Hacking Medical Devices

Cloud Context

ERNW providing security.

Florian Grunow

- Security Analyst
- ERNW in Heidelberg
- Team Lead:
  - Pentest
  - ERNW Academy
- Research:
  - Medical Devices
  - Connected Cars

Agenda

- Motivation
- Publications
- The Problem
- Targets
- Wrap Up
- Questions

ERNW
providing security.

Disclaimer

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

ERNW
providing security.

Motivation

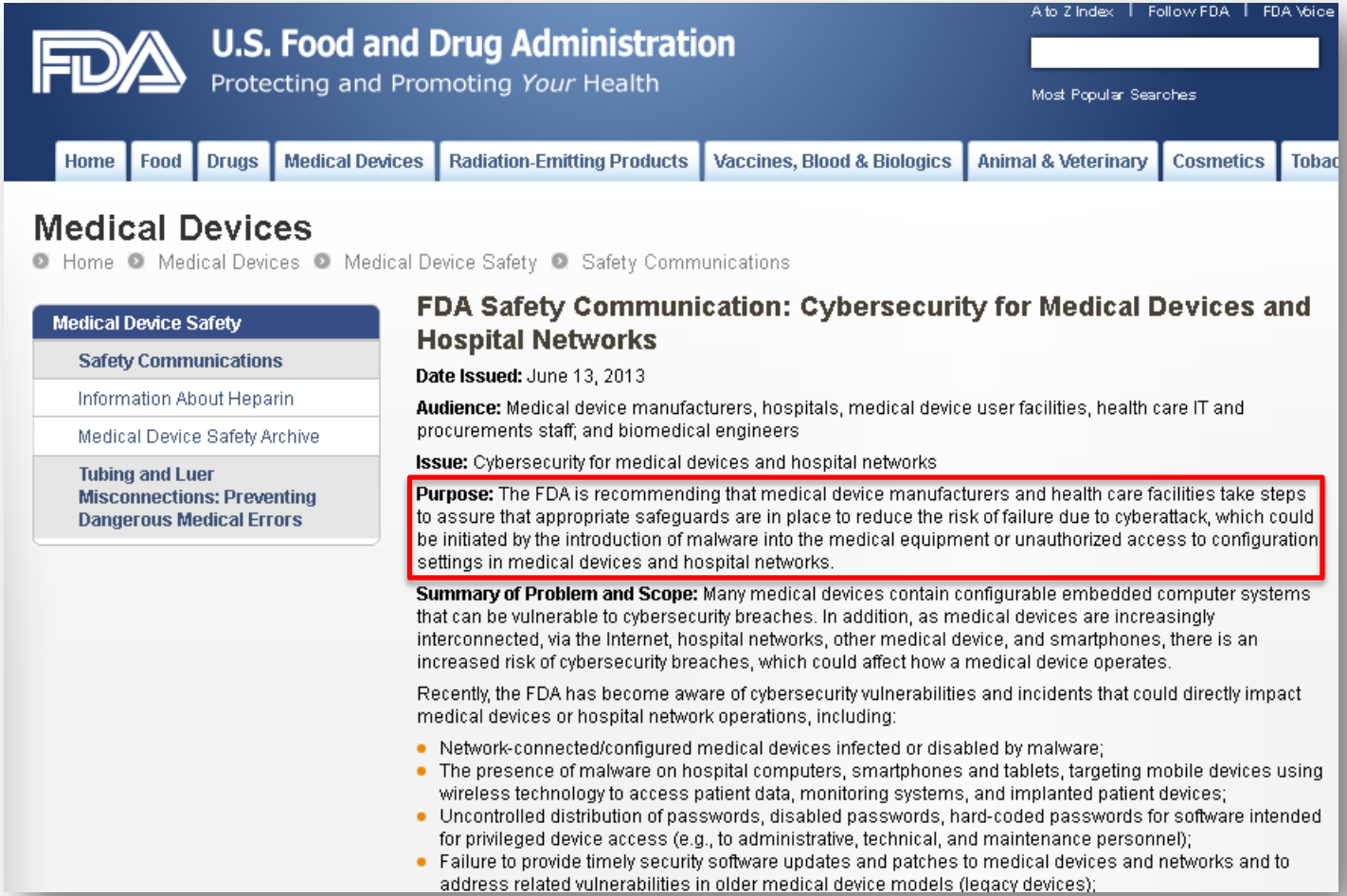
Make the world a safer place ...

Motivation

- Importance
  - We trust these devices
  - Doctors trust these devices
  - Cloud will play a major role in the future
- 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

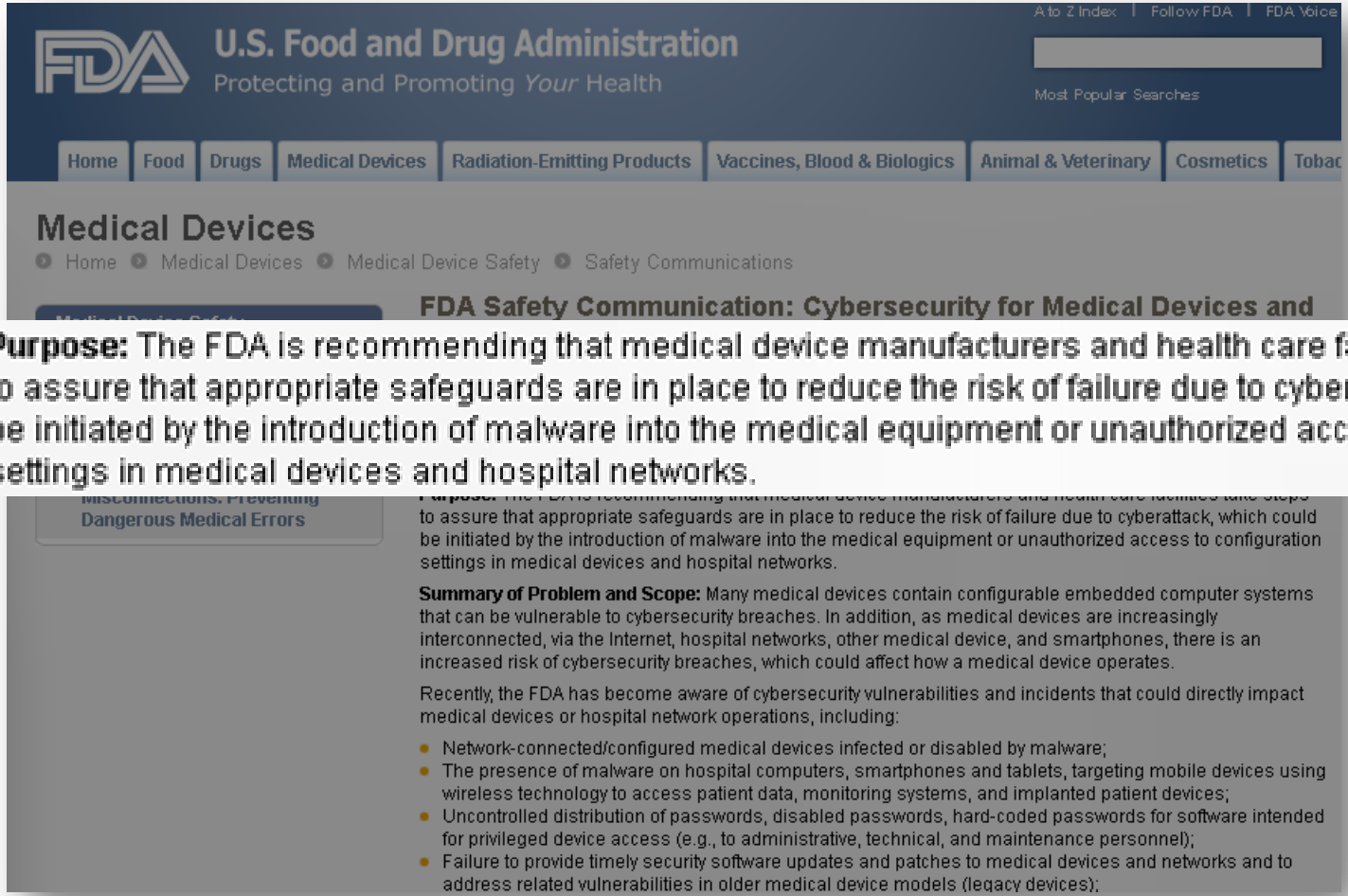
Issue: Cybersecurity for medical devices and hospital networks

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);



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.

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)

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 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[†]
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

***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

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.

ERNW
providing security.

The Problem

Anamnesis ...

Siemens Sirecust BS1

In the old days …

Nihon Kohden Neurofax EEG

In the old days ...

The Change

- New com options available
- Optimization of processes
- Interoperability
  - E-Health records
  - PACS
  - Personal Health

→ Lowering costs!

→ Data will be going to the cloud!

The Old Cloud!

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?)

→ Cloud seems to solve some of these problems!

Are we Ready?

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

→ Privacy in the cloud?

ERNW
providing security.

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
0626533343234633465373630343030300002002000737363616c6577732e77697468696e67732e6e65743a38302f6367692d62696e004c0004007103000000d000401030
000003d0a573e0ad7233eae47e13d00000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000004
cba073f3f1b963e51f20a3e000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000009f41ea3
9247bb2395269753900000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000003a4b313f1783c
33e166c383e0000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000002f009c000500d500d60
0d600d700d70000000000000000000000fd03fd03fd03fd03fd030000000000000000000000048826782778296829d8200000000000000000003d0036003c003b003d000
000000000000000000001a07cf0684063306e5050000000000000000000000851f881f891f891f891f0000000000000000000fb001b0342062c0b171200000000000000000
0000005006400fc006400fc006666e63e3000520004005a0d98074a0457020000000000000000000000000570ddc074e044f020000000000000000000000000d800d800d
800d80000000000000000000000000000d800d800d800d80000000000000000000000000021004e00577e0100000048420000c8420000164308180020051204001001002
00100000018180020250804000001ff1f0c6aff1f8578050030180020100100 20efad0500f8ffff1f03000000a04100e02b4626008200030000048420000c84200001
643000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000cdcc4c3ecdcc4c3e9a99993e000
00000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000c004e01577e0100030032000000064000
0009600000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000fe42135fc8629545045
c14465aa15f46000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000d35ea345f7522446a
0957446000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000b47705fe65b87458b9a064
665e84a46000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000ec3f95455c7a164693d55
f46000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000014004c000e234842f2b5c742a0e
215430000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000016434c35154400000000f
fff000000000e6875800020009004600480020a0000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000
000000000000000000000000000000000000000001001c00160082b0eb98029ca824ea6993a33ff7abbe433557147f7b2d0078000182b0eb98029ca824ea6993a33ff
7abbe433557147f7b0000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000
00000000000000000000000000000000000000000000000000000000000000000000000016000400444500004400040006000000200004000000000000a0016000
0000000000000000000000000000000000000000000000004000c00201c000090474c54100e000005008002ff6e2f00464c4f0051d3475300008300cdcccc3f0000f041397
4984200000000000000000000000000016f2f0046524100bbd3475301000400cdcccc3f0000f041333361420000000000000000002000000000000000000000000000000
00000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000
00000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000
00000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000
00000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000
00000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000
00000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000
00000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000
00000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000
0000000000000000000000f00040080f2475307000600656e5f5553000800100035 7f010001000000000000000010000000e00240076104953 4f12495301000000ab0
d4953000000004a12495300000000010000000100000009006c00776974680000000000000000000000000000000000000000000000000000000004000006f6d6677
374667500000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000080000000300000
01b0004000000000022001800fe2000004d1d000000000002f00000023000000000000002c008a02000000000000000000000000000000000000000000000000000000
000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000086f
2475329f8475332ff47533a064853420d485349144853521b48535a224853612948536a3048537137 48537a3e4853814548538a4c4853915348539a5a4853a1614853a
a684853b16f4853ba764853c17d4853ca844853d18b4853da924853e1994853eaa04853f1a74853faae485301b6485309bd485312c4485319cb485322d2485329d9485
332e0485339e7485342ee485349f5485352fc4853590349536 20a4953ad0e49530000000000000000000000000000000000000000000000000000000000000000000
000000000000000000000005a02540262023d0255024f024602590263026202550255026b026b02720273025e0266026f0257024102570252025a023d02450256024f0
240025802430 23c023c02530261027802770 2aa02ac02d102640369030000000000000000000000000000000000000000000000000000000000000000000000000
00000000000000e100e100e000e000e000df00e900e600e500e400e400e300e300e300e200e200e200e100e100e100e100e000e000df00df00df00de00de00dd00dc0
0dc00db00db00db00da00db00db00dc00de00df00f900ee000000000000000000000000000000000000000000000000000000000000000000000000000000000000000
00000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000
00000000000000000000000000000000000000000001900080064000000080bd4510004c0001000000050000002d0000000150000000852000001000000000000000023000
0002900000002600000005000000050000000000000000000000f00000000000000[...]

Privacy?

HTTP!

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
- Lack of awareness on vendor side
- Safety vs. Security

→ This could kill you!

Targets

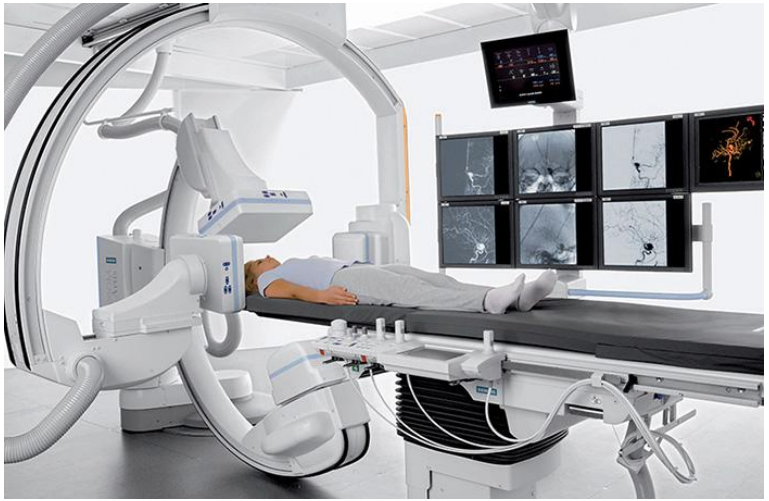
What are we looking at?

Targets

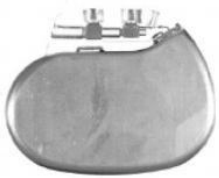
- Medical devices with enabled com
  - Com is in places you would never suspect
- “Severity Rating”:
  - Low: Monitoring stuff
  - Medium: Diagnostic systems
  - High: Feedback to patient

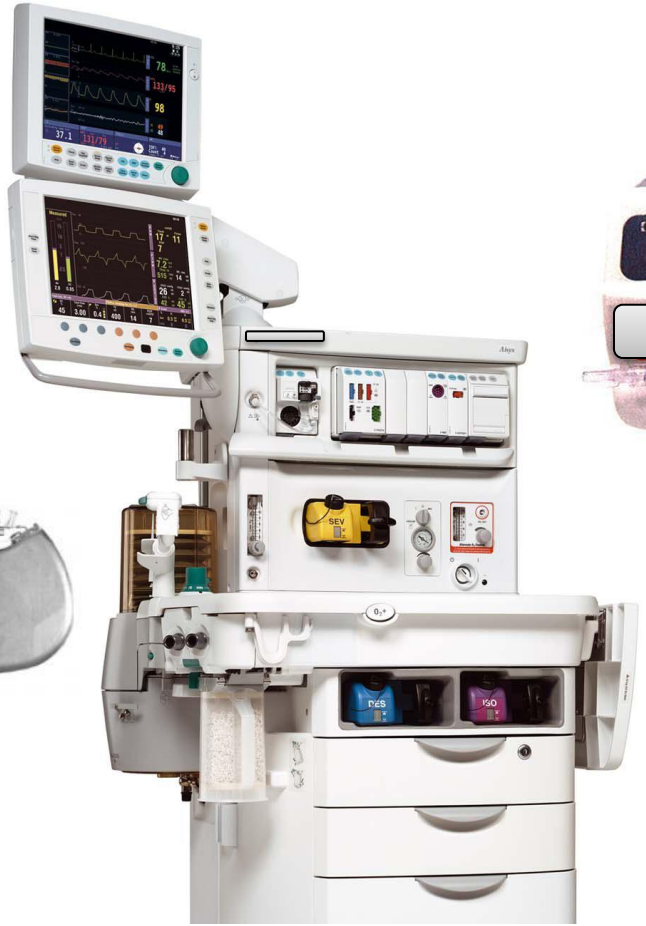
Monitoring

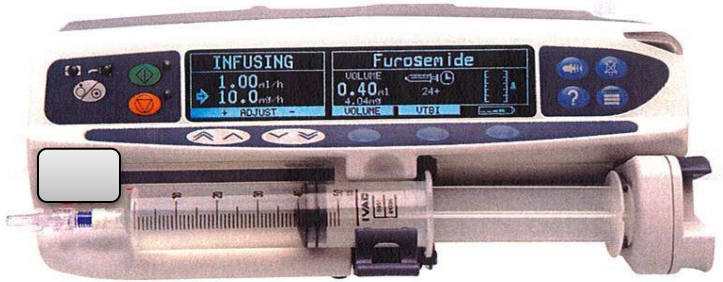
Diagnostic



Feedback







Targets

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

→ Hard to test!

ERNW
providing security.

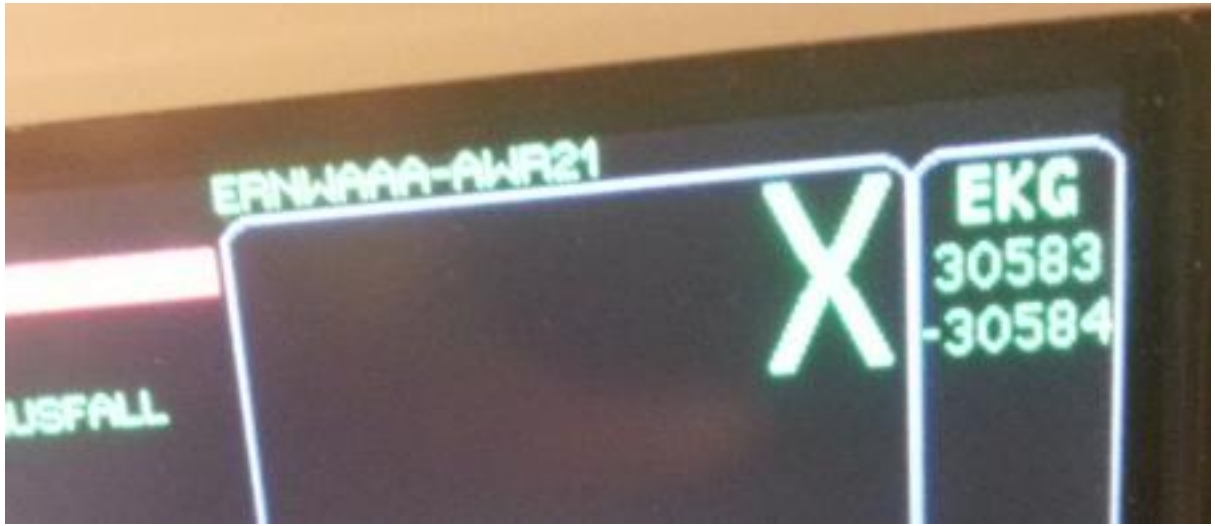
Targets

What we looked at so far ...

ERNW
providing security.

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

Unreasonable Configuration

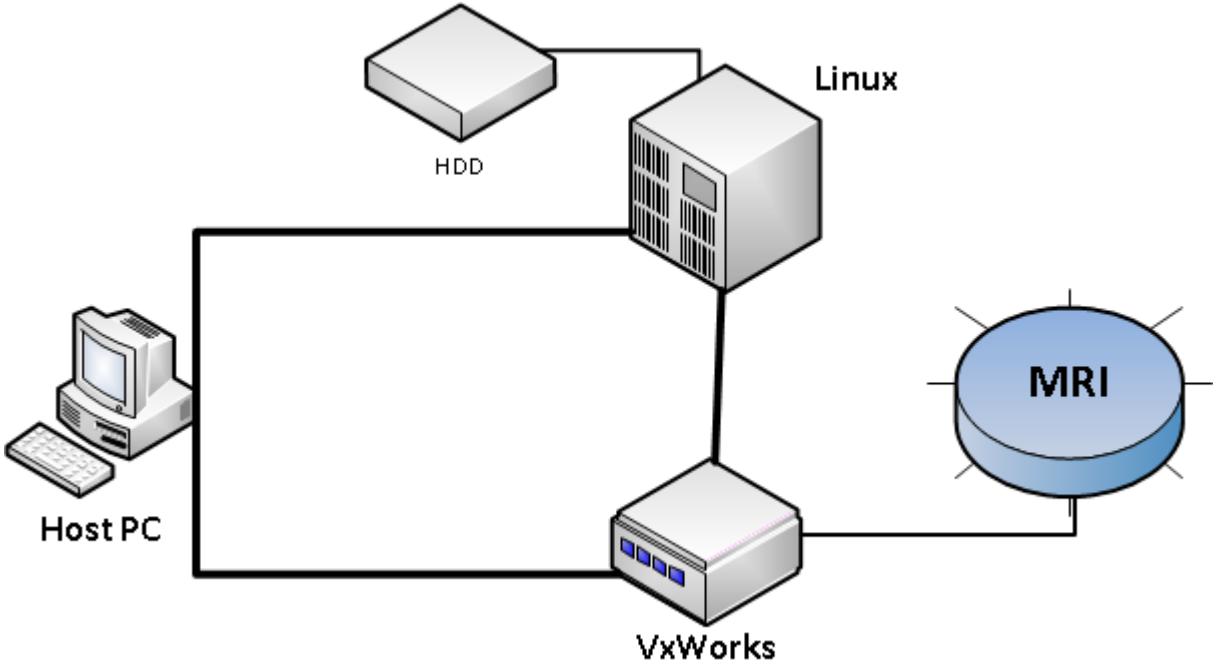
Target: MRI

- Really cool! ☺

Target: MRI

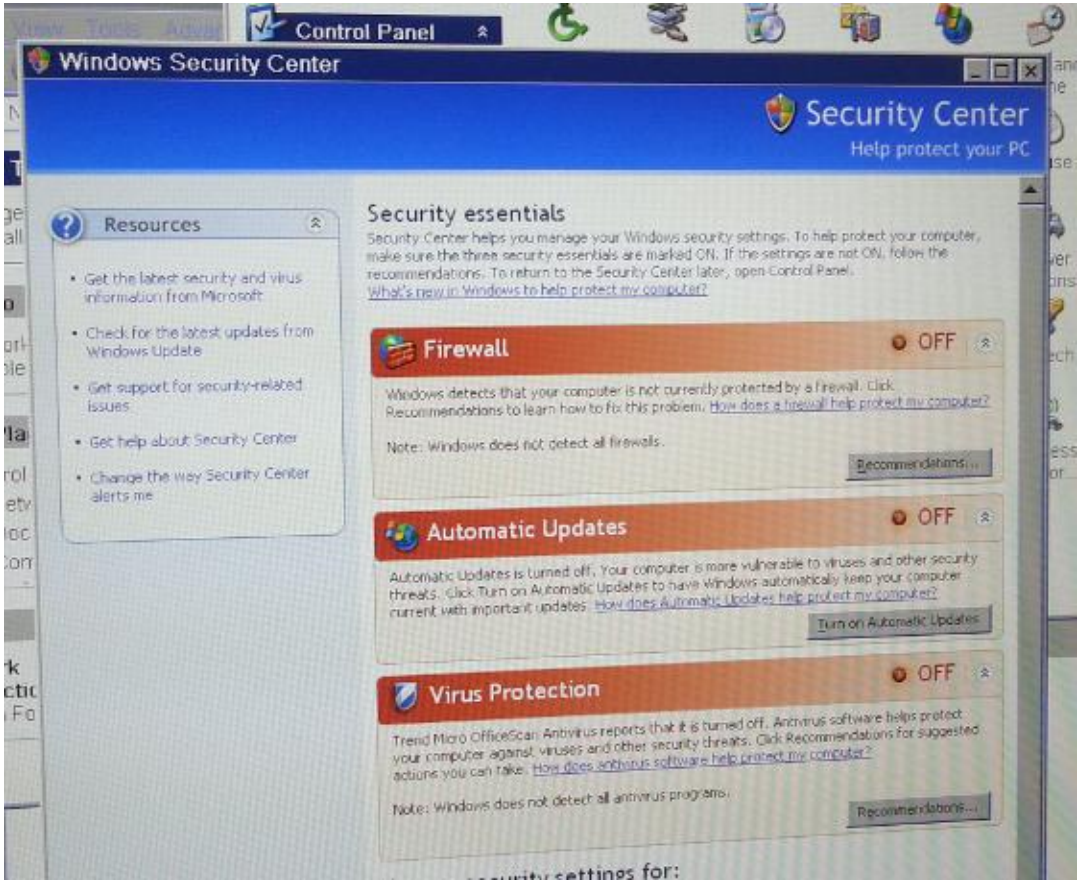
- Consists of:
  - Host System
    - Windows based PC
  - Image Processing System
    - Retrieves the raw data and constructs images
  - Control System
    - Controls hardware of the MRI (basically patient table, coils, etc.)

Target: MRI



Target: MRI

- Host System



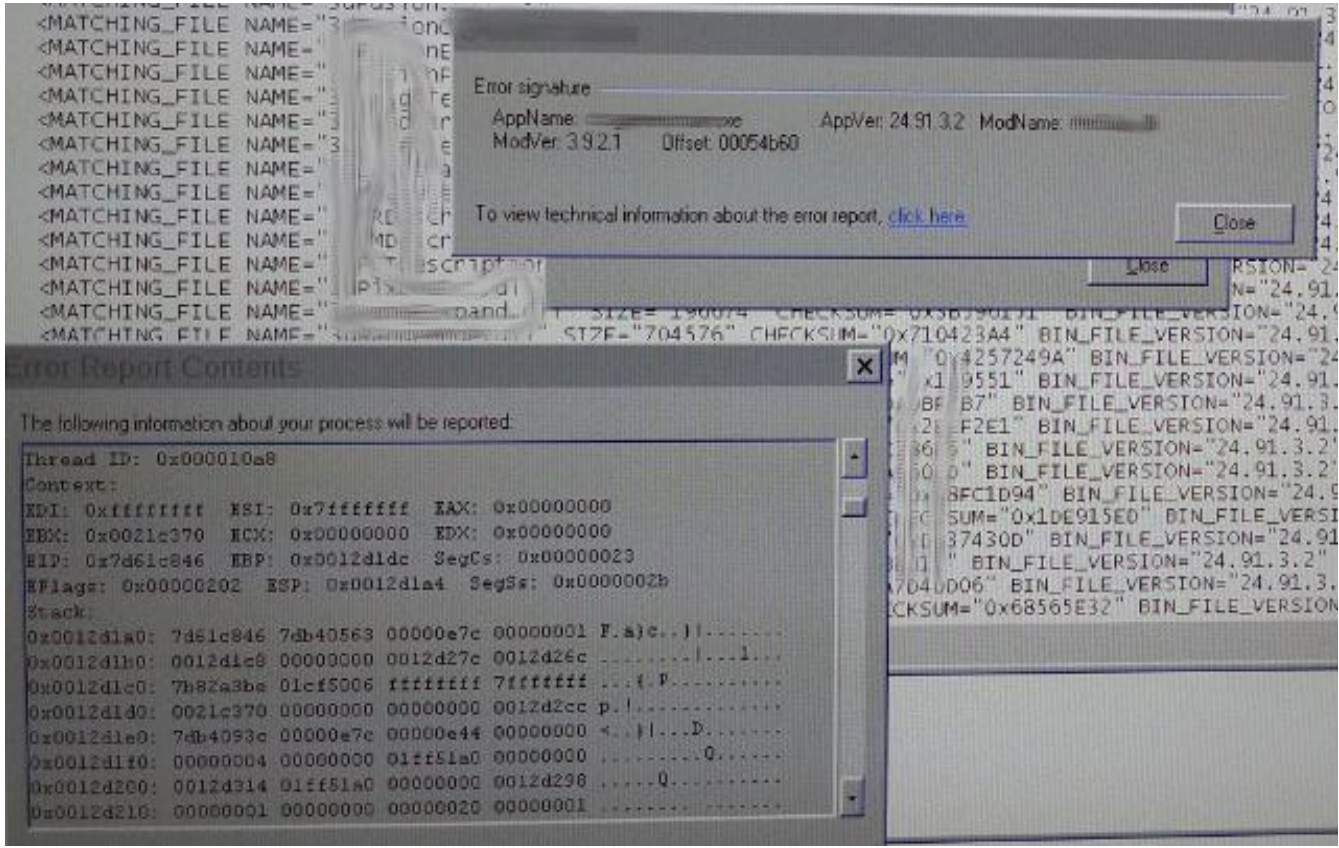
Target: MRI

- Host System
- Open Ports: 114

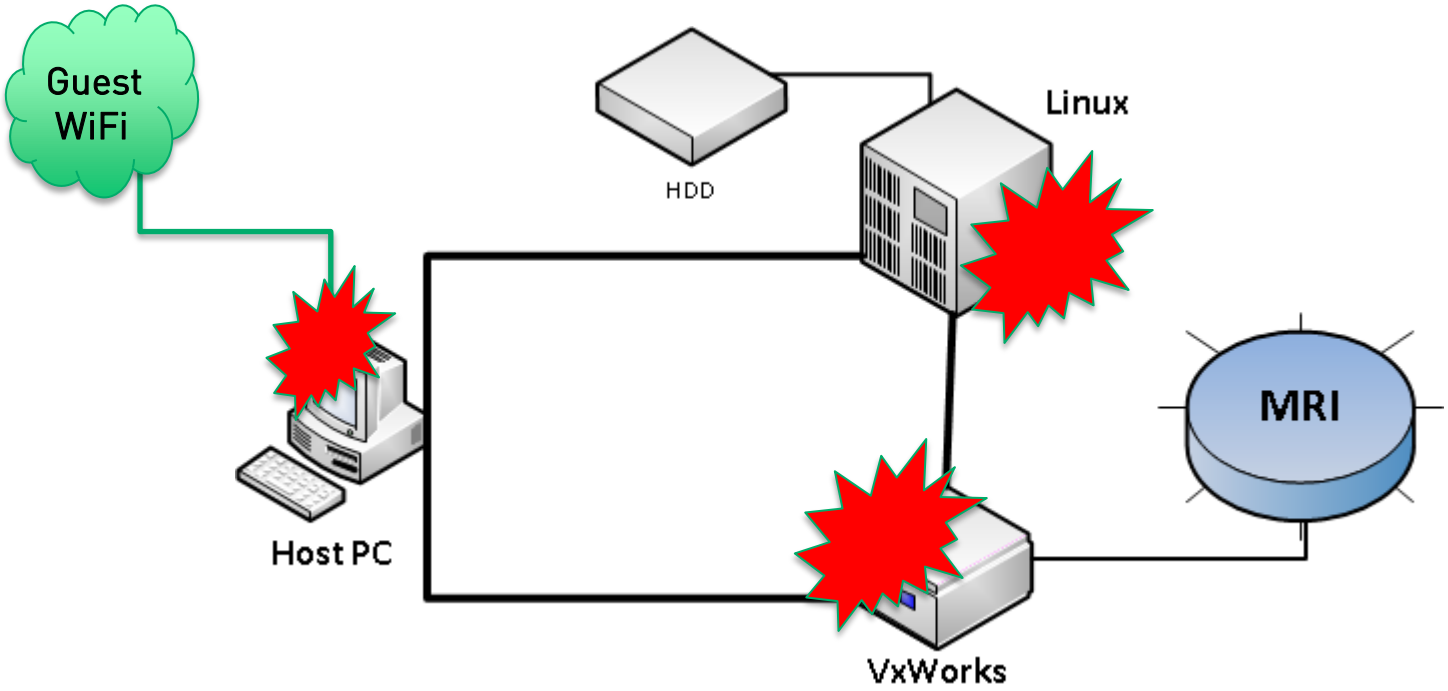
```
Host is up (0.0059s latency).
Scanned at 2014-04-04 15:04:16 CEST for 167s
Not shown: 65410 filtered ports
PORT     STATE  SERVICE
80/tcp   open   http
104/tcp  open   acr-nema
135/tcp  open   msrpc
443/tcp  open   https
1084/tcp  open   ansoft-lm-2
1087/tcp  open   cplscrambler-in
1088/tcp  open   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

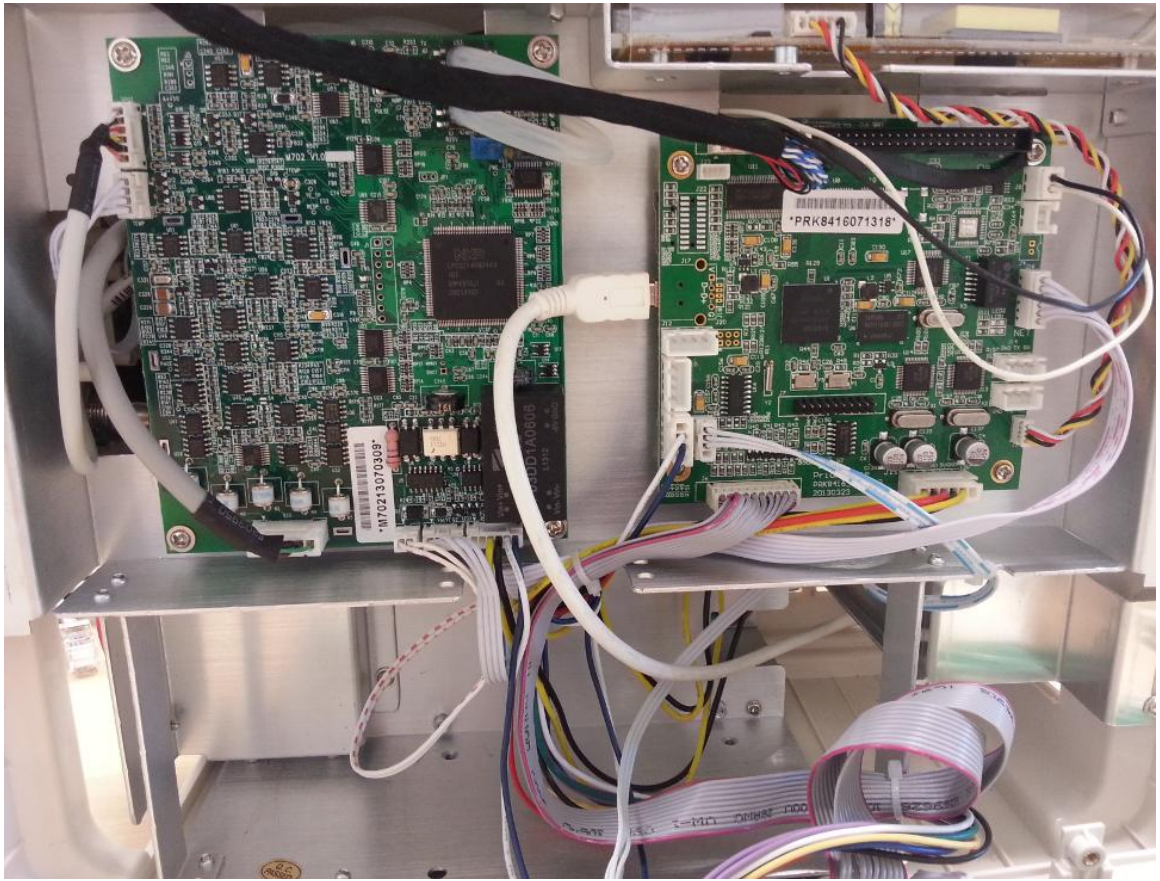


Target: MRI



Target: Syringe Pump

Demo: Infusion Override



Target: Patient Monitor 2

Signal Processing / Frontend

ERNW
providing security.

Target: Patient Monitor 2

Demo: Pwning vital signs

Cloudification

- How do we authenticate?
  - Devices not adequately capable
  - Violation of best practices
- Secure the weakest link!
  - Not necessarily the cloud but the “Things”
  - Hospital environment
- Data privacy?
  - Especially in Germany hot topic

Final Words …

- We need to test these devices!
- There will be more publications from ERNW!
- For the Cloud:
  → Consider the IoT (”**I**nternet **o**f **T**hreats”)!

Questions?

ERNW
providing security.

Thank you!

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