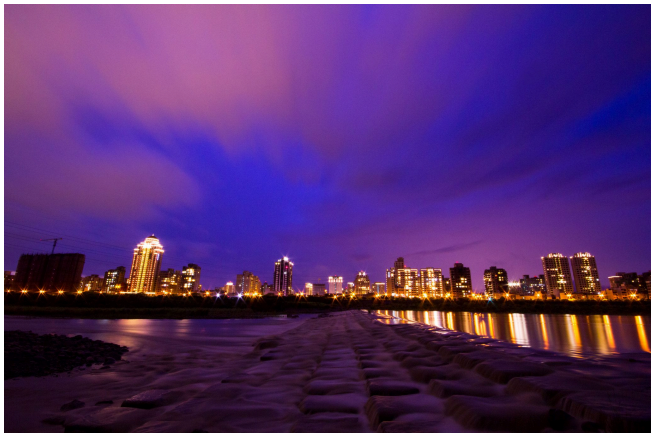
Considerations for Healthcare Applications in the Internet of Things

Phillip A. Laplante
Pennsylvania State University
plaplante@psu.edu

Nancy L. Laplante
Widener University
nllaplante@mail.widener.edu

Jeffrey M. Voas
National Institute of Standards and Technology
jeff.voas@nist.gov



Abstract - In this paper we review an approach to characterizing healthcare applications for the Internet of Things. We then discuss some of the challenges in eliciting requirements from patients and discuss privacy issues in this context.

Keywords - internet of things, healthcare, security, privacy, sensors, surveillance

1. Introduction

The technology evolution and telecommunication paradigm The now clichéd "Internet of Things (IoT)" includes devices, sensors, actuators, communication, and computational elements tethered to the Internet. There is a great deal of excitement about the seemingly limitless uses for this technology, but none promises to aid human kind more than those for healthcare. Healthcare applications for the IoT will be able to deliver comprehensive patient care in various settings. We have introduced a structured approach for describing specialized, provisioned IoTs for healthcare. The approach involves defining general classes of system types, classifying the healthcare delivery settings, and then using a structured approach to describing the elements for a particular use case [1].

In particular, healthcare can be delivered in three broad-based setting types: acute care, community-based care and long-term care, and three application types, tracking humans, tracking things, or tracking both. Acute care refers to a hospital setting. Long-term care refers to nursing homes, or other skilled nursing facilities. Community-based care is delivered outside the acute care and long-term care settings, in community settings.

The three application types we term Class A, B, and C. Class A systems track humans (e.g. patients, caregivers, family members). For example, geo-locating patients throughout their stay in a hospital. Class B systems involve "things" such as medical devices, supplies, and specimens. Class C systems are a hybrid of Classes A and B, comprising both people and things. Taking into consideration the dimensionality of care settings and IoT application classes, the cross product of setting type and system classes yields nine use case classes for a healthcare IoT: acute (A, B, C), long-term (A, B, C), home (A, B, C) [1].

When specifying the functionality for IoT healthcare applications, attention is naturally focused on such concerns such as fitness of purpose, wireless interoperability, energy efficiency, and so on. Conventional techniques such as domain analysis, Joint Application Development (JAD), and Quality Function Deployment (QFD) among others [2] are usually adequate for these kinds of requirements. But in healthcare IoT applications security, safety and privacy requirements are probably of greater concern.

There has been work on addressing security considerations for medical devices, for example, Landwher [3] proposed a "building code" for medical devices, and this approach would be essential in healthcare IoT applications. Safety concerns address questions such as: is the system operating as intended? Is the system providing needed levels of care? Is it providing unintended functionality? The US Underwriters Laboratories has proposed a fault-tree analysis approach for specifying hazards in wearable devices [4], and this approach would be appropriate for healthcare applications using IoT technology. Using traditional techniques for defining misuse and abuse cases would also be appropriate. But privacy concerns are of special importance in healthcare applications because of the sensitive, personal nature of the information. It these types of requirements that we wish to consider in more detail.

2. Privacy Concerns

Privacy concerns have always been a crucial aspect of health care. Patients expect that their personally identifiable information (PII) will remain confidential and that health care providers will protect them. Similarly, IoT-based healthcare systems must assure privacy but allow for sharing of information that is needed to provide high quality care across the care continuum.

Privacy requirements are derived from policy, regulations, standards, and patient need. In the US, for example, the Health Insurance Portability and Accountability Act (HIPAA) of 1996 prevails in how a patient's personally identifiable information (PII) can be used and shared. At its inception, HIPAA recognized that health information was shared in many ways, including electronic formats, and sought to protect all individually identifiable health information; this information is also referred to as protected health information (PHI).

Considering that protected information includes demographic data, past/present/future physical and mental health conditions, social security number, and date of birth, it is easy to recognize the need to secure this information. Note also that many of the devices used in a provisioned, specialized IoT will collect various data whether that surveillance is known or not. If so, where does that data go? Who owns it? And why is it being collected in the first place? Sensors and surveillance will be huge concerns to overcome if to argue convincingly for compliance when the economic benefits to healthcare providers are overwhelming for this technology.

Note that there are similar privacy laws similar to HIPAA in other countries. For example, in the United Kingdom there is the Data Protection Act (1998) and in Canada the Personal Information Protection and Electronic Documents Act (2001). Both are in compliance with European Union's "The Data Protection Directive" (1995), which regulates the processing of personal data within the European Union, and various other countries in the EU have privacy laws that are in compliance.

3. Other Requirements

In addition to privacy laws, healthcare IoT applications will have to comply with various others standards and laws, for example, for medical equipment safety and component interoperability. The derived requirements from these can be managed in the usual ways. For example, using Domain Analysis, that is, essentially an analysis of similar and competing systems. Patients may have other requirements pertaining to a special need, for example the use of a service dog that would need be tracked, or other specific needs based on cultural or religious considerations. These custom requirements could be determined using interviews and ethnographic observation. Prototyping models (both executable and non-executable) also have a place in requirements elicitation [2]. Patient role playing could be effective in prototype based requirements elicitation.

4. Final Remarks

Our work focuses on the development of techniques for specifying healthcare IoT applications and the identification of emergent issues, in particular, patient centered ones. Despite the anticipated benefits for these systems, new challenges will arise. For example, in obligations to report illegal activity information captured by IoT that run up against privacy considerations. These issues warrant further research by legal scholars.

References

[1] Laplante, Phillip A., Laplante, Nancy L and Jeffrey M. Voas, "A Structured Approach for Describing Healthcare Applications fir Internet of Things," 2015 (unpublished).

[2] Laplante, Phillip A., "Requirements Engineering for Software and Systems," Second Edition, Taylor & Francis, 2013.

[3] Landwehr, Carl E. "A building code for building code: Putting what we know works to work." Proceedings of the 29th Annual Computer Security Applications Conference. ACM, 2013.

[4] Kirk, Stephen. "The Wearables Revolution: Is Standardization a Help or a Hindrance?: Mainstream technology or just a passing phase?." Consumer Electronics Magazine, IEEE 3.4 (2014): 45-50.

Phillip A. Laplante is Professor of Software Engineering at The Pennsylvania State University. He received his B.S., M.Eng., and Ph.D. from Stevens Institute of Technology and an MBA from the University of Colorado. He is a Fellow of the IEEE and SPIE and has won international awards for his teaching, research and service. Since 2010 he has led the effort to develop a national licensing exam for software engineers. He has worked in avionics, CAD, and software testing systems and he has published 27 books and more than 200 scholarly papers. He is a licensed professional engineer in the Commonwealth of Pennsylvania and a Certified Software Development Professional. He is also a frequent technology advisor to senior executives, investors, entrepreneurs and attorneys. His research interests are in software testing, requirements engineering and software quality and management. Prior to his appointment at Penn State he was a software development professional, technology executive, college president and entrepreneur. More information can be found at www.perso

Nancy Laplante is Associate Professor of Nursing at Widener University teaching in the undergraduate and graduate nursing programs. She earned her BSN from William Paterson University, her MSN from West Chester University, and a PhD from Widener University. Dr. Laplante is board certified in advanced holistic nursing. Her research interests include health care applications for the Internet of Things (IoT), the image of nursing in media, and creating authentic presence in online nursing courses. Dr. Laplante believes in a holistic approach to nursing education and patient care, and integrates holistic nursing core principles in coursework throughout her undergraduate and graduate teaching. Dr. Laplante is a regular contributor to nursing textbooks, an Associate Editor for the *Journal of Holistic Nursing,* and has published in the areas of holistic nursing education and Service-Learning.

Jeffrey Voas is a computer scientist at the US National Institute of Standards and Technology (NIST) in Gaithersburg, MD. Before joining NIST, Voas was an entrepreneur and co-founded Cigital: www.cigital.com. Voas co-authored two John Wiley books (Software Assessment: Reliability, Safety, and Testability [1995] and Software Fault Injection: Inoculating Software Against Errors [1998]. He received two U.S. patents and has over 200 publications. Voas received his undergraduate degree in computer engineering from Tulane University (1985), and received his M.S. and Ph.D. in computer science from the College of William and Mary (1986, 1990 respectively). Voas is a Fellow of the Institute of Electrical and Electronics Engineers (IEEE), the Institution of Engineering and Technology (IET), and the American Association for the Advancement of Science (AAAS). Voas received the U.S. Department of Commerce's Gold medal in 2014 for his efforts in vetting apps for smartphones for U.S. soldiers in mid-East conflicts.