Security and Privacy for Implantable Medical Devices

Introduction

Some of the devices we're talking about here are pacemakers, implantable cardiac defibrillators, drug delivery systems, and neurostimulators. Over 25 million US citizens are reliant on IMD's. Currently- this was written in 2008- there is defense against accidents like ID numbers and redundancy but there hasn't been any defense against intentional harm such as replay attacks. Security can differ between different IMD devices.

Safety and utility goals

Traditional IMD design goals include safety and utility.This to the author also encompasses reliability and treatment efficiency.

- data access - provides access to the right people
- data accuracy - as it sounds
- device identification - broadcasting its identity to those who need to know of its existence.
- configurability - being able to change the appropriate settings on the device
- updatable software - since removing implanted devices can be dangerous, the safest way to recall defective devices is through a software update
- multidevice coordination - at the time of writing this wasn't as commonplace as it is now
- auditable - being able to track the devices operational history
- resource efficient - with more communication comes more power consumption

Security and privacy goals

The authors will be looking at how confidentiality, integrity, and availability of computer security apply to these implantable devices. They will be focusing on the security goals for the device itself, not on the security goals of storing the patient's data on a back end server.

- authorization - This has several broad categories

- personal authorization - making sure that each role has its corresponding rights. most obvious example is patients vs. doctors. reminds me of computer privileges.
- role-based authorization - actually this seems pretty much the same as the last point
- IMD selection - ensuring that when a device talks to another device that it is only talking to the devices it wants to talk to, not broadcasting its information to the world. Something quite interesting that the authors bring up here is how a device might be configured to ignore authorization rules if there is an emergency situation in which intervention even by an anonymous source is better than no intervention at all.
- availability - they say it plain and simple right off the bat: 'an adversary should not be able to mount a successful denial of service attack against an IMD.' Adversaries shouldn't be able to drain battery, overflow data storage, or stop communication traffic.
- device software and settings - there should be bounds on the settings so that adversaries and patients themselves can't do anything stupid like set the device in dev mode. A great example the authors give is not being able to increase the amount of morphine expelled from a device. Physicians shouldn't have too much power, and should be restricted from altering audit logs or debug mode. These devices should only accept authorized firmware updates.
- device-existence privacy - the fact that a patient has an IMD should be unknown. This is an interesting one because I hadn't thought of this before. You would be making it quite a bit more difficult for an adversary if you made it relatively unclear if a patient has an implanted device or not.
- device type privacy - even if the device is known, it should further ensure that the type of the device is not know. The authors give some interesting examples, such as if there was a device to treat a social stigma, a terminal illness, or if the device is very expensive. So even if it was known that you were using an IMD, it wouldn't be giving away much about why.
- specific device ID privacy - 'an adversary should not be able to wirelessly track individual IMDs.'
- measurement and log privacy - basically, the adversary shouldn't be able to find out any information from the device.
- bearer privacy - even if the adversary is able to track a device, they souldn't be able to find out who's actually using the device. On a side note, I think it's interesting that the author's chose all of these angles to look at security. It becomes obvious that they expect at least one of these security goals to fail, and still have that failure

- be relatively ok since the other security goals prevent the adversary from doing too much harm. This is a smart way to look at it, as often the goals of computer security fail.
- data integrity - no adversary should be able to change the data of patients or their events.

Classes of adversaries

- passive adversaries - those that eavesdrop to the signals of the devices
- active adversaries - those that can initiate malicious communications with the device
- coordinated adversaries - like a tag team between someone who's close with a patient and someone who's a device programmer
- insiders - healthcare professionals, software developers, hardware engineers, and patients.

Equipment of adversaries

- standard equipment - using commercial equipment, perhaps stealing a device programmer from a clinic.
- custom equipment - personally build equipment that doesn't necessarily follow the laws of transmitter power, etc.

Tensions - Security versus accessibility

There are some tensions between security and privacy goals and traditional goals. The more secure the device is, the more difficult it could be for an operation, especially one in which you are not operated on by professionals you are used to seeing.

Security versus device resources

Strong security methods like pki can be exhaustive of resources. If a device uses cryptographic functions it could decrease its performance and shorten its lifespan. Something else I didn't know before: using cryptographic functions in a device could actually amplify the negative effect of a denial of service attack since the there can be repeated attempts at authentication which require greater use of resources or exhaust memory.

security versus usability

This is seen in traditional applications as well. The more secure you make something the harder it can be to use. User interaction quality may go down as a result of over-complication. This is especially a concern for medical users during an emergency situation. Another example is distance at which the device can communicate. This is shortened as the level of security increases.