Around Device Interaction for Inconspicuous Authentication?

James Nicholson
Culture Lab, School of Computing Science
Newcastle University, United Kindgdom
james.nicholson@ncl.ac.uk

Vasilis Vlachokyriakos
Culture Lab, School of Computing Science
Newcastle University, United Kindgdom
v.vlachokyriakos@ncl.ac.uk

Paul Dunphy
Culture Lab, School of Computing Science
Newcastle University, United Kindgdom
paul.dunphy@ncl.ac.uk

Patrick Olivier
Culture Lab, School of Computing Science
Newcastle University, United Kindgdom
patrick.olivier@ncl.ac.uk

CHI 2014 Workshop on Inconspicuous Interaction, April 26, 2014, Toronto, ON, Canada.

Abstract

New interactive technologies tend to bring new challenges and opportunities for designing inconspicuous interaction. In this short paper we discuss the viability of *Around Device Interaction* (ADI) as a method for inconspicuous user interaction. We firstly review related work in the HCI field in ADI, and then propose challenges and opportunities for ADI when applied to inconspicuous interaction.

Introduction

User authentication has become a requirement for everyday interaction with digital devices. The threat of shoulder surfing further disrupts the authentication experience. The obvious case that comes to mind is a stranger overlooking a victim to steal their PIN code, but it is possible for a friend, family member or colleague to obtain the login credentials by simply being in the vicinity of the interaction. While explicitly obscuring the interaction (e.g. by placing hands over keypad or screen) is a tried and tested method against unknown threats – that is not to say that users actually *do* use it – doing so amongst known people can be seen as distrusting and thus is less common.

Shoulder surfing on mobile devices is usually thought of as observing a user interact directly with the screen – mostly in a point-and-touch manner. HCI research has looked at Around Device Interaction (ADI) – where the device's sensors are used to extend the interaction space beyond the device itself – and we discuss whether there is a route forward for Around Device Authentication, or 'touchless authentication', for covert security interactions.

Related Work

Previous work has looked at designing multi-touch authentication methods for communal spaces with the aim of blurring the process and limiting the success of shoulder surfers [4]. Four principles were identified for disrupting observations: **reduce visibility**, **subdivide action**, **dissipate attention**, and/or **knowledge transformation**. Pressure Grid was found to be significantly more resistant to observation attacks than a PIN when entered on a tabletop - with a Faces variant of the system being completely unbreakable by observers. Pressure Grid met three of the four principles, demonstrating that adhering to them can result in observation-resistant systems. ADI presents a different interaction style to multitouch input, but the four principles still apply. A look at recent work in the area shows that no ADI systems utilise the principles of Subdividing Attention and Knowledge Transformation, but the other two principles are covered below.

Dissipate Attention

This principle focuses on presenting an attacker with extra irrelevant information with the aim of overwhelming them. Generally speaking, ADI methods that rely on gestures fall into this principle as the attacker is required to observe the gesture and replicate it on a 3D plane – e.g. 3D signatures that are very difficult to replicate even when playing back HD footage of the action [8]. uWave, another gesture-based ADI method, allows the personalisation of gestures but an evaluation shows that the scheme is vulnerable to observation attacks, suggesting that systems based on this principle are not always effective [5]. Furthermore, while using gestures for identification was a great success, they experienced a range of problems when users had to authenticate with uWave.

Tapping as an interaction method has been shown to be acceptable to users [7]. Single taps were shown to be problematic from an implementation point of view due to false positives but double taps were successfully implemented. Participants experienced higher than expected false positive rates when tapping through a coat pocket and while in motion due to the lack of immediate feedback, demonstrating the weaknesses associated with this principle. Whack Gestures [3], meanwhile, demonstrated that the interaction can be more easily recognised by having a obvious beginning and terminating actions (in this case a forceful tap, or 'whack').

From a security perspective, tapping has been applied to screen unlocking [6] with an advantage of being usable without direct feedback – i.e. under a table. Similarly, users can wake up their tablet using Bezel-Tap Gestures [9] by tapping on the bezel and immediately after touching the screen. Evaluations found very few false positives when using devices at home, although rates increased when used on the go.

Reduce Visibility

Reducing the visibility of the interaction is perhaps the most effective way to prevent observation attacks. Traditionally this has been achieved by placing a spare hand over the interaction or by using the body to shield the interaction, but systems usually do not implement this principle in the actual design, but rather rely on the user doing it of their own accord. An example of a system implementing reduced visibility is BoD Shapes, where the user is required to enter their credentials on the back of the device rather than on the primary (front-facing) screen [2].

New Opportunities

The numerous sensors embedded in smart mobile devices – accelerometer, gyroscope, proximity, barometer, thermometer and various others – could be used to make the authentication process more complex for an observer – to the point where the interaction no longer becomes a point and select exercise. In fact, the combination of these sensors could facilitate 'touchless' authentication – where the user does not interact with the screen itself, preventing smudge attacks [1]. This would be akin to reducing visibility – probably the most usable of the principles – without the need to explicitly obfuscate the interaction. The implications of such approach would be very interesting, where the user is able to perform an action the way it was intended yet an attacker would not necessarily be able to copy the action. The other three principles in effect penalise the user to the same extent as the attacker – e.g. the extra information that is displayed when dissipating attention is also present for the user when authenticating. On the other hand, performing a gesture – be it a full-body gesture or simply a sequence of taps – should be more intuitive than performing sub-actions or reverse actions to divert the attention of attackers which in essence ends up placing even more cognitive demands on the user. 'Touchless' authentication, then, could mark a departure from existing shoulder surfing protection standards towards a more usable principle: reduce visibility.

New Challenges

AD authentication on mobiles means users can authenticate without directly selecting objects (digits, images, etc.) on the screen, and thus potentially makes it more difficult for an attacker to copy the actions. However, can users be persuaded away from direct input methods that they have always used towards more unconventional interactions involving tapping and/or other gestures? Past work suggests that users are happy to interact with their devices using gestures that are discreet (e.g. tapping [7]) but whether they would choose to do so on a regular basis remains to be seen.

The level of security provided by ADI could become an adoption barrier, e.g. the number of taps required to make it comparable to a four-digit PIN could potentially make it difficult for users to remember and/or perform. Realistically a tap-to-unlock mechanism would only work for low-security authentication scenarios – e.g. as a replacement for having no passcode. However, it is possible that other gestures can be successfully combined to be used for high-security authentication, although convincing users about its security may not be an easy task.

Evaluating the user experience of new AD authentication can be tricky. It is already very challenging to design ecologically valid studies for established systems (e.g. alphanumeric passwords) in the wild, but what is the best way to evaluate techniques that require learning from users in a natural setting, as well as assessing their resistance to shoulder surfing? Additionally, new measurements may be required to fully understand a user's holistic experience with AD techniques. Traditionally time and accuracy has been used, but AD techniques are likely to take longer than inputting a four-digit PIN directly on a screen, while accuracy could be very difficult to measure objectively when the authentication process is being carried out implicitly.

Conclusions

In this position paper we explored the potential use of around device interactions for inconspicuous authentication. We covered some opportunities that are afforded by current and new embedded sensors – the use of 'touchless' authentication to prevent the user from interacting with the screen directly. We also touched upon challenges that are likely to arise from such interactions, e.g. adoption and the evaluation methods.

References

[1] Aviv, A. J., Gibson, K., Mossop, E., Blaze, M., and Smith, J. M. Smudge attacks on smartphone touch screens. In *Proceedings of the 4th USENIX conference on Offensive technologies*, USENIX Association (2010), 1–7.

[2] De Luca, A., von Zezschwitz, E., Nguyen, N. D. H., Maurer, M.-E., Rubegni, E., Scipioni, M. P., and Langheinrich, M. Back-of-device authentication on smartphones. In *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems*, CHI '13, ACM (2013), 2389–2398.

[3] Hudson, S. E., Harrison, C., Harrison, B. L., and LaMarca, A. Whack gestures: inexact and inattentive interaction with mobile devices. In *Proceedings of the fourth international conference on Tangible, embedded, and embodied interaction*, ACM (2010), 109–112.

[4] Kim, D., Dunphy, P., Briggs, P., Hook, J., Nicholson, J. W., Nicholson, J., and Olivier, P. Multi-touch authentication on tabletops. In *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems*, CHI '10, ACM (2010), 1093–1102.

[5] Liu, J., Zhong, L., Wickramasuriya, J., and Vasudevan, V. uwave: Accelerometer-based personalized gesture recognition and its applications. *Pervasive and Mobile Computing 5*, 6 (2009), 657–675.

[6] Marques, D., Guerreiro, T., Duarte, L., and Carriço, L. Under the table: Tap authentication for smartphones. *Proceedings of BCS HCI–The Internet of Things XXVII* (2013).

[7] Ronkainen, S., Häkkilä, J., Kaleva, S., Colley, A., and Linjama, J. Tap input as an embedded interaction method for mobile devices. In *Proceedings of the 1st international conference on Tangible and embedded interaction*, ACM (2007), 263–270.

[8] Sahami Shirazi, A., Moghadam, P., Ketabdar, H., and Schmidt, A. Assessing the vulnerability of magnetic gestural authentication to video-based shoulder surfing attacks. In *Proceedings of the 2012 ACM annual conference on Human Factors in Computing Systems*, ACM (2012), 2045–2048.

[9] Serrano, M., Lecolinet, E., and Guiard, Y. Bezel-tap gestures: quick activation of commands from sleep mode on tablets. In *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems*, ACM (2013), 3027–3036.