# Low-end Chinese IoT wearables
# A dive into privacy and security concerns

# Low-end Chinese IoT wearables
## Chi siamo

**Massimo Bozza**

Ingegnere Elettronico, Security Consultant, Redbull addicted…
Mi occupo principalmente di sicurezza applicativa e dei sistemi embedded.

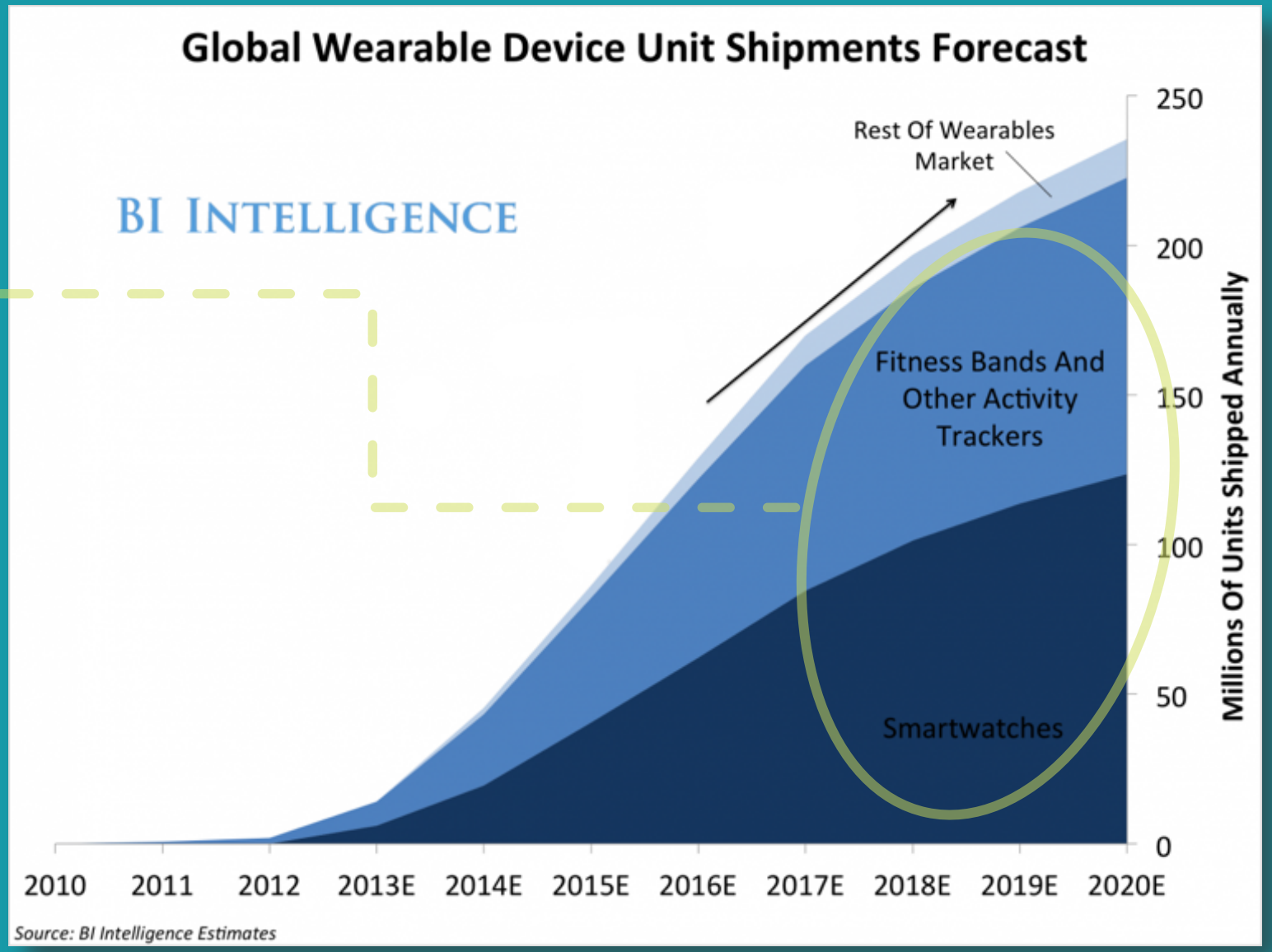
twitter: @maxbozza

**Pietro Stroia**

Ingegnere Informatico, Security Consultant nel campo della sicurezza applicativa.
Appassionato del mondo open-source e della sua filosofia, con un debole per la crittografia e il «low-level» ☺

# Low-end Chinese IoT wearables
# Panoramica del mercato «wearable»

Mercato costituito prevalentemente da Activity Tracker e Smartwatches



# Low-end Chinese IoT wearables
# Panoramica del mercato «wearable»

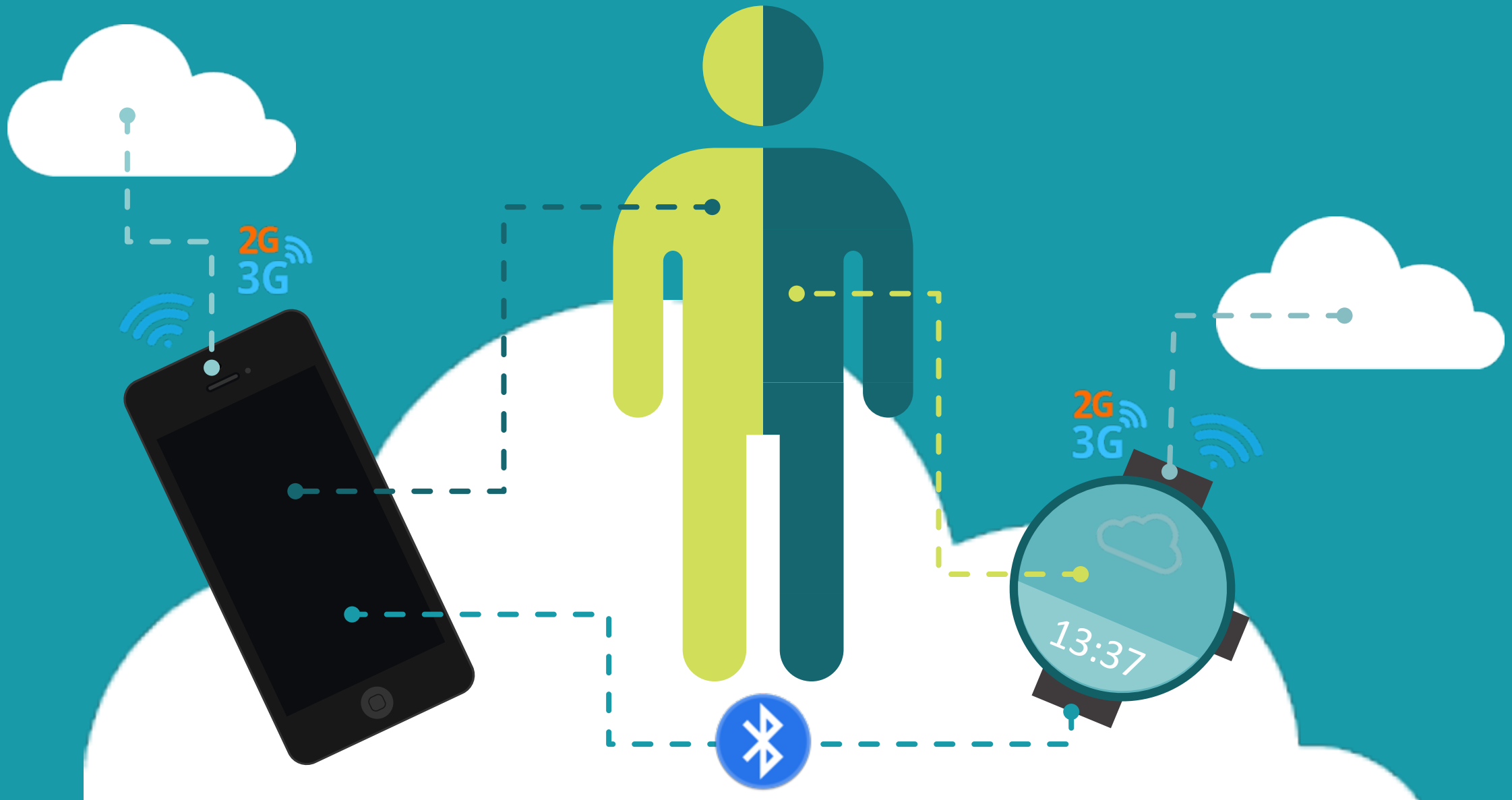
Top di gamma $$$:

- Apple iWatch
- Pebble
- Samsung Gear
- …

Low cost cinesi 15$:

- U8
- DZ09
- GT08
- M26
- …

# Low-end Chinese IoT wearables
# Ecosistema «wearable»



# Low-end Chinese IoT wearables
# I chipset MediaTek

| | GSM/GPRS | Bluetooth | FM Radio | MCU | Public SDK / Documentation |
|---|---|---|---|---|---|
| MT 6260 | ✓ | 3.0 | ✓ | ARMv7 | |
| MT 6261A | ✓ | 3.0 | ✓ | ARMv7 | |
| MT 6261DA | ✓ | 3.0 | ✓ | ARMv7 | |
| MT 6261MH | ✓ | 3.0 | ✓ | ARMv7 | |
| MT 2502 | ✓ | 4.0 | ✓ | ARMv7 | ✓ |

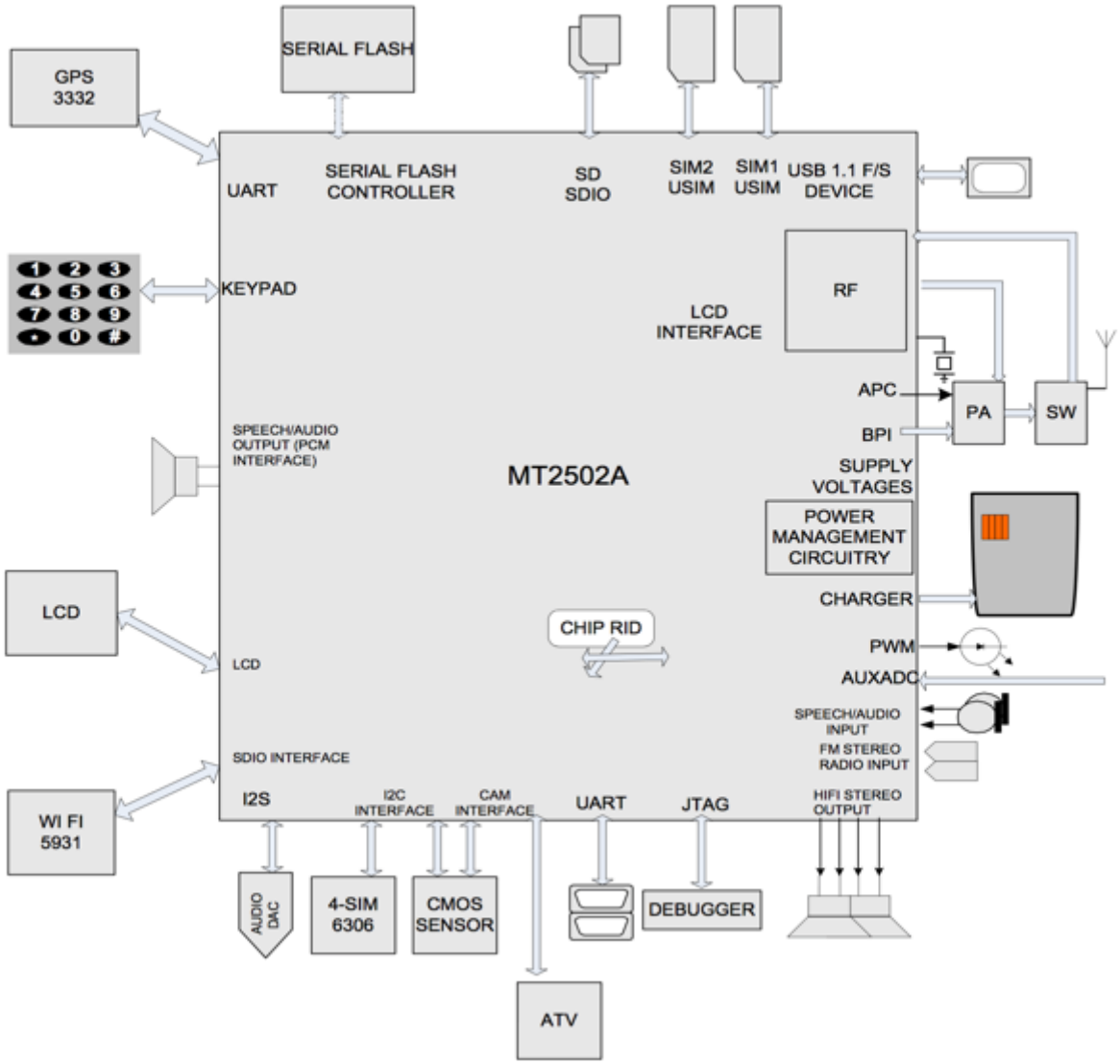
# Low-end Chinese IoT wearables
# MTK chipset blueprint

## MCU subsystem

- ARM7EJ-STM 32-bit RISC processor
- Dedicated DMA bus
- On-chip boot ROM for factory flash programming

## Test and debugging

- Built-in digital and analog loop back modes for both audio and baseband front-end
- DAI port complies with GSM Rec.11.10.
- JTAG port for debugging embedded MCU



# Low-end Chinese IoT wearables
# Dispositivi esaminati - MT6261D

**Dispositivi analizzati:**

- GT38 – GPS Tracker
- W88 - Smartwatch

**Caratteristiche:**

- Basati su chipset MT6261D
- Utilizzano una companion app per smartphone
- Cloud proprietario accessibile da app e web

# Low-end Chinese IoT wearables
# GT38, W88 – Considerazioni su software e firmware

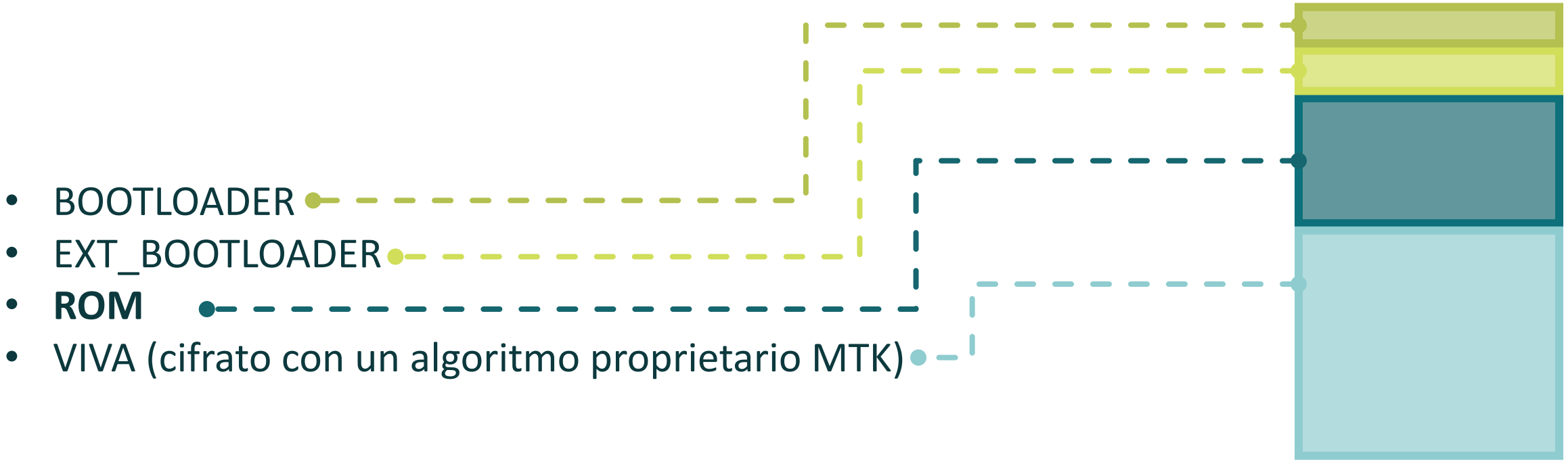
- **Voglio installare la mia app preferita.**
  Sfortunatamente non è presente nessun supporto alle «app», nonostante una interfaccia grafica che richiama molto Android/WatchOS.

- **Posso riprogrammare il dispositivo con un firmware da me modificato?**
  Per sviluppare un firmware bisogna acquistare l'SDK. Il sistema operativo è «Nucleus RTOS».

- **E quanto costa la licenza?**
  Probabilmente troppo se non si è un OEM (100K) ☺

# Low-end Chinese IoT wearables
# GT38, W88 – Considerazioni su software e firmware

- **E se facessimo un reversing della piattaforma per capirne di più?**
  MediaTek mette a disposizione FlashTool che permette di leggere e scrivere il firmware. Inoltre sono stati sviluppati dalla comunità dei tool che consentono di partizionare il firmware nei seguenti 4 files:



# Low-end Chinese IoT wearables
# GT38, W88 – Considerazioni su software e firmware

- **E se facessimo un reversing della piattaforma per capirne di più?**

```
Offset(d)  00 01 02 03 04 05 06 07 08 09 10 11 12 13 14 15

00000000   4D 4D 4D 01 38 00 00 00 46 49 4C 45 5F 49 4E 46  MMM.8...FILE_INF
00000016   4F 00 00 00 01 00 00 00 00 01 07 00 00 50 00 10  O............P..
00000032   A0 34 0C 00 FF FF FF FF FC 03 00 00 00 00 00 00   4..ÿÿÿÿü.......
00000048   FC 03 00 00 03 00 00 00 4D 4D 4D 02 30 01 00 02  ü.......MMM.0...
00000064   4D 32 38 4B 48 52 46 4E 31 5F 50 43 42 30 31 5F  M28KHRFN1_PCB01_
00000080   67 73 6D 5F 4D 54 36 32 36 30 5F 53 30 30 2E 4D  gsm_MT6260_S00.M
00000096   32 38 5F 4B 48 52 5F 46 4E 31 5F 56 30 30 34 2E  28_KHR_FN1_V004.
00000112   62 69 6E 00 00 00 00 00 00 00 00 00 00 00 00 00  bin.............
00000128   00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ................
00000144   00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ................
00000160   00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ................
00000176   00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ................
00000192   4D 32 38 5F 4B 48 52 2E 46 4E 31 2E 56 30 30 34  M28_KHR.FN1.V004
00000208   00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ................
00000224   00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ................
00000240   00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ................
00000256   01 00 00 00 00 01 00 00 00 00 00 00 00 00 00 00  ................
00000272   00 00 00 00 00 00 00 00 00 00 00 00 01 00 00 00  ................
00000288   00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ................
00000304   00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ................
```

L’ostacolo principale, come in tutte le attività di reversing, è comprendere il formato del file ROM. Purtroppo il formato è molto poco documentato, eccezion fatta per qualche riferimento ad esso su github, XDA e siti russi o cinesi dove viene specificato che il formato varia da versione a versione.

In generale, la nostra impressione è che il file ROM contenga istruzioni ARM non cifrate, eseguite attraverso una copia in RAM o XIP (execute-in-place).

# Low-end Chinese IoT wearables
# W88 – Considerazioni a livello di rete

- **Cosa possiamo capire da una analisi del traffico di rete per lo smartwatch?**
  Il dispositivo ha un canale preferenziale di trasmissione su rete 3G.

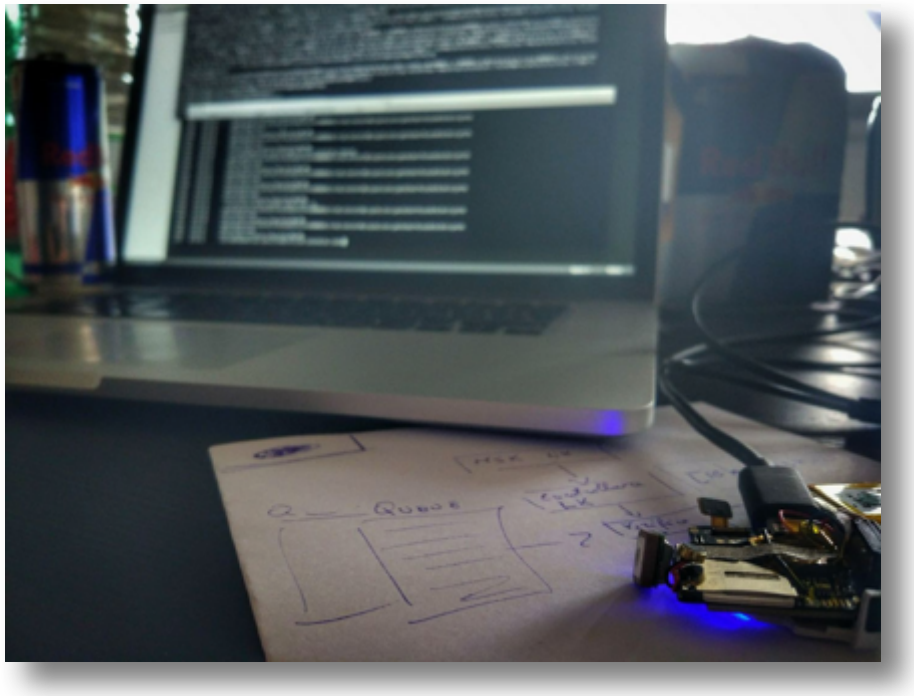
  Abbiamo però compreso che tutto il traffico relativo alla sensoristica viene inviato in un cloud cinese, dove vengono mostrati i percorsi preferiti degli utenti durante le attività di running, le calorie bruciate e molto altro...


**Bonus point**: evidenti vulnerabilità web da una semplice analisi passiva!

# Low-end Chinese IoT wearables
# GT38 – Considerazioni a livello di rete

- **Cosa possiamo capire da una analisi del traffico di rete per il GPS Tracker?**
  Il canale di comunicazione preferenziale del dispostivo resta il 3G.
  Grazie alla presenza di una porta seriale con dati di debug è stato possibile effettuare il debug del protocollo e indagare sulle attività in corso sul dispositivo durante l'interazione.

  Il dispositivo, può ricevere comandi remoti attraverso una comunicazione raw TCP, **senza alcuna forma di autenticazione e crittografia!**
  Abbiamo ricreato un backend e ci siamo interfacciati con il dispositivo.

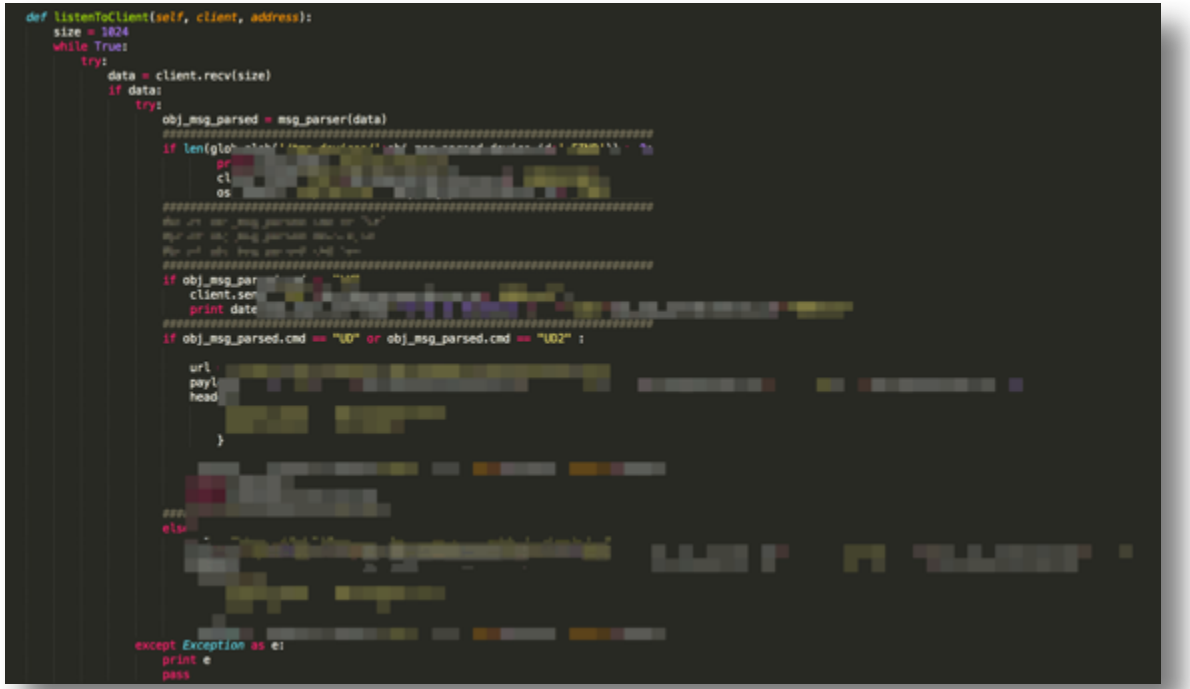


# Low-end Chinese IoT wearables
# GT38 – Considerazioni a livello di protocollo di rete

- Il dispositivo supporta l'aggiornamento firmware da remoto attraverso un preciso comando su raw TCP.
- Abbiamo intercettato, tramite l'output del debug, una chiamata verso un FTP cinese al momento del boot (cablata in firmware).

```
NetRange:       47.88.0.0 - 47.91.255.255
CIDR:           47.88.0.0/14
NetName:        AL-3
NetHandle:      NET-47-88-0-0-1
Parent:         NET47 (NET-47-0-0-0-0)
NetType:        Direct Allocation
OriginAS:
Organization:   Alibaba.com LLC (AL-3)
RegDate:        2015-05-18
Updated:        2017-04-26
Ref:            https://whois.arin.net/rest/net/NET-47-88-0-0-1


OrgName:        Alibaba.com LLC
OrgId:          AL-3
Address:        400 S El Camino Real, Suite 400
City:           San Mateo
StateProv:      CA
PostalCode:     94402
Country:        US
RegDate:        2010-10-29
```



# Low-end Chinese IoT wearables
# GT38 – Considerazioni a livello di protocollo di rete

Struttura comandi:

[VID * UID * LEN * CMD,ARGs]

Alcuni comandi enumerati:

- [VID * UID *0013*CALL,0039XXXXXXXXX]
- [VID * UID *00XX*SMS,Number,Text]
- [VID * UID *0005*RESET]
- [VID * UID *00XX*UPGRADE,URL]
- [VID * UID *00XX*IMEI,IMEI Number]

# Low-end Chinese IoT wearables
# GT38 – Considerazioni a livello di protocollo di rete

- L’amministratore del backend ha pieno controllo delle funzioni del device.
- Si può forzare il device ad un aggiornamento del firmware remoto (FOTA)
- Il device potrebbe essere utilizzato per l’ascolto ambientale all’insaputa dell’utente.
- La completa assenza di crittografia espone la comunicazione a rischi di hijack.

# Low-end Chinese IoT wearables
# W88 – Le app di «supporto» per i telefonini Android

Lo smartwatch W88 ha diverse «app» a supporto del suo utilizzo, installabili su un dispositivo Android compatibile. Non tutte le applicazioni sono pubblicate sul market ufficiale, dunque per il pieno utilizzo del dispositivo è necessario il download di applicazioni *non-trusted.*

- “Companion” App
- “Companion” Position Android – **fuori dal market ufficiale! Viene richiesta installazione manuale di un file APK.**
- “Companion” BTNotification

# Low-end Chinese IoT wearables
# W88 – Le app di «supporto» per i telefonini Android

Attraverso una analisi statica degli APK, è emerso come le “app” richiedano permessi universalmente considerati **pericolosi** in caso di una volontà di abuso da parte degli sviluppatori:

- USE_CREDENTIALS
- AUTHENTICATE_ACCOUNTS
- ACCESS_FINE_LOCATION
- READ_CONTACTS/SMS
- WRITE_CONTACTS/SMS
- CALL_PHONE
- READ/WRITE_EXTERNAL_STORAGE

# Low-end Chinese IoT wearables
# G38, W88 – Una sgradevole sorpresa

Tra tutte gli scenari di rischio per la privacy degli utilizzatori di questi dispositivi, ciò che ci ha più colpito è stata la presenza di due tipologie di comando presenti sul G38 e potenzialmente anche sul W88 essendo provvisto di SIM:

1. **«call»: effettua una chiamata verso un numero specificato dal comando**
2. **«automatic response»: auto-risposta a determinati numeri in chiamata**

Questi due messaggi rendono possibile utilizzare il dispositivo a tutti gli effetti come uno strumento di tracciamento e di intercettazione **«ambientale»**, specialmente per via della concreta **possibilità di aggiornamento del firmware in maniera «silente»** da parte degli sviluppatori o altri attori malevoli.

# Low-end Chinese IoT wearables
# Outlook

## Come evidenziato anche nell'ultimo rapporto del DNI statunitense (Worldwide Threat Assessment of the US Intelligence Community)

*"The widespread incorporation of "smart" devices into everyday objects is changing how people and machines interact with each other and the world around them, often improving efficiency, convenience, and quality of life. Their deployment has also introduced vulnerabilities into both the infrastructure that they support and on which they rely, as well as the processes they guide. Cyber actors have already used IoT devices for distributed denial-of-service (DDoS) attacks, and we assess they will continue. In the future, state and non-state actors will likely use IoT devices to support intelligence operations or domestic security or to access or attack targeted computer networks."*

## Gli oggetti IoT saranno sempre più sfruttati come vettori di attacco di tipo cyber sia da cyber criminali che da gruppi sponsorizzati da stati.

https://www.dni.gov/files/documents/Newsroom/Testimonies/SSCI%20Unclassified%20SFR%20-%20Final.pdf

# Grazie per l’attenzione!