Cyber-Security, IoT, Wearables and the Quantified Self (QS)

Life Sciences Technical Community (LSTC) Mini-Symposium & Panel at IEEE EMBC 2016 and IEEE HealthCom 2016

By Nahum Gershon

IEEE is able to provide a wide diversity of expertise, information, and resources that are related to health and to the life sciences. This expertise, however, is often distributed across many organizations, thus posing challenges for integrating the expertise and collaboration among organizations. One of the important functions of the Life Sciences Technical Community (LSTC) is its ability to bring together expertise from the various IEEE societies and organizations and have these entities work as a whole.

This function was demonstrated both during a mini-symposium at EMBC 2016 and a HealthCom2016 panel. In these events, LSTC brought together expertise in issues related to the Internet of Things, wearables, and the Quantified Self (QS), as well as cyber security aspects in these areas, and notable experts from various IEEE societies and organizations participated in these sessions.

The Quantified Self Movement

Donna Hudson, Past Chair of LSTC, Past President of the Engineering in Medicine and Biology Society (EMBS) and IEEE Lifetime Fellow, discussed the Quantified Self movement that works to "incorporate technology into data acquisition for all aspects of a person's daily life in terms of input." This could be quite useful for individuals and for treating physicians. However, Dr. Hudson added that "such monitoring needs to be balanced to avoid potential individual hypochondria."

Using Wearable and Implantable Medical Devices for Both Remote Sensing and Treatment

Drawing upon his experience with devices for neuro-sensing and neuro-stimulation,

Mohamad Sawan, IEEE Fellow, discussed using wearable and implantable medical devices for both remote sensing and treatment. Focusing on brain wireless area networks, one of the challenges is how to manage the multichannel data and draw the right conclusions from the massively parallel measurements of physiological activity that these devices could produce. Some of these devices could be actuators enhancing or recovering the patient's medical functions. Thus, processing and analyzing the sensing data and deciding the course of action need to be done in real time. Another challenge is providing power to a myriad of devices implanted inside the body. Among the case studies both epilepsy and vision were discussed.

Cyberspace, Privacy, and Information Security in the Healthcare Sector: Social Implications of Technology

Luis Kun, IEEE Lifetime Fellow, addressed the ongoing transformation of health care into "a wellness-centric enterprise where prevention is key" rather than focusing only on curing diseases. This is a positive shift but there are still a number of issues that need to be addressed. The integration of multiple sets of data, information, and knowledge will include genetic as well as environmental and other areas (i.e., water and air quality, food and drugs, vaccines traceability, etc.). This "big data" will allow for very large population studies and generate new challenges as well. Among them are privacy and security that arise when there is a massive data and information flow among devices and systems. These issues are related to the general threats of cyber security and privacy that our society as a whole faces these days. Strategies on personal, local, state, country, and international levels need to be further developed to counter these threats.

Up Close and Personal: Cybersecurity in Medical IoT Devices

Stefano Zanero, IEEE Senior Member, and **Eric Evenchick**, IEEE Member, have argued that none of the cybersecurity challenges are more pressing and timely than those associated with the Internet of Things especially when it comes to medical devices (in particular implantable ones). These devices are often small and constrained in power consumption and heat generation and reside within or on the

human body requiring high precision and safety. They are wirelessly connected but need to be insulated from the public internet. Needless to say that firmware updates might be unfeasible or risky.

Moreover, Zanero and Evenchick pointed out that:

> there are also challenges with the mindset of designers and engineers. Safety-critical systems, as well as medical devices, are most often tested according to standards and regulatory specifications: Unfortunately, it is well known that this type of testing is inapplicable, as of our current understanding, to security engineering, where most testing is negative (i.e., conducted by trying to break the system). Also, security assessment and design needs a systemic approach, whereby all components of a system are tested together, observing their interactions.

Lessons from the Home Front: Systems Engineering Approach and the Quantified Us

Nahum Gershon, IEEE Senior Member, addressed the apparent inaccuracy of some commercial IoT devices (one device, for example, indicated that he climbed 39 floors while he was sitting through a 4-hour bus ride). He then addressed the need for looking at a system of devices rather than considering them as a collection of individual devices (more systems engineering approaches). Wise approaches of planning the composition and variability of the collection could reduce the vulnerability of systems of IoT devices, hubs, wearables, implantables, and skinnables to cyber infringements.

The Quantified Self phenomenon is expected to revolutionize medicine where both the physician and the patient will monitor the medical situation. Active and self-informed patients might also detect early signs and participate in the medical decision process. In addition to just focusing on the individual (Quantified Self), looking at the data about small and large groups of people (Quantified Us) could

teach us the science and practice of crowd behavior and state. This approach has a promise, for example, in conducting clinical or semi-clinical studies of populations.

Publication Call

We plan to issue a peer-reviewed publication (a book or a journal special issue) on the topic of "Cyber-Security, IoT, Wearables, and the Quantified Self (QS)". If you are interested in contributing to this effort, please contact Nahum Gershon at <schmooz@mac.com>.

Participants in the topical events included:
Eric Evenchick – Computer Society
Donna Hudson – Engineering in Medicine and Biology Society
Luis Kun - Society on Social Implications of Technology
Mohamad Sawan - Circuits & Systems Society
Stefano Zanero - Computer Society
Nahum Gershon, LSTC, Moderator & Organizer