Intentionality and agency in security

Kat Krol, David Llewellyn-Jones, Seb Aebischer,
Claudio Dettoni, and Frank Stajano

Department of Computer Science and Technology,
University of Cambridge, Cambridge, UK,
{kat.krol, david.llewellyn-jones, seb.aebischer,
claudio.dettoni, frank.stajano}@cst.cam.ac.uk,
https://mypico.org

Abstract. In this paper we explore the tension between automatic security and intentionality. During a user trial of Pico we offered two proximity authentication modalities: scanning a QR code, or pressing a button in the Pico app that is available only when the user is in Bluetooth range of a machine they can authenticate to. The feedback from this trial provides an insight into users' expectations with regard to intentionality. We discuss how this relates to the Pico authentication solution, how it has informed future Pico design decisions, and we suggest some ways in which security and usability researchers could address the issue of intentionality in future security design.

1 The user experience of security

Weiser [22] said that "the most profound technologies are those that [just blend in and] disappear". Security software has been at odds with this principle because it attempts to attract user attention whenever possible—it has been largely designed to be *visible* to the user and ask them to *take action*. For example, anti-virus software proudly tells the user how many viruses it has stopped, while websites display padlocks and security seals. Users are disrupted in their work by security notifications; they are asked to read warnings and decide whether they want to heed or ignore them.

One may question the motives behind software wanting to be more visible and requiring user action. Arguably, the best security experience would be that nothing bad ever happens, therefore good security should mitigate threats in the background and never be visible to the user. However, the parties offering security products aim to sell their offerings, and informing the user how effective they are is part of their sales strategy. Users should be satisfied that buying a security product to protect their devices is the right thing to do, and that they're not just wasting money on software that might not be doing anything at all. Vendors therefore design their products to make users aware of what the product is doing. At the heart of designing security software there has always been a conflict between truly effective security and business interests, as highlighted by Anderson [1].

Author preprint of 2018-06-22

More practically, when it comes to user actions, security software sometimes requires a decision from the user because it may not be ready to handle all situations. Often this boils down to a question of liability—by ignoring a warning, the user is forced to concede they are not making the company liable for any damage that might occur to their machine.

This sad state of affairs has led security researchers to argue that demanding more user attention and effort cannot be the way forward. Herley [8] emphasises that rejecting security advice may be rational from an economic point of view because certain security mechanisms are broken. For example, most certificate warnings are false positives and heeding them may cost users time and thus result in unfinished work. Elsewhere, Herley [9] calculates that, if every one of the two billion online users spends five seconds a day entering a password, this will result in a cost of 1,389 person-years of human effort per day. He stresses that human effort is a valuable resource and should be used wisely.

There has been a persistent view that "security has to be hard to be effective" and for many years now there has been a movement to blame failed security on a failure to educate users. As a consequence of this, people now feel their involvement in the security process is an intrinsic requirement for maintaining security. Users feel the need to perform certain tasks—security rituals, if you will—to ensure their active participation in the security process, even though in practice these tasks don't improve security in any tangible way, as shown in a study on 2-factor authentication in online banking by Krol *et al.* [12]. There remains a tension between automatic security and intentionality, which the security community must understand empirically if it is to truly achieve seamless security. In this paper, we will explore this tension, how it relates to the Pico authentication solution, and some of the ways security and usability researchers can attempt to address this in future security design.

2 Authentication and agency

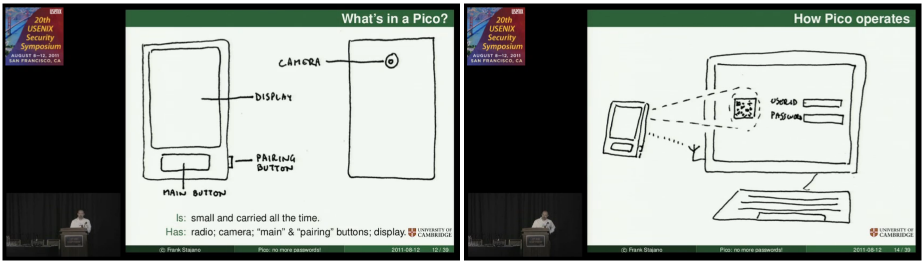
The user experience of passwords has not been great. Users today are asked to create a strong, long and unique password for various devices, websites and services. They are asked not to reuse passwords and to have a Chinese Wall in their head not mixing personal and work-related passwords. Despite passwords being a user experience disaster, alternatives have not taken off. Passwords are still superior on several security, usability and deployability fronts. Passwords are very flexible and alternatives might not offer enough control. It might be, for example, because some password alternatives do not support the features of passwords that users like, such as delegation: while it is easy to share your Facebook password with your best friend as a sign of trust, it is impossible to do so with something that is secured by biometrics. Users might be uncomfortable trusting a third party with access to all their accounts.

One of the fundamental considerations of human-computer interaction (HCI) is that there is a tension between human agency and computer agency—between how far the user has to express their intention as opposed to the computer anticipating user needs and taking action on their behalf.

Agency is related to the concepts of *automaticity* and *intentionality.* As devices and systems are becoming smaller and more pervasive, the user cannot keep making choices all the time and expressing their actions because it would be too time consuming, and it would require a user interface that isn't available, so there is a gradual shift towards more automaticity. There are many ways in which the user can indicate intentionality. Jia *et al.* [11] discuss the notions of *human and object agency* for Internet of Things (IoT) devices saying these can adopt more intuitive modalities such as input relying on movement and other natural actions. The authors bring up the example of E-ZPass tags which are active RFID transponders attached to a car that facilitate the collection of toll tax. As the car passes by a toll booth, the presence of a unique radio signature is registered and the driver is charged for the use of the motorway. The presence of the E-ZPass tag is sufficient for the car to be charged. There are alternative models across the world, commonly with gates where the user has to stop at a booth, queue until it's their turn, pay the toll by cash or card and only then can continue on their journey. Research by Currie and Walker [4] has demonstrated that E-ZPass has improved traffic fluidity, led to reduced congestion and air pollution, and improved health for those living in proximity of the collection areas. However, the E-ZPass has also attracted criticism from civil liberty campaigners [10] because a government agency has deployed E-ZPass readers throughout Manhattan at many more locations than needed for paying road tolls. Location data coming from the E-ZPass has also been used against the intended purpose. Ulatowski describes its regular use as evidence in civil lawsuits [21] for example; as often happens, we see here a tension between convenience and security/privacy.

Another example of intentionality in automatic payment is the deployment of contactless cards where the user only taps their card on a reader and no longer has to slot their card into a Point of Sale machine and enter their PIN. While contactless cards have a usability advantage in that the number of steps to make a payment has been reduced and the user no longer has to recall and enter their PIN, users have been worried about making accidental purchases without realising as shown in a study on payment methods by Krol *et al.* [13]. For example, Transport for London (TfL) allows passengers to pay for travel using either a dedicated travel smartcard—the Oyster card—or a contactless bank card. If the user taps their wallet containing both cards at an entry point to the London transport network, they might be charged on the card they did not intend to pay with. As a result, TfL [20] has been advising passengers to touch only one card on their card reader instead of a whole wallet in order to avoid a card clash. In terms of security, contactless cards have been demonstrated to be easy to attack as illustrated by Emms and colleagues [5,6] so users not only worry about accidental payments but also about attackers stealing their money.

There are similar problems in other mechanisms, for example in the case of smart keys for cars. When using a traditional key, the user expresses their


What's in a Pico?

Is: small and carried all the time.

Has: radio; camera; "main" & "pairing" buttons; display.

© Frank Stajano Pico: no more passwords! 2011-08-12 12 / 39

How Pico operates

© Frank Stajano Pico: no more passwords! 2011-08-12 14 / 39

Fig. 1: Ways of expressing intentionality for login with Pico as proposed by Frank Stajano in his USENIX 2011 talk [18]. On the left, a drawing of a Pico device shows a camera and a main button. On the right, scanning a QR code was proposed as a way of expressing the intention to log in.

intention to unlock the car (and *that* particular car) by taking their key out, putting it in the keyhole, turning it and opening the door. With a smart key, the user can just approach the car, keeping the key in their pocket, and the doors unlock and the engine starts without them having to touch their key. However, this great convenience and presumed intentionality can have security implications. Relay attacks have been demonstrated both in academic research by Francillon *et al.* [7] and real-life cases as publicised by the media [3]. If more intentionality was required and the user had to press a button on the key, the type of attack where someone else unlocks the car while the victim was otherwise concerned and didn't intend to unlock any car at all would be far less likely to succeed. What does this mean for computer security?

3 Intentionality and Pico

During the design of Pico [19,14], we have always worked from the assumption that users would want to explicitly express their intention as to whether they would like Pico to log them in or not. We first worked on Pico as a dedicated physical device and envisioned the user could express intentionality in different ways. In his talk at USENIX 2011 [18], Frank Stajano suggestioned that the user express intentionality by pointing the Pico's camera at a QR code and pressing a button (see Figure 1). Since then, the idea has evolved from a physical device to a smartphone application.

3.1 Our study

Between October 2016 and March 2017, we conducted a trial of the Pico smartphone application in our immediate environment, the University of Cambridge Computer Laboratory. It consisted of a four-week pilot with five participants and a ten-week main deployment with 13 participants using Pico to log in to their computers, periodically completing questionnaires and participating in a debriefing interview at the end. The login interaction was designed with intentionality in mind: in order to log in, the user had to take out their phone, unlock it, open the Pico app and then scan a QR code or tap a button.

3.2 Procedure

Participants were recruited through a department-wide call for participants sent to staff and students of the Computer Laboratory. We asked them to complete a pre-screening questionnaire to make sure Pico could be installed on their devices. At that time, we supported Windows (8 and higher), Ubuntu (16.04) and Android phones (4.4 and higher). We received 39 responses. After excluding those who were ineligible or did not respond to our emails, we obtained a final sample consisting of 13 participants and we were able to conduct interviews with 10 of them.

Once we established a participant's eligibility, we sent them an information sheet and a consent form that they were asked to read and sign. In the forms, they had the option to request access to the source code of the Pico software. We also encouraged participants to ask questions. They could hand in their signed consent form by either visiting our office or sending a scanned document by email. Before starting the trial, we offered every participant a Bluetooth dongle in case their computer did not already have Bluetooth hardware.

Once we ascertained eligibility and consent, we sent installation instructions to every participant via email. Two days after this, they received a feedback questionnaire asking them about the installation process and their experiences with Pico so far. Another questionnaire followed three weeks later and a final questionnaire another three weeks later. During this time, we could be contacted via email with any issues participants might have had. Depending on a participant's availability, they were invited for a feedback interview around 10 weeks after the installation. After the end of the trial, participants were free to continue or stop using Pico.

The study received an ethics approval from the Ethics Committee of the University of Cambridge Computer Laboratory (approval number: 404).

3.3 Research aims

Our goal was to explore the user experience with Pico when used to log in to a computer, either Linux or Windows. We offered our participants two ways of logging in, both involving the Pico app for Android—they could either open the Pico app on their phone and scan the QR code displayed on their computer screen or press a button within the app. Using the QR code option to log in required an Internet connection on both devices, while pressing a button inside the app required a Bluetooth connection between the computer and the phone as well. These two methods of logging in varied in terms of the interaction they required (scanning *vs* pressing a button) and the type of connection needed (Internet *vs* Bluetooth). User behaviour with QR codes has been studied academically

Fig. 2: A Bluetooth button inside the Pico app at the time of the study (blur added for emphasis).

before, for example by Shin *et al.* [17], and the results showed user acceptance to be strongly influenced by interactivity, meaning users saw scanning a QR code as a way to interact and engage with others. More broadly, one could interpret the result to mean that users were willing to scan QR codes if they saw them useful in achieving a certain goal. Using Bluetooth for login is a fairly new idea. At the moment, at least three commercial products use phone-based Bluetooth for authentication: SAASPASS lets the user log in using their phone [15], Apple Watch can be used to unlock a Macbook [2] and Windows offers a feature to lock your computer when your phone is absent [23]. However, we were unable to find any academic research studying user perceptions of and experiences with such solutions. Our study is therefore valuable in gauging participants' willingness to use Bluetooth to log in. While entering a password is very tangible because it requires cognitive and physical effort, scanning a QR code is less tangible and pressing a button even less so. Hence, our goal was to explore the user experience of these less tangible ways of expressing intentionality to log in.

3.4 Findings

In what follows, we present the qualitative and quantitative results of our study. While we do not present the quantitative results of the pilot study as we used preliminary versions of our questionnaires, we do include some of the participant quotes.

Overall perceptions There was a general perception that participants liked the 'coolness' of Pico. P01 (Windows)[1] explained: *"Overall, I liked it. [...] It was quite fancy, you scan a barcode and everything just turns on."* and later said: *"you need to open the app so it probably even takes more time but on the other hand, it is just cooler to do that."* P03 (Windows) stated *"It was mostly fun."* and went on to discuss some connectivity issues and bugs they encountered. PP2[2] (Ubuntu) told us: *"It's different from passwords, it's a fun thing to use."*

[1] With each new mention of a participant, we report the operating system they used Pico on.

[2] For quotes from pilot participants, we use the format of PPX, that is "pilot participant" followed by a number.

Experience of using Pico with QR codes and Bluetooth We received 13 responses to the post-installation questionnaire. Out of these 13 participants, seven were able to set up Pico to work with Bluetooth, which in practice meant going through the normal Pico setup procedure and then Bluetooth pairing their computer and phone through the standard interfaces on their devices. Three participants stated that they had not tried it yet. Two stated that it did not work for them, citing problems such as *"Do not know how to setup bluetooth on Xubuntu."*[3] (P09, Xubuntu) and *"I couldn't Bluetooth pair my phone with my computer."* (P05, Kubuntu). One participant stated that they preferred not to use Bluetooth, later explaining in their interview that the use of Bluetooth increased the number of channels through which their devices could be compromised, and that having Bluetooth on would drain their battery quicker.

We also asked participants who switched between login modalities (QR code and Bluetooth) about what influenced their choice of interaction. P03, who stated they used both modalities "50-50", explained: *"I don't know. I just sometimes would put the camera up. Sometimes... It depends. If my phone is already in my hand, I feel there is the Bluetooth button at the top."* PP3 (Ubuntu) preferred Bluetooth, saying: *"I'm using the Bluetooth a lot more than the scanning because the scanning is fiddly. Slightly fiddly to line this up on the screen get it to... It takes up to 10 seconds wobbling the phone around to get it to recognise the QR code but the Bluetooth is really good."* PP2 preferred scanning a QR code as they enjoyed the tangibility of the login process:

> *"I used the scan version more often than the Bluetooth one. I think because there is more physical action to doing it so... there is something more responsive about scanning than just press the button, I think. [...] because there is the physical action involved of you picking up and scanning the screen rather than pressing the button and sort of waiting for a little bit for the computer to respond."*

Later in the interview, PP2 and the interviewers speculated that a preference for QR codes or Bluetooth might be due to reliability—if the user's camera scans the QR code reliably, they would prefer this option, while if their Bluetooth is reliable, they might prefer that. PP2 elaborated: *"With Bluetooth, you are just pressing a button but there is no feedback as to what is going on. But I guess for people, for whom scanning doesn't work reliably, it's still better."*

Problems using Pico In all three questionnaires, we asked participants to report on any problems they had experienced while using Pico. All but one participant reported experiencing problems. In six out of 12 cases, the problems were related to connectivity; in most cases the participant did not have an Internet connection on their phone (but probably didn't notice it until they attempted to log in), while in isolated cases it was down to failure of the Bluetooth

[3] Any participant quotes coming from questionnaires are reproduced as written by our participants.

connection. It's worth mentioning that at this stage in Pico's development, an Internet connection was required in order to authenticate, independent of the use of Bluetooth. P03 explained their laptop had problems connecting to some WiFi networks:

> *"If I come up here [to the Computer Laboratory] and my laptop wants to connect to Eduroam, the first time it turns on, it won't automatically log on. [...] You can try to connect to Eduroam but the laptop won't do it because you have not logged in yet."*

Other problems could have had something to do with connectivity but they were mentioned in their own right. Two participants mentioned app crashes. Three participants felt Pico was slow to log them in. Another three participants mentioned a bug in our software whereby the password field would keep refreshing when their computer did not have an Internet connection.

Expressing intentionality Although a small-scale trial with computer scientists as participants, a large proportion of our participants felt the expression of intentionality that we required was too much—they didn't like to take out their phones, enter a PIN, go to the app and press a button to be logged in. P07 (Windows) explained:

> *"It would be better if it could work automatically. The requirement to press the button on my phone for the computer to unlock makes it more effort than a password."*

PP1 (Ubuntu) would have preferred a login mechanism that did not require them to take their phone out of their pocket:

> *"It would be better if I would be able to just not even have to click or choose maybe. Like, I feel it's alright if I rely on my Bluetooth sensitivity and say it's around a couple of metres from my machine and then and I'm fine to use it like that and I don't have to press anything. And once I get back in my room with my phone in my pocket, it unlocks."*

PP1 then immediately reflected on the security of this approach and explained that there are many parts to an attack:

> *"It is really hard to talk about these things, there is so many scenarios we can think about, like sometimes you have to balance, you have to trade off ease of use between actual need of security between how disciplined people are. [...] If I leave my phone like this and someone steals my phone, they can get into my account, these kinds of things. Then what happens once he gets to my computer? [...] But on the other hand, if he steals my phone and he already has access to my emails... You see, there are all sorts of different parts."*

This implies that every user would need to take the decision whether to use an automatic login based on their personal circumstances and context of use. P02 (Windows) explained in their interview that they would not like automatic login because of the particular threat model they have:

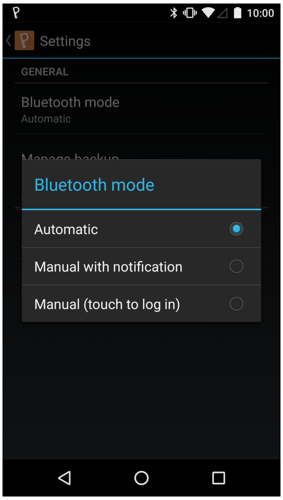
> *"The 'Log me in automatically as I approach' I actually don't want. I think this is the danger of you just walking past your computer and it unlocking. I don't really want that. It would also mean that somebody that stole my laptop out of my bag in a coffee shop, could sit behind me and use my laptop."*

3.5 Subsequent development of the Pico app

Even in a small sample like ours, we saw a great diversity in terms of preferences for expressing intentionality. These might have had to do with universal personal preferences but also with the risk levels the individuals perceived. When subsequently developing the Android application, we introduced three Bluetooth login modes that varied how much intentionality the user had to express (see Figure 3):

- *Automatic*: The user will always be automatically logged in when their phone is in range of a Pico-enabled computer.
- *Manual with notification*: When the user's phone is within range, Pico puts up a notification that appears in their phone's notification tray, with an accompanying vibration. The user can tap the notification to log in, without having to switch application.
- *Manual*: Each time the user wants to log in, they need to open the Pico app and press a button inside the app. In this case there is no notification, so the user makes their own assessment that they are within range of a Pico-enabled computer.

In the case of *automatic*, there is no action or intent required from the user. This means less effort for the user to log in, but with the associated risk that the user may be logged in to a machine without being aware. In the cases of *manual with notification* and *manual*, the user must make an explicit action on their phone, which may involve having to remove it from their pocket, and so comes with additional effort. However, the risk of the user being logged in to a machine without being aware of it is greatly reduced. The distinction between the two manual cases rests on whether the user wants to be made explicitly aware that a usable machine is nearby. In some cases this may be obvious for the user based on context (for example, if the user always logs in to the same machine at the same desk) and so no notification is needed. Indeed, notifications in this case may simply be an annoyance. However, in other cases, such as where a user is moving between machines, the notification may provide value. In both cases the user has chosen to require the affirmative action of tapping a button on their phone to log in.



GENERAL

Bluetooth mode
Automatic

Manage backup

Bluetooth mode

Automatic ●

Manual with notification ○

Manual (touch to log in) ○

Fig. 3: A screenshot of the Pico app for Android showing the three login modes, varying the level of intentionality the user has to express to be logged in.

A further mode, where the user is authenticated automatically but notified in a passive manner, such as through vibration, would address the case where the user is made aware, but only has to take action to reverse an unwanted authentication. This was not included in our trial, but would make an interesting topic to explore in future work.

4 Designing secure and usable systems

In common with Sasse *et al.* [16], we hold the belief that security designers should strive for products that excel in terms of both security and usability, avoiding any security-usability tradeoffs. However, the different login modes and ways of expressing intentionality highlight the tension between security (awareness and control over each login event) and usability (logging in without having to intervene manually) and allow the user to select the combination that best matches the risk context (logging in to a personal machine at home *vs* logging in to a hotdesking machine in an open plan office).

Although this provides flexibility, some will consider any request for user input as a cop-out: it pushes responsibility onto the user to decide and, if the security software can't figure out the appropriate response, the question being asked will sound like gobbledygook to the user, who will not be in a position to make an informed decision. If the designer wanted to choose ahead of time on behalf of the user, the dilemma is therefore whether to push the slider towards security (protecting but annoying the user) or towards usability (seamless operation but greater risk of attacks). We believe the slider should be set by default towards greater usability but also that people who, rightly or wrongly, don't feel secure without the added ritual should be offered the option to express their intentions more explicitly and to be notified of (and given a chance to block) any actions that are taken automatically on their behalf. There remains the question of how much responsibility the designer bears if a user falls prey to an attack when the default was set to favour usability. Avoiding such liability is probably one of the main reasons why most commercial software still pushes the choice onto the user.

5 Conclusion

Although only a small-scale trial, the feedback highlighted a number of interesting differences between participants. We allowed users the flexibility to authenticate either by scanning a QR code, or by touching a button in the Pico app that appears when in Bluetooth range of a Pico-enabled machine. There was no clear-cut overall preference for one or the other, but we could conclude that the expressed desire was towards a more seamless experience than towards more overt or demanding modes of expressing intentionality. The subsequent design of Pico has been adjusted based on these results and, as discussed above, we have identified four levels of intentionality that apply. Fully automatic login based on proximity remains the most controversial option, and we hope can be the subject of future work to identify where the appropriate balance lies between seamless usability and expression of intentionality. In particular, our hope is that future work will find the relationship between usability, intentionality and security as it applies to authentication and software security more generally.

Acknowledgements

We thank the European Research Council (ERC) for funding this research through grant StG 307224 (Pico).

References

1. R. Anderson. Why information security is hard – an economic perspective. In *Computer Security Applications Conference (ACSAC 2001)*, pages 358–365. IEEE, 2001.
2. Apple Support. How to unlock your Mac with your Apple Watch. https://support.apple.com/en-us/HT206995, January 2018.
3. BBC. 'Relay crime' theft caught on camera. http://www.bbc.co.uk/news/av/uk-42132804/relay-crime-theft-caught-on-camera, November 2017.
4. J. Currie and R. Walker. Traffic congestion and infant health: Evidence from E-ZPass. *American Economic Journal: Applied Economics*, 3(1):65–90, 2011.
5. M. Emms, B. Arief, L. Freitas, J. Hannon, and A. van Moorsel. Harvesting high value foreign currency transactions from EMV contactless credit cards without the PIN. In *Conference on Computer and Communications Security (CCS)*, pages 716–726. ACM, 2014.

6. M. Emms and A. van Moorsel. Practical attack on contactless payment cards. In *HCI2011 Workshop – Heath, Wealth and Identity Theft*, 2011.
7. A. Francillon, B. Danev, and S. Capkun. Relay attacks on passive keyless entry and start systems in modern cars. In *Network and Distributed System Secruity Symposium*, 2011.
8. C. Herley. So long, and no thanks for the externalities: The rational rejection of security advice by users. In *New Security Paradigms Workshop (NSPW 2009)*, pages 133–144. ACM, 2009.
9. C. Herley. More is not the answer. *IEEE Security & Privacy*, 12(1):14–19, 2014.
10. M. Hirose. Newly Obtained Records Reveal Extensive Monitoring of E-ZPass Tags Throughout New York. https://www.aclu.org/blog/privacy-technology/location-tracking/newly-obtained-records-reveal-extensive-monitoring-e-zpass, April 2015.
11. H. Jia, M. Wu, E. Jung, A. Shapiro, and S. S. Sundar. Balancing human agency and object agency: An end-user interview study of the Internet of Things. In *ACM Conference on Ubiquitous Computing*, pages 1185–1188. ACM, 2012.
12. K. Krol, E. Philippou, E. De Cristofaro, and M. A. Sasse. "They brought in the horrible key ring thing!" Analysing the usability of two-factor authentication in UK online banking. In *NDSS Workshop on Usable Security (USEC)*, 2015.
13. K. Krol, M. S. Rahman, S. Parkin, E. De Cristofaro, and E. Vasserman. An exploratory study of user perceptions of payment methods in the UK and the US. In *NDSS Workshop on Usable Security (USEC)*, 2016.
14. J. Payne, G. Jenkinson, F. Stajano, M. A. Sasse, and M. Spencer. Responsibility and tangible security: Towards a theory of user acceptance of security tokens. In *NDSS Workshop on Usable Security (USEC)*, 2016.
15. SAASPASS. About: What is SAASPASS? https://saaspass.com/about.html, February 2018.
16. M. A. Sasse, M. Smith, C. Herley, H. Lipford, and K. Vaniea. Debunking security-usability tradeoff myths. *IEEE Security & Privacy*, 14(5):33–39, 2016.
17. D.-H. Shin, J. Jung, and B.-H. Chang. The psychology behind QR codes: User experience perspective. *Computers in Human Behavior*, 28(4):1417–1426, 2012.
18. F. Stajano. Pico: No more passwords! https://www.usenix.org/conference/usenix-security-11/pico-no-more-passwords. Talk at USENIX Security 2011.
19. F. Stajano. Pico: No more passwords! In *Security Protocols XIX*, pages 49–81. Springer, 2011.
20. Transport for London. Card clash. https://tfl.gov.uk/fares-and-payments/oyster/using-oyster/card-clash, February 2018.
21. L. M. Ulatowski. Recent developments in RFID technology: Weighing utility against potential privacy concerns. *Journal of Law and Policy for the Information Society*, 3:623, 2007.
22. M. Weiser. The computer for the 21st century. *Scientific American Special Issue on Communications, Computers and Networks*, 265(September):94–104, 1991.
23. Windows Support. Lock your Windows 10 PC automatically when you step away from it. https://support.microsoft.com/en-gb/help/4028111/windows-lock-your-windows-10-pc-automatically-when-you-step-away-from, 2017.