ST. JUDE MEDICAL™

MORE CONTROL. LESS RISK.

The Hack on St. Jude

By: Patrick Snow

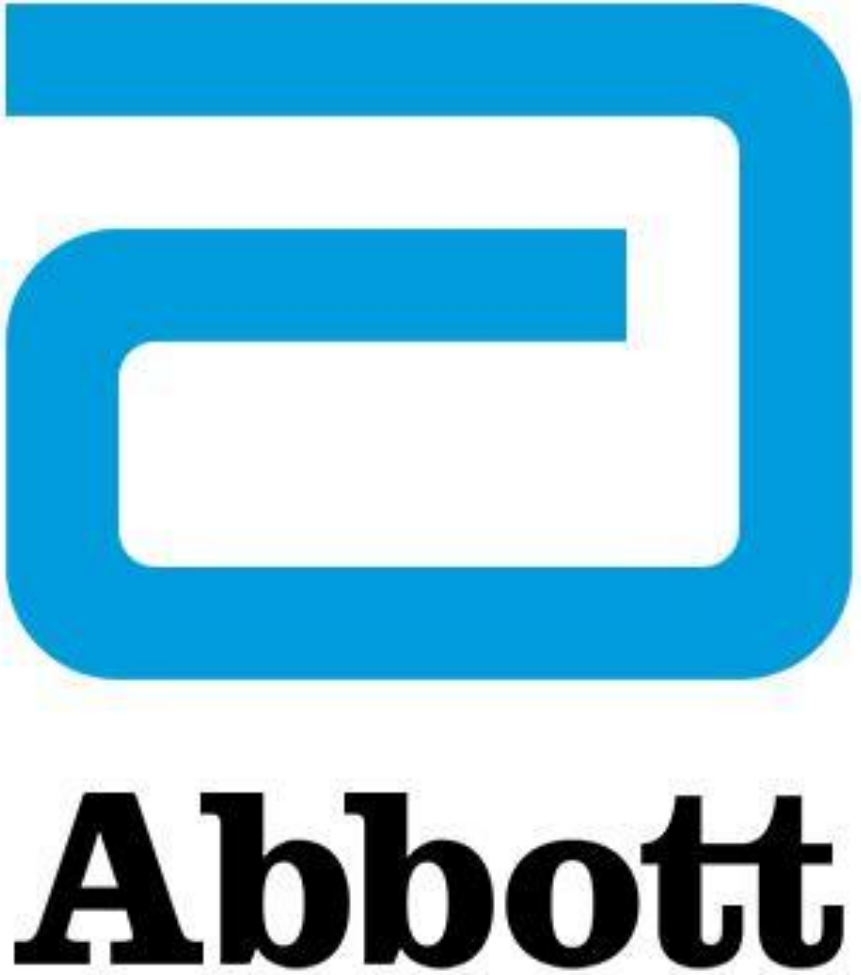
What Happened

- Flaws were discovered in the programming of St. Jude pacemakers.
  - The pacemakers came from Abbott(who is the head company that provides equipment and standards to other subsidiary companies such as St. Jude) in early 2017.
- Hackers would have been able to remotely alter variables in the St. Jude Medical's RF-enabled implantable cardiac pacemakers.
- The main reason why it can be devastating if a hacker could gain access to someone else's pacemaker is because they could have drained the battery which would have resulted in a death.

These are the vulnerable pacemakers created by St. Jude Medical

Hacking a pacemaker

- It was found that the medical device could be hacked from 7 feet.
- Most people who hack medical devices do it for malicious intent or keeping a person's life hostage.
- Abbott made cheap pacemakers which did not have many encryptions which makes it easier to access from anyone who has the knowledge and equipment.



Ways that a Pacemaker could become hacked

- 1. Medical devices today do not have enough memory or battery life to support encryption from random access control.
  - Hospital Industries like to be cheap sometimes so they would rather make medical devices without hardware chips that would have the increased encryptions.
- 2. Many medical devices do not require passwords or usernames mainly because doctors thought it would be easier to access it in case of an emergency.
- 3. Doctors and patients did not want to go through many surgeries in order to access the firmware of the medical device so they made it have remote monitoring.

- MedSec(a security researcher) discovered the vulnerability in their devices.
- The FDA sued the provider of the cardiac pacemaker and St. Jude Medical for marketing them.
- St. Jude admitted that two patients died and 10 fainted from this hack. They did not want to admit to anymore after that.
- St. Jude sued MedSec for defamation because they released the information on how the pacemaker could have been hacked.

MedSec

- Is a cybersecurity firm that tries to find vulnerabilities in medical devices and healthcare industries.
- MedSec has found numerous weaknesses in St. Jude Medical in past years.
- St. Jude even has sued MedSec for disclosing the weaknesses that they would discover.
  - St. Jude cares more about making money instead of fixing their weaknesses.

The Consequences of Poor Security Measures

- Since the hacker could have gained access to the battery life of the pacemaker then they could have killed anyone or everyone that had one.
  - 465,000 pacemakers were discovered to have this vulnerability.
- The FDA sent a warning after finding the claims of the hackable devices.
  - This sent the shares of Abbott down 2% to $42.61.

Solution

- The best way to prevent a hacker from remotely controlling the pacemakers is to make the security access stronger.
- It should require more specific information in order to alter the pacemakers rhythm.
- It should only be allowed to change the firmware at the designated hospital and by an approved doctor of that specialty.
- The doctor needs to have a special login that only he/she would know to access the firmware so it could be easily monitored on who tries to tamper with the pacemaker.

Solution(con.)

- The best consistent way to beat a hacker is to have multiple software patches but that does not always fix all the problem.
- It has been known that even though a patient with the pacemaker from St. Jude could get a software update they could still be potentially hacked.
- The reason why they can still be hacked is because there is a universal code that could allow hackers to control the implants.
- In the future, medical devices could become more advanced and cheaper. They could have low-cost encrypted hardware chips.