



# Hacking Medical Devices

All your vital signs are belong to us ...

## Florian Grunow

- Security Analyst
- ERNW GmbH in Heidelberg
- Pentesting
- Application Security
- Research: Medical Devices



## Agenda

---



- Motivation
- Publications
- The Problem
- Targets
- Findings so far
- Questions

# Disclaimer

---

All products, company names, brand names, trademarks and logos are the property of their respective owners!

# Motivation

---

Make the world a safer place ...

# Motivation

## ▢ Importance

- We trust these devices
- Doctors trust these devices

## ▢ Technology

- Rocket science: e.g. MRI
- Proprietary protocols
- Every device is different

# Publications so far ...

---

What has been done ...



## Medical Devices

Home Medical Devices Medical Device Safety Safety Communications

### Medical Device Safety

#### Safety Communications

Information About Heparin

Medical Device Safety Archive

#### Tubing and Luer

#### Misconnections: Preventing Dangerous Medical Errors

## FDA Safety Communication: Cybersecurity for Medical Devices and Hospital Networks

**Date Issued:** June 13, 2013

**Audience:** Medical device manufacturers, hospitals, medical device user facilities, health care IT and procurements staff, and biomedical engineers

**Issue:** Cybersecurity for medical devices and hospital networks

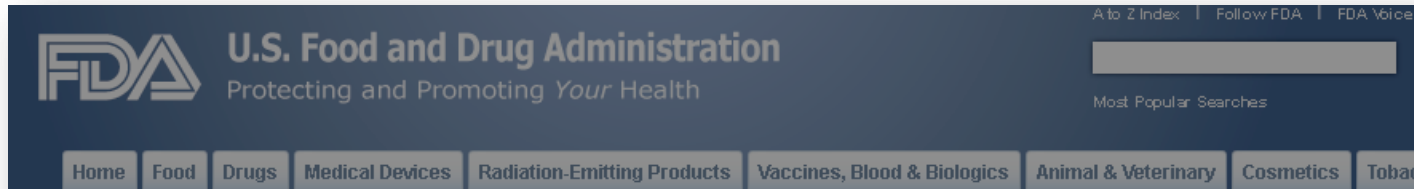
**Purpose:** The FDA is recommending that medical device manufacturers and health care facilities take steps to assure that appropriate safeguards are in place to reduce the risk of failure due to cyberattack, which could be initiated by the introduction of malware into the medical equipment or unauthorized access to configuration settings in medical devices and hospital networks.

**Summary of Problem and Scope:** Many medical devices contain configurable embedded computer systems that can be vulnerable to cybersecurity breaches. In addition, as medical devices are increasingly interconnected, via the Internet, hospital networks, other medical device, and smartphones, there is an increased risk of cybersecurity breaches, which could affect how a medical device operates.

Recently, the FDA has become aware of cybersecurity vulnerabilities and incidents that could directly impact medical devices or hospital network operations, including:

- Network-connected/configured medical devices infected or disabled by malware;
- The presence of malware on hospital computers, smartphones and tablets, targeting mobile devices using wireless technology to access patient data, monitoring systems, and implanted patient devices;
- Uncontrolled distribution of passwords, disabled passwords, hard-coded passwords for software intended for privileged device access (e.g., to administrative, technical, and maintenance personnel);
- Failure to provide timely security software updates and patches to medical devices and networks and to address related vulnerabilities in older medical device models (legacy devices);





FDA U.S. Food and Drug Administration  
Protecting and Promoting *Your* Health

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

## Medical Devices

Home Medical Devices Medical Device Safety Safety Communications

### FDA Safety Communication: Cybersecurity for Medical Devices and

**Purpose:** The FDA is recommending that medical device manufacturers and health care facilities take steps to assure that appropriate safeguards are in place to reduce the risk of failure due to cyberattack, which could be initiated by the introduction of malware into the medical equipment or unauthorized access to configuration settings in medical devices and hospital networks.

Misconnections: Preventing  
Dangerous Medical Errors

**Purpose:** The FDA is recommending that medical device manufacturers and health care facilities take steps to assure that appropriate safeguards are in place to reduce the risk of failure due to cyberattack, which could be initiated by the introduction of malware into the medical equipment or unauthorized access to configuration settings in medical devices and hospital networks.

**Summary of Problem and Scope:** Many medical devices contain configurable embedded computer systems that can be vulnerable to cybersecurity breaches. In addition, as medical devices are increasingly interconnected, via the Internet, hospital networks, other medical device, and smartphones, there is an increased risk of cybersecurity breaches, which could affect how a medical device operates.

Recently, the FDA has become aware of cybersecurity vulnerabilities and incidents that could directly impact medical devices or hospital network operations, including:

- Network-connected/configured medical devices infected or disabled by malware;
- The presence of malware on hospital computers, smartphones and tablets, targeting mobile devices using wireless technology to access patient data, monitoring systems, and implanted patient devices;
- Uncontrolled distribution of passwords, disabled passwords, hard-coded passwords for software intended for privileged device access (e.g., to administrative, technical, and maintenance personnel);
- Failure to provide timely security software updates and patches to medical devices and networks and to address related vulnerabilities in older medical device models (legacy devices);

# McAfee Hacker Says Medtronic Insulin Pumps Vulnerable to Attack

By Jordan Robertson - 2012-02-29T15:00:00Z

Some [Medtronic Inc. \(MDT\)](#) insulin pumps are vulnerable to a hacking attack that could let someone break into the devices from hundreds of feet away, disable security alarms and dump insulin directly into diabetics' bloodstreams, according to a computer-security researcher at McAfee Inc.

Barnaby Jack, who works as a professional hacker for [McAfee](#), said he can remotely control several types of Medtronic pumps. After first discussing the vulnerability last year at a small hacker conference in [Florida](#), he has discovered more ways to exploit the weakness, including overriding security features such as vibration warnings.

Jack, who plans to spotlight the flaw this week at the [RSA security conference](#) in San Francisco, is trying to increase awareness of the risks of medical devices. Insulin pumps are pager-sized gadgets that diabetics wear to dispense the lifesaving hormone into the body. Such technology is increasingly relying on wireless communications, making it vulnerable to the same hacking that afflicts personal computers.

"These are computers that are just as exploitable as your PC or Mac, but they're not looked at as often," Jack, 34, said in an interview. "When you actually look at these devices, the security

# McAfee Hacker Says Medtronic Insulin Pumps Vulnerable to Attack

By Jordan Robertson - 2012-02-29T15:00:00Z

Some [Medtronic Inc. \(MDT\)](#) insulin pumps are vulnerable to a hacking attack that could let

Barnaby Jack, who works as a professional hacker for [McAfee](#), said he can remotely control several types of Medtronic pumps. After first discussing the vulnerability last year at a small hacker conference in [Florida](#), he has discovered more ways to exploit the weakness, including overriding security features such as vibration warnings.

hacker conference in [Florida](#), he has discovered more ways to exploit the weakness, including overriding security features such as vibration warnings.

Jack, who plans to spotlight the flaw this week at the [RSA security conference](#) in San Francisco, is trying to increase awareness of the risks of medical devices. Insulin pumps are pager-sized gadgets that diabetics wear to dispense the lifesaving hormone into the body. Such technology is increasingly relying on wireless communications, making it vulnerable to the same hacking that afflicts personal computers.

"These are computers that are just as exploitable as your PC or Mac, but they're not looked at as often," Jack, 34, said in an interview. "When you actually look at these devices, the security

## Alert (ICS-ALERT-13-164-01)

### Medical Devices Hard-Coded Passwords

Original release date: June 13, 2013



#### SUMMARY

Researchers Billy Rios and Terry McCorkle of Cylance have reported a hard-coded password vulnerability affecting roughly 300 medical devices across approximately 40 vendors. According to their report, the vulnerability could be exploited to potentially change critical settings and/or modify device firmware.

Because of the critical and unique status that medical devices occupy, ICS-CERT has been working in close cooperation with the Food and Drug Administration (FDA) in addressing these issues. ICS-CERT and the FDA have notified the affected vendors of the report and have asked the vendors to confirm the vulnerability and identify specific mitigations. ICS-CERT is issuing this alert to provide early notice of the report and identify baseline mitigations for reducing risks to these and other cybersecurity attacks. ICS-CERT and the FDA will follow up with specific advisories and information as appropriate.

The report included vulnerability details for the following vulnerability

Vulnerability Type	Remotely Exploitable	Impact
Hard-coded password	Yes, device dependent	Critical settings/device firmware modification

The affected devices have hard-coded passwords that can be used to permit privileged access to devices such as passwords that would normally be used only by a service technician. In some devices, this access could allow critical settings or the device firmware to be modified.

# Alert (ICS-ALERT-13-164-01)

More Alerts



## Medical Devices Hard-Coded Passwords

Original release date: June 13, 2013

[Print](#) [Tweet](#) [Send](#) [Share](#)

### SUMMARY

Researchers Billy Rios and Terry McCorkle of Cylance have reported a hard-coded password vulnerability affecting

Researchers Billy Rios and Terry McCorkle of Cylance have reported a hard-coded password vulnerability affecting roughly 300 medical devices across approximately 40 vendors. According to their report, the vulnerability could be exploited to potentially change critical settings and/or modify device firmware.

affected vendors of the report and have asked the vendors to confirm the vulnerability and identify specific mitigations. ICS-CERT is issuing this alert to provide early notice of the report and identify baseline mitigations for reducing risks to these and other cybersecurity attacks. ICS-CERT and the FDA will follow up with specific advisories and information as appropriate

The report included vulnerability details for the following vulnerability

Vulnerability Type	Remotely Exploitable	Impact
Hard-coded password	Yes, device dependent	Critical settings/device firmware modification

The affected devices have hard-coded passwords that can be used to permit privileged access to devices such as passwords that would normally be used only by a service technician. In some devices, this access could allow critical settings or the device firmware to be modified.

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

Daniel Halperin<sup>†</sup>  
University of Washington

Thomas S. Heydt-Benjamin<sup>†</sup>  
University of Massachusetts Amherst

Benjamin Ransford<sup>†</sup>  
University of Massachusetts Amherst

Shane S. Clark  
University of Massachusetts Amherst

Benessa Defend  
University of Massachusetts Amherst

Will Morgan  
University of Massachusetts Amherst

Kevin Fu, PhD\*  
University of Massachusetts Amherst

Tadayoshi Kohno, PhD\*  
University of Washington

William H. Maisel, MD, MPH\*  
BIDMC and Harvard Medical School

**Abstract**—Our study analyzes the security and privacy properties of an implantable cardioverter defibrillator (ICD). Introduced to the U.S. market in 2003, this model of ICD includes pacemaker technology and is designed to communicate wirelessly with a nearby external programmer in the 175 kHz frequency range. After partially reverse-engineering the ICD's communications protocol with an oscilloscope and a software radio, we implemented several software radio-based attacks that could compromise patient safety and patient privacy. Motivated by our desire to improve patient safety, and mindful of conventional trade-offs between security and power consumption for resource-constrained devices, we introduce three new zero-power defenses based on RF power harvesting. Two of these defenses are human-centric, bringing patients into the loop with respect to the security and privacy of their implantable medical devices (IMDs). Our contributions provide a scientific baseline for understanding the

this event to a health care practitioner who uses a *commercial device programmer*<sup>1</sup> with wireless capabilities to extract data from the ICD or modify its settings without surgery. Between 1990 and 2002, over 2.6 million pacemakers and ICDs were implanted in patients in the United States [19]; clinical trials have shown that these devices significantly improve survival rates in certain populations [18]. Other research has discussed potential security and privacy risks of IMDs [1], [10], but we are unaware of any rigorous public investigation into the observable characteristics of a real commercial device. Without such a study, it is impossible for the research community to assess or address the security and privacy properties of past, current, and future devices. We address that gap in this paper

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



Daniel Halperin<sup>†</sup>  
University of Washington

Thomas S. Heydt-Benjamin<sup>†</sup>  
University of Massachusetts Amherst

Benjamin Ransford<sup>†</sup>  
University of Massachusetts Amherst

Shane S. Clark  
University of Massachusetts Amherst

Benessa Defend  
University of Massachusetts Amherst

Will Morgan  
University of Massachusetts Amherst

**Abstract**—Our study analyzes the security and privacy properties of an implantable cardioverter defibrillator (ICD). Introduced to the U.S. market in 2003, this model of ICD includes pacemaker technology and is designed to communicate wirelessly with a nearby external programmer in the 175 kHz frequency range. After partially reverse-engineering the ICD's communications protocol with an oscilloscope and a software radio, we implemented several software radio-based attacks that could compromise patient safety and patient privacy. Motivated by

trade-offs between security and power consumption for resource-constrained devices, we introduce three new zero-power defenses based on RF power harvesting. Two of these defenses are human-centric, bringing patients into the loop with respect to the security and privacy of their implantable medical devices (IMDs). Our contributions provide a scientific baseline for understanding the

PH\*  
School  
commercial  
ract data  
Between  
Ds were  
cal trials  
survival  
discussed  
but we  
the ob-  
servable characteristics of a real commercial device. Without such a study, it is impossible for the research community to assess or address the security and privacy properties of past, current, and future devices. We address that gap in this paper

# The Problem

---

Anamnesis ...





## Siemens Sirecust BS1

In the old days ...



## Nihon Kohden Neurofax EEG

In the old days ...

# The Change

- ▢ Optimization of processes
  - Good or bad?
- ▢ New com options available
  - Lowering costs
- ▢ Especially on Intensive Care Units (ICUs)
- ▢ Interoperability
  - E-Health records
  - PACS
  - Personal Health



## The Gathering

---

Standard anesthesia devices

# Are we Ready?

- What about IT in hospitals?
  - Resources / Know-how
  - Different types of networks
    - Doctors
    - Patients
    - Devices
    - Guests
    - Research
  - “Semi-New” technologies on the rise -> No experience
  - Remote maintenance (non-optional?)

# Are we Ready?

- What about home monitoring?
  - Devices for personal health
  - Transmitting wireless / Upload to provider
  - Need to be integrated without hassle
    - What could possibly go wrong?
    - Think pre-calculated encryption keys in home routers
  - Must not be expensive

# Are they Ready?

- What about the vendors?
  - Same mistakes again?
  - Learning curve
    - WiFi
    - Car keys
    - Exploiting like in the old days?

# What is Important for Compliance?

- **Focus is on safety not security**
  - Especially important in Germany
  - We do not even have these words ...
  - Safety mostly works
  - Does security?
  - Certification
    - Focus on safety, too



## Problem Summary

- Little resources on customer's side
- Little experience with incidents on vendor/hospital side
- Safety vs. Security

→ This could kill you!

# Targets

---

What are we looking at?

# Targets

- Medical devices with enabled com
  - Com is in places you would never suspect
- “Severity Rating”:
  - Low: Monitoring stuff
  - Medium: Diagnostic systems
  - High: Feedback to patient

# Monitoring



# Diagnostic



# Feedback



# Targets

- Hard to get hands on devices
  - Vendors have little interest?
    - Lack of experience?
  - Expensive
  - Cooperations
    - What about liability?
- Hard to test!

# Targets

---

What we looked at so far ...



## Target Example: EEG

- Measures “brain waves”
- Used in small/medium sized medical offices
- Grey box and software on a host
- Communication via LAN
  - Can be deployed in different rooms
- Grey box <- UDP -> Host
- No auth, no encryption, no security
- Full remote control of the box

## Off-Topic for a Second ...

- ▭ OpenEEG project
- ▭ Build your own EEG
- ▭ Do crazy Biofeedback stuff
- ▭ Brain-to-computer interface



## DIY: EEG

---

OpenEEG Project

# Disclaimer

---

There will be no details yet on how the exploits work as this might pose a threat to life or the physical condition of patients!

# Target: Patient Monitor 1

- Widely used in hospitals
  - ICU
  - During operation
- Monitors critical vital signs
  - SpO2
  - Blood Pressure
  - ECG
  - Temperature
  - Respiration
  - More ...

# Target: Syringe Pump

---

Demo: Infusion Override

# Target: Patient Monitor 2

## - 2 central elements

- ARM for peripherals and probably signal processing
  - Control the pump for blood pressure
  - Maybe FFT
- ARM for user interaction
  - RX / TX to the peripheral board
  - ARM926EJ-S @ 400MHz
  - 64MB RAM

# Target: Patient Monitor 2

---

Demo: Pwning vital signs



# Targets

- There is more to come!
  - Cooperations with hospitals
- Information Gathering reveals promising results
  - Radiology Equipment:
    - MRIs
    - X-Rays
  - Hospital Infrastructure

## Final Words ...

- We need to test these devices!
- Responsible disclosure process is critical!
- Get your hands dirty! 😊
- There will be more publications from ERNW!

→ Stay tuned!



# Thank you!

Please consult your doctor or pharmacist for risks and side effects of this presentation ...