Security for the Collective Reality of the Smart Home

Ross Koppel
Department of Sociology
University of Pennsylvania
rkoppel@sas.upenn.edu

Jim Blythe
Information Sciences Institute
University of Southern California
blythe@isi.edu

Vijay Kothari
Department of Computer Science
Dartmouth College
vijayk@cs.dartmouth.edu

Sean W. Smith
Department of Computer Science
Dartmouth College
sws@cs.dartmouth.edu

ABSTRACT

A single end user will struggle to configure a single "smart" device. However, the problem of securing the smart home is often exponentially worse due to the existence of multiple users, multiple devices, and the complex web of interconnections among these users and smart home devices. In this paper, we enumerate three key challenges and their subchallenges, which emerge when we consider this collective reality.

1. INTRODUCTION

A single user will find it difficult to understand and configure the security settings of a smart home device, be it a baby monitor, a doorway video camera, or a smart refrigerator. This difficulty exists even when we consider a single user and a single smart home device. However, this problem becomes significantly more complex when we consider a collective reality involving many different users, many different smart home devices, and various interconnections among these users and devices. Indeed, as recent work by Zeng et al. [9] reveals, user mental models and risk mitigation strategies pertaining to smart home security are often inadequate— and they may result in users configuring their devices in a manner that does not align with their intentions. Given the intrinsic complexity of the smart home, which may entail many ad hoc and often unintended networks of devices that users live with and depend upon, what measures can be taken to help users to achieve the desired security and privacy settings for their smart home?

The smart home has rightfully generated great interest among security and privacy researchers. For some examples: Some research aims to improve our conceptualization of security and privacy concerns within the smart home, e.g., Denning et al. [2] propose a wonderful taxonomy of goals for securing the modern home and a risk evaluation framework for devices within it. Interesting attacks on smart home devices have been demonstrated, e.g., Ronen et al. [7]. User perceptions of various aspects of the smart home have been an area of interest, e.g., Wilson et al. [8]. Data visualization techniques have also been proposed to help users reason about smart home security and privacy, e.g., Dirkzwager et al. [4].

In this work, we focus on three key challenges to address the collective vulnerabilities of smart homes. In addition to the multitude of devices, we consider the multiple stakeholders, e.g., users, device manufacturers, installers, potential third parties that may help set policy and provide aggregating tools. We also briefly reflect on the difficulty of addressing these challenges when taken together as a whole. We hope this exploration will stimulate discussion that fosters the development of solutions for securing the smart home moving forward.

2. CHALLENGES

Below, we list three key challenges to securing the smart home in light of the collective reality presented by various smart home devices and multiple stakeholders. While the list is not exhaustive, we believe it touches on many challenges with securing the smart home.

Challenge 1: End users must be able to implement security and privacy settings for the collective population of devices in the smart home.

- Human-computer interfaces must allow end users to configure each device's individual security controls, but they should also provide users with a way to express the users' desired security settings for the collective population of devices—as the interaction of two or more devices may create threats not present in any one device (e.g., as noted by Denning et al. [3]). These considerations prompt important questions when considering the security of smart home devices: Are there security settings that allow users to express their security preferences over the smart home network including all its complexity? That is, can users be reasonably certain that the interactions of their smart home devices in ad hoc or even in intentional networks can be configured to achieve their complex security needs?
- It is insufficient for interfaces alone to reflect these

USENIX Symposium on Usable Privacy and Security (SOUPS) 2018.
August 12–14, 2018, Baltimore, MD, USA.

complex interactions. Software and hardware updates must also reflect the collective security settings that affect the entirety of the smart home and the separate IoT devices within it, e.g., firmware updates, new (paid) versions, use of security software.

- There are many users— witting or unwitting— of smart home devices. A resident may believe she is using a smart home device only when she intends to; however, she may also inadvertently interact with a smart home device. For example, an ad campaign [5] or even background noise [1] may trigger a smart home device, changing its state from inattentive to keenly listening. A friend may visit and unwittingly have information about them collected. Multiple users may live in the same household, but the smart home devices may belong to a single individual. Perhaps a child is using an internet-connected toy bought by the parent [6]. Best efforts should be taken to ensure the security and privacy settings for these devices align with user expectations. Users should also be able to express their preferred settings. Moreover, as user behavior in the home is ultimately dictated by user beliefs and expectations regarding devices in the home, information should be provided to users to ensure these beliefs and expectations coincide with the reality.

- Products should be developed to test, evaluate, and express the collective security of the smart home in pursuit of empowering the user to make better security decisions for their smart homes. These products should:

  - display easily-interpretable collective security information to end users.
  - allow users to easily make improvements and changes.

- Functionality and controls should provide end users with the ability to allow or to prohibit the collection and transmission of data from the smart home or IoT devices as they interact with each other, e.g., smart watch or exercise equipment reports of physical activities, alcohol consumption to medical insurance carriers, smart refrigerator inventory data to local grocery stores or advertisers.

Challenge 2: Information should be provided to end users to help them reason about collective (network) security. That is, information should seek to accomodate and expand users' mental models of what is possible and what can be accomplished.

- Comprehensible security instructions, explanations, and general knowledge should be provided to help end users make well-informed decisions that conform to their intentions. This information should be provided not only to help users think about and ultimately configure the individual security of devices, but also for the collective (network) security and privacy properties they desire.

- Previous work by Zeng et al. suggests a multitude of different mental models for reasoning about smart home security and privacy [9]. The information presented to users should empower them to configure their devices so that desired properties within their mental model are upheld in reality.

- There should be clear visualizations of connections and links from smart home devices to other IoT devices, including those that may not be in the home or home network, but may nevertheless affect overall security, e.g., automobile entertainment systems, purchases at on-line stores, cell phone locations and cell phone use. Data and data visualization techniques may also be useful to those whose data are not collected, e.g., a caregiver.

- Some people may argue that there should be less focus on giving information to the user and having them configure devices— and that, instead, we should focus on having these devices automagically do what the user wants. This begs the question: should we make decisions for the user or should we aim to provide users with information so that they are best equipped to make decisions for themselves? Given the caveat that either approach may produce an undesirable outcome for the user, what are the usable and ethical trade-offs between different approaches? How should we balance them and best serve the user?

Challenge 3: Security policies and regulations should reflect the collective reality of devices and users.

- As with the tragedy of the commons, some solutions require policies that incorporate more than one developer and more than one user. That is, a societal-level or industrial-level policy–perhaps by the government, industry association, or insurance companies in concert–needs to provide a framework that addresses the exponentially expanded vulnerabilities created by many unknown combinations of IoT devices that may be interacting. This is a problem that is not limited to individual manufacturers. While device developers have the responsibility to provide secure settings for their own devices, they will probably not be aware of the other devices present in the home. They are also not aware of shortcuts and workarounds in use at the home, which may be motivated by a combination of other devices yet centered on their own. That is, there's a mismatch between what the developer considers reasonable when thinking about their own suite of IoT devices, and what is needed at a policy-level in light of the complexity of the smart home.

  Such policies must also extend to those who implement complex systems. Do they carry any, some, or all of the responsibility for the security of the devices they install? Cynically, this situation might also lead to a culture of plausible deniability for the IoT developer. A third party who takes on security for the home as a whole might be needed, but how are we to ensure they act responsibly? Are there any regulations for such participants? Need there be codes of ethics or expectations? How are delinquent players to be sanctioned? How are conscientious firms to be incentivized and promoted? Should policy extend to evaluations and recommendations?

- Policy options may include:

  - industry standards that reflect pan-device vulnerabilities
  - required human agent modeling of behaviors in situ
  - required test beds that reflect multiple devices used together and model likely human behavior across the devices
  - legislation
  - insurance company requirements for security and reporting, e.g., an analogy to the underwriters laboratory (UL) for cybersecurity in multi-device, complex settings.

- Requirements for transparency of data collection and data use:
  - What data do the IoT devices collect? What information do the many devices convey when collectively combined?
  - With whom are those data shared–especially in light of the reality that there are probably many vendors?
  - What protections are there for data privacy, not only individually, but in concert?
  - If there is an effort to anonymize data, is that effort defeated when data from several sources are combined?
  - How will the data be used by the many and differing entities that receive them?
  - Do one or more companies collect more or different information than the user expects (even the user who reads all privacy policies)? For example, recent work reveals that smart devices are collecting audio data beyond the realms of what humans can hear [10]. How can the several entities with access to the data separate out only the data that may be relevant only to them? Is any effort at disaggregation even attempted?

We note that simultaneously achieving each of these sub-challenges is non-trivial and may even be a fool's errand, not only in practice, but also in theory. Given this complexity, how do we go about precisely defining these challenges and sub-challenges. If we can't achieve every sub-challenge, how do we strike the right balance? And how do we go about enacting the requisite changes to the smart home industry to realize these objectives?

3. CONCLUSION

Humans struggle to secure their devices. Some of the blame is due to: unwieldy user interfaces and cumbersome controls to configuring devices' security settings (e.g., daunting menus that have sub-menus, sub-sub-menus, and so forth); instructions may be opaque or worse; and manufacturer-supplied "explanations" assume a level of computer knowledge few users possess. The struggle to correctly configure the security and privacy settings of devices is exponentially increased by introducing many devices in concert that interact with each other in ways that few understand. Added to this, the hardware and software of individual devices are often not developed with the need for networked security. The legacy of stand-alone hardware predominates even when the products are marketed for complex settings.

We suggested three challenges required to address the enhanced vulnerabilities created by the IoT in larger systems and smart homes: (1) reducing users' struggles with effecting collective (network) security and privacy settings; (2) expressing the complexity of collective (network) security to laypersons in a way that conforms to their mental models and enables them to make better decisions; and (3) ensuring security policies incorporate the collective reality of interacting systems. While we only outlined needed steps, we hope the presentation of these three challenges may advance discussion of the needed solutions for collective smart home security.

Acknowledgements

We appreciate the valuable feedback provided by the reviewers.

4. REFERENCES

[1] Max Barr. Amazon responds after Portland woman claims Alexa records private conversation. WFMYNews2. `https://www.wfmynews2.com/article/tech/amazon-responds-after-portland-woman-claims-alexa-records-private-conversation/283-557963237`, 2018.

[2] Tamara Denning, Tadayoshi Kohno, and Henry M Levy. Computer security and the modern home. *Communications of the ACM*, 56(1):94–103, 2013.

[3] Tamara Denning, Cynthia Matuszek, Karl Koscher, Joshua R Smith, and Tadayoshi Kohno. A spotlight on security and privacy risks with future household robots: attacks and lessons. In *Proceedings of the 11th international conference on Ubiquitous computing*, pages 105–114. ACM, 2009.

[4] Aimee Dirkzwager, J Cornelisse, T Brok, and L Corcoran. Where does your data go? Mapping the data flow of Nest. *Masters of Media*, 2017.

[5] Sapna Maheshwari. Burger King 'O.K. Google' Ad Doesn't Seem O.K. With Google. The New York Times. `https://www.nytimes.com/2017/04/12/business/burger-king-tv-ad-google-home.html`, 2017.

[6] Emily McReynolds, Sarah Hubbard, Timothy Lau, Aditya Saraf, Maya Cakmak, and Franziska Roesner. Toys that listen: A study of parents, children, and internet-connected toys. In *Proceedings of the 2017 CHI Conference on Human Factors in Computing Systems*, pages 5197–5207. ACM, 2017.

[7] Eyal Ronen, Adi Shamir, Achi-Or Weingarten, and Colin O'Flynn. Iot goes nuclear: Creating a zigbee chain reaction. In *Security and Privacy (SP), 2017 IEEE Symposium on*, pages 195–212. IEEE, 2017.

[8] Charlie Wilson, Tom Hargreaves, and Richard Hauxwell-Baldwin. Benefits and risks of smart home technologies. *Energy Policy*, 103:72–83, 2017.

[9] Eric Zeng, Shrirang Mare, and Franziska Roesner. End User Security & Privacy Concerns with Smart Homes. In *Symposium on Usable Privacy and Security (SOUPS)*, 2017.

[10] Guoming Zhang, Chen Yan, Xiaoyu Ji, Tianchen Zhang, Taimin Zhang, and Wenyuan Xu. Dolphinattack: Inaudible voice commands. In *Proceedings of the 2017 ACM SIGSAC Conference on Computer and Communications Security*, pages 103–117. ACM, 2017.