

Hacking Medical Devices for Fun and Insulin: Breaking the Human SCADA System

Analisi delle vulnerabilità del sistema CGM

Francesco Montelli

CeSeNa

2017

Analisi delle vulnerabilità del sistema CGM

- ▶ Ipotesi
- ▶ Analisi
- ▶ Esperimenti
- ▶ Considerazioni
- ▶ Conclusione

Ipotesi

- ▶ Crittografia?
- ▶ Tipo di comunicazione
- ▶ Di che cosa “si rende conto” il sensore?

Analisi

- ▶ Read the manual

Transmitter/Reciver Frequency	402.142 MHz
Bandwidth	300 KHz
Modulation	On-Off Key
Data Rate	8192 bits/Sec
Total Packt	76 bit
Transmit Duty Cycle	9.28 ms evry 5 minutes

Analisi

- ▶ FCC Recon Research
- ▶ Brevetti
- ▶ Smontare il CGM
 - ▶ Nome del chip visibile (AMIS 52100M)
 - ▶ Stesso chip usato in ambienti SCADA

Esperimenti - How to Listen

- ▶ Arduino
- ▶ Problemi
 - ▶ Tanti registri (80+)
 - ▶ Tante impostazioni
 - ▶ Chip fuori produzione - \therefore nessun supporto del produttore
- ▶ Scoperte
 - ▶ Nessun controllo di consistenza ai valori assegnati ai registri

Esperimenti - CGM Signal Dissection

- ▶ Modulazione OOK
- ▶ Segnale = 1, Nessun segnale = 0
- ▶ $8192 \text{ bits/sec} * 9\text{ms} = \text{circa } 76\text{bit}$

Esperimenti - CGM Signal Dissection

- ▶ Modulazione OOK
- ▶ Segnale = 1, Nessun segnale = 0
- ▶ $8192 \text{ bits/sec} * 9\text{ms} = \text{circa } 76\text{bit}$
- ▶ Parametri richiesti per comunicare
 - ▶ Preambolo (non menzionato nel datasheet)
 - ▶ Sync Word: parola per autorizzare la comunicazione, impostata nel costruttore CRC
- ▶ Direct Mode
- ▶ Raccolta manuale dei pacchetti e relativa decodifica

Considerazioni finali

- ▶ Troppe combinazioni di impostazioni, impossibile avere un controllo fine
- ▶ Nessuna documentazione utilizzabile
- ▶ Nessuna esperienza d'uso in questa modalità

Conclusioni - Rischi per la sicurezza

- ▶ Replay Attack
- ▶ DOS
- ▶ Ogni attacco ideato risulterebbe in una semplice interruzione di servizio, nulla di grave considerando che si può tranquillamente misurare con il sangue
- ▶ Necessità di trovarsi vicino al bersaglio considerando la natura della trasmissione