Hidden in Plain Sight: Using Lockscreen Content for Authentication on Mobile Devices

Sarah Prange
Bundeswehr University
LMU Munich
Munich, Germany
sarah.prange@unibw.de

Lukas Mecke
University of Applied Sciences Munich
LMU Munich
Munich, Germany
lukas.mecke@ifi.lmu.de

Yasmeen Abdrabou
Bundeswehr University
German University in Cairo
Munich, Germany
yasmeen.essam@unibw.de

Florian Alt
Bundeswehr University
Munich, Germany
florian.alt@unibw.de

Figure 1: We investigated content features of lockscreens. We found relevant features in the three areas status bar (top), main area (center) and bottom bar. Common features were time, battery and network status.

Abstract
Current knowledge-based authentication mechanisms are vulnerable to replay and guessing attacks. In this work, we propose a novel approach for generating dynamic passwords based on lockscreen content. We conducted an online survey (N=90), collecting lockscreens from users in the wild. From the survey we derive a design space, highlighting both possible and commonly used lockscreen interface elements. Our work is complemented by a discussion on feature properties and their impact on our proposed authentication scheme with regards to security as well as usability.

Author Keywords
authentication, mobile devices, usability, security

Introduction
Knowledge-based authentication is often used on mobile phones, both as primary authentication (e.g., PIN, password or pattern) and as fallback for other methods (e.g., fingerprint). Previous work found them to be susceptible to replay attacks based on shoulder surfing [6], smudges [4] or thermal traces [1]. One option to counteract those threats is the use of dynamic passwords (e.g., Google Authenticator[1]) as secrets automatically change and thus cannot be replayed. We propose to apply this idea for authentication

[1] https://play.google.com/store/apps/details?id=com.google.android.apps.authenticator2&hl=de, last accessed May 24, 2019

on mobile devices, using lockscreen content as input for a dynamic secret. We believe this content to be suitable, as it is available before the actual login. While there are apps (e.g., Screen Lock - Time Password[2]) implementing a simplified version of this, they use a static secret for every user (i.e., the time) and their security depends on the secrecy of the mechanism. In this work, we collected lockscreens (cf. Fig. 1) from users in the wild with an online survey (N=90) to inform a design space of interface elements that can be used as a basis for generating dynamic secrets (cf. Fig. 2). We propose a set of commonly available features and discuss how their properties impact suitability for generating dynamic passwords with regards to security as well as usability. Finally, we illustrate implications on the design of content-based mechanisms for authentication and beyond.

Content-Based Login

Example: As a simplified example, assume a lockscreen on a phone with *13%* charge at *5:26*pm on 18^{th} September (cf. Fig. 1). With those features, users may choose time and charge of their phone as components for a dynamic password, yielding e.g., *052613*. Using the same features users might also reorder single elements or use them multiple times, yielding e.g., *50621331*.

Background & Related Work

Conventional knowledge-based authentication mechanisms have proven their vulnerability to shoulder surfing [6] and guessing attacks [5]. With the use of built-in device features (i.e., screen content), we can enhance knowledge-based authentication to become dynamic, hence increasing its security and thus increase its resistance to guessing attacks. *Dynamic* is being used in different contexts of security mechanisms, such as two-factor-authentication [2] and one time passwords [7]. Research also considers picture passwords to be considered as dynamic passwords, as picture positions are randomized every time [13]. Furthermore, Michael W. Pinch introduced dynamic patterns with varying position of nodes [11]. Hang et al. [8] suggest to add dynamics to the concept of security questions[3]. While having dynamic answers, the suggested questions remain the same (e.g., “Who did you call yesterday?”).

[2] https://play.google.com/store/apps/details?id=com.adriadevs.screenlock.ios.keypad.timepassword, last accessed May 24, 2019

[3] questions that the system may ask to restore a user’s lost access

Dynamic parts have also been integrated in conventional passwords by adding time [10], time and MAC address [12] or even a server generated random number [9]. From that we learn that adding *dynamics* is a feasible mean to enhance knowledge-based authentication. For smartphone unlocking mechanisms, we believe that lockscreen content itself provides promising aspects to serve as input for dynamic authentication components. We look at the composition of users’ lockscreens in more detail with this work.

Concept: Content-Based Authentication

We propose authentication with dynamic secrets based on lockscreen content, more specifically, e.g., the state (e.g., time or network strength), presence (e.g., Bluetooth symbol) and appearance (e.g., background or icon color) of UI elements shown on a lockscreen. Those can be combined in a unique way to form a secret that will change together with those elements. As such, the creation strategy becomes the secret for authentication rather than the entered password itself (refer to sidebar for an example).

Online Survey: Exploring the Design Space

We set out by understanding how users’ lockscreens are composed. In an online survey, we collected different lockscreens as used on various devices and OS.

Survey Design

To understand the design space, we asked participants to upload a screenshot of their lockscreen[4]. The survey contained 15 questions, collecting demographics (e.g., background, computer literacy), unlock mechanisms used and permission to use and publish the submitted images. The survey was distributed via university mailing lists and social media. The data collection phase lasted for 4 weeks.

[4] We added a guide on how to take a screenshot along with a sample.

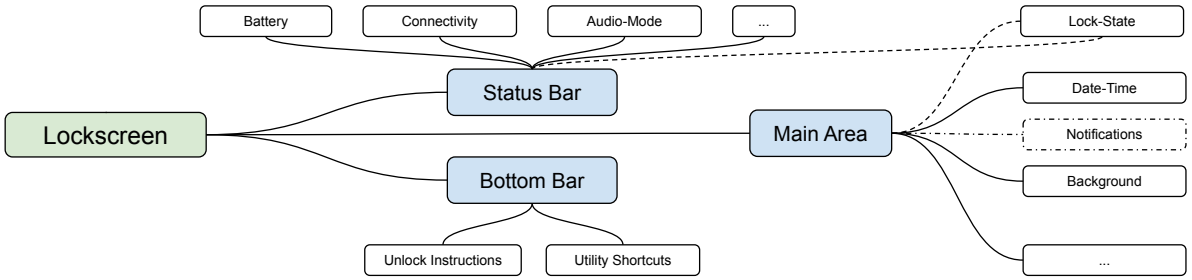

Figure 2: We found lockscreen features evolving around three areas of the screen: status bar (top), main area (center), and bottom bar. For Lock-State, we found indications in different areas of the screen. Note that we found notifications in less than 10% of screenshots.

Unlock Mechanism	PIN	Pattern	Fingerprint	Face Recognition
PIN	9.8	-	45	-
Pattern	-	7.6	12	-
Fingerprint	45	12	17.4	3.3
Face Recognition	-	-	3.3	-

Table 1: Combinations of unlocking mechanisms used by the participants. Table entries are percentages. The most common combination was fingerprint with PIN as a fallback (45%).

Participants

We received 99 responses (63 females, 27 males; age 17 to 42, M=22.70, SD=3.87). We excluded 9 responses due to screenshots not containing lockscreens. All participants pursue(d) a college degree with different backgrounds (e.g., Engineering, Philosophy, Medicine, ...) and at different stages (postgraduate, master or PhD). Participants' are mostly German (50%) and Egyptian (43%). Table 1 shows the unlocking mechanism used by the participants (i.e., main and fallback mechanism). In addition, one participant used face recognition, one used iris scan and three stated not to use any unlock mechanism.

Limitations

Our sample of participants comprised higher educated smartphone users from Germany and Egypt. While we found some cultural differences (e.g., some Egyptian participants had a Gregorian as well as an Islamic calendar on their lockscreen), we did not evaluate further differences to other cultures. Some participants reported to have modified their lockscreens, in particular by removing notifications, due to sensitive content. This might have lead to an under-representation of this feature in our design space.

Design Space

We analyzed a total of 90 screenshots of lockscreens. By inspecting a subset, three researchers established an initial set of potential features (i.e., interface elements). We then independently coded the lockscreens using the established features, discussing and adding new features where necessary. Fig. 2 depicts a high level overview over the features and Table 2 provides counts on the occurrences of each feature with at least 10 occurrences in our data set.

Discussion

General & Personal Content

We found a set of features that were universally present, namely *time*, a *battery symbol* and *network signal strength*. Battery charge in percent, the network provider, the date and a camera shortcut in the bottom bar were present in all but a few exceptional cases. Some features (e.g., weather information, 1/90) occurred rarely or never (refer Tab. 2). We believe that an implementation should consider all universal features as input. Less frequent features may be used for other purposes (e.g., reversing the input if a certain element is present to further increase security).

	Category	Symbol	#
Status Bar	Apps	message	9
	Audio	vibration	11
		silent	19
	Battery	**symbol**	**89**
		percentage	80
		color	20
		charging	12
	Connectivity	Wifi	59
		signal strength	**87**
		network	28
		standard	
		network provider	81
		Bluetooth	12
	Lock State	lock icon	39
	System	screen orientation	22
	Time	alarm icon	24
Background	Photo	anything	35
		people	16
	Standard	coloured	34
		etc.	
Lockscreen	Text	standard	11
	Time	**hours**	**90**
		minutes	**90**
		weekday	85
		month	85
		month day	85
Bottom Bar	System	unlock-instruction	42
		telephone	17
		microphone	12
		camera	83

Table 2: Feature categories and occurrences in our data set, sorted by screen area. We only report on features that appeared on more than 10% of the screenshots. Features in bold were universally present, though sometimes encoded differently (e.g. signal strength was missing in offline mode; the mode indicates no signal by itself).

Dynamics & Changing Frequency

Some features we found on participants' lockscreens change quite frequently (e.g., minutes), others rarely to never (e.g., network provider). Hence, passwords relying on features with low change rates may become replayable when authenticating frequently (e.g., in the same minute). This may be prevented by adding artificial cues, i.e., systematically ensuring that two lockscreens will differ. Examples include changing elements (e.g., step counters, charge or signal strength) where artificial changes are hard to distinguish from real ones or adding artificial content (e.g., as part of the background image). To avoid replay in case the creation strategy is obtained, content-based passwords may still be complemented by a static, knowledge-based component.

Memorability & Clues

Our concept shifts the effort from memorizing a password to memorizing a password generation strategy. This opens up new possibilities to ease memorability, e.g., by choosing elements based on a visual pattern or elements that contribute greater amounts of input (e.g., using the full date and time). How users would actually choose their strategies is a question we propose to answer in future work.

Password Choice & Potential Attacks

By including lockscreen features for password generation, the theoretical password space can be enhanced, depending on the users' features. However, "sweet spots" [3] may evolve (i.e., users might choose similar secrets based on popular features). Furthermore, attackers knowing the mechanism could apply "smart" guessing attacks based on common lockscreen features.

Lockscreen Content Beyond Authentication

Beyond the introduced authentication scenario, we see great potential for the use of lockscreen content. Options include, but are not limited to, giving subtle notifications to the user by artificially changing specific elements, use other input methods to select interface items (e.g., touch or gaze) or adding hidden functionality to certain interface elements.

Towards Designing Content-Based Authentication on Mobile Devices

How Do Features Influence Security

Depending on the desired level of security, different content features may be used. Features with higher changing frequency may be harder to observe or guess. This may also hold for features that are not placed prominently on the lockscreen, but rather "hidden" in the status bar.

How Do Features Influence Usability

By using visible cues on the lockscreen, we aim at supporting users (i.e., providing a visible memory aid for password composition) while at the same time preserving security (i.e., allowing for dynamic passwords). Compared to, e.g., password stores, the visual clue is a) co-located with the authentication (i.e., on the lockscreen), and b) dynamic.

Feature Choice & Lockscreen Design

We see two directions for further research based on our design space. On one hand, we proposed a set of features as occurred in our data sample (N=90) and also highlighted how they influence security as well as usability. On the other hand, future lockscreens may also provide ideal features by design (e.g., with high changing frequency).

Conclusion

With our work, we suggest to consider content-based authentication, in particular for mobile devices. We collected 90 lockscreens from in-the-wild users on which we base our design space and suggest directions for designing such authentication mechanisms. We hope to stimulate discussions around the security as well as the usability of our concept.

Acknowledgments

We thank Deniz Mardin and Peter Warmhold for their part in creating the idea for this concept.

REFERENCES

1. Yomna Abdelrahman, Mohamed Khamis, Stefan Schneegass, and Florian Alt. 2017. Stay Cool! Understanding Thermal Attacks on Mobile-based User Authentication. In *Proceedings of the 35th Annual ACM Conference on Human Factors in Computing Systems (CHI '17)*. ACM, New York, NY, USA.
2. Sagar Acharya, Apoorva Polawar, and PY Pawar. 2013. Two factor authentication using smartphone generated one time password. *IOSR Journal of Computer Engineering (IOSR-JCE)* 11, 2 (2013), 85–90.
3. Florian Alt, Stefan Schneegass, Alireza Sahami Shirazi, Mariam Hassib, and Andreas Bulling. 2015. Graphical Passwords in the Wild: Understanding How Users Choose Pictures and Passwords in Image-based Authentication Schemes. In *Proceedings of the 17th International Conference on Human-Computer Interaction with Mobile Devices and Services (MobileHCI '15)*. ACM, New York, NY, USA, 316–322.
4. Adam J. Aviv, Katherine Gibson, Evan Mossop, Matt Blaze, and Jonathan M. Smith. 2010. Smudge Attacks on Smartphone Touch Screens. In *Proceedings of the 4th USENIX Conference on Offensive Technologies (WOOT'10)*. USENIX Association, Berkeley, CA, USA, 1–7.
5. Joseph Bonneau. 2012. The Science of Guessing: Analyzing an Anonymized Corpus of 70 Million Passwords. In *2012 IEEE Symposium on Security and Privacy*. 538–552.
6. Malin Eiband, Mohamed Khamis, Emanuel von Zezschwitz, Heinrich Hussmann, and Florian Alt. 2017. Understanding Shoulder Surfing in the Wild: Stories from Users and Observers. In *Proceedings of the 2017 CHI Conference on Human Factors in Computing Systems (CHI '17)*. ACM, New York, NY, USA, 4254–4265.
7. Neil Haller. 1995. The S/KEY one-time password system. (1995).
8. Alina Hang, Alexander De Luca, and Heinrich Hussmann. 2015. I know what you did last week! do you?: Dynamic security questions for fallback authentication on smartphones. In *Proceedings of the 33rd Annual ACM Conference on Human Factors in Computing Systems*. ACM, 1383–1392.
9. M. Lei, Y. Xiao, S. V. Vrbsky, C. . Li, and L. Liu. 2008. A Virtual Password Scheme to Protect Passwords. In *2008 IEEE International Conference on Communications*. 1536–1540.
10. Detchasit Pansa and Thawatchai Chomsiri. Web security improving by using dynamic password authentication.
11. Michael W Pinch. 2013. Dynamic Patterns for Mobile Device Authentication. (Sept. 5 2013). US Patent App. 13/709,048.
12. Xuguang Ren and Xin-Wen Wu. 2012. A novel dynamic user authentication scheme. In *2012 International Symposium on Communications and Information Technologies (ISCIT)*. IEEE, 713–717.
13. Xiaoyuan Suo, Ying Zhu, and G Scott Owen. 2005. Graphical passwords: A survey. In *21st Annual Computer Security Applications Conference (ACSAC'05)*. IEEE, 10–pp.