KHRS 2021 The 13th Annual Scientific Session of the Korean Heart Rhythm Society

Insecurity by Obscurity: A Cybersecurity Risk Assessment of Cardiac Implantable Electronic Devices

Sang-Weon Park M.D.

Bucheon Sejong Hospital, Korea

Korean Heart Rhythm Society
COI Disclosure

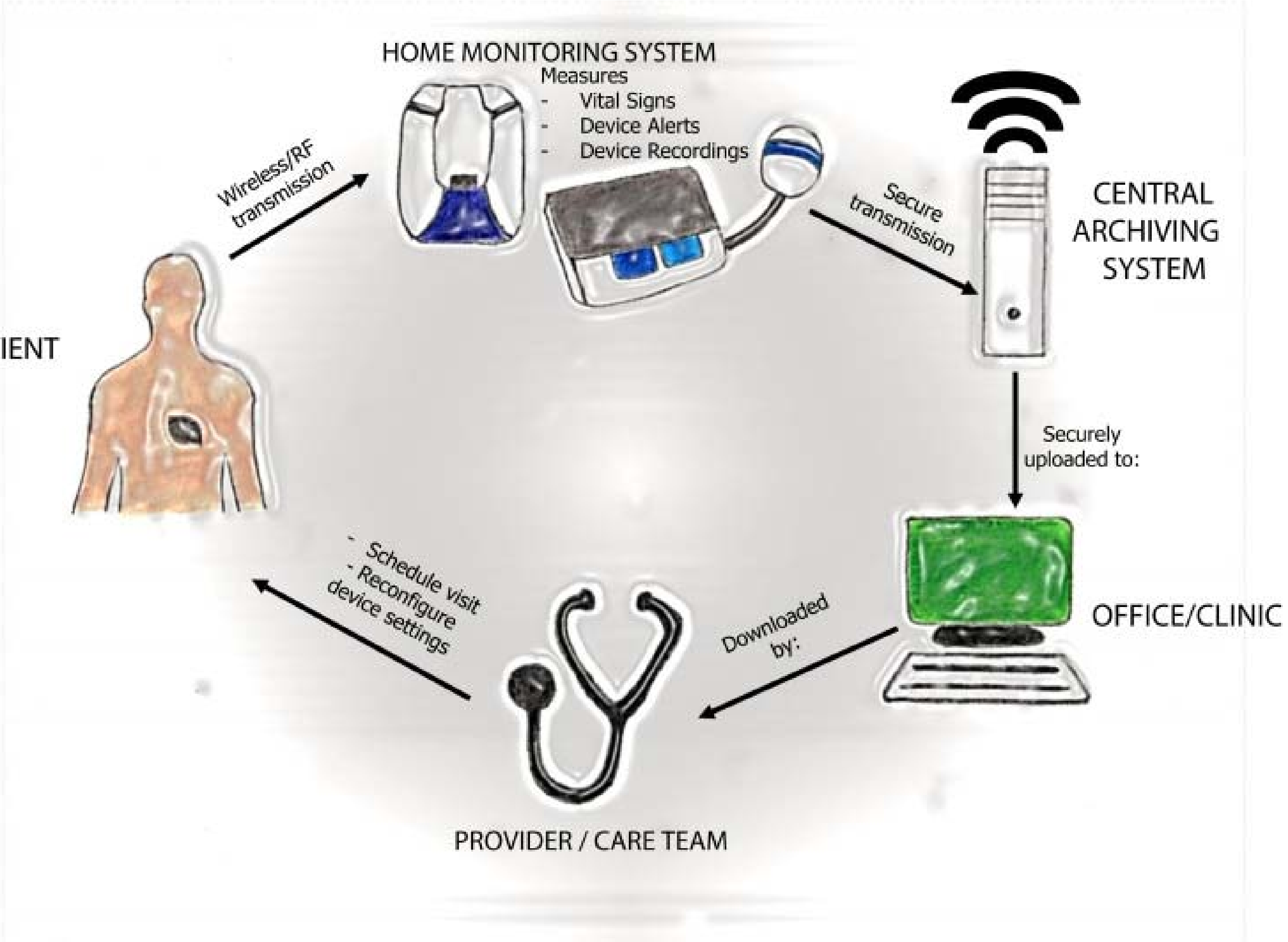
Sang Weon Park

The authors have no financial conflicts of interest to disclose concerning the presentation

Remote monitoring(RM) of CIED

- RM has been developed as a new standard of care in the follow up of patients with CIEDs.
  - Early detection of clinically actionable events
  - Decrease in the frequency and need for in personal evaluation
  - improved patient satisfaction, quality of life and adherence to follow up

CIED Remote Monitoring



(Heart Rhythm 2021;18:473–481)

Cybersecurity Risk of RM

- However, this increased dependency on the Internet of Things comes with risks in the form of cybersecurity lapses and possible attacks.

- The CIED universe comprises a complex interplay of devices, connectivity protocols, and sensitive information flow between the devices and the central cloud server.
- Various manufacturers use proprietary software and black-box connectivity protocols that are susceptible to hacking

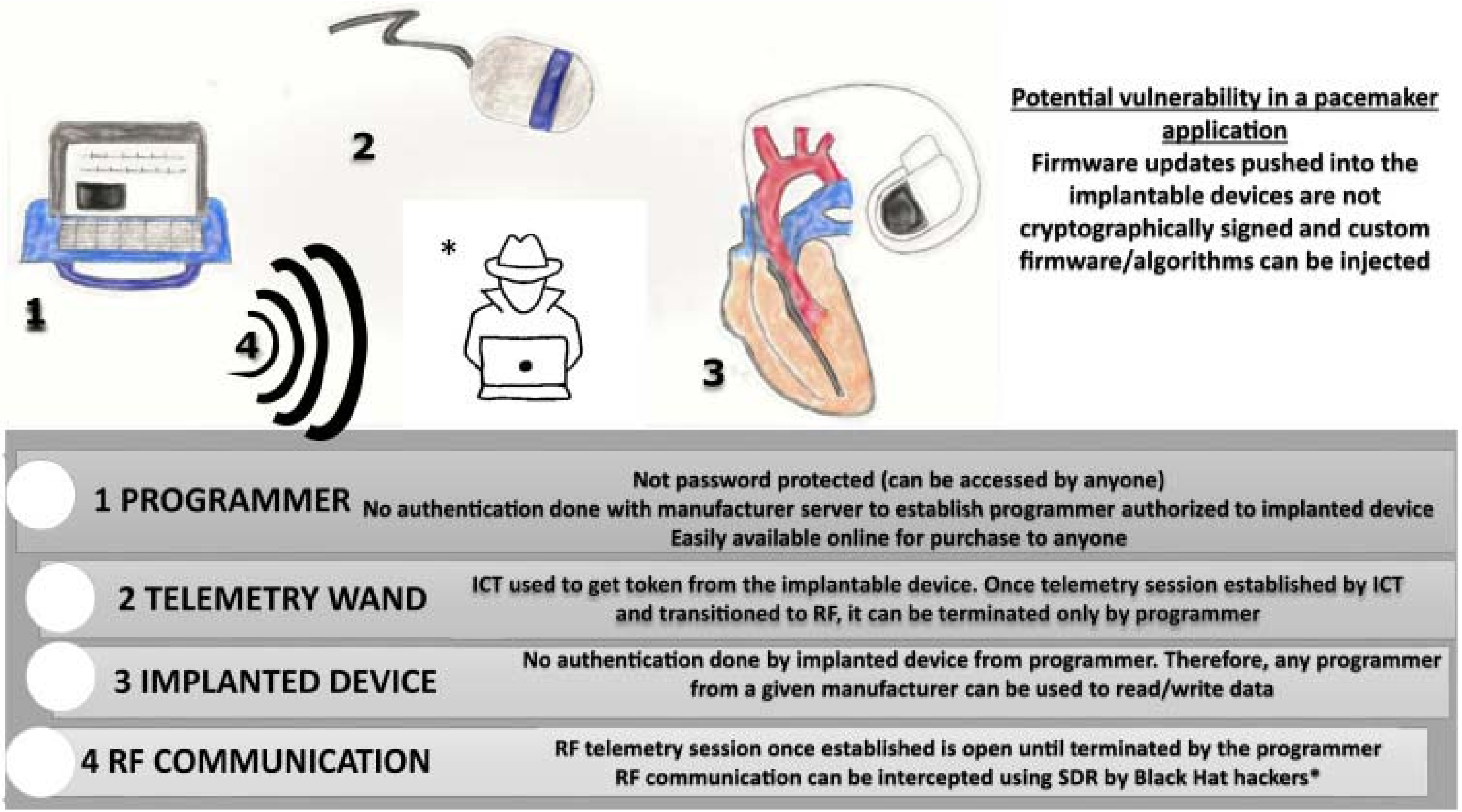
Cyber Attack to RM system

- Passive cyber-attacks aimed at theft of sensitive information
- Active cyber-attack aimed at manipulation of information or pacing/defibrillation settings.

- No cyberattack leading to patient harm has been reported to date, the threat is real and has been demonstrated in research laboratory scenarios and echoed in patient concerns

the assassination of the Vice President of the United States
by a terrorist remotely hacking into the victim’s pacemaker

Security vulnerabilities

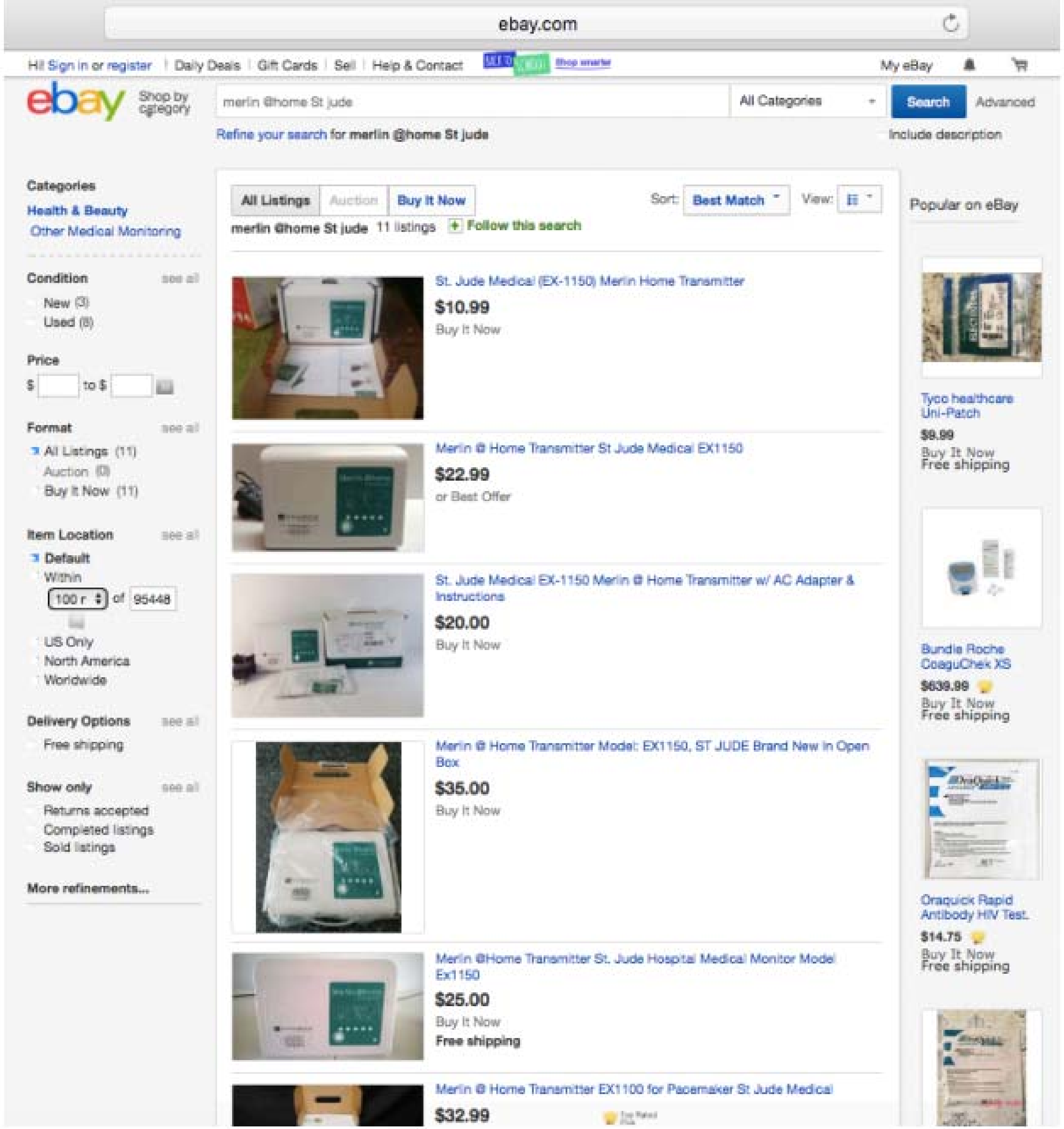


Potential vulnerability in a pacemaker application
Firmware updates pushed into the implantable devices are not cryptographically signed and custom firmware/algorithms can be injected

1 PROGRAMMER	Not password protected (can be accessed by anyone) No authentication done with manufacturer server to establish programmer authorized to implanted device Easily available online for purchase to anyone
2 TELEMETRY WAND	ICT used to get token from the implantable device. Once telemetry session established by ICT and transitioned to RF, it can be terminated only by programmer
3 IMPLANTED DEVICE	No authentication done by implanted device from programmer. Therefore, any programmer from a given manufacturer can be used to read/write data
4 RF COMMUNICATION	RF telemetry session once established is open until terminated by the programmer RF communication can be intercepted using SDR by Black Hat hackers*

- ICD = inductive coil telemetry
- RF = radiofrequency
- SDR = software-defined radio.

(Heart Rhythm 2021;18:473–481)



merlin @home St jude

Refine your search for **merlin @home St jude**

Categories

Health & Beauty

Other Medical Monitoring

Condition see all

New (3)

Used (8)

Price

$ to $

Format see all

All Listings (11)

Auction (0)

Buy It Now (11)

Item Location see all

Default

Within 100 r of 95448

US Only

North America

Worldwide

Delivery Options see all

Free shipping

Show only see all

Returns accepted

Completed listings

Sold listings

merlin @home St jude 11 listings + Follow this search

St. Jude Medical (EX-1150) Merlin Home Transmitter
$10.99
Buy It Now

Merlin @ Home Transmitter St Jude Medical EX1150
$22.99
or Best Offer

St. Jude Medical EX-1150 Merlin @ Home Transmitter w/ AC Adapter & Instructions
$20.00
Buy It Now

Merlin @ Home Transmitter Model: EX1150, ST JUDE Brand New in Open Box
$35.00
Buy It Now

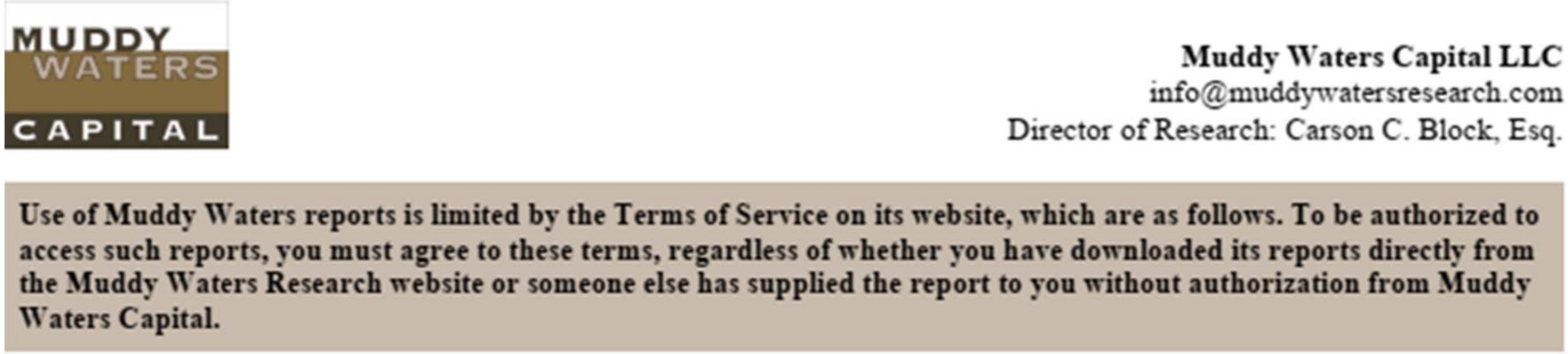
Merlin @Home Transmitter St. Jude Hospital Medical Monitor Model Ex1150
$25.00
Buy It Now
Free shipping

Merlin @ Home Transmitter EX1100 for Pacemaker St Jude Medical
$32.99 Top Rated Plus

Tyco healthcare Uni-Patch
$9.99
Buy It Now
Free shipping

Bundle Roche CoaguChek XS
$639.99
Buy It Now
Free shipping

Oraquick Rapid Antibody HIV Test.
$14.75
Buy It Now
Free shipping



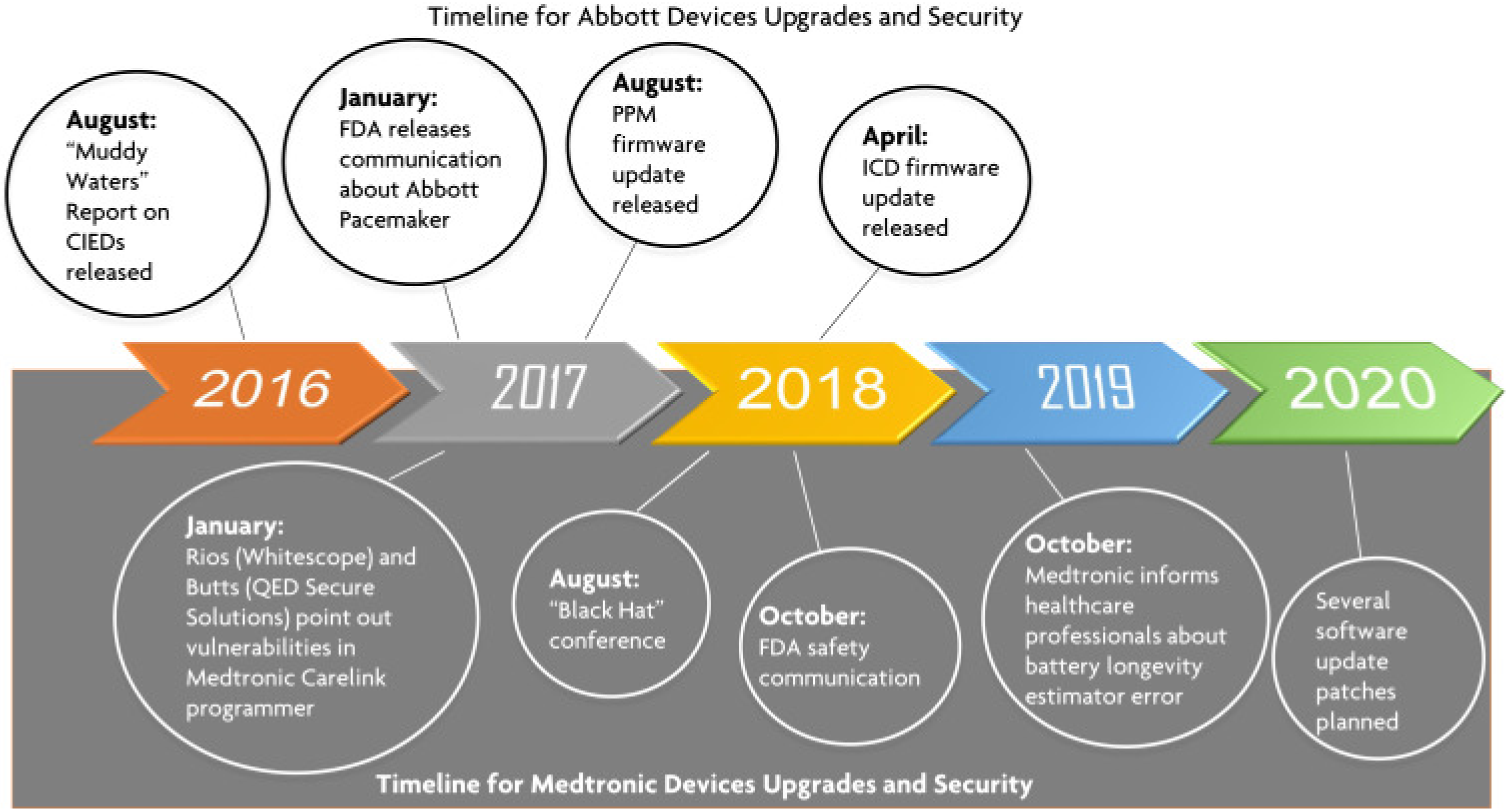
Muddy Waters Capital LLC
info@muddywatersresearch.com
Director of Research: Carson C. Block, Esq.

Use of Muddy Waters reports is limited by the Terms of Service on its website, which are as follows. To be authorized to access such reports, you must agree to these terms, regardless of whether you have downloaded its reports directly from the Muddy Waters Research website or someone else has supplied the report to you without authorization from Muddy Waters Capital.

in August of 2016, St. Jude Medical (now Abbott) was put in the public spotlight following the release of short-sell report by Muddy Waters LLC outlining

two methods by which their pacemaker cybersecurity could be breached in what was termed a “crash attack” and a “battery drain attack.”

Timeline of cybersecurity events



Timeline for Abbott Devices Upgrades and Security

August: "Muddy Waters" Report on CIEDs released

January: FDA releases communication about Abbott Pacemaker

August: PPM firmware update released

April: ICD firmware update released

January: Rios (Whitescope) and Butts (QED Secure Solutions) point out vulnerabilities in Medtronic Carelink programmer

August: "Black Hat" conference

October: FDA safety communication

October: Medtronic informs healthcare professionals about battery longevity estimator error

Several software update patches planned

Timeline for Medtronic Devices Upgrades and Security

(Heart Rhythm 2021;18:473–481)

Adverse event during Upgrade

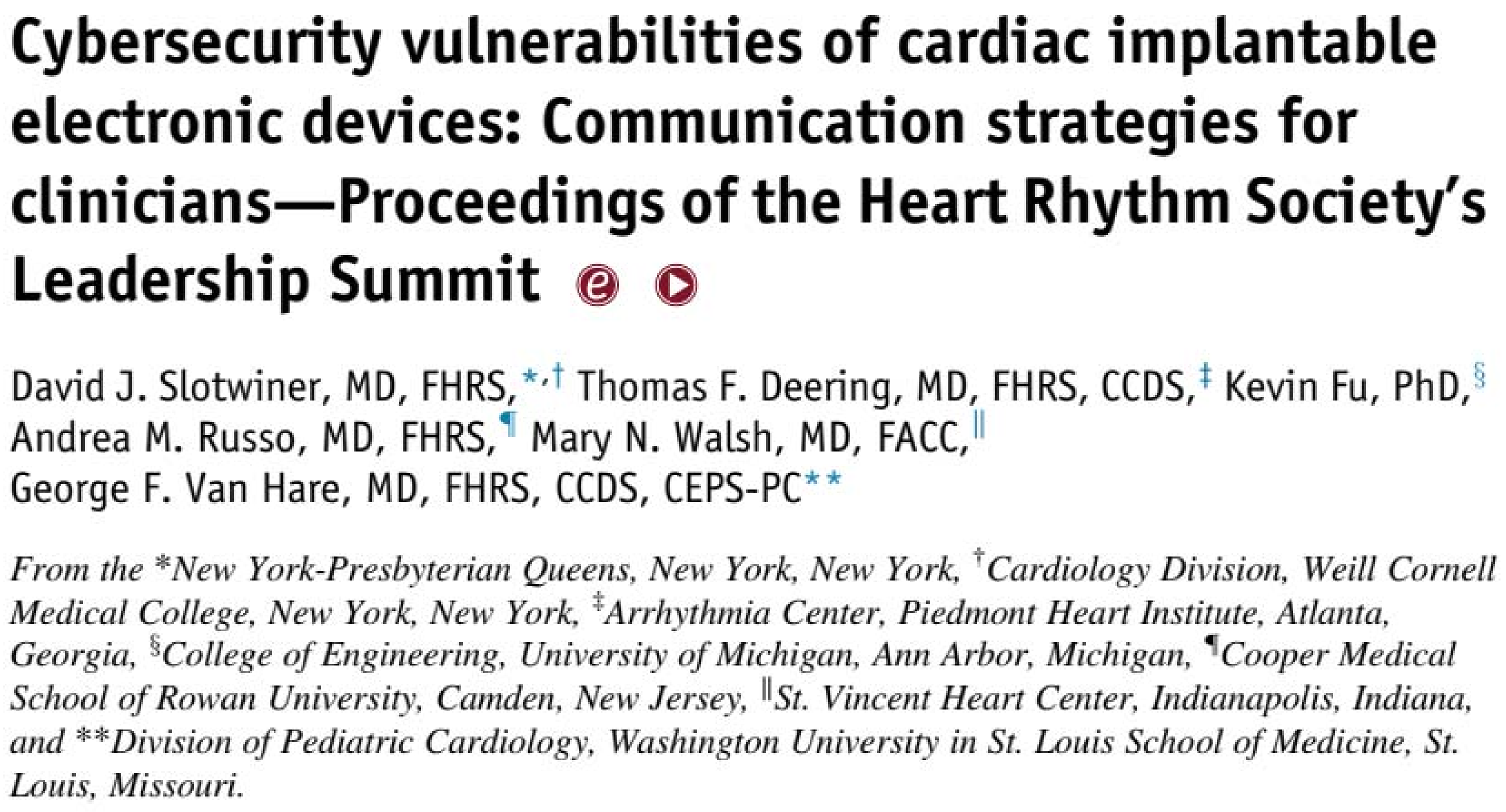
Abbot has quoted the following small, but not insignificant, risk of adverse events:

- complete loss of function (0.003%)

- loss of device settings (0.023%)

- failure of the update (0.161%)

Due to these risks, it has been recommended that the upgrade take place in a center with the ability to perform urgent temporary pacing.



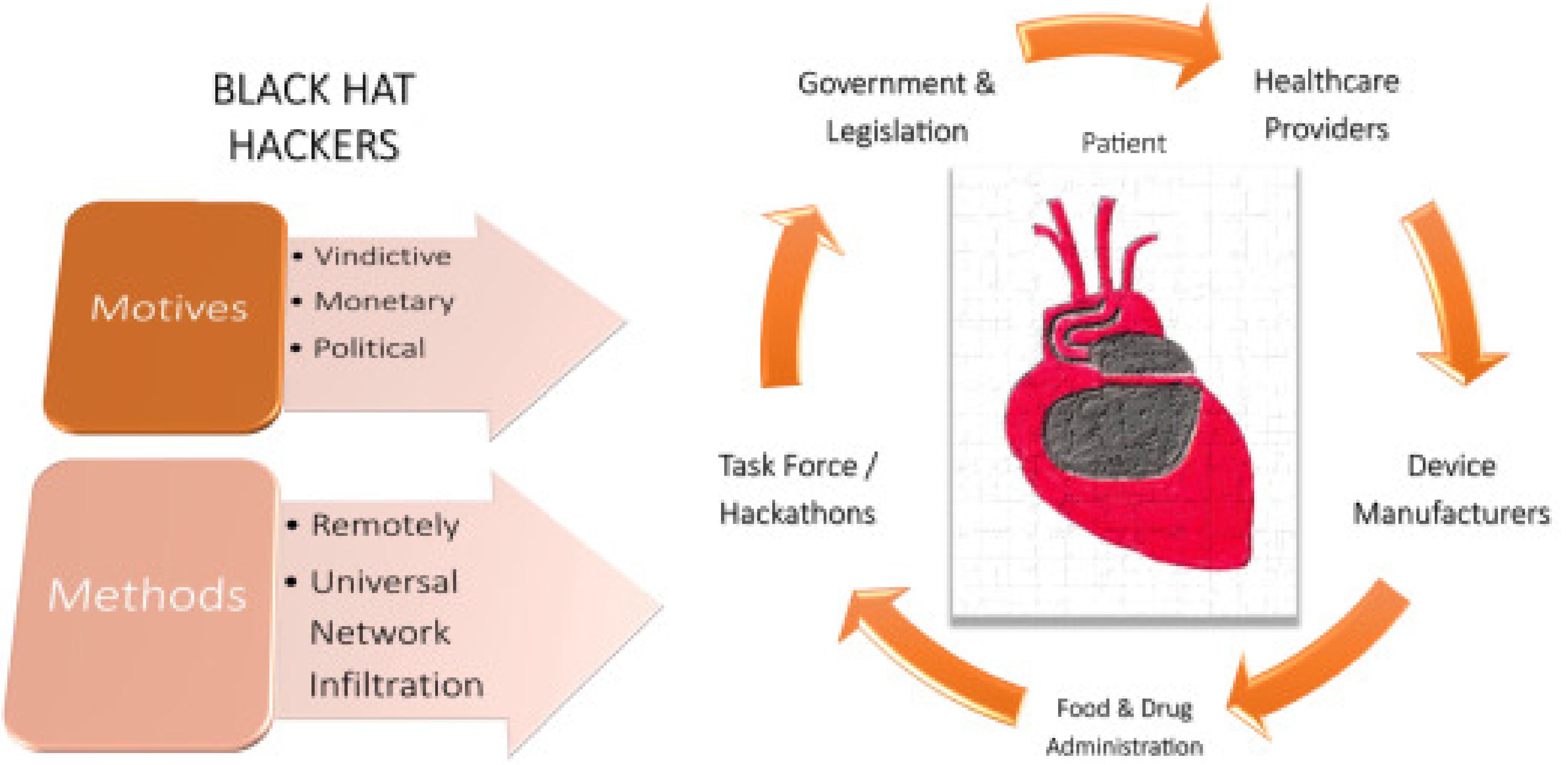
Cybersecurity vulnerabilities of cardiac implantable electronic devices: Communication strategies for clinicians—Proceedings of the Heart Rhythm Society's Leadership Summit

David J. Slotwiner, MD, FHRS,[*,†] Thomas F. Deering, MD, FHRS, CCDS,[‡] Kevin Fu, PhD,[§] Andrea M. Russo, MD, FHRS,[¶] Mary N. Walsh, MD, FACC,[||] George F. Van Hare, MD, FHRS, CCDS, CEPS-PC[**]

From the [*]New York-Presbyterian Queens, New York, New York, [†]Cardiology Division, Weill Cornell Medical College, New York, New York, [‡]Arrhythmia Center, Piedmont Heart Institute, Atlanta, Georgia, [§]College of Engineering, University of Michigan, Ann Arbor, Michigan, [¶]Cooper Medical School of Rowan University, Camden, New Jersey, [||]St. Vincent Heart Center, Indianapolis, Indiana, and [**]Division of Pediatric Cardiology, Washington University in St. Louis School of Medicine, St. Louis, Missouri.

Heart Rhythm, Vol 15, No 7, July 2018

CYBERSECURITY THREATS AND COUNTERMEASURES



The primary goal is to educate health care providers about the risks and new initiatives by stakeholders to incorporate cybersecurity considerations into early stages of product design as well as about the infrastructure in place to evaluate and mitigate specific vulnerabilities when they arise.

Health care professionals for cyber security

- Potential consequences if the vulnerability is exploited,
- Strategies to mitigate their vulnerability,
- Risks associated with a CIED software/firmware update
- Technical feasibility of exploiting the vulnerability,
- Long-term solutions to eliminate the vulnerability,
- Benefits of continued device therapy vs risk of vulnerability.

Conclusion

- Cybersecurity is the responsibility of all stakeholders and will require increased collaboration, communication, and education across the community.
  - *device manufacturers*
  - *regulatory government*
  - professional organizations
  - physicians
  - information technology (IT)
  - security experts
  - patients (including advocacy groups)

- It is necessary to improve safety and security for healthcare system, patients and CIEDs, as cyber threats are expected to increase in the future

Thank you for your attention!