Usable Security of Emerging Healthcare Technologies for Seniors

Abstract
Older adults were found to have a very diverse set of privacy and security attitudes and concerns compared to younger population. Seniors per sé constitute a more diverse group of population than younger adults. With increasing longevity and advances in medicine, older adults are becoming the main end users of emerging healthcare technologies (EHT). Yet not all EHT are designed for the needs of geriatric population. Due to novelty, complexity, and collection of vast amount of sensitive healthcare information, EHT pose serious privacy and security concerns. To address those concerns, a better understanding of seniors’ privacy and security mental models is needed. We plan to conduct a series of semi-structured interviews and surveys with senior citizens and their formal and informal caregivers to explore the tension between their views regarding the use of EHT, related privacy and security attitudes, mental and threat models. We also will involve senior users into participatory design and experimental testing to make recommendations for effective privacy and security EHT control systems.

Author Keywords
Emerging technologies; healthcare; Internet of Things.

ACM Classification Keywords
• Usability in security and privacy • Empirical studies in HCI • Human-centered computing • Participatory design • Empirical studies in accessibility • Social and professional topics • Seniors

Alisa Frik
International Computer Science Institute (ICSI)
Berkeley, CA 94703, USA
afrik@icsi.berkeley.edu

Serge Egelman
ICSI
Berkeley, CA 94703, USA
egelman@icsi.berkeley.edu

Joyce Lee
University of California
Berkeley, CA 94703, USA
joyceslee@berkeley.edu

Nathan Malkin
University of California
Berkeley, CA 94703, USA
nmalkin@cs.berkeley.edu

Florian Schaub
University of Michigan
Ann Arbor, MI 48109, USA
fschaub@umich.edu

Permission to make digital or hard copies of all or part of this work for personal or classroom use is granted without fee provided that copies are not made or distributed for profit or commercial advantage and that copies bear this notice and the full citation on the first page. Copyrights for third-party components of this work must be honored. For all other uses, contact the Owner/Author.

CHI’18, April 21, 2018, Montreal, Canada
Copyright is held by the owner/author(s). Publication rights licensed to ACM.
Introduction
In recent years, older adults have been increasingly involved in the use of emerging technologies, especially in the domain of healthcare. A few examples include wearable devices for medical measurements, context-aware safety monitoring, fall sensors, and therapeutic robots [1]. These are all “Internet of Things” (IoT) devices, albeit for a niche user base. These technologies aid in improving elderly people’s safety and health, in addition to supporting independent living. However, due to potentially limited technological literacy and high probability of physical or mental impairments, older adults are particularly vulnerable to the cyber-security risks and privacy threats posed by these devices. Our research thus aims at (1) better understanding the privacy and security attitudes of the geriatric population with respect to emerging healthcare technologies (EHT), and (2) designing an effective system that will empower informed decisions, better control over personal data, and improved security for these users.

We plan to conduct three studies to achieve these goals. First, we will conduct semi-structured interviews with both senior citizens and their formal and informal caregivers to explore the tension between their views regarding the use of EHT. We will explore their privacy and security attitudes, threat models, and mitigation and control strategies. The result of this first qualitative study will then be used to build security mental models of elderly people with regard to EHT. The second study will use surveys to empirically validate these models at scale, examining how various factors—such as type of device, type of data and method of its collection, data recipients, context of use—impact elderly people’s privacy and security perceptions of EHT. The third study, based on the relevant identified factors, will involve participatory design and experimental testing to make recommendations for effective privacy and security control systems for the EHT. We wish to participate in CHI Workshop to gather feedback to improve our proposed research agenda.

Related Work
Over the past several decades, the average life expectancy has grown significantly due to developments in medicine and technology [20]. Accordingly, the number of elderly people has grown. For instance, in the United States, the number of citizens over 65—who are most likely to suffer from chronic diseases—is expected to double by 2060, accounting for 24% of the total population [16]. At the same time, due to demographic shifts, the labor market (including caregiving workers) will shrink during that period. It is particularly likely to affect the rural Midwest areas with high “aging in place” rates due to significant outflow of young people. About 8.3 million Americans received Medicaid home care in 2004, which is 25% more than in 1995 [15]. By 2030, more than 2.3 million senior Americans will require nursing home care, which translates into a 75% increase compared to 2010. A similar demographic situation is observed in Europe [6]. These trends explain a noticeable ICT uptake in the area of healthcare technologies aimed at sustaining independent living, increasing the quality of life, and preventing health issues of older adults via early detection.

A number of technological solutions attempt to meet the needs of elderly people in various domains, including health, nutrition, safety, communication, localization, and navigation (see review in [1]). Wearable devices are one area of significant progress. A few examples include devices mounted on the body or clothes, embedded with gyroscopes, magnetometers, accelerators, and other sensors that collect information on orientation, movements, blood pressure, glucose level, temperature, etc. [e.g., 10, 18]. Another major area of innovation is the context-aware systems that use sensors and cameras installed in the home to monitor daily activities or detect falling [e.g., 7, 14]. Some of the systems are stand-alone devices embedded within the home, such as the vHAB camera developed by Multimodal Health [22], which tracks the muscle activity information for adjustment of the therapeutic program after a stroke or trauma.
However, there are also more complex and dynamic care companions being developed, such as the PARO [23] therapeutic robot and Joy For All Companion Pets [24] carebot. The most comprehensive group of systems represents a network of devices connected via Wi-Fi, Zigbee protocols, or other bridges. For example, 2net Platform from Qualcomm Life [25] integrates spirometers, drug delivery devices, respiratory vests, point-of-tests, and other medical devices into a united ecosystem for comprehensive health monitoring and services. Secure independent living system Wellness from Alarm.com [26] likewise combines wireless sensors with wearable alert buttons for remote monitoring of seniors.

While EHT improve health monitoring and safety of elderly people by enabling easier monitoring, their effectiveness is dependent on the amount of data collected. The more data these technologies collect, the greater is their potential in preventing health complications and faster assistance delivery, which is particularly critical in emergency situations. However, extensive data collection and non-stop surveillance trigger privacy and security concerns among the senior end users of those technologies. Melander-Wikman et al. [12] conducted a series of focus groups where they presented elderly people with videotaped activity scenarios featuring ubiquitous computing use cases. They found that trust and privacy are the core factors affecting adoption of ubiquitous technologies. Similar results were obtained in research conducted in [4]. User-based experiment in [11] found that privacy and security are the primary concerns among the users of wearable devices, especially with respect to video recording and financial data.

Caine et al. [3] discovered a need for privacy management among older adults, and demonstrated that seniors favor and are able to use data controls, such as the ones embedded in a medical system DigiSwitch. However, due to generally low technological literacy, elderly people often hold inaccurate beliefs about the security of the technological systems they use. For instance, one participant in a study by [9] felt confident about sharing her bank details with Amazon because “the complete number isn’t displayed, only the last two digits” (p. 7064). Such misconceptions about actual data collection and storage may cause underestimation of security risk and therefore the choice of inadequate levels of protection by the users. On the other hand, WHO [19] argues that misconceptions, e.g., about what data the system collects, may raise false concerns that disappear when appropriate explanations are provided.

In addition to types of collected data, existing research suggests that the recipients of data matter to seniors, i.e. who accesses the data and how often, and to what level of detail. A related concern is associated with the lack of feedback from the monitoring system about when it is recording, and when the data is being accessed. Elderly people often rely on family members in “dealing with technology” [9]. However, delegation of security choices is not a safe security behavior strategy. Additional issues were detected with creating, remembering, and entering strong passwords.

Nevertheless, elderly participants in [9] demonstrated strong privacy attitudes in certain cases. They copied many online behaviors that researchers introduced to them while teaching how to use a messaging app, such as sharing pictures of their meals, landscape, or objects. The seniors, however, never shared online photos of their family members, even though the researchers did so. Some participants employed mitigating security strategies, e.g., basic encryption of their passwords. Interestingly, seniors created stronger passwords and made a bigger effort in protecting them for bank accounts, but not for tablet apps. Individual differences were also found to affect privacy and security preferences. Seniors with severe health conditions are more likely to share their information [2, 19], and generally value independence and safety more than privacy [5, 13, 17].

All together, these findings provide a strong insight on context-dependent and heterogeneous privacy and security attitudes of elderly people, and demonstrate that seniors’ mental models of security
and privacy may differ from those of younger people. Moreover, older adults represent a more diverse group of population than younger people \[8\], due to a striking difference in their health conditions, education, living conditions, and experience. Furthermore, older adults may suffer from severe physical and cognitive impairments, which further complicate the usability issues. Therefore, it is important to further study privacy and security attitudes of older adults in detail and for different scenarios. As this population grows, it will be critical to develop recommendations for effective design of control systems design that will enable informed decisions and choices, better control over personal data, and improved security for seniors, an especially vulnerable group of EHT users.

**Methodology**

We plan to recruit \(^1\) participants among the inhabitants of senior centers, “smart” nursing homes and residences, members of associations and cultural organizations for retired people, and user bases of startups developing smart technologies for elderly people. Due to expected low/moderate technological literacy and potential physical impairments among elderly people, we plan to conduct research in a variety of ways to engage a diverse population: by phone, in-person, online, and using analog methods (paper-and-pencil). We now describe three studies we plan to conduct to address the research goals.

**Study 1: Interviews**

First we will conduct a screening survey to recruit for the follow-up interviews a diverse group of older adults age 65+, with various backgrounds, technological literacy and skills, health status, living arrangements, education, income, experience with EHT, etc.

The structure of our interviews is inspired by the study in [21], where 15 inhabitants of smart homes were interviewed about their privacy and security attitudes, behaviors, threat models, and mitigation strategies. However, our study will differ from the work of [21] in the following ways: 1) we will focus on the population of elderly people rather than young and middle-aged adults, 2) we will focus on healthcare connected devices and nursing homes rather than ordinary smart homes, 3) we will interview older adults that are currently not using EHTs and their caregivers, in addition to the senior users of EHT, and 4) we will consider wearable devices in addition to context-aware smart technologies.

In these interviews, we plan to discuss four main topics related to smart technologies for elderly people: general opinions on emerging technologies and daily needs and difficulties that seniors are facing, mental models about data collected by EHT and recipients of this information, privacy- and security-related concerns and threats, and user control strategies. Additionally, we will collect information about participants’ individual characteristics (socio-demographics, familiarity with technology, level of independence, living arrangements, health status, etc.)

Once interviews are concluded, we will transcribe and code the responses using several independent coders, and classify the data based on the arisen clusters. We will then interpret the results and generate a model based on the identified concepts and categories. We will compare the views of seniors with the views of caregivers, on average, and pairwise (i.e. older adult vs. his/her caregiver) to identify similarities and tensions. Finally, we will compare the beliefs and preferences of senior users and non-users of EHT, to identify potential barriers in adopting those technologies.

---

\(^1\) The North, West and Downtown Oakland Senior Centers, Seniors Without Walls association, and Community Technology Network, and MultiModal Health and Neurotrack startups have already agreed to collaborate with us on this research.
Study 2: Surveys
After distilling the important aspects of privacy- and security-related attitudes from exploratory interviews, we plan to empirically validate with a survey a model of privacy- and security-related attitudes, quantifying the impact of various factors on these attitudes. The survey will include multiple-choice questions based on the concepts and categories included in the model emerged from the interview data, as well as open-ended questions for further clarification of respondents’ opinions. We are interested in examining the factors that may impact security and privacy attitudes related to the use of EHT, such as wearable devices vs. context-aware sensors, stand-alone vs. connected devices, single- vs. multi-user (or shared) systems, type of data (medical, location, communication), recipients of data (same system, other systems, self, other humans), use cases (health, safety, nutrition, activity monitoring, localization, communication), reference group (family and friends vs. doctors and caregivers), and modality of control (smartphone vs. voice sensors; contextual triggers, e.g., time of day, location, etc. vs. physical triggers, e.g., buttons, toggles, etc.).

Study 3: Experiment
Based on the results from interviews and surveys, we plan to develop recommendations for designers and developers of smart systems, as well as suggestions for future research. We also plan to distribute actual smart healthcare devices to the seniors and involve them in the participatory design to create and test prototypes of control systems that would allow configuration of privacy and security settings. Our experiments will gather information about what settings users choose, whether their actual choices are aligned with the stated attitudes and preferences, whether they change the settings according to different situations and contexts, etc. The development of control systems will include user testing to ensure comprehension and usability.

Potential Impact
Our research will contribute to better understanding of privacy and security attitudes regarding smart healthcare technologies used by seniors, a particularly vulnerable group of users. We will establish what factors affect privacy and security preferences of this population, and study the difference in attitudes between actual users and non-users of these technologies, and their caregivers. Better understanding of the reasons inhibiting the adoption of smart healthcare devices will provide insights on how to overcome those barriers, as well as increase security and privacy standards. This research thus has the potential to increase the application of technology that improves longevity and quality of life, prolonging the independent living of older adults. Moreover, we will design and test effective and usable, privacy- and user-friendly control systems, tailored specifically for the needs and abilities of senior users. Additionally, we will provide guidelines for developers regarding the principles of effective design for security and privacy control systems and interfaces of smart healthcare technologies and connected devices. We will also suggest directions for future research. Finally, seniors can be considered “extreme users” [21] of smart healthcare devices, whose needs and ability limitations are amplified with respect to more general population. Therefore, studying the attitudes of elderly people, including non-users, will help us to understand the concerns surrounding emerging technologies across more general populations and discover deeper insights that may be overlooked in the studies with typical user communities.

Acknowledgements
We thank all the colleagues, who provided helpful comments on previous versions of this document. This work is supported by a grant from the Center for Long-Term Cybersecurity (CLTC) at U.C. Berkeley.
References


