Hacking Medical Devices

All your vital signs are belong to us …

Florian Grunow

- Security Analyst
- ERNW GmbH in Heidelberg
- Team Lead: Pentests
- 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

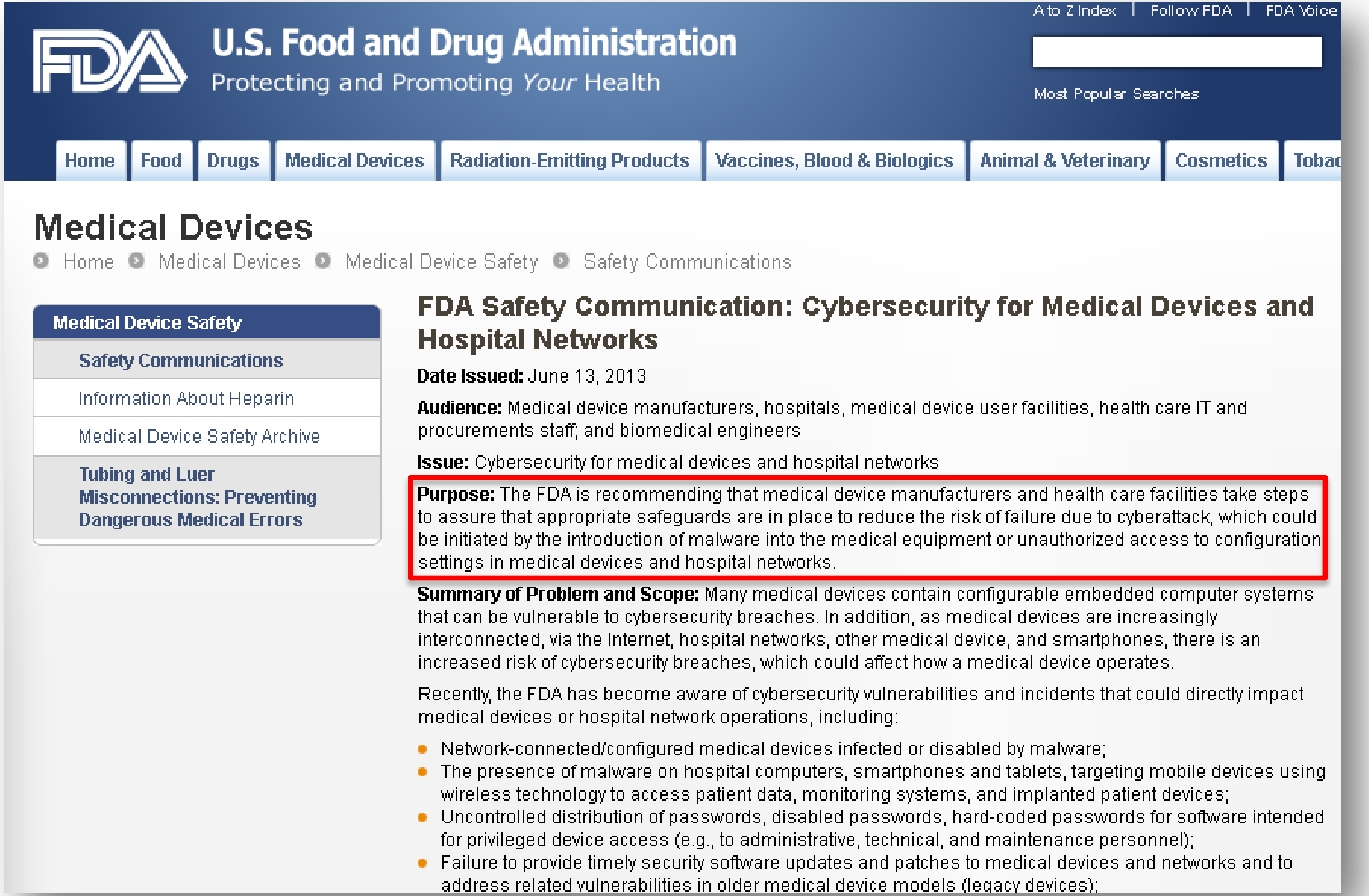
Make the world a safer place …

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 …



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

A to Z Index | Follow FDA | FDA Voice

Most Popular Searches

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

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

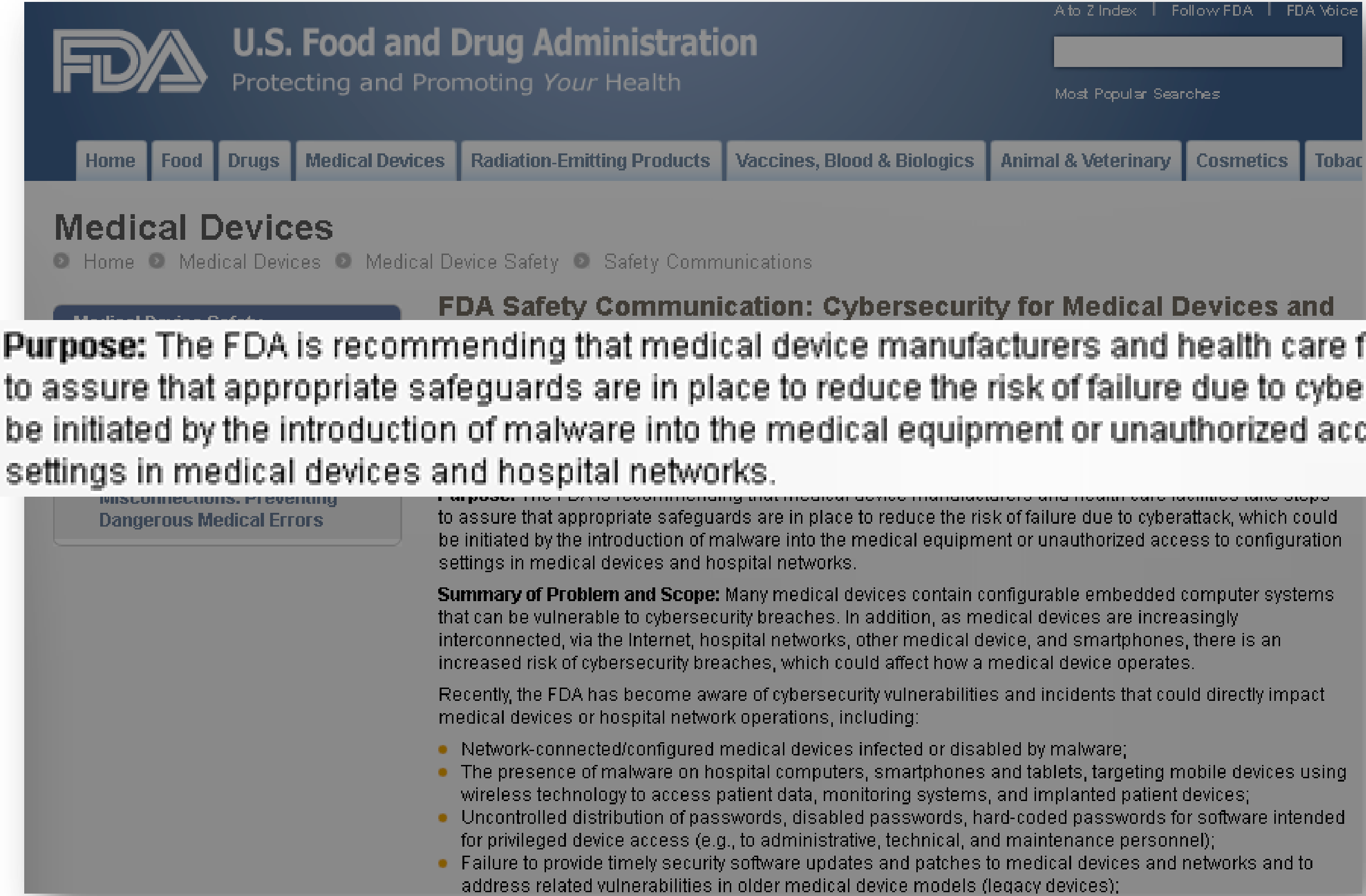
Issue: Cybersecurity for medical devices and hospital networks

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);



A to Z Index | Follow FDA | FDA Voice
Most Popular Searches
Home
Food
Drugs
Medical Devices
Radiation-Emitting Products
Vaccines, Blood & Biologics
Animal & Veterinary
Cosmetics
Tobac

U.S. Food and Drug Administration

Protecting and Promoting *Your* Health

Medical Devices

Home › Medical Devices › Medical Device Safety › Safety Communications

Misconnections: Preventing Dangerous Medical Errors

FDA Safety Communication: Cybersecurity for Medical Devices and

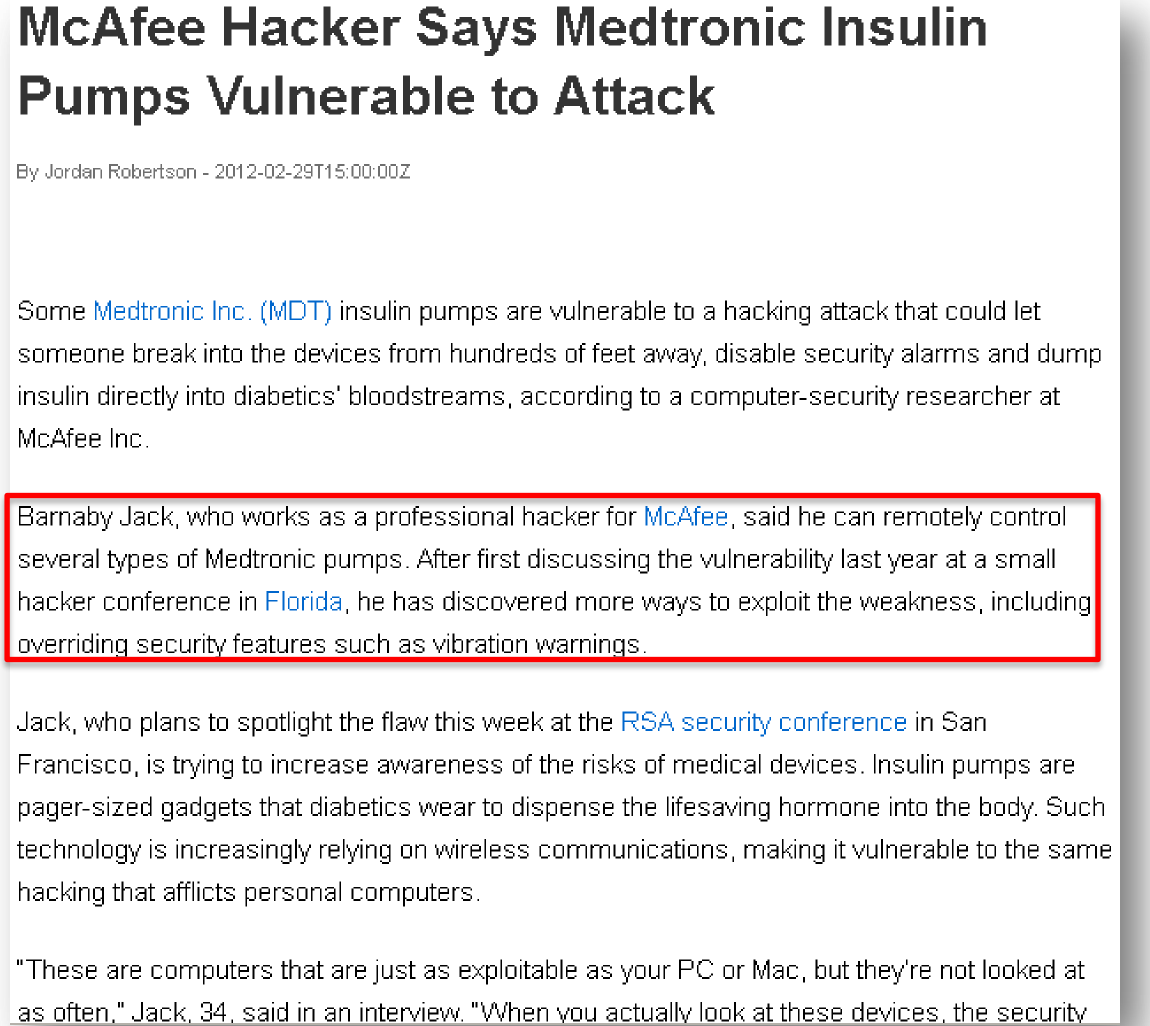
Purpose: The FDA is recommending that medical device manufacturers and health care facilities take steps to assure that appropriate safeguards are in place to reduce the risk of failure due to cyberattack, which could be initiated by the introduction of malware into the medical equipment or unauthorized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

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

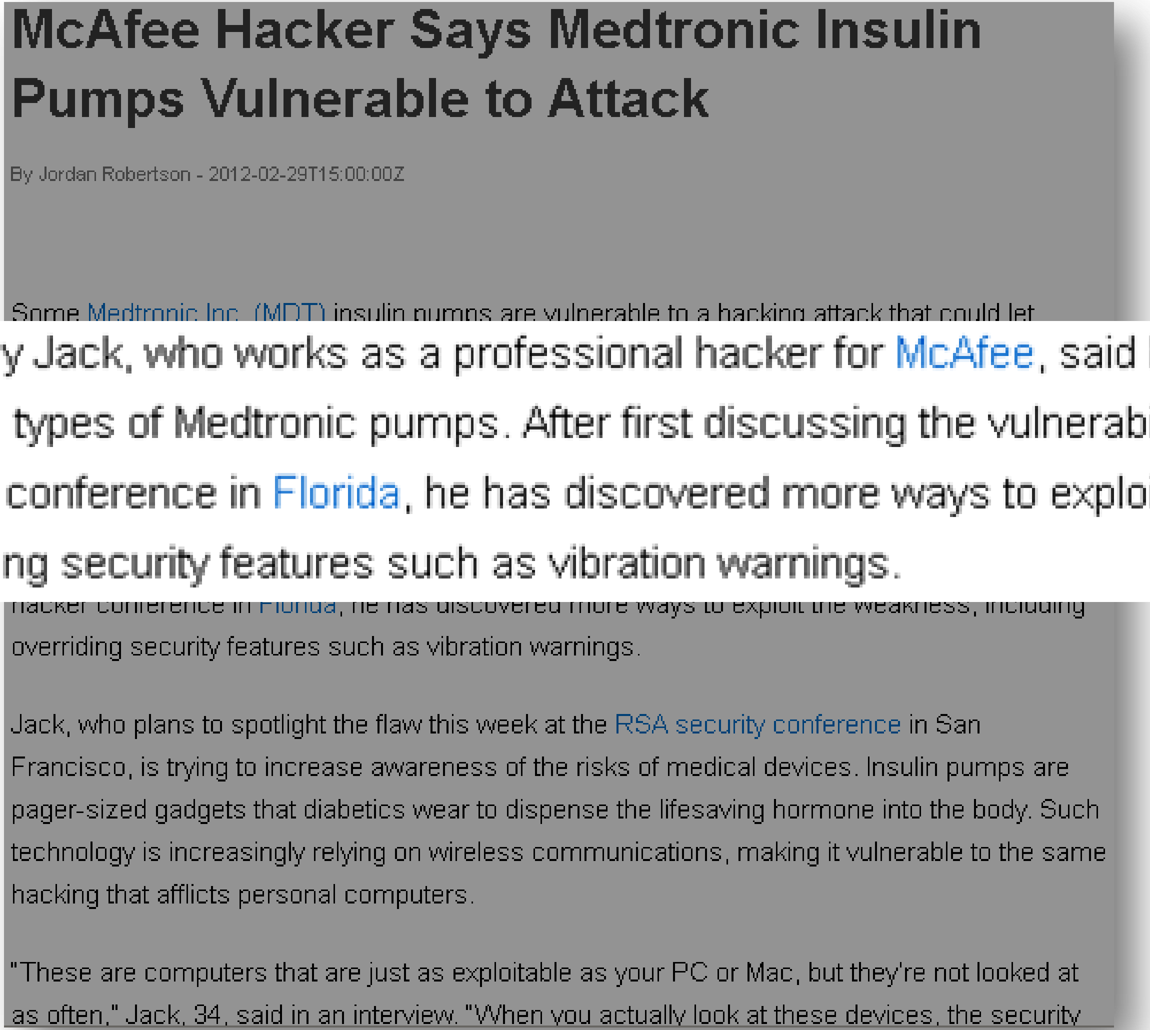
By Jordan Robertson - 2012-02-29T15:00:00Z

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

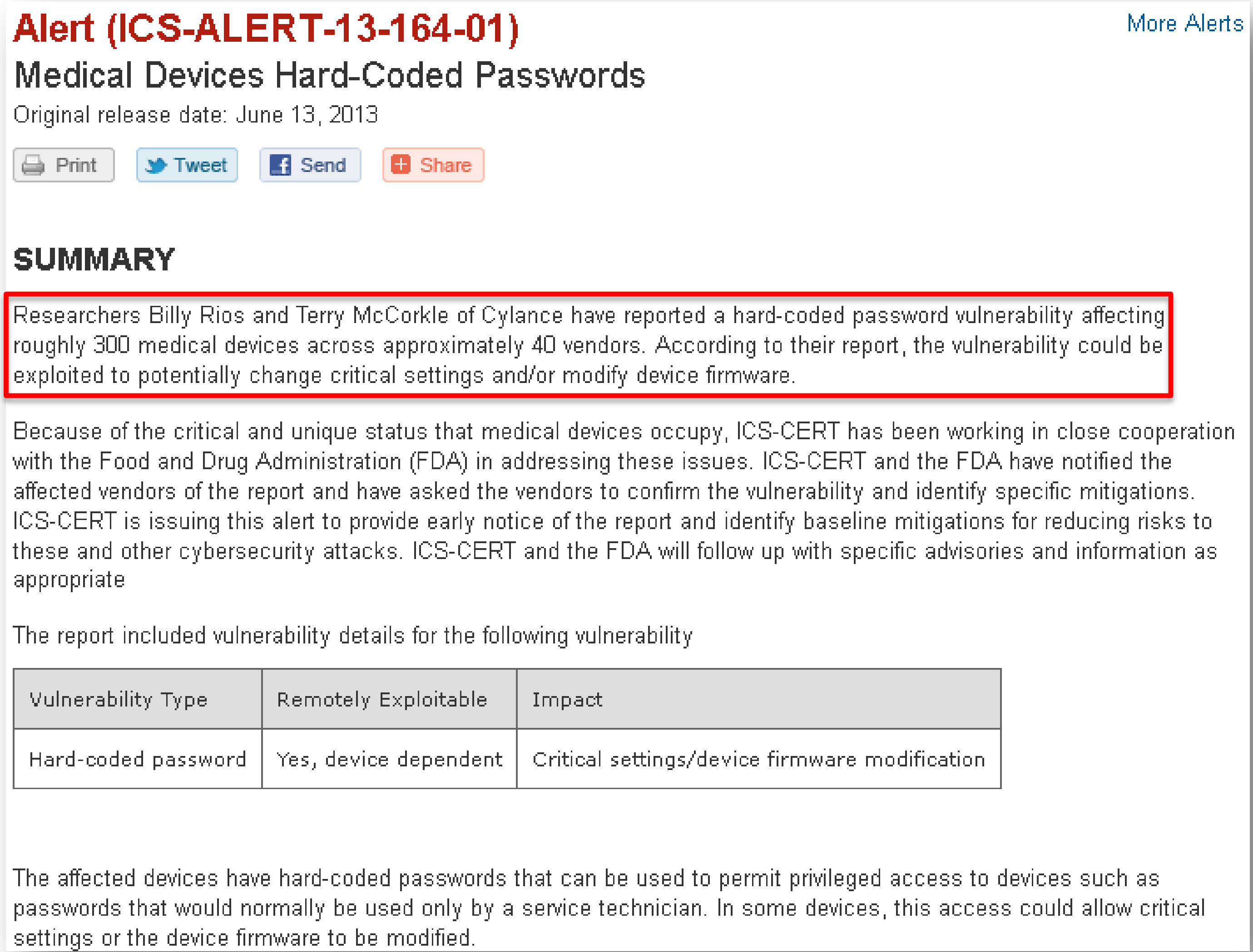
Some Medtronic Inc. (MDT) insulin pumps are vulnerable to a hacking attack that could let

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

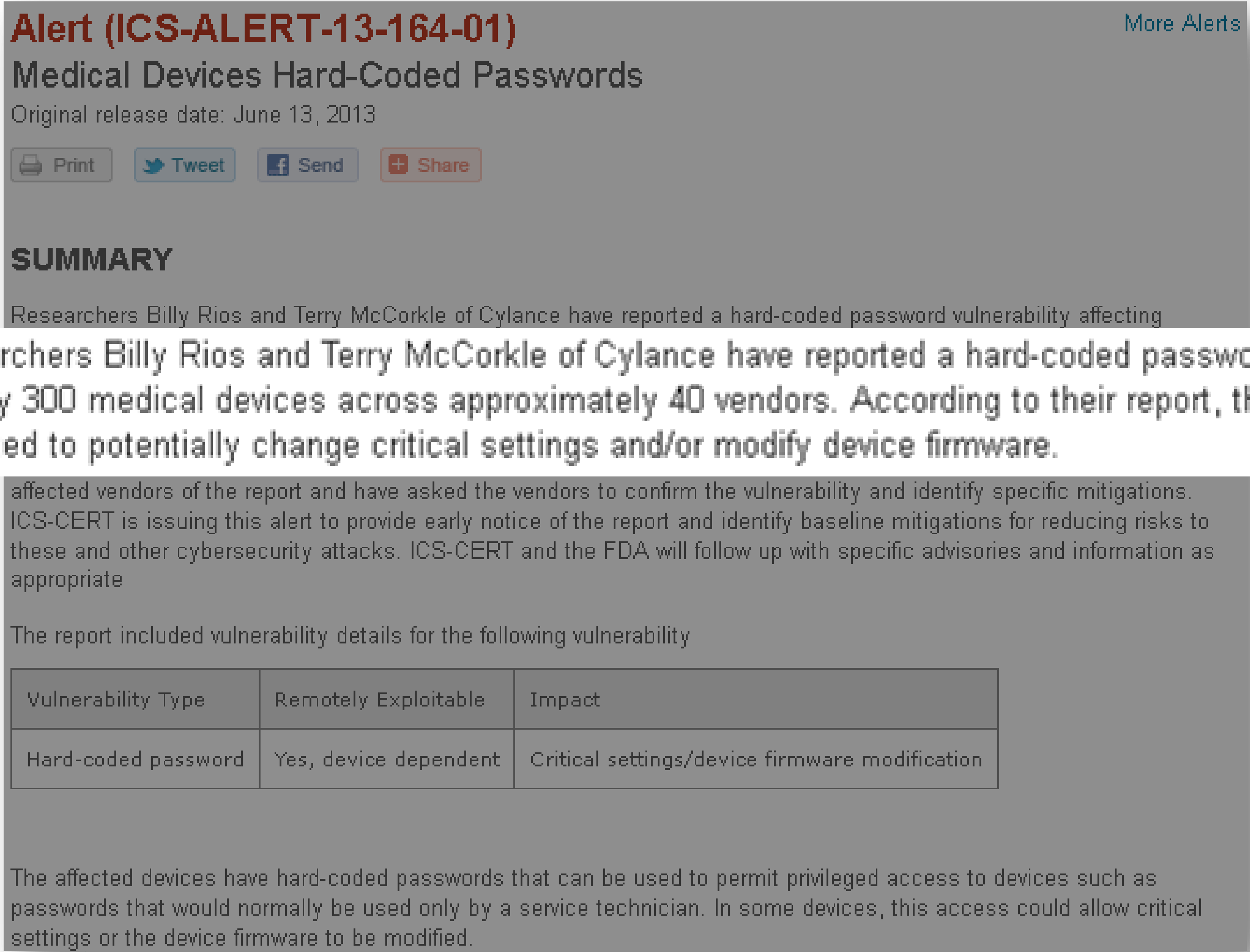
Researchers Billy Rios and Terry McCorkle of Cylance have reported a hard-coded password vulnerability affecting roughly 300 medical devices across approximately 40 vendors. According to their report, the vulnerability could be exploited to potentially change critical settings and/or modify device firmware.

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)

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

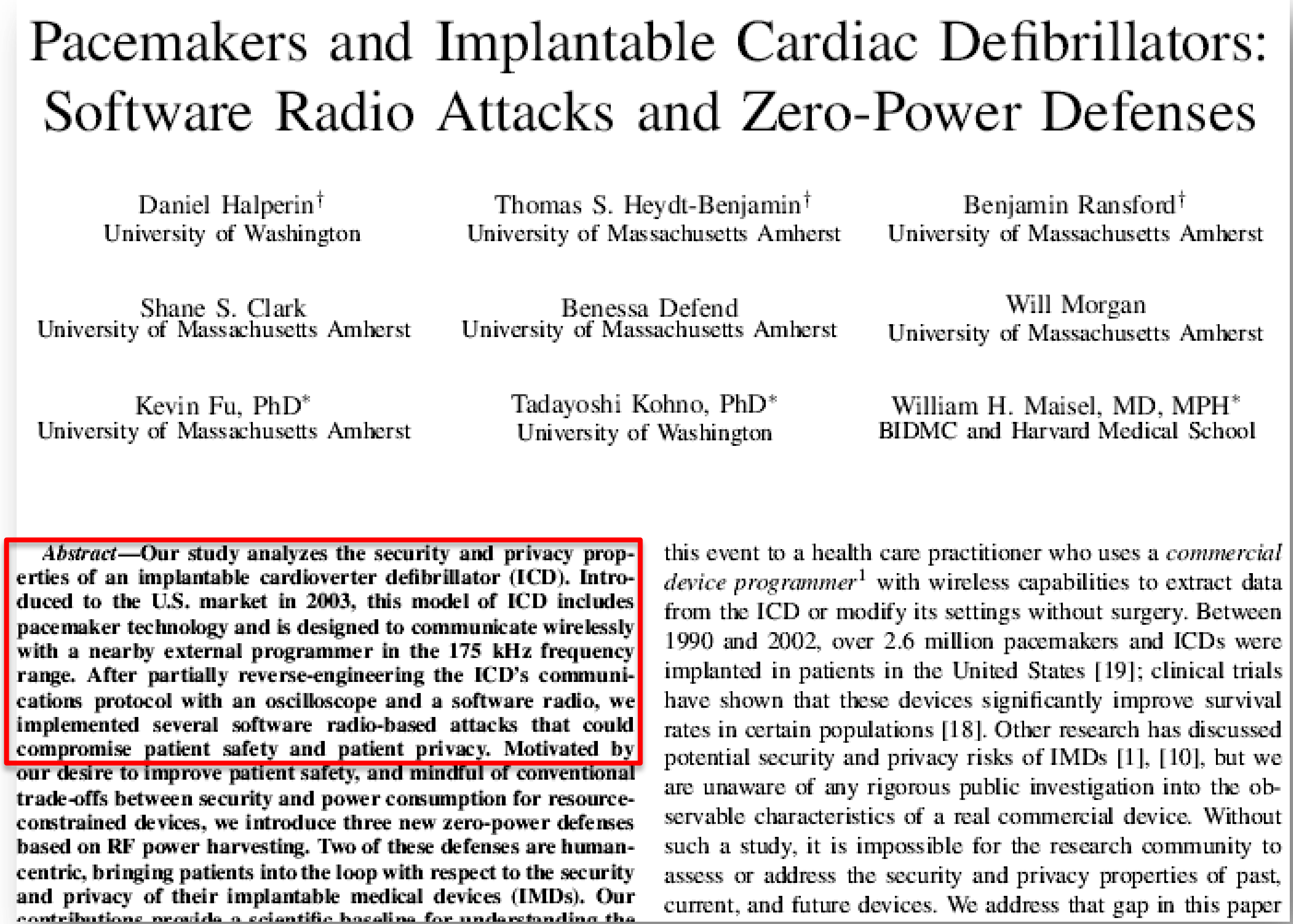
Researchers Billy Rios and Terry McCorkle of Cylance have reported a hard-coded password vulnerability affecting roughly 300 medical devices across approximately 40 vendors. According to their report, the vulnerability could be exploited to potentially change critical settings and/or modify device firmware.

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†
University of Washington

Thomas S. Heydt-Benjamin†
University of Massachusetts Amherst

Benjamin Ransford†
University of Massachusetts Amherst

Shane S. Clark
University of Massachusetts Amherst

Benessa Defend
University of Massachusetts Amherst

Will Morgan
University of Massachusetts Amherst

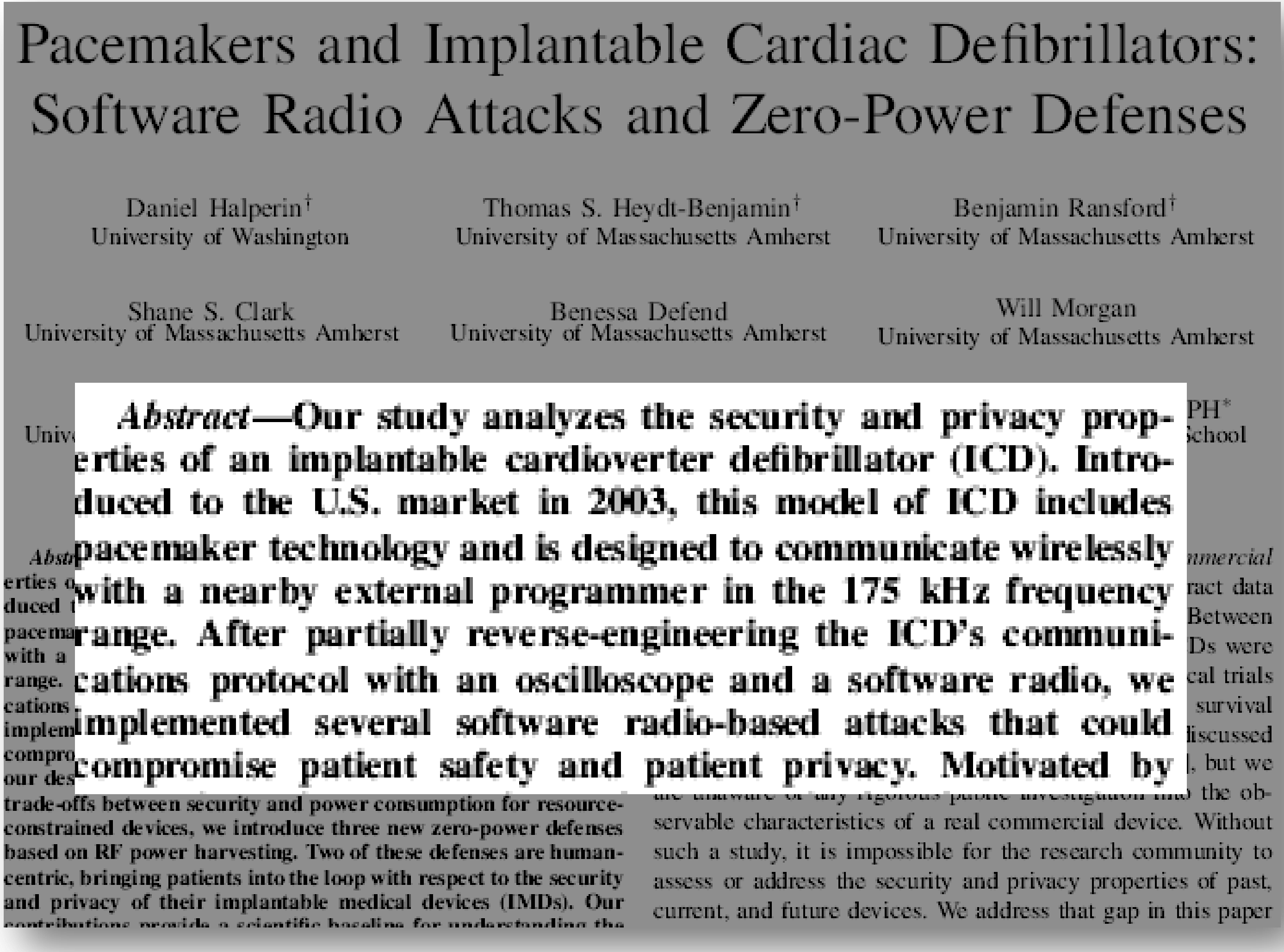
Kevin Fu, PhD*
University of Massachusetts Amherst

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*[1] 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[†]
University of Washington

Thomas S. Heydt-Benjamin[†]
University of Massachusetts Amherst

Benjamin Ransford[†]
University of Massachusetts Amherst

Shane S. Clark
University of Massachusetts Amherst

Benessa Defend
University of Massachusetts Amherst

Will Morgan
University of Massachusetts Amherst

Univ

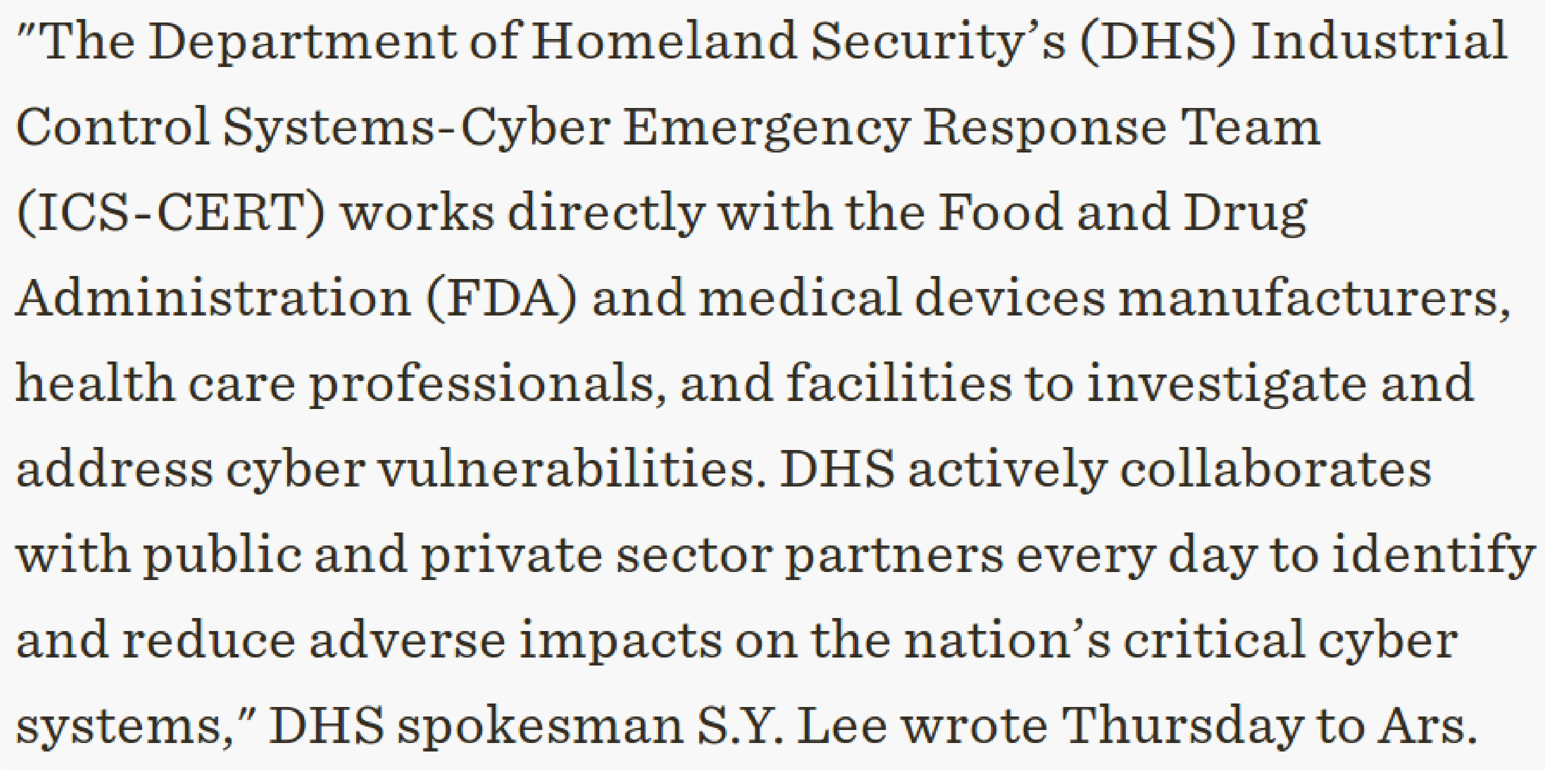
PH*
School

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

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

mmercial
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

http://arstechnica.com/tech-policy/2014/10/feds-examining-medical-devices-for-fatal-cybersecurity-flaws/



"The Department of Homeland Security's (DHS) Industrial Control Systems-Cyber Emergency Response Team (ICS-CERT) works directly with the Food and Drug Administration (FDA) and medical devices manufacturers, health care professionals, and facilities to investigate and address cyber vulnerabilities. DHS actively collaborates with public and private sector partners every day to identify and reduce adverse impacts on the nation's critical cyber systems," DHS spokesman S.Y. Lee wrote Thursday to Ars.

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?)

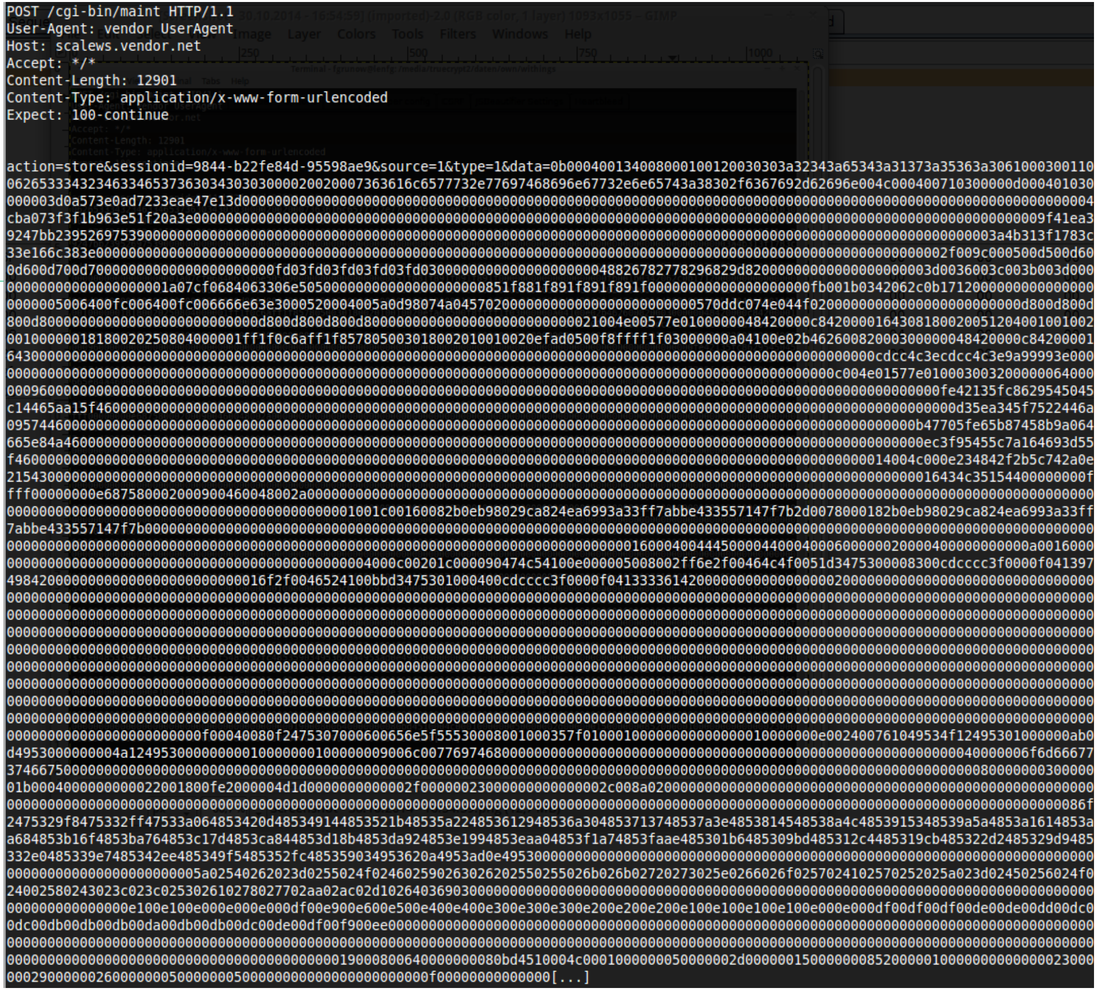
Are we Ready?

- 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
  - Privacy?

The Scale

Home Monitoring

Privacy?

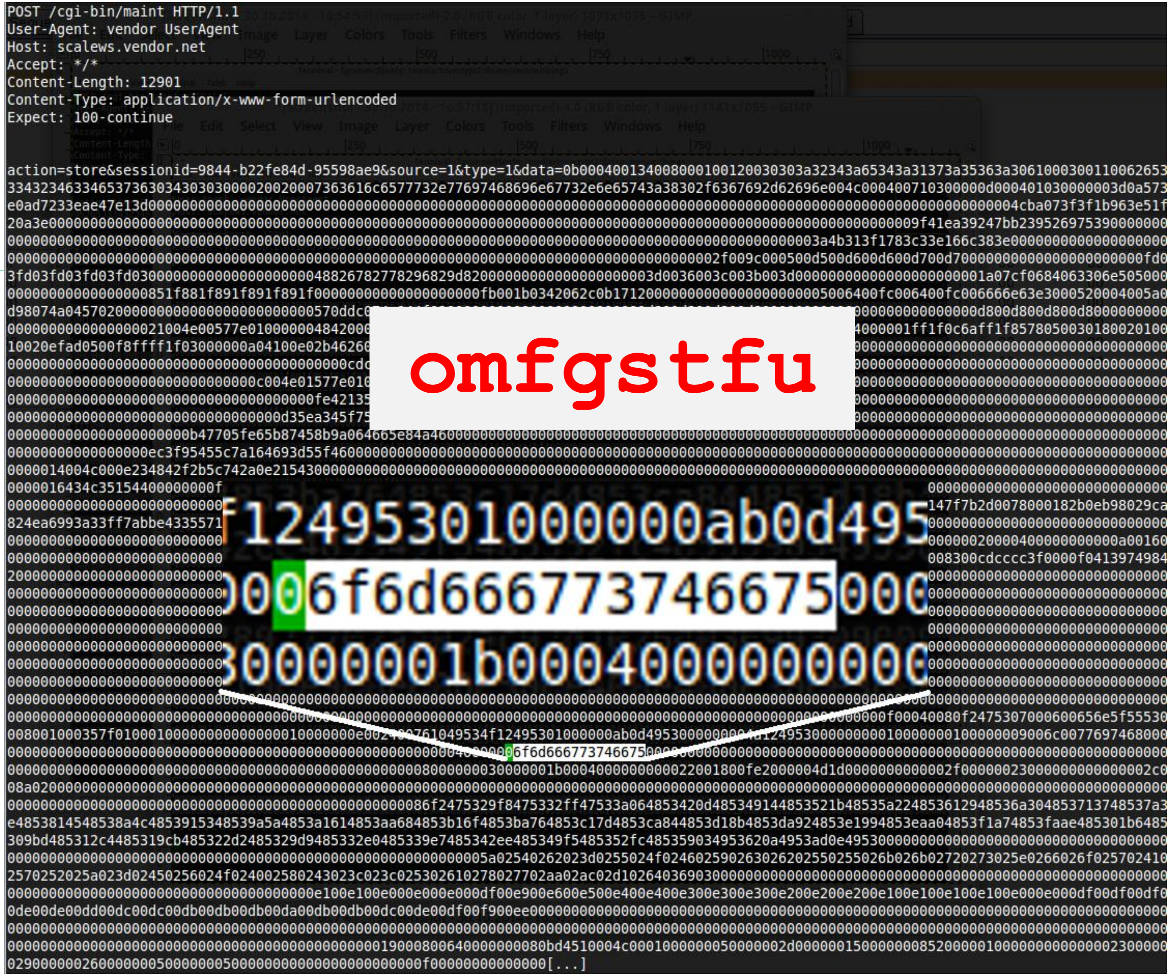


```
POST /cgi-bin/maint HTTP/1.1
User-Agent: vendor UserAgent
Host: scalews.vendor.net
Accept: */*
Content-Length: 12901
Content-Type: application/x-www-form-urlencoded
Expect: 100-continue

action=store&sessionid=9844-b22fe84d-95598ae9&source=1&type=1&data=0b000400134008000100120030303a32343a65343a31373a35363a3061000300110
06265333432346334653736303430303000020020007363616c6577732e77697468696e67732e6e65743a38302f6367692d62696e004c000400710300000d000401030
000003d0a573e0ad7233eae47e13d000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000004
cba073f3f1b963e51f20a3e000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000009f41ea3
9247bb23952697539000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000003a4b313f1783c
33e166c383e000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000002f009c000500d500d60
0d600d700d70000000000000000000000fd03fd03fd03fd03fd0300000000000048826782778296829d820000000000000000000000000000003d0036003c003b003d000
00000000000000000001a07cf0684063306e50500000000000000000000851f881f891f891f891f00000000000000000000fb001b0342062c0b1712000000000000000
0000005006400fc006400fc006666e63e3000520004005a0d98074a04570200000000000000000000000000570ddc074e044f020000000000000000000000d800d800d
800d8000000000000000000000000d800d800d800d80000000000000000000000000000021004e00577e0100000048420000c8420000164308180020051204001001002
00100000018180020250804000001ff1f0c6aff1f857805003018002010010020efad0500f8ffff1f03000000a04100e02b46260082000300000048420000c84200001
64300000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000cdcc4c3ecdcc4c3e9a99993e000
000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000c004e01577e010003003200000064000
00096000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000fe42135fc8629545045
c14465aa15f4600000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000d35ea345f7522446a
09574460000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000b47705fe65b87458b9a064
665e84a4600000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000ec3f95455c7a164693d55
f4600000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000014004c000e234842f2b5c742a0e
2154300000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000016434c35154400000000f
fff00000000e687580002000900460048002a0000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000
0000000000000000000000000000000000000000001001c00160082b0eb98029ca824ea6993a33ff7abbe433557147f7b2d0078000182b0eb98029ca824ea6993a33ff
7abbe433557147f7b000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000
000000000000000000000000000000000000000000000000000000000000000000000000000001600040044450000440004000600000020000400000000000a0016000
000000000000000000000000000000000000000000004000c00201c000090474c54100e000005008002ff6e2f00464c4f0051d3475300008300cdcccc3f0000f041397
49842000000000000000000000000016f2f0046524100bbd3475301000400cdcccc3f0000f0413336142000000000000000000020000000000000000000000000000000
00000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000
00000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000
00000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000
00000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000
00000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000
00000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000
00000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000
00000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000
00000000000000000000000f00040080f2475307000600656e5f55530008001000357f0100010000000000000000010000000e002400761049534f12495301000000ab0
d4953000000004a12495300000000100000001000000009006c0077697468000000000000000000000000000000000000000000000000000000000040000006f6d66677
37466750000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000080000000300000
01b000400000000002200180
0fe20000004d1d0000000000002f00000023000000000000000002c008a020000000000000000000000000000000000000000000000000000
000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000086f
2475329f8475332ff47533a064853420d485349144853521b48535a224853612948536a304853713748537a3e4853814548538a4c4853915348539a5a4853a1614853a
a684853b16f4853ba764853c17d4853ca844853d18b4853da924853e1994853eaa04853f1a74853faae485301b6485309bd485312c4485319cb485322d2485329d9485
332e0485339e7485342ee485349f5485352fc485359034953620a4953ad0e4953000000000000000000000000000000000000000000000000000000000000000000000
000000000000000000000005a02540262023d0255024f024602590263026202550255026b026b02720273025e0266026f025702410257025202 5a023d02450256024f0
24002580243023c023c025302610278027702aa02ac02d10264036903000000000000000000000000000000000000000000000000000000000000000000000000000000
000000000000000e100e100e000e000e000df00e900e600e500e400e400e300e300e300e200e200e200e100e100e100e100e000e000df00df00df00de00de00dd00dc0
0dc00db00db00db00da00db00db00dc00de00df00f900ee000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000
00000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000
000000000000000000000000000000000000000190008006400000000080bd4510004c00010000000050000002d000000150000000852000001000000000000000023000
0002900000002600000005000000050000000000000000000000f00000000000000[...]
```

Privacy?

HTTP!



```
POST /cgi-bin/maint HTTP/1.1
User-Agent: vendor UserAgent
Host: scalews.vendor.net
Accept: */*
Content-Length: 12901
Content-Type: application/x-www-form-urlencoded
Expect: 100-continue

action=store&sessionid=9844-b22fe84d-95598ae9&source=1&type=1&data=0b000400134008000100120030303a32343a65343a31373a35363a306100030011062653
33432346334653736303430303000020020007363616c6577732e77697468696e67732e6e65743a38302f6367692d62696e004c000400710300000d000401030000003d0a573
e0ad7233eae47e13d000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000004cba073f3f1b963e51f
20a3e000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000009f41ea39247bb239526975390000000
0000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000003a4b313f1783c33e166c383e00000000000000000000
00000000000000000000000000000000000000000000000000000000000000000000000000000000000002f009c000500d500d600d600d700d70000000000000000000000fd0
3fd03fd03fd03fd0300000000000000048826782778296829d820000000000000000000000003d0036003c003b003d000000000000000000000001a07cf0684063306e505000
0000000000000000851f881f891f891f891f000000000000000000000fb001b0342062c0b17120000000000000000000005006400fc006400fc006666e63e3000520004005a0
d98074a045702000000000000000000000000570ddc0                                                           00000000000000d800d800d800d8000000000
000000000000000021004e00577e0100000048420000                                                           4000001ff1f0c6aff1f8578050030180020100
10020efad0500f8ffff1f03000000a04100e02b46260                                                           0000000000000000000000000000000000000
000000000000000000000000000000000000000cdc                                                             0000000000000000000000000000000000000
00000000000000000000000000000c004e01577e010                                                            0000000000000000000000000000000000000
000000000000000000000000000000000000fe42135                                                            0000000000000000000000000000000000000
00000000000000000000000000000000d35ea345f75                                                            0000000000000000000000000000000000000
000000000000000000000b47705fe65b87458b9a064665e84a460000000000000000000000000000000000000000000000000000000000000000000000000000000000000000
0000000000000000ec3f95455c7a164693d55f460000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000
0000014004c000e234842f2b5c742a0e215430000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000
0000016434c3515440000000f                                                                         00000000000000000000000000000
00000000000000000000000000                                                                        147f7b2d0078000182b0eb98029ca
824ea6993a33ff7abbe4335571                                                                        00000000000000000000000000000
00000000000000000000000000                                                                        00000020000400000000000a00160
00000000000000000000000000                                                                        008300cdcccc3f0000f0413974984
20000000000000000000000000                                                                        00000000000000000000000000000
00000000000000000000000000                                                                        00000000000000000000000000000
00000000000000000000000000                                                                        00000000000000000000000000000
00000000000000000000000000                                                                        00000000000000000000000000000
00000000000000000000000000                                                                        00000000000000000000000000000
00000000000000000000000000                                                                        00000000000000000000000000000
00000000000000000000000000                                                                        00000000000000000000000000000
00000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000
0000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000f00040080f2475307000600656e5f55530
008001000357f0100010000000000000000100000000e00240076104953 4f124953010000000ab0d4953000000004a1249530000000010000000100000009006c0077697468000
00000000000000000000000000000000000000000000000000000004000006f6d666773746675000000000000000000000000000000000000000000000000000000000000000
000000000000000000000000000000000000008000000030000001b0004000000000022001800fe2000004d1d0000000000002f000000230000000000000002c0
08a02000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000
0000000000000000000000000000000000000086f2475329f8475332ff47533a064853420d485349144853521b48535a224853612948536a304853713748537a3
e4853814548538a4c4853915348539a5a4853a1614853aa684853b16f4853ba764853c17d4853ca844853d18b4853da924853e1994853eaa04853f1a74853faae485301b6485
309bd485312c4485319cb485322d2485329d9485332e0485339e7485342ee485349f5485352fc485359034953620a4953ad0e49530000000000000000000000000000000000
000000000000000000000000000000000000000000000000000005a02540262023d0255024f024602590263026202550255026b026b02720273025e0266026f025702410
2570252025a023d02450256024f024002580243023c023c025302610278027702aa02ac02d1026403690300000000000000000000000000000000000000000000000000000
0000000000000000000000000000000000000e100e100e000e000e000df00e900e600e500e400e400e300e300e300e200e200e200e100e100e100e100e000e000df00df00df0
0de00de00dd00dc00dc00db00db00db00da00db00db00dc00de00df00f900ee00000000000000000000000000000000000000000000000000000000000000000000000000000
00000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000
0000000000000000000000000000000000000000000000000000000000000000019000800640000000080bd4510004c000100000000500000002d00000001500000008520000001000000000000002300000
029000000260000000500000005000000000000000000000f00000000000000[...]
```

f12495301000000ab0d495

006f6d666773746675000

30000001b0004000000000

omfgstfu

Are they Ready?

- What about the vendors?
  - Same mistakes again?
  - Learning curve
    - WiFi
    - Car keys
    - Exploiting like in the old days?
  - “We are not really using this port, the board came with it!“
  - “We are fine, we have two network interfaces (trusted/untrusted)!”

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
    - Still have bugs like: "Device showing asystole alarm when patient is fine"
  - Does security?
    - "We only need to make sure that there are proper authorization mechanisms …"
    - "A hacker will always find a way …"
    - "510(k) assumes there is no hostile environment, doctor will not harm patient, patient will not harm himself or doctor"
  - 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?

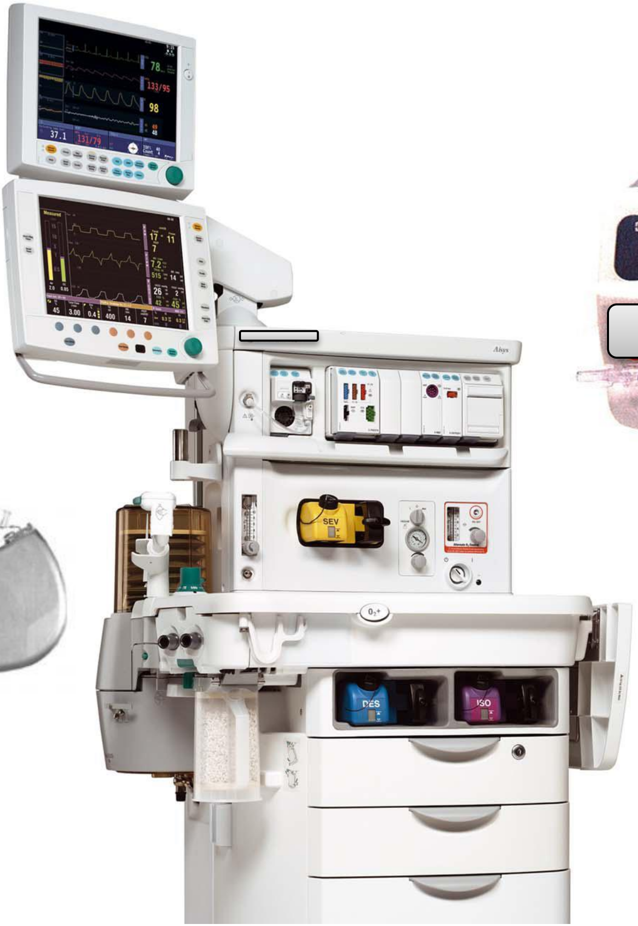
Targets

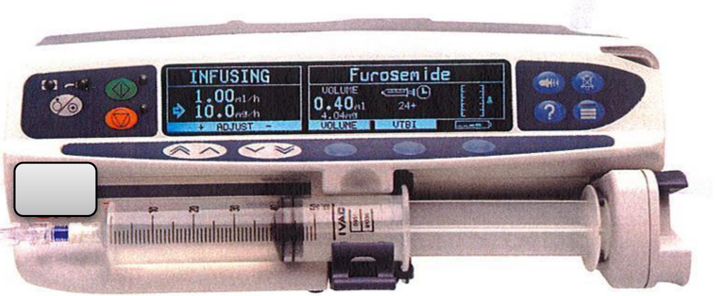
- Medical devices with enabled com
  - Com is in places you would never suspect
- “Severity Rating”:
  - Low: Monitoring stuff
  - Medium: Diagnostic systems
  - High: Feedback to patient

Monitoring

Diagnostic

Feedback


SEV
DES
ISO


INFUSING
1.00 ml/h
10.0 mg/h
ADJUST
Furosemide
VOLUME
0.40 ml
4.04mg
24+
VOLUME
VTBI
IVAC

Targets

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

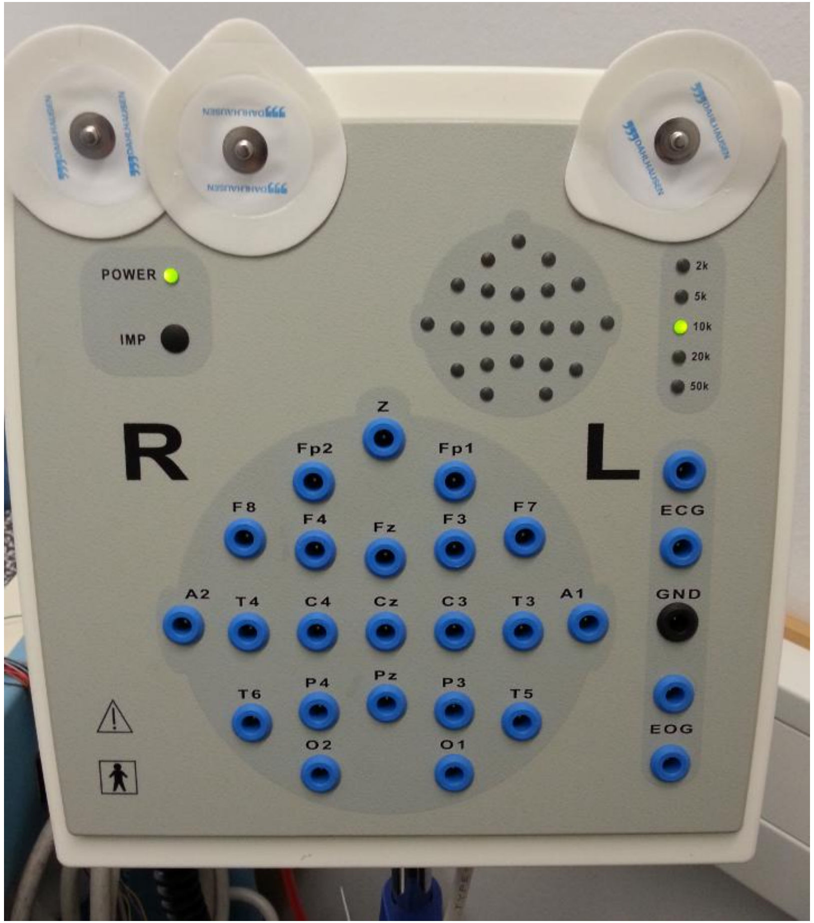
→ Hard to test!

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



Target example: EEG

Box for electrodes

Off-Topic for a Second …

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

DIY: EEG

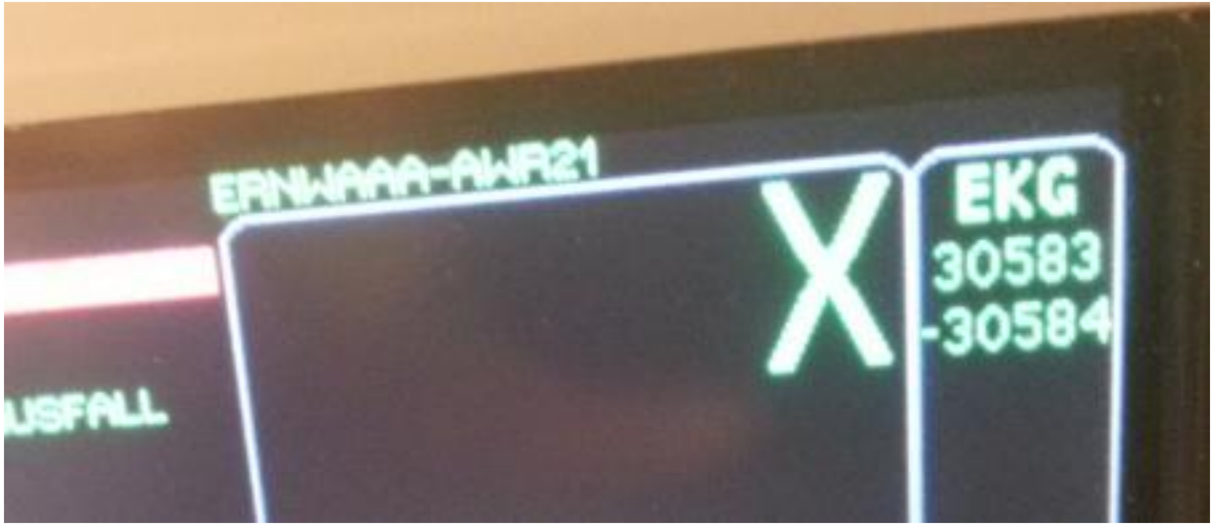
OpenEEG Project

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: Patient Monitor 1

Unreasonable Configuration

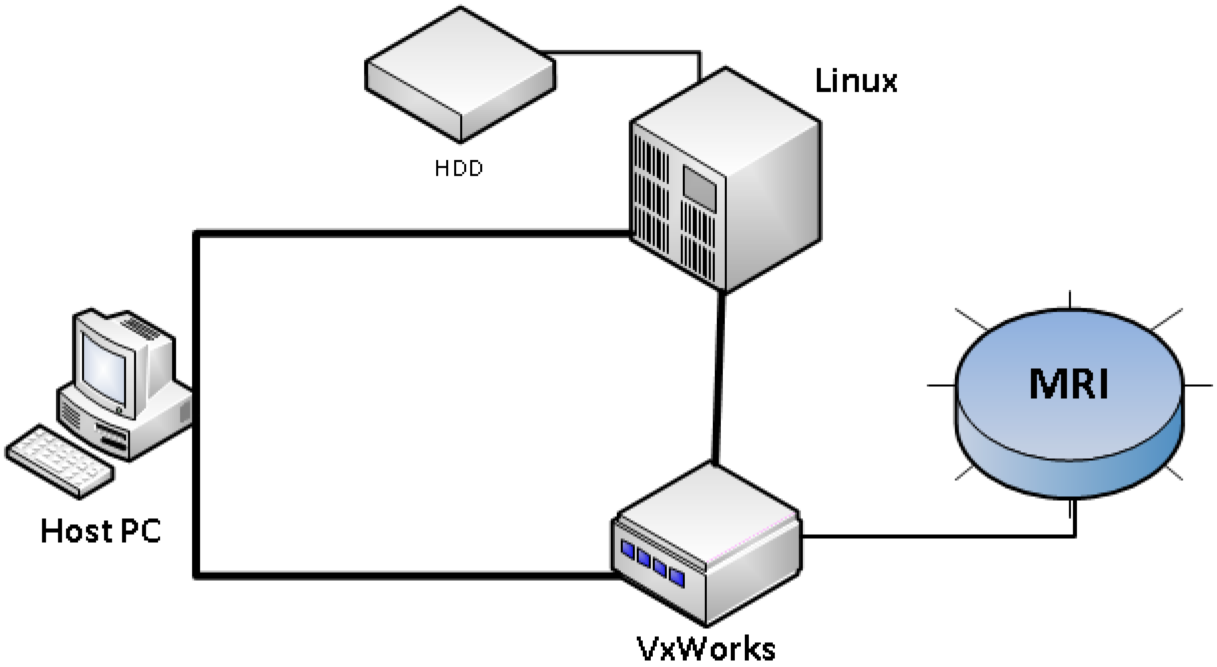
Target: MRI

- Really cool! ☺

Target: MRI

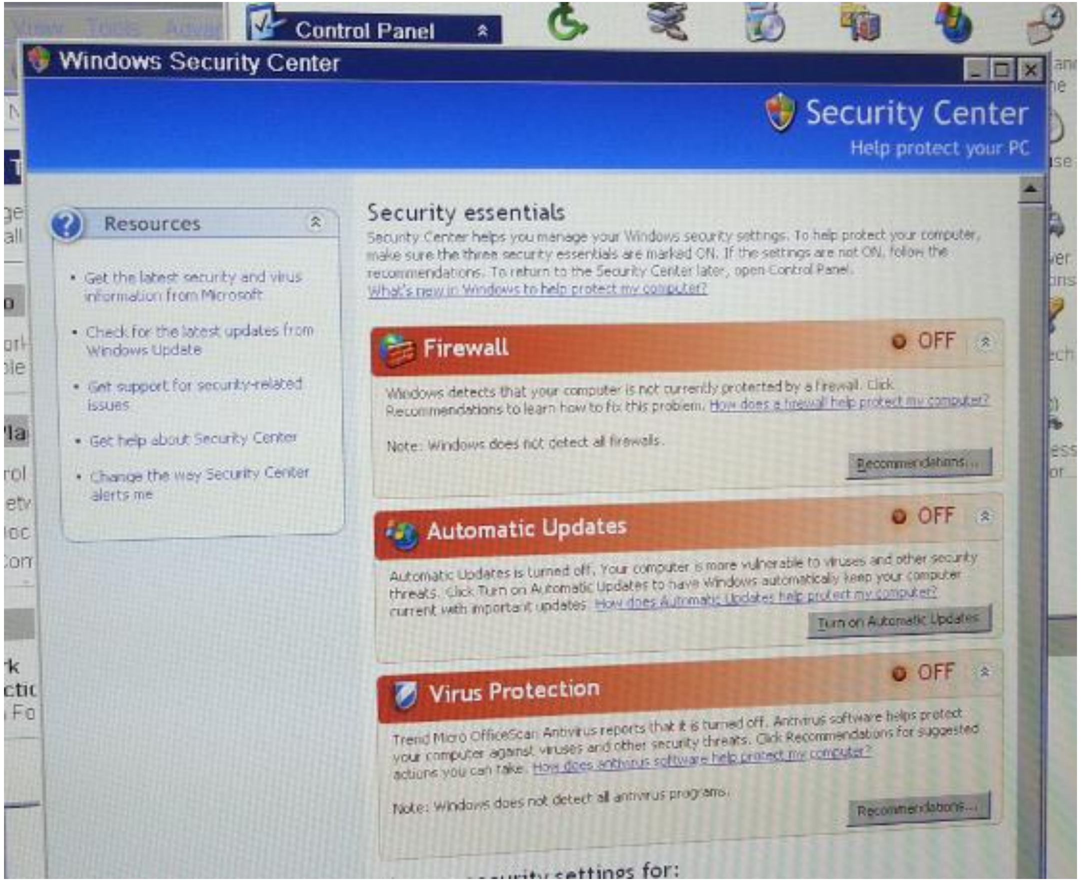
- Consists of:
  - Host System
    - Windows based PC
  - Image Processing System
    - Retrieves the raw data and constructs images
  - Control System
    - Controls hardware of the MRI (basically patient table, coils, etc.)

Target: MRI



Target: MRI

- Host System



Resources

- Get the latest security and virus information from Microsoft
- Check for the latest updates from Windows Update
- Get support for security-related issues
- Get help about Security Center
- Change the way Security Center alerts me

Security essentials

Security Center helps you manage your Windows security settings. To help protect your computer, make sure the three security essentials are marked ON. If the settings are not ON, follow the recommendations. To return to the Security Center later, open Control Panel.
What's new in Windows to help protect my computer?

Firewall ● OFF

Windows detects that your computer is not currently protected by a firewall. Click Recommendations to learn how to fix this problem. How does a firewall help protect my computer?

Note: Windows does not detect all firewalls.

Recommendations...

Automatic Updates ● OFF

Automatic Updates is turned off. Your computer is more vulnerable to viruses and other security threats. Click Turn on Automatic Updates to have Windows automatically keep your computer current with important updates. How does Automatic Updates help protect my computer?

Turn on Automatic Updates

Virus Protection ● OFF

Trend Micro OfficeScan Antivirus reports that it is turned off. Antivirus software helps protect your computer against viruses and other security threats. Click Recommendations for suggested actions you can take. How does antivirus software help protect my computer?

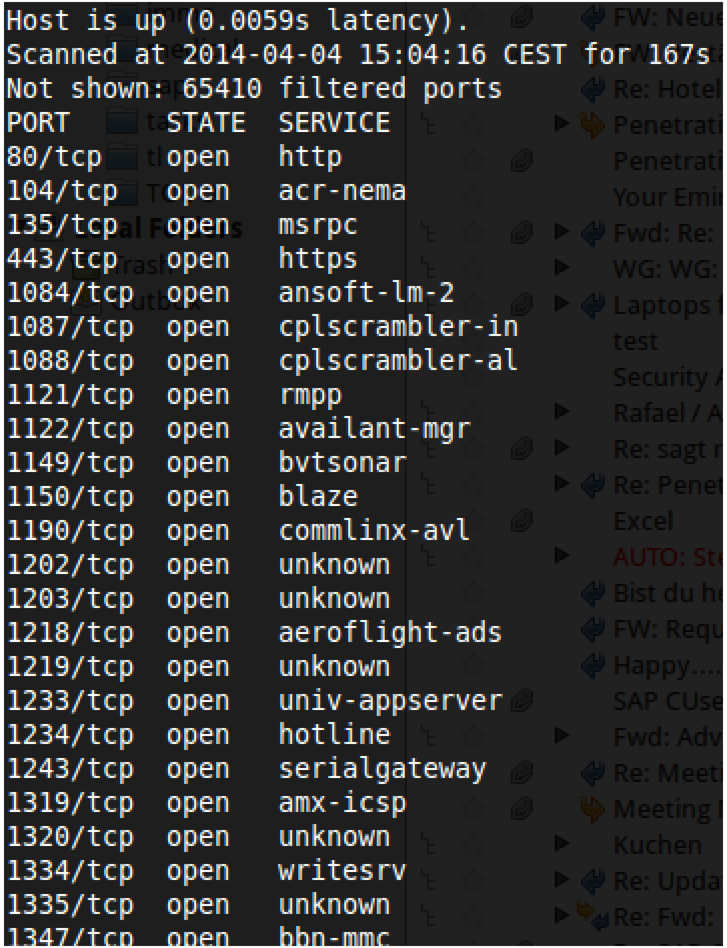
Note: Windows does not detect all antivirus programs.

Recommendations...

security settings for:

Target: MRI

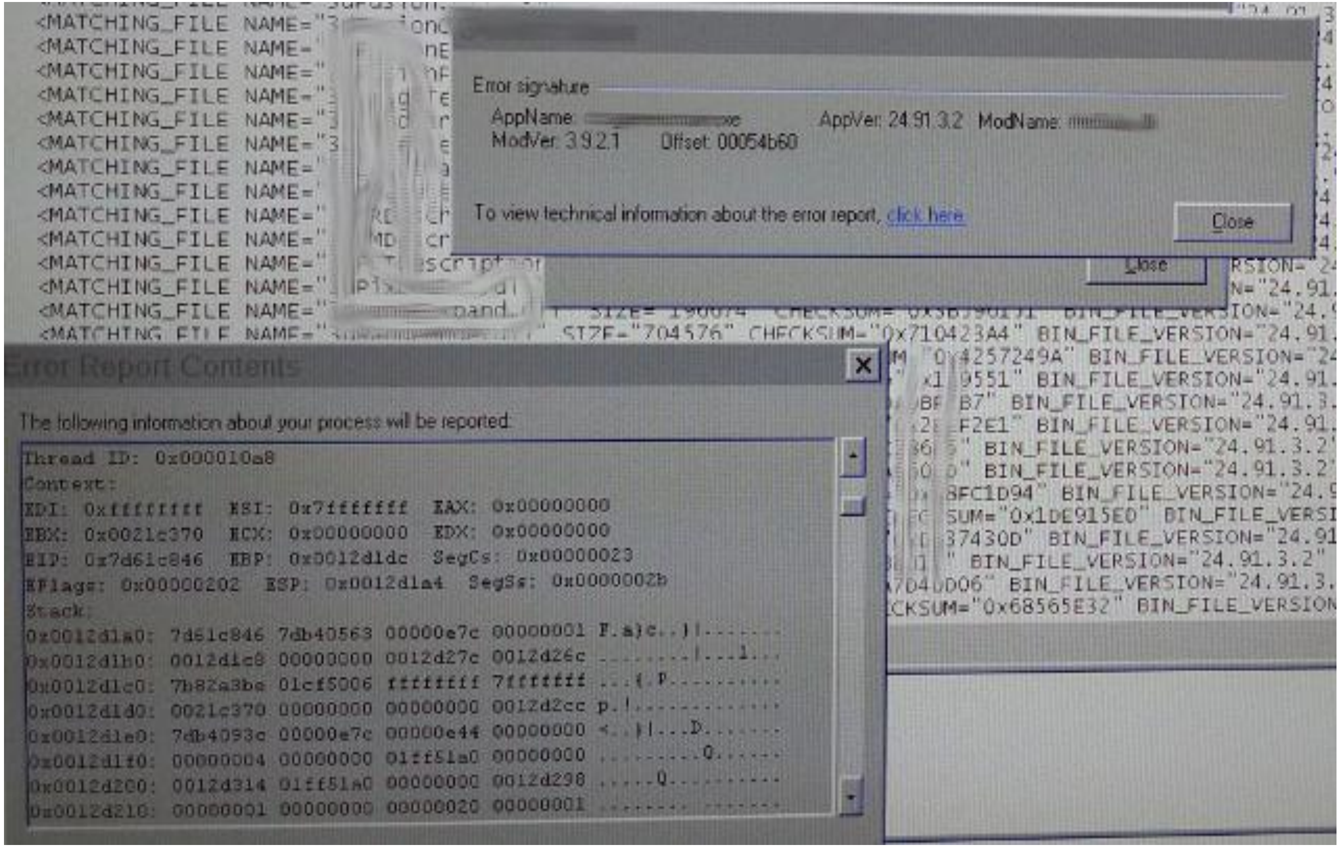
- Host System
- Open Ports: 114



```
Host is up (0.0059s latency).
Scanned at 2014-04-04 15:04:16 CEST for 167s
Not shown: 65410 filtered ports
PORT      STATE  SERVICE
80/tcp    open   http
104/tcp   open   acr-nema
135/tcp   open   msrpc
443/tcp   open   https
1084/tcp  open   ansoft-lm-2
1087/tcp  open   cplscrambler-in
1088/tcp  open   cplscrambler-al
1121/tcp  open   rmpp
1122/tcp  open   availant-mgr
1149/tcp  open   bvtsonar
1150/tcp  open   blaze
1190/tcp  open   commlinx-avl
1202/tcp  open   unknown
1203/tcp  open   unknown
1218/tcp  open   aeroflight-ads
1219/tcp  open   unknown
1233/tcp  open   univ-appserver
1234/tcp  open   hotline
1243/tcp  open   serialgateway
1319/tcp  open   amx-icsp
1320/tcp  open   unknown
1334/tcp  open   writesrv
1335/tcp  open   unknown
1347/tcp  open   bbn-mmc
```

Target: MRI

- Host System
- After portscan



```
<MATCHING_FILE NAME=" [redacted]
<MATCHING_FILE NAME=
<MATCHING_FILE NAME="
<MATCHING_FILE NAME="
<MATCHING_FILE NAME="
<MATCHING_FILE NAME="
<MATCHING_FILE NAME=
<MATCHING_FILE NAME=
<MATCHING_FILE NAME="
<MATCHING_FILE NAME="
<MATCHING_FILE NAME="
<MATCHING_FILE NAME="
<MATCHING_FILE NAME="
<MATCHING_FILE NAME="
```

Error signature

AppName: [redacted] AppVer: 24.91.3.2 ModName: [redacted]
ModVer: 3.9.2.1 Offset: 00054b60

To view technical information about the error report, click here

Close

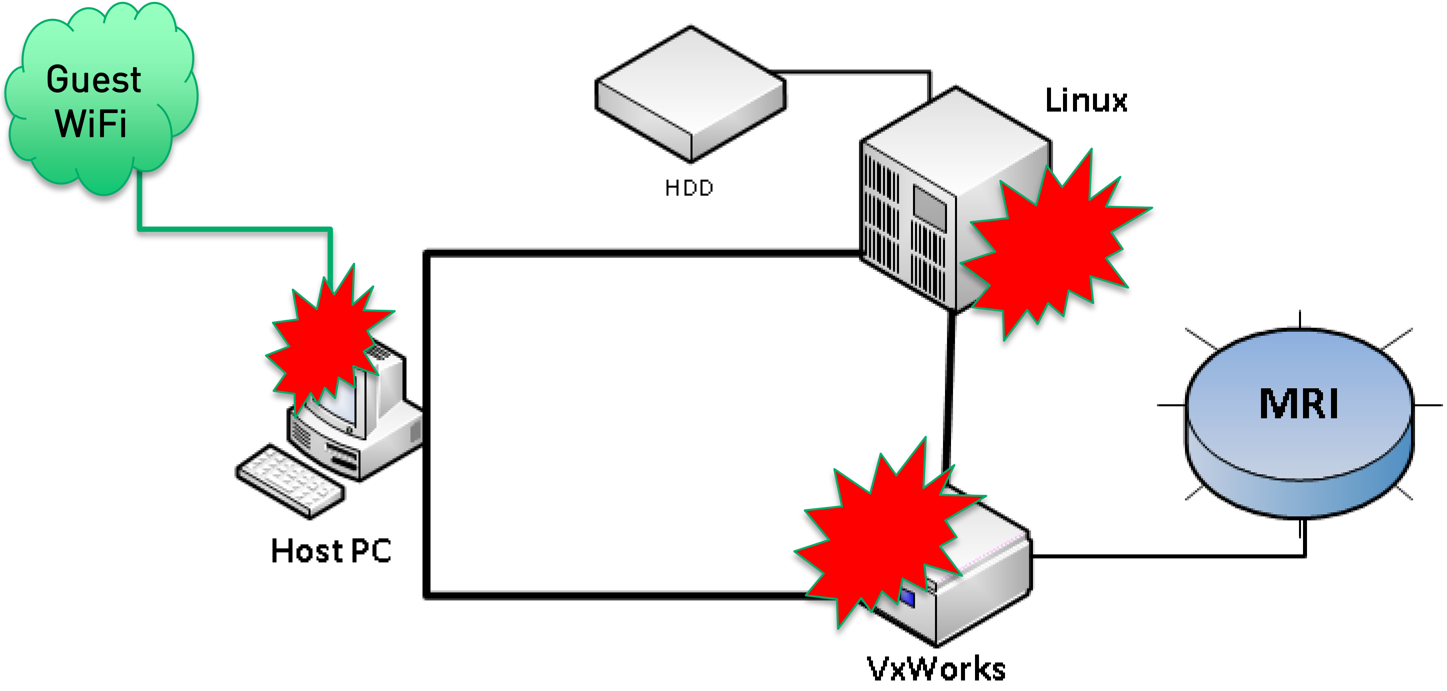
Error Report Contents

The following information about your process will be reported:

```
Thread ID: 0x000010a8
Context:
EDI: 0xffffffff  ESI: 0x7fffffff  EAX: 0x00000000
EBX: 0x0021c370  ECX: 0x00000000  EDX: 0x00000000
EIP: 0x7d61c846  EBP: 0x0012d1dc  SegCs: 0x00000023
EFlags: 0x00000202  ESP: 0x0012d1a4  SegSs: 0x0000002b
Stack:
0x0012d1a0: 7d61c846 7db40563 00000e7c 00000001 F.a}c..}|.......
0x0012d1b0: 0012d1c8 00000000 0012d27c 0012d26c ........|...l...
0x0012d1c0: 7b82a3be 01cf5006 ffffffff 7fffffff ...{.P..........
0x0012d1d0: 0021c370 00000000 00000000 0012d2cc p.!.............
0x0012d1e0: 7db4093c 00000e7c 00000e44 00000000 <..}|...D.......
0x0012d1f0: 00000004 00000000 01ff51a0 00000000 .........Q......
0x0012d200: 0012d314 01ff51a0 00000000 0012d298 .....Q..........
0x0012d210: 00000001 00000000 00000020 00000001 ................
```

```
SIZE="704576" CHECKSUM="0x710423A4" BIN_FILE_VERSION="24.91
M "0x4257249A" BIN_FILE_VERSION="24
x1 9551" BIN_FILE_VERSION="24.91.
BF B7" BIN_FILE_VERSION="24.91.3.
2 F2E1" BIN_FILE_VERSION="24.91.
" BIN_FILE_VERSION="24.91.3.2"
" BIN_FILE_VERSION="24.91.3.2"
8FC1D94" BIN_FILE_VERSION="24.9
SUM="0x1DE915E0" BIN_FILE_VERSI
37430D" BIN_FILE_VERSION="24.91
" BIN_FILE_VERSION="24.91.3.2"
7D4 D06" BIN_FILE_VERSION="24.91.3.
CKSUM="0x68565E32" BIN_FILE_VERSION
```

Target: MRI

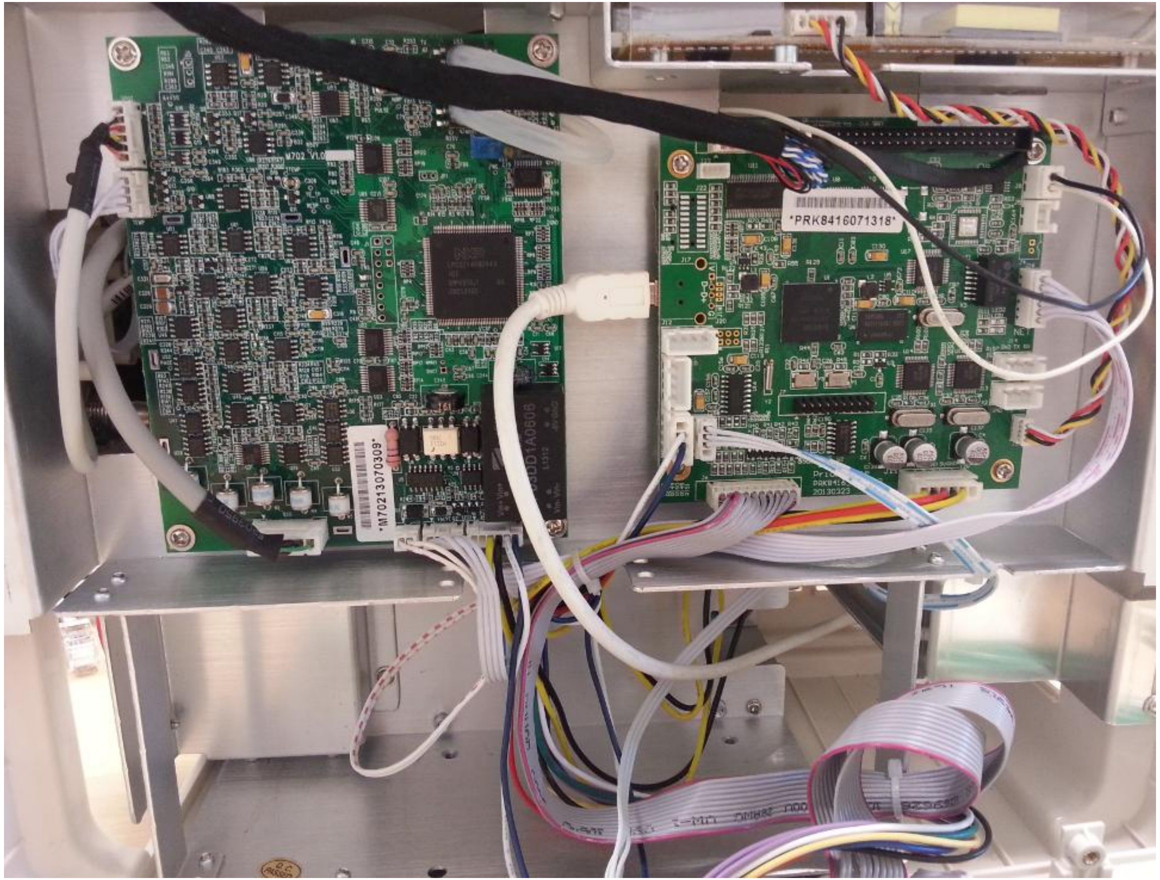


Target: Syringe Pump

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

Signal Processing / Frontend

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
    - Physical Access Control Systems
  - Aneasthesia devices

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!

Questions?

Thank you!

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