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

Analisi delle vulnerabilità negli Infusori

Francesco Montelli

CeSeNa

2017

Considerazioni iniziali

- Deve funzionare 24/7
- E' in grado di ricevere le misurazioni del CGM
- Disponibile un controllo remoto per somministrare insulina
- Porta USB per programmare l'infusore e scaricare dati
- Pensato per durare nel tempo, aggiornamenti quasi totalmente assenti

Analisi

- Comunicazini più complesse
- Programmi di configurazioni antiquati, basati su XP
- Nel programma di configurazione è possibile impostare la quantità dele informazioni di log su HIGH

Analisi dei log

```
INFO: XXXXXX Command-sendCommand: SENDING CMD 0x5A
(Set RF Power On-command packet)
INFO: XXXXXX Command-encode: about to encode bytes =
<0xA7 0x31 0x33 0x70 0x5A 0x00 0xA8>
INFO: XXXXXX SerialPort-write(int buffer[])(20MS):
writing <0x0A 0x0B 0xA8 0x6D 0x16 0x8E 0x39 0xB2
0x94 0xB5 0x55 0xA9 0xA5>
```

Figure: esempio di cattura di un pacchetto