Dr. Andrés Molina-Markham introduced the topic of discussion by first highlighting the potential of mHealth in healthcare and then pointing to some challenges of securing mHealth devices and infrastructure.

According to Dr. Yih-Chun Hu, there are two types of adversaries in mHealth: “honest but curious,” someone who provides a service to users and has access to the data generated by the users; and “less honest, but equally curious,” someone who attempts to access data in transit or attacks systems of service providers to get access to data at rest. Dr. Hu said that we need to solve the access-control and authorization problem in healthcare, e.g., how should we decide who should have access to which device or what data? His group is working on the problem of securing a body-area network (BAN) by sharing a secret among the devices on the body. Their approach is to use the body as a communication channel.

Dr. Jaeyeon Jung presented privacy related challenges that mobile phone users and mobile app developers face. Currently, according to Dr. Jung, the burden of protecting user privacy is on the user. In her recent project, called Privacy Leaks, her group developed an app that helps users better understand what their mobile apps are sharing - with or without their knowledge. According to Dr. Jung, we need to reduce the gap between users' expectations and applications' actual data collection behavior. Her other project, PriScreen, attempts to do that by providing app developers with better privacy analysis tools.

Dr. Jacob Sorber pointed out that the consequences of a security or privacy leak in mHealth can be severe, and often the resources available for mHealth devices are limited. His mHealth research focus is on making safe, privacy-preserving, and efficient computing ecosystems. In his prior project, Plug-n-Trust, he developed a method to do secure computation and communication on an untrusted mobile phone. Currently, he is involved in designing and building a wearable device that is the security manager of a BAN, provides trusted I/O to the user, and acts as a glue for all the devices in a user's BAN.

An audience member asked a question about data ownership and who gets to decide who can see the data, suggesting that maybe patients should control access to their data, e.g., allowing access to only their doctors. Dr. Hu said it is not clear whether patients should control the data because in some cases patients do not have a choice about which doctor will treat them (e.g., in emergency units), and in some cases we do not want patients to read their records (e.g., their psychiatrist notes). Another audience member asked what we could do to help users choose better privacy settings. Dr. Jung said that the one approach usability researchers take is to avoid users having to make decisions for every setting, but instead choosing good defaults for them based on other similar users. Dr. Hu agreed that we need good default settings because many users are considered functionally illiterate.

An audience member expressed the difficulty of quantifying privacy leaks. Dr. Jung said there are two ways to look at it: first, app stores have specific rules regarding privacy while handling user data, and when an app violates those rules we say it leaked private information, and second, the meaning of privacy from the user's point of view is hard to define because different people have different expectations and different levels of understanding of the system or apps. Dr. Hu said we can go to an extreme and define any information theoretic leakage as a privacy leak, e.g., if you express an interest in medication it tells something about you. However, the problem with this definition is that it is too strict to work with and also users do not think like that. Dr. Sorber added that users’ privacy preferences change over time, so any system that we design should be flexible enough to handle changing preferences and should evolve accordingly. Dr. Hu agreed with an audience member's comment that people are only concerned about privacy when it gets violated, and he added that this is why we need laws and regulations for privacy. Dr. Jung, said that normal users do not understand inference attacks, and moreover, we cannot enumerate all the possible inference attacks - these attacks will get better with time. So the question for researchers is how can we arm the user to make better decisions when we do not know all the possible inference attacks.
In response to a question on how we can enforce the privacy policies on mobile apps, Dr. Jung said that her group has explored the possibility of extending their previous work on identifying leaks to achieve this. However, one challenge is that apps break or usability suffers when the programmer is not aware of the user’s privacy settings. She said a better solution is to add support in mobile platforms that offers users granular control and the flexibility to change access permissions for apps. However, she was skeptical that mobile platforms would do so because it would put a burden on app developers.