



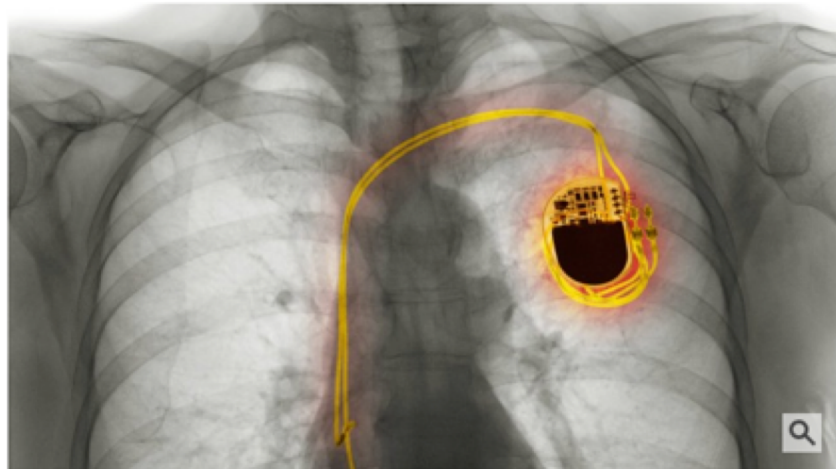
500.000 recalled pacemakers 2 billion \$ stock value loss - The story behind

Tobias Zillner, MMSc

» > Digital > IT-Sicherheit > IT-Lücke in Herzschrittmachern betrifft Hunderttausende

31. August 2017, 14:50 Uhr IT-Sicherheit

Hacker können Schwachstelle in Herzschrittmachern ausnutzen



Hacker könnten sich Zugriff auf Herzschrittmacher verschaffen, warnt die Pharmafirma Abbott. (Foto: imago/Science Photo Library)



- Hacker könnten sich Zugriff auf Hunderttausende Herzschrittmacher verschaffen, warnt die Pharmafirma Abbott in den USA.
- Um das zu verhindern sei ein Update der entsprechenden Software notwendig.
- Ein Angriff sei möglich, erfordere aber viel technisches Verständnis. Die

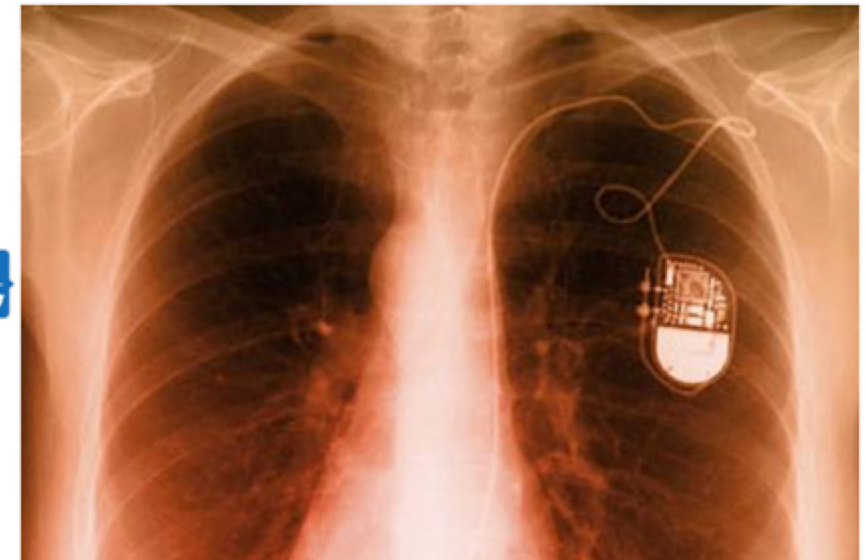
Nachrichten > Gesundheit > Ratgeber > Herz & Kreislauf > News > Schrittmacher mit Sicherheitslücke: Hacker können

Angriff auf Herzschrittmacher

Tausende Deutsche betroffen: Hacker könnten ihren Herzschlag stoppen

Teilen

★★★★★ 4



Herzschrittmacher geben kranken Herzen den Puls vor

photodisc



FOCUS-Online-Autorin **Petra Apfel**

Freitag, 01.09.2017, 15:34

In den USA soll fast eine halbe Million Menschen ins Krankenhaus, um ihren Herzschrittmacher sicher gegen Hackerangriffe zu machen. Auch 13.000 Deutsche tragen die Risiko-Schrittmacher – wie groß ist die Gefahr für ihr Herz wirklich?

HACK

Rückrufaktion für 500.000 unsichere Herzschrittmacher

Rund eine halbe Million Patienten in den USA müssen ins Krankenhaus - und sich ein [Firmware](#)-Update für ihren Herzschrittmacher aufspielen lassen. Dieser hatte zuvor Befehle per Funk ohne Authentifizierung akzeptiert.

Die US-Lebensmittel- und Medizinbehörde FDA hat einen [Rückruf für rund eine halbe Million Herzschrittmacher angeordnet](#) [↗](#), nachdem erhebliche Sicherheitsmängel nachgewiesen wurden. Die Geräte können manipuliert werden, um etwa die Batterie gezielt zu leeren oder das Tempo des Schrittmachers [zu bestimmen](#) [↗](#).



Herzschrittmacher von St. Jude Medical haben erneut Sicherheitsprobleme. (Bild: St. Jude Medical)

Datum: 31.8.2017, 11:30

Autor: Hauke Gierow

Themen: [Firmware](#), [IoT](#), [Internet](#), [Security](#)

Teilen:



May I introduce myself ?

Tobias Zillner, BSc MMSc

Lead IT Security Consultant | Co-Founder

- Expertise:
 - Industrial Security
 - IoT security
 - OSINT
 - Wireless security (SDR)
 - Offensive security
- Lecturer at FH St. Pölten, Uni Wien
- Speaker at international security conferences (Blackhat, Defcon, Deepsec, ...)



"He's a cool guy. His name is 'two beers'."

"Two beers?"

"Yes, it's a german name!"

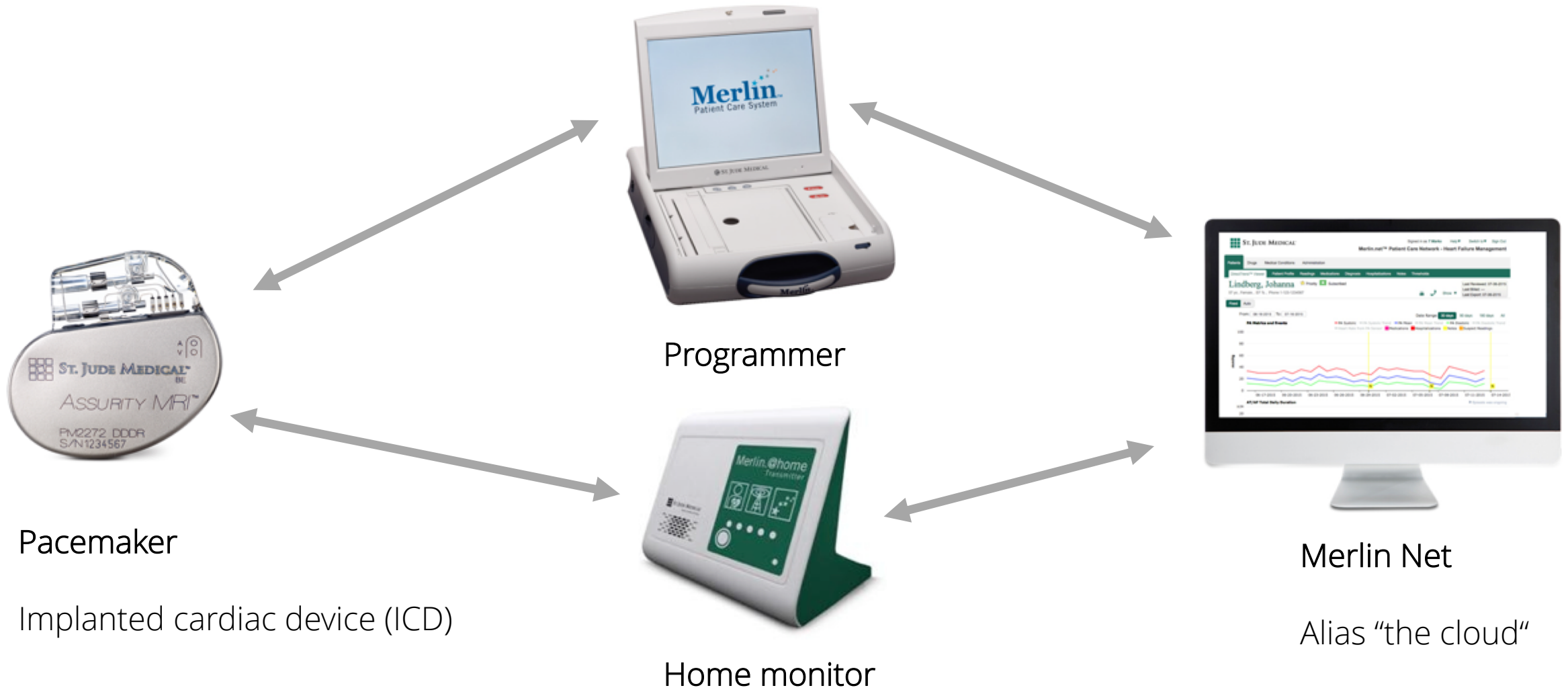
"Ohh! Tobias!"

How it all started

- Early 2016 a new medical security company decided to assess pacemakers
- **Goal: Find 0-day vulns in pacemakers**



The ecosystem



- New generation is able to communicate wireless
- Medical Implant Communication System (MICS)
 - low-power, short-range (2 m)
 - high-data-rate
 - 401–406 MHz (the core band is 402–405 MHz)
 - accepted worldwide for transmitting data to support the diagnostic or therapeutic functions associated with medical implant devices.
- Software Defined Radio / GNURadio



First vulns identified :D

- Energy depletion attack
- Crash attack



STJ Pacemaker Crash Attack

2 years ago | More



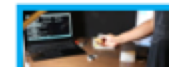
Muddy Waters Capital LLC

PRO

+ Follow

More from Muddy Waters Capital LLC

☒ Autoplay next video

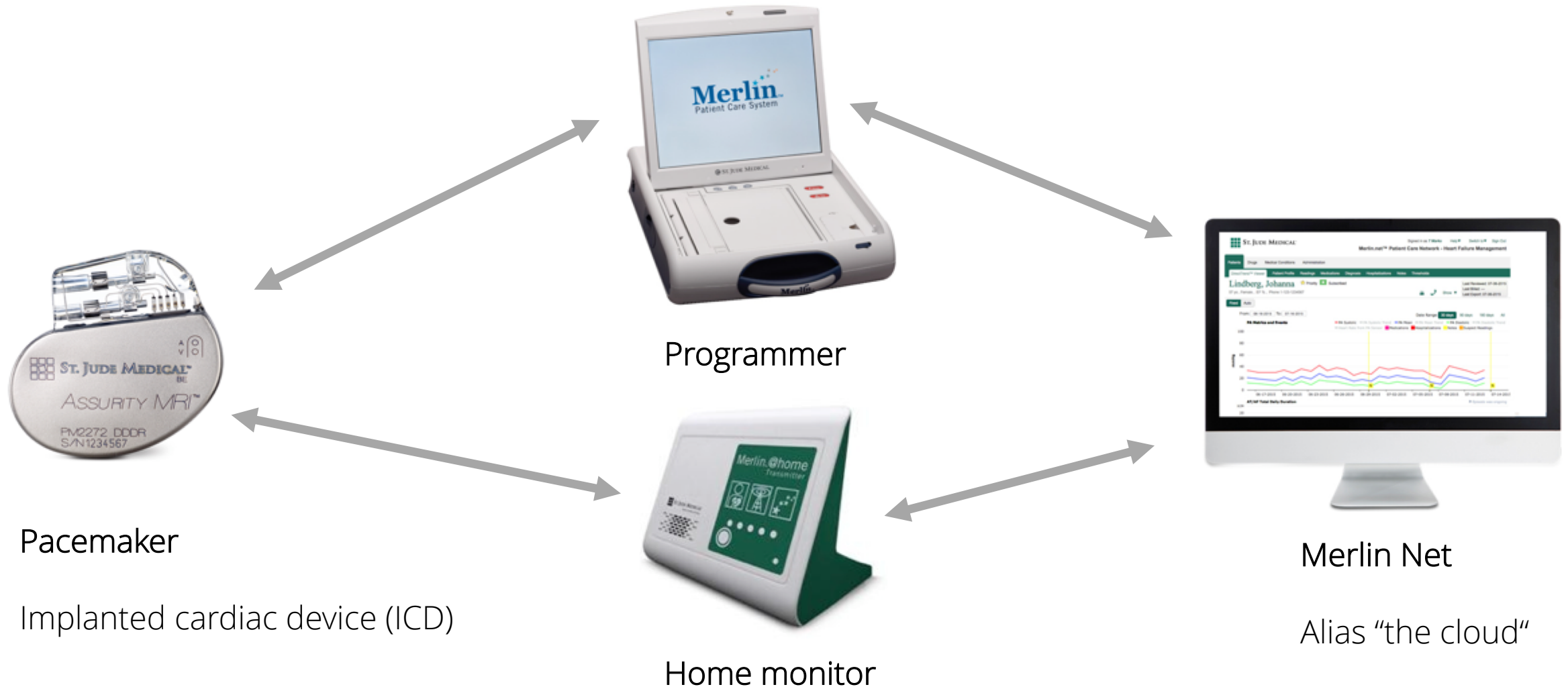


STJ Pacemaker C...

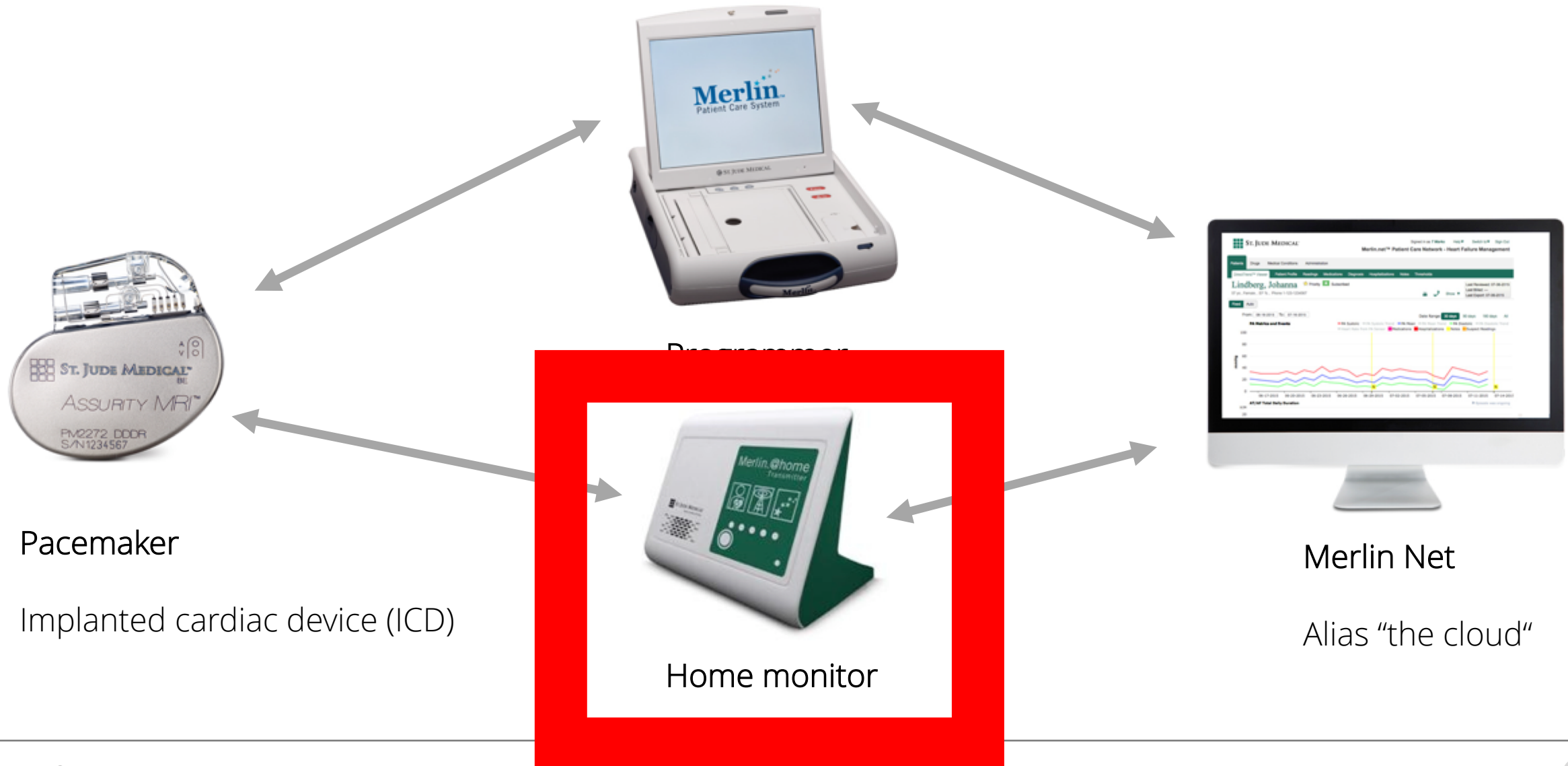
We got stuck...

- Reverse engineering time intensive
- Researcher time is expensive
- Weak crypto is also hard to crack only with your eyes
- **Decision point**
 1. We go into cryptoanalysis
 2. Look for other attack vectors




What else to attack?

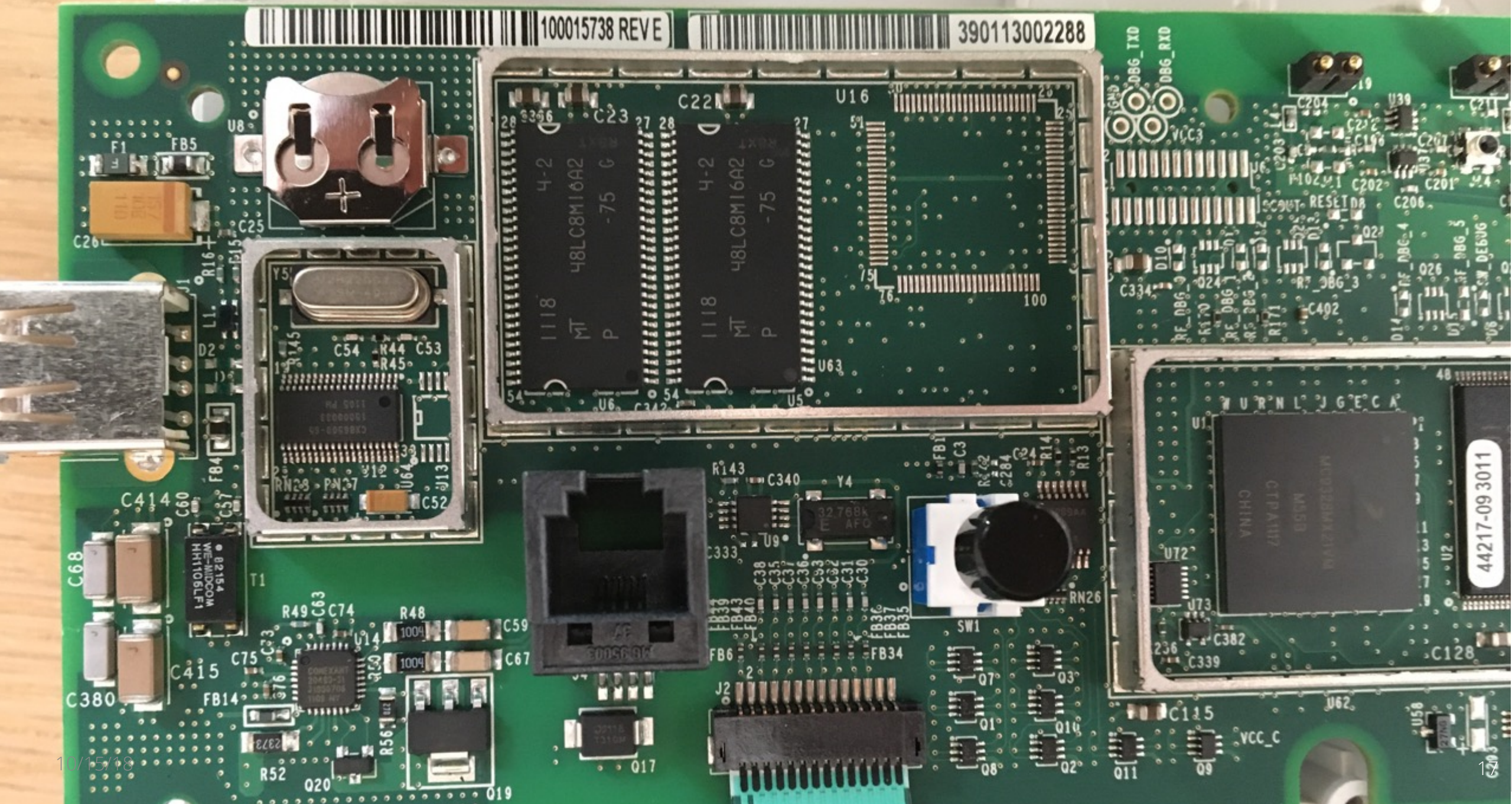


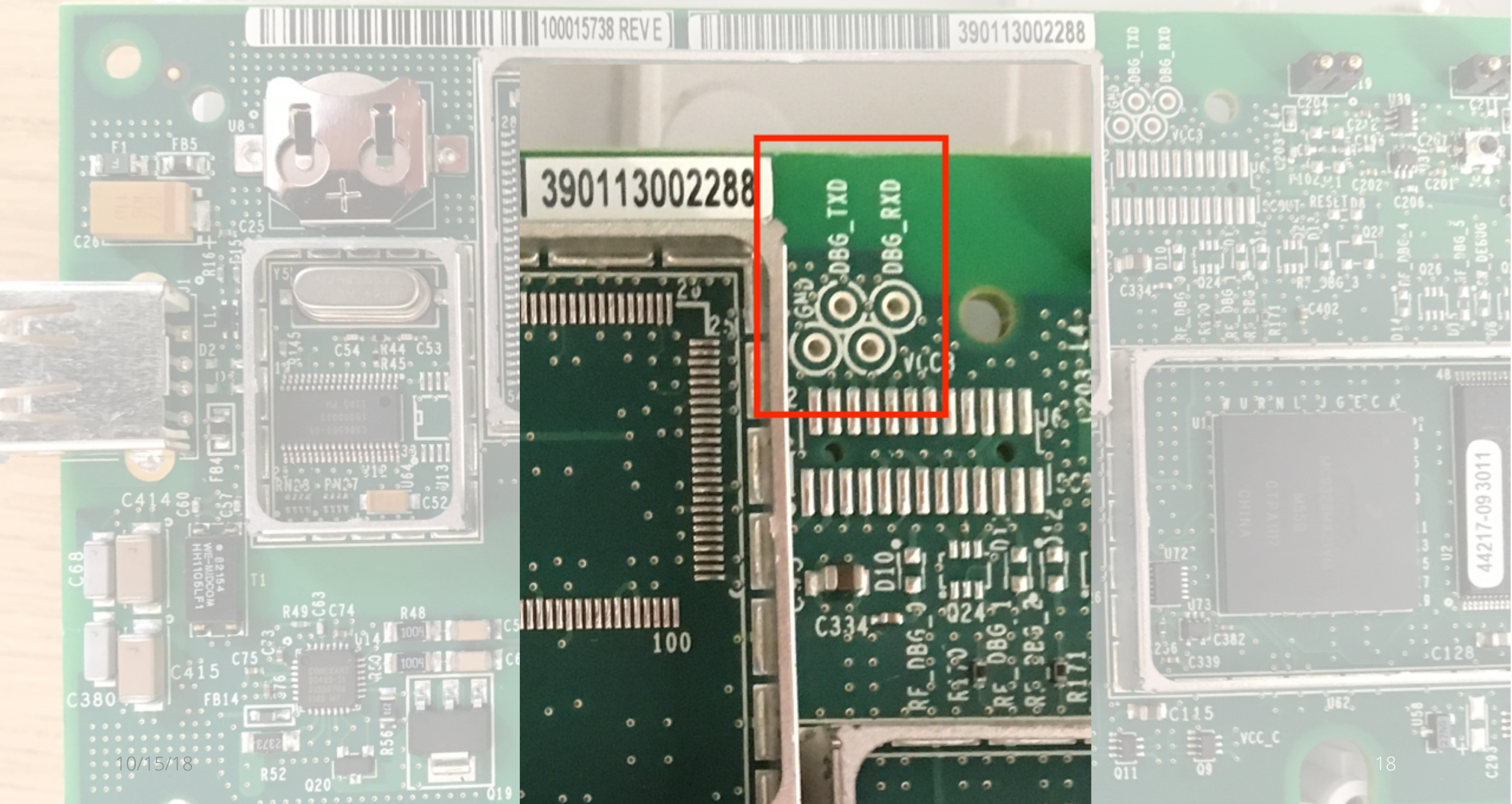
What else to attack?

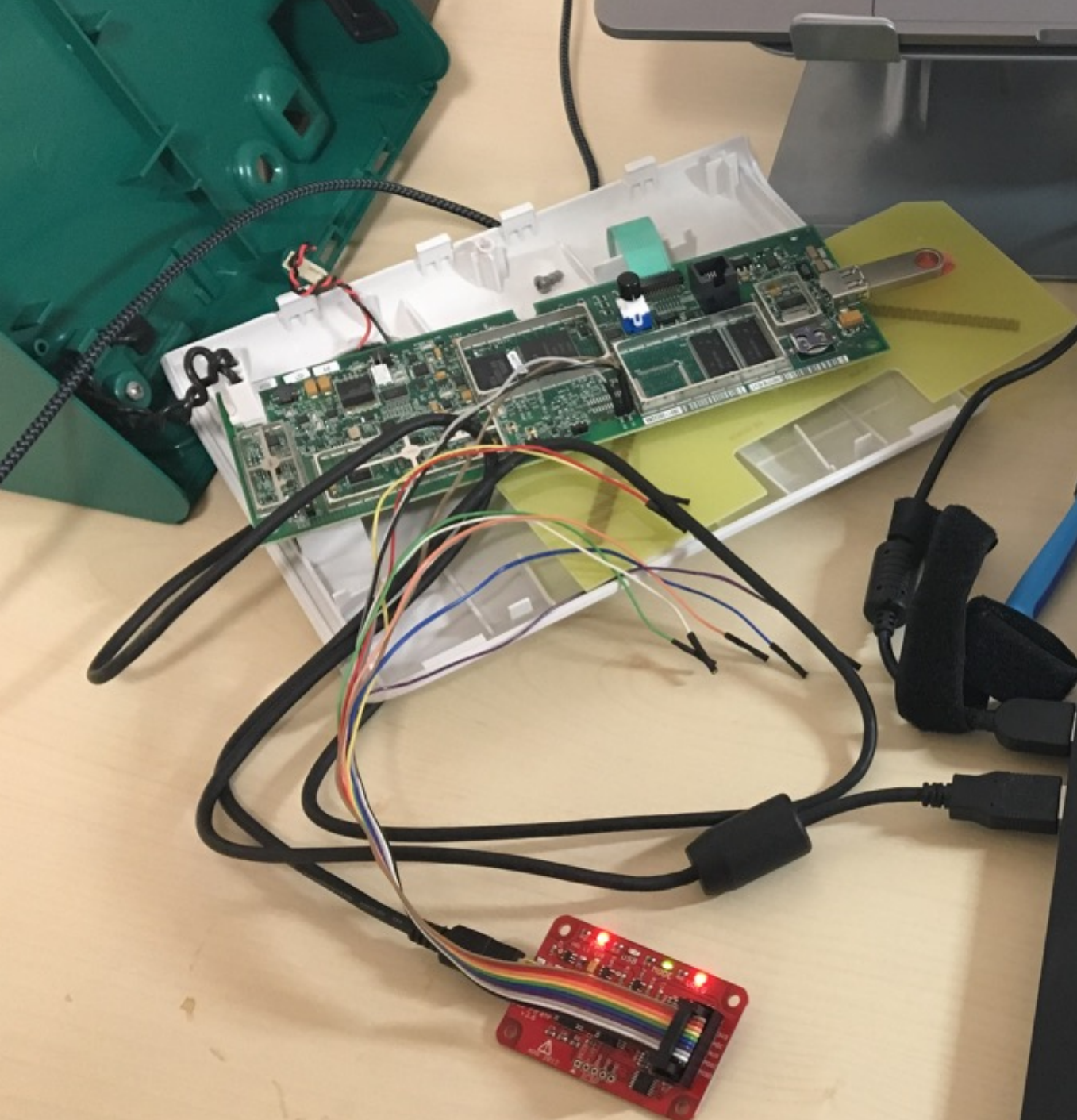


- Home monitor for patients
- Transmits health data to doctor
- Huge comfort benefits for patient
- Available interfaces
 - RJ11 jack
 - USB interface

	<p>Merlin At Home Transmitter -Model#EX1150</p> <p>Pre-Owned</p> <p>\$33.00</p> <p>Buy It Now +\$13.64 shipping</p> <p>Customs services &</p>
	<p>Merlin At Home Transmitter -Model#EX1150</p> <p>Pre-Owned</p> <p>\$29.75</p> <p>Was: \$35.00 or Best Offer +\$16.68 shipping 15% off</p> <p>Customs services &</p>
	<p>MERLIN@HOME TRANSMITTER Model EX1150</p> <p>Pre-Owned</p> <p>\$18.00</p> <p>Buy It Now +\$28.75 shipping 4 new & refurbished from \$35.00</p> <p>Customs services &</p>







```
root@raspi: /home/raspi
operator@none:~$
operator@none:~$
operator@none:~$
operator@none:~$
operator@none:~$ id
uid=12(operator) gid=0(root)
operator@none:~$ ls
devel_install.sh setdev.sh
operator@none:~$ cd
operator@none:~$ ls
devel_install.sh setdev.sh
operator@none:~$ ls -la
drwxr-xr-x  3 root  root
drwxr-xr-x 20 root  root
-rw-r--r--  1 root  root
-rw-r--r--  1 root  root
drwx----- 2 root  root
-r-xr-xr-x  1 root  root
-r-xr-xr-x  1 root  root
-r-xr-xr-x  1 root  root
operator@none:~$ cd /
operator@none:/$ ls
apps boot dev home mnt  proc sbin usr  vpd
bin  data etc  lib  opt  root tmp  var
operator@none:/$ id
uid=12(operator) gid=0(root)
operator@none:/$
```

setlog.sh

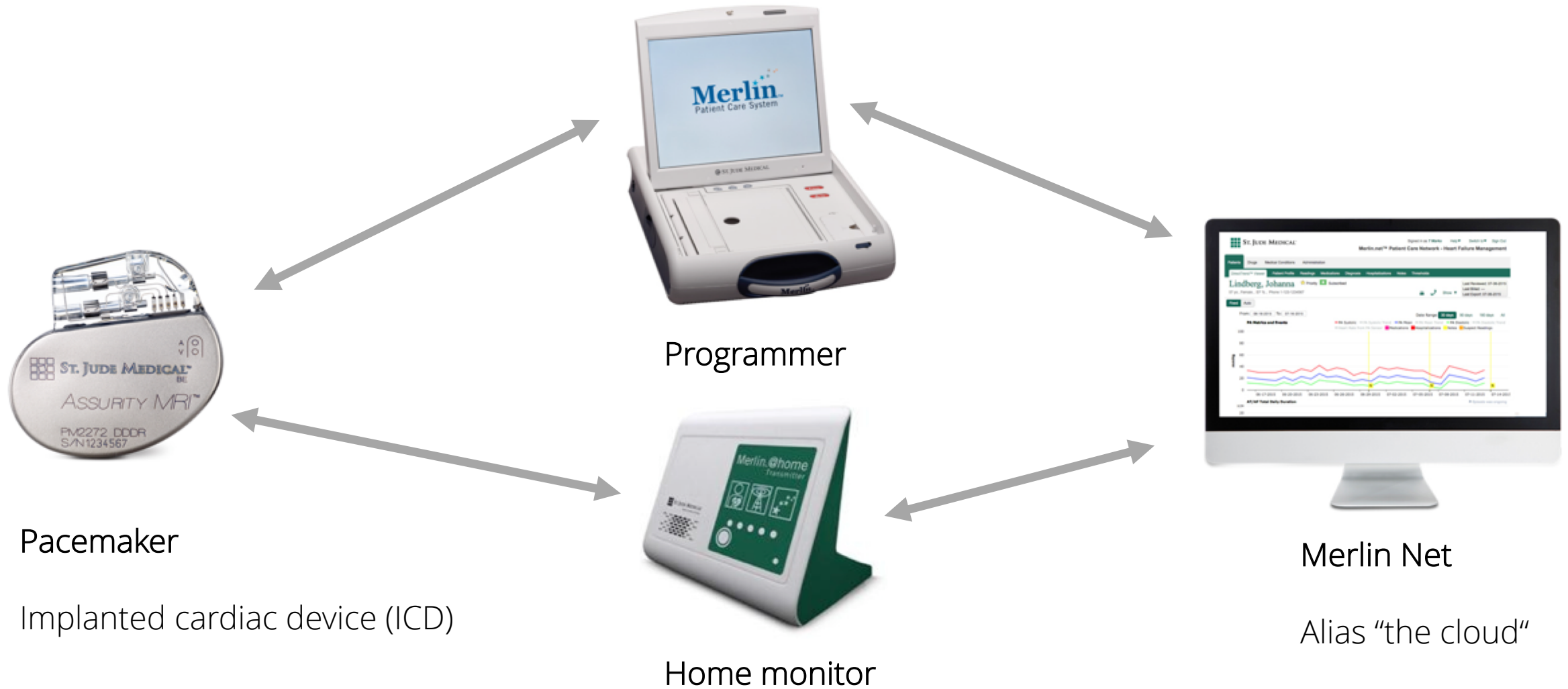
setlog.sh

0 Oct 11 2011 .
0 Jan 1 00:00 ..
0 Apr 21 2008 .bash_history
52 Apr 24 2008 .bash_profile
0 Oct 11 2011 .ssh
2584 Jul 13 2011 devel_install.sh
443 Jul 13 2011 setdev.sh
267 Jul 13 2011 setlog.sh

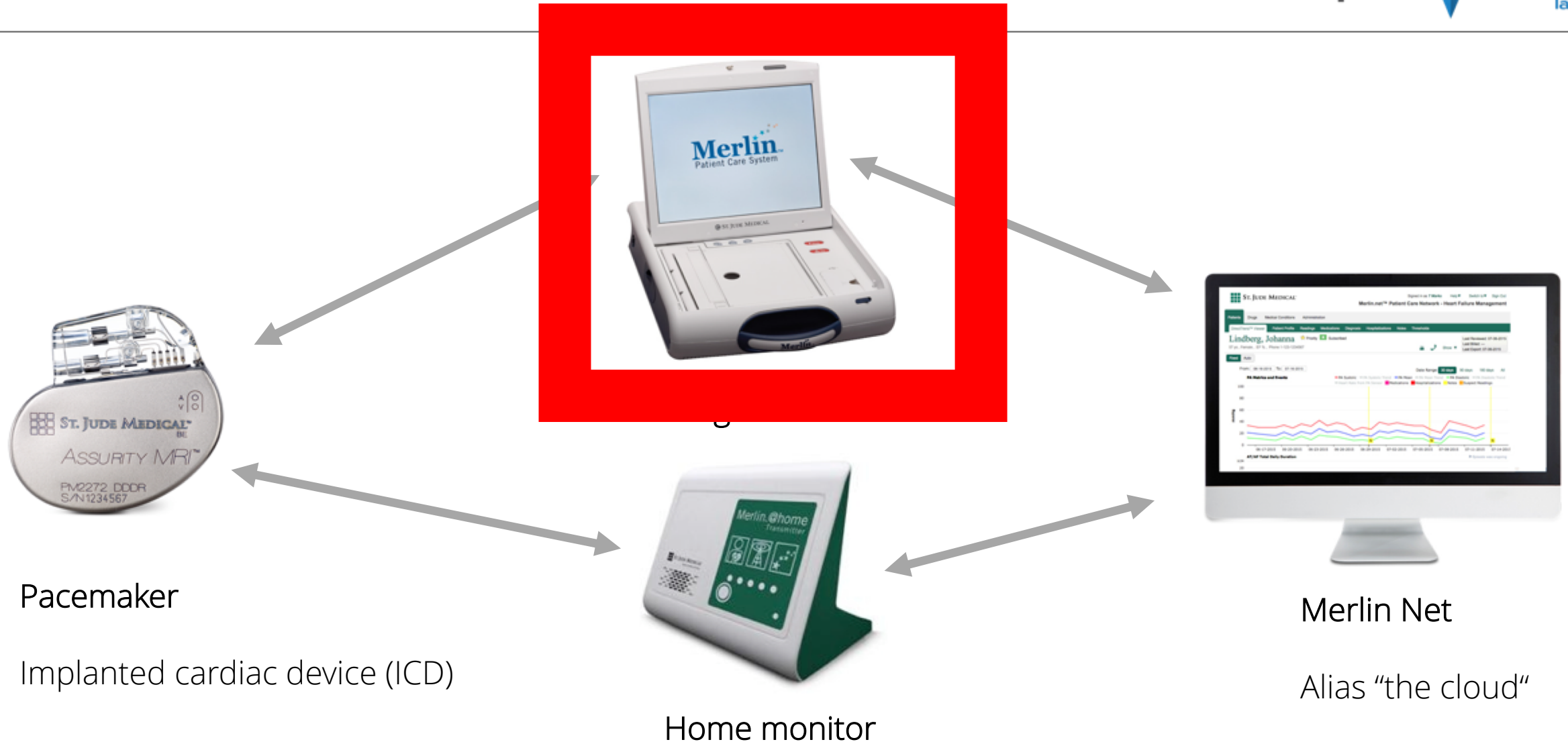
The hacker's perspective

Live Demo

What else to attack?



What else to attack?



What about the programmer?



St. Jude Medical 3510 Pacemaker Programmer with Warranty!!

Pre-Owned

\$1,000.00

or Best Offer
+\$67.37 shipping

From United States

Customs services and international tracking provided



ST.Jude Medical Model 3510 programmer System

Pre-Owned

\$585.00

or Best Offer
+\$665.37 shipping

From United States



St. Jude Medical Pacemaker Programmer Model 3510 with Warranty!!

Pre-Owned

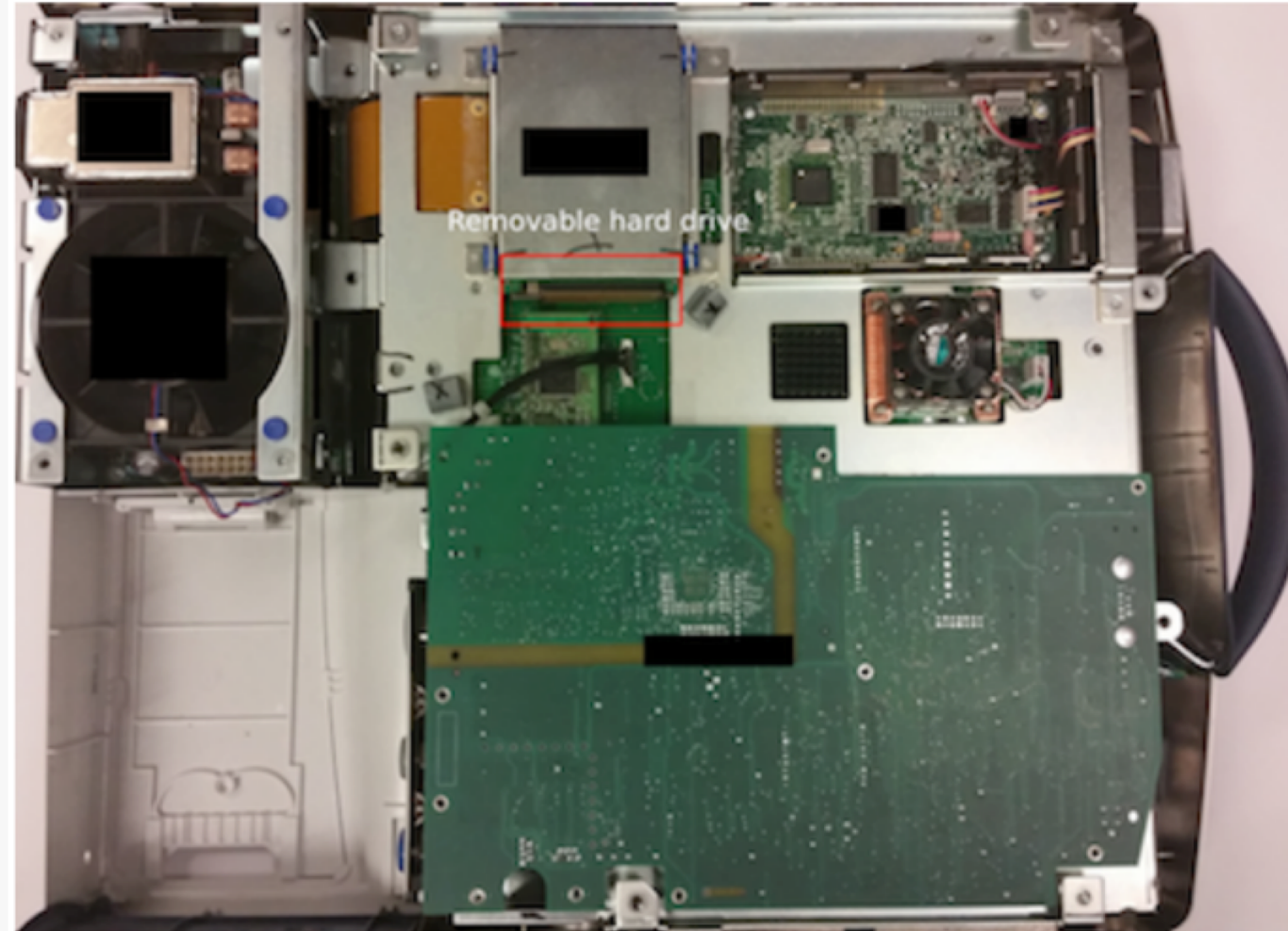
\$2,200.00

or Best Offer
+\$78.29 shipping

From United States

Customs services and international tracking provided

Tell us what you think



The final piece in the puzzle

- Reverse engineering of code
- Unencrypted HD
- Java JAR files :D
- No obfuscation

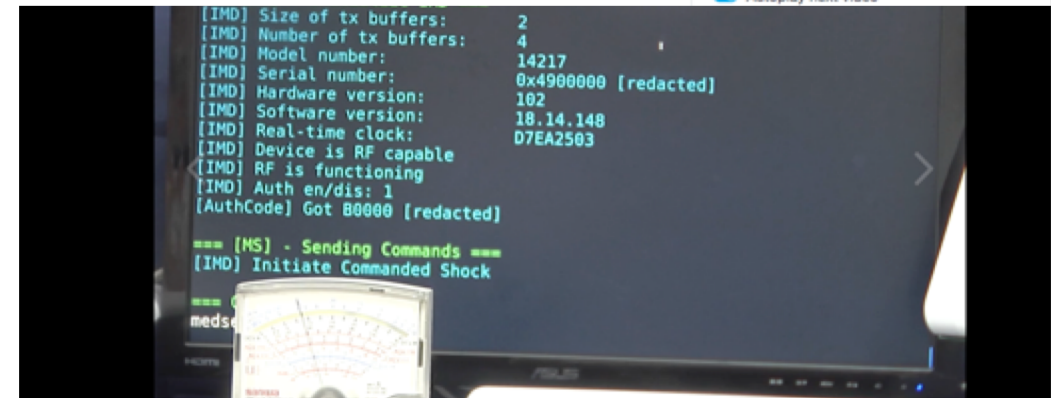
Merlin@Home as attack device

- Emergency shock
- Disable Tachy
- Vibrate
- T-Shock
- Demo videos released
 - Still available on Vimeo



VIBRATE

More from Muddy Waters Capital LLC
[Autoplay next video](#)



EMERGENCY SHOCK

More from Muddy Waters Capital LLC
[Autoplay next video](#)

Which message authentication code (MAC) is used?

- A. No authentication
- B. Proprietary (*Let's build our own „crypto“*)
- C. Hardcoded 24 bit RSA
- D. 56bit DES
- E. 1024bit RSA



Which message authentication code (MAC) is used?

- A. No authentication
- B. Proprietary (*Let's build our own „crypto“*)
- C. Hardcoded 24 bit RSA**
- D. 56bit DES
- E. 1024bit RSA



Other crypto mistakes?

- A. “homebrewed” cryptographic algorithm
- B. Hardcoded “Universal Key” as backdoor
- C. hard-coded 32-bit RSA public keys
- D. Truncate calculated keys because of memory



Other crypto mistakes?

- A. “homebrewed” cryptographic algorithm**
- B. Hardcoded “Universal Key” as backdoor**
- C. hard-coded 32-bit RSA public keys**
- D. Truncate calculated keys because of memo**



Technical Summary

- Critical vulnerabilities with potentially lethal impact discovered
- Unauthorized user could remotely access a patients implanted cardiac device over wireless interface
- Very easy debug access to Merlin@home device using an insecure hardware interface
- Insecure storage of source code on the home device/programmer
- Simple replay attacks for battery depletion
- Reprogramming of the pacemaker using wireless
- Static keys everywhere



INFORMATION SECURITY GUIDE

Broadband Kit

Executive Summary



This document describes the information security controls in place at St. Jude Medical in connection with the Broadband Kit (PCN). The Broadband Kit Assurance Program (BKA) is the first medical device control and network to be awarded ISO/IEC 27001:2005 certification, a stringent worldwide information security standard.

INFORMATION SECURITY GUIDE

Broadband Kit

Executive Summary



This document describes the information security controls in place at St. Jude Medical to protect health information as it connects to the Merlin.net PCN (Patient Care Network). St. Jude Medical utilizes a holistic approach to protecting the confidentiality, integrity and availability of health information by addressing the risks to the entire information lifecycle, thereby providing high levels of security and assurance of compliance. Merlin.net PCN is the first medical device control network to be awarded ISO/IEC 27001:2005 certification, a stringent worldwide information security standard.

What was special?


- MedSec licensed research to Muddy Waters (Hedge fond)
- Muddy Waters is an investment company known for investigating companies, finding problems like accounting fraud, and profiting by shorting the stock of misbehaving companies.
- Muddy Waters took short position in St.Jude Medical stock and bought shares from competitors

Security

Muddying the waters of infosec: Cyber upstart, investors short medical biz – then reveal bugs

Some sharks wear suits and ties

By [Iain Thomson](#) in San Francisco 26 Aug 2016 at 00:37

20  [SHARE](#) ▼



Analysis A team of security researchers tipped off an investment firm about alleged software vulnerabilities in life-preserving medical equipment in order to profit from the fallout.

Muddy Waters published findings report

- Vulnerability disclosure process?
- No notification to vendor

"We were worried that they would sweep this under the rug or we would find ourselves in some sort of a hush litigation situation where patients were unaware of the risks they were facing," said Bone, an experienced security researcher and the former head of risk management for Bloomberg LP, the parent of Bloomberg News. "We partnered with Muddy Waters because they have a great history of holding large corporations accountable."



Muddy Waters Capital LLC
info@muddywatersresearch.com
Director of Research: Carson C. Block, Esq.

Use of Muddy Waters reports is limited by the Terms of Service on its website, which are as follows. To be authorized to access such reports, you must agree to these terms, regardless of whether you have downloaded its reports directly from the Muddy Waters Research website or someone else has supplied the report to you without authorization from Muddy Waters Capital.

By downloading from, or viewing material on the Muddy Waters Research website, you agree to the following Terms of Service. You agree that use of Muddy Waters Capital LLC's research is at your own risk. In no event will you hold Muddy Waters Capital LLC, Muddy Waters, LLC or any affiliated party liable for any direct or indirect trading losses caused by any information on this site. You further agree to do your own research and due diligence before making any investment decision with respect to securities covered herein. You represent that you have sufficient investment sophistication to understand and evaluate the content of any opinion contained herein. You further agree that you will not communicate the content of this report to any third party without the prior written consent of Muddy Waters Capital. If you download or otherwise use this report, you are binding your principal to these same Terms of Service.

You should assume that as of the publication date of our reports and research, we with or through our members, partners, affiliates, employees, and/or consultant and/or their clients and/or investors, has a short position in all stocks (and/or options to the stock) and bonds covered herein, and therefore stands to realize significant declines. We intend to continue transacting in the securities of issuers covered and we may be long, short, or neutral at any time regardless of our initial position.

This is not an offer to sell or a solicitation of an offer to buy any security, nor shall it be made by any person through this report or reports on the website. Muddy Waters Capital only in the United States, but it does not render investment advice to anyone unless it is evidenced in writing.

If you are in the United Kingdom, you confirm that you are accessing research and information falling within Article 19 of the Financial Services and Markets Act 2000 ("FSMA"); or (b) high net worth entity falling within Article 49 of the FSMA.

Our research and reports express our opinions, which we have based upon generally accepted and deductions through our due diligence and analytical process. To the best of our knowledge, the information is accurate and reliable, and has been obtained from public sources we believe are insiders or connected persons of the stock covered herein or who may otherwise owe the issuer. However, such information is presented "as is," without warranty of any kind. Muddy Waters Capital LLC makes no representation, express or implied, as to the accuracy, completeness, or with regard to the results to be obtained from its use. Further, any report is for informational purposes only. All expressions of opinion are subject to change without notice, and we reserve the right to update or supplement any reports or any of the information, analysis and conclusions.

You agree not to distribute this information (whether the downloaded file, copies / in any manner other than by providing the following link: <http://www.muddywaters.com>) in any manner other than by download from that link going to that link and agreeing to the Terms of Service. You further agree that any distribution or other materials on the Muddy Waters Research website shall be governed by the terms of any conflict of law provisions. You knowingly and independently agree to the jurisdiction of the superior courts located within the State of California and waive your right to enforce any right or provision of these Terms of Service shall not constitute a waiver of these Terms of Service is found by a court of competent jurisdiction to be invalid, the provisions of these Terms of Service shall remain in full force and effect, in particular as to this governing law and jurisdiction. If any state or law to the contrary, any claim or cause of action arising out of or related to this report must be filed within one (1) year after such claim or cause of action arose or is discovered.

Report Date: August 25, 2016	Stock Price: \$81.88
Company: St. Jude Medical, Inc.	Market Cap: \$23.3 billion
Ticker: STJ US	Float: 97.5%
Industry: Medical Devices	Average Volume: 1.9 million shares

This version has been updated to state that Dr. Nayak speaks for himself, and not his employer.

Summary

Muddy Waters Capital is short St. Jude Medical, Inc. (STJ US).¹ There is a strong possibility that close to half of STJ's revenue is about to disappear for approximately two years. STJ's pacemakers, ICDs, and CRTs might – and in our view, should – be recalled and remediated. (These devices collectively were 46% of STJ's 2015 revenue.) Based on conversations with industry experts, we estimate remediation would take at least two years. Even lacking a recall, the product safety issues we present in this report offer unnecessary health risks and should receive serious notice among hospitals, physicians and cardiac patients.

We have seen demonstrations of two types of cyber attacks against STJ implantable cardiac devices ("Cardiac Devices"): a "crash" attack that causes Cardiac Devices to malfunction – including by apparently posing at a potentially dangerous rate, and, a battery drain attack that could be particularly harmful to device dependent users.² Despite having no background in cybersecurity, Muddy Waters has been able to replicate in-house key exploits that help to enable these attacks.

We find STJ Cardiac Devices' vulnerabilities orders of magnitude more worrying than the medical device hacks that have been publicly discussed in the past. These attacks take less skill, can be directed randomly at any STJ Cardiac Device within a roughly 50 foot radius, theoretically can be executed on a very large scale, and most galling, are made possible by the hundreds of thousands of substandard home monitoring devices STJ has distributed.³ The STJ ecosystem, which consists of Cardiac Devices, STJ's network, physician office programmers, and home monitoring devices, has significant vulnerabilities. These vulnerabilities highly likely could be exploited for numerous other types of attacks.

Key vulnerabilities can apparently be exploited by low level hackers. Incredibly, STJ has literally distributed hundreds of thousands of "keys to the castle" in the form of home monitoring units (called "Merlin@home") that in our opinion, greatly open up the STJ ecosystem to attacks. These units are readily available on Ebay, usually for no more than \$35. Merlin@homes generally lack even the most basic forms of security, and as this report shows, can be exploited

¹ The short positions are held by funds Muddy Waters Capital LLC manages.

² See Demonstrated Attacks – Likely Just Two of Many Possibilities infra.

³ It would have been illegal to attempt to validate the large scale attack theories.

The Impact

- Stock price fell **12%** before trading being halted the day they went public
- 2 billion \$ value loss
- **2.000.000.000 \$** value loss



Sicherheitsmitteilung

Merlin@Home™ und Merlin.net-Fernüberwachung Verbesserungen bei der Cybersecurity

**Merlin@Home™-Software Modell EX2000 v8.2.2 für die
Merlin@Home™ Sender, Modelle EX1150, EX1150W, EX1100,
und EX1100W**

03 April 2017

Wenngleich das Risiko äußerst gering ist, besteht die Möglichkeit, dass ein hochqualifizierter Hacker, der unerlaubt Zugang zu einer Kommunikationsinfrastruktur (z.B. durch Spoofing von Mobiltelefonmasten oder Telefonnetzwerken) und Kenntnis der Merlin@home™-Kommunikationsprotokolle erhält oder besitzt, potenziell eine Schwachstelle ausnutzen könnte, um Änderungen am Merlin@home™-Transmitter vorzunehmen. Der veränderte Merlin@home™-Transmitter könnte dann genutzt werden, um dem implantierten Gerät des Patienten Programmierbefehle zu erteilen bzw. Programmierbefehle zu verändern, was zu einer vorzeitigen oder beschleunigten Batterieentleerung und/oder Abgabe unangemessener Stimulationsimpulse oder Schocks führen könnte. Wie bereits erwähnt, wurde kein derartiger Angriff im Zusammenhang mit einem auf dem Markt befindlichen Merlin@home™-Transmitter berichtet.

*"We have examined the allegations made by Capital and MedSec on August 25, 2016 regarding the safety and security of our pacemakers and defibrillators, and while we would have preferred the opportunity to review a detailed account of the information, based on available information, **we conclude that the report is false and misleading.** Our top priority is to reassure our patients, caregivers and physicians that our devices are secure and to ensure ongoing access to the proven clinical benefits of remote monitoring. **St. Jude Medical stands behind the security and safety of our devices** as confirmed by independent third parties and supported through our regulatory submissions."*

- St. Jude disputed vulnerability claims and sued the researches and Muddy Waters



The screenshot shows a web browser displaying the St. Jude Medical website. The address bar shows the URL: media.sjm.com/newsroom/news-releases/news-releases-details/2016/St-Jude-Medical-Brings-Legal-Action-Against-... The website header includes the Abbott logo, navigation links for NEWSROOM, CAREERS, and INVESTORS, a language selector for ENGLISH (UNITED STATES), and social media icons. Below the header, there are links for HEALTH CARE PROFESSIONALS, PATIENTS, and ABOUT ST. JUDE MEDICAL. The main content area is titled "NEWS RELEASE DETAILS" and features the headline "ST. JUDE MEDICAL BRINGS LEGAL ACTION AGAINST MUDDY WATERS AND MEDSEC" dated SEPTEMBER 07, 2016. The sub-headline reads: "St. Jude Medical Turns to the Court to Hold Muddy Waters and MedSec Accountable for their Financially Motivated False Statements and Scare Tactics Aimed at Patients with Heart Conditions". The body text begins with: "ST. PAUL, Minn.--(BUSINESS WIRE)-- St. Jude Medical, Inc. (NYSE:STJ), a global medical device company, announced today that it has filed a lawsuit against Muddy Waters Consulting LLC, Muddy Waters Capital LLC, MedSec Holdings, Ltd., MedSec LLC, and three individual defendants who are principals in these firms, for false statements, false advertising, conspiracy and the related manipulation of the public markets in connection with St. Jude Medical's implantable cardiac management devices. With this action, St. Jude Medical seeks to hold these firms and individuals accountable for their false and misleading tactics, to set the record straight about the security of its devices, and to help cardiac patients and their doctors make informed medical decisions".

→ ↻ ⓘ Not Secure | media.sjm.com/newsroom/news-releases/news-releases-details/2016/St-Jude-Medical-Brings-Legal-Action-Against-... ☆ 🔍

NEWSROOM CAREERS INVESTORS 🌐 ENGLISH (UNITED STATES) 📧 📺 📺 📺 🔍

Abbott HEALTH CARE PROFESSIONALS ▾ PATIENTS ▾ ABOUT ST. JUDE MEDICAL

[Home](#) | [Newsroom](#) | [Archived News Releases](#) | [News Release Details](#)

NEWS RELEASE DETAILS

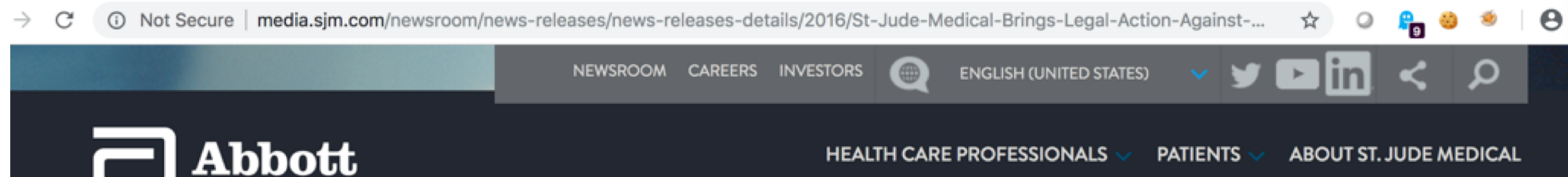
ST. JUDE MEDICAL BRINGS LEGAL ACTION AGAINST MUDDY WATERS AND MEDSEC

SEPTEMBER 07, 2016

St. Jude Medical Turns to the Court to Hold Muddy Waters and MedSec Accountable for their Financially Motivated False Statements and Scare Tactics Aimed at Patients with Heart Conditions

ST. PAUL, Minn.--(BUSINESS WIRE)-- St. Jude Medical, Inc. (NYSE:STJ), a global medical device company, announced today that it has filed a lawsuit against Muddy Waters Consulting LLC, Muddy Waters Capital LLC, MedSec Holdings, Ltd., MedSec LLC, and three individual defendants who are principals in these firms, for false statements, false advertising, conspiracy and the related manipulation of the public markets in connection with St. Jude Medical's implantable cardiac management devices. With this action, St. Jude Medical seeks to hold these firms and individuals accountable for their false and misleading tactics, to set the record straight about the security of its devices, and to help cardiac patients and their doctors make informed medical decisions

- St. Jude disputed vulnerability claims and sued the researches and Muddy Waters



St. Jude Medical seeks to hold these firms and individuals accountable for their false and misleading tactics, to set the record straight about the security of its devices, and to help cardiac patients and their doctors make informed medical decisions about products that enhance and save lives every day.

ST. JUDE MEDICAL BRINGS LEGAL ACTION AGAINST MUDDY WATERS AND MEDSEC

SEPTEMBER 07, 2016

St. Jude Medical Turns to the Court to Hold Muddy Waters and MedSec Accountable for their Financially Motivated False Statements and Scare Tactics Aimed at Patients with Heart Conditions

ST. PAUL, Minn.--(BUSINESS WIRE)-- St. Jude Medical, Inc. (NYSE:STJ), a global medical device company, announced today that it has filed a lawsuit against Muddy Waters Consulting LLC, Muddy Waters Capital LLC, MedSec Holdings, Ltd., MedSec LLC, and three individual defendants who are principals in these firms, for false statements, false advertising, conspiracy and the related manipulation of the public markets in connection with St. Jude Medical's implantable cardiac management devices. With this action, St. Jude Medical seeks to hold these firms and individuals accountable for their false and misleading tactics, to set the record straight about the security of its devices, and to help cardiac patients and their doctors make informed medical decisions

- In October 2016 an independent 3rd Party verified the claims



**IN THE UNITED STATES DISTRICT COURT
FOR THE DISTRICT OF MINNESOTA**

St. Jude Medical, Inc.,
Plaintiff,
vs.

Muddy Waters Consulting LLC, Muddy
Waters Capital LLC, Carson C. Block,
MedSec Holdings Ltd., MedSec LLC,
Justine Bone and Dr. Hemal M. Nayak,
Defendants.

Case No. 0:16-cv-03002 (DWF/JSM)

**DEFENDANTS' ANSWER AND
DEFENSES**

11. Bishop Fox replicated first-hand many of the attacks described in the Muddy Waters report dated August 25, 2016¹.

- We verified that the Merlin@home devices can be used to reprogram and issue Programmer commands to pacemakers and ICDs
- We replicated an attack that used a modified Merlin@home and a laptop to cause an ICD to deliver a T-wave shock² – the kind of shock used to induce ventricular fibrillation
- We replicated an attack that used a Merlin@home to switch off all therapy on an ICD
- We replicated the battery drain attack
- We gained administrative access to a Merlin@home and a PCS Programmer by following and replicating a set of steps in a document provided by MedSec
- We observed that the wireless ("RF") protocol used by Merlin@homes, PCS Programmers, pacemakers, and ICDs was fundamentally compromised by flaws in its use of cryptography and by St. Jude Medical's inclusion of a "backdoor" that obviated entirely the need to perform cryptographic operations when communicating with a pacemaker or ICD. The backdoor is



ICS-CERT
INDUSTRIAL CONTROL SYSTEMS CYBER EMERGENCY RESPONSE TEAM

HOME ABOUT ICSJWG INFORMATION PRODUCTS TRAINING FAQ

Control Systems

Home

Advisory (ICSMA-17-009-01A)
St. Jude Merlin@home Transmitter Vulnerability (Update A)
Original release date: January 09, 2017 | Last revised: February 06, 2017

Cybersecurity Vulnerabilities Identified in St. Jude Medical's Implantable Cardiac Devices and Merlin@home Transmitter: FDA Safety Communication

[f SHARE](#) [TWEET](#) [in LINKEDIN](#) [PIN IT](#) [EMAIL](#) [PRINT](#)

Date Issued:

January 9, 2017

ST. JUDE MEDICAL ANNOUNCES CYBERSECURITY UPDATES

JANUARY 09, 2017

Company continues to lead the way in advancing cyber security protections in partnership with FDA and ICS-CERT



ICS-CERT

INDUSTRIAL CONTROL SYSTEMS CYBER EMERGENCY RESPONSE TEAM

[HOME](#)[ABOUT](#)[ICSJWG](#)[INFORMATION PRODUCTS](#)[TRAINING](#)[FAQ](#)

Control Systems

Home

Advisory (ICSMA-17-009-01A)

St. Jude Merlin@home Transmitter Vulnerability (Update A)

Original release date: January 09, 2017 | Last revised: February 06, 2017

Cybersecurity Vulnerabilities Identified in St. Jude Medical's Implantable Cardiac Devices and Merlin@home Transmitter: FDA Safety Communication

[f SHARE](#)[TWEET](#)[in LINKEDIN](#)[PIN IT](#)[EMAIL](#)[PRINT](#)


Date Issued:

January 9, 2017

ST. JUDE MEDICAL ANNOUNCES CYBERSECURITY UPDATES

JANUARY 09, 2017

Company continues to lead the way in advancing cyber security protections in partnership with FDA and ICS-CERT

**U.S. FOOD & DRUG
ADMINISTRATION**

A to Z Index | Follow FDA | En Español

Search FDA

Home | Food | Drugs | Medical Devices | Radiation-Emitting Products | Vaccines, Blood & Biologics | Animal & Veterinary | Cosmetics | Tobacco Products

Medical Devices

Home > Medical Devices > Medical Device Safety > Safety Communications

Safety Communications
2018 Safety Communications
2017 Safety Communications

Firmware Update to Address Cybersecurity Vulnerabilities Identified in Abbott's (formerly St. Jude Medical's) Implantable Cardiac Pacemakers: FDA Safety Communication

[f SHARE](#) [TWEET](#) [in LINKEDIN](#) [PIN IT](#) [EMAIL](#) [PRINT](#)

Date Issued

August 29, 2017

Audience

- Patients with a radio frequency (RF)-enabled St. Jude Medical implantable pacemaker
- Caregivers of patients with an RF-enabled St. Jude Medical implantable cardiac pacemaker
- Cardiologists, electrophysiologists, cardiothoracic surgeons, and primary care physicians treating patients with heart failure or heart rhythm problems using an RF-enabled St. Jude Medical implantable cardiac pacemaker

HACK

Rückrufaktion für 500.000 unsichere Herzschrittmacher

Rund eine halbe Million Patienten in den USA müssen ins Krankenhaus - und sich ein [Firmware](#)-Update für ihren Herzschrittmacher aufspielen lassen. Dieser hatte zuvor Befehle per Funk ohne Authentifizierung akzeptiert.

Die US-Lebensmittel- und Medizinbehörde FDA hat einen [Rückruf für rund eine halbe Million Herzschrittmacher angeordnet](#) [↗](#), nachdem erhebliche Sicherheitsmängel nachgewiesen wurden. Die Geräte können manipuliert werden, um etwa die Batterie gezielt zu leeren oder das Tempo des Schrittmachers [zu bestimmen](#) [↗](#).



Herzschrittmacher von St. Jude Medical haben erneut Sicherheitsprobleme. (Bild: St. Jude Medical)

Datum: 31.8.2017, 11:30

Autor: Hauke Gierow

Themen: [Firmware](#), [IoT](#), [Internet](#), [Security](#)

Teilen:



The FDA has reviewed information concerning potential cybersecurity vulnerabilities associated with St. Jude Medical's RF-enabled implantable cardiac pacemakers and has **confirmed that these vulnerabilities, if exploited, could allow an unauthorized user (i.e. someone other than the patient's physician) to access a patient's device using commercially available equipment.** This access could be used to modify programming commands to the implanted pacemaker, which could result in patient harm from rapid battery depletion or administration of inappropriate pacing.

- If it is not secure, it is not safe
- ISO 27001 certificate is not equal „I am secure“
- Lot's of potential attack vectors
- New way of monetising vulnerabilities
- Is it ethical to profit from shorting stock while dropping 0day?

VulnDisclosure - The traditional way

- Billy Rios & Jonathan Butts
- Security assessment of Medtronic Pacemakers
- Disclosed bugs they had discovered in Medtronic's software delivery network
- Discovered a chain of vulnerabilities in Medtronic's infrastructure that an attacker could exploit to control implanted pacemakers remotely, deliver shocks patients don't need or withhold ones they do, and cause real harm.
- Medtronic took 10 months to vet the submission, at which point it opted not to take action to secure the network.



- "Medtronic has **assessed the vulnerabilities per our internal process,**" the company wrote in February. "These findings revealed **no new potential safety risks** based on the existing product security risk assessment. The risks are controlled, and residual risk is acceptable."
- "Medtronic deploys a robust, coordinated disclosure process and **takes seriously all potential cybersecurity vulnerabilities in our products and systems.** ... In the past, WhiteScope, LLC has identified potential vulnerabilities which we have assessed independently and also issued related notifications, and we are not aware of any additional vulnerabilities they have identified at this time."

- Still unpatched vulnerabilities
- Medtronic downplays the findings
- Some vulnerabilities are even neglected

What is the better way?

Vielen Dank!

Alpha Strike Labs GmbH

Mail: tobias.zillner@alphastrike.io

Web: www.alphastrike.io

Mobile: +43 (0) 664 8829 8290

Fax: You think I have fax?