SafePass: Authentication under Duress for ATM Transactions

Sufian Hameed, Syed Atyab Hussain, Sohail Hussain Ali
CS Department, FAST-NUCES, Karachi Campus, Pakistan.
sufian.hameed@nu.edu.pk, k102230@nu.edu.pk, k102207@nu.edu.pk

***Abstract*—With the proliferation of ATM installations throughout the world, billions of transactions are being conducted annually. This easy, location independent and 24 hours access to money has also given birth to ATM related thefts and this situation is more pronounced in developing countries with poor law and order situation.**

Panic passwords can be used as an effective mean to signal stress during authentication. Panic password scheme provides a safe way to avoid a forced authentication or signal stress when authentication is a result of coercive action. In this paper, we introduce *SafePass*, a new panic password scheme that can be easily deployed over the ATM infrastructure. In *SafePass*, special attention is given from the usability perspective as it would be extremely valuable for large scale proliferation.

***Index Terms*—panic password, ATM transaction, authentication, stress authentication**

I. Introduction

Since its inception in 1960s, the installation of ATM has proliferation throughout the world. This vast scale deployment has resulted in billions of ATM transactions worth trillions of dollars annually. This easy access to currency withdrawals has also attracted attackers and in the recent years there has been a noticeable hike in the crime wave against the ATMs. According to EAST (European ATM security) [1], ATM related physical attacks on European ATMs have increased by 13% in 2012, when compared with previous years. In the developing countries, the landscape of ATM related crime is far worse where several incidents have resulted in loss of precious human lives as well [2].

ATM systems are generally secure against unauthorized access to customer accounts by malicious parties. This is primarily achieved by using essential cryptographic primitives to encrypt and decrypt the information in transmission between the ATM terminal and the central server. The security measures currently deployed in ATM networks have proofed to be effective in disrupting and preventing malicious attacks in the normal transaction processing of ATMs. However, all these robust security measure are not sufficient against the common and ongoing threat of stress authentication that is imposed upon an ATM user under serious danger of physical harm by an arm thief.

Duress or stress authentication typically constitutes a situation where an ATM user is forced by an arm thief to make cash withdrawal from his account. In order to avoid any harm, the helpless ATM user has no choice but to comply with the instructions of the thief. Failure to follow the thief's commands, whether intensionally or under confusion, will most likely place the user in serious danger of retaliation from the thief. Due to increasing number of duress cases, it is very important that the ATM networks introduce a new security mechanism designed to recognize the transaction made under duress.

One way of handling duress is by allowing the victimized ATM user to discreetly trigger a distress signal to police or other concerned monitoring authorities without being recognized. This distress signal will enable a prompt response to the ongoing criminal activity. However, this mechanism might completely fail in developing countries with poor law and order situation, specially when the response time of police or law enforcement agencies is unpredictable. A better approach in this situation would be to use *panic passwords*. Panic passwords can be defined as a special password that can used to signal the server that the user is under duress and the password is being entered as the product of a coercive action.

Numerous efforts have been made over the years by the scientific community to strengthen passwords and to enhance their usability. A few noteworthy efforts include [3]–[5], [7]–[9], [11]. Despite a large volume of research on the use of passwords, there is a clear deficit of academic study on panic passwords. Panic passwords are currently used in home security systems to trigger a silent alarm. Besides that, there are several online scenarios where panic passwords can be effectively applied. In [6], Clark provides a basis to attract the attention of research community towards the usage of panic passwords. Clark discussed couple of panic password schemes with Internet-based voting as the primary representative scenario.

In this paper, we introduce *SafePass*, a new panic password scheme that can easily be deployed over the ATM infrastructure. In *SafePass*, special attention is given from the usability perspective as it would be extremely valuable for large scale proliferation. Unlike typical perception, in *SafePass*, the ATM users do not have to maintain any panic password. He just needs to be very sure about his regular PIN

code. In duress scenario the user can simply enter a different final digit in the 4-digit PIN. This will trigger the duress situation and the ATM machine will respond according. This approach reduces the memory load on the user. If the user makes an incorrect entry for the first 3 digits, it will be treated as normal invalid entry. Thus reducing the chance of triggering the panic situation for genuine mistakes.

The rest of the paper is organized as follows. §II describes the state of the art. §III discusses the design and usage flow of *SafePass*. Finally we conclude the paper in §IV.

II. Current State of Panic Password Schemes

Panic passwords also known as *distress passwords* or *duress codes* have strong applicability in military and intelligence scenarios. But due to their classified nature in military domain, the exact extent to which these schemes are applied or studies is still unknown. On the other hand the academic study or the survey of the non-classified literature reveals very little. In this section we have discuss some handful of schemes we came across in the literature.

A. Reverse PIN Hoax

In September 2006, a seemingly helpful heads-up began circulating on the Internet which claims that entering your PIN in reverse at any ATM summons the police. The actual text goes something like this:

If you should ever be forced by a robber to withdraw money from an ATM machine, you can notify the police by entering your PIN # in reverse.

For example if your pin number is 1234 then you would put in 4321.

The ATM recognizes that your pin number is backwards from the ATM card you placed in the machine. The machine will still give you the money you requested, but unknown to the robber, the police will be immediately dispatched to help you.

Please pass this along to everyone possible.

Despite Internet-circulated claims dating to September 2006, ***no ATMs have or have had an emergency-PIN system based on "reverse PIN" technology***. This is just an hoax which is not even capable of handling palindromic PINs (e.g., 2002, 7337, 4884).

B. Patented Technology

In [10], a panic password scheme is discussed as a subset of a larger system. Being part of a patented technology, the exact method or elaborate discussion is not included in the document. At the superficial level the patent document discuss that the ATMs will display a list of words from which the user may choose a predefined word for normal authentication and any other word to signal duress i.e. generation of a silent alert signal to the authorities. As discussed before, this mechanism might completely fail in developing countries with poor law and order situation, specially when the response time of police or law enforcement agencies is unpredictable.

C. Panic Password in Internet-Voting

Motivated by the deficit of academic literature exploring the topic of panic passwords, Clark [6] has outlined couple of panic password schemes with Internet-voting as the primary representative scenario. The discussion on the proposed schemes are as follows.

1) Two Passwords(2P): In `2P` scheme, the user is given two passwords `p1` and `p2`. The user can use `p1` for normal authentication and `p2` to communication duress. This scheme is easy to use and impose low memory load on the user to remember two different passwords whether they are related or not.

This approach is secure only for a very limited scope and cannot be applied in public ATMs as attacker can ask the victim to give him both of his passwords. When the victim surrenders and provides his regular and panic password to the attacker, the attacker will have a good 50% chance of entering the regular password. The goal of panic password schemes is to decrease the chances of theft by increasing the chance that the attacker is not able to enter a regular password and a success rate of 50% is not good enough.

2) 2P Time Lock: The `2P` time lock is an extension to the previous `2P` scheme. The user is provided with two passwords `p1` and `p2` for normal and duress authentication respectively. The user can perform normal authentication using `p1` multiple times within the window of `t1`. Using the same password each time will not lock the user account. Similarly, the user can enter `p2` to communicate panic, the system will follow what the scenario dictates, but this does not lock the account. However, if the two different passwords are used within the time window of `t1`, the account of the user will be locked for some definite period.

In `2P-lock` the chances for theft remains 50%, provided the attacker gets both of the passwords by force. The `2P-lock` scheme is specifically designed to protect against an iteration attack. It is not clear how this scheme will handle genuine mistake i.e. when the user first enters a wrong password and then he may re-enter the password again.

3) P-Compliment: In *P-Compliment* the user only maintains one password for normal authentication. The user can enter any password other than the real one to communicate a panic state. The biggest drawback of this approach is that it cannot distinguish between mistakes and panic state.

4) 5-Dictionary: In this scheme the user selects a set of five dictionary words as a panic password. This approach might have some application in Internet voting, but it cannot

be applied in ATM networks.

5) 5-Click: In 5-click, a user is presented with a sequence of five images and he has to click on a valid region in each image. In order to communicate duress, the user has to click another valid region for at least one of the image. Just like 5-dictionary, this scheme cannot be easily applied to ATM duress authentication.

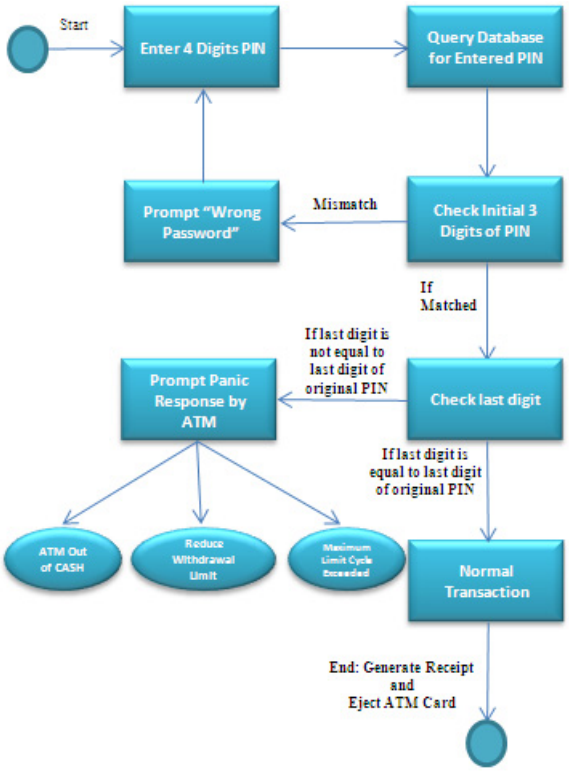

Fig. 1. ATM usage flow with SafePass.

III. SafePass: Design and Usage Flow

In this section we discuss the design goals of an efficient panic password scheme for ATM networks followed by the design and usage flow of *SafePass*. Special attention is given from the usability perspective as it would be extremely valuable for easy deployment and large scale proliferation over the ATM infrastructure.

A. Design Goals

At the outset, we seek a solution that works well with the current, entrenched system. This means that the system should have the following desired properties.

- **Reasonable number of panic PINs:** This property will make the panic password scheme strong against an iteration attack even without the application of locks. In 2P and 2P-lock schemes discussed above the attacker have a 50% success rate by iterating through the set of regular and panic password.
- **Large set of invalid PINs:** This property increase the probability that a mistype PIN code is treated as invalid entry, instead of a panic code.
- **Close relation between regular and panic PINs:** The reason for this property is to reduce the memory load on the ATM user. Since, under the duress situation, it is highly likely that the panicked ATM user could go blank and not remember any part or variation of the assigned panic PIN. This might place the innocent ATM user at a high risk of retaliation.

B. SafePass Design

Before we go into the design details of *SafePass*, lets consider that the ATM PIN space is denote by $\mathtt{P}$ and constitute of four digits. Each PIN $\mathtt{p} \in \mathtt{P}$ is in one of two sets, $\mathtt{V}$ for valid or $\mathtt{I}$ for invalid. As in any password scheme, a regular PIN $\mathtt{p}$ is selected from $\mathtt{P}$ and is included in $\mathtt{V}$. To extend the notion of PIN to panic authentication we define panic PIN as $\mathtt{p}\star \in \mathtt{P}$ and include it in $\mathtt{V}$. Our scheme includes more than one PIN used for panic authentication. All elements of $\mathtt{P}$ other than $\mathtt{p}$ and $\mathtt{p}\star$ are invalid. If an invalid PIN is entered it will result in an error and has no further consequence.

In *SafePass*, the ATM user just needs to know one PIN $\mathtt{p}$, which is used for regular authentication. The user is not required to maintain or remember any panic PIN to communicate duress. This design choice will help reduce the memory load on the ATM user in duress situation.

In the working scenario, the ATM user could use a four digit PIN, $\mathtt{d1d2d3d4}$, as $\mathtt{p}$. For communicating duress, the user can very easily construct a panic PIN $\mathtt{p}\star$ by changing the fourth digit ($\mathtt{d4}$) of the regular PIN $\mathtt{p}$ i.e. $\mathtt{p}\star = \mathtt{d1d2d3d4'}$. For instance lets suppose the ATM user has a regular $\mathtt{p} = 9471$. In case of stress authentication he can change the last digit and convert the regular PIN into panic PIN. For this particular example the possible values of $\mathtt{p}\star$ are 9470, 9472, 9473, 9474, 9475, 9476, 9477, 9478, 9479. In *SafePass*, instead of memorizing the set of panic PINs, the user just needs to be very sure about his regular PIN and the panic PIN can be created on the fly from the set of possible options.

1) Set of Panic PINs: In *SafePass* we have a single regular PIN, while all the remaining 9 combinations can be used as panic PIN i.e. $|\mathtt{p}\star| = 9$. In case of theft, a victim can easily give one of the panic PINs by changing the last digit of his original PIN. It will not be easy for the attacker to identify weather the given PIN will signal panic or not. Assuming the attacker knows the scheme being used; still he cannot distinguish between different PINs. If the attacker randomly chooses a PIN of his liking based on what the user has told him, he will only have a 10% chance of success. Comparing this with 2P and 2P-lock schemes, this is an increase in

strength by 80% and the chances of iteration based attacks are also minimized.

Fig. 2. Card insertion in ATM.

2) Set of Invalid PINs / States: The *P-Compliment* scheme allow the users to enter any PIN other than the real one to communicate panic. This leads to design a flaw where the system cannot distinguish between genuine mistakes and panic state. In *SafePass* there are 10 valid states, which include the normal authentication state using the regular PIN $\mathtt{p}$ and 9 possible panic states using the PIN $\mathtt{p}\star$. If we take the above example with $\mathtt{p}$ = 9471, the possible values of $\mathtt{p}\star$ are 9470, 9472, 9473, 9474, 9475, 9476, 9477, 9478, 9479. Based on that the valid set $\mathtt{V}$ = 9471, 9470, 9472, 9473, 9474, 9475, 9476, 9477, 9478, 9479.

All the remaining 9990 possible combinations will be treated as invalid input or in other words genuine input mistakes prompting ”wrong input”. If the user is opting for a normal authentication, he must take extra care while entering the 4th digit, because any mistake/change at only the 4th digit will trigger the panic state.

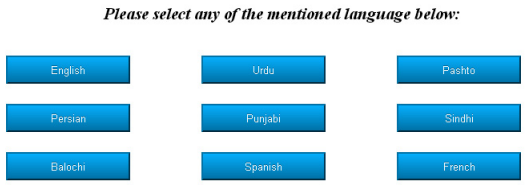

Fig. 3. Language selection interface.

3) Panic Response: In *SafePass*, the system response for duress authentication will remain unpredictable. If ATM system throws a similar response on each panic state, this could make the thief suspicious. The core idea is to keep the response random such that the thief cannot distinguish between normal and panic state. Some possible responses are listed below. We left further response on the creativity of banks and ATM vendors.

- ATM out of cash.
- Reduce withdrawal limit.
- Minimum limit cycle exceeded.

4) SafePass-*Lock:* In order to further mitigate the iteration attack, a lock can also be introduced in *SafePass*. This can be implemented by making the account unaccessible from *regular authentication* for t period of time, if any of the panic PIN is used. This will restrict the attacker from iterating over different combinations of PINs.

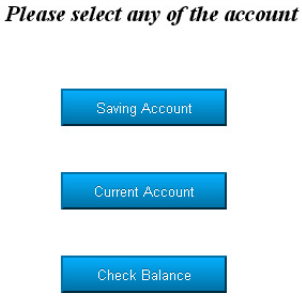

Fig. 4. Selection of different account types.

C. ATM Usage Flow with SafePass

In Fig. 1 we have presented the standard usage flow of ATM with *SafePass*. *SafePass* prototype runs in the following standard manner like all ATMs.

Suppose a user is short on cash, so he will walk over to the ATM. After approaching the ATM terminal, the user will insert his card into the card reader as shown in fig. 2. After inserting the card, the ATM terminal will prompt the user to select his desired language. It should be noted that the language selection varies from country to country. Fig. 3 displays a sample of how a generalized language selection interface may look like.

In the next step, the user will be provided options to select his account type if he wishes to make some transactions. The user can also simply inquire about his balance and leave (see fig. 4).

If the user is interested in withdrawing money or making some transfers, the ATM terminal will ask for a valid PIN code (see fig. 5). Based on the entered PIN the ATM terminal will perform a complete authentication procedure as follows.

- In the first iteration of the authentication procedure, the first 3 digits of the entered PIN code are validated against the regular PIN code assigned to the user.
- If the first 3 digits are mismatch, the server will prompt ”wrong input” and the user will have to re-enter the PIN.
- If the first 3 digits are matched, the server will proceed and verify the last digit. On successful verification the user will be allowed to make withdrawals (see fig. 6).

Fig. 5. Insertion of PIN code.

- In contrary, lets suppose a thief enters into the ATM room and the user has to perform authentication under duress. In this situation if the user will enter the panic PIN, the verification of 4th digit will fail and the ATM terminal will prompt the panic response like *out of cash, host not responding, maximum limit cycle exceeded* ... etc. In extreme cases, fake money can also be issued.

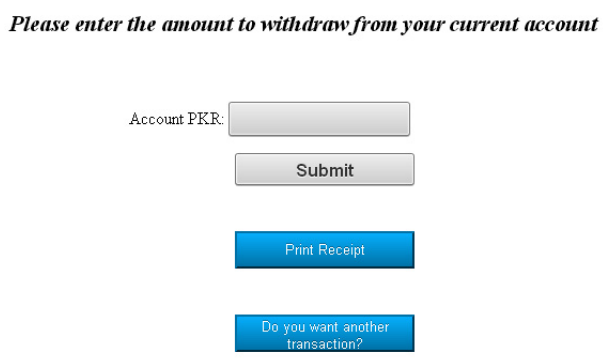

Fig. 6. Entering desired withdrawal amount.

IV. Conclusion

The domain of electronic passwords has been well studied and documented over the years. On the other hand there is a clear deficit of academic study on panic passwords. The literature review of non-classified documents reveals that panic passwords have applications in home security system and Internet voting. Despite the increasing number of physical thefts on ATMs, none of the ATMs have or have had a panic password based security mechanism to signal stress during authentication.

In this paper, we introduce *SafePass*, a new panic password scheme that can be easily deployed over the ATM infrastructure. In *SafePass*, the ATM users have to maintain one single PIN for regular authentication. In duress scenario the user only needs to change the final digit of the PIN. This will trigger the duress situation and the ATM machine will respond according. In *SafePass*, special attention is given from the usability perspective as it would be extremely valuable for large scale proliferation. Future work in this direction would be to conduct a user study among various age groups related to the usability of the proposed scheme.

References

[1] European atm security. https://www.european-atm-security.eu/.
[2] New way of atm robbery in karachi. http://www.unewstv.com/4661/new-way-of-atm-robbery-in-karachi-beware-while-using-atm-machines.
[3] Truecrypt. http://www.truecrypt.org/.
[4] William Cheswick. Johnny can obfuscate: beyond mother's maiden name. In *Proceedings of the 1st USENIX Workshop on Hot Topics in Security*, HOTSEC'06, pages 6–6, Berkeley, CA, USA, 2006. USENIX Association.
[5] Sonia Chiasson, Alain Forget, Elizabeth Stobert, P. C. van Oorschot, and Robert Biddle. Multiple password interference in text passwords and click-based graphical passwords. In *Proceedings of the 16th ACM conference on Computer and communications security*, CCS '09, pages 500–511, New York, NY, USA, 2009. ACM.
[6] Jeremy Clark and Urs Hengartner. Panic passwords: authenticating under duress. In *Proceedings of the 3rd conference on Hot topics in security*, HOTSEC'08, pages 8:1–8:6, Berkeley, CA, USA, 2008. USENIX Association.
[7] Katherine M. Everitt, Tanya Bragin, James Fogarty, and Tadayoshi Kohno. A comprehensive study of frequency, interference, and training of multiple graphical passwords. In *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems*, CHI '09, pages 889–898, New York, NY, USA, 2009. ACM.
[8] Dinei Florêncio, Cormac Herley, and Baris Coskun. Do strong web passwords accomplish anything? In *Proceedings of the 2nd USENIX workshop on Hot topics in security*, HOTSEC'07, pages 10:1–10:6, Berkeley, CA, USA, 2007. USENIX Association.
[9] Marcia Gibson, Karen Renaud, Marc Conrad, and Carsten Maple. Musipass: authenticating me softly with "my" song. In *Proceedings of the 2009 workshop on New security paradigms workshop*, NSPW '09, pages 85–100, New York, NY, USA, 2009. ACM.
[10] R. K. Russikoff. Computerized password verification system and method for atm transactions. United States Patent, 6871288, 2005.
[11] Matt Weir, Sudhir Aggarwal, Michael Collins, and Henry Stern. Testing metrics for password creation policies by attacking large sets of revealed passwords. In *Proceedings of the 17th ACM conference on Computer and communications security*, CCS '10, pages 162–175, New York, NY, USA, 2010. ACM.