Security Begins at Home: Everyday Security Behaviour and Lessons for Cybersecurity Research

ERIC SPERO, Carleton University
ROBERT BIDDLE, Carleton University

An important challenge in cybersecurity is that many users have only weak understanding of the threats involved, and the defences against them. This means that, even when defences are available, user behaviour sometimes allows successful attacks. In the everyday world, however, most people have well-established security practices, and we speculate that learning about these practices might help identify patterns for software to better support secure user behaviour. This papers presents a focus group we conducted to start learning about the everyday security practices of people. Our analysis of the discussion shows several themes, including the role of context, various forms of dissuasion, checking before and after an absence, monitoring while away, and forms of insurance should an attack be successful. Overall, we came to see there was a cycle of behaviour from being at *home*, where people felt safer, and *away*, where risks were expected. We consider how these themes and the overall cycle might apply to cybersecurity.

Categories and Subject Descriptors: K.6.5 [**Management of Computing and Information Systems**] Security and Protection; H.1.2 [**Models and Principles**]: User/Machine Systems—*Human Factors*

General Terms: Usable security

Additional Key Words and Phrases: Human-computer interaction, cybersecurity, mental models

ACM Reference Format:

Spero, E. and Biddle, R. 2019. Security Begins at Home: Everyday Security Behaviour and Lessons for Cybersecurity Research. HILLSIDE Proc. of Conf. on Pattern Lang. of Prog. 26 (October 2019), 9 pages.

1. INTRODUCTION

We are interested in learning more about the security practices people use in their everyday lives, with future plans to support these practices in software. Examples of everyday security practices might include using a key to lock your front door, and then trying to open it to ensure it's locked, and concealing valuables in the back seat of a car.

Much of life is now lived online, so cybersecurity is now critical for everyone. Support for security must involve network and software infrastructure, (for example, see the patterns identified in Schumacher et al. [2006]), but also consideration of user behaviour and user interfaces. This paper presents a study which is part of a larger project that takes the latter approach to improving software security. We would like to help users develop richer understandings of concepts related to cybersecurity so that they can better defend against attacks.

According to an influential line of cognitive science research, people make decisions based on their understanding of the world, which takes the form of internal representations called *mental models* [Craik 1943; Johnson-Laird 1983]. Mental models are created in response to observations of events in the world—with special attention to their causal properties. Mental models work in the same way as their real-world counterparts, which means they can be used to simulate behaviour and its consequences before acting. The prevalence of cybersecurity incidents related to poor security behaviour [Leach 2003] suggests a need for improved mental models related to cybersecurity.

In their day-to-day lives, people use strategies for ensuring their security, and we think that learning about these strategies could provide important lessons for cybersecurity researchers. For example, we think it is possible that some problems arise with computer security because of differences between the real world and the online environment. Before starting this project we were not able to find extant research on the security strategies people use in their everyday lives; the work we present here is therefore an attempt at a "new beginning" to identify ways we can improve cybersecurity.

We conducted a focus group on everyday security behaviour with seven attendees of the 26th Conference on Pattern Languages of Programs[1]. We describe our methodology in Section 2, and in Section 3 we present a summary of the key themes of our group discussion. We find that these themes relate to each other in important ways: We noticed that the behaviours were essentially tied to *place*, namely behaviours enacted while at *home* and behaviours enacted while *away* from home. We also noticed that these behaviours could be ordered sequentially relative to one another inside cycles of *going away* and *returning home*. The cycle evolves over time as the person gains experience, influencing future behaviours. In Section 4 we describe a model that captures these relations. Finally, we extract a set of lessons which could be useful for cybersecurity research and in the development of software, which are described in Section 5.

2. PROCEDURE

In a focus group setting, the interviewers' control is necessarily limited. Our role in the discussion was to stimulate and steer conversation. We prepared a series of questions beforehand designed to elicit reports of our participants' everyday security behaviour without suggesting any particular behaviour. We began by asking "do you engage in any special behaviours for security purposes?" and let the conversation evolve. When the conversation stayed on the same topic too long, we would attempt to shift the topic by asking other questions. We asked what kinds of things participants tried to keep secure, under what circumstances would they engage in security-preserving behaviour, how they measured the success of security behaviours, how they know when their behaviour is 'complete', and whether these behaviours have changed over time.

During the conversation we took notes, and we recorded audio so that we could revisit the conversation in cases where our notes needed clarification.

Data Analysis

We performed a thematic analysis of the data gathered. This started with us going through our notes and the audio recording and identifying participant responses which related to everyday security behaviours. We tagged each of these quotes according to one or more themes (i.e. categories). These themes make up the subsections in Section 3. We then found relations between the themes, and developed a model that describes these relations. This model is described in Section 4.

3. THEMES

3.1 Context

The security behaviours people deploy varies depending on contextual factors. People appear to be relying on a model of the adversary, including what attracts them to a target, when they typically carry out attacks, their demographic characteristics, and their number in the environment. Many reported participant behaviours were linked to a prior experience where they felt unsafe, and their present behaviours were designed to prevent a similar situation from occurring again.

3.1.1 *Knowledge of Adversary.* It was suggested by some participants that the socioeconomic status of a person predicts the likelihood that they will commit a theft. P3 says that he does not believe this to be true

[1] This study was cleared by our Research Ethics Board (Clearance # 111506).

where he lives, claiming that he does not regard those of relatively low wealth as threats, as this group tends to be highly religious, and of good moral character. Rather, the thieves who commit home break-ins in his area are “professionals” who are highly calculating in selecting their target and carrying-out the theft. He therefore carefully manages his appearance and the appearance of his possessions so that he appears unappealing to these professional thieves.

P1 remarked that what they do depends on the country they are in. When in a developing country they are careful not to leave valuable electronics unattended where they might get taken, but in developed countries they feel more free to leave valuables unattended. P2 agreed that the level of economic development of the country they are in is an important factor: in developing countries they feel it is more important to protect their valuables. But they also note that even within rich countries such as the United States there can be areas where one should be as mindful about protecting valuables as in developing countries.

If P1 is leaving his home, his practices depend on the distance he will be from his home, and the amount of time he will be away. He will lock his house if he is leaving town, but not if he is walking to the local coffee shop.

P3’s knowledge of the security dangers of his area inform his security behaviour. Where he lives there are people who “roam around looking for a house to break into”, so he is fastidious in his home security practices.

P4 works at a well-known American university, many of whose laboratories—including her own—are open to the public. Every day tourists and other people not affiliated with the university walk through her lab, which contains lots of expensive equipment. P4 does not worry in the slightest about these expensive items being stolen, and takes no special measures to ensure the security of these objects. When it comes to leaving expensive items publicly visible in her parked car, however, she has strict security practices. Each time she leaves her vehicle she checks to make sure nothing expensive is left inside; if her passengers have expensive items, they are required to take them with them.

3.1.2 *Bad Past Experiences Shape Present Behaviour.* A number of participants made explicit links between their present security behaviours and a negative prior experience. Every time P4 leaves her locked car in a public space she is careful to ensure that no valuable items are visible through the car windows. This behaviour is linked to a previous break-in of her vehicle, when an expensive laptop was stolen, and she had to pay the large cost of a replacement window. P1 was “taken advantage of” by someone close to him and whom he trusted. He installed security cameras inside his home, and is now more careful about whom he trusts. He seems to have an increased recognition of the importance of community and building relationships: everyone can keep a watchful eye on each other, increasing the chances of detecting criminal activity in an area. P3 has a rigorous set of security practices which he uses every day to minimize a security breach, which he attributes to growing up on a remote farm where he never felt safe. P5 used to leave her car unlocked when it was parked in her driveway at home. However, one night some event tickets and a pair of sunglasses were stolen from inside her car. Since that incident, she is always sure to lock her car.

3.2 Dissuasion

The theme with the highest number of instances of reported security behaviour was *dissuasion*, where people adopt a variety of strategies for reducing their appeal to adversaries. Reported strategies can be placed into one of five sub-classes of dissuasion. Four of them signal to adversaries that:

(1) they are low-value targets,
(2) they are capable of inflicting physical harm,
(3) they are present at the scene, or
(4) their property is protected.

Participants also:

(5) plant decoys (comparatively low-value items) to dissuade attackers from searching for higher-value items.

3.2.1 *Low Value.* P1 tries to minimize the number of valuable items they keep inside their home. This strategy is effective for protecting against adversaries who know what is inside one's home: P1 was previously the victim of a theft which was perpetrated by someone close to them, and this strategy is perhaps meant to reduce the possibility of this happening again. Similarly, P4 never leaves valuable items visible in her car to avoid tempting passers-by. As a general rule, P3 avoids owning expensive things because doing so increases the odds of a security breach.

P3 is careful to use his externally-visible property to communicate that they are less likely to possess valuable material goods than their neighbours. P3's home is in a suburb of a major metropolitan area. They drive an older pickup truck, which is unusual for inhabitants of his neighbourhood. The interior of the truck is kept messy: for example, they leave out used fast food packaging. This choice of vehicle and the condition in which it is kept is meant to communicate to outsiders several things, one of which is that they have less money than their neighbours, which makes them a relatively low-value target for thieves. P3 also places books in areas visible to the outside, which presumes hackers regard habitual readers as lower-value targets than non-readers.

3.2.2 *Dangerous.* P3 uses his personal appearance to signal that he is physically threatening. P3 is large in stature, and several times per day he walks up and down his street while attempting to look intimidating and mean. They try to look like the kind of person who owns a firearm. The appearance of his older pickup truck is meant to amplify this signal that they own firearms: they intend for it to call to mind the stereotype of a person who lives in a rural area, who owns firearms and is predisposed toward using them in self-defence or in defence of their property.

3.2.3 *Present.* A number of participants make efforts to appear like someone is present in their home when in actuality nobody is. The assumption being made is that thieves prefer to choose empty homes as targets because it is easier for them to commit a theft without facing negative consequences. P3 plays distinctive music throughout the day every day, both when they are home and when they are not. P5 leaves a light on inside when not at home. When P1 is away for an extended period of time he asks someone he trusts to pick up his mail for him, as accumulated mail is an obvious sign that the owner is away.

3.2.4 *Protected.* P5 and P6 note that iron bars on windows are often used as an effective countermeasure for theft. Would-be thieves would need heavy, expensive, and loud equipment with them to enter these homes through the window.

3.2.5 *Planting Decoys.* Several participants report planting decoys to help minimize the cost of a potential security breach. P1 carries with him a relatively inexpensive cellular phone with him to give to someone in the event of a mugging, in hopes that this would satisfy them while allowing him to keep his more expensive device. P3 carries a messenger bag with him when out in public, from which he has had items stolen from before. He places his wallet in a difficult to reach area of his bag. He also carries a second wallet which looks like it could be his main wallet except its contents are far less valuable. This second wallet is left in an easy-to-reach area, for the same reason P1 carries a second cellular phone. When P3 leaves his home for an extended period, he leaves relatively inexpensive jewellery in highly visible areas, and keeps more valuable jewellery in more difficult to find areas.

3.3 Pre- and Post-Checking

People perform verification methods to help verify that their property is secure. When they leave the house, P3 and P1 both check that the door to their home is locked by trying to open the door. P1 does the same for his windows, and verifies that his in-home camera is turned on. P1 also places objects like pieces of paper inside his door frame which will serve as an alert that someone has opened that door while he was away. P5 uses a remote device to lock her car, and listens for the 'click' locking sound before leaving her vehicle. When checking to see if there are any visible valuables in her car, P4 looks as if through the eyes of a would-be thief.

Upon entering his home for the first time after being away for an extended period, P3 will look for signs of a break-in, paying particular attention to out-of-place items. When P4 enters her car she similarly looks for signs that it has been broken into, which include an open glove box, an open centre console, and out-of-place items.

3.4 Monitoring

P1 has placed a camera inside his home with motion-detection capabilities, which he turns on before leaving the house. P1 also will let his neighbours know if he plans to be away from home for an extended period, so they can check on his house and let him know if anything is wrong.

3.5 Insurance

P3 is highly concerned about the loss of data related to his professional life, and has rigorous methods related to data backup which help ensure no data could ever be fully lost. Each hour, whatever he is working on is copied to multiple drives, which are presumably attached to multiple physical machines. Each hour a backup is also made to a remote server owned by a trusted colleague. Periodically, he brings physical drives containing backups to a friend's house and leaves them there unplugged. These practices ensure that P3's data is protected against ransomware attacks, the physical theft of his devices, and even catastrophic damage to one of the building the data is stored in. P4 is similarly unconcerned about the loss of her data because of cloud backups.

4. HOME-AWAY EVERYDAY SECURITY CYCLE

Our participants made a clear distinction between security behaviour when *home* and *away*. People are concerned about having their valuables stolen when away from home (or their vehicle), so when they are at home they do things to reduce the chance of a robbery occurring while they are out. Most of our themes can be situated in a short-term or long-term loop where they travel back and forth between home and away. Participant behaviours were strongly informed by two kinds of contextual information: past experiences of security incidents, and of their knowledge of the adversary. The diagram in Fig. 1 depicts these relationships between themes.

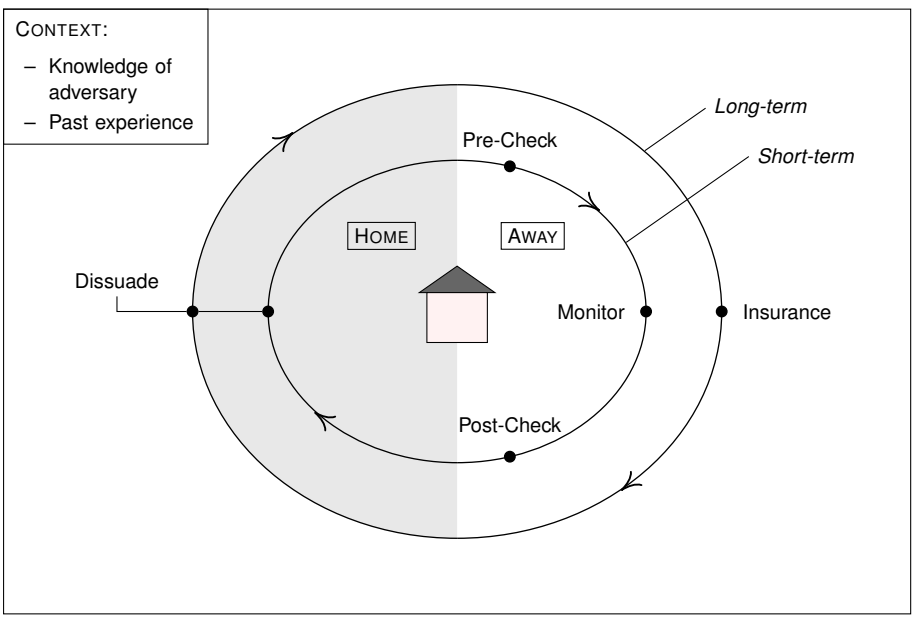

Fig. 1. Home-away everyday security cycle

Each of these short- and long-term cycles begins with dissuasion behaviours. Short term dissuasion behaviours include planting decoys, and signalling that they are protected and present. Both apply to situations where the attacker is physically near their home and potentially ready to attempt a breach of security. Long-term dissuasion strategies include signalling that they are a low-value target, and that they are dangerous. These behaviours are meant to dissuade attackers who observe potential targets over a prolonged period building a model which they will use to estimate the expected benefit of a security breach.

In the short-term, when leaving home (after performing dissuasion behaviours), the physical security status of the home is checked. They may look through windows to see if any valuable items are visible, and check that windows and doors cannot be opened by attempting to open them. While out, their home is being monitored for activity though video cameras. Upon returning to the home, they look for signs that their home has been unlawfully entered: for example, broken glass, items out of place, and triggered makeshift alarms (e.g. tape on a door frame). Curiously, home alarm systems were never mentioned in our discussions. These offer an effective form of short-term protection from security incidents which is a combination of protection-signalling and monitoring.

In the long-term, people have insurance procedures in place to replace and items which have been taken. One participant mentioned elaborate data backup processes. *Insurance* such as that provided by insurance companies was also conspicuously absent from our discussions, which is a form of financial protection from security incidents.

Regarding contextual information, our participants' reported behaviour could often be linked to a prior security incident, with the linked behaviour seemingly designed to prevent similar incidents from occurring again. Participants also appear to have a model of potential adversaries, which includes how they select potential targets, and how and under what circumstances they carry out security incidents.

This system is a cycle not just because they have a sequential order (i.e. post-check necessarily happens after a pre-check), but because earlier behaviours feed into later behaviours, locally and distally. For example, during pre-check, one might discover a flaw in their dissuasion technique: they may have left something valuable visible in the window, or they may have left the back door unlocked. Something similar may happen during post-check, where one finds signs of unlawful entry to the home. If this post-check discovery was due to an oversight in the pre-check routine, future pre-checks might also be modified as a consequence. As experience and knowledge of the adversary accumulate over time, this feedback loop hones behaviour and improves their security practices.

5. LESSONS FOR CYBERSECURITY RESEARCH

5.1 Key Differences Between Everyday Security in the 'Real' World and Online

The concepts *home* and *away*, which were important in user's security behaviour, are essentially physical. Home is a location, and anywhere outside the home is away. Home is a safe enclosed place (home or automobile), and it is safest when the homeowner is present. People's main expressed concerns were for physical things, and the farther one is from their home the less safe these things were—they are less able to protect them—and therefore the greater the need for performing dissuasive actions. This is true both of objects stored inside the home and automobiles, and objects carried on their person while they were away. When leaving home people ensure the security status of things like doors and windows, and when returning home they use the appearance of things to determine if their security has been breached.

Are these practices and associated concepts applicable to the world of cybersecurity? The two worlds are not as different as they may seem at first. Cybersecurity attacks happen through a casual chain of material interactions, and concepts such as value, harm, and security self are essentially non-physical: they only exist for human observers.

For us, the essential distinction between cybersecurity and real-world behaviour is that the causal properties of cybersecurity incidents are *invisible* to the naked eye, and therefore foreign to lived experience. For example, people know that locking their door when they leave home is effective in large part because they have been seeing and interacting with doors and door locks for their entire lives. Most people do not have any direct experience of

things like firewalls and encryption, so their implications for cybersecurity are unknown. End users are typically not able to establish a home for themselves in software.

However, a user's data is often stored at a distance (e.g. cloud services), which creates new cybersecurity challenges. In this case, people are never "with" their items of value, and users have far less control over the infrastructure which protects it. Users have means to access this data, but those means may become available to attackers, either by password attacks or by attacking the infrastructure. This situation is analogous to storing valuables in a bank (e.g. money or items in a safety deposit box). In such cases, user security relates to protection of credentials, and to choice of the organization and its ability to protect valuables.

5.2 Themes' Relevance for Cybersecurity

In this section, we reflect on how each of the themes of everyday security behaviour might be relevant for software design and use.

5.2.1 *Context.* To defend against any security threat, end users need a good model of the attacker, including their motivations and capabilities. Users' knowledge of cyber-adversaries is generally weak: Cyber-crime requires technical knowledge and the use of technical tools that far surpasses the knowledge and skill of most users. For example, users tend to assume that attackers attempting to commit online identity theft by guessing their particular password using known facts about them, and are not aware of strategies like dictionary attacks [Zhang-Kennedy et al. 2013]. Online services could provide updates to users about the kind of attacks they have detected lately to help users get a better understanding of what attacks are possible.

5.2.2 *Dissuasion.* Users can signal they are dangerous by curating their publicly-available information to make them appear so. For example, users could choose user names, wireless SSIDs, or write personal profile information to make them appear to be skilled computer users or law enforcement agents.

One can mask the value of public-facing services like web servers by, for example, choosing a non-default directory name, or placing something innocuous in a directory with the default name. Disabling `ping` on routers masks that there is a public-facing device at that location, and closing unused ports reduces the attack surface.

Protection can be signalled through two-factor authentication (2FA). Like iron bars on a window, 2FA makes it so that it takes an order of magnitude more effort to breach the target's security.

Signalling presence is much less effective in the online world, as attacks can be carried out while the user is present without them knowing.

Decoys were described by our participants are low-value items that dissaude attackers from looking for more. Similar practices are possible online, for example where important-seeming names are used for low-value documents or photos, and high value items are hidden elsewhere. More support would be possible, however, whereby higher-value items might be hidden by default. For example, online banking might show only low-value accounts, with higher-value account requiring access in-person.

5.2.3 *Pre- and Post-Check.* Behaviour we heard about several times from our participants involved checking the security of the house or car when they leave it, and checking for signs of theft when they return. In the online world a pre-check might involve making sure one is logged out after using services, but might also include using a password strength meter when creating a password. On social networks, it would also mean checking the access that others have to one's items. While services typically support this, it can be difficult and laborious [Lipford et al. 2010]. For post-checks, some services will display the time of last login, so users can check that was authorized. One can also check for suspicious activity when logging in, but it can often be laborious to check everything that has changed.

5.2.4 *Monitoring.* As our focus group showed, when people are away, they sometimes monitor their house or possessions. They might have security cameras with motion detection, or they might arrange for trusted friends to check periodically and contact them if something seems wrong. In the online world, there are some parallels to

this. For example, some services will send alerts by email or text message when an account is accessed from an unusual device or location. Other services, such as social media, might also alert you when there is benign activity that might warrant your attention or interaction. For many services, however, there is little support for alerting users to changes.

5.3 Contribution and Future Work

There is prior work in the study of everyday computer security behaviour (e.g. [Dourish et al. 2004; Ion et al. 2015; Vines et al. 2012]), but we could not find any prior research on the everyday physical security practices of typical people. To our knowledge, then, this study and its findings represents a unique contribution to the literature.

This study marks the inception of a new line of research, and there is much work to be done. Future studies should attempt to test the generalizability of our themes and model to the general population, perhaps in an online survey. Our ultimate aim is to see if these everyday security practices can be supported in software, so another focus group with cybersecurity experts may be useful.

Towards Patterns of Everyday Security Behaviour. It is too early to describe specific patterns of everyday security behaviour, however we do think the results of this focus group suggest some key elements of patterns, particularly *contexts* and *forces*. The key contexts for our participants' reported behaviour were *home* and *away*. It was not explicitly stated during our conversation, but presumably some important forces at work are *the need to keep oneself and one's possessions safe*, and a countervailing force of *the need to go out into the world to live their lives*. The world contains material and experiential rewards which are essential for supporting our quality of life. However, the world contains dangers, and while there one's home is more susceptible to security breaches. Forces relating to the adversary must also be considered when choosing one's security practices. Adversaries act under the force of needing to commit crimes, and to get as much value out of their exploits as possible, and countervailing forces of not wanting to be caught. This explains why, and the countervailing force of not wanting to be caught. This is the reason they do things like target high-value individuals, look for easy access to homes, wait until homeowners are away before attempting a breach.

We think many practices that came up in our conversation could in principle be straightforwardly described as a pattern for effective everyday security behaviour, and this should be the subject of future work. In addition, we believe that consideration of the contexts and forces our conversation revealed could yield entirely new patterns corresponding to behaviours which were not mentioned by our participants.

6. CONCLUSION

In this paper we reported on a focus group that explored the practices people use for every physical security. Our eventual goal relates to cybersecurity, and improving the design of software that people use to stay security online. The focus group was a starting point, and we hoped to learn things about their real-world behaviour that might help us identify ways to improve software design.

In our discussion, we found several common themes, and a common overall structure. People were aware of context, and then made preparations at *home*, for greater risks when *away*. We found several ways in which the themes relate to cybersecurity, but the distinction between home and away presents challenges in the online world.

Our analysis is based on a single focus group, so we must be cautious about any generalization. We are encouraged, however, that we found that the focus group partipants had clearly thought about the issues in some depth, and their security behaviour was conscious and principled. In further work, we home to further explore and develop the themes and models we identified, with the hope of identifying patterns to support better design for security software.

REFERENCES

Kenneth James Williams Craik. 1943. *The Nature of Explanation*. Cambridge University Press, Cambridge, UK.

Paul Dourish, Rebecca E Grinter, Jessica Delgado De La Flor, and Melissa Joseph. 2004. Security in the wild: User strategies for managing security as an everyday, practical problem. *Personal and Ubiquitous Computing* 8, 6 (2004), 391–401.

Iulia Ion, Rob Reeder, and Sunny Consolvo. 2015. "...no one can hack my mind": Comparing expert and non-expert security practices. In *Eleventh Symposium On Usable Privacy and Security (SOUPS 2015)*. USENIX Association, Ottawa, ON, 327–346.

Philip N. Johnson-Laird. 1983. *Mental Models: Towards a Cognitive Science of Language, Inference, and Consciousness*. Harvard University Press, Cambridge, MA.

John Leach. 2003. Improving user security behaviour. *Computers & Security* 22, 8 (2003), 685–692.

Heather Richter Lipford, Jason Watson, Michael Whitney, Katherine Froiland, and Robert W Reeder. 2010. Visual vs. compact: A comparison of privacy policy interfaces. In *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems*. ACM, ACM, Atlanta, GA, 1111–1114.

Markus Schumacher, Eduardo Fernandez-Buglioni, Duane Hybertson, Frank Buschmann, and Peter Sommerlad. 2006. *Security Patterns: Integrating Security and Systems Engineering*. John Wiley & Sons, Hoboken, NJ.

John Vines, Mark Blythe, Paul Dunphy, Vasillis Vlachokyriakos, Isaac Teece, Andrew Monk, and Patrick Olivier. 2012. Cheque mates: Participatory design of digital payments with eighty somethings. In *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems*. ACM, Austin, TX, 1189–1198.

Leah Zhang-Kennedy, Sonia Chiasson, and Robert Biddle. 2013. Password advice shouldn't be boring: Visualizing password guessing attacks. In *2013 APWG eCrime Researchers Summit*. IEEE, San Francisco, CA, 1–11.

PLoP'19, OCTOBER 7–10, Ottawa, Ontario, Canada. Copyright 2019 is held by the author(s). HILLSIDE 978-1-941652-14-5