MiBand2 tool it is possible to read live data on a Linux device.

Discussion

- Only three smartwatches were investigated
- Results Mediatek and BLE
- Countermeasures NCSC

Conclusion

- Smartwatches in a business environment
  - email, agenda notifications and text messages.
- Attack scenarios
- Tamper with, read or intercept with the data

Future work

Categorize devices on communication protocol or chipset

Develop generic tools to test security per protocol or chipset

Questions?