A security researcher, a safety engineer, and a regulator walk into a bar: Lessons learned from 9 months of institutional anthropology at the FDA

Dr. Eugene Vasserman, Kansas State University

Speaking Points (1)

Disclaimer: Not speaking for the FDA, nor disclosing any material covered by NDAs

- Why medical CPS?
  - "The hardest" :)
  - Diverse multi-stakeholder
  - Extreme resource constraints, long lifetime of devices
- Why FDA?
  - Safety "vs." security: should be both, right?

Speaking Points (2)

- "Why is 'no one' adopting our solutions?"
  - Manufacturer statistics from Junod [1]
  - Manufacturers do not always have resources to hire security people (but they *MUST* have safety people)
  - Is security AUTOMATICALLY addressed in safety analyses (e.g. FMEA, STPA)? **In theory.** Probably not in practice.
  - "Can your device do X?" … "Can it be *MADE* to do X?"
    - "Reasonably foreseeable misuse" (from regulations)
  - "Hasn't been a problem." Could such problems be detected if they occurred? Perhaps they already have.
  - Potential patient safety hazards *from* security solutions

Speaking Points (3)

- "Why is 'no one' patching?"
  - MYTH: Every patch must be FDA-reviewed (Otherwise, every Patch Tuesday would be nightmare at FDA!)
  - Manufacturers do not always have time to test third-party patches
  - Facility statistics from AHA [2] and CDC [3] (We got very lucky with WannaCry :)
  - Operators (not regulated by FDA) are responsible for secure *deployment*
  - Conflicting requirements of operators: IT "vs." biomedical engineering

- Standards and requirements:
  - "…and nothing else" is not satisfiable

References

1. S. Junod. “Commemorating the 40th anniversary of the 1976 medical device amendments.” Food Drug Law Journal, 72(1):26—31, 2017.
   - US: 8,995 medical device manufacturers (18,716 worldwide total)
   - Marketing >175,000 different devices
   - 75% have fewer than 10 employees
   - Only 3.7% have more than 100 employees
2. http://www.aha.org/research/reports/tw/chartbook/ch2.shtml Latest report from 2016, based on 2014 survey data.
   - TrendWatch Chartbook analyzes the latest in hospital and health system trends. Produced by the AHA and Avalere. Charts from Chapter 2.
3. https://www.cdc.gov/nchs/data/hus/2015/089.pdf Latest report from 2015, but reporting 2013 data sourced from the American Hospital Association (AHA) Annual Survey of Hospitals: “Hospital Statistics”, 1976, 1981, 1991–92, 2002, 2012, 2014, and 2015 editions.
   - Hospitals, beds, and occupancy rates, by type of ownership
     - Table 89. Hospitals, beds, and occupancy rates, by type of ownership and size of hospital: United States, selected years 1975–2013
     - US: 5,686 hospitals (with 914,513 beds)
     - So, average of 161 beds per hospital
     - 46% of hospitals have 100 beds of fewer (For some reason the total percentage of beds is 87.5%.)