Vision: Stewardship of Smart Devices Security for the Aging Population

LORENZO DE CARLI, Worcester Polytechnic Institute, USA
INDRAKSHI RAY, Colorado State University, USA
ERIN T. SOLOVEY, Worcester Polytechnic Institute, USA

IoT devices can monitor the health, safety, and security of aging adults, and automate many household tasks, enabling independence far into old age. However, such devices also 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 elderly may be particularly vulnerable and uncomfortable with new technologies. Existing network management interfaces are designed for domain experts, and are impracticable for non-technical users.

We propose an agenda for exploring the design of (1) interfaces and guidelines to enable senior users to manage the security posture of IoT devices, and (2) security tools that identify such issues and collaborate with the user to resolve them. We structure this agenda around the core concepts of autonomy, control, and delegation, summarized by the concept of explainable stewardship. We argue that goal (1) must be addressed with qualitative studies of user attitudes towards prototype interfaces. Goal (2) requires the integration of existing network anomaly detection algorithms into techniques which can summarize and explain their meaning.

Much remains to be done to ensure older users can take advantage of smart devices without suffering cybersecurity incidents. We hope this article can act as a call for further research in this field.

CCS Concepts: • **Security and privacy → Usability in security and privacy**; **Social aspects of security and privacy**; • **Human-centered computing → HCI theory, concepts and models**.

Additional Key Words and Phrases: network security, IoT security, older users

ACM Reference Format:
Lorenzo De Carli, Indrakshi Ray, and Erin T. Solovey. 2021. Vision: Stewardship of Smart Devices Security for the Aging Population. In *EuroUSEC '21: European Symposium on Usable Security, October 11–12, 2021, Online.* ACM, New York, NY, USA, 9 pages. https://doi.org/10.1145/nnnnnnn.nnnnnnn

1 INTRODUCTION

Smart, internet-connected home devices, such as smart cameras, household appliances, thermostats, smart locks, etc. are being increasingly installed in residential settings. Internet-connected wearable sensors, used to guide physical exercise and monitor health, are likewise increasing in popularity. It is common to refer to the interconnected set of such devices as the "Internet of Things", and to individual devices as "IoT devices".

One of the great promises of IoT devices is safe and independent living for the aging population. In recent years, researchers have produced a rich literature on using IoT devices to enable autonomous living for seniors, and we expect that IoT devices will perform an important role in assisted living as the population continues to age.

One class of devices on which much attention has been focused targets health monitoring [30, 34]. However, there is also interest in a broader class of IoT devices for home automation, including internet-connected home appliances and

Manuscript submitted to ACM

actuators [24], which can help with home management and even personal care and leisure [18]. Indeed, research on elder users' concept of independence (and how smart technology can enable it) evidences that health monitoring is only one factor; other components—such as tools for easy remote interaction—are necessary [4]. While these kinds of smart devices can be helpful to any population, they are particularly likely to be impactful for older adults who may encounter difficulties in independently performing everyday activities. As Majumder et al. put it, "smart homes may allow the elderly to stay in their comfortable home environments instead of expensive and limited healthcare facilities" [24].

In order to realize this promise, however, it is necessary to overcome a significant hurdle: the poor state of IoT device security. As evidenced by a long stream of reports, it is common for IoT devices to be affected by easy-to-exploit security vulnerabilities. These include lack of access control [19], default and/or hardcoded passwords and access keys [25], and others; the types of security vulnerabilities that are frequently detected in IoT devices run the full gamut of typical software vulnerabilities. The consequence is that attackers can easily gain access to devices, performing various types of privacy invasions and cybercrime operations.

Two factors are oftentimes indicated as culprits for this state of things. First, many manufacturers of IoT devices have expertise on implementing embedded hardware and low-level software, but expertise on building secure internet-connected software may not be available in-house. As a result, the onboard software (firmware) running on a device may not be built according to security best practices [20]. Second, historically there has been limited incentive in improving the security posture of IoT devices, as users tend to ignore decreased security/privacy as long as the devices increase the convenience of performing household chores [35].

To further compound the problem, designing secure devices is inherently difficult—even for experienced designers and developers—due to the wide variety of unforeseen contexts where they may be installed. 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. Indeed, past analysis of IoT systems has shown that even device interaction in the physical world can propagate cyberattacks [14].

This state of things clashes with the vision of a world where older adults depend on smart, internet-connected devices for safe and healthy living. Devices that cannot be properly secured create two types of issues: first, users may be wary to deploy them due to the perceived risk. Second, their use may create danger for the user. Consider, for example, a smart lock that can be opened remotely by an attacker. The goal of this paper is to call attention to the gap between the cybersecurity skills of an aging population and the skills needed to maintain the current generation of IoT devices securely. Further, we propose a research agenda aimed at closing this gap, which includes: (i) building a detailed model of attitudes towards and understanding of cybersecurity in the aging population; and (ii) designing new algorithmic tools to assist this demographic in identifying and resolving security issues arising within home IoT networks.

2 RELATED WORK

Understanding the context. An ethnographic study of households in the UK and US showed that residential network setup and maintenance must be considered in the collaborative social setting of a household [16]. The study also evidenced a gap between the modes through which the internet evolves and provides services, and the needs and expectations of a household. As a result, home networking setup and maintenance often was nontrivial, even in households with highly technical members. It is important to note that the complexity of home network setups has a direct bearing on its security, since a user who cannot fully control the network configuration is disempowered to properly secure it. Interestingly, while this study presented itself as a call-to-arm for more usable and human-centric

household network design, home network technology has arguably evolved in the opposite direction. In the years since this study, IoT technology has rapidly expanded, and home networks have become more complex and more diverse.

The matter is further complicated by the fact that research on IoT devices may suffer from significant selection bias. Recently, Desjardins et al. drew attention to the design assumptions in most domestic IoT research, which often focuses on detached single family North American homes with two parents and children [13]. While this work did not discuss network security, it highlights the importance of broadening assumptions beyond these "stereotypical" homes. Indeed, a household including older users, either by themselves or as part of a larger family, does not fit this definition.

Understanding general user attitudes towards IoT device security. Prior work explored user perceptions of smart home IoT privacy [35]. For example, users highly valued convenience of IoT devices, over both privacy and security. In addition, they did not understand the implications of non-camera-based devices on privacy. In another study, researchers found that people have limited or incorrect knowledge about IoT security, and often do not consider it before purchasing [15]. For example, half of the participants could not differentiate privacy from security. After purchasing, more individuals became concerned about security issues, and during the interview process, almost all participants voiced some interest in having information about the security of their IoT device, ranking privacy and security as the most influential factors after price and features for purchase decisions. Further, many individuals viewed security as an "innate, uncontrollable property", lacked knowledge of risks and mitigation strategies, and found it overly burdensome. Finally, a study in the UK [27] found that individuals tend to go to friends, family and coworkers with some technical knowledge for help in keeping their network secure. The problematic relationship between non-expert users and IT security suggests the need for algorithms and tools that hide some of the complexity of security management, making the problem manageable. This theme informs the notion of *autonomy* in our research agenda, which we discuss in detail later in this article.

Smart devices and older users. Steele et al. looked at issues of perception of wireless sensors for health monitoring in older users [30]. The study found that privacy concerns are not a barrier for acceptance, but that cost concerns may be. Steele et al. also identified an aspect which is crucial to our research agenda: the necessity for older users to retain a degree of *control* over the system that they find appropriate. More recently, Wu and Munteanu investigated the perception related to a specific type of device, a fall sensor [34]. Their analysis found that acceptance is possible, particularly if devices come accompanied by contextual information and practically useful instructions. Ambe et al. provided a rare example of participatory design, in the IoT space, focusing on older users [1]. The experiment emphasizes the importance, for the target demographic, of agency over automation, again emphasizing the theme of control.

Senior users' attitudes towards cybersecurity. An analysis of cybersecurity information sources found that the material generally available online is not tailored to older users, and properly educating this population would require the creation of more accessible material [11]. Researchers have also looked at the usability of web applications used to control smart home devices, with particular focus on older users [32]. This study found again that existing technology is unfriendly to this demographic, and a redesign of existing tools may be necessary. Carlene Blackwood-Brown [5] investigated elderly cybersecurity skill levels and motivations in acquiring cybersecurity skills. This work found that skill levels depend on a variety of factors, and cybersecurity awareness training has the potential of increased older users' command of cybersecurity skills. In a different but related domain, recent work investigated issues related to caregivers accessing healthcare portals as proxies for the elderly. These studies identified significant privacy concerns of older patients in regard to which information can be accessed by others [22]. They also identified shortcomings in technical means for delegation, which forces users to resort to sharing passwords [21]. These works emphasize the need for controlled *delegation* of security, another central theme of our research.

Discussion. Overall, the selection of works reviewed above strongly suggests that older users can benefit from, and are willing to accept, the presence of smart devices that increase their autonomy. It also highlights the need for techniques and tools which can assist with securing smart devices, and are specifically designed with this population in mind. There are, however, caveats. The first is the problematic relationship between unskilled users and cybersecurity of home computing devices. Over and over, analyses of cybersecurity attitudes have found a problematic interface between computing devices and humans, which leave users worried, frustrated, and generally perceiving that they do not fully understand their devices. Systems should take this into account, and hide fine-grained details of security deployment, thus working—at least in part—autonomously. The second is the recurring need of retaining control and agency, which appear particularly pronounced in the elderly population. This theme has significant implications for our research agenda: just securing devices without allowing users to understand how and why security is being applied is likely to be insufficient. The third is that older users may delegate security-sensitive operations to third parties, like caregivers or family. Such delegations must be properly supported.

3 BACKGROUND

3.1 Cybersecurity risks associated with IoT devices

Compromise of smart devices can happen through a variety of means; discussing them is beyond the scope of this article. The general consequence of a successful attack is that an attacker gains control of one or more smart devices in the home, and/or the ability to intercept and observe the data the devices send and receive over the home network. Depending on attacker goals and actions, such a situation can result in harm to two different categories of users.

General harm to other internet users. Skilled cybercriminal routinely run large-scale campaigns which result in compromise of large swaths of IoT devices, which are then organized in botnets. Attacks may involve for example denial-of-service, where a large number of bots send large volumes of traffic to the same destination, causing it to fail [2]. Compromised devices can also be used for other garden-variety cybercrime operations such as ad-fraud [10] and spam campaigns [9]. Note that while these operations are not aimed at harming the device owner directly, they may do so indirectly. For example, a device commandeered to run a denial-of-service attack may cease to perform its main function; an ISP detecting a flurry of spam from a home network may temporarily cut connectivity to that home.

Direct harm to the device owner. An emerging phenomenon is the use of IoT devices as tools of domestic abuse [6]. Someone familiar with a smart device owner (e.g., a former partner, a roommate) may use access credentials they retain for controlling the device after they have ceased to live in the household. Consequences include privacy invasions (e.g., spying on users' private activities) and harassment (e.g., changing thermostat settings to make the house uncomfortable). While there have been no reports of such attacks specifically targeted at the elderly yet, there exist ample cases of smart device-based harassment. Furthermore, direct attacks against device owners are not always targeted. Poorly secured devices left connected to the internet have been used by attackers to randomly spy on households; a chilling example of this activity involved attackers commandeering the speaker and camera of internet-connected baby monitors [33].

3.2 Issues in securing home smart devices

We believe the issues reviewed in the previous section justify the need for better IoT device security. We intend to focus specifically on the older demographic because this class of users is anticipated to strongly depend on these devices for improvements in their quality of life, more so than the rest of the user population.

IoT devices, like other computing devices, can generally be made more secure by running security software on the device themselves. Software tools aimed at improving device security (e.g., anti-malware tools), referred to as host-based threat protection tools, are however unsuitable for IoTs. This is due to the fact that these devices lack the computation capabilities and storage to execute additional security software, and their onboard software may be hard or impossible to update. More promising is the analysis of device network traffic to identify compromise. All devices within the scope of our work communicate over the network to perform their function, most commonly over wireless links. Communication typically involves reporting data and receiving commands; endpoints of the communications are the devices themselves, smartphone IoT apps, and cloud software maintained by the manufacturer [23]. The network traffic generated and received by a compromised computing device differs from the traffic generated during its normal functioning, and network security literature contains a large array of techniques used to detect such anomalies, including signature-based [29], specification-based [8] and anomaly-based [26] attack detection. Such techniques could be executed for example on a home gateway, to identify attacks.

However, we argued in previous work [12] that these and other network monitoring algorithms cannot be directly applied to the scenario at hand, for several reasons. First, in a residential network with non-technical users, information about network traffic and attack patterns is of little use as the users may lack the background to interpret this information and put it in context. This observation leads to the question, *can a network monitoring system for home IoT devices work fully autonomously and avoid the user altogether?* Unfortunately, fully autonomous security systems (i.e., algorithms able to detect and block attackers without user involvement) also cannot be realized.

Briefly, attacks are rare events (compared to normal network activity), and thus even extremely accurate detectors may fall prey of the base-rate fallacy [3], thus suffering from too high false positive rates to work fully autonomously. As a case-study, consider the Kitsune detector [26], a recently-proposed anomaly-based intrusion detection algorithm for IoT networks. In network intrusion detection, an important parameter for a detector is the Bayesian detection rate, i.e., the probability that an alert corresponds to a true attack. As reported in literature [12, 26] Kitsune's Bayesian detection rate oscillates between 65% and 0.4%, with a median of 43%. In other words, a warning generated by this algorithm, in ideal conditions, has 35% probability of being a false alarm. If a system with these characteristics is allowed to autonomously block traffic flagged as malicious, it will likely result in unnecessary disruptions to network functionality.

Even if accuracy were not an issue, a fully autonomous attack prevention tool would result impenetrable and unexplainable to the user. Our literature review suggests that the relationship between non-expert users and computer security is problematic; these issues are worsened in the IoT context by the deeply invasive nature of IoT security breaches (e.g., access of video/audio from within the home). It is important to avoid worsening the relationship between users and security technology, by avoiding the deployment systems making obscure (and potentially incorrect) decisions.

The goal of our research agenda is then to determine guidelines for the design of network security systems that do not only identify attacks, but interact and cooperate with users to explain and resolve them. These interactions should not assume the user has security expertise.

4 PROBLEM CHARACTERIZATION

Having discussed above why building fully autonomous security tools is not feasible, and having concluded that network monitoring algorithms alone cannot solve the problem (due to the deep technical expertise necessary to interpret their results), we set to define how to design a new generation of tools and algorithms for IoT home security, one which keeps humans in the loop. In particular, the end-goal is to determine design principles for residential network

security systems that are usable by—and useful to—senior users. Such systems would consist of algorithms to detect and remediate breaches, and user interfaces supporting elderly 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. Through critical analysis of this domain, as well of the related work, we identified three conceptual areas of focus: *autonomy*, *control*, and *delegation*.

4.1 Autonomy

Even expert users may find confronting security issues stressful and technically complex. Furthermore, the current and upcoming generations of seniors are not digital natives (i.e., were not exposed to ubiquitous computing devices during their formative years), and they may perceive smart devices as difficult or extraneous. It is therefore reasonable to design systems that operate autonomously, compatibly with the accuracy limitations described above. Some unsophisticated attacks (e.g., a portscan) can be identified with high confidence, and mitigated without disruption to other communications. The system may therefore deploy simple countermeasures automatically, or choose to ignore certain low-risk vulnerabilities. The system should also be able to recover from unsophisticated attacks and continue to operate. As an example, the detection of a compromised device generating denial-of-service traffic may be contained by deploying network filters which isolate the device, while allowing it to continue its core operations.

4.2 Control and Explainability

While the autonomy and resilience principles dictate that the system should automatically remediate simple, clear-cut problems, in many situations ambiguity arises which cannot be resolved by existing tools. For example, an unusual network traffic pattern may be caused by an attack, but also by a benign change in user habits. There also exist intrusions which are simple to detect, but require user involvement to be resolved. For example, some compromised devices may only be restored by having the user manually performing a factory reset. This tension between automation and operator control is a classic one in system interface design [28].

Here, we propose to let automated algorithms deal with low-level network security problems which can be resolved easily, while presenting high-level summaries and requests for actions to the user in other cases. For example, the user may be informed that unusual activity was detected, and rebooting a wireless router is recommended. Or they may be requested to provide information concerning device usage to disambiguate an attack. 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 human-computer interaction for aging. While threat detection algorithms have been extensively studied, their interaction with non-technical senior users have not.

4.3 Delegation

Delegating control of the system to a service provider or to a caregiver, or a family member may also be helpful. Indeed, of the properties we identified, delegation is the most specific to the older user population. While there is a well-developed body of work on the technological aspect of delegating security management of IoT networks [31], the human side of the problem has been less studied: not all users may wish to perform such delegation, and not all decisions may be delegated. It is important that delegation of control is done without causing relaxation of security, or

mistrust. Therefore, the system should clearly illustrate to an elderly user the consequences of delegation, and provide an interface that allows delegating some permissions while retaining control over others.

4.4 Explainable Stewardship

Overall, we connect the three requirement categories above through the core concept of *explainable stewardship* of IoT device security: the idea that network monitoring systems designed for older users' homes should manage security on behalf of its owners, while ensuring that those owners remain privy to the system's findings and decisions. This is an ambitious goal which requires integrating threat detection algorithms with a system that can interpret their output and present it in understandable form to non-technical users. In our work, we focus particularly on the *interface* between the system and the human, rather than focusing on attack detection (for which existing technology can be largely reused). When closely examining how such an interface should be structured, several relevant research questions emerge:

- **Autonomy:** (i) How can the system determine which attacks should be dealt with automatically, and which should be escalated to a human?
- **Control and explainability:** (ii) How can low-level network signals be mapped to human-understandable explanations? (iii) Do warnings communicated using different modes (e.g., audio vs text) receive the same attention? (iv) How can security notifications be formulated to ensure the user understands the situation without receiving undue stress?
- **Delegation:** (v) How should warnings be managed in a multi-user household, or one in which a caregiver proxy manages IoT devices?
- **Cross-cutting concerns:** (vi) How do the specific expectations and needs of the older population (and subsets therein) affect and inform interaction design?

5 PROPOSED RESEARCH

5.1 Human-centered Interface and Language Design

Most of the problems we identified require the design of *interfaces* and *language* which are understandable and actionable by the target demographic. Our review of related work underscores how our understanding of attitudes towards IoT security in the older population is limited. We believe it is necessary to conduct formative studies with elderly IoT devices owners and prospective owners to collect data establishing the understanding, expectations, beliefs, concerns, competency and motivation of end users related to IoT security in the home. It is also necessary to investigate requirements and preferences for IoT network security threat detection and remediation interfaces.

Once the community has built a bedrock of understanding of elderly attitudes, the next step will be to design novel interfaces for interacting with home network security systems. It is important to ensure design is performed *with* the target demographic, and not just with an understanding of their expectations. This can be accomplished by (i) iteratively designing, developing and evaluating prototypes of security stewardship user interfaces, and (ii) conducting participatory design sessions (similar to Ambe et al. [1]).

We also believe interfaces by themselves are not sufficient to entail productive interaction with the user. Questions concerning the *language* that should be used to explain security facts are crucial, as the same fact (e.g., a smart camera compromise) can be explained in ways which generate panic (someone is spying on me!), cause confusion (what is an IP address?), or produce an appropriate response (it may be wise to turn off the camera). The choice of appropriate language can again be determined by iterative and/or participatory design.

5.2 Interpretation and Explanation Algorithms

The gap we highlighted in existing knowledge is largely related to human factors. However, our research question (ii) (How can low-level network signals be mapped to understandable explanations?) necessitate different, algorithmic solutions. The question is non-trivial, and requires novel research to be solved. Note that, as a corollary, we do not believe producing new network monitoring algorithms to be a priority; designing techniques that can explain the output of existing algorithms is more important.

The problem of mapping low-level events identified by network monitoring systems to higher-level alerts has been studied in the domain of enterprise security. We expect those techniques to be relevant here. In the field of intrusion detection, root cause analysis (see for example Julisch [17]) combines a large number of low-level events (e.g., individual anomalous network flows) into a high-level event causing them (e.g., evidence of an ongoing port-scanning operation). This can be accomplished for example by clustering individual alerts, possibly mapping the resulting cluster centroids to likely root causes. While this operation does not solve the explainability problem, it produces high-level data that may be easier to analyze and interpret than individual alerts. As machine learning is widely deployed for identification of network attack, the concept of explainability of machine learning models also becomes important. Explainable models are those whose decisions (e.g., flagging a device as compromised) can be partly explained by mathematical analysis, for example by identifying which features of the input are most relevant for decisions [7].

None of the techniques above solve the issue of plainly explaining an alert raised by an algorithm to a non-technical user. However, they can act as a starting point to develop novel techniques for understandable security alerts.

6 CONCLUSIONS

In this article, we highlighted how the poor security of smart home devices can negatively affect their potential to improve the quality of life of the elderly. After motivating the necessity for tools that can assist users in securing their devices, we argued that such tools must (i) be network-based, i.e., identify attacks by analyzing device network traffic; and (ii) keep the user in the loop, i.e., interact with the user to solve security problems.

We further identified the three concepts of autonomy, control and delegation as design principles to guide the design of future network security systems created for the elderly. We summarized those three requirements using the core concept of *explainable stewardship*: the fact that network security tools should work autonomously when possible, and involve the user using understandable language when an autonomous response is not possible.

Overall, we hope our work will highlight gaps in the existing understanding of the relationship between the elderly and the security of their smart devices, and act as a call for more research in this area.

ACKNOWLEDGEMENT

The work of Indrakshi Ray was supported in part by funds from NSF under award number CNS 1822118 and from NIST, Statnett, Cyber Risk Research, AMI, and ARL.

REFERENCES

[1] Aloha Hufana Ambe, Margot Brereton, Alessandro Soro, Min Zhen Chai, Laurie Buys, and Paul Roe. 2019. Older People Inventing Their Personal Internet of Things with the IoT Un-Kit Experience. In *ACM CHI*.

[2] Manos Antonakakis, Tim April, Michael Bailey, Matthew Bernhard, Elie Bursztein, Jaime Cochran, Zakir Durumeric, J Alex Halderman, Luca Invernizzi, Michalis Kallitsis, Deepak Kumar, Chaz Lever, Zane Ma, Joshua Mason, Damian Menscher, Chad Seaman, Nick Sullivan, Kurt Thomas, and Yi Zhou. 2019. Understanding the Mirai Botnet. In *USENIX Security Symposium*. 19.

[3] Stefan Axelsson. 1999. The Base-Rate Fallacy and Its Implications for the Difficulty of Intrusion Detection. In *ACM CCS*.

[4] Jeremy Birnholtz and McKenzie Jones-Rounds. 2010. Independence and Interaction: Understanding Seniors' Privacy and Awareness Needs for Aging in Place. In *ACM CHI*.

[5] 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 Southern University.

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

[7] Brandon Carter, Jonas Mueller, Siddhartha Jain, and David Gifford. 2019. What Made You Do This? Understanding Black-Box Decisions with Sufficient Input Subsets. In *AISTATS*.

[8] Marco Caselli, Emmanuele Zambon, Robin Sommer, Frank Kargl, and Johanna Amann. 2017. Specification Mining for Intrusion Detection in Networked Control Systems. In *USENIX Security Symposium*.

[9] Catalin Cimpanu. 2018. IoT Botnet Infects 100,000 Routers to Send Hotmail, Outlook, and Yahoo Spam. https://www.zdnet.com/article/iot-botnet-infects-100000-routers-to-send-hotmail-outlook-and-yahoo-spam/

[10] Catalin Cimpanu. 2019. IoT Botnet Used in YouTube Ad Fraud Scheme. https://www.zdnet.com/article/iot-botnet-used-in-youtube-ad-fraud-scheme/

[11] David M Cook, Patryck Szewczyk, and Krishnun Sansurooah. 2011. *Securing the Elderly: A Developmental Approach to Hypermedia Based Online Information Security for Senior Novice Computer Users.* Technical Report 12223. Security Research Centre, Edith Cowan University.

[12] Lorenzo De Carli and Antonio Mignano. 2021. Network Security for Home IoT Devices Must Involve the User: A Position Paper. In *FPS*.

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

[14] Wenbo Ding and Hongxin Hu. 2018. On the Safety of IoT Device Physical Interaction Control. In *ACM CCS*.

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

[16] 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 Transactions on Computer-Human Interaction* 16, 2 (June 2009), 8:1–8:28.

[17] Klaus Julisch. 2003. Clustering Intrusion Detection Alarms to Support Root Cause Analysis. *ACM Transactions on Information and System Security* 6, 4 (Nov. 2003), 443–471.

[18] Bethany Kon, Alex Lam, and Jonathan Chan. 2017. Evolution of Smart Homes for the Elderly. In *WWW '17 Companion*.

[19] Brian Krebs. 2017. Dahua Backdoor — Krebs on Security. https://krebsonsecurity.com/tag/dahua-backdoor/

[20] Brian Krebs. 2018. Naming & Shaming Web Polluters: Xiongmai — Krebs on Security. https://krebsonsecurity.com/2018/10/naming-shaming-web-polluters-xiongmai/

[21] Celine Latulipe, Syeda Fatema Mazumder, Rachel K. W. Wilson, Jennifer W. Talton, Alain G. Bertoni, Sara A. Quandt, Thomas A. Arcury, and David P. Miller, Jr. 2020. Security and Privacy Risks Associated With Adult Patient Portal Accounts in US Hospitals. *JAMA Internal Medicine* 180, 6 (June 2020), 845–849.

[22] Celine Latulipe, Sara A. Quandt, Kathryn Altizer Melius, Alain Bertoni, David P. Miller Jr, Douglas Smith, and Thomas A. Arcury. 2018. Insights Into Older Adult Patient Concerns Around the Caregiver Proxy Portal Use: Qualitative Interview Study. *Journal of Medical Internet Research* 20, 11 (2018).

[23] Hui Liu, Juanru Li, and Dawu Gu. 2020. Understanding the Security of App-in-the-Middle IoT. *Elsevier Computers & Security* 97 (Oct. 2020).

[24] Sumit Majumder, Emad Aghayi, Moein Noferesti, Hamidreza Memarzadeh-Tehran, Tapas Mondal, Zhibo Pang, and M. Jamal Deen. 2017. Smart Homes for Elderly Healthcare—Recent Advances and Research Challenges. *Sensors* 17, 11 (Nov. 2017).

[25] Kieren McCarthy. 2019. Here's a Great Idea: Why Don't We Hardcode the Same Private Key into All Our Smart Home Hubs? https://www.theregister.com/2019/07/03/zipato_hardcoded_key/

[26] Yisroel Mirsky, Tomer Doitshman, Yuval Elovici, and Asaf Shabtai. 2018. Kitsune: An Ensemble of Autoencoders for Online Network Intrusion Detection. In *NDSS*. Internet Society.

[27] Norbert Nthala and Ivan Flechais. 2018. Informal Support Networks: An Investigation into Home Data Security Practices. In *SOUPS*.

[28] Charles Perrow. 1999. *Normal Accidents: Living with High-Risk Technologies.* Princeton University Press, Princeton, N.J.

[29] Robin Sommer and Vern Paxson. 2003. Enhancing Byte-Level Network Intrusion Detection Signatures with Context. In *ACM CCS*.

[30] 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 (Dec. 2009), 788–801.

[31] Curtis R. Taylor, Craig A. Shue, and Mohamed E. Najd. 2016. Whole Home Proxies: Bringing Enterprise-Grade Security to Residential Networks. In *IEEE ICC*.

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

[33] Amy B. Wang. 2018. 'I'm in Your Baby's Room': A Hacker Took over a Baby Monitor and Broadcast Threats, Parents Say. *Washington Post* (Dec. 2018). https://www.washingtonpost.com/technology/2018/12/20/nest-cam-baby-monitor-hacked-kidnap-threat-came-device-parents-say/

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

[35] Serena Zheng, Noah Apthorpe, Marshini Chetty, and Nick Feamster. 2018. User Perceptions of Smart Home IoT Privacy. *Proceedings of the ACM on Human-Computer Interaction* 2, CSCW (Nov. 2018), 1–20.