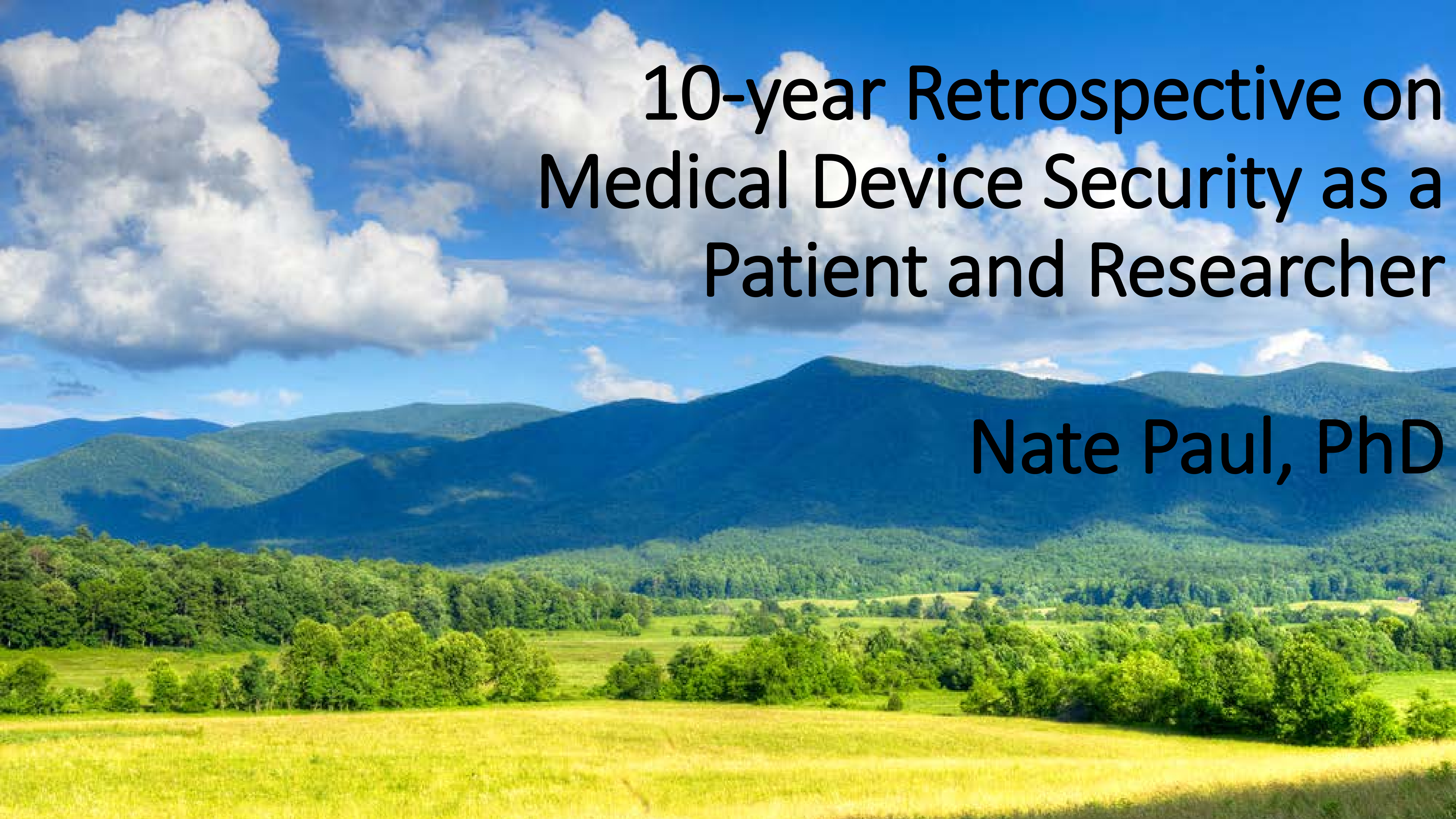


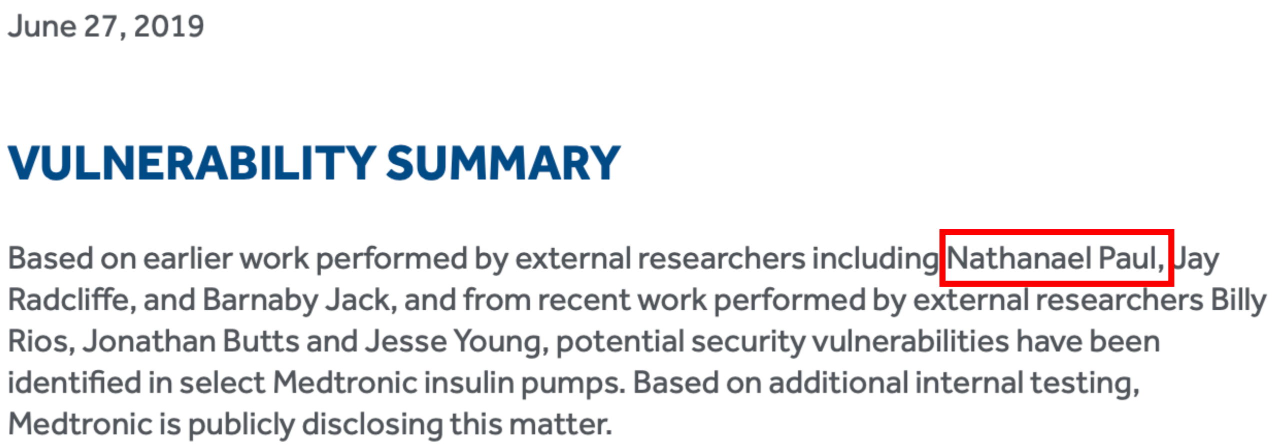
10-year Retrospective on Medical Device Security as a Patient and Researcher

Nate Paul, PhD

My Remarks/Opinions Are My Own

- **All remarks/opinions are my own** and in no way reflect on any private sector medical device company
  - Not the opinion of Medtronic, Abbott, Dexcom, Insulet, Tandem, or any other company
  - Today, in this talk, I'm just a patient/researcher

Affiliation



June 27, 2019

VULNERABILITY SUMMARY

Based on earlier work performed by external researchers including Nathanael Paul, Jay Radcliffe, and Barnaby Jack, and from recent work performed by external researchers Billy Rios, Jonathan Butts and Jesse Young, potential security vulnerabilities have been identified in select Medtronic insulin pumps. Based on additional internal testing, Medtronic is publicly disclosing this matter.

- Who am I
  - Patient with Type 1
  - (Previous) Researcher with a focus on malware detection and system security
  - First reported on pump security issues to FDA almost 10 years ago
  - Still use a “vulnerable” Medtronic pump in a DIY system
- Adjunct prof at Univ. of Tenn.
- New (this year): Am responsible for all non-IT security for private sector medical device manufacturer

DIY Quality of Life: 2017

Recommended Next Steps/Requests (1 of 2)

- **Don't:** Shut down DIY community
  - Recalls work to shutdown DIY community and don’t really address security risk
  - Patients may use less safe hacks that may increase probability of negative safety incident (analog hole)
  - Reduces patients' abilities to have needed care
  - Chilling effect on future innovations
- **Do**: Work with DIY community
  - Allow manufacturers to support DIYers through different process than we have now
  - Allow Medtronic to redistribute received Paradigm pumps
- **Don't**: Force certain policy enforcement regarding manufacturers and key management
  - Don’t interfere with enforcement policies on key usage
- **Do:** Work with manufacturers to help with security
  - Some manufacturers are less ready to absorb work to do security mitigations
  - Accept but not mitigate risk

Recommended Next Steps/Requests (2 of 2)

- Two types of attackers in our model – let's fight the right battle
- Hackers are financially motivated and may inflate risk
  - Address this through panel of experts to assess risk in reported vulnerabiliteis
- Risk change with hybrid-closed loop systems
  - We can account for that
- Thank you for the work that you do!

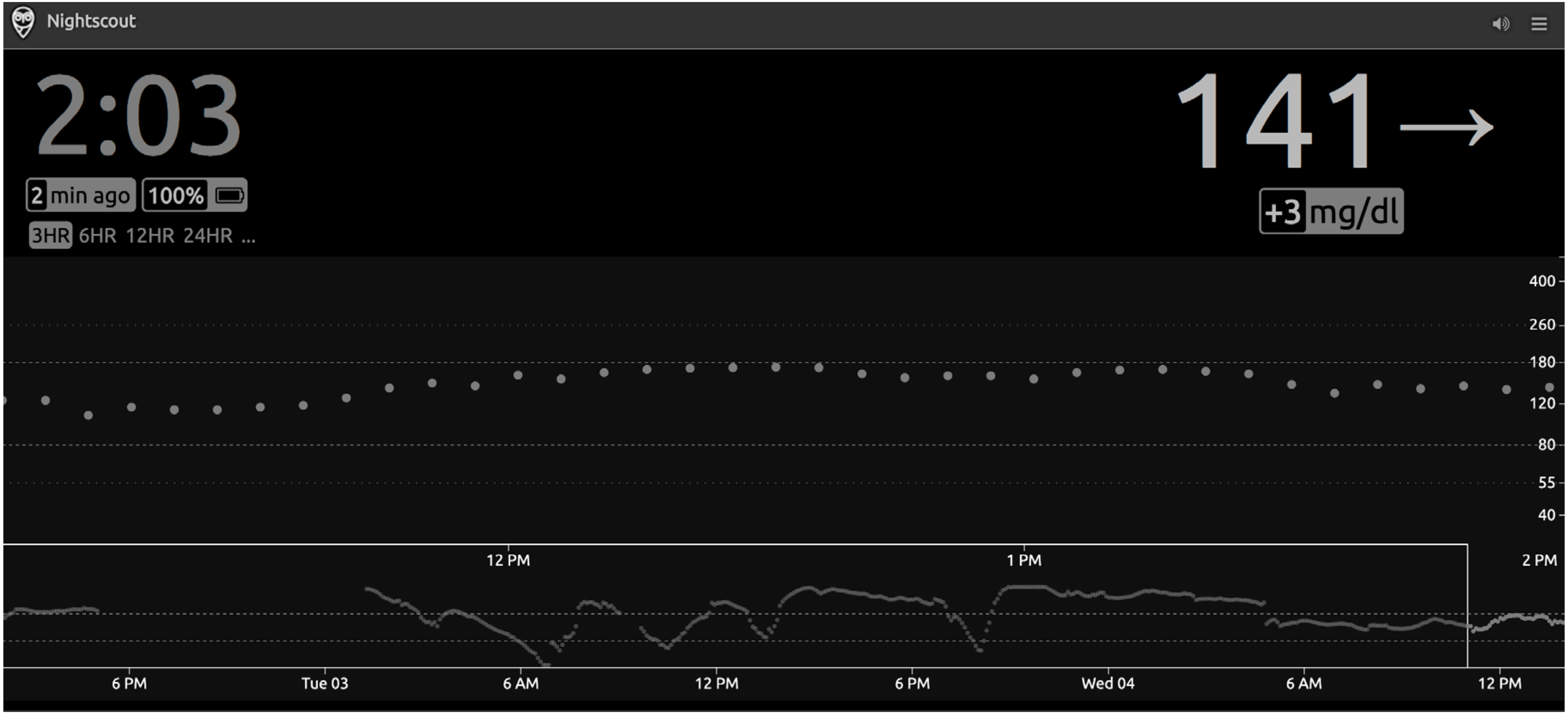
Questions

pauln@utk.edu

Digital Rights Management

- Change: manufacturer now creates software/hardware for insulin delivery
  - Digital rights management around blood glucose data (DRM decades-old issue)
- Medical devices *still* challenged by design
  - Used to be constrained by manufacturer releasing blood glucose values in tables in PDF docs – let's not return to that!
  - Patients should be able to access and control their data as they see fit
  - Biggest threat to DIY glycemic control is the removal of previously-obtainable “vulnerable” pumps
- Bottom line: Give acceptable commercial solution and/or data to allow patients to get an acceptable treatment (#weAre**<u>Still</u>**Waiting)

Last Year: How to Attack OpenAPS Patient Population (Unpublished self-study of external attack)



Nightscout
2:03
2 min ago
100%
3HR 6HR 12HR 24HR ...
141→
+3 mg/dl
400
260
180
120
80
55
40
12 PM
1 PM
2 PM
6 PM
Tue 03
6 AM
12 PM
6 PM
Wed 04
6 AM
12 PM