Modeling Tradeoffs of Security Risks in Telemetric Cardiac Pacemakers (work in progress)

Aparna Ananthasubramaniam, akananth@umich.edu, School of Information, University of Michigan

Background

Wireless implantable medical devices improve cost-effectiveness:

- Improves patient outcomes via real-time monitoring, facilitating early detection of potential cardiac events and device failure (Nichol et. al. 2004)
- Reduces time and money spent on doctor's appointments (patients, payers)
- Makes more efficient use of doctor's time (hospitals)

But they also introduce major, costly security risks

- Many unsecure points of failure, including the device, hospital systems, and wireless communication networks (Ankarali et al. 2015)
- Breaches are costly to patients (Burri and Senouf 2009, Singh 2009, Zoler 2005), manufacturers, and hospitals (Ponemon Institute 2019)

Qualitative assessments are used to evaluate security risks:

- Most cost-effectiveness assessments (including FDA's pre-market approval process) do not include the risks and costs of security breaches.
- Solutions (including FDA suggestions) are often general-purpose recommendations, not evaluated for their own tradeoffs

Our work: use Markov models to quantitatively evaluate the impact of security risks and proposed solutions to various stakeholders

Findings

Security events are rare but costly

- Only payers profit from wireless pacemakers over regular pacemakers
- Reduce patient benefit, increase costs for manufacturers and hospitals

"Wait and see" approach is (sadly) prudent for payer and manufacturer

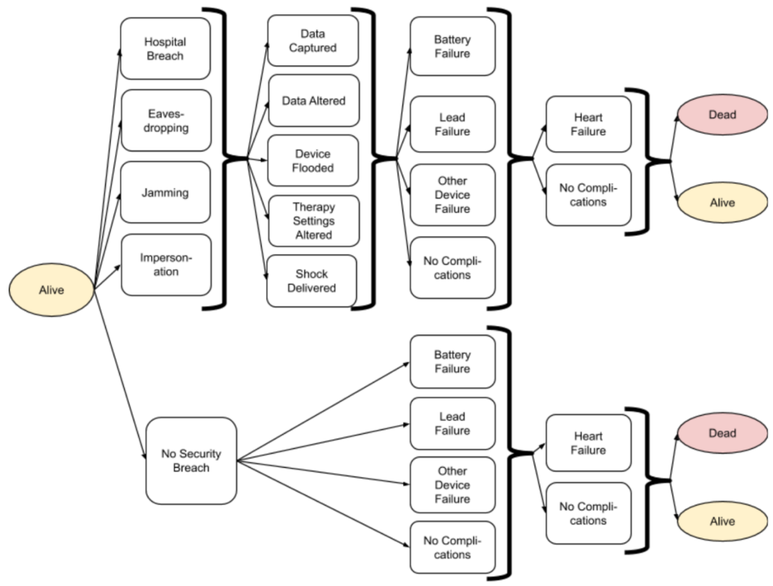
- Near-term benefit: before security event, better outcomes and lower costs
- Stakeholder impact is sensitive to risk aversion and fixed costs, both of which go down over time as people become inured to security risks
- Even with a security event, there is a market for these devices: risk-tolerant start-ups build, risk-neutral payers pay

Solving this problem requires innovative technology (not general-purpose security measures) and more attention to security risk

- Improvements to device security result in fewer breaches but cause high rates of malfunction, worsen patient outcomes, and increase cost to payers
- Improvements to hospital security reduce breaches, but requires action by many hospitals, who often lack the technical capacity
- Advocacy and educational efforts have limited impact on cost or benefits
- New technology, like adding a secondary "authenticator and encryptor" device, could reduce breaches and be feasible

Methods

Markov Model State Diagram

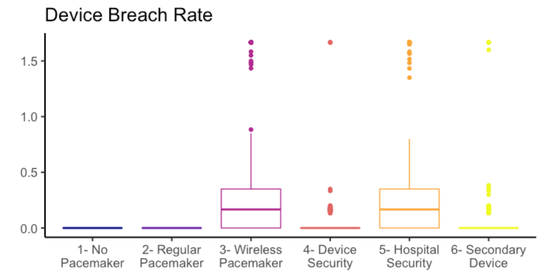


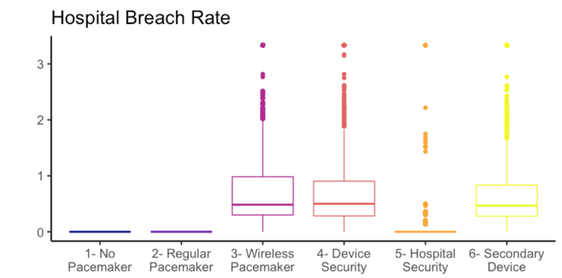
Stakeholder Costs and Benefits

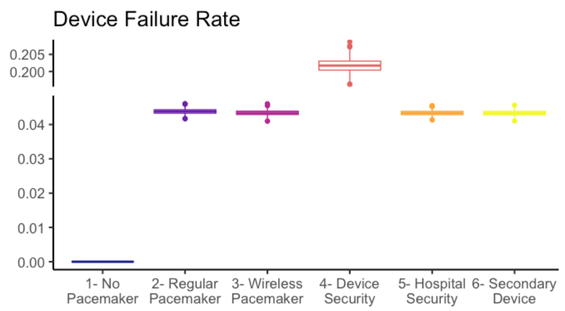
	Payer	Device Manufacturer	Hospital	Patient
Baseline	Device + Installation Monthly Maintenance Cost of Heart Failure Cost of Device Repair	-	-	Quality-Adjusted Life Years (QALY) Monthly Costs
Benefit of Wireless Pacemaker	Decrease in above	Profit (fixed)	Profit (fixed)	QALY Lower Costs and Time Spent
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

Results

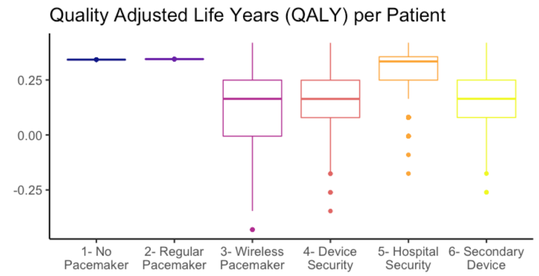
Security Events and Device Failures

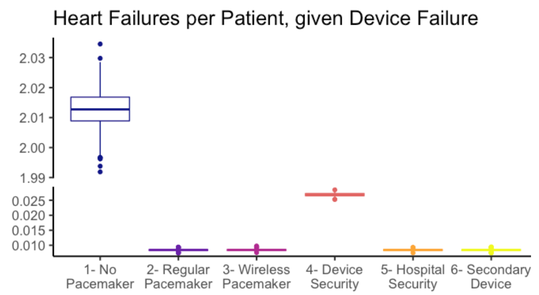


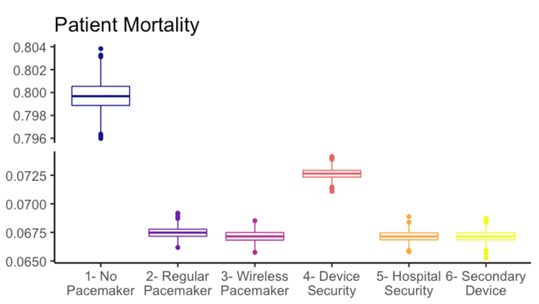




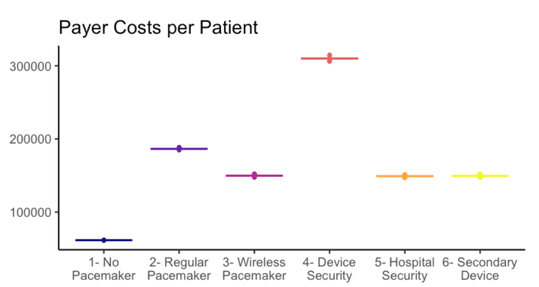
Patient Outcomes

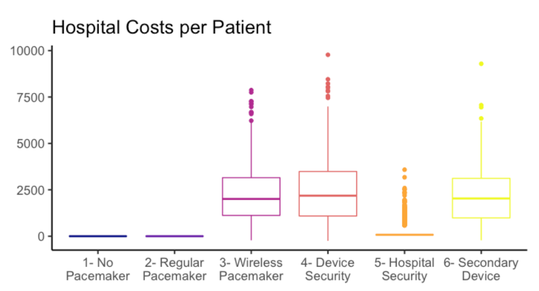


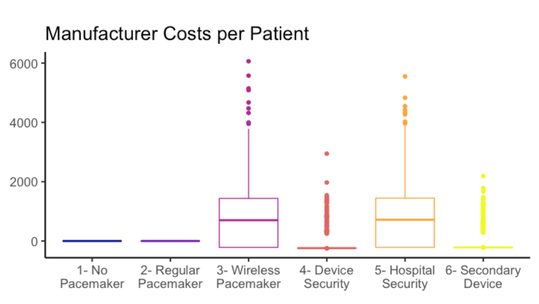




Stakeholder Costs







Scenarios

1- No Pacemaker

Cardiac patient without pacemaker. Used as a comparison for cost benefit analysis.

2- Regular Pacemaker

Pacemaker without telemetric capabilities. No security risks, but no benefits. Used as a comparison for cost benefit analysis.

3- Wireless Pacemaker

Pacemaker has telemetric capabilities, which reduces costs and improves patient outcomes, but also introduces risks of breaches at device and hospital endpoints.

4- Device Security

Wireless pacemaker has been outfitted with several security enhancements -- including stronger authentication and encryption -- and receives regular upgrades to patch security weaknesses. This leads to lower security risk but higher risk of device failure and heart failure mortality. (Camara et. al. 2015)

5- Hospital Security

Hospital takes measures to improve the security of its systems -- including staff training and system upgrades. This leads to lower security risk without compromising outcomes, but has higher fixed cost to the hospital. (Online Trust Alliance 2015)

6- Secondary Device

Wireless pacemaker goes through a secondary device (e.g., patient's cell phone) to authenticate the programmer and encrypt data. This leads to lower security risk without compromising outcomes, but has higher cost to the payer. (Wu et. al. 2015)