THE SECURITY OF ATMS AND BANKS

Vijay Bhardwaj[1], Sandeep Kaur[2]
[1,2]Guru Kashi University, Talwandi Sabo

ABSTRACT

With the increase of automated teller machine (ATM) frauds, new authentication mechanisms are developed to overcome security problems of personal identification numbers (PIN). Those mechanisms are usually judged on speed, security, and memorability in comparison with traditional PIN entry systems. It remains unclear, however, what appropriate values for PIN-based ATM authentication actually are. We conducted a field study and two smaller follow-up studies on real-world ATM use, in order to provide both a better understanding of PIN-based ATM authentication, and on how alternative authentication methods can be compared and evaluated. Our results show that there is a big influence of contextual factors on security and performance in PINbased ATM use. Such factors include distractions, physical hindrance, trust relationships, and memorability. From these findings, we draw several implications for the design of alternative ATM authentication systems, such as resilience to distraction and social compatibility

Keywords ATM, security, authentication, design implications, field study, lessons learned

I. Introduction

New authentication systems are mostly created with the goal to be “better” than PIN or password. “Better” usually refers to being more memorable, more secure, or both. Security is certainly the most important aspect when designing authentication systems for public settings (e.g. ATMs), yet memorability directly affects security as well, as hard to memorize secrets get written down and thus overall security suffers. The standard approach to verify the appropriateness of a new ATM authentication system is to compare it to PIN entry in controlled laboratory experiments. However, such a laboratory experiment can never mirror completely the real situation when using an ATM. The role of the authentication process with respect to the entire interaction at an ATM remains unclear, since the actual process of ATM authentication outside of laboratory settings has not been sufficiently examined yet. For example, overall interaction speed is a very important aspect of public authentication, and it has been argued that alternative authentication mechanisms should thus also be judged by this factor. PIN entry typically is faster than proposed alternatives, yet without knowing the “big picture” of an entire ATM interaction, it is difficult to assess the significance of this faster speed. Previous research, based on semi-structured interviews, helped to identify basic factors that influence the decision to use an ATM, like privacy, social density, and time pressure. Nevertheless, the actual use of ATMs was not explored. Consequently, we decided to perform a number of field observations involving ATM use, in order to explore how people actually interacted with ATMs. As it has been previously shown in the domain of public display interactions, field studies have the potential to uncover important facts and practices that otherwise cannot be asserted. The main focus of our observations was on the ATM authentication process, i.e., how people enter their PIN, whether and how people protect their PIN entry from skimming attacks, and what contextual factors affect security and secure behavior.

II. Methodology

All observations were performed by the same researcher. No other person helped recording the data. This was necessary to keep the data comparable, since different people might apply different standards during the observation, deliberately or not. Even though multiple observers might have reduced the risk to accidently miss data, we opted for this solution and since we considered consistency more important than efficiency (speed of collecting the data). In order not to bias the results, the observer was located at unsuspicious spots like bars, restaurants and coffee bars that had tables outside. ATMs were also chosen with respect to this criteria. Interestingly, a huge amount of the outdoor ATMs that we could find were close to such spots. Thus, finding appropriate locations was not an issue. Considering these precautions, it is very unlikely that the observer did arouse suspicion amongst the users. Additionally, the observation sessions were chosen rather short to minimize this risk.

III. Ethical and Legal Considerations

Reasons for failed observations were mainly cars or other people that suddenly blocked the view to the ATM or the user. Roughly one third of all observations were thus discarded. There were some rare instances of interesting behavior (e.g. a user leaving the ATM after a failed authentication attempt) that lead to failed observations and was thus not added to the data set. However, these instances were written down as additional comments in case they would help to gain further insights. In the countries where we conducted the studies, no ethical review boards are in place for this kind of research. However, legal issues have to be considered. For instance, German privacy regulations state that without the explicit consent from the subjects, data can only be collected and stored anonymously. 1 However, once data has been rendered anonymous, it can then be used freely for scientific purposes. Since none of our subjects can be identified by any means (no videos and photos were taken), our data collection is truly anonymous. Furthermore, as the study was conducted in public spaces without the use of AV-equipment, our local legal counsel informed us that no consent from any institution (e.g., banks or city administration) was required. In connection with the previously mentioned measures to protect the subjects’ privacy (e.g., not being able to see the actual PIN entered), we did not identify any legal or ethical issues with this study.

Since ATM interaction is a sensitive and private task, it was very important for us not to disturb the users’ privacy. Therefore, we decided not to engage them in interviews after the observation. Consequently, some of our findings are necessarily based on (speculative) reasoning about the observed behavior, rather than on actual user feedback. Especially inferences on the use of security, the influence of company, and queuing strategies were not verified with those users exhibiting these behaviors. To fill these gaps, we performed additional interviews in public spaces with a focus on these aspects (cf. section 2.3 below). When analyzing the observational data from our first study – and especially the comments – it became apparent that the time measured from entering the ATM card to the moment of money withdrawal was not entirely sufficient. Many users blocked the ATM for a significantly longer amount of time before and after the actual cash withdrawal, which we called preparation phase and cleanup phase, respectively. These phases include simple tasks like getting the ATM card from the wallet or putting down shopping bags. Based on our experiences from the first study, we reckoned that this overhead might in some cases be around 50% to 100% to the “interaction times” that we measured.

IV. Authentication only a minor task

The numbers from our observations suggest that authentication only takes a marginal part of the whole interaction time with an ATM. With 46 seconds on average (or 54.9s when considering preparation and cleanup), more than 90% of ATM interaction is spent navigating menus and waiting for the withdrawn money (and optional receipts) to appear, etc. Distractions such as minding bags or talking to friends add further delay. Being seen as a minor task that has to be done to be able to perform the actual task (e.g., withdraw money), it is questionable wether significantly slower authentication systems will be accepted by users. Considering an interaction time of 52.9 seconds, a system that takes, say around 12 seconds (e.g. [9]) adds an overhead of around 18% to the overall time. The fact that we rarely observed longer queues (>2) during the observation, and that in our interviews we found that people based their decisions to queue or not on manifold factors, renders the “threat” of accumulated waiting times less significant. We can therefore support survey findings from that people judge waiting time with respect to their time constraints and their need for cash. It seems that a queue length of two is a borderline that many people are only willing to cross if it is urgent and if their time constraints allow for it. However, increased authentication time can also have an influence on people waiting in the queue and would increase overall waiting times over accumulation. Considering common authentication mechanisms from the literature, waiting and overall interaction times can increase drastically if the authentication mechanisms takes significantly more time. If for instance the interaction time for an authentication mechanism takes around 45 seconds, which is the average overall interaction time that was observed during the field study, the second user in the queue would have to wait twice as long as with PIN authentication. This highlights, that when creating an authentication system for public terminals, time is a very important factor that can decide over acceptance or rejection of a system. Within this work, we cannot provide an exact borderline on how long an authentication mechanism for ATMs should be. However, we argue that PIN authentication is only accepted by users since it is very easy and – maybe most impor- tantly – extremely fast. Therefore, it is highly appropriate for ATMs, since the overall task is very short and PIN still only requires a small fraction of the overall time. A rule of thumb might be that an alternative authentication mechanism for ATMs should only require a fraction of the overall time (< 10%) that a user spends at the machine.

V. Limitations of the results

Since the main observation took place in two central European cities, it has only limited validity with respect to other cultural areas (e.g., Asia) or in less urban settings. The unobtrusive nature of the observations did not allow for in-depth findings on whether people check the hardware of an ATM (keypad or card slot) for manipulations. However, our general findings suggest that people only rarely use this security measure. As for any study that involves direct contact to the participants, the field interviews might have been slightly biased since the participants might have wanted to “look good” or “do it right”. Therefore, the numbers on hidden input might be higher than they are in reality, which our field observations seem to confirm.

VI. Conclusions

On the basis of a field study, an additional in-depth study, and a small set of street-interviews, we were able to identify several factors that are likely to influence the performance and security of authentication mechanisms for ATMs. Our observations revealed practices that suggest specific design decisions for ATM authentication systems. For example, over 65% of users did not hide their PIN entry at all, or did so only weakly. This suggests that security for ATMs cannot rely on the user but needs security features which are "built in" into the authentication mechanism. That is, the security of a system should not rely on active secure behavior of a user. The observations further helped to identify contextual factors that can have a great impact on the systems. Simple factors like prams, shopping bags, phone calls, etc., can be a reason for not applying security or for being slow. We also found that social factors (showing trust) can be a reason for bad security decisions. However, there are aspects of ATM authentication mechanisms that this study cannot answer, but which are nonetheless of great importance when creating respective authentication systems. Most likely deployment cost are one of the most decisive factors in this context: how much will it cost service providers to update all their ATMs (or public terminals) to a new system? Other factors could be, e.g., resistance to vandalism. This work represents a first step in uncovering ATM use in the wild, hopefully helping to gain a broader insight on the real factors and constraints of ATM authentication. For future work, we would like to extend our observations to other forms of electronic payment (e.g., ticketing machines, supermarket checkout), where we expect slightly different circumstances leading to noticeable differences in use. For instance, we believe that in a supermarket setting, we might experience even more insecure behavior. Also, we would like to encourage other researchers to perform similar studies in different cultural and/or urban settings since we are highly interested in how these findings will apply there.

VI. References

Catherine, N., Geofrey, K. M., Moya, M. B., &Aballo, G. (2018). Effort expectancy, performance expectancy, social influence and facilitating conditions as predictors of behavioural intentions to use ATMs with fingerprint authentication in Ugandan banks. *Global Journal of Computer Science and Technology*.

Mbogoro, F. (2020). Adoption of cash deposits through Automated Teller Machines (ATMs) by banks in Tanzania: a case of selected commercial banks in Dar es Salaam. *898111358*.

Wang, S. Y. K., & Hsieh, M. L. (2021). Why Rob Banks? That's Where the Money is...... Even Online!. In *Digital Robbery* (pp. 7-13). Springer, Cham.

Wang, S. Y. K., & Hsieh, M. L. (2021). Why Rob Banks? That's Where the Money is...... Even Online!. In *Digital Robbery* (pp. 7-13). Springer, Cham.

Biberaj, A., Tafaj, I., Shurdi, O., Agastra, E., &Rakipi, A. (2021, June). Security of Automated Teller Machines (ATM's). In *International Conference "New Technologies, Development and Applications"* (pp. 596-606). Springer, Cham.

Sahni, A., & Singh, S. (2021). Improving E-Banking Security via Biometric ATMS. *International Journal of Computer Science & Programming languages*, *7*(1), 15-19.

Mbachu, C. B., &Ogamba, M. O. SECURITY VIOLATION MANAGEMENT FOR ATMS TRANSACTIONS IN THE BANKING SECTORS USING BIOMETRIC FINGERPRINTS.

Othman, A. K., Hamzah, M. I., & Hassan, L. F. A. (2020). Modeling the contingent role of technological optimism on customer satisfaction with self-service technologies: A case of cash-recycling ATMs. *Journal of Enterprise Information Management*.

Afriyie, O. K., &Arkorful, V. (2019). Enhancing security of automated teller machines using biometric authentication: A case of a Sub-Saharan University. *Researchgate Publication*, *9*(7), 7-22.

Nanyanzi, I. M. (2021). *Automated Teller Machines (ATM) Adoption Strategies and Customer Satisfaction in Commercial Banks in Uganda: A Case of Centenary Rural Development Bank Branches in the Central Business District of Kampala* (Doctoral dissertation, Uganda Christian University).

Ladanu, W. K. ASSESSMENT OF BANKS AUTOMATED TELLER MACHINES IN THE SATISFACTION OF ENTREPRENEURS IN ILORIN METROPOLIS.