Pacemakers and Implantable Cardiac Defibrillators: Software Radio Attacks and Zero-Power Defenses

Daniel Halperin, Thomas S. Heydt-Benjamin, Benjamin Ransford, Shane S. Clark, Benessa Defend, Will Morgan, Kevin Fu, Tadayoshi Kohno, William H. Maisel

IEEE S&P' 08

YONGHWA LEE

Contents

Introduction

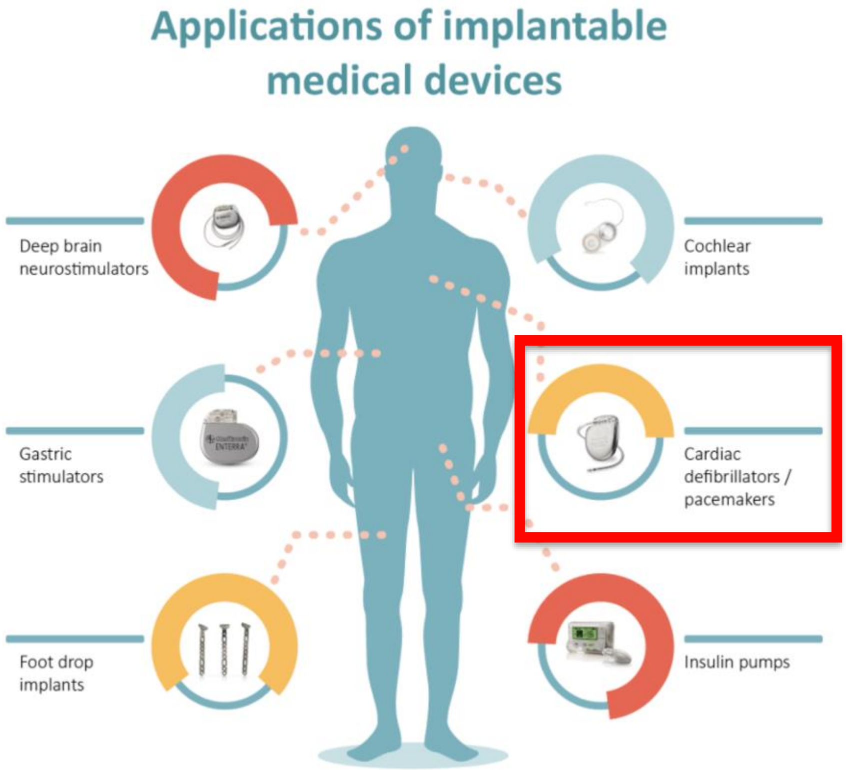
❖ Security & Privacy properties in **Implantable Medical Device (IMD)**

❖ **IMD**

- Electronic devices within body to **monitor** and **treat** medical conditions
  - Ex) **Pacemakers, Implantable Cardioverter Defibrillator (ICD)**

❖ 1990~2002 : 2.6 million Pacemakers and ICDs implanted in US patients

Implantable Medical Device (IMD)

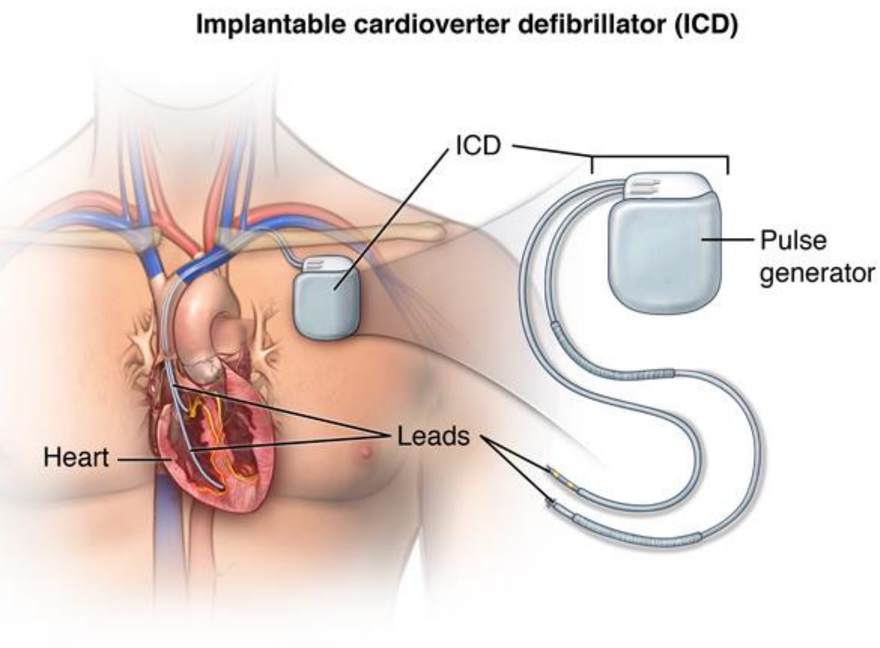


Motivation

- **No** public investigations into **realistic security & privacy risks of IMDs**
- To Demonstrate that IMD's security & privacy **vulnerability** exists
- To Assess & address problems with IMDs with **actual attacks**
- To Suggest **realistic solution** (Defense & mitigation techniques)

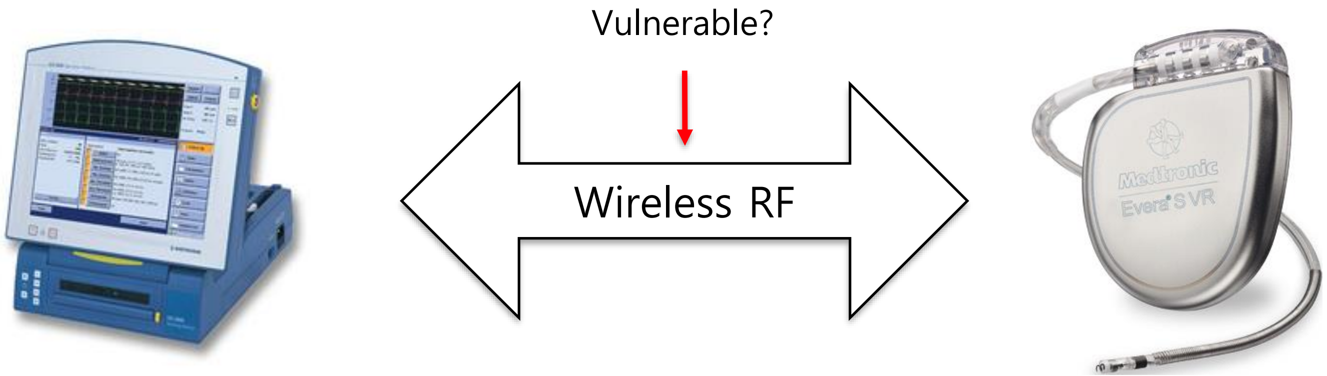
Implantable Cardioverter Defibrillator (ICD)

- Monitors, responds to heart activities
  - **Defibrillation** - emergent large shock
  - **Pacing** - periodic small stimulations
    - ICD Includes Pacemaker's role
- Self-contained power & connectivity
  - Non-rechargeable internal battery
    - Lasts for several years
  - No physical external connection



Implantable Cardiac Defibrillator (ICD)

❖ (Re)Programmable by ICD programmer device
- Perform **diagnostics**
- Read & Write patient's **private data**
- Set **therapy options**



ICD programmer

ICD

Vulnerabilities & Security Models

- ICD can be made to communicate **without authentication** process
  - Adversary with **unauthorized** ICD programmer

- **Unencrypted** wireless communication between ICD <-> ICD programmer
  - Adversary can **eavesdrop**

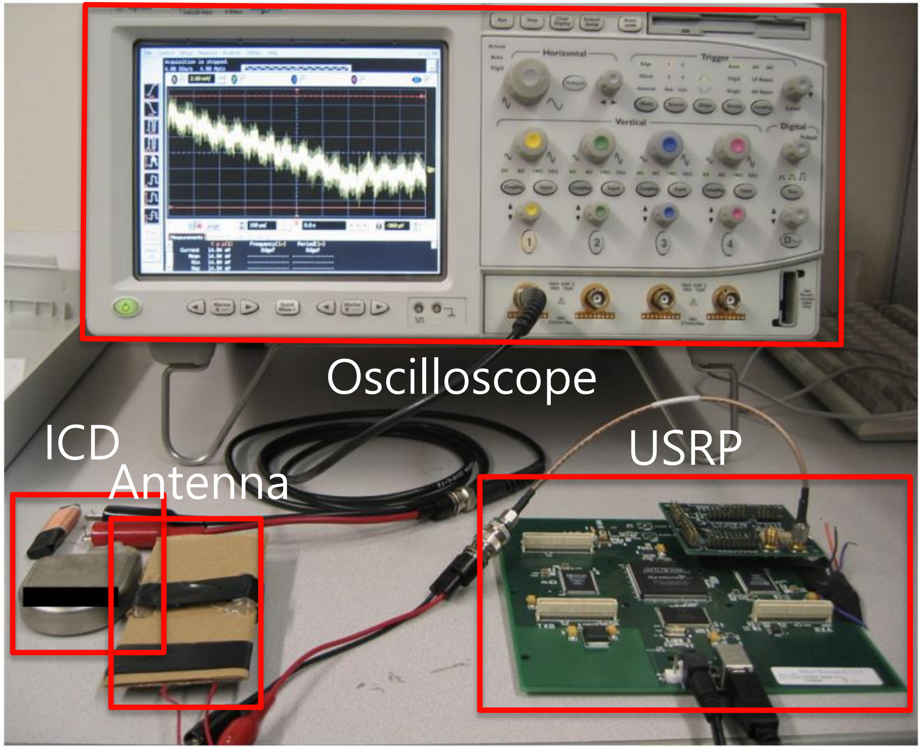
- ICD can be **re-programmed** by an **unauthenticated** device
  - Adversary can **generate** malicious RF traffic

Equipments for Reverse Engineering

- **Hardwares**
  - Oscilloscope
    - ★ Displays signal as a waveform
  - Universal Software Radio Peripheral (USRP)
    - ★ Interacts with open source GNU Radio libraries

- **Eavesdropping Antenna**

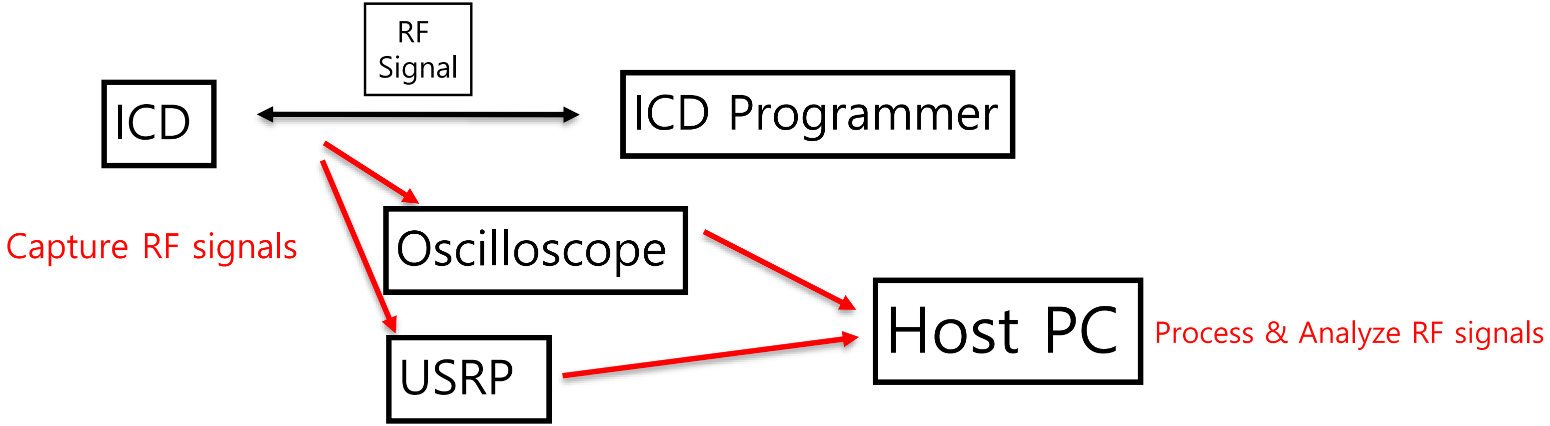
- **Softwares**
  - GNU Radio toolchain
  - Matlab & Perl



Reverse Engineering Transmissions

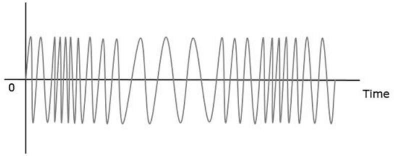
- Captured RF transmissions around **175 kHZ**

- Processed RF traces (signals) using GNU Radio & Matlab
  - Analyzing ICD protocols



Reverse Engineering Transmissions

- ❖ Transmissions from ICD programmer
  - Obtained **raw bits** to be transmitted
    - ★ By tapping **serial connection**
  - Compared **raw bits** with the **encoded & modulated** RF signals



RF signals output

Compare

0	1	1	0	…	1

Tapped raw bits

Serial Connection

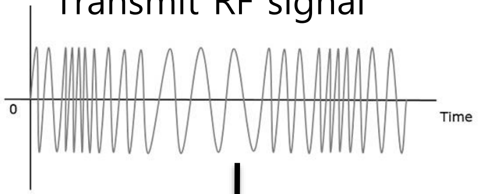
programmer ⟷ head

Reverse Engineering Transmissions

- ❖ Transmissions from ICD
  - **No** serial connection like programmer
  - Inserted **specific information**
    - ★ Used arbitrary patient name (ex. ‘AA’, ‘AAAA’)
    - ★ Analyzed RF signals to **identify modulation & encoding** scheme

programmer —— Set Name ‘AA’, ‘AAAA’, ~ ——→ ICD

Transmit RF signal



Analyze patterns in signals

```
(a)    101010100000001|...|000000100|111111011|000000100|111111011|...|1111111
(b)    _11111110000001|...|100000x10|100000x10|100000x10|100000x10|...|1000000
(c)    ------SFD------               A         A         A         A     --EFD--
```

Fig. 5. Part of a sample programmer transmission containing the crib text AAAA. Row (a) represents the demodulated bits, (b) are the NRZI-decoded bits, and (c) are the bits rendered as ASCII. The Start-of-Frame and End-of-Frame Delimiters pictured mark the beginning and end of each packet.

Modulation & Encoding Schemes

❖ With analyzing signals from ICD, ICD programmer

- Encoding scheme
  - ★ Both : Non-Return-to-Zero Inverted (NRZI)

- Modulation scheme
  - ★ ICD : Differential Binary Phase Shift Keying (DBPSK)
  - ★ ICD programmer : Binary Frequency Shift Keying (2-FSK)

Passive Attack (Eavesdropping)

- Eavesdropper
  - Used **USRP** with **GNU Radio libraries**
    - To Capture and store signals

  - Wrote code in **Matlab & Perl**
    - To analyze signals

  - Integrated some functions written in C++
    - To eavesdrop in real time
    - Modified C++ codes (removed 87, added 44 lines)

Passive Attack (Eavesdropping)

- Establishing a transaction timeline
  - Easy to infer based on analyzed signals

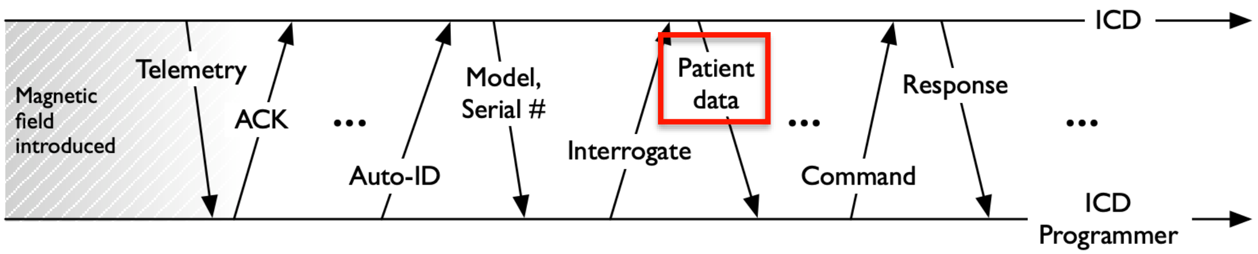


Fig. 4. Timeline of a conversation between an ICD programmer and an ICD. If a programmer is present it will acknowledge each packet automatically. When told by an operator to do so, the programmer asks the ICD for identifying information, which the ICD provides. The programmer then interrogates the ICD for patient data, which the ICD provides. Other commands (such as ICD programming commands) and their responses follow.

Passive Attack (Eavesdropping) #1

- Intercepting Patient Data
  - No encryption
  - Cleartext representations of patient data
  - Easily extractable
  - Personal & sensitive data
    - ★ Patient name, date of birth, medical ID number, history
    - ★ Physician’s name, phone number

Passive Attack (Eavesdropping) #1

Passive Attack (Eavesdropping) #2

- ❖ Intercepting Telemetry **(Sniffing Vital Signs)**
  - ICD broadcasts telemetry data in **cleartext**
    - ★ With magnet of 700 gauss, within 5cm of target ICD
  - Telemetry data
    - ★ Contain patient's **electrocardiogram** (EKG - 심전도) readings
    - ★ Data : heart rate and other private information

Active Attacks

- All active attacks are **replay attacks**
  - **“Deaf”** (Transmit-only) Attacks with USRP & GNU Radio
  - **Limitations**
    - ★ Close range, only one ICD tested, not optimized, takes many seconds

- Attack scenarios
  - Disclosing patient & cardiac data
  - Changing patient name
  - Setting the ICD’s clock
  - **Changing therapies**
  - **Inducing fibrillation**
  - **Denial of Service Attack**

Active Attack #1 : Changing Therapies

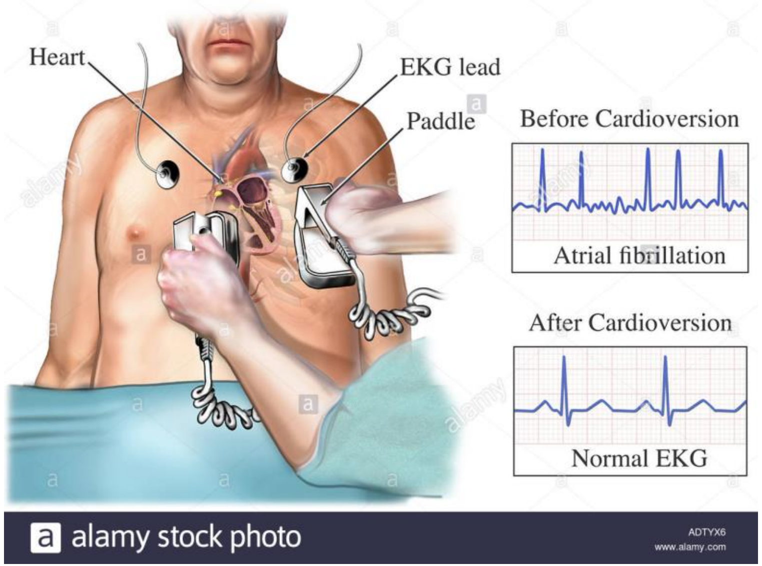
- **Therapies** : ICD's responses to cardiac events

- Replay attack can **quietly turn off therapies**
  - "Stop detecting fibrillation", "Stop detecting slow heartbeats"

- After 24 replay attempts, more than one succeeded at **disabling all the therapies**

Active Attack #2 : Inducing Fibrillation

❖ ICD can induce **Ventricular Fibrillation** with setting a testing mode
  - Can send **137.7V** shock to patient's heart with specific commands



Active Attack #3 : Denial of Service Attack

- Frequent RF communication (like "**Ping**" in networking)
  - **Drains battery -> Decreases battery like faster**

Active Attack : Other Attack Vectors

- Other **potential** attack vectors in IMDs
  - Insecure software updates
  - System's vulnerability like Buffer-Overflow

Defenses : Defense Goals

- Prevent or deter attacks by insiders & outsiders
- Draw no power from primary battery
- Security-sensitive events should be detectable by patients

Defenses : Zero-Power Defense

❖ WISPer - Wireless Identification and Sensing Platform + piezo-element

❖ WISPer harvests RF energy from RFID reader
- No power from ICD's primary battery

❖ Security Mechanisms
- Zero-power **notification**
- Zero-power **authentication**
- **Sensible key exchange**

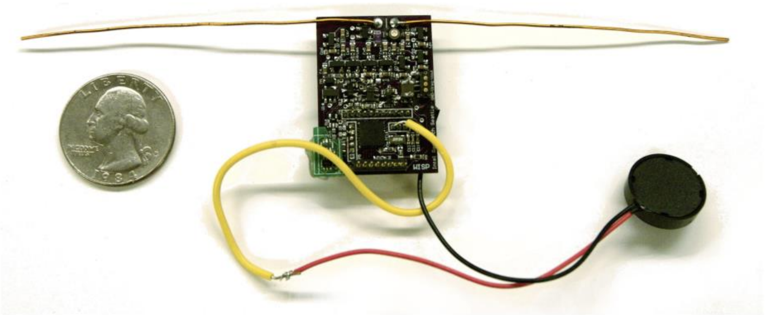
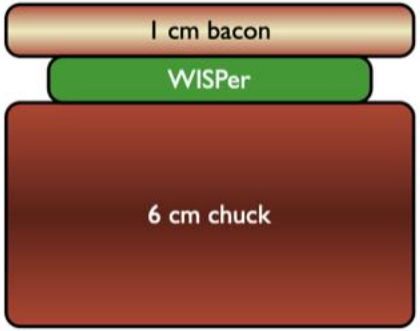


Fig. 7. The WISP with attached piezo-element.

Defense #1 : Zero-Power Notification

- ❖ Audible detection
  - WISPer alerts a patient with "**Beep**"
    - ★ "**Beep**" means ICD may start RF communications
    - ★ Via piezo-electric speaker

- ❖ Tested with Simulated Human body (Bacon)
  - Measured 84 dB of sound at the surface
    - ★ Normal conversation : 60dB



WISPer in a bag containing bacon and ground beef

SysSec
System Security Lab

Defense #2 : Zero-Power Authentication

- RC5 based challenge-response protocol
- ICD is activated only after successful authentication process
- Use power from WISPer's RFID reader
  - No use primary battery

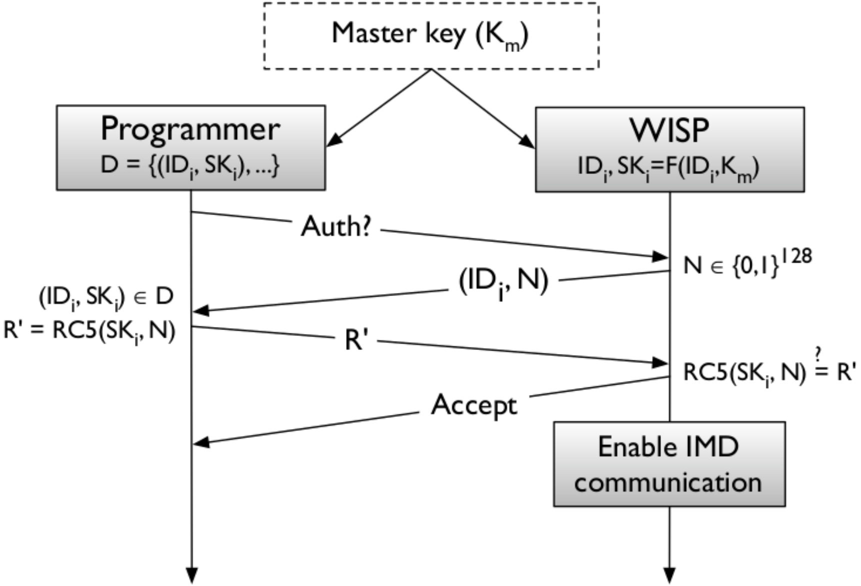


Fig. 10. The protocol for communication between an ICD programmer and a zero-power authentication device (a WISP RFID tag, in the case of our prototype).

Defense #3 : Sensible Key Exchange

- Key distribution over a **audio** channel
  - **Vibration** based
- Transmit modulated **sound wave**
  - Nonce (Secret Key)
- Patient can feel, but hard to eavesdrop at a distance
- Key can be used in authentication (#2)

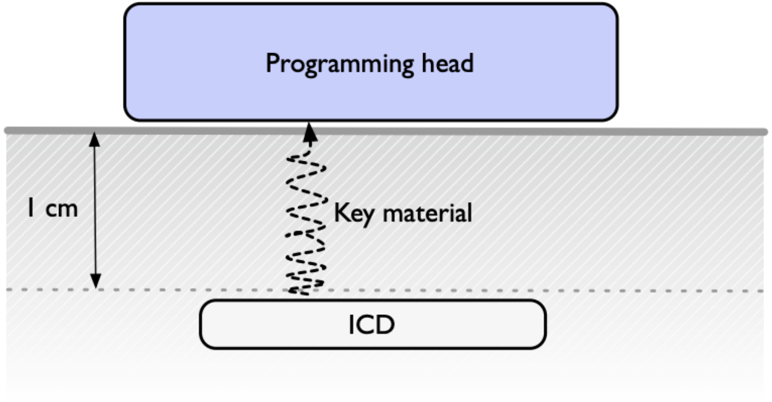


Fig. 9. Zero-power sensible key exchange: a nonce is transmitted from the ICD to the programmer using acoustic waves. It can be clearly picked up only if the programmer is in contact with the patient's body near the implantation site, and can be used as the secret key in the authentication protocol from the previous section. (1 cm is a typical implantation depth. Diagram is not to scale.)

Related Works

- IMD Security & Privacy
  - D.Halperin et Al. @ 2008
  - ★ **Security and privacy for implantable medical devices**

- Wireless Body Network
  - S.Warren et Al. @ 2005
  - ★ **Interoperability and security in wireless body area network infrastructures**

- Software Radios in Leveraging Wireless Protocols
  - D.Spill and R.J. Anderson. @ 2007
  - ★ **BlueSniff: Eve meets Alice and Bluetooth**

  - J.Lackey and D.Hulton. @ 2007
  - ★ **The A5 cracking project: Practical attacks on GSM using GNU radio and FPGAs**

Conclusion

- ❖ **First** to use general-purpose software radio for security analysis on **IMDs**
  - Leverage unknown IMD's wireless communication protocol

- ❖ Proved that IMDs like ICD is vulnerable to realistic attacks
  - Privacy leakage
  - Intended malfunctioning

- ❖ **Security and privacy properties should be considered in IMDs**
  - **<u>Tremendous changes after this research</u>**

Follow-Ups : Academia

❖ IMD Security & Privacy - 2011

- #1. S.Gollakota et Al. @ **SIGCOMM '11**
- **They can hear your heartbeats: non-invasive security for implantable medical devices**

  ⇥ Suggested better defense mechanisms without modifying the device itself
  ⇥ Extended research from 08's paper

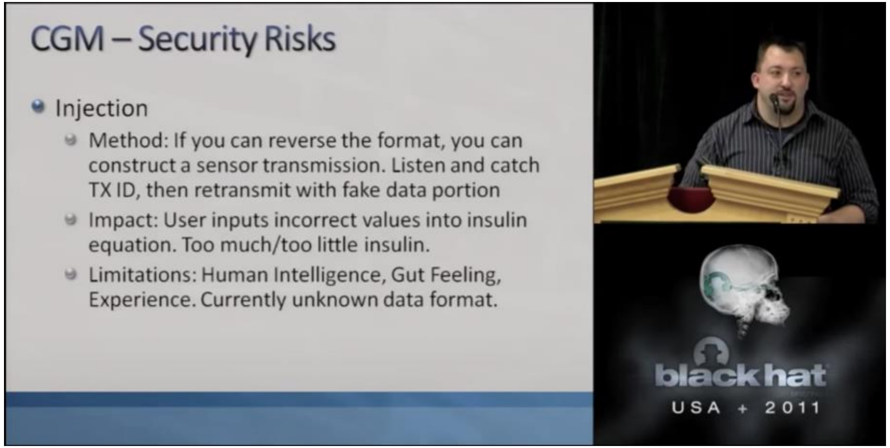
- #2. DF Kune et Al. @ **IEEE S&P '13**
- **Ghost Talk: Mitigating EMI Signal Injection Attacks against Analog Sensors**

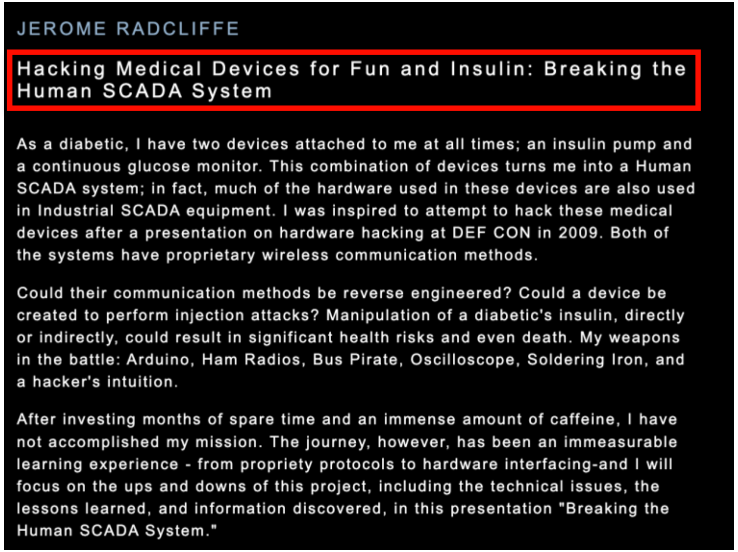
  ⇥ State-of-the-art attacks using EMI on ICDs

- #3. Youngseok Park Al. @ **WOOT' 16**
- **This Ain't Your Dose: Sensor Spoofing Attack on Medical Infusion Pump**

J.Radcliffe - Insulin Pump

- Jerome Radcliffe in **Blackhat 2011**
  - Hacked insulin pump, himself was a diabetic





JEROME RADCLIFFE

Hacking Medical Devices for Fun and Insulin: Breaking the Human SCADA System

As a diabetic, I have two devices attached to me at all times; an insulin pump and a continuous glucose monitor. This combination of devices turns me into a Human SCADA system; in fact, much of the hardware used in these devices are also used in Industrial SCADA equipment. I was inspired to attempt to hack these medical devices after a presentation on hardware hacking at DEF CON in 2009. Both of the systems have proprietary wireless communication methods.

Could their communication methods be reverse engineered? Could a device be created to perform injection attacks? Manipulation of a diabetic's insulin, directly or indirectly, could result in significant health risks and even death. My weapons in the battle: Arduino, Ham Radios, Bus Pirate, Oscilloscope, Soldering Iron, and a hacker's intuition.

After investing months of spare time and an immense amount of caffeine, I have not accomplished my mission. The journey, however, has been an immeasurable learning experience - from propriety protocols to hardware interfacing-and I will focus on the ups and downs of this project, including the technical issues, the lessons learned, and information discovered, in this presentation "Breaking the Human SCADA System."

SysSec
System Security Lab

J.Radcliffe in 2016

- Jerome Radcliff in **2016**
  - Again discovered more vulnerabilities in insulin pumps

R7-2016-07: Multiple Vulnerabilities in Animas OneTouch Ping Insulin Pump

Oct 04, 2016 | 7 min read | Tod Beardsley

Today we are announcing three vulnerabilities in the Animas OneTouch Ping insulin pump system, a popular pump with a blood glucose meter that services as a remote control via RF communication. Before we get into the technical details, we want to flag that we believe the risk of wide scale exploitation of these insulin pump vulnerabilities is relatively low, and we don't believe this is cause for panic. We recommend that users of the devices consult their healthcare providers before making major decisions regarding the use of these devices. More on that further down in this post.

Users should also be receiving notification of this issue, along with details for mitigating it, directly from Animas Corporation, via physical mail. We recommend you pay close attention to this communication.

Summary of findings

The OneTouch Ping insulin pump system uses cleartext communications rather than encrypted communications, i

its proprietary wireless management protocol. Due to this lack of encryption, Rapid7 researcher Jay Radcliffe discovered that a remote attacker can spoof the Meter Remote and trigger unauthorized insulin injections.

Barnaby Jack - Insulin Pump

- ❖ Barnaby Jack In **Hacker Halted 2011**

Barnaby Jack hacks diabetes insulin pump live at Hacker Halted

Perhaps most famous for his live hack of an ATM machine at Black Hat Las Vegas in 2010, Jack captivated the Hacker Halted audience by proving the insecurity of a particular (unspecified) brand of insulin pump.

Jack began the presentation by assuring the audience that his motives are honourable and stating the importance of "getting it out in the open".

At Black Hat this summer, a diabetes sufferer demonstrated that he could hack and shut down his own pump – but only his own. The display resulted in a lot of press coverage and the manufacturer in question released the following statement:

"The chance of an attack is very unlikely and almost impossible. It would be extremely difficult for a third-party to tamper remotely with a pump".

Jack proved this statement incorrect by scanning radio frequency and accessing implanted insulin pumps within a 300 meters range.

Jack used his friend, a diabetes sufferer, in the audience to demonstrate how he could then control the insulin dispersed remotely, or shut it down.

Jack received the biggest applause of the day from Hacker Halted delegates.

Related to This Story

ATM Hacker Barnaby Jack Dies at Age 35

The Insecure Pacemaker: FDA Issues Guidance for Wireless Medical Device Security

Barnaby Jack - IMD Security

- Barnaby Jack was **scheduled to be** In **BlackHat 2013**
  - Hacked Pacemakers

IMPLANTABLE MEDICAL DEVICES: HACKING HUMANS

PRESENTED BY

Barnaby Jack

In 2006 approximately 350,000 pacemakers and 173,000 ICD's (Implantable Cardioverter Defibrillators) were implanted in the US alone. 2006 was an important year, as that's when the FDA began approving fully wireless based devices. Today there are well over 3 million pacemakers and over 1.7 million ICD's in use.

This talk will focus on the security of wireless implantable medical devices. I will discuss how these devices operate and communicate and the security shortcomings of the current protocols. Our internal research software will be revealed that utilizes a common bedside transmitter to scan for, and interrogate individual medical implants.

I will also discuss ideas manufacturers can implement to improve the security of these devices.

Barnaby Jack Could Hack Your Pacemaker and Make Your Heart Explode

Having your heart wirelessly hacked and set to explode at 830 volts could be viewed as a bit of a setback if you're considering getting a pacemaker fitted. It could also be viewed as the kind of thing that would only happen in a Jason Statham movie...

Barnaby Jack, the director of embedded device security for computer security firm IOActive, developed software that allowed him to remotely send an electric shock to anyone wearing a pacemaker within a 50-foot radius. He also came up with a system that scans for any insulin pumps that communicate wirelessly within 300 feet, allowing you to hack into them without needing to know the identification numbers and then set them to dish out more or less insulin than necessary, sending patients into hypoglycemic shock.

Also slightly worrying is the software used in rudimentary hospital equipment. Relatively important medical devices—such as heart and blood pressure monitors, for example—use old software that is incredibly vulnerable to malware. Meaning anyone inclined to do so could corrupt the software, make it display the wrong vital signs and fool doctors into administering unnecessary medical procedures.

Barnaby Jack - IMD Security

- ❖ Barnaby Jack **Not** In **BlackHat 2013**
  - **Died a week before presentation**

The Switch

RIP Barnaby Jack: The hacker who wanted to save your life

By Andrea Peterson

July 29, 2013

Security researcher Barnaby Jack was found dead by a loved one in San Francisco Thursday night. Jack, 36, had been scheduled to make a presentation at the Black Hat Conference in Las Vegas on Aug. 1 showing how he was able to remotely shock a pacemaker. The San Francisco police have not released details about the death other than it was "not foul play." Survivors include Jack's mother and sister, who live in his native New Zealand.

Elite Hacker Barnaby Jack 'overdosed on drugs'

3 January 2014

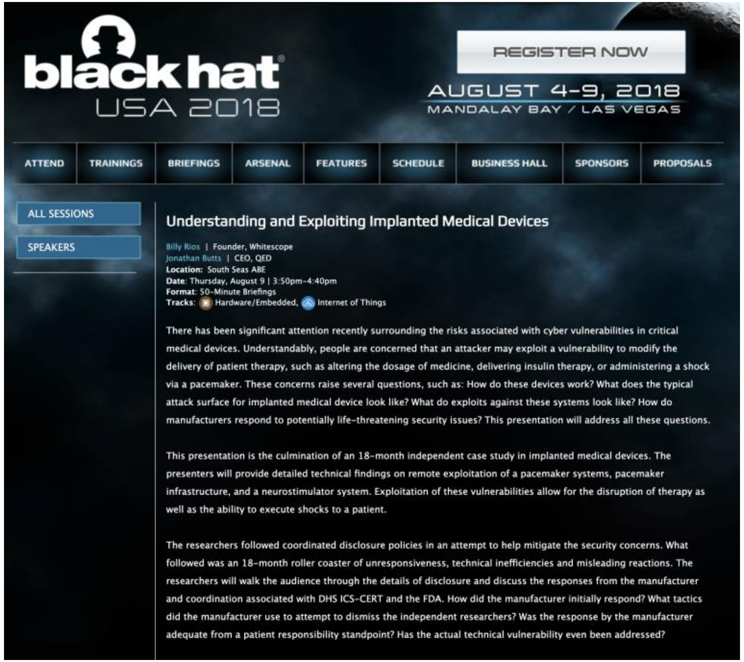
Barnaby Jack rose to fame after demonstrating how to hack a cashpoint

A world-renowned hacker, who died in San Francisco in July, overdosed on a mix of heroin, cocaine and other drugs, a coroner's report shows.

Billy Rios - New Pacemaker Vulnerabilities

❖ Billy Rios in **Blackhat 2018**

- Multiple Vulnerabilities in Pacemaker systems



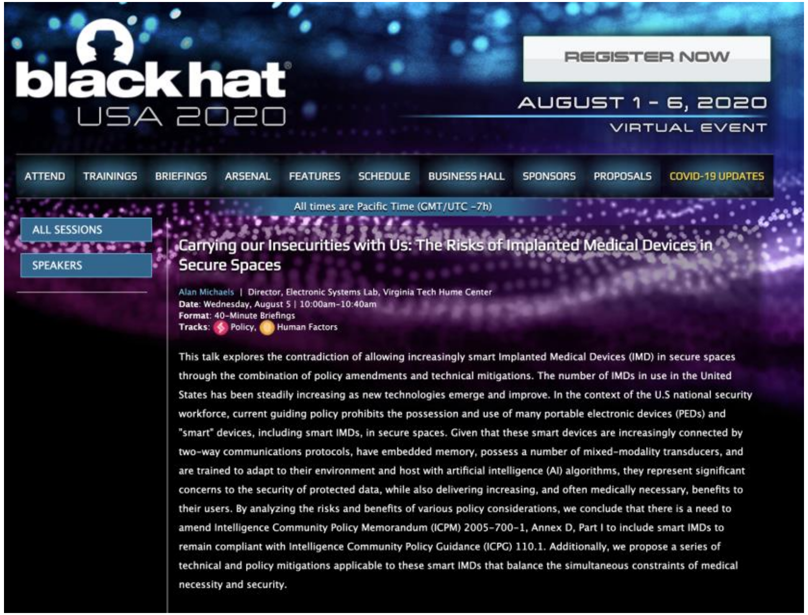
SysSec
System Security Lab

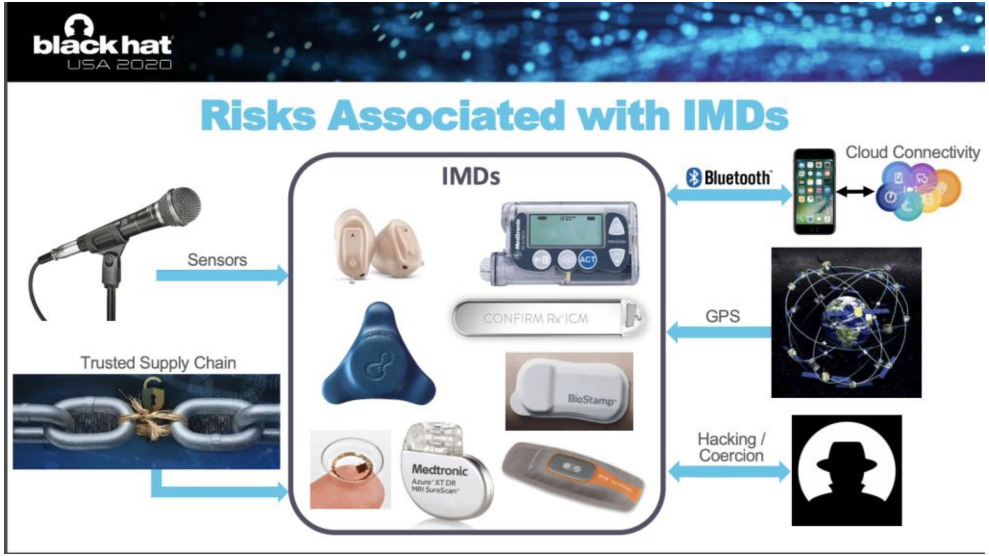
ARMIS - URGENT/11

❖ ARMIS in **Blackhat 2019**
- Found Vulnerabilities in **Vxworks RTOS**
  - ★ Used in medical devices (patient monitor, MRI, etc.)

Recently, in Blackhat 2020

- Alan Michales in **Blackhat 2020**
  - Multiple vulnerabilities in various medical devices



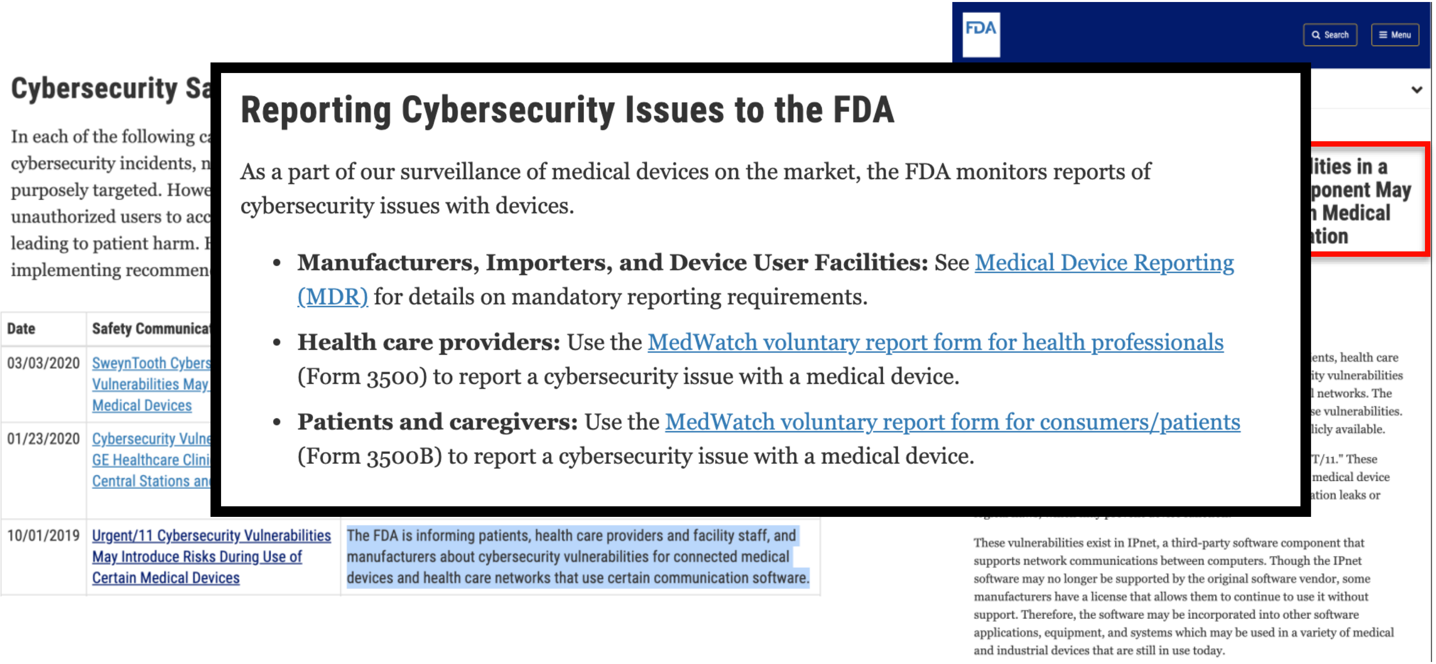


SysSec
System Security Lab

U.S. FDA - Safety Communications

❖ FDA informs critical security issues with '**Safety Communications**'

- Practices & Recommendations



SysSec
System Security Lab

U.S. FDA - Guidances

- FDA releases guidances for medical device industry
  - Dealing with both premarket & postmarket processes

FDA on Cybersecurity-related Content of Premarket Submissions

Jun 10, 2021

Cybersecurity Guidances

Date	Title	Description
10/18/2018	Draft Guidance: Content of Premarket Submissions for Management of Cybersecurity in Medical Devices	Provides recommendations to industry regarding cybersecurity device design, labeling, and documentation to be included in premarket submissions for devices with cybersecurity risk. When final, the recommendations are intended to supplement these guidance documents: • Guidance for the Content of Premarket Submissions for Software Contained in Medical Devices • Guidance to Industry: Cybersecurity for Networked Medical Devices Containing Off-the-Shelf (OTS) Software
12/27/2016	Final Guidance: Postmarket Management of Cybersecurity in Medical Devices	Provides recommendations to industry for structured and comprehensive management of postmarket cybersecurity vulnerabilities for marketed and distributed medical devices throughout the product lifecycle.
10/02/2014	Final Guidance: Content of Premarket Submissions for Management of Cybersecurity in Medical Devices	In addition to the specific recommendations contained in this guidance, manufacturers are encouraged to address cybersecurity throughout the product lifecycle, including during the design, development, production, distribution, deployment and maintenance of the device. The recommendations are intended to supplement these guidance documents: • Guidance for the Content of Premarket Submissions for Software Contained in Medical Devices • Guidance to Industry: Cybersecurity for Networked Medical Devices Containing Off-the-Shelf (OTS) Software
1/14/2005	Cybersecurity for Networked Medical Devices Containing Off-the-Shelf (OTS) Software	A growing number of medical devices are designed to be connected to computer networks. Many of these networked medical devices incorporate off-the-shelf software that is vulnerable to cybersecurity threats such as viruses and worms. These vulnerabilities may represent a risk to the safe and effective operation of networked medical devices and typically require an ongoing maintenance effort throughout the product life cycle to assure an adequate degree of protection. The FDA issued guidance to clarify how existing regulations, including the Quality System (QS) Regulation, apply to such cybersecurity maintenance activities.

U.S. FDA - Guidances

- FDA collaborates with other working groups for security issues in Medical Devices
  - **Global medical device cybersecurity guide** with **IMDRF**

Other Collaborations on Cybersecurity in Medical Devices

International Medical Device Regulators Forum (IMDRF): The FDA serves as a co-chair of the IMDRF working group tasked with drafting a global medical device cybersecurity guide. The purpose of the guide is to promote a globally harmonized approach to medical device cybersecurity that at a fundamental level ensures the safety and performance of medical devices while encouraging innovation. The guide is thus intended to provide medical device cybersecurity advice for stakeholders across the device lifecycle on topics including but not limited to medical device cybersecurity terminology, stakeholders' shared responsibility, and information sharing. The finalized guide was published on March 18, 2020.

IMDRF/CYBER WG/N60FINAL:2020

IMDRF International Medical Device Regulators Forum

FINAL DOCUMENT

Title: Principles and Practices for Medical Device Cybersecurity

Authoring Group: Medical Device Cybersecurity Working Group

Date: 18 March 2020

Dr Choong May Ling, Mimi, IMDRF Chair

Q&A

- ❖ Best Question #1 by Jun-Ha Jang
  - **Safety (IEC 61508) vs Security**
    - → **Gap** between their perceptions about safety and security

- ❖ Best Question #2 by Jeong-Han Yoon
  - The range of attack is too short (Within 10cm). **Is it possible to attack in longer distance?**
    - → Definitely possible with RF signals
    - → Barnaby Jack's Insulin Pump hacking : Hacked from 90m, using **high-gain antenna (HGA)**

- ❖ Other **Not Selected** Questions

Thank You

yhlee0078@kaist.ac.kr

KAIST

SysSec
System Security Lab