MEDICAL DEVICES SECURITY

Wireless Implantable medical devices

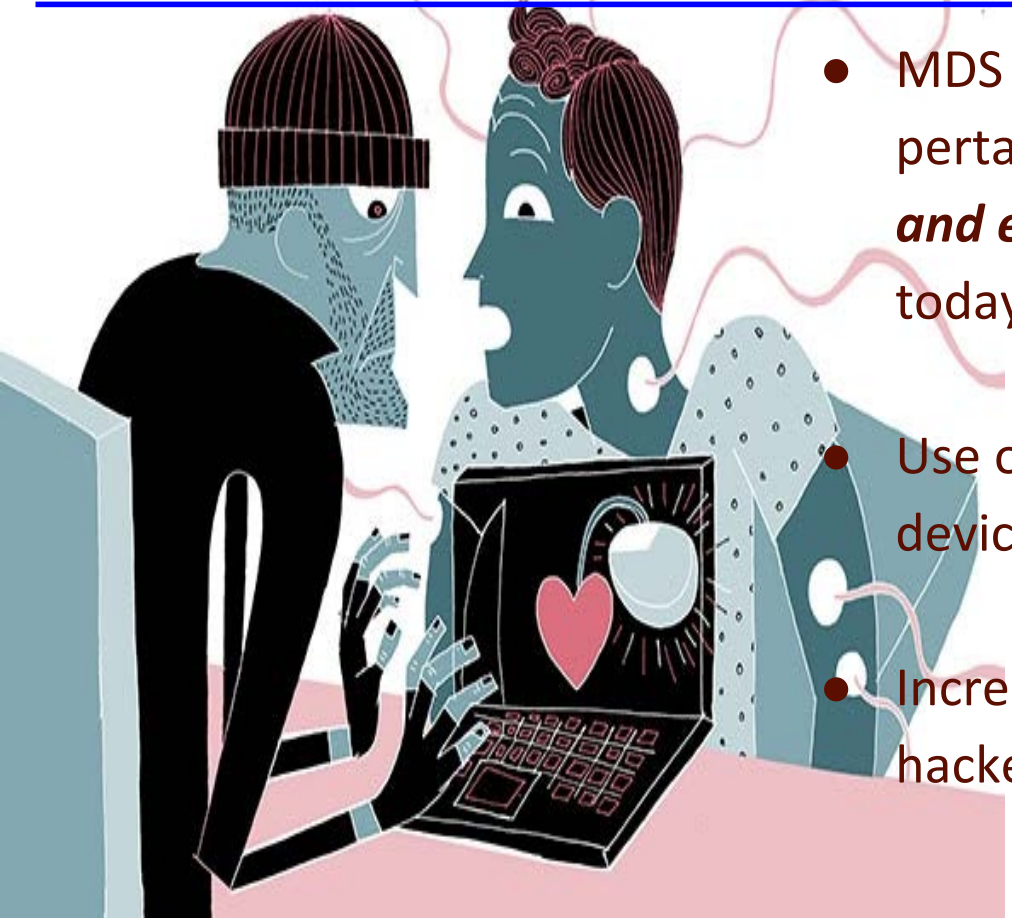
Introduction to Computer Security
EECS 3482

Presenters
Atoosa Etedali
Eric Sekyere
Rizvana Buhari

What are Medical Devices?

- Instruments used in diagnosis, management and treatment of various pathologies
- Also used in drug administration.
- Can be implanted {i.e. inserted into human body}
- Can be used Externally{i.e attached outside the human body}
- Common types of medical devices: Cardiac pacemakers, Infusion Pumps, Anesthesia devices etc...

What is Medical Device Security?



- MDS describes and examines all issues pertaining to the; ***use, safety,functionality and efficiency*** of all medical devices used today in health care
- Use of ***wireless IMD's*** (implantable medical devices) has become common currently
- Increase use of Wireless IMD's has allowed hackers to ***compromise security and privacy***

Example of wireless Implanted Medical Devices

- Gastric Stimulators
- Cochlear Implants
- Insulin Pumps
- DBS
- Pacemakers

Why should we be concerned:

- ➔ 2.5 million people rely on IMDs
- ➔ Increasing demand for IMDs ~ 7.7% annually
- ➔ Industry growth expected hit $52 billion by the end of 2015
- ➔ U.S. FOOD AND DRUG ADMINISTRATION (FDA)
  - ◆ Released draft guidance for cybersecurity concerns
  - ◆ Development a cybersecurity laboratory

What *THREATS* are we facing?

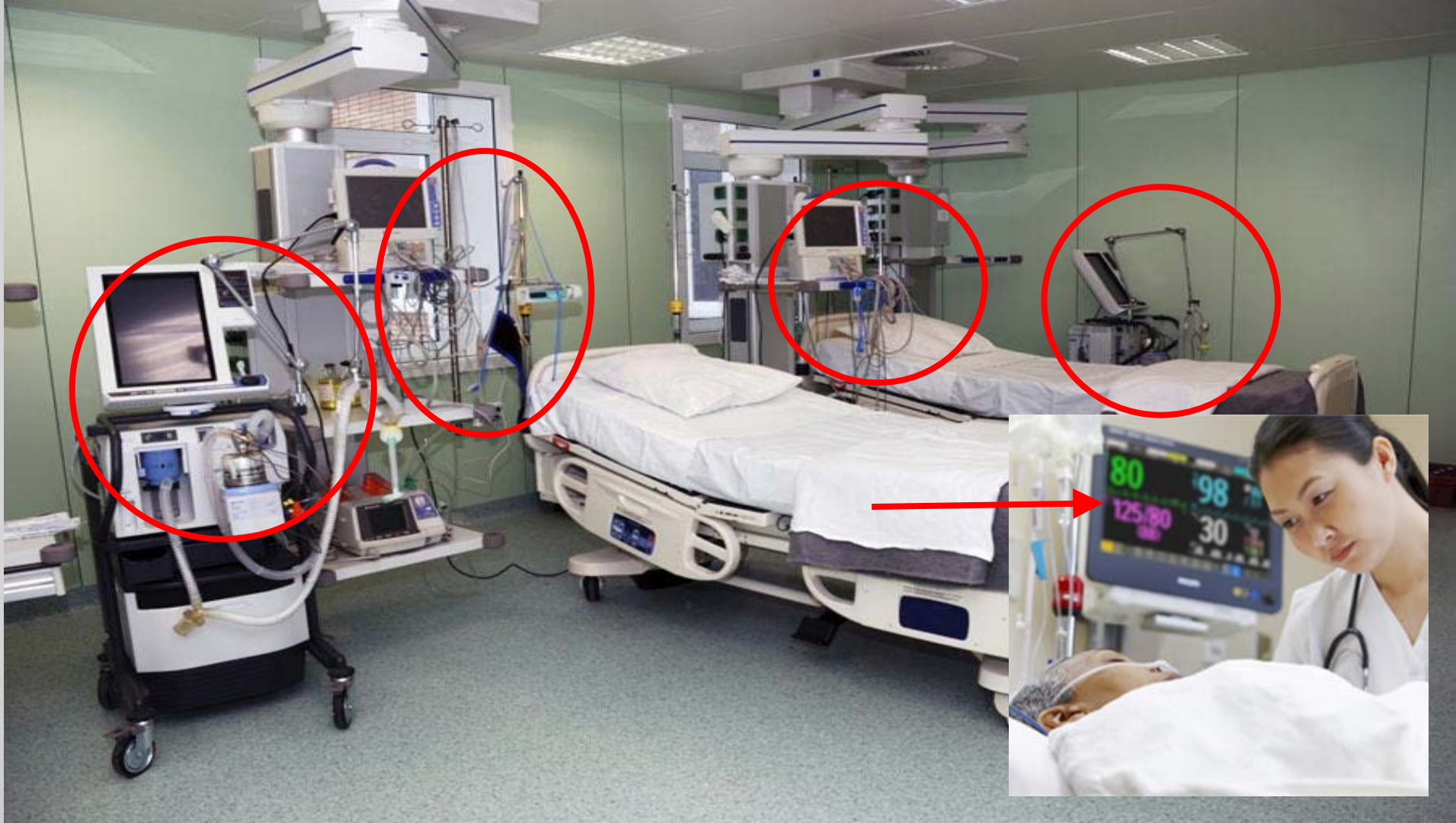
Data extraction

Device reprogramming

Repeated access attempts

Data tampering

Data flooding

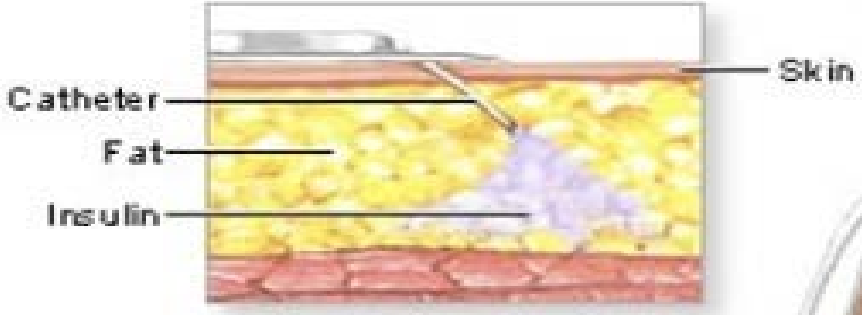

80
98
125/80
30

VULNERABILITIES

- Unsecured communication channels
- Inadequate authentication and access control
- Weak audit mechanisms
- Inadequate storage

INSULIN PUMP

an example...



Dosage instructions are entered into the pump's small computer and the appropriate amount of insulin is then injected into the body in a calculated, controlled manner

Insulin pump

http://www.wired.co.uk/news/archive/2011-08/22/medical-device-security/viewgallery/270048

How is the attack done?

1. Using a high-powered antenna, an attacker can remotely manipulate the medical device without the patient's knowledge.

2. If the medical device does not have authentication or authorization, it allows the attacker to inappropriately access the device.

3. Using the laptop and antenna, the attacker can manipulate the medical device by adjusting the settings or turning it off.

NOTABLE RESERCHE(R)S

Jack Barnaby: Researcher @ McAfee Inc.

Accomplisments: 2012

•Hacked Insulin pumps in home lab
•Up to 300 feet away, scan for pumps
•Force them to dispense fatal insulin doses
•Doesn't need to be close to the victim
•No serial number of device necessary
•Demonstrated pacemakers can be remotely controlled
•commanded to deliver a 830-volt shock via a laptop

Jerome Radcliffe: Researcher, Senior Security Analyst @ InGuardians

Accomplishments: 2011

•A Type 1 diabetic patient, Hacked his own insulin pump
•Required serial number
•Close to victim

Kevin Fu: Researcher, Computer Scientist @ U of Michigan, U of Massachusetts

•Various research papers on Security of Medical Devices
•(In) Security and Privacy Research (SPQR) Lab use the artificial cadaver to test and
•Develop the security and privacy of various medical devices, including heart rate sensors,
•pacemakers, defibrillators, drug delivery systems, and neurostimulators

Medical Device Security vs IT Security

- Responsibility of device manufacturers, hospitals and healthcare facilities
- A priori approach: regulatory, software and operating environments in hospitals/home and applications(medicine)
- Impossible to even install/maintain an anti-virus

- Responsibility of everyone who access/handle corporate data
- Client-Server Model
- Server: Firewall/IPS and Client: anti-virus

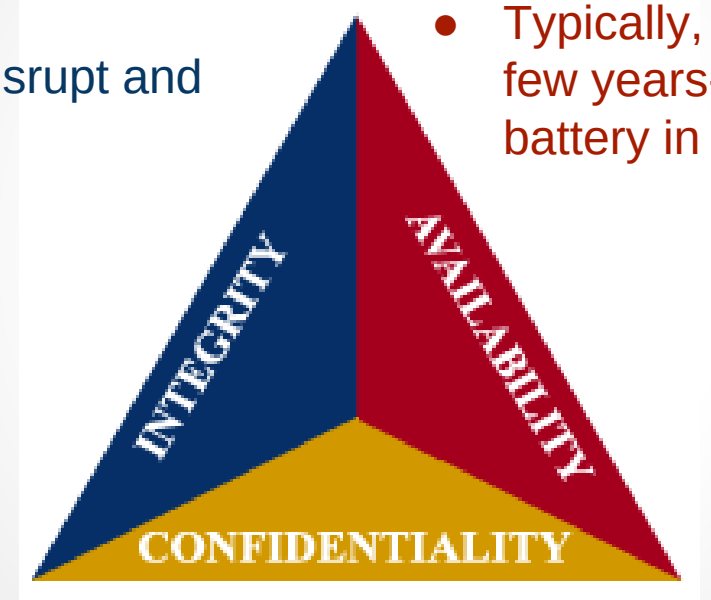
vulnerable to attacks : VIRUS

vulnerable to attacks : VIRUS

CIA TRIANGLE

HACKER CAN...

- Modify health info stored in device
- Raise false alarms / make diagnosis incorrectly
- Send commands to disrupt and degrade therapy



- DOS attack: keep sending queries; drain battery quickly; severe impact/ nullify device's function
- Typically, an IMD's battery life spans a few years- DOS attacks can drain battery in few hours

- Access any patient's personal details and up-to-date health info

GOOD NEWS !

- Currently there aren't any real life incidents to worry about !
  -Technical skill required means that mass attacks are unlikely
- Awareness: popular T.V. series "Homeland" where VP assassinated by hacking into his pacemaker

BUT…

- Vulnerabilities remain open
- According to research studies, hacking medical devices, and tampering with data (i.e.medicine) is possible
- Sooner than later !

ANY HELP OUT THERE?!

eProtex

- Offer services in RISK ASSESSMENT and RISK MANAGEMENT of medical devices
- Serves > 100 healthcare facilities nationwide

SANS: Securing the Human

- Training on awareness and compliance of information security
- Provide computer based training for the end user
- Offer phishing testing

Challenges

Intentional or Unintentional or System failure?

Few Considerations …

- ★ Chances are your smart phones, tablets and personal computers receive regular updates and patches for known vulnerabilities. Because of FDA restrictions & manufacturer practices, most medical devices DO NOT
- ★ Half of the medical devices run on Windows OS, whose familiarity facilities *intentional & unintentional breaches*
- ★ Many OS in Medical Devices are no longer supported by the original designer. In fact, some life-saving devices still run on DOS, the iconic black screen of the 80's.
- ★ More than 97% of medical devices *can not have anti-malware* software added to them because the manufacturer (and FDA) will not allow it.
- ★ Many medical devices *do not have ability to comply to basic HIPAA requirements* (e.g. unique logins and passwords, user log maintenance, etc.)

Status of MDS today ...

- **Potential for danger**
- **Current area of research/study aim: prevention program**
- **In comparison, industry falling behind in developments of protecting “medical cybercrime”**

DIFFERED OPINIONS:

At this time we believe that the risk is low and the benefits of the therapy to people with diabetes outweigh the risk of an individual criminal attack.

Amanda McNulty Sheldon, Director of Public Relations for Medtronic Diabetes.

Proposed Solutions

- ENCRYPTION
  - Encrypting the data signals in the IMDs
  - Pro:
    - Very effective
  - Cons:
    - Increase in processing power and time
    - Impacts functionality of device
- MEDMON, a FIREWALL
  - Safeguards against present and future innovations
  - Fends of suspicious command and data irregularities
- OPEN-SOURCE
  - Start making open-source devices, so more people can learn how to these devices work.

CONCLUSION

Would you be worried about your medical device? Whose will you hold responsible in case of an attack?

Serious risks require serious attention. Is this area of study worth investing into?

- **Yes. These attacks are deadly! Causing catastrophic harm to millions of people.**

At this time, implantable medical devices aren't the only weak link in the chain. Other medical equipment do contain vulnerabilities.

References

1. http://www.tripwire.com/state-of-security/vulnerability-management/medical-device-security-forget-everything-thought-knew/
2. https://www.youtube.com/watch?v=2vP9V880X
3. http://www.infosecurity-magazine.com/news/medical-device-security-not-as/
4. https://www.infosecurity-magazine.com/magazine-features/the-prognosis-for-medical-device-security/
5. http://csrc.nist.gov/news_events/cps-workshop/cps-workshop_abstract-1_gupta.pdf
6. http://www.cio.com/article/2833830/hipaa-security-privacy/medical-device-security-benchmarks-emerging.html
7. http://www.slideshare.net/hcl/security-for-implantable-medical-devices-imds?next_slideshow=1
8. http://www.itpro.co.uk/643633/security-industry-players-highlight-growing-risk-of-medical-device-hacks
9. https://threatpost.com/medical-device-security-need-major-upgrade-101712/77121
10. http://www.homelandsecuritynewswire.com/dr20150319-wireless-implantable-medical-devices-vulnerable-to-hacking
11. http://resources.infosecinstitute.com/hcking-implantable-medical-devices/
12. http://www.girltalkhome.com/blog/danger-ahead-timely-cautions/
13. http://www.businessreviewusa.com/finance/4008/Financial-challenges-facing-small-businesses-in-2014
14. https://spqr.eecs.umich.edu/papers/49SS2-3_burleson.pdf