Breakout Session 1: How Health IT Disrupts Traditional Security Engineering, and What To Do About It

Moderated by Sean Smith, Professor of Computer Science, Dartmouth

Attendees

- Ann Flood, Dartmouth College
- Kelly Caine, Indiana University
- Khaled El Emam, Children's Hospital of Eastern Ontario Research Institute
- Mark Frisse, Vanderbilt University
- Ross Koppel, University of Pennsylvania
- Jesse Walker, Intel Labs
- Laurie Williams, North Carolina State University
- Alec Wolman, Microsoft Research
- Kai Zheng, University of Michigan

Discussion

Sean Smith began by asking why security is so hard in this space. He's done some automatic redaction work, but was not allowed to reveal screenshots used in the project (standard EMR NDAs consider such UI details as "proprietary"). He was studying access control in a large hospital, and wanted to study circumvention, but the IRB said that it could get subjects in trouble. Standard EMR NDAs also prevent clinicians from on-the-record discussion of flaws in EMR software.

Jesse Walker said that those in the industry have a vested interest in limiting the amount of embarrassing publicity. Mark Frisse talked about how the industry is warped because you do not pay for what you get. It promotes the exclusion of the least healthy patients from the system. The system encourages complexity and computers make it possible to implement this complexity. Kelly Caine remarked that patients simultaneously want to keep their health information private, but need to reveal it to get healthcare providers. Laurie Williams stated that while software engineers have difficulty implementing functional requirements already, there's more difficulty in implementing legal requirements, which they aren't trained to do. Ross Koppel mentioned there are two problems to address: security, which is preventing people from gaining access to information they should not have, and access, which is absolutely critical to the healthcare industry. The janitor shouldn't see the data, but which nurse shouldn't? It's really a different model than people are used to in terms of access to data.

Kai Zheng said healthcare is an exception-driven business. When information systems and security policies are being designed, normal cases are defined, but there are always issues with the remaining exceptions; healthcare has too many exceptions, which lead to workarounds. How can these be anticipated? Ross Koppel commented that there's
more ambiguity and unknowns in medicine than any other field. Mark Frisse remarked that we inherit a lot of terminology from a flawed economic infrastructure that describes transactions, not people. Ross Koppel said that a lack of data standards and interoperability makes it difficult to track a patient's health after he or she has left the clinic.

Jesse Walker wondered what obstacles prevent the medical community from coming together and defining standards. Kelly Caine said since patient health data is extremely valuable, there's disincentive for vendors to share information. Ross Koppel said vendors wanted to deploy first and link everyone together afterwards. There are no data standards as to how data is portrayed in EHRs and no incentive to share data. Khaled El Emam said we have the same problems even in other systems. Getting people to communicate with each other is a big struggle in data sharing. Mark Frisse reiterated that EHR systems are designed to facilitate economic transactions.

Sean Smith wondered what drives standardization. He asked if we could use previous standards evolution as a model. Ross Koppel said absolutely and mentioned a few examples including the standardization of clocks, railroads, driving on the right side of the road, and screws, which helped drive Industrial Revolutions. Successful standardizations can be handed down from government but vendors don't want EHR systems to be standardized. If standardization occurred, many vendors would disappear, risking data loss. Alec Wolman pointed to the Internet. There are lots of standards but vendors still try to build their own premium experiences (e.g., app stores). Mark Frisse said that the agents that have the most access to data are health plans and they do not serve in the patient's best interest. Why would they help competitors?

Sean Smith asked if a single data standard would solve everything. Mark Frisse said no—we need to post the real prices. Until that happens, we'll be reacting to an over-priced, overly engineered system. Kai Zheng remarked that there's been discussion about standardization, but what about free text? There are clinicians who use free text only and choose random data to put into structured data fields. Many times, people can't find what they are looking for in predefined list. Ross Koppel noted that clinicians deal with ambiguity for a living. How can the structure of the software deal with that? Patients lie systematically, intentionally or otherwise. What is the most common allergy listing in EHRs? "Other." Kelly Caine remarked that these are human factors problems. Khaled El Emam said never have compulsory data entry. Any kind of enforcement fails miserably.

Sean Smith said we heard from large EMR customers (off-the-record) who say that they ended up sending inexperienced team members to talk to vendors during customization—because the experienced members were too busy. How do other systems deal with these errors? Kelly Caine said airlines deal with errors in a very reasonable way by bringing in human factors experts who blame the system design rather than the user. This could be a good model for HIT. Ross Koppel spoke of a doctor who learned EHRs from three different hospitals. Kelly Caine said that if we designed
these systems well, they would be more usable. She added that patients don't understand why when they visit a clinic they are just there to provide the physician with data.

Ross Koppel elaborated on some concerns: suppose a patient has a list of drugs they come in with, which needs to be reconciled with information from the patient's physician(s), the hospital, etc. Before discharge you want everything to match up. It's terribly complex.

Mark Frisse explained that physicians are working to make their time reimbursable. Kai Zheng said vendors have people talking to physicians. Why are the systems they design so far from the reality? When you ask physicians what they want, they describe textbook workflow. But what they do may be very different. Mark Frisse said flexibility should be built into the system.

Ann Flood remarked on why things are being recorded at all. For retrieval, yes, but also for billing and legal compliance. Mark Frisse said we have to fill everything in on the charts because it's expected of us. Meaningful use ensures that we have more implementations, but not good implementations. Ross Koppel remarked that we wanted to get into digital healthcare in the worst way possible and we've succeeded.