Enabling IoT Residential Security Stewardship for the Aging Population

Lorenzo De Carli
Worcester Polytechnic Institute
Worcester, MA 01609, USA
ldecarli@wpi.edu

Indrakshi Ray
Colorado State University
Fort Collins, CO 80523, USA
indrakshi.ray@colostate.edu

Erin Solovey
Worcester Polytechnic Institute
Worcester, MA 01609, USA
esolovey@wpi.edu

CHI'20,, April 25–30, 2020, Honolulu, HI, USA
ACM 978-1-4503-6819-3/20/04.
https://doi.org/10.1145/3334480.XXXXXXX

Abstract
Smart home devices (IoT devices, or IoTs) can monitor the health, safety, and security of aging adults, and automate many household tasks, enabling independence far into old age. However, IoT devices have many inherent vulnerabilities, which make them a popular target for cyberattacks. The heterogeneity of IoT devices and their interactions may make them susceptible to new types of attacks, and also make usability difficult for the aging population. Furthermore, the aging population may be particularly vulnerable and diffident to new technologies. Existing network management interfaces are designed for domain experts, and are impracticable for non-technical users. In our work, we are exploring the design of (i) interfaces and guidelines to enable senior users to manage the security posture of IoT devices, and (ii) AI systems that identify such issues and collaborate with the user to resolve them.

Author Keywords
Internet of things; IOT; network security; aging.

CCS Concepts
•Human-centered computing → Human computer interaction (HCI); •Security and privacy → Network security;

Introduction

One of the great promises of smart inter-connected home devices is safe and independent living for the aging population. This promise is, however, hampered by the poor state of IoT device security: these devices tend to be affected by easy-to-exploit security vulnerabilities which make them popular targets for cyberattacks. Highly publicized examples abound (e.g., [7, 2]).

Designing secure devices is inherently difficult due to the wide variety of unforeseen contexts where they may be installed. Also, many vendors tend to have poor security practices, shipping products with vulnerabilities that are easy to discover and exploit. IoT devices, catering to a wide variety of functions, are heterogeneous; this heterogeneity and interaction of devices make them harder to use and also may result in emergent vulnerabilities. This state of things clashes with the vision of a world where older adults depend on them for safe and healthy living.

Our work aims at understanding and overcoming the gap between cybersecurity skills of an aging population and the skills needed to maintain the current generation of IoT devices securely. In order to close this gap, we are working to: (i) build a detailed model of attitudes towards and understanding of cybersecurity in the aging population; and (ii) design new algorithmic tools to assist this demographic in identifying and resolving security issues arising within home IoT networks.

Background

Older Users, IoT, and Cybersecurity

There exists a rich literature on using IoT devices to enable autonomous living for seniors (e.g., [15, 12, 14]), and we expect that IoT devices will perform an important role in assisted living as the population continues to age. These works propose valuable approaches to enable use of IoTs as assistive devices, but they typically do not discuss security implications. Other works discuss seniors' attitudes towards security/privacy issues and cybersecurity tools [1, 6, 8]. They tend to focus either on high-level problems (e.g., the perception of risk related to the use of internet-connected devices), or traditional computing devices (e.g., home firewall configuration). Overall, there has been limited analysis of IoT-specific usable security for older adults.

Securing residential networks

There is a vast literature on detecting and resolving network security breaches, dating back more than 20 years (e.g., [10]). However, much of this literature focuses on enterprise security and/or traditional computing devices such as PCs and laptops. Furthermore, it generally assumes the availability of a human expert (network administrator) to understand and act upon the output of security tools. IoT devices come in various forms and flavors, use different protocols, and interact in subtle ways. This suggests that securing IoT devices requires not only new modes of user interactions, but novel security systems and algorithms.

Understanding the Context

Recent work by Desjardins et al. [3] suggests that most domestic IoT research assumes a detached single family North American home with two parents and children. Although this work does not focus on network security, it highlights the importance of broadening assumptions beyond stereotypical homes. This is particularly important when focusing on an understudied population such as aging users.

Understanding User Motivation and Knowledge

Prior work on user perceptions of smart home IoT privacy [16] suggests that users highly value the convenience of IoT devices, over both privacy and security. Other work [4] provides evidence that people have limited or incorrect under-

standing about IoT security, and often do not consider it before purchasing. Further, many individuals view security as an "innate, uncontrollable property" and lack knowledge of risks and mitigation strategies, and found it overly burdensome. Grinter et al. [5] showed that home networking setup and maintenance often was nontrivial, even in households with highly technical members. A study in the UK [9] found that individuals tend go to friends, family and coworkers with some technical knowledge for help in keeping their network secure. Taken together, these findings demonstrate an overall cultural problem—lack of perception of security issues as a serious threat. They also demonstrate a gap between the knowledge of average users and the knowledge necessary to properly secure consumer IoT devices.

Enabling IoT Network Stewardship

Our work focuses on the concept of IoT security stewardship: the idea that a residential network of vulnerable IoT devices should be able to gain understanding of basic security issues arising within the network itself, and deploy countermeasures at the network level.

Oftentimes, attackers controlling devices within a network result in anomalous device-generated network traffic. In preliminary work, we designed and tuned classification algorithms for traffic analysis that can (i) fingerprint devices, (ii) fingerprint the actions a user is performing on a device, and (iii) distinguish whether a device is being remotely controlled by the legitimate owner or a hostile user (based on patterns of actions). For example, in preliminary characterization of a Netgear Arlo Q security camera, our algorithm was able to map network traffic to the action being performed (stream video, toggle LED status/speaker/night vision/motion sensitivity, rotate image) with 99.7% accuracy. Likewise, given two different user action profiles (the legitimate owner, and a privacy-invading attacker), our algorithm was able to distinguish them with 96% accuracy.

In a residential network with non-technical users, however, information about traffic and action patterns is of little use as the users may lack the background to interpret this information and put it in context. Our goal is to determine guidelines for the design of network security systems that do not only individuate attacks, but interact and cooperate with such users to resolve them. These interactions should not assume the user has security expertise. In particular, we focus on older users, due to the potentially transformational role that smart devices can have on their lives.

Toward Design Principles for Aging Users

Designing for older users entails numerous domain-specific problems, from visual interface design to the nature of interactions themselves. Elderly populations are often vulnerable; we must make sure that such interactions do not cause alarm. At the same time, provided information must be specific enough to ensure that the user feels in control of the situation. Furthermore, if users come to depend on IoT devices for autonomous living, it is important for a security system to avoid disrupting the functioning of such devices.

The end-goal of our research is to determine design principles for residential network security systems that are usable by—and useful to—senior users. Such systems will consist of algorithms to detect and remediate breaches, and interfaces towards the residential user. Through critical analysis of this domain, as well of the related work, we identified four conceptual areas of focus: *autonomy*, *resilience*, *control*, and *delegation*.

Even expert users may find confronting security issues (e.g. an attacker commandeering a webcam) stressful and technically complex. Furthermore, the current and oncoming generations of seniors are not digital natives (i.e. were not

exposed to ubiquitous computing devices and the internet during their formative years), and they may perceive smart devices as difficult or extraneous. It is therefore reasonable to design systems that operate *autonomously* as far as possible. For example, such a system may deploy simple countermeasures automatically, or choose to ignore certain low-risk vulnerabilities.

Further, the systems should be *resilient*, i.e. able to recover from unsophisticated attacks and continue to operate—possibly with reduced functionality. The goal here is to reduce user involvement to the minimum necessary, to avoid creating undue burden. System design must also pay attention to reducing *false positives*—alerts that generate stress to the user but are issued in error.

In order to avoid distrust or alienation towards the system, it is also important to ensure that the user retains *control* of it. The tension between automation and operator control is a classic one in system interface design [11]. Here, we propose to resolve it by letting automated algorithms identify low-level network security problems, while presenting high-level summaries and requests for actions to the user. For example, the user may be informed that unusual activity was detected, and rebooting a wireless router is recommended. Determining the appropriate representation and content of such communications is an open problem, as they must be informative while avoiding generating stress. Indeed, many of the novel problems in this area lie at the intersection of network security, human-AI interaction, and HCI for aging. While threat detection algorithms have been extensively studied, their interaction with non-technical senior users have not.

Finally, we point out that *delegating* control of the system to a service provider—or even to a skilled family member—may also be helpful. There is a well-developed literature on the technical aspects of delegating security management of IoT networks (e.g., [13]). However, not all users may wish to perform such delegation, and not all decisions may be delegated to third parties. Therefore, it is important to illustrate to an elderly user the consequences of delegation and allow an interface that allows delegating some permissions while retaining control over others.

Conclusion

IoT devices have the potential to be immensely useful as assistive devices as the population continue to age. Before seniors can depend on such devices for independent living, significant cybersecurity issues must be resolved. In order to improve the security of IoTs, we investigate new usable security systems that can discover issues and interface with older users in a helpful and informative manner. Design of such systems is based on the principles of *autonomy*, *resilience*, *control*, and *delegation*.

Author Background

Lorenzo De Carli is an Assistant Professor of Computer Science at Worcester Polytechnic Institute. His research interests focus on the security of the internet-of-things, the web, and clouds. He has expertise in network traffic analysis, malware analysis, and high-performance networking.

Indrakshi Ray is a Professor of Computer Science at Colorado State University. Dr. Ray's research interests include security and privacy, database systems, software engineering. Her current research focuses on IoT security, healthcare security, and security of cyber physical systems.

Erin Solovey is an Assistant Professor of Computer Science at Worcester Polytechnic Institute. Her research expertise is in human-computer interaction, with a focus on accessibility and emerging interaction techniques.

REFERENCES

[1] Carlene G. Blackwood-Brown. 2018. *An Empirical Assessment of Senior Citizens' Cybersecurity Awareness, Computer Self-Efficacy, Perceived Risk of Identity Theft, Attitude, and Motivation to Acquire Cybersecurity Skills*. Ph.D. Dissertation. Nova Southeastern University.

[2] Nellie Bowles. 2018. Thermostats, Locks and Lights: Digital Tools of Domestic Abuse. (Aug. 2018). https://www.nytimes.com/2018/06/23/technology/smart-home-devices-domestic-abuse.html

[3] Audrey Desjardins, Jeremy E. Viny, Cayla Key, and Nouela Johnston. Alternative Avenues for IoT: Designing with Non-Stereotypical Homes. In *CHI, 2019*.

[4] Pardis Emami-Naeini, Henry Dixon, Yuvraj Agarwal, and Lorrie Faith Cranor. Exploring How Privacy and Security Factor into IoT Device Purchase Behavior. In *CHI, 2019*.

[5] Rebecca E. Grinter, W. Keith Edwards, Marshini Chetty, Erika S. Poole, Ja-Young Sung, Jeonghwa Yang, Andy Crabtree, Peter Tolmie, Tom Rodden, Chris Greenhalgh, and Steve Benford. 2009. The Ins and Outs of Home Networking: The Case for Useful and Usable Domestic Networking. *ACM Trans. Comput.-Hum. Interact.* 16, 2, Article 8 (June 2009).

[6] Dominik Hornung, Claudia Müller, Irina Shklovski, Timo Jakobi, and Volker Wulf. Navigating Relationships and Boundaries: Concerns Around ICT-uptake for Elderly People. In *CHI, 2017*.

[7] John Leyden. 2018. New Mirai botnet species 'Okiru' hunts for ARC-based kit. (Jan. 2018). https://www.theregister.co.uk/2018/01/16/arc_iot_botnet_malware/

[8] Wiebke Maaß. 2011. *The Elderly and the Internet: How Senior Citizens Deal with Online Privacy*. Springer Berlin Heidelberg, Berlin, Heidelberg, 235–249.

[9] Norbert Nthala and Ivan Flechais. Informal support networks: an investigation into home data security practices. In *SOUPS, 2018*.

[10] Vern Paxson. 1999. Bro: a system for detecting network intruders in real-time. *Comput. Netw.* 31, 23-24 (Dec. 1999).

[11] Charles Perrow. 1999. *Normal accidents: living with high-risk technologies*. Princeton University Press, Princeton, N.J.

[12] Robert Steele, Amanda Lo, Chris Secombe, and Yuk Kuen Wong. 2009. Elderly persons' perception and acceptance of using wireless sensor networks to assist healthcare. *International journal of medical informatics* 78, 12 (2009), 788–801.

[13] Curtis R. Taylor, Craig A. Shue, and Mohamed E. Najd. Whole home proxies: Bringing enterprise-grade security to residential networks. In *ICC, 2016*.

[14] Letícia Diniz Tsuchiya, Raphael Winckler de Bettio, and André Pimenta Freire. Evaluation of Web Applications to Control Intelligent Homes with Guidelines for Elderly Users. In *IHC, 2017*.

[15] Alan Yusheng Wu and Cosmin Munteanu. Understanding Older Users' Acceptance of Wearable Interfaces for Sensor-based Fall Risk Assessment. In *CHI, 2018*.

[16] Serena Zheng, Noah Apthorpe, Marshini Chetty, and Nick Feamster. 2018. User Perceptions of Smart Home IoT Privacy. *Proc. ACM Hum.-Comput. Interact.* 2, CSCW, Article 200 (Nov. 2018), 20 pages.