

Table of Contents

Nature of Involvement	1
Credentials.....	1
Information Considered.....	2
Background	3
Summary of Opinion	4
Detail of Opinion.....	6
Merlin@home Emergency Shock and T-wave ("Shock-on-T") Attacks.....	6
Merlin@home Disable Tachy Therapy Attack	12
RF Protocol Vulnerabilities	13
Attainable Distance of RF Communications.....	15
Attacks against Merlin@home	17
Attacks against the PCS Programmer	25
Merlin@home Battery Drain Attack	27
Merlin@home Crash Attack	32
Security by Obscurity	40
Large-Scale Attacks.....	41
Potential Additional Analyses.....	42
References	43
Glossary	46

Nature of Involvement

1. Bishop Fox ("BF") has been retained to provide an expert opinion on behalf of Muddy Waters, LLC, Muddy Waters Capital LLC (collectively "Muddy Waters"), Carson C. Block, MedSec Holdings Ltd., MedSec LLC (collectively "MedSec"), Justine Bone and Dr. Hemal M. Nayak (collectively "Defendants") versus St. Jude Medical, Inc. ("Plaintiff" or "St. Jude Medical") in case no. 16-cv-03003, a lawsuit filed in federal court in Minnesota. For the purposes of this report, I have been asked to provide my opinion in relation to Muddy Waters' claims regarding the security vulnerabilities in specific St. Jude Medical devices.
2. The involvement of Bishop Fox and that of the independent evaluation team we assembled is limited to providing technical evaluation of security matters relating to the St. Jude Medical lawsuit, and no position is held by Bishop Fox or the evaluation team in respect to the Defendants or the Plaintiff. Any statements made by MedSec or Muddy Waters are wholly their own and do not necessarily represent the opinions of Bishop Fox or the independent team.

Credentials

3. I am one of five Partners at Stach & Liu, LLC d/b/a Bishop Fox, a security consulting firm specializing in providing cybersecurity services to Fortune 500, global financial

Preliminary Expert Report of Carl D. Livitt, October 23, 2016

institutions, high-tech startups, medical institutions, media companies and law offices. Bishop Fox was founded in 2005, and I joined the firm in 2007. We have offices in New York, Atlanta, and San Francisco, and we are headquartered in Phoenix, Arizona. We have satellite offices in Colorado, Texas, and Tokyo. My practice focuses on offensive security by providing penetration testing services (break-and-enter hacking), social engineering (people hacking), as well as web application, mobile/cellular, and Internet of Things security. Over the past 9 years at Bishop Fox I have performed security assessments for organizations around the world. A large part of my role is to mentor members of my team in many security disciplines, from circuit board hacking to global-scale penetration test engagements. I was a contributing author to *Hacking Exposed: Web Applications 3rd Edition*¹³ and was a technical advisor for *Network Security Assessment 1st Edition*¹⁴. I have been quoted in several publications, including *USA Today*^{15,16}, *eWeek*^{17,18}, *PCWorld*^{19,20}, *eSecurity Planet*²¹, and I was interviewed on NPR²² in relation to the security of Apple payment systems. I am an active security researcher^{34,35,36} and have published several reports^{23,24,25} on security^{26,27,28} vulnerabilities^{29,30,31} in common software^{32,33}. I was guest speaker on the topic of Responding to Cybersecurity Risks at The Association of Corporate Counsel's annual Compliance and Risk Management Forum in Denver, 2016³⁷. A UK citizen, I immigrated to the USA in 2007. Prior to that I worked for Agenda Security Services, a UK security firm specializing in biomedical and pharmaceutical industries. I worked as a penetration tester; much like Bishop Fox, my job was to hack into computer systems and report my findings. It was in this role that I was invited to be an advisor and guest speaker on cybersecurity matters for a small number of UK police and domestic counter-terrorism agencies, including Special Branch³⁸, the National Extremism Tactical Coordination Unit ("NETCU")³⁹, and the National Counter Terrorism Security Office ("NaCTSO")⁴⁰.

Information Considered

4. My opinions in this case are based on careful analysis and replication of MedSec's research into security vulnerabilities pertaining to St. Jude Medical devices. The analysis was conducted at the MedSec offices in Miami by two consultants from Bishop Fox: myself and Baker Hamilton, Security Analyst at Bishop Fox and licensed physician, specializing in penetration testing and emergency medicine. We were joined by four independent 3rd-party subject matter expert consultants: Drew Porter, founder of Red Mesa, specializing in radio frequency security; Joe Grand, founder of Grand Idea Studio, specializing in hardware security; Nick Selby, Director at Secure Ideas Response Team, specializing in cybersecurity incident response, legal compliance, and forensics; and Matthew D. Green, Assistant Professor at Johns Hopkins University, specializing in cryptography. The analysis was conducted between September 26, 2016 and September 29, 2016. Further analysis of additional security research by MedSec was carried out by myself and Rob Ragan, Managing Security Associate at Bishop Fox, on October 17, 2016 at MedSec's offices in

Miami. All of the St. Jude Medical devices used during our tests were provided by MedSec. During the analysis my team replicated where possible, and using only the technical details provided by MedSec, the research and attacks described by Muddy Waters in its report dated August 25, 2016. The results of our hands-on testing and analysis form the basis of my opinion in this matter, and while my opinions are formed on the basis of work performed by a team of which I was a part, the opinions and conclusions expressed herein are solely my own, with the exception of the opinion pertaining to RF communications, which was provided by Drew Porter, founder of Red Mesa.

Background

5. The scope of work performed by Bishop Fox was to independently evaluate MedSec's security research pertaining to four key parts of the St. Jude Medical cardiac device ecosystem: the PCS Programmer ("Programmer") and induction wand, Merlin@home, Implantable Cardioverter Defibrillator ("ICD"), and pacemaker.

6. Pacemakers are designed to provide therapy that keeps a patient's heart beating according to settings specified by a physician. ICDs can do the same thing, but also provide features that can take corrective action if abnormal heart activity occurs. The Merlin@home is designed to sit by a patient's bed and communicate with pacemakers and ICDs (collectively "cardiac rhythm management devices ('CRMs') or "cardiac devices") using wireless ("RF") technology to extract ("interrogate") medical data and event history from cardiac devices. The Merlin@home also uploads patients' medical data to St. Jude Medical computer systems for further analysis. The Programmer is designed for use by physicians to configure cardiac devices by setting parameters such as pacing rate, to issue emergency shocks, and to configure therapeutic settings that control how ICDs respond to abnormal cardiac activity. An inductive wand is a small device that uses a close proximity (one or two inches) wireless protocol to communicate with a cardiac device; the Programmer uses the inductive wand to wake up cardiac devices prior to communicating with ("interrogating") them.

7. In order to remain objective and impartial, we conducted no research or penetration testing of our own, and we followed written reproduction steps provided by MedSec wherever such documentation existed; where no documentation existed we followed verbal instructions.

8. This report contains significant levels of technical nomenclature. Efforts have been made to describe all of the nomenclature in the glossary at the end of the document.

9. This report also contains detailed technical information regarding reproduction of MedSec's attacks. In an effort to balance the need to provide evidence for my opinions and the need to exercise responsible disclosure, the Defendants and I agreed to redact some of the more sensitive technical details. I am happy to make the redacted details available to the court if ordered to do so by a judge or if compelled to do so by other legal obligation.

Summary of Opinion

10. My overall opinion regarding the security of the St. Jude Medical implantable cardiac device ecosystem is that the security measures I observed do not meet the security requirements of a system responsible for safeguarding life-sustaining equipment implanted in patients. In particular, the wireless protocol used for communication amongst St. Jude Medical cardiac devices has serious security vulnerabilities that make it possible to convert Merlin@home devices into weapons capable of disabling therapeutic care and delivering shocks to patients at distances of 10 feet, a range that could be extended using off-the-shelf parts to modify Merlin@home units. I found that Muddy Waters' and MedSec's statements regarding security issues in the St. Jude Medical implant ecosystem were, by and large, accurate.

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

- a. We verified that the Merlin@home devices can be used to reprogram and issue Programmer commands to pacemakers and ICDs
- b. 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
- c. We replicated an attack that used a Merlin@home to switch off all therapy on an ICD
- d. We replicated the battery drain attack
- e. 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
- f. 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 essentially a secret code that permits anyone who knows it to issue therapeutic programming commands to St. Jude Medical cardiac devices. Assuming one has access to a Programmer, the backdoor is relatively easy to discover and understand.

12. It is common in the cybersecurity industry to refer to “a chain of exploits”⁴¹ that describes how one successful attack often makes it possible to conduct another attack, which makes a third attack possible, ad infinitum. A similar situation was found with the St. Jude Medical PCS Programmer, Merlin@home, ICD, and pacemaker devices: by exploiting the general pattern of missing or ineffective security controls, the MedSec researchers have shown how to take a standard Merlin@home and reconfigure it to act as a weapon that can be used to attack patients with implanted St. Jude Medical cardiac devices.

13. For example, there is the potential for a chained attack in which a Merlin@home would be used to first turn off therapeutic functions (“tachy therapy”)⁷ of an ICD before issuing a T-wave shock⁸ to a patient’s heart. I understand this would cause the patient to enter ventricular fibrillation⁹, which can lead to cardiac arrest. It is also my understanding that an ICD with its tachy therapy disabled would make no attempt to deliver therapy in case of a medical emergency⁷.

14. Some of the features and technology that make it possible for the Merlin@home to monitor patient devices while patients sleep are exactly the same features exploited by MedSec in their research. For example, the underlying channel (“protocol”) over which the Merlin@home, Programmer, and cardiac devices communicate is fundamentally flawed in both its design and implementation, making it possible to repurpose Merlin@home devices to emulate a Programmer and issue, for example, shocks to patients.

15. During testing, I observed that Merlin@home units can communicate with cardiac devices at a distance of approximately 11 ft (Bishop Fox measured 10 ft under controlled conditions) without requiring any interaction or even knowledge on the part of the patient. Calculations show that it would be possible to extend this range by adding commercially available antennae to the Merlin@home, which would facilitate communication with cardiac devices at a distance of approximately 45 ft; further calculations showed that if carefully configured radio communication systems (“Software Defined Radios” or “SDRs”) were used instead of Merlin@home devices, the attacks could plausibly be carried out from a distance of approximately 100 ft (see “Detail of Opinion”, below, for details), although no such SDR attack has been demonstrated at the time of writing and more precisely tailored calculations would need to be made; the current calculations for SDR distances were made using reasonable hypothetical numbers.

16. Bishop Fox validated that further vulnerabilities in the Merlin@home and the Programmer enabled MedSec to get administrative “root” (i.e. complete administrative) control of both devices with relative ease and little requirement for sophisticated

techniques; having root on the devices was MedSec's first step towards reverse engineering the St. Jude Medical RF command protocol used to control and configure the delivery of therapeutic care to cardiac devices.

17. A system's security requirements should always reflect the system's exposure to risk, and, because of this, one would expect to see a high degree of sophistication in the security measures applied to the Merlin@home device ecosystem. This appears not to be the case with the Merlin@home and associated components, as during testing Bishop Fox observed fundamental security issues such as a flawed RF protocol, exposed JTAG headers and clearly labeled UART connectors on the Merlin@home circuit board, hard-coded cryptographic keys, and lack of basic protections against reverse engineering and exploitation. Additionally, based on information provided by MedSec, there is credible evidence to suggest that well-documented serious vulnerabilities such as "buffer overflows" are present in Merlin@home software. These vulnerabilities are not mitigated by anti-exploitation countermeasures such as ASLR or non-executable stacks, and there is evidence that basic security precautions such as "stripping binaries" have not been taken.

Detail of Opinion

Merlin@home Emergency Shock and T-wave ("Shock-on-T") Attacks

18. The following statement was made in the St. Jude Complaint:

19. *"[...] changes to therapeutic parameter settings on patients' devices require use of the in-clinic programming device and cannot be performed by the Merlin@home transmitters."*

(Complaint, paragraph 42)

20. The above statement is demonstrably false, as shown in multiple tests documented herein, all of which rely upon Merlin@home transmitters for key functionality.

21. MedSec demonstrated, and the Bishop Fox ("BF") team reproduced and verified, two different remote shock attacks against ICDs that used Merlin@home devices to send shock commands to the ICDs. The attacks were developed by MedSec and conducted by running their exploit software on a Merlin@home to deliver both emergency shocks and T-wave shocks to ICDs. MedSec also demonstrated that the same method can successfully make the ICD's internal vibration motor turn on and off.

22. MedSec first performed the emergency shock demonstration using a rooted Merlin@home running version "8.2-rev2" of the St. Jude Medical software ("firmware"), which MedSec stated was updated on Tuesday, September 27, 2016.

23. BF used a different Merlin@home loaded with version "8.1.1 PR_8.11.2" of the firmware, and a different ICD to reproduce the emergency shock attack. The Merlin@home that the BF team used was the same one used for the local hardware root attacks from earlier BF experiments. This was a device that MedSec stated had not been tampered with until it was given to us. The BF team verified that the tamper-evident label covering a screw hole was intact at the time the BF team received it.

24. The ICD used for the BF verification of the emergency shock attack was the same one the BF team used for the battery drain tests (used at the completion of BF battery drain tests).

25. Due to the unavailability of ICD leads, the on-site team was not able to measure the specific voltage of the shock provided by the ICD in situ during the emergency shock attack. However, the PCS Programmer displayed in its "HV Charging & Non-sustained V Oversensing Details" log that the ICD had indeed issued a manual charge of ">845 volts". This is an indication that the device's internal capacitor was charged for that level, and the Programmer's log indicated that the charge had been delivered. Based on the Programmer log, I have no reason to doubt that the shock was delivered.

26. The Bishop Fox team arrived at MedSec's headquarters at 9 am EST on Thursday September 29, 2016, and met the MedSec team, who had prepared the attacks for the vibrate and emergency shock commands via a Merlin@home unit. The on-site team observed visually, took photographs and video, and captured the RF traffic exchanged between the Merlin@home and the ICD during the demonstration. The shock-on-T and disable tachy therapy attacks were verified by Bishop Fox on October 17, 2016.

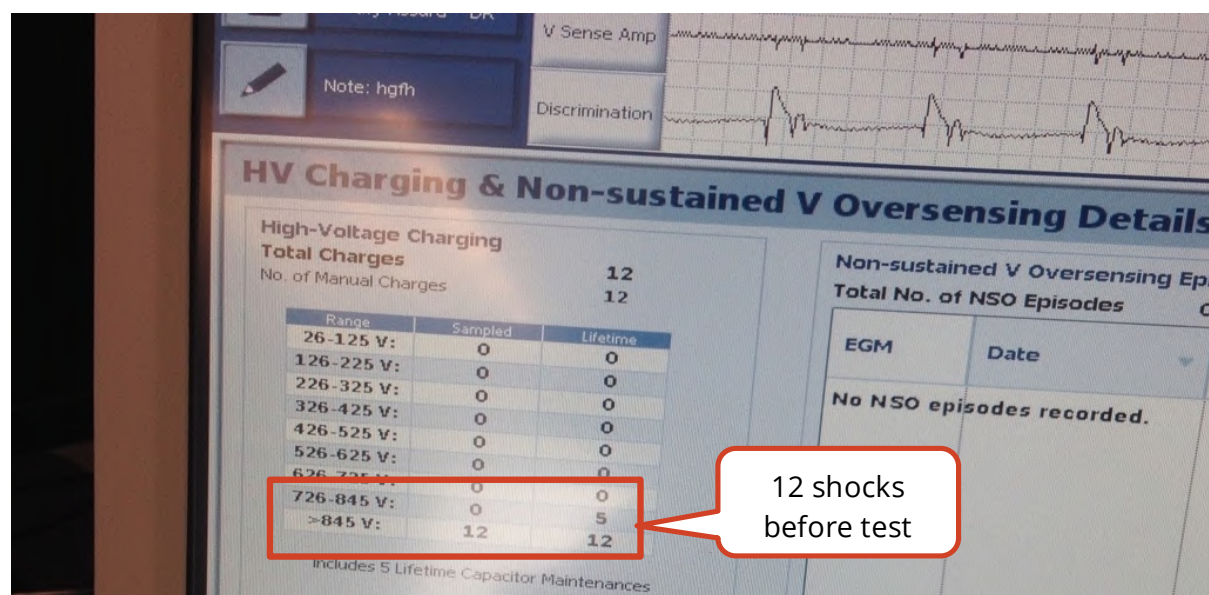
27. The MedSec team used a Linux virtual machine ("VM") on a MacBook Pro laptop, which was connected to a rooted Merlin@home by an Ethernet crossover cable. The ICD used for the emergency shock demonstration was a Fortify Assura DR 2357-40C, with serial number [REDACTED].

28. The MedSec team first demonstrated how their attack allowed the Merlin@home to interact with the ICD using a "calculated key" to authenticate commands. The calculated key is derived using the repurposed Java library described under "RF Protocol Vulnerabilities", above, and is used by ICDs to verify that incoming commands are sent by a legitimate Programmer. The Merlin@home was used to transmit to the ICD a "vibrate" command. The device vibrated. This was repeated several times.

29. The MedSec team used the same technique to send a command to perform an “emergency shock”, which is described in the St. Jude Medical Bradycardia and Tachycardia Devices Help Manual⁵ as follows:

30. *“The currently programmed DeFT Response™ Technology Settings (Shock Waveform) (page 97) are used for the shock. If the Zone Configuration (page 75) settings Off, the DeFT Response settings are set to a biphasic waveform with a 65% fixed tilt. The shock is delivered synchronously with the next sensed event. If sensed event does not occur, the shock is delivered after the next bradycardia pacing time-out. If bradycardia pacing is disabled, the shock is delivered as if the device were pacing at 30 bpm. The delivery of an emergency shock triggers the storage of an EGM. If the capacitors have started charging and the telemetry link is lost, the capacitors continue to charge and the emergency shock is delivered. After the shock is delivered, the detection counters are reinitialized and the device is ready to detect a new tachyarrhythmia episode.”*

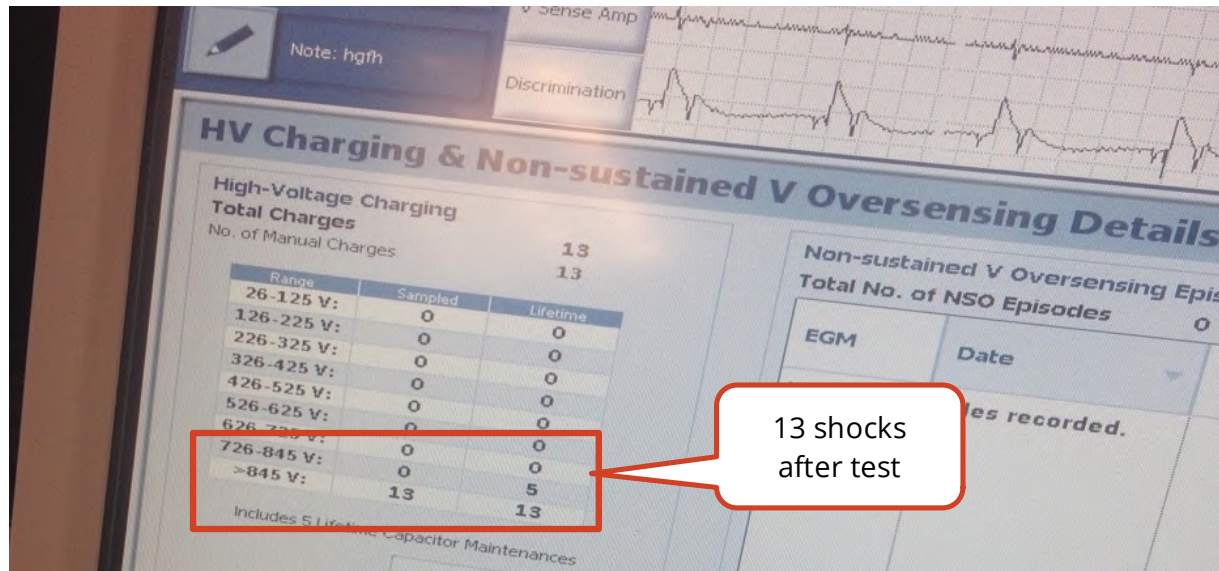
31. Before commencement of the attack, the MedSec team used a PCS Programmer to interrogate the ICD, and an inventory was taken of the existing episode history. The Programmer provides several screens on which emergency shock history is shown. The “HV Charging & Non-sustained V Oversensing Details” log showed the total number of high voltage charges issued by the ICD; there were 12 recorded episodes:



32. Pre-test history of high voltage charges on target ICD

Preliminary Expert Report of Carl D. Livitt, October 23, 2016

33. After running the exploit, feedback from the exploit script indicated that the shock had been delivered. The MedSec team then re-interrogated the ICD, and another inventory was taken of the episode history. The total number of high voltage charges on the ICD was observed to have increased from 12 to 13:

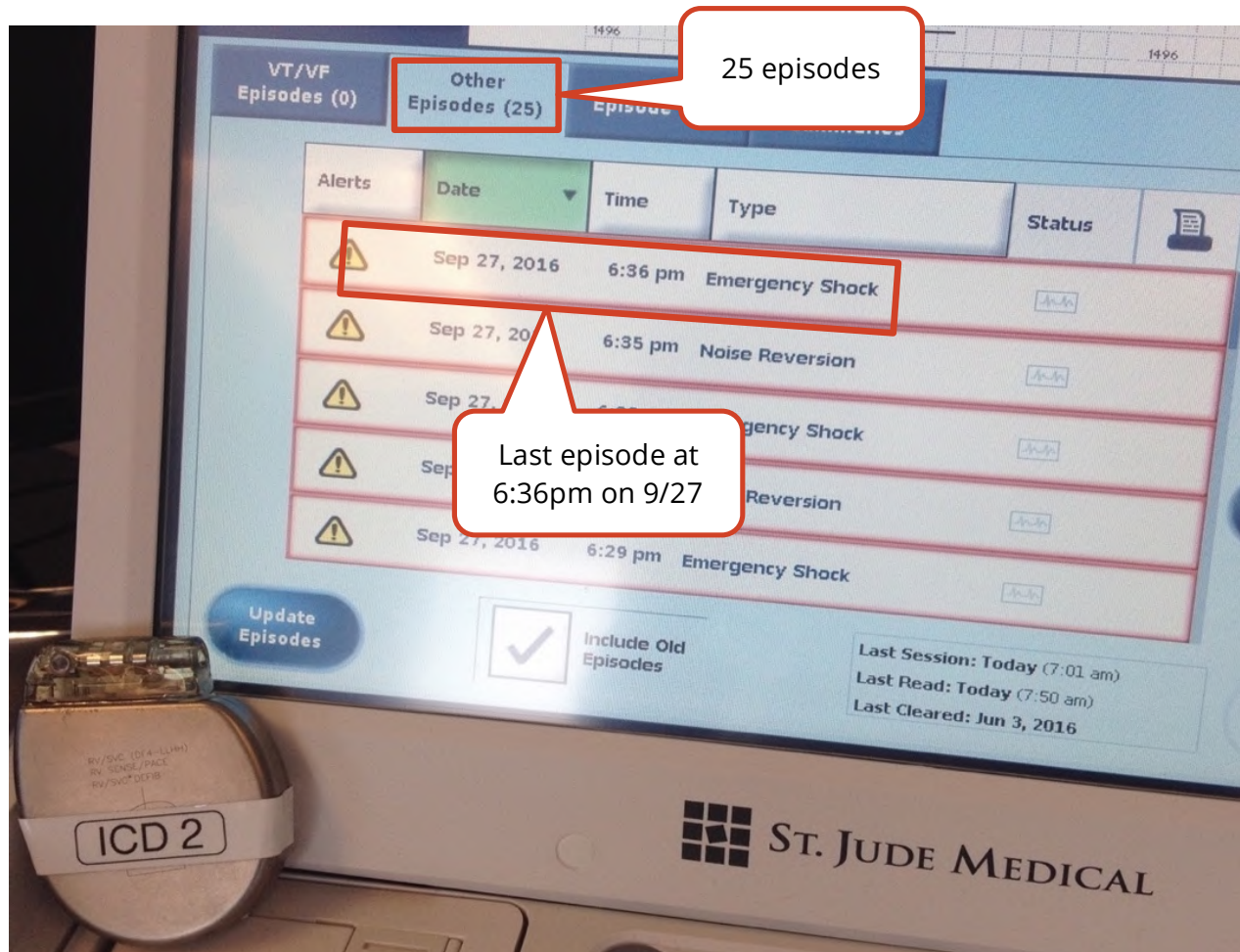


34. Additional high voltage charge on the target ICD after running the exploit

35. The attack was then reproduced and verified by the Bishop Fox team using a completely different rooted Merlin@home running firmware version "8.1.1 PR_8.11.2". The device had been rooted by Bishop Fox on Monday, September 26, 2016. Prior to being rooted, Bishop Fox verified that the Merlin@home had an intact tamper-evident label.

36. A different ICD was used in the Bishop Fox tests than was used in the MedSec demonstrations. In our tests, an Ellipse VR1311-36Q with serial number [REDACTED] was the target. Before the attack began, the ICD was interrogated using the Programmer, and an inventory was taken of the date and time of the last delivered emergency shock. It reported September 27, 2016 at 6:36pm:

Preliminary Expert Report of Carl D. Livitt, October 23, 2016

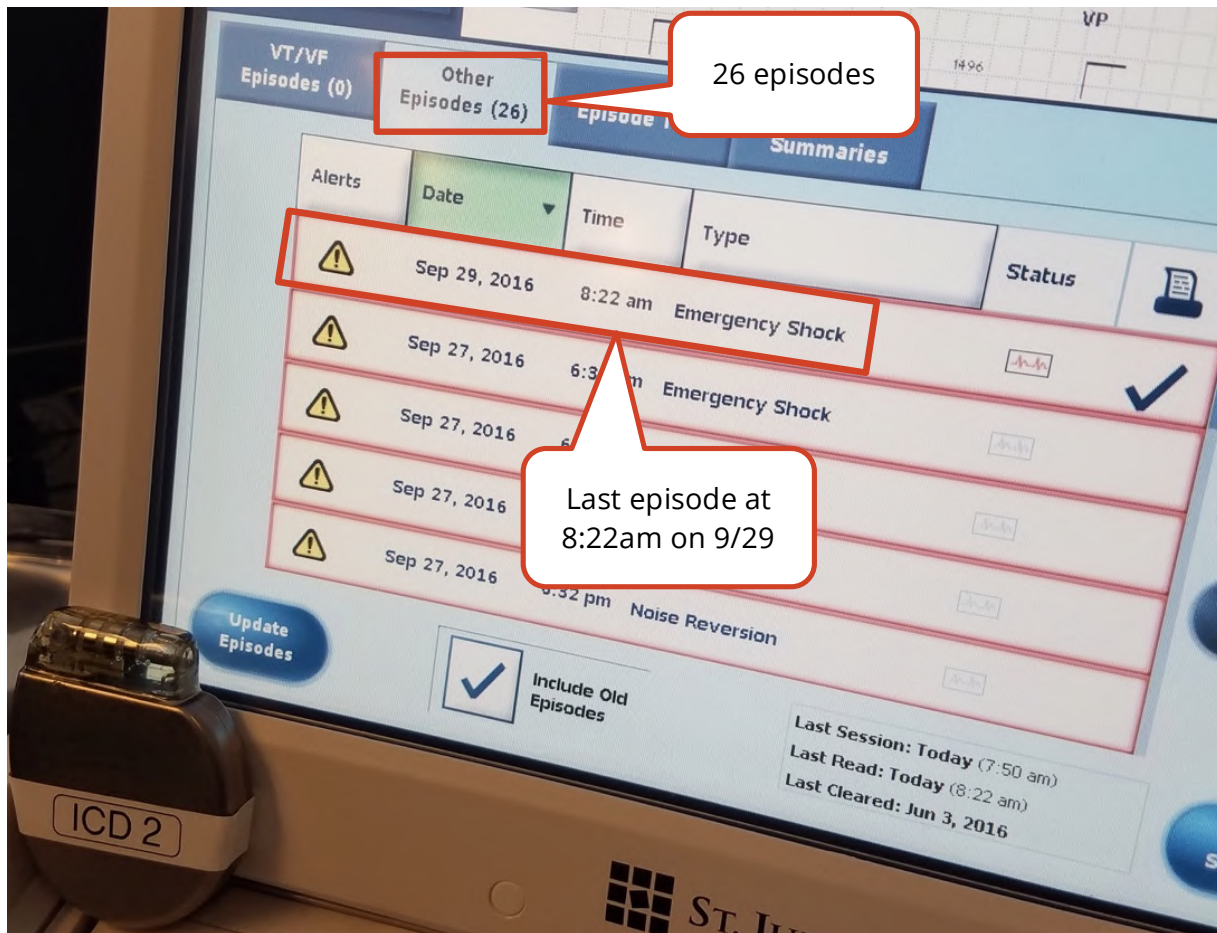


37. Emergency shock record before the attack

38. To launch the attack, the Bishop Fox team replicated MedSec's setup, using a MacBook pro laptop owned by Bishop Fox connected to the Merlin@home by an Ethernet cable, and, like the MedSec setup, the exploit was run inside a Linux VM. The first version of the exploit code provided to Bishop Fox by the MedSec researchers was designed to exploit a Merlin@home to send a "vibrate" command to the ICD. Because the variant of the exploit used for this test contained neither the backdoor key (see "RF Protocol Vulnerabilities", below) nor a calculated key, the attack failed.

39. MedSec then provided an exploit that used the backdoor key (also known as the "universal key") to send commands from the Merlin@home to the ICD. Using the same procedure as before, the Bishop Fox team used the exploit to issue an emergency shock command to the ICD. The attack was launched and the exploit indicated that the shock had been successful. The ICD was interrogated using the Programmer a final time. It showed that a new shock had been delivered:

Preliminary Expert Report of Carl D. Livitt, October 23, 2016



40. Emergency shock record after the attack

41. The time of the shock was reported as 8:22am on September 29, 2016, which was an hour behind the actual time of 9:22am. This was due to the Programmer's clock being incorrect, not any other factor. This concluded the reproduction and verification of the remote emergency shock exploit.

42. Bishop Fox's verification of the shock-on-T attack used the same Merlin@home and laptop setup as the emergency shock attack, the only difference being that instead of sending an emergency shock command to an ICD, a shock-on-T command was sent instead. The ICD under test was an Ellipse VR™ with serial number [REDACTED]. This test was performed on October 17, 2016. The attack took 18 seconds and, like the emergency shock attack, the Programmer was used to verify that the shock had been delivered. The shock-on-T is described as follows in the St. Jude Medical Bradycardia and Tachycardia Devices Help Manual⁶:

"Shock-on-T. Delivers overdrive pacing followed by a properly timed high-voltage shock (V. Fibber Test only)."

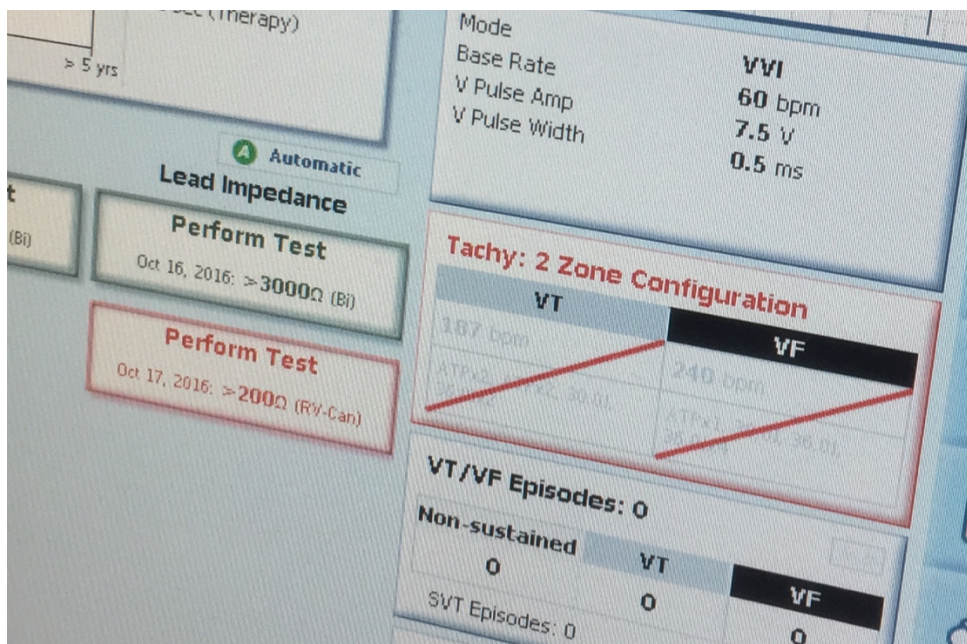
43. During reproduction of the shock-on-T attack, leads were made available for the ICD under test, and a multimeter was used to verify that the ICD emitted a voltage spike approximately 18 seconds after the shock-on-T command had been sent from the Merlin@home to the ICD. This was consistent with the data observed on the Programmer.

Merlin@home Disable Tachy Therapy Attack

44. In an attack that follows the same pattern as the two shock attacks described above, it is possible to cause a Merlin@home to send a command that turns off the therapeutic functions ("tachy therapy") of an ICD; based on information provided in the St. Jude Medical Bradycardia and Tachycardia Devices Help Manual, it is my understanding that when tachy therapy is in the disabled state, an ICD does not deliver therapy in case of an arrhythmic episode⁷:

"[...]disable VT/VF detection and therapy delivery without affecting other programmed parameters. This is useful prior to noise-generating medical procedures such as electrocautery, where the device could detect noise from the equipment, interpret it as an arrhythmic episode, and deliver therapy. When therapy is disabled, diagnostic data are not updated or cleared."

45. After executing the attack, the Programmer clearly showed that the ICD was no longer providing tachy therapy by displaying red cross-hatches across the relevant sections of the screen:



46. Disabled tachy therapy

47. By combining this attack and the shock-on-T attack it appears that it would be possible to first disable the therapeutic functions of the ICD and then issue a shock-on-T to trigger ventricular fibrillation in the patient⁸; it is my understanding that this can lead to cardiac arrest⁹, and it also my understanding that in the event of an ICD's tachy therapy being disabled, the ICD will not delivery therapy to recover from the episode⁷. Based on this understanding, I believe that this chain of exploits could present a life-threatening scenario.

RF Protocol Vulnerabilities

48. Carson Block made the following statement on Bloomberg TV:

49. *"[the St. Jude. Medical] communication protocol has been compromised"* (Bloomberg TV, August 25, 2016)

50. Relatedly, the following claim was made by St. Jude Medical in their Complaint:

51. *"[St. Jude Medical] and independent analysts determined that St. Jude's device technology was not compromised and that Block's statements were demonstrably incorrect."* (Complaint, paragraph 83)

52. Mr. Block's statement appears to be credible, not only because of weak cryptography, discussed below, but due to the fact that the protocol contains a backdoor, also discussed below, which by definition compromises the protocol.

53. The following analysis is based on discussions with MedSec researchers, hands-on validation, and a brief review of Java source code files extracted from a Programmer by MedSec. A rigorous cryptanalysis of the St. Jude Medical RF protocol was not undertaken.

54. The St. Jude Medical RF protocol implements a form of cryptographic verification that consists of a specially calculated 3-byte value included within the command payload sent by the Programmer (or by the Merlin@home in the case of an active attack) to a cardiac device. Ordinarily, if the cardiac device receives a command in which the 3-byte value has not been correctly calculated, the command is rejected with an error.

55. There are several major issues with this implementation; there may be more. The first issue is that St. Jude Medical included a fixed 3-byte "backdoor" key within the Programmer and cardiac devices that, if used in place of a correctly calculated 3-byte value,

is accepted as valid by the device. The 3-byte hexadecimal value for the backdoor value is [REDACTED]. The presence of this backdoor compromises the security of the protocol by (a) negating the need to calculate the correct value, (b) simplifying the process of issuing commands to a cardiac device, and (c) distributing a backdoor that is built into cardiac devices and is very difficult, perhaps impossible, to revoke or disable.

56. Another issue is that the St. Jude Medical RF protocol relies for security on a weakened variant of the RSA algorithm¹⁰, a widely used and peer reviewed encryption algorithm based on a mathematical primitive called “modular exponentiation”, and which derives its security from the practical difficulty of factoring the product of two large prime numbers. The St. Jude Medical RSA variant truncates all of its output to 3 bytes (24 bits) in length, which erodes security. It is this insecurely derived 3-byte value that is checked by cardiac devices to verify that they are communicating with an approved device, such as a PCS Programmer. A full discussion of cryptographic operations and nomenclature is beyond the scope of this document, however the glossary contains a starting point for further reading.

57. The third major issue is the extremely small “key space” of a 3-byte value, for which there are only 16,777,216 possible values. This may seem like a large number, but in computing terms this is in fact a tiny number that, based on my experience with other such small key spaces, could potentially be determined (or “brute forced”) by writing an exploit to try every possible value until the backdoor value was discovered; the brute force attack could be done against any ICD or pacemaker, and need not be implanted in a patient. It is not known if ICDs and pacemakers implement countermeasures to mitigate brute force attacks, nor is it known how long such an attack might take.

58. Another issue is that regardless of the backdoor and the cryptographic weaknesses, the 3-byte value was calculated by a Java library, taken from the Programmer, that was repurposed by MedSec to perform the necessary calculations without ever having to write an exploit, use the backdoor, or conduct a brute force search.

59. Based on all of the issues identified in the protocol, it is my opinion that describing the protocol as compromised is credible. Based on my observations so far, it is likely that a thorough cryptanalysis of the St. Jude Medical RF protocol would reveal further issues.

Attainable Distance of RF Communications

60. The “Attainable Distance of RF Communications” opinion is provided by Drew Porter, founder of Red Mesa.

61. The Merlin@home system operates at both 2.45GHz and 402MHz-405MHz, also known as the Medical Implant Communications Service band (“MICS band” or “400MHz radio”). The system has two antennas for the 400MHz radio and one for the 2.45GHz antenna. The remote wake up feature is activated using the 2.45GHz radio, and data is exchanged using the 400MHz radios.

62. Measurements and experiments performed by Bishop Fox using a simulated in vivo⁴ scenario showed that unmodified Merlin@home units could communicate with cardiac devices at a distance of 10ft.

63. Calculations show that modifications could be made to a Merlin@home to achieve communication over greater distances. The formulas used to perform the calculations were provided by the MedSec team and have been reviewed by the Bishop Fox team. While these formulas do not account for every possible environmental factor, they are sufficiently accurate to provide a reasonable level of confidence in the results. To find the approximate range of a Merlin@home or SDR, the following formula is used, where R = range in meters:

$$R = \frac{\lambda_0}{4\pi} \left(\frac{P_T G_T G_R}{P_R L_B L_R L_T} \right)^{1/\gamma}$$

P_R: The receive power

P_T: The transmit power

G_T: The transmit antenna gain

G_R: The receive antenna gain

λ₀: The wavelength corresponding to the frequency of the transmission

L_B: Loss due to human body

L_R: Loss on receiver (matching, cables, connectors, etc.)

L_T: Loss on transmitter (matching, cables, connectors, etc.)

γ: Path Loss Exponent

64. There are two main limiting factors to increasing the range of the RF attacks: (a) the communicable distance of the 2.45GHz radio is less than that of the 400MHz radios, and (b) the signal strength of responses sent from pacemakers and ICDs to Merlin@home devices is weak due to the small amplifier and antenna in the cardiac devices.

Preliminary Expert Report of Carl D. Livitt, October 23, 2016

65. The 2.45GHz band is used only to wake up cardiac devices. No data is exchanged at 2.45GHz and therefore attention need only be paid to improving the 2.45GHz transmit strength of the Merlin@home unit, not the 2.45GHz receiver sensitivity. The 400MHz band is bidirectional, which means that the Merlin@home or SDR must be able to receive as well as transmit data to/from a cardiac device at 400MHz. This is a more difficult proposition than unidirectional 2.45GHz communication.

66. This first set of calculations shows the effective 2.45GHz range of (a) an unmodified Merlin@home, (b) a Merlin@home with 24dBi antenna, and (c) a modified Merlin@home with a 24dBi antenna and 44.7dBm power amplifier. The value "R" on the last row represents the approximate distance in meters that a Merlin@home could realistically achieve when transmitting to a cardiac device in the 2.45GHz band:

Unmodified Scenario				Antenna-Only Scenario				Antenna+Amplifier Scenario			
Log-Va [Units] Values		[Units]		Log-Vals [Units] Values		[Units]		Log-Vals		[Units] Values	[Units]
P _R	-80 dBm	1.00E-08 mW		P _R	-80 dBm	1.00E-08 mW		P _R	-80 dBm	1.00E-08 mW	
P _T	23 dBm	2.00E+02 mW		P _T	23 dBm	2.00E+02 mW		P _T	44.7 dBm	2.95E+04 mW	
G _T	3 dBi	2.00		G _T	24 dBi	251.19		G _T	24 dBi	251.19	
G _R	0 dBi	1.00		G _R	0 dBi	1.00		G _R	0 dBi	1.00	
L _B	17.22 dB	52.72		L _B	17.22 dB	52.72		L _B	17.22 dB	52.72	
L _T	6 dB	3.98		L _T	6 dB	3.98		L _T	6 dB	3.98	
L _R	6 dB	3.98		L _R	6 dB	3.98		L _R	6 dB	3.98	
λ ₀		0.13 m		λ ₀		0.13 m		λ ₀		0.13 m	
Y		3.00		Y		3.00		Y		3.00	
R	3.61 m			R	18.07 m			R	95.58 m		

67. Distances attainable by Merlin@home in the 2.45GHz band

68. Based on these calculations, the approximate distances over which an ICD or pacemaker could be woken up over 2.45GHz are as follows:

- Unmodified Merlin@home: 3.6m (11.8ft)
- Modified Merlin@home with a 24dBi antenna: 18m (59.2ft)
- Modified Merlin@home with a 24dBi antenna and a 44.7dBm amplifier: 95.6m (313.6ft)

69. The approximate distances over which a cardiac device and a Merlin@home could communicate in the 400MHz band were calculated as follows:

Preliminary Expert Report of Carl D. Livitt, October 23, 2016

Unmodified Scenario			Antenna-Only Scenario			Antenna+Improved Receiver Scenario		
Log-Va	[Units]	Values	Log-Vals	[Units]	Values	Log-Vals	[Units]	Values
P _R	-99 dBm	1.26E-10 mW	P _R	-99 dBm	1.26E-10 mW	P _R	-115 dBm	3.16E-12 mW
P _T	-16 dBm	2.51E-02 mW	P _T	-16 dBm	2.51E-02 mW	P _T	-16 dBm	2.51E-02 mW
G _T	0 dBi	1.00	G _T	0 dBi	1.00	G _T	0 dBi	1.00
G _R	2 dBi	1.58	G _R	10 dBi	10.00	G _R	10 dBi	10.00
L _B	9.92 dB	9.82	L _B	9.92 dB	9.82	L _B	9.92 dB	9.82
L _T	6 dB	3.98	L _T	6 dB	3.98	L _T	6 dB	3.98
L _R	6 dB	3.98	L _R	6 dB	3.98	L _R	6 dB	3.98
λ ₀		0.75 m	λ ₀		0.75 m	λ ₀		0.75 m
Y		3.00	Y		3.00	Y		3.00
R		7.56 m	R		13.97 m	R		47.70 m

70. Distances attainable by the Merlin@home in the 400MHz band

71. The approximate distances for two-way communication at 400MHz are therefore as follows:

- Unmodified Merlin@home: 7.5m (24.8ft)
- Modified Merlin@home with 10dBi antenna: 13.9m (45.8ft)
- SDR with 10dBi antenna: 47.7m (156.5ft)

72. Given that bidirectional communication between cardiac devices and the Merlin@home is an essential part of any attack, the limiting factor becomes the smallest distance at which all of the radios involved can perform their intended functions.

- Assuming an unmodified Merlin@home, the maximum communicable distance is expected to be approximately 11.8ft. Bishop Fox verified a distance of 10ft in simulated in vivo conditions.
- Assuming modified antennae on a Merlin@home, the approximate maximum effective distance over which communication could expect to be conducted is 45.8ft. Bishop Fox did not test this scenario.
- Assuming an SDR, range could be increased significantly. However, it should be noted that no such attack has been developed or tested, and the figures would need to be calculated using data pertaining to specific SDRs and antennae instead of the theoretical values used in the calculations.

Attacks against Merlin@home

73. The St. Jude Medical complaint makes the following statement:

74. *"Operating system access controls protect the Remote Transmitter from unauthorized access, and its lack of built-in programming helps ensure therapy selection is provided only by and as directed by the patient's physician."* (Complaint, paragraph 42)

75. I found both of the points made in this statement to be false: access controls do not protect the transmitter from unauthorized access, as will be shown below. The statement

Preliminary Expert Report of Carl D. Livitt, October 23, 2016

that the Merlin@home's "lack of built-in programming helps ensure therapy selection is provided only by and as directed by the patient's physician" is demonstrably incorrect. I verified that built-in components of the Merlin@home units are in fact currently a prerequisite for MedSec's therapy-altering attacks; with additional work it is feasible that the same attacks could be implemented using SDRs with no dependency on St. Jude Medical hardware or software.

76. Carson Block made the claim on Bloomberg TV on August 25, 2016 that there is "*low hanging fruit for attackers to exploit*" in the Merlin@home components and protocols. "Low hanging fruit" is a common term in cybersecurity and is used to refer to vulnerabilities in a system that are easily discovered and easily exploited. Based on the information presented below, and based on Bishop Fox's experience reproducing MedSec's research, I believe Block's statement to be credible. For example:

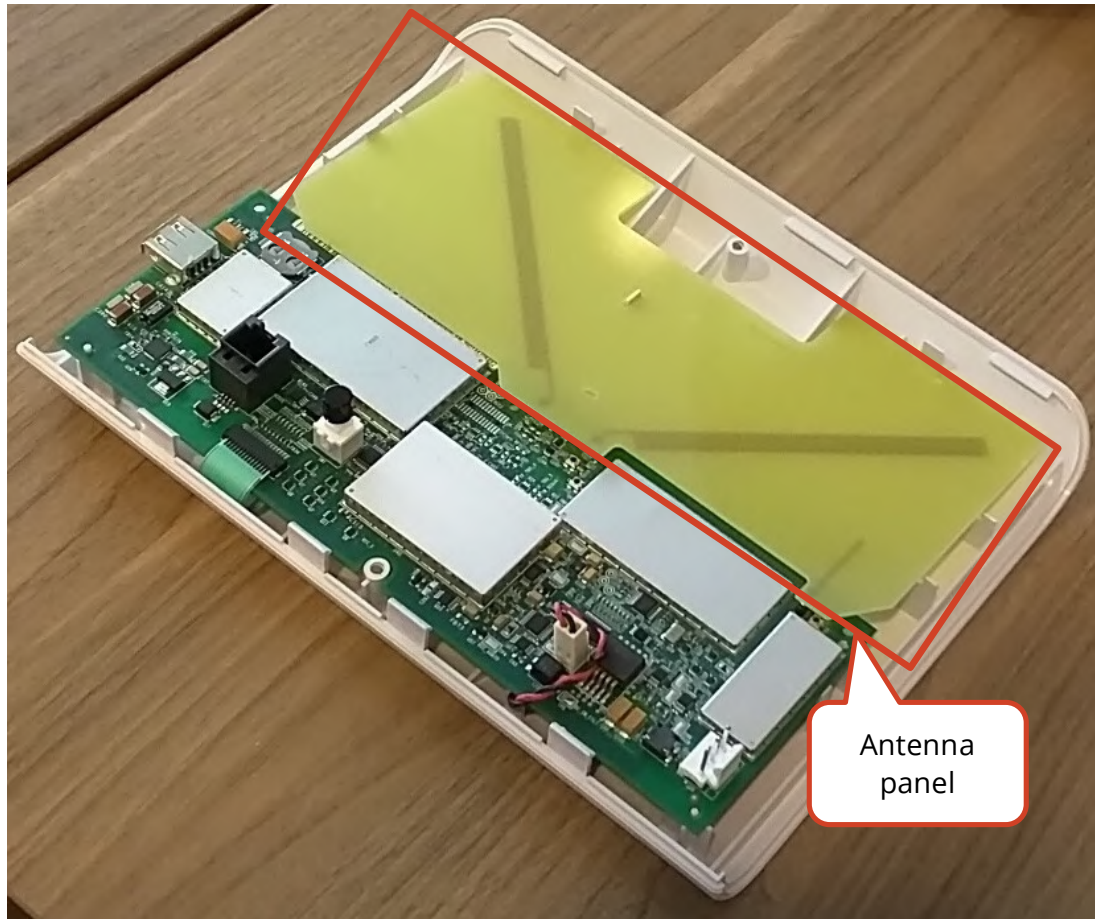
77. The procedure to defeat the "operating system access controls" was procedural, quick, and typical for a Linux-based embedded system. The procedure leverages techniques that are common practice, and each is well-documented in academic and industry literature/presentations. The process is made easier by the standard JTAG headers and clearly labeled UART connections on the Merlin@home.

78. The Bishop Fox team began the test with a boxed Merlin@home, which MedSec reported it had acquired from eBay. Upon opening the Merlin@home box, the non-standard screw head (a Torx bit) on the rear of the device was observed to be in place and the tamper-evident label covered the screw at the middle top of the rear of the device:



79. Tamper-evident label shows that the unit's interior had not been tampered with

80. The BF team then removed the screws and outer casing and unfastened the power supply cable from the rear outer casing. The team observed components shielded by metal coverings and an antenna array panel:



81. Antenna and shielded components

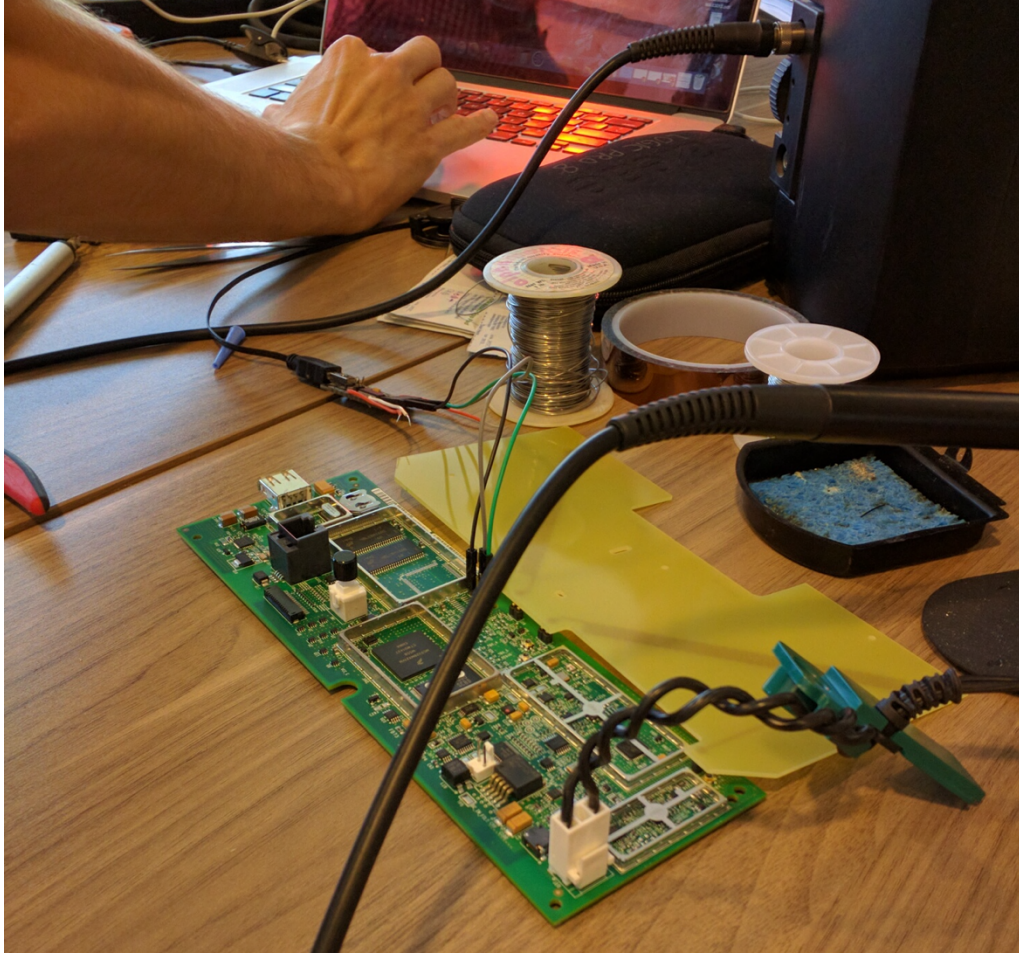
82. The BF team removed the metal shields to expose all components on the circuit board, and after removing the antenna and unplugging the keypad and speaker connectors from the Merlin@home's main circuit board ("motherboard"), the Bishop Fox team freed the motherboard entirely:



83. Motherboard removed from outer casing

84. Once the board was exposed, opened and ready to be connected, wires were soldered into the UART test points identified on the circuit board with silkscreen markings and as described in the MedSec documentation: GND, VCC3, DBG_TXD, DBG_RXD.

85. The antenna was placed back onto its connectors on the motherboard, and a USB-to-Serial adapter was connected to the GND, DBG_TXD, and DBG_RXD pins and plugged into a computer running the CoolTerm terminal program:



86. Connection through UART interface

87. The Merlin@home was powered on and the BF team observed start-up messages being sent from the Merlin@home to CoolTerm via the serial port. As expected on newer versions of the Merlin@home (per MedSec), the messages eventually stopped, the system was unresponsive to the team's key presses, and no root shell was provided. Access to a root shell would have given immediate administrative control over the Merlin@home. The following output shows the last messages received at boot:

```
Post device verification...
Time taken by POST : [0.069000] seconds
nand_init: manuf=0x000000EC device=0x000000F1
scanning for bad blocks...
nand_check_blocks: nand_read_page() failed, addr=[REDACTED]
nand_check_blocks: nand_read_page() failed, addr=[REDACTED]
nand_check_blocks: nand_read_page() failed, addr=[REDACTED]
...omitted for brevity...
blob release: d20081014_platform_4_16
Memory map:
[REDACTED] @ [REDACTED] (32 MB)
ram_post executing...

Data Bus Test
```

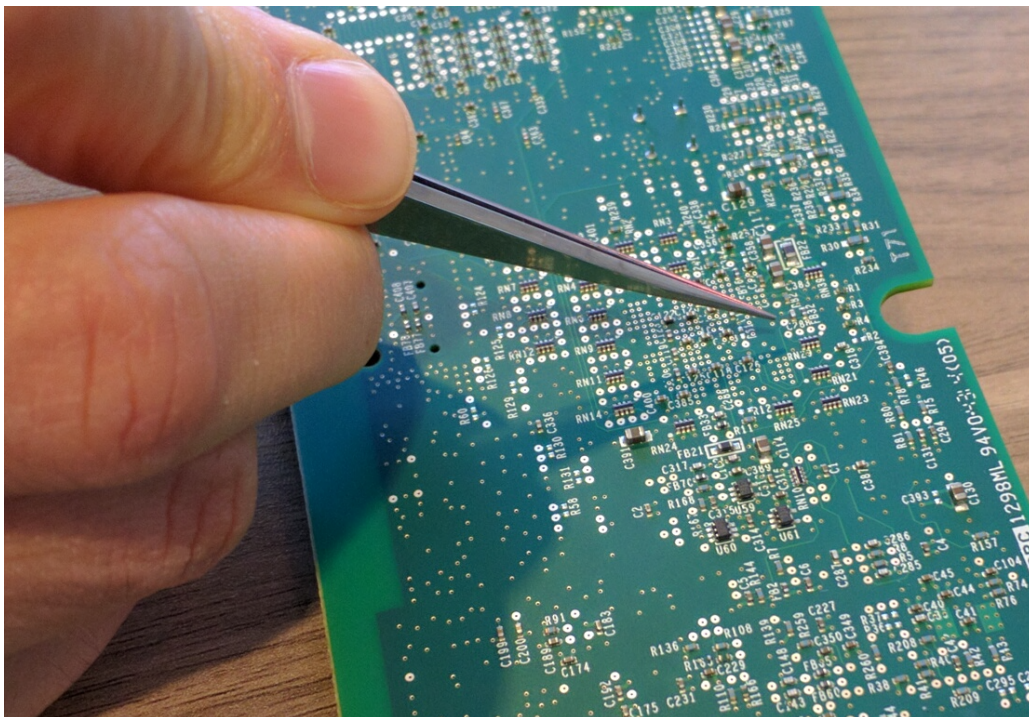
Preliminary Expert Report of Carl D. Livitt, October 23, 2016

Address Bus Test
Data Qualifier Test
Device Test

[REDACTED]status_next, board type = RF board revision = (3)
[REDACTED]

88. No command prompt was presented via the UART connection

89. The next step was to follow the MedSec documentation to achieve JTAG access in order to bypass the access control presented through the UART interface. The BF team reset the system and unplugged the power. Using a photograph in the MedSec documentation, the test points used by MedSec to connect to JTAG were identified on the back side of the board. Unpopulated solder pads, which are points on a circuit board intended for future additions of components, were found on the front side of the motherboard near the UART test points with a footprint that is consistent with a common JTAG debugging interface. The Bishop Fox team chose to forgo use of the JTAG interface and instead used test points on the back of the board to exactly replicate the original attack by MedSec. The team soldered wires directly to the test points and soldered the other end of the wires to a double-row male header.



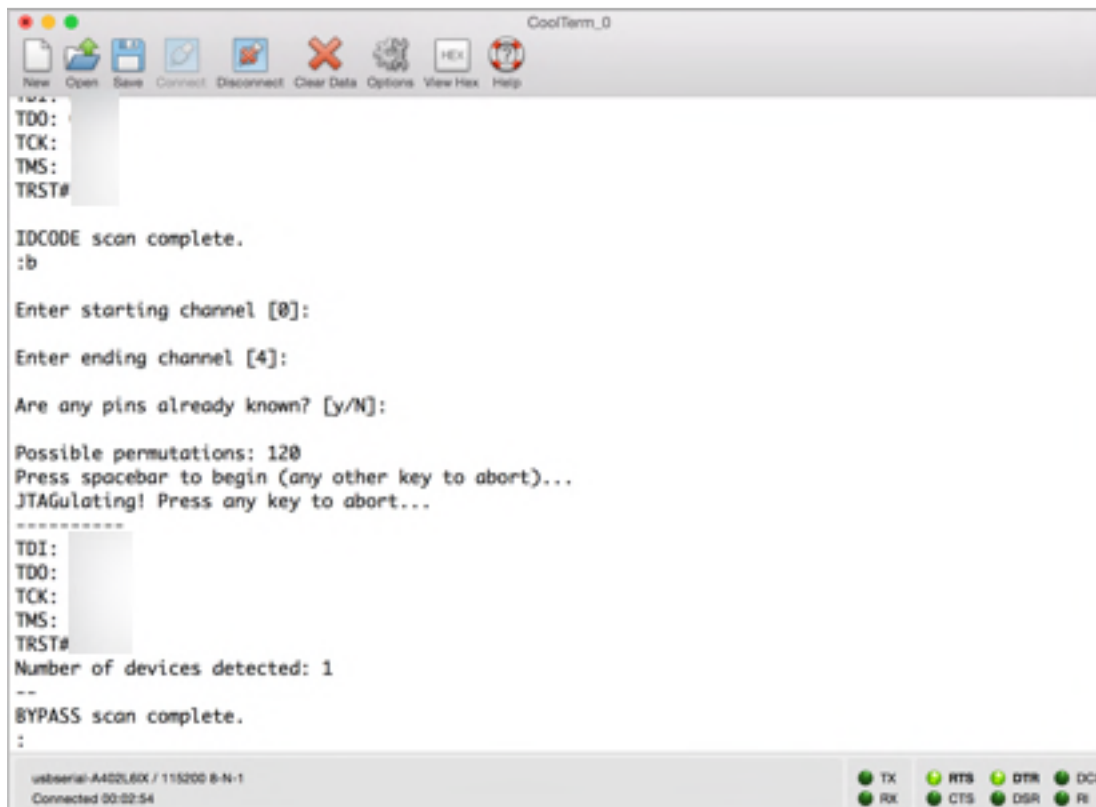
90. Team member indicating location of JTAG pins on the motherboard

91. The pins were attached to a JTAGulator (a hardware hacking tool) channels 0 through 4 in order to confirm the JTAG connections (labelled as #TRST, TMS, TDI, TCK, TDO, GND). The team first examined MedSec's JTAGulator to discover the version of the

Preliminary Expert Report of Carl D. Livitt, October 23, 2016

firmware (1.3) used on that tool. Then the team connected the Merlin@home to a JTAGulator running the same version of the firmware (1.3) as the MedSec JTAGulator.

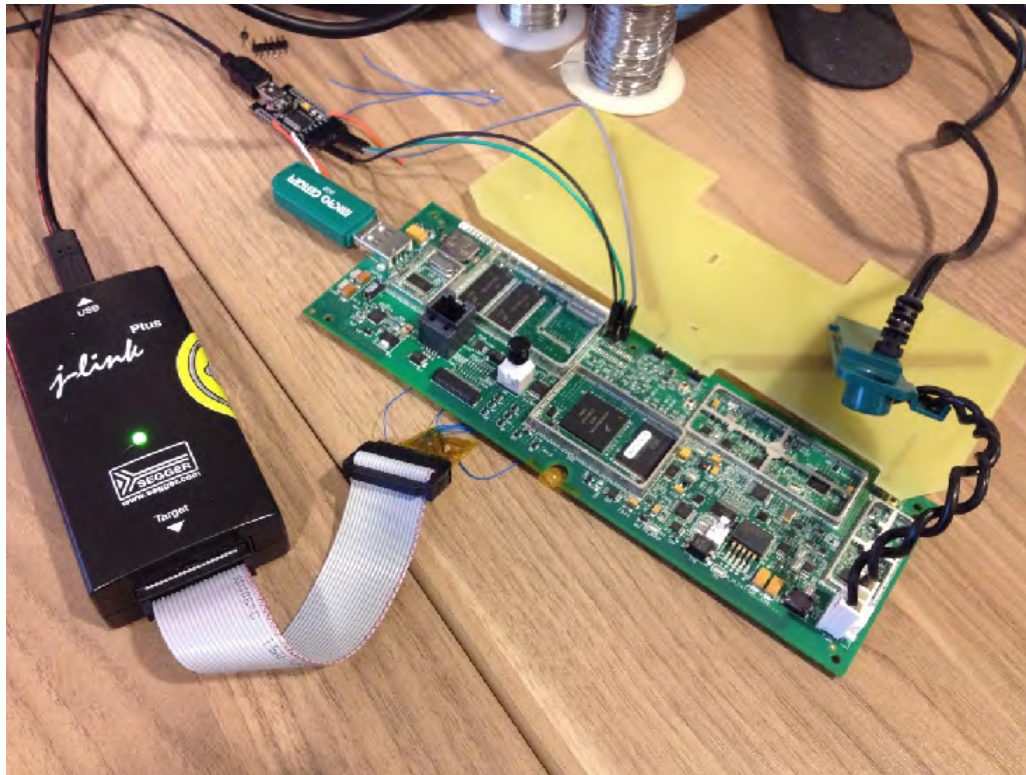
92. The JTAGulator's IDCODE scan and BYPASS scan commands were used to enumerate the JTAG pin connections and confirm successful detection of a processor on the Merlin@home motherboard. Having detected the processor, it was possible to interact with it and control the behavior of the Merlin@home's operating system.



93. JTAGulator results confirming JTAG detection (pin numbers have been redacted)

94. With the JTAG connections successfully tested and identified, the next step was to attach to the Segger J-Link Plus JTAG Debug Probe. While doing so, the BF team determined that MedSec did not mention in the instructions they provided to Bishop Fox that a wired connection to [REDACTED] on the JTAG connector was also required for successful interfacing with the Segger tool. MedSec told the Bishop Fox team that this was consistent with their results, and confirmed that MedSec had connected it to achieve their results, but that it had been unintentionally omitted from the instructions. The final JTAG pinout has been redacted from this report.

95. The Merlin@home device was then connected to the Segger tool:



96. Connection of Merlin motherboard to Segger J-Link JTAG interface

97. The Segger J-Link Command Link software was run and the device connected using the "connect" command. The MC9S328 CPU chip on the Merlin responded with a Device ID of [REDACTED]. This confirmed that the Bishop Fox team had successfully attached via the J-Link interface to the processor on the Merlin@home motherboard.

98. The following process was replicated based on verbal commands from MedSec. The black reboot button on the board was pressed and the "halt" command sent to the Merlin@home after the Device Test started during the system boot-up (displayed via the UART interface). After halting the CPU, the Bishop Fox team executed:

```
mem32 [REDACTED],10
```

99. to retrieve some memory locations and ensure that memory could be correctly read. The team then ran the following command to change the location of the CPU's program counter and manipulate the flow control of the program such that the bootloader, the software responsible for booting the Linux operating system of the Merlin@home, was presented to CoolTerm via the serial port:

```
setpc [REDACTED]
```

100. After typing "go," the system resumed operation and presented the prompt of the "Blob" bootloader prompt.

101. The next steps were to reconfigure the Linux startup settings in order to cause the Merlin@home to present a root shell (i.e. complete administrative access) on the serial port. The steps to perform this were replicated based on verbal instructions from MedSec researchers and have been redacted from this report. Once the steps were followed, the Merlin@home restarted and gave the Bishop Fox team full root shell access via the serial port.

102. The next step was to program persistence into the boot sequence, so that the bootloader always presented a root shell at startup. This permits further administrative action without requiring the use of the JTAG interface each time the Merlin@home is switched on. The Bishop Fox team followed basic Linux configuration steps provided by MedSec to rewrite the startup configuration and to add a new user to the system. The configuration was saved and when the system was rebooted, the Bishop Fox team confirmed that a persistent root shell was enabled. The exact nature of the modifications are redacted from this report.

The Bishop Fox team further verified that it was possible to extract the contents of the permanent storage memory ("Flash" memory) on the Merlin@home motherboard through the JTAG interface. The process is also known as "dumping the firmware" and was replicated based on verbal commands from MedSec using the Segger J-Link tool.

103. The version of firmware identified on the compromised device was as follows:

```
VERSION=EX2000 v8.1.1 PR_8.11.2
Linux (none) 3.0.94-iGL_Kirin_tantobasic_V1.0 #1 PREEMPT Thu Feb 5 17:14:19 PST 2015
armv5tej1 GNU/Linux
```

This concluded verification of the local root exploits against the Merlin@home device.

Attacks against the PCS Programmer

104. The Muddy Waters report dated August 25, 2016, made the following claim:

105. *"the physician office programmers are not well secured either... if the applications are reverse engineered it could potentially allow an attacker to emulate the full functionality of the programmer"*

106. In my opinion, this statement is credible. The first part of the statement, that Programmers are not well secured, is demonstrated below. The second part of the statement, that Programmer applications could be reverse engineered to allow emulation of the Programmer's full functionality, is demonstrably correct and is proven by attacks like the remote shock attacks, which were constructed using information, such as the RF protocol backdoor, gleaned by reverse engineered applications on the Programmer.

107. The PCS Programmers are not physically secured against someone with physical access to the Programmer, which are essentially repackaged PC computers that contain a removable hard drive. By removing the hard drive, connecting it to a laptop, modifying specific Linux configuration parameters, and replacing the hard drive back into the Programmer, Bishop Fox replicated the MedSec research that showed how to connect to the Programmer over the network and obtain a root shell (via "SSH"). The process takes approximately 15 minutes and is described below.

108. The Programmer's outer case was removed, and its hard disk was extracted and connected to a laptop using an IDE to USB adapter:



109. Hard drive from the PCS Programmer connected to USB/IDE adapter

110. By connecting the hard drive to a laptop using the USB/IDE adapter, the files on the drive were made accessible to the laptop. The startup script [REDACTED] was modified to assign a static IP address to a network adapter plugged into the Programmer; the IP address made it possible to connect to the programmer via a network.

111. When using IPv4 (as opposed to IPv6, the most recent version of the internet communications protocol), the Linux Netfilter firewall prevents incoming connections to the Programmer from the network; the firewall rules were changed during the testing process to allow SSH access to the Programmer. MedSec informed us that there are no firewall rules for IPv6, leaving the Programmer open to IPv6 traffic. MedSec provided Bishop Fox with screenshots illustrating this, however firewall rules were not evaluated by Bishop Fox.

112. After modifying the Programmer's startup files, the hard drive was reinstalled in the Programmer, and an external network adapter was inserted. The team then connected to the Programmer over the network through SSH, and successfully logged in with the root user credentials provided by MedSec's researchers (user: root, password: [REDACTED]).

113. At this point I concluded that it was straightforward to obtain root access to a St. Jude Medical PCS Programmer.

Merlin@home Battery Drain Attack

114. The Muddy Waters report dated August 25, 2016, made the following claim regarding a battery drain attack against cardiac devices:

115. *"MedSec has demonstrated a battery drain attack that generates signals from the Merlin@home device to run down batteries in Cardiac Devices at a greatly accelerated rate. The attack version MedSec tested depleted the batteries at approximately three percent of capacity per 24-hour period."*

116. The Bishop Fox team reproduced and verified the attack. It was confirmed that a battery drain attack can be successfully mounted via a Merlin@home device that drains the battery of an ICD at a rate of approximately three percent (3%) per 24-hour period. Because the patient into whom an ICD has been implanted sleeps near to the Merlin@home device, based on these results, such a battery drain attack could completely deplete the battery of an ICD in 33 days if left to run continuously. Given a sleep period of eight hours, an attack conducted against a recumbent patient with a fully charged ICD would take approximately three months.

117. Two Merlin@home transmitters, rooted in the method described in "Attacks Against Merlin@home Device", above, were loaded with exploits written by MedSec to perform the battery drain attack.

118. The attacks were mounted between September 28 and 29, 2016 in a conference room at the MedSec headquarters in Miami, Florida. The control device was placed within three Faraday bags (a bag, within a bag, within a bag, specially designed to shield the contents from radio waves) and kept outside the testing area. Faraday bags prevent RF transmissions from reaching devices inside the bag. The target device was placed next to the Merlin@home units for the duration of the test, except for periods of approximately 5 minutes where the ICDs were temporarily taken to a PCS Programmer to perform battery level tests before being returned to their original places. No in vivo simulation was used during this particular test, although the RF distance tests were conducted using in vivo simulation.

119. The test was performed with two ICDs, both marked as Ellipse VR model CD1311-36Q High Voltage Cans.

120. Before starting the experiment, both the control ("ICD 1") and the target ("ICD 2") were interrogated using the Programmer and the current remaining capacity to ERI (Elective Replacement Interval) and serial number were noted. A rooted Merlin@home was loaded with custom code provided by MedSec (`launch_drain.sh` and supporting files) that provided the battery drain attack functionality. This code was designed to query all devices within range, attempt to interrogate the device(s), and then disconnect. If multiple devices are within range, then multiple devices would be interrogated and therefore subject to the attack. During set up of the test, the Bishop Fox team observed that multiple devices could be detected using the rooted Merlin@home and MedSec's exploit code.

121. The control device was triple-bagged (placed into a small Faraday bag, then into a larger one, and into a yet larger one; all three were properly sealed using the Ziploc) and placed in an environment away from the test setup. The on-site team confirmed that the Merlin@home device used for the test was not able to detect the control.

122. The test was configured in the same fashion as the original MedSec battery drain attack. ICD 2 was placed approximately 2 inches from the locally rooted Merlin@home:



123. Placement of device next to modified Merlin@home during battery drain test

124. ICD 2 was exposed to free air on a lab bench and, as stated, was not subject to anything that would simulate being implanted within a human body (e.g., no barrier of meat, gel, etc.). MedSec's battery drain attack is designed to wake up the target ICD with the 2.4GHz data transmission, interrogate the device via 400MHz communication, and then close the session. The process was repeated continuously in a loop.

125. At each measurement interval, ICD 2 was removed from the test setup and, along with the control device, ICD 1, was interrogated by the Programmer and the remaining capacity to ERI was recorded. ICD 2 was then placed back into the test setup at its previous location and ICD 1 was re-bagged. Photos of the Programmer screen and ICDs were taken at each interval.

126. The test was conducted for a total elapsed time of 35 hours and 18 minutes. The following shows a table of Remaining Capacity to ERI (Elective Replacement) and Time for the control device:

Date	Time	Remaining Capacity to ERI	Elapsed Time (HH:MM)
09/27/2016	2130ET	38%	Pre-test
09/28/2016	0925ET	38%	11:26
09/28/2016	1453ET	38%	16:58
09/28/2016	2112ET	38%	23:17

Preliminary Expert Report of Carl D. Livitt, October 23, 2016

09/29/2016

0915ET

38%

35:20

127. Control device: "ICD 1", serial number [REDACTED]

128. This is a similar graph showing Remaining Capacity to ERI (Elective Replacement) and Time for ICD 2:

Date	Time	Remaining Capacity to ERI	Elapsed Time (HH:MM)
09/27/2016	2130ET	57%	Pre-test
09/28/2016	0923ET	55%	11:28
09/28/2016	1451ET	55%	16:56
09/28/2016	2113ET	54%	23:18
09/29/2016	0913ET	53%	35:18

129. Test device: "ICD 2", serial number [REDACTED]

130. The Programmer returned the Remaining Capacity to ERI in single-digit resolution as a whole integer. It is unknown whether the percentage is on the upper end or lower end of the number due to the lack of numeric precision provided by the Programmer.

131. In summary, the control device lost no detectable battery charge. By contrast, ICD 2 lost 4% of its battery charge during the same period.

132. St. Jude Medical made several statements in relation to Muddy Waters' claims regarding battery drain attacks:

133. *"Those statements concerning the tests performed by MedSec are false and misleading because Defendants omit, among other things, that the tests were not representative of real world conditions and did not account for the significant differences in tests performed on devices on a lab bench versus conditions simulating an implanted CRM Device."* (Complaint, paragraph 69)

134. Bishop Fox tested the battery drain exploit under simulated real world conditions during the RF range tests, and observed that the attack was functional at a distance of 10ft using a standard Merlin@home. The process involved using a rooted Merlin@home onto

Preliminary Expert Report of Carl D. Livitt, October 23, 2016

which the battery drain exploit provided by MedSec was loaded. The Merlin@home used its standard antenna and no additional amplification or other hardware modifications. A 10ft measuring tape was placed on the MedSec hallway floor from the location of the Merlin@home, and the Bishop Fox researchers stood at the 10ft mark. The ICD was placed into a plastic Ziploc bag, covered at its radio-facing side with 1cm of bacon, and at the rear (non-radio facing) side 4 cm of 85% lean hamburger meat. The ICD was completely covered during the test:



135. ICD placed in bag containing meat to simulate human tissue during RF test

136. The testing was conducted in a hallway within the MedSec offices between 12:45pm and approximately 1:30pm on September 28, 2016.

137. The bag containing the radio was held by a researcher at a distance of ten feet from the radio. The send_wakeup portion of the battery drain attack script was invoked, and the computer was monitored:

Preliminary Expert Report of Carl D. Livitt, October 23, 2016

```

root@(none):~/Send_wakeup/Drain_PMA ./send_wakeup
Setting receive timeout to: 1
Connecting to 127.0.0.1:1213
Thu Jan 1 00:05:18 1970
IMD Found: XXXXX58
root@(none):~/Send_wakeup/Drain_PMA ./send_wakeup
Setting receive timeout to: 1
Connecting to 127.0.0.1:1213
Thu Jan 1 00:07:50 1970
IMD Found: XXXXX58      Devices Found: 1

      ITERATIONS: 1

Thu Jan 1 00:08:30 1970
Devices Found: 0

      ITERATIONS: 2
Thu Jan 1 00:09:10 1970
IMD Found: XXXXX58      Devices Found: 1

      ITERATIONS: 3
Thu Jan 1 00:09:53 1970

CTRL-A Z for help | 115200 8N1 | NOR | Minicom 2.7 | VT102 | OFFLINE | ttyUSB0

```

138. Battery drain application sending wakeup commands to ICD at 10 feet

139. The Merlin immediately identified the ICD device at a distance of ten feet, a feat photographed and recorded on video by the Bishop Fox team.

140. St. Jude also claims the devices *"are designed to trigger a vibratory or auditory alert for the patient indicating a low battery and doctors can also monitor battery life through remote monitoring and in person office visits. The patient alert is typically triggered when there are still months of use before the battery can no longer operate the CRM Device. Accordingly, there is no credible threat that the device will stop operating and harm the patient due to battery depletion as Defendants misrepresented."* (Complaint, paragraph 86(j))

141. I disagree that "there is no credible threat" due to the battery drain attack. The attack works, it is reliable, repeatable, and works under real world conditions. "Months of use before the battery can no longer operate" only applies under normal circumstances; under an attack, the time to complete depletion would be considerably less.

Merlin@home Crash Attack

142. Muddy Waters made the following statement in their report dated August 25, 2016:

143. *"In many cases, the Crash Attack made the Cardiac Device completely unresponsive to interrogations from Merlin@home devices and Merlin programmers. It was therefore impossible*

Preliminary Expert Report of Carl D. Livitt, October 23, 2016

to tell whether, and how the Cardiac Devices, are functioning. MedSec strongly suspects they were in many cases "bricked" – i.e., made to be non-functional. "

The following statement was made by St. Jude Medical in response to the above statement:

144. *"MedSec claimed that it had caused a pacemaker to stop operating because MedSec was unable to detect activity in the pacemaker using a St. Jude programming device. However, MedSec's transmission of radio waves during its purported hack attack had caused the pacemaker they appear to have used to lock out their transmissions – a feature of the design that effectively blocked MedSec's efforts while allowing the pacemaker to continue to function. In their purported test, Defendants misrepresented a pacemaker design feature which protects battery life and enhances battery longevity – another security feature – as if it were evidence of a fatal flaw. Other safeguards in CRM Devices can cause them to revert to a 'Safe Mode,' under certain circumstances, including when battery life drops below certain levels. The 'Safe Mode' causes the CRM Devices to revert to default hardware settings as a further protection against, among other things, low battery life."* (Complaint, paragraph 86(h))

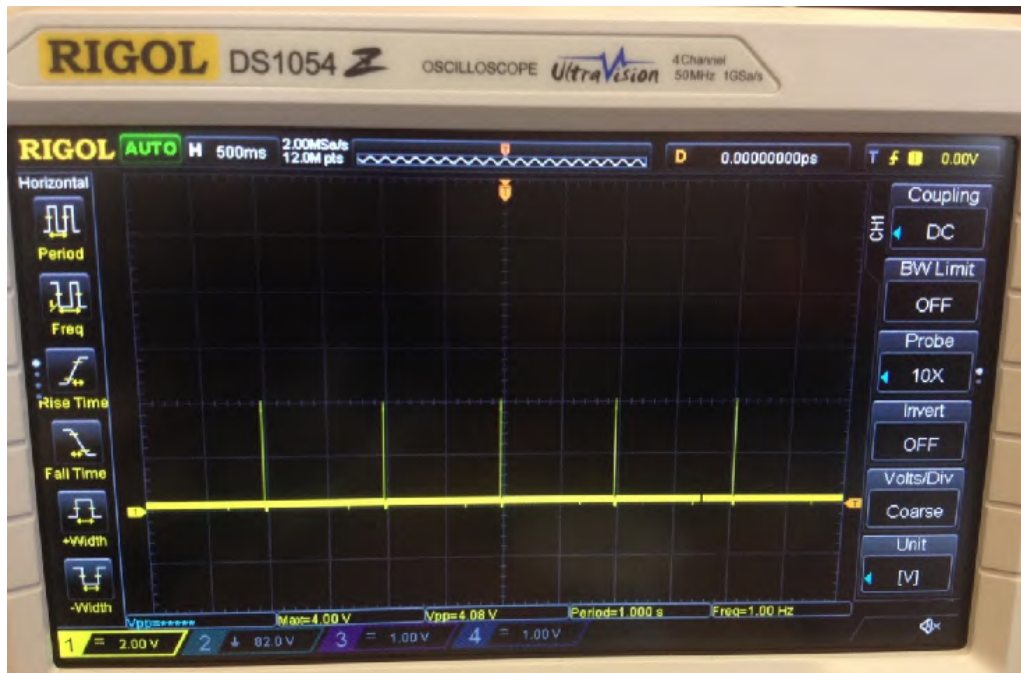
145. St. Jude Medical's statement that MedSec *"had caused a pacemaker to stop operating"* is misleading because that is not what was claimed in the Muddy Waters report; the actual claim was that *"the Crash Attack made the Cardiac Device completely unresponsive to interrogations from Merlin@home devices and Merlin programmers."* The key distinction here is that "Cardiac Devices" covers both pacemakers and ICDs, whereas St. Jude Medical mentioned only pacemakers, something that Bishop Fox found to be an important omission during our tests. In addition, the Muddy Waters report does not say the implantable devices "stopped operating," but rather were "completely unresponsive to interrogations."

146. Bishop Fox tested MedSec's crash attacks against an ICD and a pacemaker. Both tests showed some form of behavioral change in the cardiac devices, described in detail below.

147. When testing against an ICD, Bishop Fox observed one attack that was not at all successful, and communication continued as normal. On two other attempts against the ICD, it was impossible to interrogate the ICD with the Programmer immediately after the attack. Yet, on subsequent attempts at interrogation, the Programmer interacted with the ICD as normal. It is my opinion that the effects of the attack can be unpredictable and may vary according to factors such as starting state of the device.

Preliminary Expert Report of Carl D. Livitt, October 23, 2016

148. The ICD test was conducted using an ICD labeled "I1." A battery measurement was taken using the Programmer before starting the test, giving a response of less than 1% remaining capacity to ERI (Elective Replacement Interval). The V Bipolar line from the ICD was connected to the oscilloscope and a baseline pacing waveform of 60bps was observed with a peak voltage of the pacing at approximately 4V:



149. ICD pacing 60bps at 4V prior to crash attack

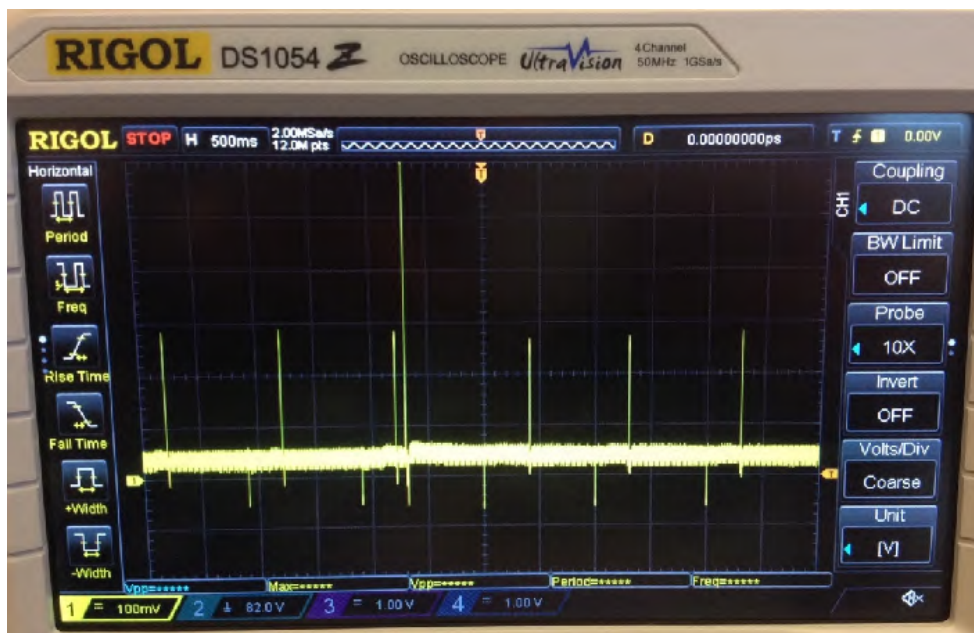
150. Somewhere between 1 hour and 1 hour and 57 minutes after launching the crash attack exploit, the on-site team observed on the oscilloscope that the ICD's V Bipolar waveform had reduced to a peak voltage of approximately 280mV:

Preliminary Expert Report of Carl D. Livitt, October 23, 2016



151. ICD pacing 60bps at reduced voltage following crash attack

152. The pacing was still operating at 60bps, but the output voltage level was much lower. At two separate intervals while observing the oscilloscope screen, there were two spikes measuring over 500mV (the signal went out of range on the oscilloscope screen, so actual maximum was unable to be determined):

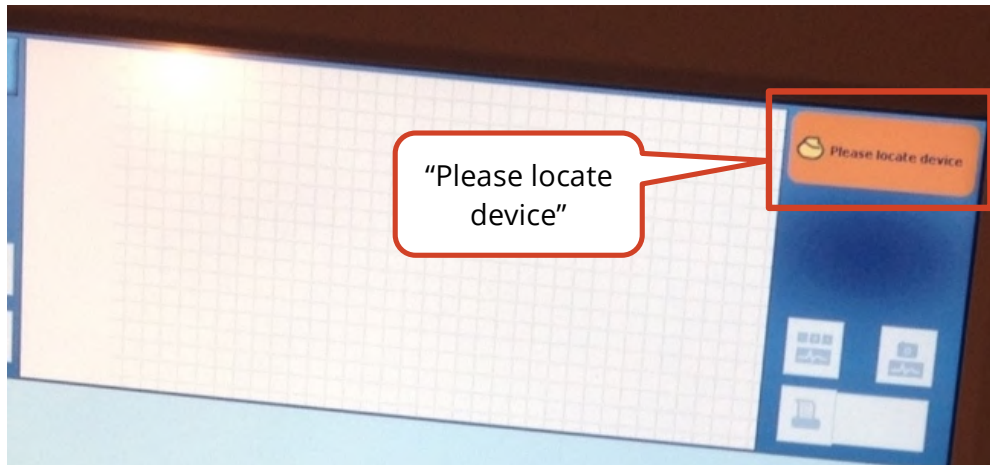


153. Irregular pacing spikes observed following crash attack

Preliminary Expert Report of Carl D. Livitt, October 23, 2016

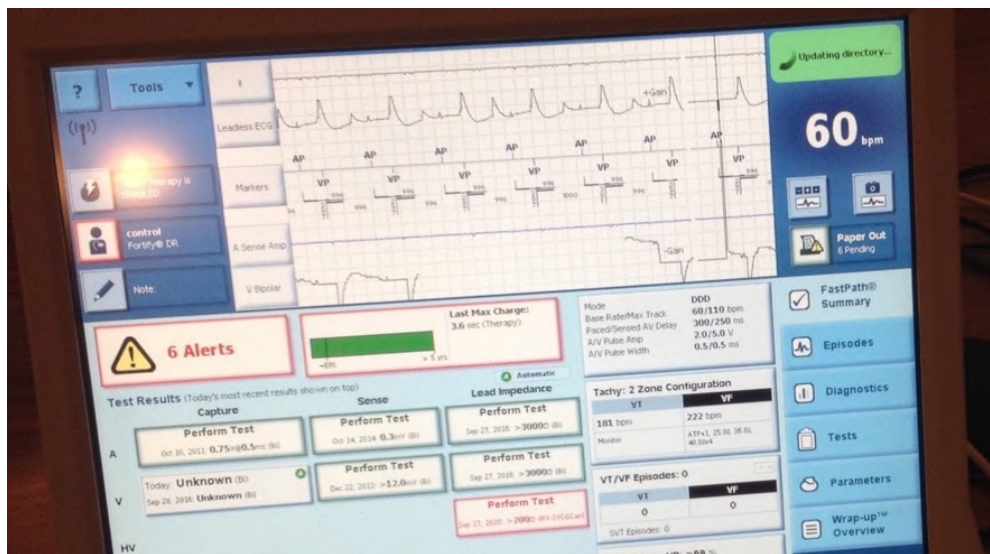
154. It should be noted that range/distance measurements were being conducted by another portion of the Bishop Fox team in an adjacent room and hallway and could potentially have been the source of the spikes seen on the oscilloscope.

155. On the first attempt at interrogating the ICD with the Programmer, the device behaved as expected and the interrogation was successful. On second and third attempts at interrogation, the Programmer was unable to interrogate the device:



156. No response to interrogation attempt

On subsequent attempts, the on-site team was able to interrogate and interact with the device as normal:



157. Successful subsequent attempt at interrogation

158. The on-site team then reconnected the ICD to the oscilloscope and noticed that the V Bipolar line was then exhibiting a negative waveform with a peak negative voltage of ~500mV at the same baseline pacing rate of 60bps.

159. The rate of the pacing was consistent throughout the test, while the voltage of the signal varied from 4V at the beginning of test to 280mV at the end of the test and -500mV after disconnecting from the oscilloscope, performing an interrogation with the Programmer, and reconnecting the oscilloscope.

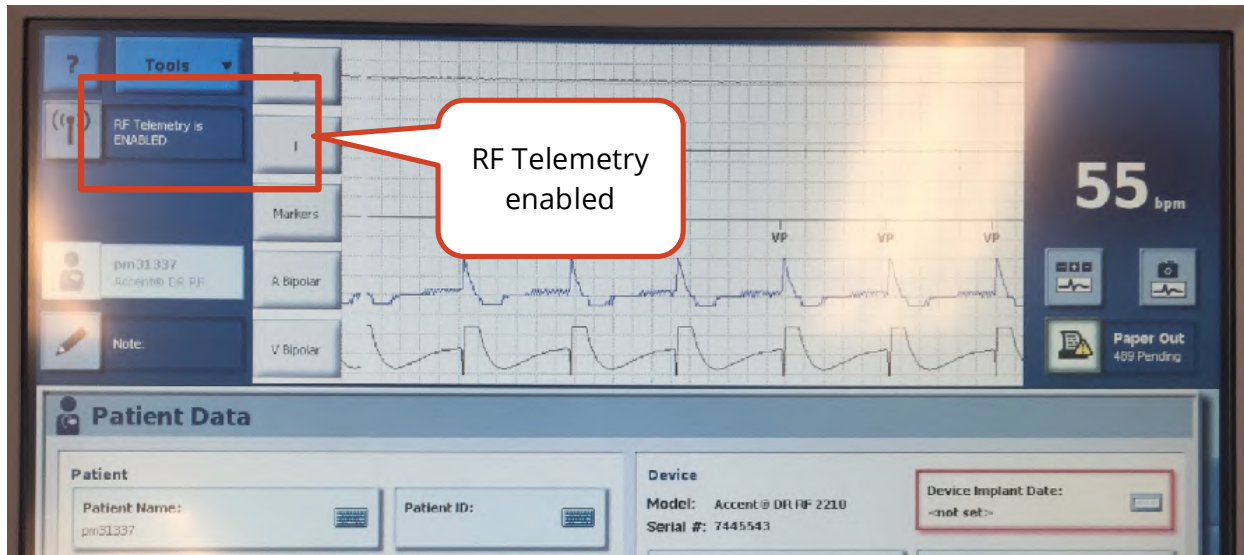
160. It is worth noting that the ICD and pacemaker crash tests were conducted in an office environment, not connected to a patient. There is a significant electrical difference between electrodes connected to human tissue and electrodes in free air; this factor could skew the values of our measurements. However, while the non-real world test conditions could have an effect on the measurements we took, the test conditions do not explain the sudden change in the ICD's behavior (reduced amplitude of pacing voltage) we observed during the crash test.

161. A crash attack was also conducted against a pacemaker. Crash tests for the pacemaker were repeated twice with the same result: the pacemaker stopped responding to RF communication. However, the device was still functional when interrogated using the inductive wand on the Programmer. The RF communications did not reactivate on the ICD while the Bishop Fox team was present at the MedSec offices, however RF communications did reactivate on the pacemaker after approximately 10 days, according to MedSec. The exact time-to-recovery is unknown. I observed that the pacemaker had indeed reactivated during our second visit to MedSec's offices; I checked the serial number of the device to ensure it was the same one tested during Bishop Fox's first visit to MedSec.

162. The pacemaker attack was conducted using a rooted Merlin@home device running an older version of the Merlin firmware: v6.1B PR_6.56. The target of the attack was an Accent DR RF 2210 pacemaker with serial number [REDACTED]. The exploit was provided by MedSec to the Bishop Fox team as a collection of shell scripts and binary files.

163. Prior to running the exploit, the pacemaker was interrogated using the Programmer to validate that the pacemaker was fully functional. The photograph below shows that the device was operating normally and could communicate using RF:

Preliminary Expert Report of Carl D. Livitt, October 23, 2016



164. Once the pacemaker had been interrogated it was placed next to the Merlin@home and the exploit was launched:

```
VERSION=EX2000 v6.1B PR_6.56
(none) login: root
Password:
root@(none):~# cd /drain
root@(none):/drain# ./launch.sh -e1
Setting receive timeout to: 1
Connecting to 127.0.0.1:1213

Error : Connect Failed
Restarting [REDACTED]
killall: [REDACTED]: no process killed
Waiting for [REDACTED] to init
lock-semop: Bad file descriptor
attach: No such file or directory.
./restart_apps.sh: line 12: 228 Killed
Restarting [REDACTED]
modprobe: Can't locate module /dev/misc/[REDACTED]_gpio
killall: [REDACTED]: no process killed
Setting receive timeout to: 1
Connecting to 127.0.0.1:1213
Thu Jan 1 00:21:08 1970
IMD Found: XXXXX43      Devices Found: 1

INTERATIONS: 1
Thu Jan 1 00:21:17 1970
Devices Found: 0
...
```

165. The attack ran for 661 iterations before the pacemaker stopped responding. The attack was allowed to run for 762 iterations in total before being terminated:

```
INTERATIONS: 661
Thu Jan 1 02:16:00 1970
```

Preliminary Expert Report of Carl D. Livitt, October 23, 2016

IMD Found: XXXXX43 Devices Found: 1

INTERACTIONS: 662

Thu Jan 1 02:16:12 1970

Devices Found: 0

INTERACTIONS: 663

Thu Jan 1 02:16:22 1970

Devices Found: 0

...

INTERACTIONS: 761

Thu Jan 1 02:25:08 1970

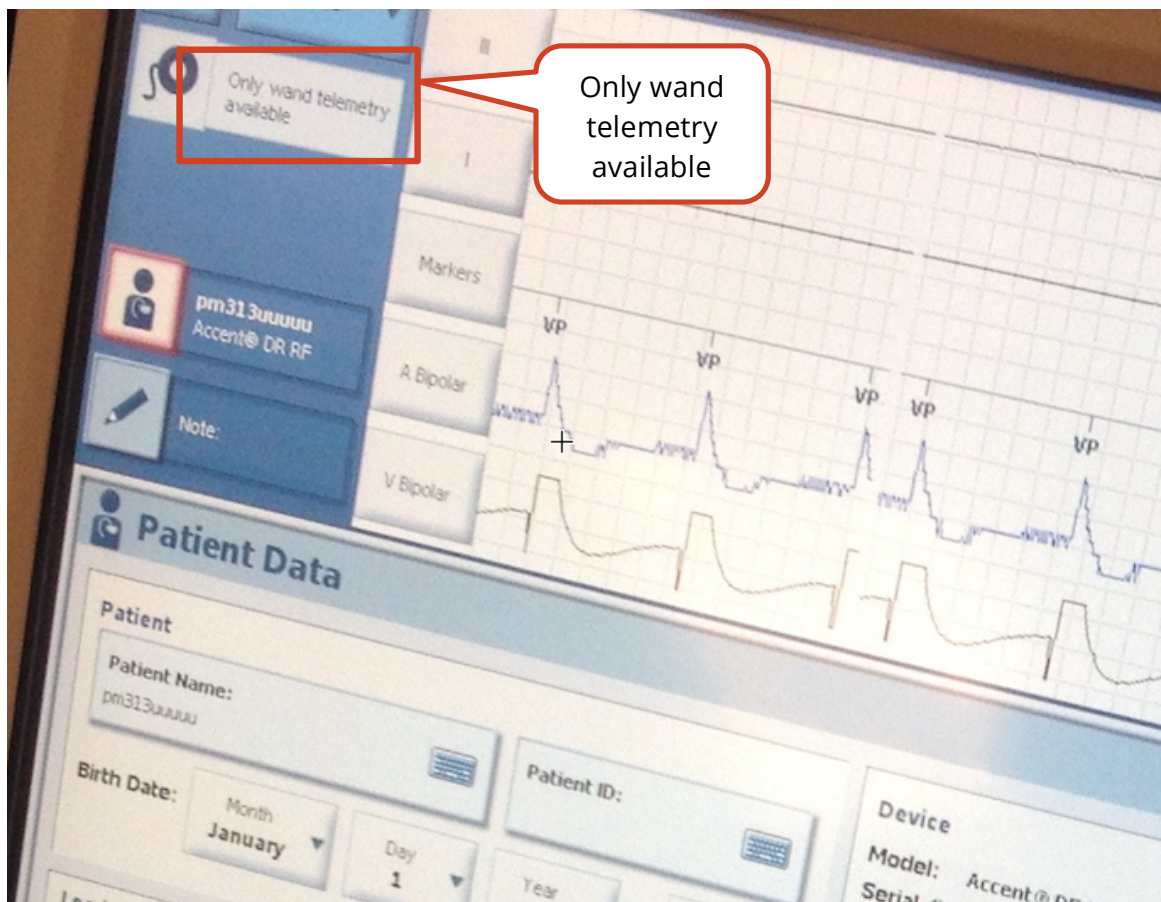
Devices Found: 0

INTERACTIONS: 762

Thu Jan 1 02:25:13 1970

root@(none):/drain#

The pacemaker was again interrogated by the PCS Programmer, and this time it showed a message stating "Only wand telemetry available":



166. Pacemaker only responds to wand telemetry

167. Despite having only wand telemetry available, the pacemaker otherwise appeared to function normally. The Bishop Fox team verified that it was still possible to reprogram the pacemaker with new patient data via the Programmer's inductive wand.

168. As with the ICD, we saw that the voltage/amplitude of pacing signals emitted by the pacemaker dropped to 280mV from the preconfigured value of 7.5V during testing of the crash attack. I do not believe that environmental factors, such as tests being undertaken on cardiac devices outside a human body without being connected to a patient, are the root cause of this observed change in behavior.

169. The crash attacks require more extensive research and testing in order to determine the root causes of the changes observed in cardiac device pacing output. At present, I do not have sufficient evidence to opine authoritatively one way or another as to the likelihood of cardiac devices becoming "bricked", or rendered non-functional during these attacks.

170. What I can say is that both devices, the ICD and the pacemaker, were rendered non-communicative over RF after conducting the crash attack, a state that lasted for approximately 10 days before the pacemaker recovered. I do not know whether the ICD recovered or not.

Security by Obscurity

171. Muddy Waters made the following statement in the report dated August 25, 2016:

172. *In MedSec's opinion, the use of off-the-shelf components and the lack of anti-debugging mechanisms made the Merlin@home device significantly easier to reverse engineer and locate numerous vulnerabilities. The manufacturer left many developmental items on the devices that should not be present, such scripts that allow debugging and development mode to be turned on. All of the competitors incorporated additional security measures. Some manufacturers required short range authentication (via a wand).*

173. St. Jude claims this is an endorsement of the "discredited notion of 'security through obscurity.'" (Complaint, paragraph 79)

174. I find the alleged endorsement to be tenuous at best. MedSec are simply observing that commonly available, off-the-shelf, well-documented hardware is often significantly easier to work with than obscure undocumented hardware. For example, off-the-shelf hardware frequently has publicly available datasheets that describe in great technical detail

Preliminary Expert Report of Carl D. Livitt, October 23, 2016

how the chip is implemented, the function of each of its pins, and how to integrate it within a circuit. This makes reverse engineering a much easier task than for chips that do not have publicly available datasheets.

175. The same principle applies to anti-debugging technologies: it is generally easier to reverse engineer something if it doesn't actively try to stop you. This is not an endorsement of security by obscurity, but an acknowledgement of a principle with which any experienced reverse engineer will be very familiar.

Large-Scale Attacks

176. The following statement was made by Muddy Waters:

177. *"MedSec outlined an exact method that could be used to launch similar attacks on a large scale basis – either through established techniques for [redacted], or possibly through STJ's network itself. It would have been illegal for MedSec to test the proof of concept."* (Muddy Waters report, August 25, 2016)

178. In the report dated August 29, 2016, Muddy Waters responded to St. Jude's criticism that *"users would have to be within seven feet of a Merlin@home in order to be vulnerable to attacks"* by stating this: *"It acknowledges that the hundreds of thousands of active Merlin@home users who sleep near their Merlin@homes would obviously be vulnerable to a large-scale attack when connected to the devices for a continuous time period."*

179. St. Jude claims that *"MedSec offers no factual basis for plausible or realistic risk of 'large scale attacks.' MedSec attempted to hack only one CRM device at a time."* (Complaint, paragraph 86(k))

180. "Large scale" is a subjective term. In the context of this work, it could mean hundreds, thousands, tens of thousands, or even hundreds of thousands of patients. For the sake of argument, I shall assume the worst case scenario of hundreds of thousands of patients and will offer a plausible scenario for a large-scale attack.

181. Based on my experience of conducting global scale penetration tests of computer systems, I can categorically state that I have on many, many occasions compromised an organization's computer systems and, with varying degrees of effort, gone on to compromise more and more deeply into the affected organization's networks. I have personally led engagements where my team have broken into a company, pivoted through the network to identify critical source code for systems like those used by St. Jude Medical,

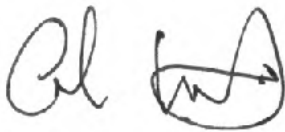
Preliminary Expert Report of Carl D. Livitt, October 23, 2016

and secured access to that source code; with this level of access it becomes very easy to modify software that will be “pushed” to embedded devices, such as cardiac devices, over the internet. Given a sufficiently skilled and motivated adversary, the process of deploying hacked software to cardiac devices on a large scale is not just within the realm of possibility, but represents a scenario that I and my team have personally and repeatedly undertaken in the past. Based on this, it is my opinion that the same techniques could plausibly be brought to bear against St. Jude Medical network infrastructure.

182. Please note that I have not in any way performed an analysis of the St. Jude Medical networks or software distribution mechanisms; my opinion in this particular matter is extrapolated and based only on past experience, not first-hand knowledge of the security posture of St. Jude’s Medical’s networks.

Potential Additional Analyses

183. I reserve the right to clarify, amend, and/or supplement my opinions based on additional information that may be provided to me and the development of additional information as this matter proceeds.

A handwritten signature in black ink, consisting of a stylized 'C' followed by a series of loops and a final flourish.

Carl D. Livitt
Partner, Bishop Fox

References

1. "MW is Short St. Jude Medical (STJ:US)", http://d.muddywatersresearch.com/wp-content/uploads/2016/08/MW_STJ_08252016_2.pdf
2. Ventricular fibrillation, https://en.wikipedia.org/wiki/Ventricular_fibrillation
3. Merlin@home™ Transmitter, <https://www.sjm.com/en/professionals/featured-products/cardiac-rhythm-management/remote-care/remote-care/merlin-home-transmitter>
4. "Analysis of Radio Propagation Inside the Human Body for in-Body Localization Purposes", Ilka Dove, http://essay.utwente.nl/66071/1/Dove_MA_TE.pdf
5. "St. Jude Medical Bradycardia and Tachycardia Devices Help Manual", St. Jude Medical, page 153, "Emergency Shock Instructions", <https://manuals.sjm.com/~media/manuals/product-manual-pdfs/2/5/25ebf95d-456c-49be-aa2c-a869dc51f907.pdf>
6. "St. Jude Medical Bradycardia and Tachycardia Devices Help Manual", St. Jude Medical, page 43, "Fibber Test", <https://manuals.sjm.com/~media/manuals/product-manual-pdfs/2/5/25ebf95d-456c-49be-aa2c-a869dc51f907.pdf>
7. "St. Jude Medical Bradycardia and Tachycardia Devices Help Manual", St. Jude Medical, page 148, "Tachy Therapy Enable/Disable", <https://manuals.sjm.com/~media/manuals/product-manual-pdfs/2/5/25ebf95d-456c-49be-aa2c-a869dc51f907.pdf>
8. "Transcutaneous T wave shock: a universal method for ventricular fibrillation induction", <https://www.ncbi.nlm.nih.gov/pubmed/9455753>
9. "Ventricular fibrillation", https://en.wikipedia.org/wiki/Ventricular_fibrillation
10. "RSA (cryptosystem)", [https://en.wikipedia.org/wiki/RSA_\(cryptosystem\)](https://en.wikipedia.org/wiki/RSA_(cryptosystem))
11. "RSA (cryptosystem)", Integer Factorization and RSA Problem", [https://en.wikipedia.org/wiki/RSA_\(cryptosystem\)](https://en.wikipedia.org/wiki/RSA_(cryptosystem))
12. "Premature Battery Depletion of St. Jude Medical ICD and CRT-D Devices: FDA Safety Communication", <http://www.fda.gov/MedicalDevices/Safety/AlertsandNotices/ucm524666.htm>
13. "Hacking Exposed: Web Applications 3rd Edition", McGraw-Hill Education, 2010
14. "Network Security Assessment 1st Edition", O'Reilly Media, 2004
15. "Will LinkedIn's new 'Intro' feature attract hackers?", USA Today, 2013, <http://www.usatoday.com/story/cybertruth/2013/10/25/will-linkedins-intro-e-mail-service-attract-hackers/3191583/>
16. "Thieves, spies move to AVTs: advanced volatile threats", USA Today, 2013, <http://www.usatoday.com/story/tech/2013/02/21/advanced-volatile-threat-malicious-software-pc-intrusions/1933975/>

17. "Google Encrypts to Evade NSA Surveillance: Should You?", eWeek, 2013, <http://www.eweek.com/security/google-encrypts-to-evade-nsa-surveillance-should-you.html>
18. "NSA Follows Cookie Trail to Track Surveillance Targets on Web", eWeek, 2013, <http://www.eweek.com/security/nsa-follows-cookie-trail-to-track-surveillance-targets-on-web.html>
19. "LinkedIn's mobile Intro tool called a lure for phishing hacks", PC World, 2013, <http://www.pcworld.com/article/2058260/linkedins-intro-tool-for-iphones-could-be-a-juicy-target-for-attackers.html>
20. "Security industry takes a hit after latest NSA disclosures", PC World, 2013, <http://www.pcworld.com/article/2083243/security-industry-takes-a-hit-after-latest-nsa-disclosures.html#!>
21. "4 Ways to Secure an Apple Mac Browser", eSecurity Planet, 2013, <http://www.esecurityplanet.com/mac-os-security/4-ways-to-secure-an-apple-mac-browser.html>
22. "Apple Pay Wants To Be Your Mobile Wallet", NPR, 2014, <http://www.npr.org/2014/09/10/347305819/apple-pay-wants-to-be-your-mobile-wallet>
23. "Nanog traceroute v6.0 to 6.1.1 local root stack overflow exploit.", 2002, <https://packetstormsecurity.com/files/30535/traceroute-exploit.c.html>
24. "Format string vulnerability in plpnfsd", 2003, <https://packetstormsecurity.com/files/30763/CLIVITT-2003-2.txt.html>
25. "Citadel/UX BBS versions 6.07 and below remote buffer overflow and insecure randomness", 2003, <https://packetstormsecurity.com/files/31373/CLIVITT-2003-4-Citadel.txt.html>
26. "Apache mod_mylo remote buffer overflow", 2003, <https://packetstormsecurity.com/files/31461/CLIVITT-2003-5.txt.html>
27. "LSH remote root exploit", 2003, https://packetstormsecurity.com/files/31682/lsh_exploit.c.html
28. "BestCrypt 0.6/0.7/0.8 - BCTool UMount Buffer Overflow", 2001, <https://www.exploit-db.com/exploits/20927/>
29. "H-Sphere Webshell 2.4 - Remote root exploit", 2003, <https://www.exploit-db.com/exploits/22129/>
30. "H-Sphere Webshell 2.4 - Local root exploit", 2003, <https://www.exploit-db.com/exploits/22128/>
31. "Webmin 0.9x / Usermin 0.9x/1.0 - Session ID Spoofing Unauthenticated Access", 2003, <https://www.exploit-db.com/exploits/22275/>

32. "Oracle WebLogic Node Manager Remote Configuration Capability Lets Remote Users Execute Arbitrary Commands", 2010, <http://www.securitytracker.com/id/1024569>
33. "SaleLogix Server and Web Client suffer from bypass authentication, privilege escalation, SQL injection, information leak, arbitrary file creation, and directory traversal flaws.", 2004, <https://packetstormsecurity.com/files/34756/Saleslogix-1-2004.txt.html>
34. "Rethinking and Repackaging iOS Apps: Part1", 2015, <https://www.bishopfox.com/blog/2015/02/rethinking-repackaging-ios-apps-part-1/>
35. "Rethinking and Repackaging iOS Apps: Part1", 2015, <https://www.bishopfox.com/blog/2015/05/rethinking-repackaging-ios-apps-part-2/>
36. "On Apple, Encryption, and Privacy: A Word About Decryption", 2016, <https://www.bishopfox.com/blog/2016/03/apple-encryption-privacy-word-decryption/>
37. "Association of Corporate Counsel", "In-House Counsel Forum - Compliance & Risk Management", "Don't be the Slowest Zebra – Understanding and Responding to Cybersecurity Risks", with Eric Whytsell, Jackson Kelly, 2016, <https://www.acc.com/chapters/colo/index.cfm?eventID=18159>
38. Special Branch, https://en.wikipedia.org/wiki/Special_Branch
39. National Extremism Tactical Coordination Unit, https://en.wikipedia.org/wiki/National_Extremism_Tactical_Co-ordination_Unit
40. National Counter Terrorism Security Office, https://en.wikipedia.org/wiki/National_Counter_Terrorism_Security_Office
41. Computer security model, "cyber kill chain", https://en.wikipedia.org/wiki/Kill_chain#Computer_security_model

Glossary

184. The following table provides a glossary of terminology used throughout this report in relation to St. Jude Medical devices:

Term	Also Known As	Description
CRM	CRM Device	Cardiac Rhythm Management (CRM) Device is the term used to encapsulate all implantable ICD or pacemaker devices.
ICD	Fortify Assura™ Implantable Cardioverter Defibrillator	<p>"An ICD is a minicomputer that is implanted under the skin of the upper chest area and is small enough to fit in the palm of your hand. It monitors your heart for fast and potentially dangerous heart rates, and delivers therapy in the form of small electrical pulses when it senses a dangerously fast heart rhythm. While helping your heart maintain its rhythm, the ICD also stores information that your doctor can use to program the ICD for the best possible therapy."</p> <p>https://www.sjm.com/en/patients/arrhythmias/our-solutions/icds</p>
Interrogate	N/A	Interrogation is the process by which a Programmer reads patient data, therapeutic settings, and event logs from a CRM. Once interrogated, the CRM can be optionally programmed with new therapeutic settings.
Pacemaker	Assurity™ or Endurity™ Pacemaker	"A pacemaker is an implantable, battery-powered minicomputer that sends electrical pulses to heart whenever it detects a slow heartbeat or no heartbeat at all. When it senses an arrhythmia or lack of a heartbeat, it then sends electrical impulses to restore or establish a normal rhythm. A pacemaker also stores important information that your doctor can use to program your pacemaker so you

		<p>can receive the best possible therapy.”</p> <p>https://www.sjm.com/en/patients/arrhythmias/our-solutions/pacemakers</p>
Programmer	Merlin™ Patient Care System	<p>“The Merlin Patient Care System supports current and previous generation devices. It is a portable computer with an LCD touch screen that enables clinicians to retrieve and analyze patient information during routine follow-up visits and quickly and easily make programming changes to the implanted devices.”</p> <p>https://www-03.ibm.com/press/us/en/pressrelease/19747.wss</p>
Remote Transmitter	Merlin@home™	<p>“The Merlin.net™ Patient Care Network and Merlin@home™ transmitter work together to make up a communication system that offers increased safety in living with your pacemaker or implantable cardioverter defibrillator (ICD). If your medical team recommends remote monitoring for you and your device, you can perform follow-ups at home or even while travelling with the Merlin@home™ transmitter.”</p> <p>https://www.sjm.com/en/patients/arrhythmias/our-solutions/remote-monitoring/merlin-net-pcn</p>
Wand	Inductive Wand	<p>The wand is an inductive coupling device used to wake up and program implantable devices, such as ICDs and pacemakers. It is designed to be used with the Merlin™ Patient Care System. Due to the use of inductive coupling, it has an effective range of only a few inches.</p>

185. The following table provides a glossary of terminology used in this document that is commonly used in discussions relating to cybersecurity, and specifically relating to the findings discussed in this report.

Term	Also Known As	Description
ASLR	Address Space Layout	ASLR is a security countermeasure designed to make the exploitation of security bugs

Preliminary Expert Report of Carl D. Livitt, October 23, 2016

	Randomization	more difficult. It involves randomizing memory locations on a computer so that it becomes infeasible for a hacker to determine the locations of specific, important pieces of data required during the exploitation of a software bug.
Backdoor	N/A	A backdoor is a mechanism implemented within a system that subverts the system's security for someone with knowledge of the backdoor. For example, a system might be backdoored such that it becomes possible to present a "magic" password that allows someone to log in as any user of the system. Backdoors are often left behind by developers, sometimes for convenience, sometimes by accident, sometimes through malicious intent. Backdoors are also commonly added to systems by hackers in order to maintain a reliable channel of access to the systems in the future.
Buffer Overflow	N/A	A buffer overflow is a security vulnerability, the root cause of which is a programmer error that incorrectly copies more data than expected into a memory space ("buffer") in a computer. The excess of data overflows the buffer, which in turn overwrites data stored outside the buffer. Skilled hackers can exploit this to alter and control the behavior of computer software.
CoolTerm	N/A	CoolTerm is a piece of software that communicates with a device (such as a Merlin@home) via a serial cable or USB-to-serial adapter. The software allows a person to view messages sent by the device, and it allows the person to type messages or commands that are sent to the device.
Debug	Debugging, debugger	To debug something is to figure out where a system malfunction occurs and to fix it: "He is debugging the issue". A debugger is a software tool designed to assist in the process of debugging by "attaching" to computer programs as they run, and presenting the user with tools to inspect, pause, and analyze software behavior. Debuggers are often used by hackers during

Preliminary Expert Report of Carl D. Livitt, October 23, 2016

		the development of exploits in order to better understand how software vulnerabilities work. Debuggers usually go hand-in-hand with disassemblers.
Disassembler	N/A	A disassembler is a software tool that takes a piece of software and converts it into human readable instructions in what is called “assembly language” or “assembly code”, which is a low level computer programming language. Skilled programmers and hackers can read the assembly code and gain an understanding of how a program works, which often makes it easier to modify or repurpose a program’s behavior.
Ethernet crossover cable	Crossover cable	This describes a cable used to create a network connection directly between two computers.
Exploit (noun)	N/A	As a noun, an exploit is generally a piece of software designed to compromise a computer system. For example, “MedSec wrote an exploit to drain the battery of a Merlin@home”. It is common for several exploits to be chained together to build a complete attack; for example, one might exploit vulnerabilities to get root on a programmer, then reverse engineer the St. Jude RF protocol, then exploit weaknesses in the protocol to conduct attacks against cardiac devices. This pattern would be referred to as an “attack chain” or “chain of exploits”.
Exploit (verb)	N/A	As a verb, exploit typically describes the process of taking advantage of a security vulnerability to compromise a computer system. For example, “I exploited a weak password to get administrative access”.
Firmware	N/A	Firmware is the term given to software that runs on devices like the Merlin@home, pacemakers, and ICDs. Manufacturers often issue firmware upgrades as a means of fixing bugs, adding features, or addressing security issues.
Getting root	Owning, rooting	To “get root” is the term given to a set of actions that culminates in a person or

Preliminary Expert Report of Carl D. Livitt, October 23, 2016

		persons obtaining access to the root user account of a computer. "I rooted the computer" simply means "I took actions that allowed me to login as the root user". Getting root usually carries the connotation that the actions required some form of hacking or exploitation of vulnerabilities in the process of rooting a system.
Header	N/A	A header is a set of electrical points on a circuit board to which connectors can be affixed.
JTAG	Debugging interface	Some microchips contain built-in debugging features that enable developers to interact closely with software running on the chip. Such debugging features are generally implemented to an industry standard called JTAG that defines how to connect to and interact with microchip debugging features. JTAG is commonly exposed as a small connector on a circuit board, and there are many commonly available JTAG interfaces and software tools that make it possible to connect a laptop to a circuit's JTAG port. With this, hackers can completely control the behavior of software running on a chip. JTAG can also be used to make copies of software running on a chip; this is commonly referred to as "dumping the firmware".
JTAGulator	N/A	JTAGulator is a hardware tool that assists in identifying JTAG and UART connections from test points, vias, or component pads on a circuit board.
Linux	"OS" or "Operating System".	Linux is an operating system. An operating system is a highly complex piece of software that is responsible for making a computer do useful things, such as accept mouse and keyboard input and displaying output on a monitor. Other operating systems include Microsoft Windows, Apple iOS, and Google Android.
Oscilloscope	N/A	An oscilloscope, previously called an oscillograph, and informally known as a scope, CRO (for cathode-ray oscilloscope), or DSO (for the more modern digital storage

Preliminary Expert Report of Carl D. Livitt, October 23, 2016

		<p>oscilloscope), is a type of electronic test instrument that allows observation of constantly varying signal voltages, usually as a two-dimensional plot of one or more signals as a function of time. Other signals (such as sound or vibration) can be converted to voltages and displayed.</p> <p>(Wikipedia, https://en.wikipedia.org/wiki/Oscilloscope)</p>
Reverse engineering	RE	Reverse engineering is the process of taking a system, such as firmware or a microchip, and figuring out how it works.
RF	Radio Frequency, wireless	RF is a shorthand term used to describe a means of wireless communication between electronic devices. Different devices communicate at different radio frequencies, expressed in Hertz or, more commonly, kilohertz ("KHz"), megahertz ("MHz"), and gigahertz ("GHz"). For example, household Wi-Fi communicates over RF; the Wi-Fi RF frequency is usually 2.4GHz or 5GHz. St. Jude Medical devices typically communicate at frequencies of 2.4GHz and 400MHz.
Root	Superuser, administrator	The "root" user account is the administrator user on Linux-based computers such as the Merlin@home. To "have root" means that a person is able to log in to a computer (or otherwise interact with the computer) as the root user. The root user has complete control over the computer (the root user can be said to possess "root permissions") and can perform administrative actions, such as installing or removing programs; reading, modifying, creating, and deleting files on the computer; adding new users, changing passwords, and other administrative actions.
Segger J-Link Plus JTAG Debug Probe	J-Link, Segger Tool	This is a hardware device made by a company called Segger. It is used to connect a laptop or other computer to a JTAG interface on a circuit board. It allows the user to issue commands that affect the operation of the processor chip being debugged.
Shell	Console, terminal,	A shell is an interactive computer program

Preliminary Expert Report of Carl D. Livitt, October 23, 2016

	command prompt	("command prompt") that allows a person to type commands into the computer. If the person "has root" or the computer "has been rooted", any commands entered by the person will be executed with the permissions of the root user. One could say "I got a shell" to describe the process of successfully hacking a computer to the point of being able to type commands into a command prompt. A "root shell" is simply a shell with root permissions.
Software Defined Radio	SDR, USRP	An SDR is a specialized piece of equipment that can be used to build RF receivers/transmitters to almost any specification. For example, SDRs can be programmed to act as cellphone towers, FM radio receivers, and car door remote controls.
SSH	Secure Shell	SSH is a service that runs on a computer and provides remote network-based access to a shell on the computer. SSH handles authentication and encryption of the connection to the shell.
Stripped binary	Stripping	A "binary" is another word for the file containing a computer program. Typically, when software is converted from human readable "source code" to a computer-readable "binary" file, the binary contains what are known as "symbols": detailed information left over from the source code that can be of great use to a hacker who seeks to understand the way in which the program works. To "strip" a binary means to remove the symbols, thereby removing a useful resource from hackers. A "stripped binary" is therefore a program that has been stripped of its symbols. "Unstripped binary" is the inverse.
UART	"Universal Asynchronous Receiver Transmitter", serial port, RS-232	A UART (also referred to as a "serial port") is typically a 3-wire connection over which two computers can communicate. Some devices, such as the Merlin@home, can be configured to present a root shell over the serial port. It can be accessed by a connecting a laptop to the device's serial port via a serial cable.

Preliminary Expert Report of Carl D. Livitt, October 23, 2016

		Software on the laptop communicates over the serial cable, allowing the laptop user to access the root shell on Merlin@home.
USB/IDE adapter	N/A	An adapter that make it possible to connect the hard drive from a PCS Programmer to the USB port of a laptop computer, thereby providing access to the files on the hard drive.
USB-to-Serial Adapter	N/A	A USB-to-serial adapter makes it possible to connect a Merlin@home's serial port to the USB port of a laptop.
Virtual Machine	VM, Virtualized Linux environment	A virtual machine ("VM") is a piece of software that emulates a real computer. Using a VM it becomes possible to run multiple operating systems at the same time on one computer. For example, a MacBook Pro laptop might run Linux in a VM.
Vulnerability	Security issue	The term "vulnerability" is used to describe a specific security weakness in a system, network, device, or piece of software. For example, "there is a vulnerability in XYZ that allows me to read your email". Hackers look for vulnerabilities in systems in order to gain access to the system, or to gain elevated permissions on the system.