Norwegian Information Security Conference
Norsk Informasjonssikkerhetskonferanse

NISK 2012

Bodø 19.–21. november 2012

Program Chair

Vladimir Oleshchuk UiA

Program Committee

Patrick Bours HiG
Katrin Franke HiG
Martin Gilje Jaatun SINTEF
Kristian Gjøsteen NTNU
Tor Helleseth UiB
Erik Hjelmås HiG
Svein Johan Knapskog Q2S
Hanno Langweg HiG
Stig Frode Mjolsnes NTNU
Geir Myrdahl Køien UiA
Leif Nilsen UNIK
Chunming Rong UiS
Ragnar Soleng UiTø
Håkon Styri NPT
Nils Kalstad Svendsen HiG
Hugues Verdure UiTø
Eli Winjum FFI

Norwegian Information Security Conference
Norsk Informasjonssikkerhetskonferanse

NISK 2012

University of Nordland, Bodø
19-21 November 2012

Program Chair
Vladimir Oleshchuk UiA

Program Committee

Patrick Bours	HiG
Katrin Franke	HiG
Martin Gilje Jaatun	SINTEF
Kristian Gjøsteen	NTNU
Tor Helleseth	UiB
Erik Hjelmås	HiG
Svein Johan Knapskog	Q2S
Hanno Langweg	HiG
Stig Frode Mjolsnes	NTNU
Geir Myrdahl Køien	UiA
Leif Nilsen	UNIK
Chunming Rong	UiS
Ragnar Soleng	UiTø
Håkon Styri	NPT
Nils Kalstad Svendsen	HiG
Hugues Verdure	UiTø
Eli Winjum	FFI

ISBN 978-82-321-0012-5

Redaktør: Vladimir A. Oleshchuk
Digital trykk og innbinding: AIT Oslo AS

Vi bruker miljøsertifiserte trykkerier

Akademika forlag
Postboks 2461 Sluppen
7005 Trondheim
Tlf.: 73 59 32 10
E-post: forlag@akademika.no
www.akademikaforlag.no

Forlagsredaktør: Lasse Postmyr (lasse.postmyr@akademika.no)

Content

Biometrics

Security evaluation

Attacks and vulnerabilities

Security Risk Management

Preface

Welcome to NISK 2012, the fifth addition of the Norwegian Information Security conference. It will take place in Bodø on the 19th-21st of November. As before, the conference will be collocated with NIK and NOKOBIT. NISK 2012 is sponsored by FRISC - Forum for Research and Innovation in Security and Communications, a value network in VERDIKT program, funded by the Norwegian Research Council.

This year we had 21 high quality submissions from 10 different institutions. One of these submissions was withdrawn. The remaining 20 submissions were reviewed by 2 members of the Program Committee each and based on their feedback 13 papers were selected for presentation and publication in the Proceedings. All 13 papers will get 30 minutes timeslot for presentation and discussions. In addition to regular presentations, we will have a special session on Biometrics organized by professor Christoph Busch and a tutorial "Bro - Intrusion detection system - Principles of operation and internal structure" given by professor Slobodan Petrovic (both from Gjøvik University College).

I would like to thank all the members of the Program Committee for their efforts and valuable comments.

NISK 2012 PC Chair
Vladimir Oleshchuk

Grimstad, October 2012

Alternative PIN Entry Method

Einar Krokan and Kirsi Helkala
Gjøvik University College, Norway
{einar.krokan, kirsi.helkala}@hig.no

Abstract

People with different disabilities have difficulties to use public access terminals. Difficulties may lower security if a person is unable to follow correct procedures, but is forced to create shortcuts. Instead of changing a PIN entry method, this paper introduces an alternative PIN entry method that is implementable already existing public access terminals, and therefore let users to choose the method that suits best for them. We carried out a pilot experiment testing both the traditional and the alternative entry method among visually impaired and people with normal vision. We focused on usability, universal principals and robustness against observation attacks.

1 Introduction

Public access terminals, like ATMs and payment terminals, are something people use daily basis. Most of us are familiar with usage procedures and find them easy. Even though usage of the public access terminals is ruinous for most of us, it is not for everyone. People with different disabilities; especially visually impaired and people with upper extremity disability find the use of these terminals troublesome.

Public access terminals are not equally accessible and similarly secure for everyone. The situation would be more satisfying, if two main shortcomings could be corrected. First issue handles on design of the terminals. Different layouts, different modes and missing tactile markings make the use of the terminals uncomfortable for people with reduced vision. This also affects security, because skimming equipments are harder to notice, even for a person with normal vision. Second issue also affects security of the PIN codes. Users do not often cover their PIN codes. This is either a mistake or caused by disability. Especially people with visual impairment or reduced movements cannot cover codes. Because the covering is not possible for everyone, the layout of the terminal could be changed so both visual and sound signals would be better covered. Also a new method to enter PIN codes could be an alternative solution.

This paper addresses to these shortcomings and presents a new PIN entry method that is implementable already existing public access terminals. Most of terminals have two keys unused on the lowest numeric row. Because the new alternative method only needs two keys, the existing terminals can adapt to the new solution.

This paper was presented at the NISK-2012 conference; see http://www.frisc.no .

Therefore, terminals would contain both the traditional and the new, alternative entry method. User adaptable methods were asked for in [5, 10].

The paper is structured as follows. Section 2 discusses on several other methods that are suggested to be used instead of the PIN codes. Section 3 presents the new, alternative PIN entry method. Experiment is described in Section 4 and results are shown in Section 5. Discussion is found in Section 6 and finally Section 7 concludes the paper.

2 Related Work

There are several methods that are suggested for replacing the PIN codes. One approach is use of graphical passwords [11]. A graphical password is a set of pictures. When it is entered, each password picture is selected from a different set of database pictures. Graphical passwords are easier to remember than character passwords [4]. However, they might be easily observed.

The Convex Hull Click (CHC) was presented by Wiedenbeck et al. [11]. Here a user has to recognize a set of pictures, create a mental convex hull and then point this area on the screen. The convex hulls are generated to different areas on the screen for each login making observation attacks difficult.

Roth et al. [9] presented a method, which they refer as cognitive trapdoor game or probabilistic cognitive trapdoor game. A user does not enter a digit directly but by selecting a right group (either black or white) containing that digit. It takes four rounds to enter a PIN code and therefore, a transaction time is much longer than with the traditional method. However, the method provides improved security against shoulder surfing attacks even when an attacker fully observes a PIN entry. The method showed to be easy to use, because after participants of the test had learned the method they did not do any more errors than with traditional method.

EyePassword, presented in [7], makes shoulder surfing also an difficult task. With this method a user enters a password or PIN code by using eyes. A camera that is able to monitor eyes of the user observes the point the user is looking at on the screen. However, solution is less likely to be used in ATMs and payment terminals, because calibration of the camera is needed for each user.

The methods discussed above might be more robust against observation attacks than traditional PIN code entry method, but they are not suitable for people with visual impairment. PIN code might be difficult, but these methods are impossible to use for them. Methods using tactile markings and feedback are better suitable.

De Luca et al. [2] present VibraPass -model where users cell phone is used to receive signals from a terminal during authentication procedure. The cell phone vibrates if the user enters a fake input. A password would then consist of both correct and incorrect inputs. An observer would not, by watching authentication procedure once, be able to get the correct password if some of the values entered by the user were incorrect. However, repeated observations would reveal the password.

Tactile feedback has also been used in [6]. Here, a special hardware was used. Tactile markings on a mouse buttons changed to form a pattern, when a user moves the mouse over an item on the screen. They claim that security is enhanced, but usability has to be improved as authentication procedure takes long time.

The presented solutions above require new hardware with new screens, cameras and input devices. Our method does not need a new hardware but can be installed to existing one.

3 Alternative PIN Entry Method

The new PIN entry method uses two separate buttons, one for providing a digit and one for separating digits. We call these keys as ”Number” and ”Next”. Figure 3 shows a new keypad. To enter a PIN code, a user will have to press ”Number” key as many times as the first digit, then press ”Next” button to indicate that the first entry is finished. Then he continues with ”Number” key and enters the second digit. This is continued until the fourth digit entry is finished. The number zero is entered with just pressing the ”Next” key as indicating that a digit entry is finished. If the PIN code is 1234 user will press ”Number” key one time and ”Next” key then ”Number” two times and ”Next” then ”Number” three times and ”Next” , and then finally ”Number” four times and ”Next” . Figure 1 shows how ”2001” is entered.

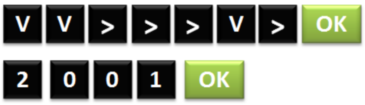


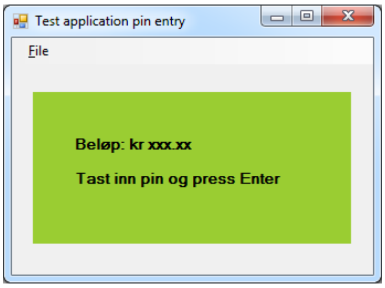
Figure 1: Code ”2001” entered with the both the new and the traditional way.

4 Experiment

We carried out an experiment to determine how the alternative PIN entry model performs compared to traditional entry method. We had persons with and without visual impairment as participants. Each participant was interviewed after PIN codes perform tests.

Visually impaired test persons were volunteers from a local association for visual impaired. The group consist of six persons, four women and two men, in age 35 to 62 years. The group of normal vision consisted of seven persons with about same age and gender diversity. However, the experience level of the participants was not equal. Among visually impaired, one person had never used payment terminals or ATM. Each participant was given same instruction before the test begun.

Figure 2 shows a Windows application, which was particularly created for the experiment. The application mimics PIN entry procedure found in most ATMs and payment terminals. For each PIN digit entered a star (*) is displayed. When ”Enter” is pressed the PIN is validated and information about correct or incorrect PIN entry is displayed. Normally, a payment terminal consists of four rows and three columns of keys with addition extra controls keys like ”Ok”, ”Cancel” and ”Abort”. Since we have only 10 numbers, the keys placed at both sides of zero-key



Beløp: kr xxx.xx

Tast inn pin og press Enter

Figure 2: The application used in experiment.

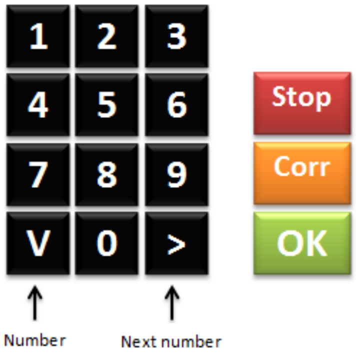


Figure 3: A keypad with the "Number" and "Next" keys on both sides of the zero key.

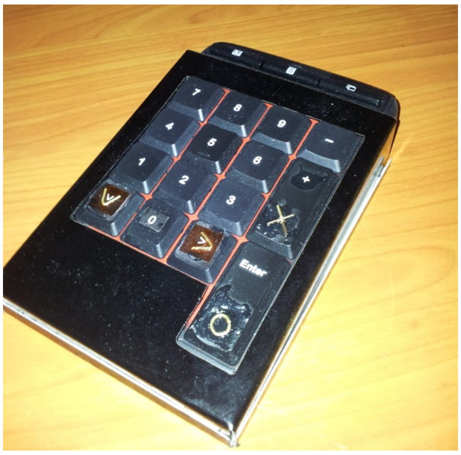


Figure 4: A picture of our prototype payment terminal keyboard.

at the bottom are not often used. Therefore, our PIN entry method uses these two keys as the alternative input method for the PIN code. Figure 3 shows an example of our new key pad. We have placed the control keys on the right side of the keypad.

Because we did not have access to a real payment terminal or ATM keyboard, we used an external wireless keypad that was modified to mimic a payment terminal. A prototype is shown in Figure 4. Tactile cues with down and right arrow are added on the keys. Both entry methods are implemented on the same prototype terminal.

Measurements

We timed PIN entries, noted down wrongly entered PIN codes, filmed each entry session and interviewed participants to compare usability, accessibility and security of the new and traditional PIN entry method.

Usability

We look usability with terms used in [8]. Terms are learnability, efficiency of use, memorability, few and non-catastrophic errors and subjective satisfaction.

Universal design

Interviews were mainly used to determine if the alternative PIN code method satisfies principals of the universal design [3]. The principals are as follows.

1. *Equitable Use*: The design is useful and marketable to people with diverse abilities.

2. *Flexibility in Use*: The design accommodates a wide range of individual preferences and abilities.

3. *Simple and Intuitive Use*: Use of the design is easy to understand, regardless of the user's experience, knowledge, language skills, or current concentration level.

4. *Perceptible Information*: The design communicates necessary information effectively to the user, regardless of ambient conditions or the user's sensory abilities.

5. *Tolerance for Error*: The design minimizes hazards and the adverse consequences of accidental or unintended actions.

6. *Low Physical Effort*: The design can be used efficiently and comfortably and with a minimum of fatigue.

7. *Size and Space for Approach and Use*: Appropriate size and space is provided for approach, reach, manipulation, and use regardless of user's body size, posture, or mobility.

Security
The new PIN entry method uses same number size than the traditional method and therefore, they both provide same search space entropy. However, it is minimum security that counts. Security is lowered by how easily PIN codes can be observed by a third person. Therefore, we are interested to compare entry methods in robustness against shoulder surfing. We recorded PIN code entries and used techniques such as slow motion and picture enlargement to observe codes from recordings.

5 Results

The alternative PIN entry method is evaluated based on its usability, compliance on universal design and robustness against shoulder surfing.

Usability

Learnability: Each participant got a brief description of the new PIN entry method and they were allowed to try the method before actual test. After the test, each participant was interviewed to evaluate learnability of the new method. The participants were mostly concerned about how to enter zero-digit and how to move to the next digit. Most of the participants found the new PIN entry method easy to learn.

	Average	Median	Min	Max
Trad. Entry Method				
Visual impairments	10.33s	3.24s	1.9s	32.23s
No visual impairments	2.8s	2.54s	1.54s	5.60s
All	5.43s	2.61s	1.54s	32.23s
New Entry Method				
Visual impairments	28.06s	20.43s	7.34s	53.73s
No visual impairments	14.64s	13.34s	7.62s	26.24s
All	19.52s	15.87s	7.34s	53.73s

Table 1: PIN code entry times for both methods.

Efficiency of use: The time to enter PIN code was measured from the first key press to the moment when the last ”enter”-key was pressed. This time also included corrected errors. Each participant typed same password three times. The first trial was not used in analysis because it was considered as a learning phase. In order to compare methods each participant used the same PIN code.

On average participants used 5,4s with the traditional method and 19,5s with the new method. For people with normal vision, average time for the traditional method was 2,8s and for the new method 14,6s. In the group with visual impairments the average time for the tradition method was 10,3s and 28,1s for the new method. Extreme values have a high effect to average, especially when the test size is small like in our case. Therefore, the better estimate of times is gotten from median values. The median time correlates better with a transaction time 2s for the traditional method found in study [1]. Average, median, minimum and maximum times are shown in Table 1.

The new method is clearly slower than the traditional method in all groups. However, this was not totally unexpected, because the new method requires more key presses, especially with high numbers. In our test case, a code 9067 was used. To type this code with the new method 24 key presses are needed.

Even though it took ca. six times longer to use the new method in the experiment, many participants thought that they would be faster after using the method a longer period of time.

Memorability of the method: Since we only had one session with participants we could not measure memorability of the method quantitatively. Based on the participants comments in the interview, the use of the method is easy to remember after one has once learned it.

Few and non-catastrophic errors: Wrongly typed codes were counted. In total, we had eight errors with the traditional method and ten with the new method. We recorded a total of 78 tests with the traditional method and 78 tests with the new method. The new method had slightly more errors than the traditional method, but there was no statistical difference. Table 2 shows error rates for both of the methods.

Subjective satisfaction: The interviews were also used to answer this question. Only one of the participants was sceptic to the alternative solution and liked the

	Number of tests	Errors with Trad. Method	Errors with New Method
Visual impairments	36	3 (8%)	6 (17%)
No visual impairments	42	5 (12%)	4 (10%)
All	78	8 (10%)	10 (13%)

Table 2: Errors in both PIN entry methods.

traditional method better. Most of the users found the new method unfamiliar, but thought it would be easier if they use it regularly. Some complained that they needed to be much more focused on the task, as they had to count silently, while others found this a good thing. Most of the visually impaired participants found it easier to locate only two buttons than operate with ten as with the traditional method.

Universal design

Equitable Use: First principle states that the design should be marketable to people with diverse abilities. The alternative PIN entry method was tested with both visually impaired and people with normal vision. Both groups were able to use the method, even though it was unfamiliar in the beginning.

Flexibility in Use Second principle states that the design should provide choice of method. Our prototype supports both the new and traditional PIN entry method being therefore adaptable to users preferring. The prototype can also be used both right and left-handed.

Simple and Intuitive Use: The interviews showed that the new entry method is simple to use after one has learned it. However, either the prototype or the new entry method fully satisfies the third principle. The principle states that a solution should provide effective prompting and feedback during and after task completion. Our prototype only provided visual feedback during the PIN entry in the form of stars (*) for each entered number. Obviously, this is not enough for visually impaired. Real terminals give similar visual feedback. In addition, some terminals provide sound when buttons are pressed. Sound feedback is dangerous with the new method, as it would make it easy to count a number when key is pressed. Some visually impaired participants mentioned that one of their biggest challenges with payment terminals in general, is to know when to enter a code, because information is only given on the screen. This problem cannot solve by any PIN entry method, because the problem occurs before actual entering.

Perceptible Information: Tactile markings were added on both keys used in the new entry method. The markings were formed as a down arrow for the key to enter the number and a left array for the next number key. In addition, Contrast colours can also used to make keys more visible for those who benefit visual cues.

Tolerance for Error: Authentication with PIN codes and passwords does not provide the possibility to be half right or half wrong. The PIN code has to be entered correctly or access is denied. Therefore it is important that a solution has an option to correct wrongly entered digits. Our prototype only offered an abort button to cancel whole entry session. The participants who made errors felt that also a cancellation of last entered digit should have been made possible because now they had to enter the entire code again from the beginning.

Low Physical Effort: Neither of the PIN entry methods need much physical effort. However, if the comparison is made, the new PIN entry needs tiny bit more physical effort due to the longer entry time.

Size and Space for Approach and Use: The new PIN entry method satisfies this last principal, because it only consists of two keys, which makes it very easily reachable for all. In reality, the terminal itself should also be placed so that it is reachable for everyone. If a terminal is placed high, it is difficult to touch when sitting on a wheel chair. The new entry method might be easier in this case, because the keys it uses are at the lowest row. However, the choice of the method should be left to a user, and terminal as a whole, should be placed low enough.

Security

Shoulder surfing: In experiment all PIN code entries were recorded. The recordings were then manipulated with several techniques, which could help the observation. We were able to reveal 63% of the traditional method entries and 51% of the new method entries. Figures 5 and 6 show charts of the results. The finding indicates that the alternative entry method is a bit more resistant against visual observation attacks that the traditional. However, the test size is too small to withdraw statistically sound results.

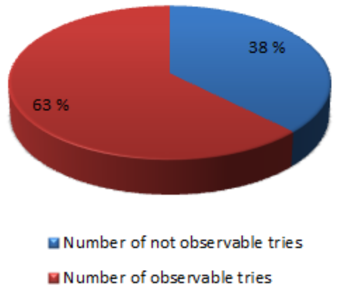


Figure 5: Percent of observed PIN codes typed with the current method.

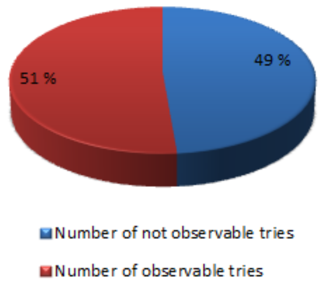


Figure 6: Percent of observed PIN codes typed with the new method.

6 Discussion

The participants of the experiment were people with normal vision and visual impairment. One of the participants was also dyslectic. He normally memorises passwords and PIN codes as a pattern on the keyboard. He liked the new method because the counting helped him to remember PIN code better.

One problem with our solution is that it does not directly tell the user what to do. Current PIN entry method is obvious to most users because it has been on use a long time. With our solution there is a larger need for explanation and training.

When studying recordings, we noticed that there was a difference in recognizing the code typed with differently handed persons when the camera was placed behind the right shoulder. The reason for this is that the fingers are partly covered by palm of the hand when the camera is placed behind the typing hand. Using two cameras on both sides would probably have given a higher percentage of observations of both methods. None of the participants covered their entries with the other hand during the experiment.

The results indicated that the new entry method might be a bit more robust against visual observation attacks. However, we found a channel that can be used to reveal PIN codes. Mechanical sound of the keys when they are pressed might be laud enough to give a way the code, even if the terminal is in a silent mode. If the method is to apply in real system, the mechanical sound needs to be eliminated somehow.

Another problem with our method is that it takes longer time. If users are able to select their own codes, they may select codes that take shorter time to type in order to save time. This could reduce security based on the search space entropy, because digits that are quick to type are small numbers.

7 Conclusion and Future Work

In this paper, we presented an alternative PIN code entry method, which uses only two keys on the normal numeric keypad. These keys are located both sides of zero button, and currently they are unused in most terminal. Therefore, this entry method can be implemented already existing public access terminals and used as an alternative for the traditional entry method.

The PIN entry method was well received by participants with and without visual impairments. They found it unfamiliar, but easy to learn. However, if the method is taken into use, the use of method needs to be thought, as it is not as intuitive as the traditional method. The visual impaired participants liked the method because it only used two keys, which, in addition, were easily located.

The method was significantly slower than the method we use today. However, it applies to universal design principals. The negative issue is the lack of the non-visual feedback. This is left for the future work.

The results implied that the new method might improve security being a bit more resistant against shoulder surfing. Especially higher numbers on PIN codes where harder to observe than smaller ones. But due to the small amount participants, the results are not statistically valid. However, it was also noticed that codes could be observed by listening mechanical sound of the keys. This is a problem, which needs to be solved before the method can be applied.

References

[1] A. De Luca, M. Langheinrich, and H. Hussmann. Towards understanding ATM security: a field study of real world ATM use. In *Proc. of the 6th Symposium on Usable Privacy and Security*, SOUPS '10, pages 16:1–16:10. ACM, 2010.

[2] A. De Luca, E. von Zezschwitz, and H. Hussmann. Vibrapass: secure authentication based on shared lies. In *Proc. of the 27th international conference on Human factors in computing systems*, CHI '09, pages 913–916. ACM, 2009.

[3] Center for Universal Design. The principles of universal design. www.ncsu.edu/project/design-projects/udi/center-for-universal-design/the-principles-of-universal-design/, May 2011 (Visited 4.5.2012).

[4] K. Fuglerud and O. Dale. Secure and inclusive authentication with a talking mobile one-time-password client. *Security Privacy, IEEE*, 9(2):27 –34, March-April 2011.

[5] K.S. Fuglerud, A. Reinertsen, L. Fritsch, and Ø. Dale. Universell utforming av IKT-baserte løsninger for registrering og autentisering, January 2009.

[6] R. Kuber and S. Sharma. Toward tactile authentication for blind users. In *Proc. of the 12th international ACM SIGACCESS Conference on Computers and Accessibility*, ASSETS '10, pages 289–290. ACM, 2010.

[7] M. Kumar, T. Garfinkel, D. Boneh, and T. Winograd. Reducing shoulder-surfing by using gaze-based password entry. In *Proc. of the 3rd Symposium on Usable Privacy and Security*, SOUPS '07, pages 13–19. ACM, 2007.

[8] J. Nielsen. *Usability Engineering.* Morgan Kaufmann Publishers Inc., San Francisco, CA, USA, 1993.

[9] V. Roth, K. Richter, and R. Freidinger. A PIN-entry method resilient against shoulder surfing. In *Proc. of the 11th ACM conference on Computer and Communications Security*, CCS '04, pages 236–245. ACM, 2004.

[10] C. Stephanidis. *The Universal Access Handbook.* CRC Press, Inc., Boca Raton, FL, USA, 1st edition, 2009.

[11] S. Wiedenbeck, J. Waters, L. Sobrado, and J.-C. Birget. Design and evaluation of a shoulder-surfing resistant graphical password scheme. In *Proc. of the Working Conference on Advanced Visual Interfaces*, AVI '06, pages 177–184. ACM, 2006.