CIS129 Notes Final

<https://www.jacc.org/doi/full/10.1016/j.jacc.2018.01.023>

Baranchuk, A., Lakkireddy, D. R., Fisher, J. D., Upadhyay, G., Kutyifa, V., Krishnan, K., Chung, M. K., Patton, K. K., & Refaat, M. M. (n.d.). *JACC journals*. Journal of the American College of Cardiology. https://www.jacc.org/doi/10.1016/j.jacc.2016.06.023

Journal of the American College of Cardiology

[Adrian Baranchuk](https://www.jacc.org/doi/full/10.1016/j.jacc.2018.01.023)

[Marwan M. Refaat](https://www.jacc.org/doi/full/10.1016/j.jacc.2018.01.023)

[Kristen K. Patton](https://www.jacc.org/doi/full/10.1016/j.jacc.2018.01.023)

[Mina K. Chung](https://www.jacc.org/doi/full/10.1016/j.jacc.2018.01.023)

[Kousik Krishnan](https://www.jacc.org/doi/full/10.1016/j.jacc.2018.01.023)

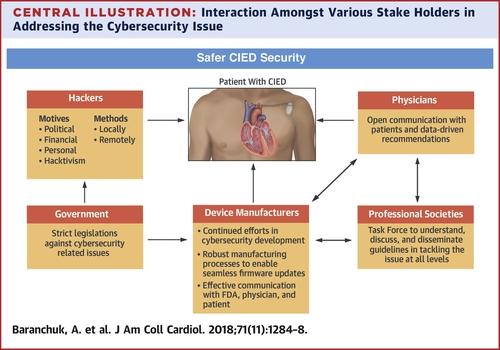
[Valentina Kutyifa](https://www.jacc.org/doi/full/10.1016/j.jacc.2018.01.023)

[Gaurav Upadhyay](https://www.jacc.org/doi/full/10.1016/j.jacc.2018.01.023)

[John D. Fisher](https://www.jacc.org/doi/full/10.1016/j.jacc.2018.01.023)

[Dhanunjaya R. Lakkireddy](https://www.jacc.org/doi/full/10.1016/j.jacc.2018.01.023)

and from the American College of Cardiology’s Electrophysiology Section Leadership



“Based on research into failure modes, this is not a problem restricted to Abbott. The risks exist for any device that is connected to the Internet. Outside of the realm of CIED management, these issues obviously also apply to other medical devices (pain pumps, insulin pumps, continuous positive airway pressure, and rhythm and hemodynamic monitoring) that are connected to the Internet for remote monitoring and programming purposes.”

<https://www.ahajournals.org/doi/full/10.1161/CIRCULATIONAHA.118.037331#:~:text=cyber%20security%20concerns.-,Hacking%20Risk,inappropriate%20shocks%2C%20the%20agency%20noted>.

Pacemaker Recall Highlights Security Concerns for Implantable Devices

Pacemaker recall highlights security concerns for implantable devices | circulation. (n.d.). https://www.ahajournals.org/doi/10.1161/CIRCULATIONAHA.118.037331

* The access might allow the hacker to drain the battery or administer inappropriate shocks to the patient
* Attack is low in chance, as attacker would need to be within feet – Chad Waters
* An analysis by Saxon and collegues show that most physicians and patients chose not to have the firmware updated after the pacemaker recall (75%)
  + Saxon states that the patients, no matter their educational level, were capable of understanding
* There are logistical challenges as well, such as update scheduling
  + [ Would updates disable certain functions? Potential security risks with updating? 75% of asked denied update, so maybe worry or uncertainty]

<https://journals.uob.edu.bh/bitstream/handle/123456789/4033/paper%2020.pdf?sequence=4&isAllowed=y>

Cyber-Attacks on Medical Implants: A Case Study of Cardiac Pacemaker Vulnerability

International Journal of Computing and Digital Systems

Pub: Nov 1 2020

Muhammad Muneed Ur Rehman, Hafiz Zia Ur Rehman and Zeashan Hameed Khan

* Medical Cyber Physical system (MCPS) is a network of regulator, communication, sensing, and actuation of the embedded components to monitor/control the patients [Essentially just a network of computers and sensors for medical assistance. I.E. pacemacker sending info to dr. hospital network, controlled drug doses with real time updates, oxygen sensors.]
  + [Essentially trying to implement more cyber solutions with physical technology by creating more overlap with the advancing IOT (internet of things) and current CPS machines]

Ur Rehman, M. M., Ur Rehman, H. Z., & Kahn, Z. H. (2020, November 1). Cyber-Attacks on Medical Implants: A Case Study of Cardiac Pacemaker Vulnerability.

<https://youtu.be/smhPhmNsvVc>

How medical devices like pacemakers, insulin pumps can be hacked

CBS Mornings

* [ Absolutely crazy stuff. Maybe include either at beginning or end of slide.]

*How medical devices like pacemakers, insulin pumps can be hacked*. YouTube. (2018, November 8). https://youtu.be/smhPhmNsvVc

<https://global.medtronic.com/xg-en/mobileapps/patient-caregiver/cardiac-monitoring/mycarelink-heart-app.html>

Medtronic

The MyCareLink Heart™ app has requirements for your phone or tablet and operating system (called the “OS” from now on) version. The app cannot transfer data between your heart device and the Medtronic CareLink™ network if the requirements are not met. The requirements for your phone or tablet and OS version will change over time. You may need to update, or replace, your phone or tablet and OS to use the app to transfer data between your heart device and the Medtronic CareLink™ network.

* [ Possible that companies make this subscription service in the future. May require constant updates on patient side. Is App just a typical log in w/ password or are there other security measures?]

*MyCareLink Heart App*. Medtronic. (n.d.). https://global.medtronic.com/xg-en/mobileapps/patient-caregiver/cardiac-monitoring/mycarelink-heart-app.html

Questions to possibly pose:

[ Updates with pacemakers have to be within a short range (within 3 feet) as of 2018, as technology advances and more services are pushed toward a care-at-home style, hacking from longer ranges becomes a more plausible event. Should user have access to pacemaker as an open system (like a personal computer) or more so a closed, private system (only settings can be changed through approved dr. creds and possible environment)?

Created Flowchart

[Remember to give gold star to yourself. This was a pain and I know you’ll forget later, Rylan]

A diagram of a company

Description automatically generated

