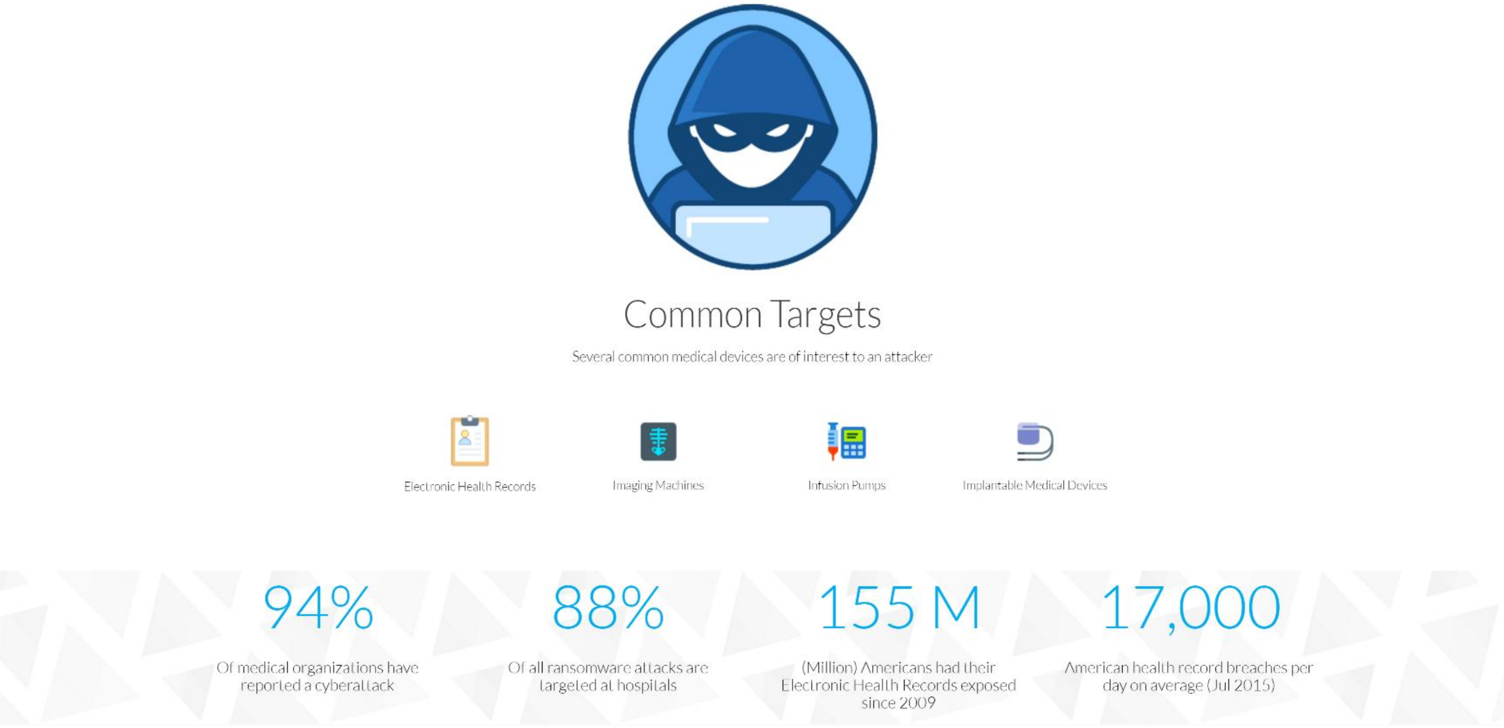
MEDICAL DEVICES SECURITY

Y. KOREN, M. MUJAHID, M. K. CHOWDHURY



Common Targets

Several common medical devices are of interest to an attacker

Electronic Health Records

Imaging Machines

Infusion Pumps

Implantable Medical Devices

94%

Of medical organizations have reported a cyberattack

88%

Of all ransomware attacks are targeted at hospitals

155 M

(Million) Americans had their Electronic Health Records exposed since 2009

17,000

American health record breaches per day on average (Jul 2015)

Welcome to North York General Hospital

We are committed to serve patients with the best possible care, funded by York University's tuition fees. We give you the best, you pay for your classes, YorkU takes most of it and then we take the rest.

PATIENT SIGN UP

Phishing and Malware attacks

Hospital employees are susceptible to being victims of giving away credentials through malicious emails, and also to using malware, typically in the form of a Trojan Horse.

In February 2016, Wyoming Medical Center experienced a phishing attack that left 3,200 patients vulnerable.

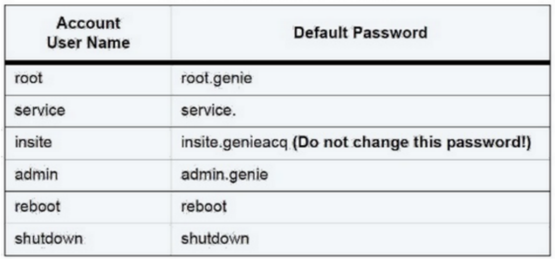
In December 2016, Three UK hospitals shut down operations for two days after a malware attack.

Ransomware

Sometimes the malware which the Hospital falls victim to is in the form of 'ransomware'.

In February 2016, Hollywood Presbyterian Medical Center in California had no choice but to pay $16,900 USD in bitcoins after its Electronic Health Records were held ransom.

Table 3-8: Acquisition Passwords



Account User Name	Default Password
root	root.genie
service	service.
insite	insite.genieacq **(Do not change this password!)**
admin	admin.genie
reboot	reboot
shutdown	shutdown

Default Passwords

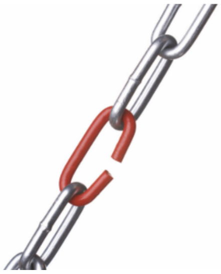
Hospitals use some medical devices which specify the user to never change default passwords for remote technical support.

An example of this is the GE Millenium MG and NC Nuclear Imaging.

Insufficient Security

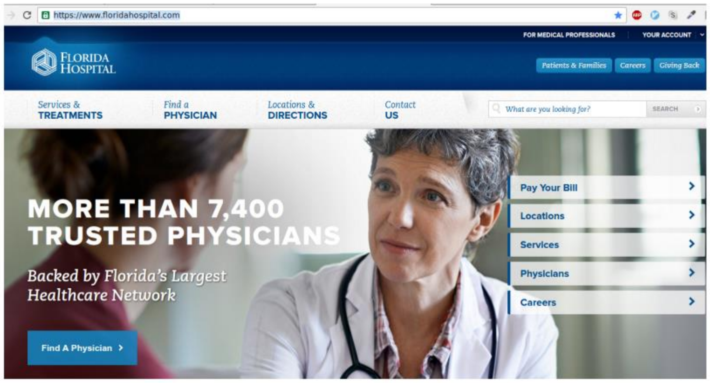
Sometimes the devices lack sufficient security or an endpoint on the Hospital's external and/or public (visitor) network is poorly protected.

The Hospira LifeCare PCA Infusion System before 7.0 Uses unauthorized Telnet sessions, which allow for an attacker to modify its settings, such as drug dosage..



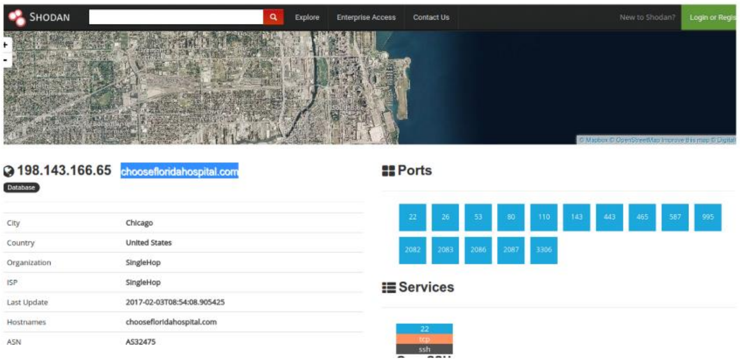
Internet Exposure

Why you should leave your internal infrastructure separate from your external.



Florida Hospital

Is a legitimate hospital site, but it has an associated site with many of its ports open.



198.143.166.65 choosefloridahospital.com

Database

City	Chicago
Country	United States
Organization	SingleHop
ISP	SingleHop
Last Update	2017-02-03T08:54:08.905425
Hostnames	choosefloridahospital.com
ASN	AS32475

Ports

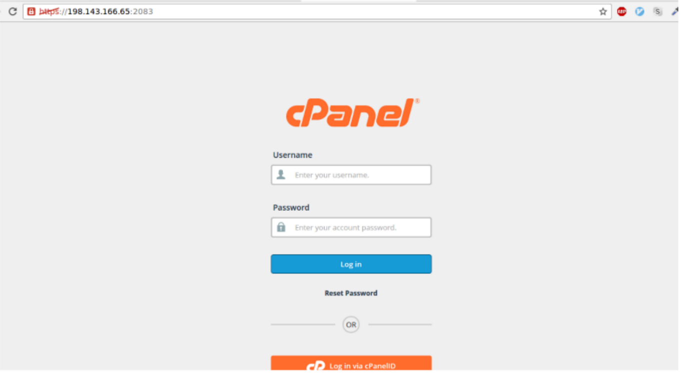
22 26 53 80 110 143 443 465 587 995
2082 2083 2086 2087 3306

Services

22
tcp
ssh

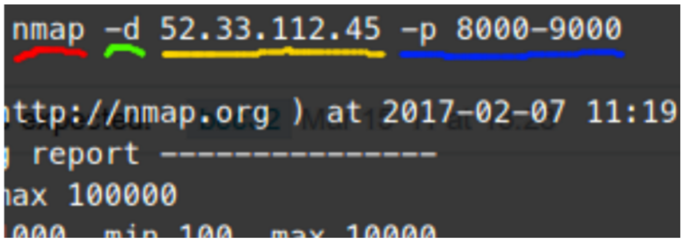
Shodan

Shodan is a database of public IP's which displays open ports and their type of service.



Exploring an open port

One of the ports turns out to be a CPanel login.



```
nmap -d 52.33.112.45 -p 8000-9000

ttp://nmap.org ) at 2017-02-07 11:19
g report ---------------
nax 100000
000  min 100  max 10000
```

Using Nmap

We can simulate a similar probe to Shodan using nmap on this site

Nmap Command

Try to see filtered ports (ports which avoid being probed)

IP of server

Ports to scan

Nonexistant Security

Telnet????

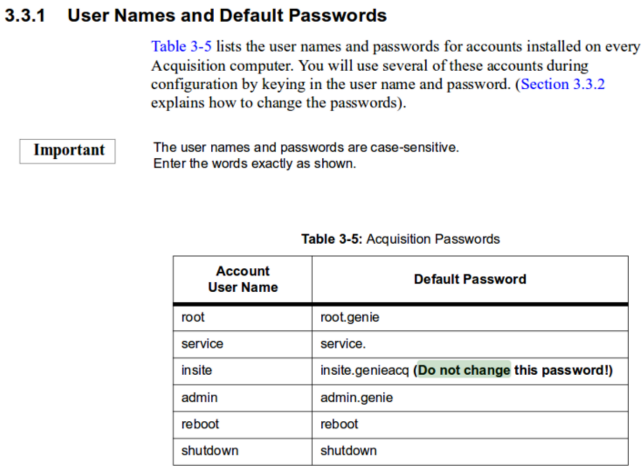
Hospira LifeCare PCA Infusion System

> Hospira Lifecare PCA infusion pump running "SW ver 412" does not require authentication for Telnet sessions, which allows remote attackers to gain root privileges via TCP port 23.

Link to CVE

Insufficient Security in Medical Devices

Why the medical device industry needs to step up their security game.



3.3.1 User Names and Default Passwords

Table 3-5 lists the user names and passwords for accounts installed on every Acquisition computer. You will use several of these accounts during configuration by keying in the user name and password. (Section 3.3.2 explains how to change the passwords).

Important The user names and passwords are case-sensitive. Enter the words exactly as shown.

Table 3-5: Acquisition Passwords

Account User Name	Default Password
root	root.genie
service	service.
insite	insite.genieacq **(Do not change this password!)**
admin	admin.genie
reboot	reboot
shutdown	shutdown

GE Healthcare Millennium MG, NC, and MyoSIGHT

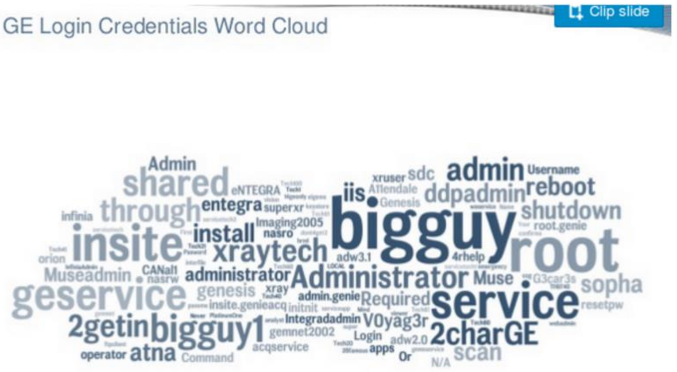
Imaging machines have default passwords which are not supposed to be changed (for remote support).

Link to manual

Using medical devices as pivot points

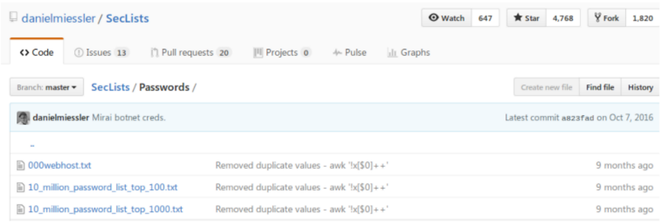
Hackers have an increased ability to move accross a hospital network if they gain access to devices on that network: These devices are used as key pivot points.

Source



Multiple CVE's for GE devices can be collected for passwords

This wordcloud was created using default passwords from GE medical devices.



danielmiessler / SecLists

Watch 647 | Star 4,768 | Fork 1,820

<> Code | Issues 13 | Pull requests 20 | Projects 0 | Pulse | Graphs

Branch: master ▾ SecLists / Passwords /

Create new file | Find file | History

danielmiessler Mirai botnet creds. Latest commit a823fad on Oct 7, 2016

..

000webhost.txt	Removed duplicate values - awk '!x[$0]++'	9 months ago
10_million_password_list_top_100.txt	Removed duplicate values - awk '!x[$0]++'	9 months ago
10_million_password_list_top_1000.txt	Removed duplicate values - awk '!x[$0]++'	9 months ago

Wordlists of likely passwords are distributed online

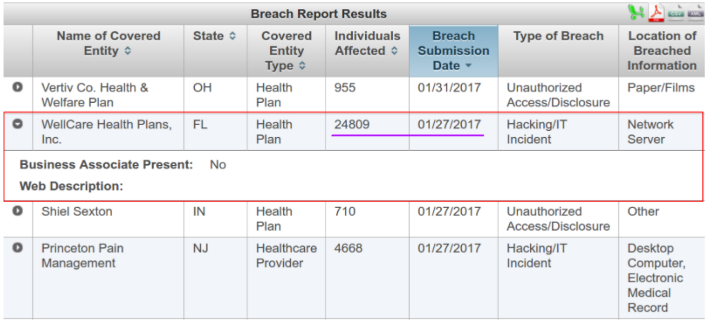
This wordlist can be retrieved from github. It was created using compromised passwords.

The Jackpot

What a hacker looks for in a hospital network

Electronic Health Records

1. Electronic Health Records are typically worth 20 times more than your credit card
2. EHRs typically contain a person's name, address, phone number, DOB, SSN, medical + employment information; selling for as low as $60USD on the black market.



Breach Report Results

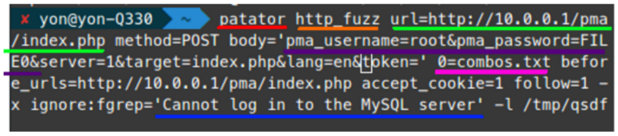
	Name of Covered Entity ⇕	State ⇕	Covered Entity Type ⇕	Individuals Affected ⇕	Breach Submission Date ▾	Type of Breach	Location of Breached Information
●	Vertiv Co. Health & Welfare Plan	OH	Health Plan	955	01/31/2017	Unauthorized Access/Disclosure	Paper/Films
●	WellCare Health Plans, Inc.	FL	Health Plan	24809	01/27/2017	Hacking/IT Incident	Network Server
	Business Associate Present: No						
	Web Description:						
●	Shiel Sexton	IN	Health Plan	710	01/27/2017	Unauthorized Access/Disclosure	Other
●	Princeton Pain Management	NJ	Healthcare Provider	4668	01/27/2017	Hacking/IT Incident	Desktop Computer, Electronic Medical Record

Electronic Health Records

1. Hospitals have only recently transitioned from paper to electronic Health Records
2. Between 2010 and 2012, there was a reported increase of 200% for EHR-related security incidents
3. Big breaches for EHRs are common and recent

Bruteforcing using wordlists

Using patator



```
✘ yon@yon-Q330 ~ patator http_fuzz url=http://10.0.0.1/pma
/index.php method=POST body='pma_username=root&pma_password=FIL
E0&server=1&target=index.php&lang=en&token=' 0=combos.txt befor
e_urls=http://10.0.0.1/pma/index.php accept_cookie=1 follow=1 -
x ignore:fgrep='Cannot log in to the MySQL server' -l /tmp/qsdf
```

Patator

Patator command

Service to bruteforce over

Server + Endpoint

Username + Password combination

Password file

Failed login message to look for in HTTP response

Implantable Medical Devices

Cyborg cybersecurity?

Implantable Medical Devices

1. IMDs are used to treat physiological conditions with the body: Pacemakers, Cardiac Defibrillators and Insulin Pumps.
2. Over 25 Million U.S citizens currently rely on IMDs
3. The newest generation of cardiac defibrillators can wirelessly communicate within 5 meters

Source

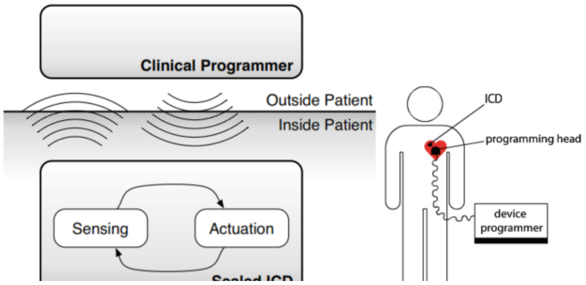
Security and Privacy goals of IMDs

1. Authorization
    1. Personal authorization
    2. Role based authorization
    3. IMD selection
2. Availability
3. Device software and Settings
4. Device-existance privacy
5. Bearer privacy
6. Data Integrity

Source

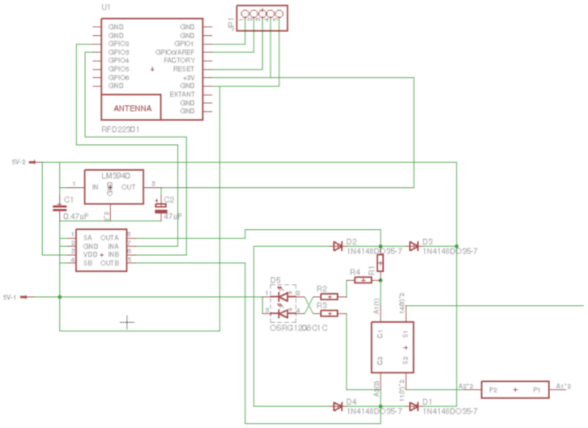
Types of Adversaries

1. Passive Adversaries
2. Active Adversaries
3. Insiders



Threat Modeling: ICDs

1. Implantable Cardiac Defibrillators(ICDs)
2. Wireless signal interception using Software-radio tools (wave listener)
3. Compromising the lifetime of the ICD



IMD Design Principles

1. Consider security in early design phases
2. Encrypt sensitive traffic where possible
3. Authenticate third party devices where possible
4. Don't rely on security through obscurity
5. Develop a realistic threat model and defend the most attractive target first

Hitting the jackpot

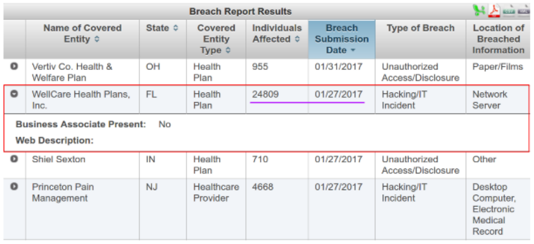
Electronic Health Records Rule Everything Around Me

Using our acquired credentials

Using our acquired credentials we can access confidential records

The Future of Medical Cybersecurity

A summary of the current state and predictions for the future



Breach Report Results

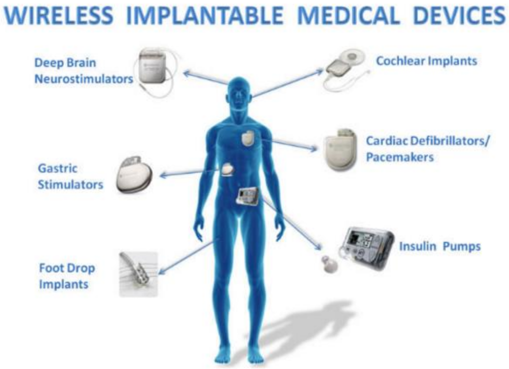
	Name of Covered Entity	State	Covered Entity Type	Individuals Affected	Breach Submission Date	Type of Breach	Location of Breached Information
	Vertiv Co. Health & Welfare Plan	OH	Health Plan	955	01/31/2017	Unauthorized Access/Disclosure	Paper/Films
	WellCare Health Plans, Inc.	FL	Health Plan	24809	01/27/2017	Hacking/IT Incident	Network Server
	Business Associate Present: No						
	Web Description:						
	Shiel Sexton	IN	Health Plan	710	01/27/2017	Unauthorized Access/Disclosure	Other
	Princeton Pain Management	NJ	Healthcare Provider	4668	01/27/2017	Hacking/IT Incident	Desktop Computer, Electronic Medical Record

Electronic Health Records

Remain valuable and are often breached

Network-connected Medical Devices

Often designed or executed by the industry in an insecure fashion

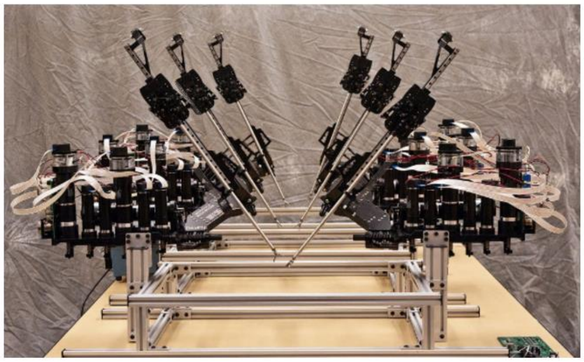

WIRELESS IMPLANTABLE MEDICAL DEVICES
Deep Brain Neurostimulators
Cochlear Implants
Cardiac Defibrillators/ Pacemakers
Gastric Stimulators
Insulin Pumps
Foot Drop Implants

Implantable Medical Devices

Are increasingly common yet poorly secured. A reflection of the current state of medical cybersecurity.

Are we ready for the future?

A preview of what is to come



Wi-Fi & Teleoperated Surgical Robots

Have non-private networks often used to operate these machines in emergency/remote locations.

The future of Electronic Health Records

> The task force calls for EHR vendors to use APIs that will enable EHRs to become more open to innovators, researchers and patients. The public APIs and data standards should be consensus based, transparent, well documented, and openly available in a fair and non-discriminatory way, it writes.

> [The American Medical Informatics Association] calls for promoting the integration of EHRs into the full social context of care, moving beyond acute care and clinic settings to include all areas of care: home health, specialist care, laboratory, pharmacy, population health, long-term care, and physical and behavioral therapies.

Source

Questions:

When is the best time for and attacker to issue an attack against an implantable cardiac defibrillator (ICD)?

A) While the ICD it is active mode
B) While the ICD is in sleep mode
C) While the ICD is communicating with device programmer
D) While the ICD is taking measurements

What is the name of the teleoperated medical device that was hacked in a demonstration by University of Washington?

A) Pigeon 88
B) Raven II
C) Wireless Medical 9000 Overclocked
D) Samsung Note 7

Why are Medical Devices connected to a network of interest of an Attacker, even if the ultimate goal of the Attacker is not associated directly with a Medical Device?

A) The Attacker can hold an Infusion Pump ransom
B) The Attacker can gain experience from hacking these devices
C) The Attacker can use these devices as pivot points to traverse the network
D) None of the above

References

W. Burleson, S. S. Clark, B. Ransford and K. Fu, "Design challenges for secure implantable medical devices," *DAC Design Automation Conference 2012*, San Francisco, CA, 2012, pp. 12-17.
doi: 10.1145/2228360.2228364

D. Halperin, T. S. Heydt-Benjamin, K. Fu, T. Kohno and W. H. Maisel, "Security and Privacy for Implantable Medical Devices," in *IEEE Pervasive Computing*, vol. 7, no. 1, pp. 30-39, Jan.-March 2008.
doi: 10.1109/MPRV.2008.16

T. Denning, A. Borning, B. Friedman, B. T. Gill, T. Kohno, and W. H. Maisel, "Patients, Pacemakers, and Implantable Defibrillators: Human Values and Security for Wireless Implantable Medical Devices," In *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems* (CHI '10). ACM, New York, NY, USA, 917-926. DOI=http://dx.doi.org.ezproxy.library.yorku.ca/10.1145/1753326.1753462

E. Marin, D. Singelée, F. D. Garcia, T. Chothia, R. Willems, and B. Preneel. 2016. On the (in)security of the latest generation implantable cardiac defibrillators and how to secure them. In *Proceedings of the 32nd Annual Conference on Computer Security Applications* (ACSAC '16). ACM, New York, NY, USA, 226-236. DOI: https://doi-org.ezproxy.library.yorku.ca/10.1145/2991079.2991094

Patricia AH Williams, Andrew J Woodward. "Cybersecurity Vulnerabilities In Medical Devices: A Complex Environment And Multifaceted Problem". *PubMed Central (PMC)*. N.p., 2017. [Online]. Available at: https://www.ncbi.nlm.nih.gov/pmc/articles/PMC4516335/ [Accessed 11 Feb. 2017].

Christina Farr, 'On The Dark Web, Medical Records Are A Hot Commodity', [Online]. Available at: https://www.fastcompany.com/3061543/on-the-dark-web-medical-records-are-a-hot-commodity [Accessed 2 Feb. 2017].

Chad Terhune, 'UCLA Health System data breach affects 4.5 million patients' [Online]. Available at: http://www.latimes.com/business/la-fi-ucla-medical-data-20150717-story.html [Accessed 2 Feb. 2017].

Accenture.com, 'Cyberattacks Will Cost U.S. Health Systems $305 Billion Over Five Years, Accenture Forecasts' [Online]. Available at: https://newsroom.accenture.com/news/cyberattacks-will-cost-us-health-systems-305-billion-over-five-years-accenture-forecasts.htm [Accessed 2 Feb. 2017].

Niam Yaraghi, 'Hackers, phishers, and disappearing thumb drives: Lessons learned from major health care data breaches' [Online]. Available at: https://www.brookings.edu/wp-content/uploads/2016/07/Patient-Privacy504v3.pdf [Accessed 2 Feb. 2017].

MediSafe, Health Security Infographic [Online]. Available at: http://wrm5sysfkg-flywheel.netdna-ssl.com/wp-content/uploads/2016/02/Medisafe-mHealth-Security-Infographic.png [Accessed 2 Feb. 2017].

RightPatient, Anatomy of Medical Device Attacks [Online]. Available at: http://www.rightpatient.com/wp-content/uploads/2016/12/Arxan_Anatomy_of_Med_Device_Attacks-1-1-1-1-121516.jpg [Accessed 2 Feb. 2017].

ESET, Healthcare IT + Cybersecurity [Online]. Available at: http://www.welivesecurity.com/wp-content/uploads/2013/08/ESET-healthcare-infographic.png [Accessed 2 Feb. 2017].

HIPAA Journal, 'Three Hospitals' Medical Devices Hacked Using Ancient XP Exploits' [Online]. Available at: http://www.hipaajournal.com/three-hospitals-medical-devices-hacked-using-xp-exploits-3487/ [Accessed 2 Feb. 2017].

Lindsey Hoshaw, ‘Millions of Americans Use Medical Devices That May Be Vulnerable to Hacking’ [Online]. Available at: http://ww2.kqed.org/futureofyou/2015/08/03/millions-of-americans-use-medical-devices-that-are-vulnerable-to-hacking/ [Accessed 2 Feb. 2017].

Jennifer Langston, ‘UW researchers hack a teleoperated surgical robot to reveal security flaws’ [Online]. Available at: http://www.washington.edu/news/2015/05/07/uw-researchers-hack-a-teleoperated-surgical-robot-to-reveal-security-flaws/ [Accessed 2 Feb. 2017].

Health Data Management. (2016). *Clicks on phishing email led to breach, hospital exec says*. [online] Available at: http://www.healthdatamanagement.com/news/wyoming-medical-security-training-didnt-prevent-attack [Accessed 4 Feb. 2017].

Millennium MyoSIGHT Nuclear Medicine Imaging System Service Manual. (2004). 4th ed. [ebook] Tirat Hacarmel, Israel: General Electrics, p.97. Available at: http://apps.gehealthcare.com/servlet/ClientServlet/2354459-100.pdf?REQ=RAA&DIRECTION=2354459-100&FILENAME=2354459-100.pdf&FILEREV=4&DOCREV_ORG=4 [Accessed 4 Feb. 2017].

National Vulnerability Database. (2017). *NVD - Detail*. [online] Available at: https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2015-3459 [Accessed 4 Feb. 2017].

Ore, J. (2016). *How hospitals are helping cybercriminals get rich quick*. [online] CBC News. Available at: http://www.cbc.ca/news/technology/hollywood-hospital-hack-ransomware-trends-1.3462062 [Accessed 4 Feb. 2017].

Zorz, Z. (2016). *Services disrupted at three UK hospitals due to virus attack - Help Net Security*. [online] Help Net Security. Available at: https://www.helpnetsecurity.com/2016/11/01/uk-hospitals-virus-attack/ [Accessed 4 Feb. 2017].

Database of Breaches: https://ocrportal.hhs.gov/ocr/breach/breach_report.jsf