

ICeeData project

Arsenijs Pičugins,
“Kiberšahs” conference

My background

- 8 years messing with computers, programming, then electronics
- Cracked a WiFi password once
- Currently develop small solutions in electronics for a living and teach Python

The problem

- Patients get ICDs
- ICDs collect data
- ICDs relay data to base stations
- Base stations relay data to manufacturers
- Manufacturers relay data to healthcare providers
- ...
- Patients often don't get to see the data

Manufacturers

- Develop base stations and sell them
- Want to earn money
- Want to do as little as possible
- Don't want negative publicity

Doctors

- Mostly just want to treat their patients (YMMV)
- Can and do it better with the data collected
- Don't always share data with the patients
 - (some argue against it to prevent self-treatment)
 - there are laws enabling patients to get data

Patients

- Follow the doctors' recommendations
 - Many people are bad with preventive healthcare
- Some want to understand their condition
 - “Yeah, you’ve had arrhythmia episode a year ago”
 - “Wait, what? ”
 - “And then a couple more”
 - “ ... ”

That data could be very useful for patients.

Right to know?

Attack vectors: ICD

- *Not really a good option*
 - Needs a scalpel and a steady hand
 - Not entirely clear if ICDs have debug ports
 - We didn't even try (missed opportunities, I know)

Risks and challenges:

- Reverse-engineering the protocol would be hard
- Able to administer shocks upon command
- Register fuzzing can literally brick a human
- We'd need to develop MICS hardware for comms

Attack vectors:

Transmissions between ICD and BS

- A better option (*much better than the previous one*)
 - Non-intrusive
 - Can get all of the data

R&C:

- Proprietary technology
- I'm not good at SDR and signal processing
 - Therefore, I can't develop a solution accessible to patients

Attack vectors:

Base station

- Now that I can do!
 - Intrusive, but not too intrusive
 - I can make it easy as well - Linux FTW
 - Hardware hacking, yaay!
- R&C:
 - Can't disassemble the station (but not the firmware ;-)
 - What if manufacturer changes the firmware after successful exploit?
 - What if data is not easy to get?

Attack vector: Base station

- Base stations on eBay in large quantities
 - Probably from deceased people
 - Any blackhat can get one
 - We got one
 - No Ethernet ports
 - USB host and ADSL ports
- Guess the backdoor?

Classic



Further research

- Some credentials left on base stations
 - Expired, though
- Scripts making manufacturer's life easier
 - Firmware update over flash drives
 - Getting reports by using a special flash drive
 - We've made a script to prepare any flash drive

Next steps

- Make an accessible solution to enable anybody to get reports from their station
...while preserving integrity of equipment
- Make my base station play music from its speaker

Ethical issues

- Disclosure
 - Need to disclose enough to make an open-source solution
 - Can't disclose too much to avoid stuff happening
 - But then, our research is easily repeatable
- Is privacy at risk?
 - Do manufacturers care?
 - Can we change anything?

And the name is...

- St. Jude Medical
- This Aug, MedSec security research startup disclosed vulns in SJM tech and cashed in on falling stocks. SJM doesn't seem to care much.
- Well, that's one way to get your "bug bounty".

Thank you for your attention

Questions?