Modeling Tradeoffs of Security Risks in Telemetric Cardiac Pacemakers

Aparna Ananthasubramaniam

aparna-ananth.github.io

@AparnaAnanth729

akananth@umich.edu

Wireless Pacemakers Have Security Vulnerabilities

mobihealthnews

TOPICS MENU

Asia Pacific | Europe/UK | Global Edition

St. Jude adds wireless upload to Merlin@home

By **Brian Dolan** | May 10, 2010 | 05:48 am

SHARE Share 23

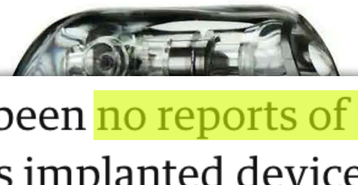
According to the company, the remote monitoring capabilities facilitated by the **Merlin@home** transmi permit automated follow-up appointments and daily checks to occur wirelessly, with limited patient actio required. This reduces unnecessary visits to the phys office, while allowing physicians to more quickly bec aware of changes with the patient's condition or dev

Hacking risk leads to recall of 500,000 pacemakers due to patient death fears

FDA overseeing crucial firmware update in US to patch security holes and prevent hijacking of pacemakers implanted in half a million people

Alex Hern

@alexhern

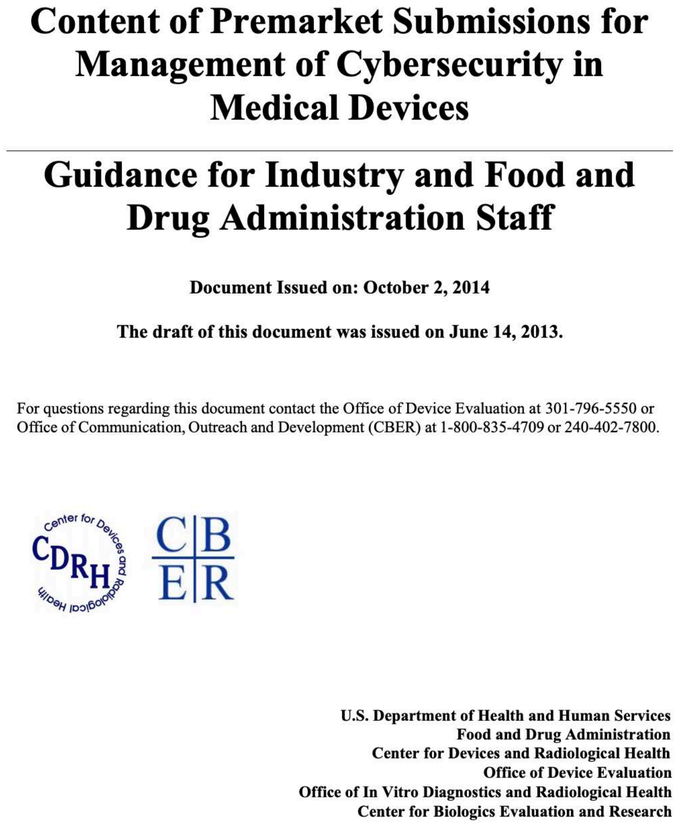


There have been no reports of unauthorised access to any patient's implanted device, according to Abbot. The FDA says that the vulnerability allows an unauthorised user to access a device using commercially available equipment and reprogram it. The hackers could then deliberately run the battery flat, or conduct "administration of inappropriate pacing". Both could, in the worst case, result in the death of an affected patient.

Current Quantitative Evaluations Do Not Weigh Security Risk

During pre-market approval, FDA requires device manufacturers to:

- Assess device cost-effectiveness without considering potential security breaches
- **List** security risks and plans to address them
- **Qualitatively assess** whether benefits outweigh security risks
- **Consider implementing** basic security measures (encryption, authentication, etc.)



Content of Premarket Submissions for Management of Cybersecurity in Medical Devices

Guidance for Industry and Food and Drug Administration Staff

Document Issued on: October 2, 2014

The draft of this document was issued on June 14, 2013.

For questions regarding this document contact the Office of Device Evaluation at 301-796-5550 or Office of Communication, Outreach and Development (CBER) at 1-800-835-4709 or 240-402-7800.

U.S. Department of Health and Human Services
Food and Drug Administration
Center for Devices and Radiological Health
Office of Device Evaluation
Office of In Vitro Diagnostics and Radiological Health
Center for Biologics Evaluation and Research

Our Research in Progress

What is the impact

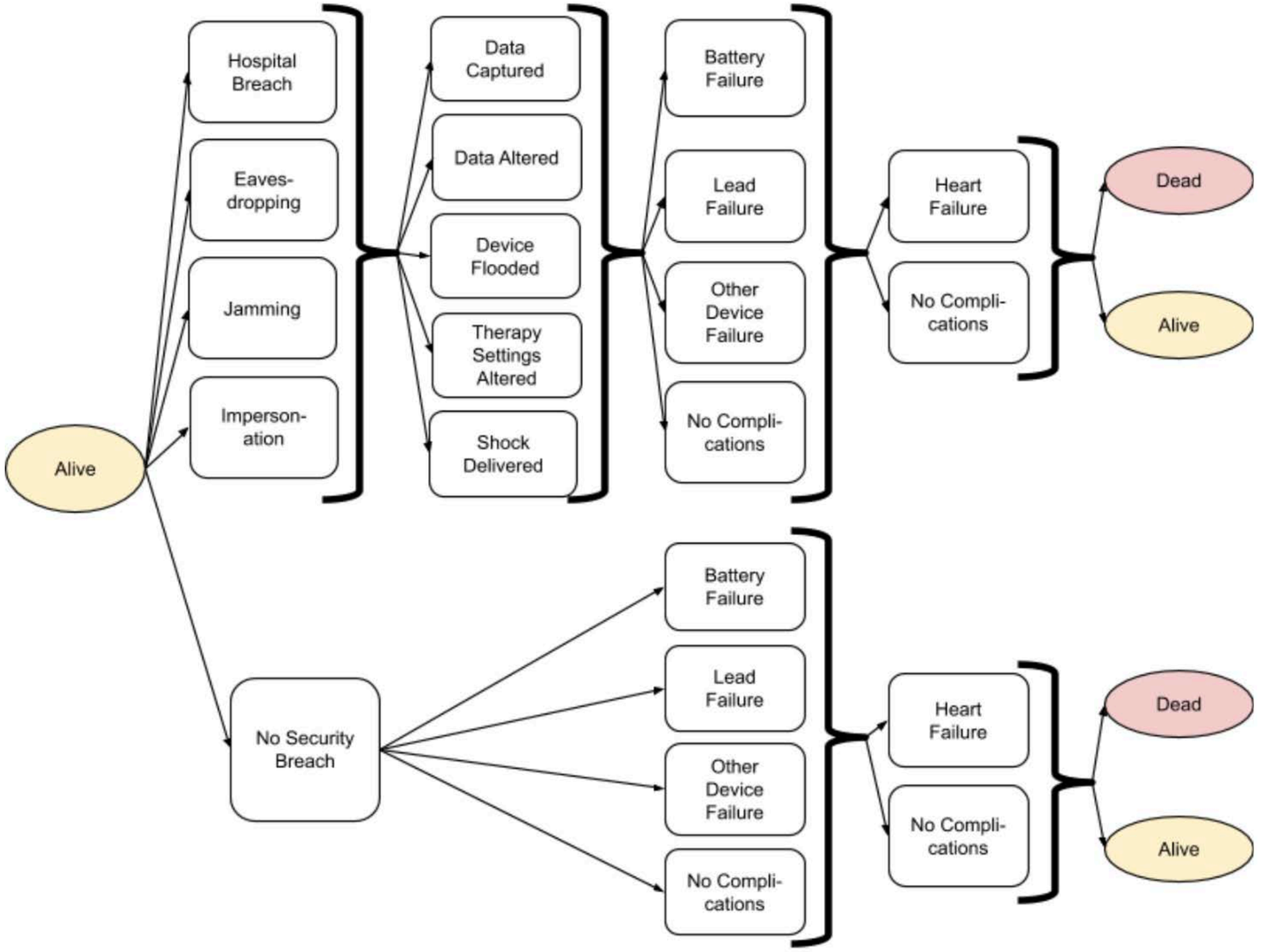
- of security risks to **patient outcomes** and **costs** of pacemakers?
- of various **proposed solutions**?
- to **each major stakeholder**: patients, payer, device manufacturer, hospitals?

Markov Model State Diagram

100,000 patients

5 years, 1 month intervals

1000 runs of the model



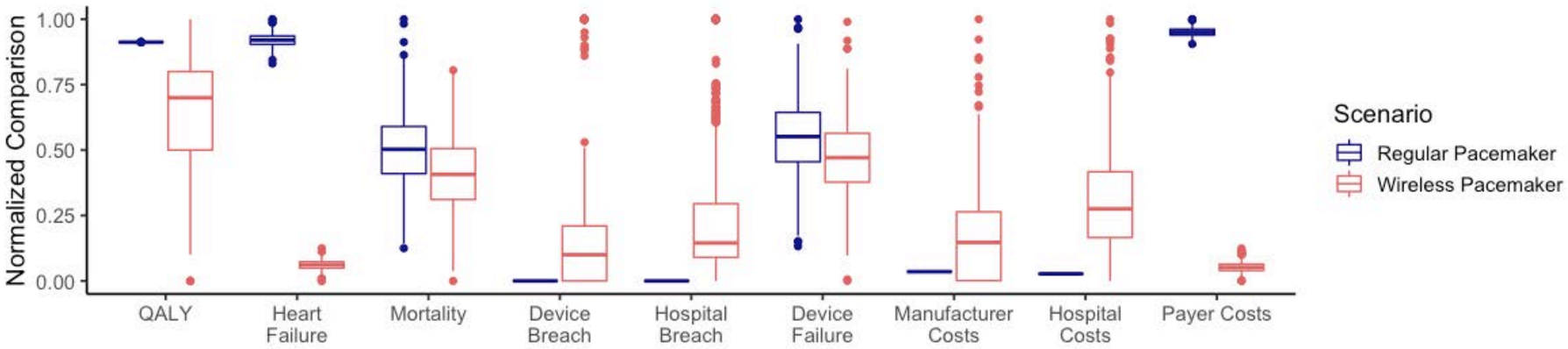
Assess the Benefits and Costs to Each Key Stakeholder

	Payer	Device Manufacturer	Hospital	Patient
Baseline	Device + Installation Monthly Maintenance Cost of Heart Failure Cost of Device Repair	-	-	Quality-Adjusted Life Years (QALY) Monthly Costs
Benefit of Wireless Pacemaker	Decrease in above	Profit (fixed)	Profit (fixed)	QALY Lower Costs and Time Spent
Costs of Security Breach	Increase in above	Customer Churn Company Valuation Legal Regulatory Staff and System Time	Customer Churn Company Valuation Legal Regulatory Staff and System Time	Pain and Suffering QALY
Risk Preference	Neutral	Established: Averse Start-Up: Highly Tolerant	Averse	Highly Averse

Quantitative Evaluation of Security Risks is a Valuable Assessment Tool

- Security events are **rare** …
  - Under 1% active attacks
  - Under 10% passive attacks
- … but **costly**
  - Worse patient outcomes
  - Loss of profit or cost-effectiveness

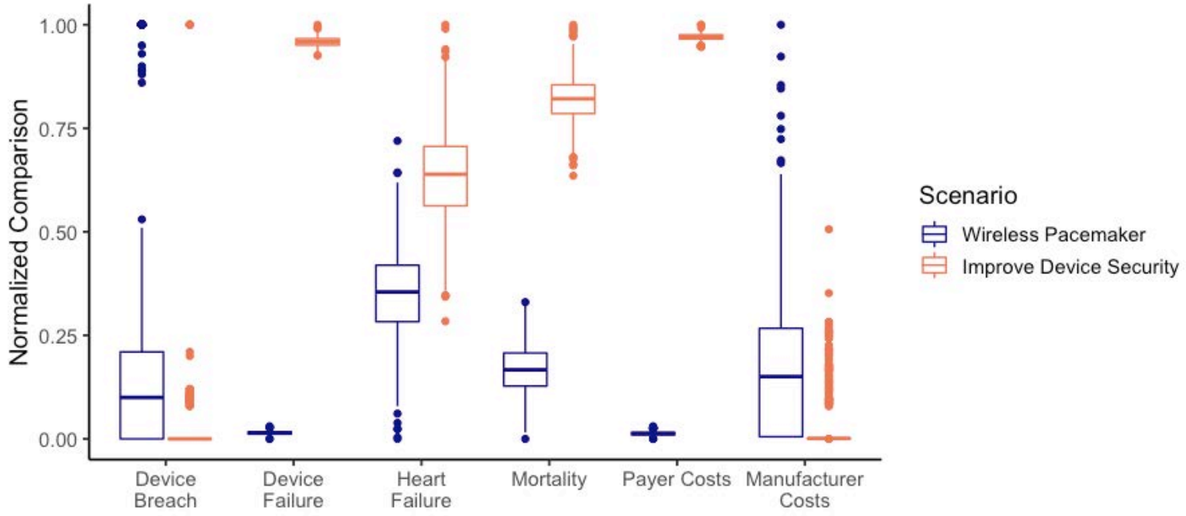
- Stakeholders affected most have:
  - High **risk aversion** (patients)
  - High **fixed costs** (hospitals, manufacturers)
- Explains "wait and see" approach
- Market for these devices persists: payers + risk-tolerant start-ups



Endpoint Security (FDA Recommendation) is Unacceptable or Infeasible

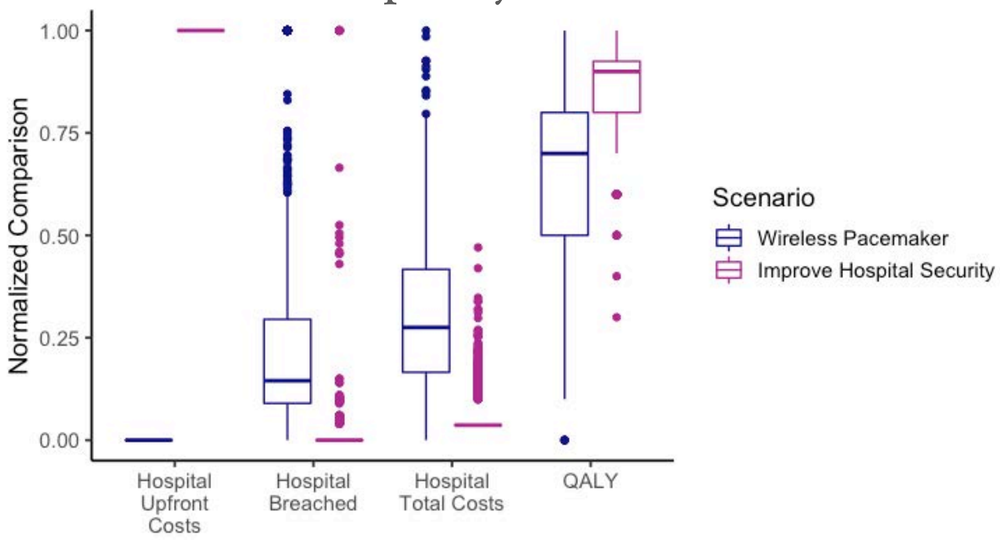
Improvements to Device Security

- Medically unacceptable tradeoff: fewer breaches but high rates of malfunction
- 3% increase in heart failure and 8% increase in deaths
- Cost increasing for payers, cost-saving for manufacturer



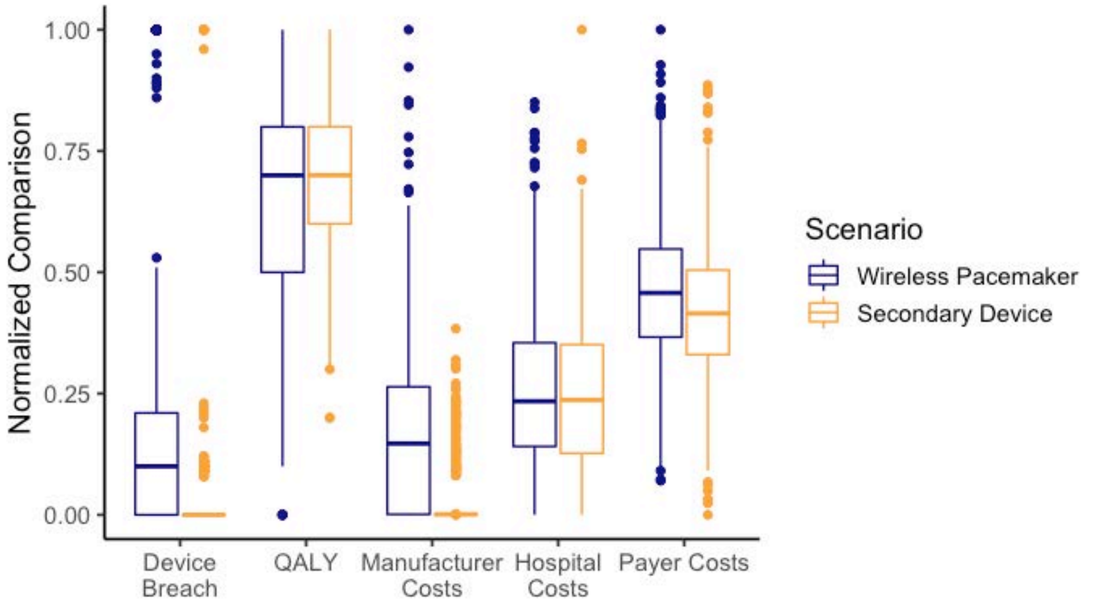
Improvements to Hospital Security

- $325K upfront costs (Smith 2017)
- 10x reduction in hospital breaches
- 10x reduction in cost for hospitals
- Problems: hard to enforce, lack of technical capacity



Other Solutions May Have Promise but Require More Resources

- **Secondary device** (“authenticator”)
  - 10x reduction in device breaches
  - Low fixed, unchanged overall costs for payer
  - Problems:
    - In early stages of development
    - Hard to use if unfamiliar with technology



- Increase patient **preparedness, awareness**, etc. for security breaches
  - Relatively small impact on cost and benefit

Takeaways

- Telemetric pacemakers have benefits but also introduce **security risks**
- **Quantitative evaluation** of costs and benefits indicates most stakeholders experience reduction of benefit and increase in costs; profitable for payers
- Improving device or hospital endpoint security (FDA recommendation) **worsens patient outcomes** or is infeasible to implement

Aparna Ananthasubramaniam
aparna-ananth.github.io
@AparnaAnanth729
akananth@umich.edu