Panel 3: Mobile Health (mHealth)

Chaired by David Kotz, Champion International Professor of Computer Science, Dartmouth
Panelists: Tanzeem Choudhury, Cornell University; Alec Wolman, Microsoft Research; Lisa Marsch, Dartmouth Psychiatric Research Center; Kevin Fu, University of Massachusetts Amherst

Summary of the Panelists’ Presentations and Panel Discussion

The mHealth panel was about mobile technology (outside clinical settings) used by patients. Professor David Kotz [Dartmouth] introduced the topic and moderated the discussion.

Today, we increasingly see people using mobile technologies for personal wellness; e.g., to improve fitness, change behavior (to quit smoking or exercise more), or improve lifestyle habits (to understand and improve sleep). Some clinicians prescribe certain medical devices to patients (e.g., pulse oximeter, blood pressure monitor) to remotely monitor their patient's health. Smart phones - a functional and capable computing device - are becoming common in day-to-day life. Taken together, Kotz defined mHealth to be the use of mobile computing and communication devices for the delivery of health care or the collection of health information.

There are some aspects of mHealth that make it different from other types of industry. Security problems with mHealth devices have a personal and immediate impact on the patient. Medical data is sensitive in nature, and the amount of data being collected is huge, rich, and diverse. Indeed, one may be able to infer private information about a person’s lifestyle, location, or social interactions, from the data collected by his or her mHealth devices. A person won’t necessarily want to share this data with his doctor because of obvious privacy reasons.

Brief presentations by panelists:

Alec Wolman [Microsoft Research]

Smart phones will play a major role in healthcare. Companies are making medical devices and apps around smartphones (e.g., iBGStar, a FDA-approve blood glucose monitoring app for the iPhone). But at the same time, malware in smartphones is becoming a rising concern. App store review process (e.g., Android App market) help filter out malicious apps, but they don’t solve the problem. This makes us wonder: how can we run health-critical apps on a such a general purpose smartphone which is vulnerable to malware. Alec Wolman's group is working on ways to leverage the trusted computing hardware for mobile platform, which can then help in ensuring integrity, authenticity of medical sensor data, and medical apps running on smartphones, and at the same time, provide some application specific transformations of sensor data that makes processing at the smartphone energy efficient.

Lisa Marsch [Center for Technology in Behavioral Health at Dartmouth]

Her team’s work is mostly focused on the people side rather than the technology side of mHealth. They work on issues around health monitoring, understanding risk and health behaviors, behavior change, prevention efforts, and treatment interventions. They have
primarily worked with under-served and vulnerable populations - veterans, substance users, mentally ill users. Due to the nature of the subjects and data/habits that are monitored, privacy is important. Her team has been focused on behavioral health and science of behavior change and how people are affected by chronic illnesses. People often make decisions based on perceived benefits vs. security and privacy risks, and with change in technology perception changes, so privacy considerations vary with technology. There are also research opportunities on cost-benefit analysis, e.g., developing models of risk and rewards. She also talked about the importance of usability (she gave the example of a psychotic patient who might have to learn how to use a new device). She also mentioned liability issues that might come up when a doctor has access to personal information entered by the patient in their health record.

Tanzeem Choudhury [Cornell University]

Her research interest is in using the smartphone (and its sensors) to gather data about individuals, and to share it with them in a way that will help improve their quality of life. In one of the projects, her group uses voice patterns captured from the microphone from people's phones to determine when they are talking, how often they are talking, and maybe with whom. Through a deployment at a local retirement community, her group has shown that face-to-face interactions can be used to assess mental well-being. The ultimate goal is to be able to use this technology to manage and improve mental health. In another project, StressSense, they tried to predict an individual's stress level with the goal of chronic stress monitoring. BeWell is a behavior change app to be released on Android App market. This app has a live wallpaper, which gives feedback to the user based on how social and active he has been. In BeWell, physical activity, sleep, and social activity are inferred using sensors on the smartphone.

Kevin Fu [University of Massachusetts Amherst]

Wireless makes devices more appealing and convenient to use, but it also increases the security and privacy risks. His group contributed to security analysis of wireless Implantable Medical Devices (IMDs), and they discovered vulnerabilities where an attacker can cause the IMD to give a shock to the patient; these vulnerabilities were primarily because the debug mode was left on in the IMD. Similarly, another researcher discovered vulnerability in insulin pumps, also due to functional debug interface on an insulin pump sold to patients. Medical devices should be trustworthy, and their improved security will enable medical device innovation.
Q & A:

Rich asked how credentials could be stored in a mobile phone, whether medical information would be stored similar to credit card information. Alec Wolman said we need a secure element inside the phone. By having a secure element as peripheral (e.g., NFC), we secure the peripheral but the I/O in mobile is left untrusted.

Joe Hall asked Kevin Fu if he could elaborate on his statement 'wireless takes away social norm that keeps people good'. Kevin Fu said the more you take away the requirement of physical presence, people are less afraid of consequences, because they don't have to face them. Eric Johnson thought it could also be the case that the separation of actions and the requirement of physical presences does not take away social norms, but it enables the people, who wouldn't adhere to social norms, to take those actions. Concluding the answer, Kevin Fu said safety is a major issue, and security is one part of it, the part that needs to be fixed.

Brad Malin asked what are the other types of medical devices we should be worried about, and what are the implications if the voice patterns end up in a widespread application. He also asked the panelists to comment on the future of mHealth and state of the field. Alec Wolman shared his concern that we might build and deploy applications without appropriate security in place, and it might result in a major mishap. Tanzeem Choudhury thinks that currently people share data on phones just for fun and to be social. There is always a trade-off between the value of sharing data, and the risks involved. Individuals can use their own mobile to collect data, and draw inferences locally (using apps), not share with anyone and still benefit from mHealth. But it is hard to imagine what exactly will happen, and how privacy will be handled. Lisa Marsch mentioned that funding organizations are focused on integrated healthcare systems (involving sensors and mHealth). This is especially true in low-economy countries, where cell phones are widespread, and can be used to prove low-cost healthcare solutions.

Jesse Walker asked how can we come up with better analytical techniques that are more tolerant to sensor data noise, because currently we don't have a good way to secure sensor hardware against tampering or prevent an adversary from tampering the environment. Tanzeem Choudhury thinks that the sensor data noise is not a distinct problem; for example, there is noise when you deal with image classification due to mislabels or other sources of noise, and analytical techniques have to deal with the noise.

Deven McGraw referred to cases where users disable security measures because they hinder their access to the device and the data in the device. She asked what policy or security mechanisms can be put in a mobile phone that the user will use and not disable them? Alec Wolman pointed out that corporations enforce you to setup security measures, and there is no way around it. Tanzeem Choudhury said in one of the studies she did with users, they looked into deploying usable security mechanisms. While doing so, one has to take into account the technology and the individual's cognitive ability as well. She agreed that it is challenging to find the right solution for each individual.

Lisa Marsch asked how much does the FDA regulate apps related to mHealth and their security. Deven McGraw said the FDA does not focus on wellness apps, but only on medical apps.
Denise Anthony said privacy preferences vary with individuals. So instead of saying these preferences vary and we don't know what to do, we should take that into account, and have a variety of settings such that different individuals can choose them as per their liking. We should bake preferences into the app (directing towards Tanzeem Choudhury) as the app is being made, right from scratch. Tanzeem Choudhury agreed with the idea. She thinks there is enormous need for bi-directional communication (between end-users and developers). Developers should come up with preferences as best they can, and end-users should give feedback, which the developers should use to iterate on the preferences. This iterative cycle should repeat until we get it right.

Ross Koppel asked what happens if devices run out of battery. Kevin Fu mentioned use and dependency on a battery is a design choice. There are some techniques that his group is working on, and one can use those techniques in some cases to get by without a battery, but otherwise energy is a big problem. Alec Wolman pointed out that battery is a resource, an important one, but it can be managed.

Merrill Warkentin wondered why password and other privacy settings couldn’t be implemented as a one-time change, but Denise responded that users might want to change privacy settings later if some adverse event occurred.