© 2015 IJSRSET | Volume 1 | Issue 6 | Print ISSN : 2395-1990 | Online ISSN : 2394-4099
Themed Section: Engineering and Technology

Study and Analysis of Shoulder-Surfing Methods

Ojaswi Kasat*[1], Dr. Umesh Bhadade[2], Ms. Naimisha Trivedi[3]

[1,3]Department of Information Technology, L.D. College of Engineering, Ahmedabad, Gujarat, India

[2]Department of Information Technology, SSBT's COET Bambhori Jalgaon, Maharashtra, India

ABSTRACT

For accessing the ATMs for doing transactions or smartphones for accessing private information like emails, contact details, chatlogs, pictures, calendars, notes etc, PIN number is used as authentication for security purpose. To prevent the PIN number to be disclosed to the observer, it is necessary to not enter the actual PIN number but to enter a virtual PIN number which will confuse the observer about the original PIN number of the user. This virtual number will be different every time the users access the ATM, thus it will help to prevent the original PIN number to be disclosed to the observer. Several methods of shoulder surfing had been proposed from textual input to graphical input. Every method had its own merits and demerits and is useful according to the situation for a particular application. This paper gives a brief description of different types of textual and graphical shoulder surfing methods. The shoulder surfing methods discussed in this paper are analyzed with respect to time required to enter the virtual PIN number.

Keywords: Shoulder-surfing, PIN, Textual password, Graphical password, Security

I. INTRODUCTION

Shoulder surfing refers to a direct observation of PINs by looking over a person's shoulder or camera-based recording, to obtain information. The entry of a password can easily be observed in crowded place by standing next to someone.

There are two types of passive adversaries. The shoulder-surfing attacker is a weaker adversary whose capabilities are confined to those of a human. On the other hand, the camera-based recording attacker is a stronger adversary equipped with automatic recording devices Since PINs are so popularly used in, smartphones, automated teller machines (ATM), and pointof-sale (PoS) terminals. There is a great need for a secure PIN entry scheme that does not significantly sacrifice usability [1].

In this paper, we present various methods to prevent from shoulder surfing attacks, which uses textual and graphical based passwords to prevent from shoulder surfing attack, and we compare all those methods by using some parameters that are method type text based password or graphical, security, usability and time. The purpose of this review paper is to focus on drawbacks and advantages of all these methods and try to make some robust method by concentration on parameters security, usability and time to prevent from shoulder surfing attack.

This paper is organised in sections where Section II describes the various methods based on shoulder surfing attack, Section III compare all those methods, finally we conclude in Section IV.

II. METHODS AND MATERIAL

2. LITERATURE REVIEW

2.1 Textual Shoulder Surfing Methods

1. Mod 10 Method

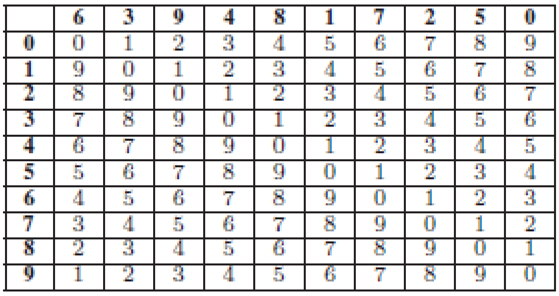
User has to remember a four digit PIN number from the set {0,1,..., 9}. User receives a challenge from the set {0, 1,..., 9}via a protected media. User will add the challenge digit with the corresponding PIN digit and will perform a modulo 10 operation. Finally he will enter back the obtained digit using a public keyboard. Suppose the first digit of the user chosen PIN is 5. User now securely receives a challenge 7 from the system. So the valid response by user will be (5+7) modulo 10 (which is equal to 2).

Advantages: This method is easy to use for math oriented people and gives good security against guessing the password.

Disadvantages: For non-math-oriented people this method is difficult to adopt. [4]

2. Mod 10 Table Method

Table I: User Lookup Table



	6	3	9	4	8	1	7	2	5	0
0	0	1	2	3	4	5	6	7	8	9
1	9	0	1	2	3	4	5	6	7	8
2	8	9	0	1	2	3	4	5	6	7
3	7	8	9	0	1	2	3	4	5	6
4	6	7	8	9	0	1	2	3	4	5
5	5	6	7	8	9	0	1	2	3	4
6	4	5	6	7	8	9	0	1	2	3
7	3	4	5	6	7	8	9	0	1	2
8	2	3	4	5	6	7	8	9	0	1
9	1	2	3	4	5	6	7	8	9	0

This Method proposed a concept of lookup table. If user chosen PIN digit is 5 and the system generated challenge is 7 then the user first goes to the row number 5 in the lookup table and subsequently goes to the digit 7 in that row. After that user will see the corresponding column number where 7 is placed (here 9) and enter back 9 as response corresponding to the first challenge. If the digits in the top row of Table I is arranged in ascending order from 0 to 9 then it will be equivalent as modulo 10 addition. [4]

Advantage: Because of lookup table easy to use as compare to Mod 10 Method.

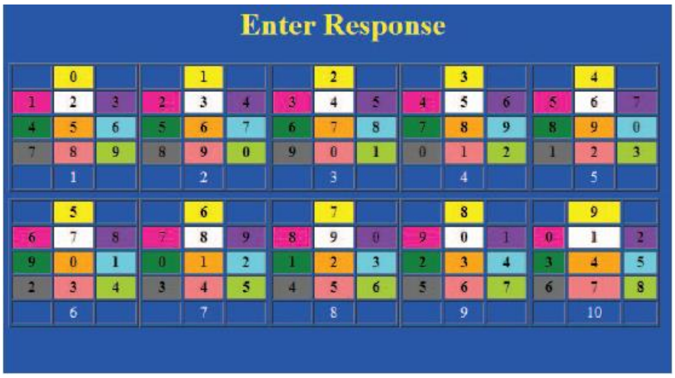
Disadvantages: Login time in this method goes high with respect to mod 10 method.

3. Color Pass Method

The proposed Color Pass interface is based on partially observable attacker model in which an attacker cannot see the challenge values generated by the system but can only see the response given by the user. While implementing user interface we have assigned unique colors to each Ci (i varies from 0 to 9) (shown in TABLE II). Ten colors is chosen in such a way so that each color is clearly distinguishable from other. The actual interface is shown in Fig. 1. For convenience we have marked each table number by white font to distinguish it from other digits (which are marked using black font) in the table. As the color cells position in each table is fixed so user can locate the desired colored cell quite quickly. This contributes in getting faster login time. Similarities between keypads in Color Pass, as shown in Fig.2 and classical PIN entry method makes our methodology more user friendly. Only the two extreme keys at the bottom row are kept unused. If user chooses Yellow Pink Violate Grey and receives challenge values 6 3 5 6 then seeing the interface in Fig.1 user will enter 5 3 7 2 using the key board showing at Fig. 2.[4]

Advantages: This Method scan be used by both math and non-math oriented people, shows significant low error rate during login procedure, robust against shoulder surfing attack.

Disadvantage: Based on partially observable attacker model.



Enter Response

	0			1			2			3			4	
1	2	3	2	3	4	3	4	5	4	5	6	5	6	7
4	5	6	5	6	7	6	7	8	7	8	9	8	9	0
7	8	9	8	9	0	9	0	1	0	1	2	1	2	3
	1			2			3			4			5	
	5			6			7			8			9	
6	7	8	7	8	9	8	9	0	9	0	1	0	1	2
9	0	1	0	1	2	1	2	3	2	3	4	3	4	5
2	3	4	3	4	5	4	5	6	5	6	7	6	7	8
	6			7			8			9			10	

Figure 1 : User Interface On Screen

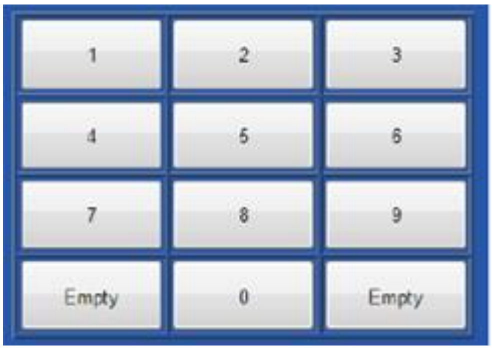
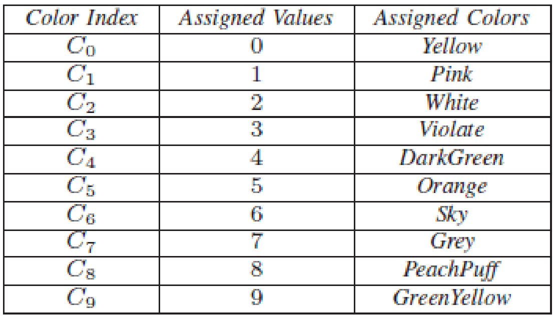


Figure 2: User Interface for Entering Response

TABLE II: Used colors for implementing feature tables



Color Index	Assigned Values	Assigned Colors
C_0	0	Yellow
C_1	1	Pink
C_2	2	White
C_3	3	Violate
C_4	4	DarkGreen
C_5	5	Orange
C_6	6	Sky
C_7	7	Grey
C_8	8	PeachPuff
C_9	9	GreenYellow

4. Randomized Square Matrix Virtual Keyboard

The primary objective of this method is to make the keyboard easily. For this reason we have created an extension for Google's Chrome browser. The extension has a popup window that has a randomized virtual keyboard containing buttons in a square matrix format. There are separate square matrices for alphanumeric and special characters. The user has to first locate that required character in the randomized keyboard. Alphanumeric keys are in the first block and special characters are in the second block. The input method is same for both. The user has to perform two button clicks to get the desired character. The first click (henceforth referred to as Row Click) can be on any button in the same row as the desired character of the PassBoard. The second click (henceforth referred to as Column Click) can be on any button in the same column as the desired character. This way he/she can input the entire password without actually pressing any of the characters that occur in his/her password, thus effectively preventing shoulder surfing. After he's done entering all the characters he/she can press the 'Done' button to copy the password onto the clipboard and subsequently paste it in the password field of the webpage.

Advantage: This also prevents keyloggers from capturing his/her keystrokes as the user does not have to use the physical keyboard to enter the password.[3]

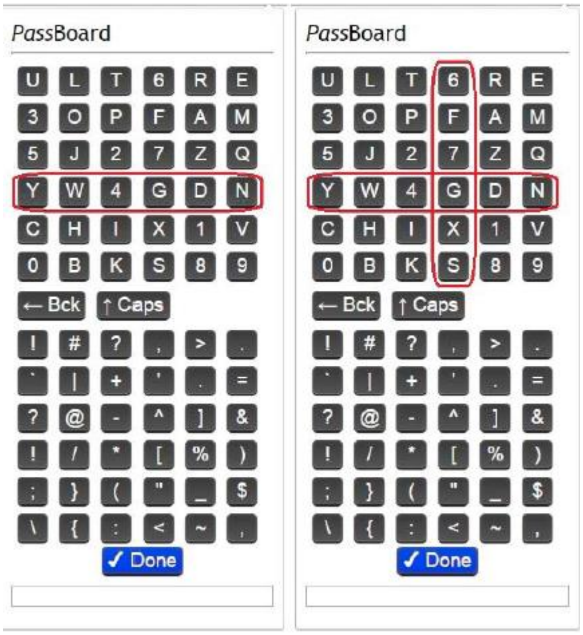


Figure 3. How PassBoard is used

2.2 Graphical Shoulder Surfing Methods

1. Puzzle Authentication Method

These panels are placed randomly in the display area. The user registers four authentication panels and four locations. Fig 4 shows an example of authentication. The user registered the four panels 5,7,4 and 9 as pass-numbers, and

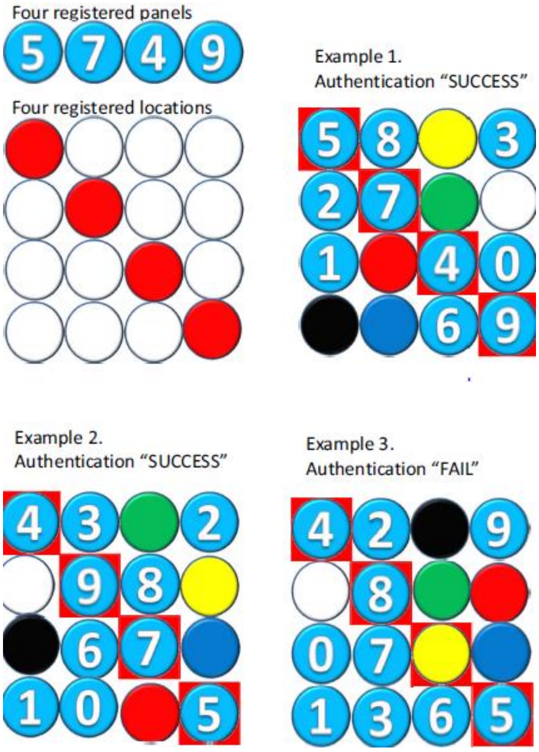


Figure 4. Example of authentication

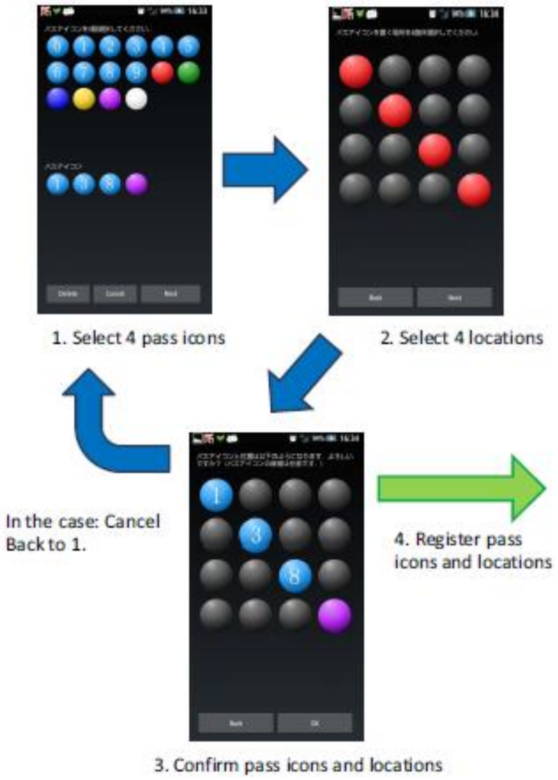

1. Select 4 pass icons
2. Select 4 locations
In the case: Cancel Back to 1.
4. Register pass icons and locations
3. Confirm pass icons and locations

Figure 5. Example of display of authentication information input

four locations(red panels) as pass-locations in Fig 4. If the four panels are placed (in any order) at the pass-locations, authentication is successful; otherwise authentication fails. The bottom left button(fig 6) called shuffle button, activates the rearranging functions, which rearranges the elements of the array randomly.

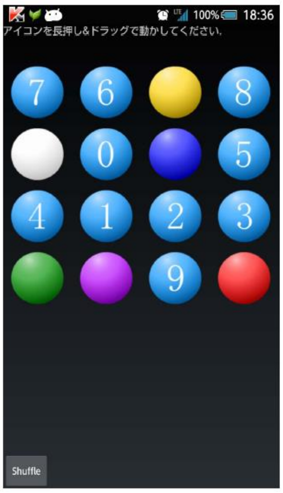


Figure 6. Example of the display for input of the authentication information.

2. Secure Pattern Based Authentication

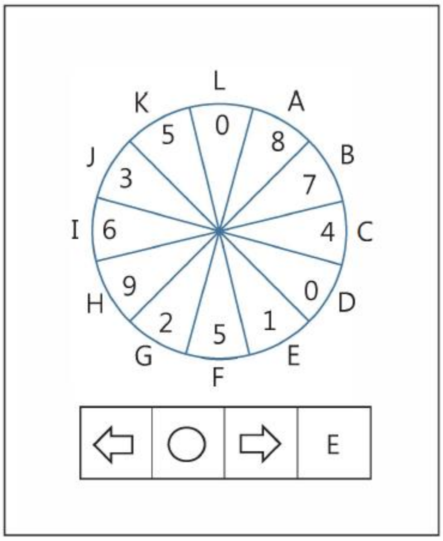


Figure 7. The view of the secure patter based authentication

Fig 7 shows the overview of the proposed scheme. The outer elements of the circle represent input gates whose position is fixed.

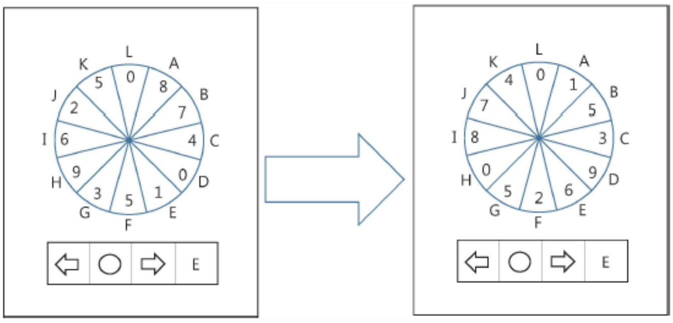


Figure 8. The example of the proposed authentication to make 1 selected (user password: 1234, input gates: AC)

The inner elements of the circle represent the input values whose position is randomly located. The process of the determination of the inner position is that first, each number in [0,9] is located randomly and then the rest of the inner blocks are determined by choosing random number in [0,9]. The below box is the interface to determine the input sequence of the user. The first box is a button to rotate the circle counter clock-wisely. The second box is a button to select the value. The small box is a button to rotate the circle clock-wisely. The last box is a button to determine the input sequence. [2]

User enrollment phase

The user enrollment phase is a step to set up a user password and environment for authentication. A user selects some numbers as a user password whose length is more than four. After selecting the password, the user should set the alphabets to make the sequence of the input gates. The length of the sequence of the input gates is in [1, N] where N is the length of the password. [2]

User verification phase

The user verification phase is a step to verify whether the input of the user and the stored password are the same. To make the valid input, the user should rotate the circle in Fig 7 and locate his password number in appropriate input gate and select the number. For example, when the password is 1234 and the sequence of the input gates is AC, then the user should locate the number 1 in A, the number 2 in C, the number 3 in A, and the number 4 in C for the successful authentication. So, in this example, the user clicks the first and third box button more than once, the second box button more than four times, and the last box button once to determine the input sequence in the end. [2]

3. BW Method

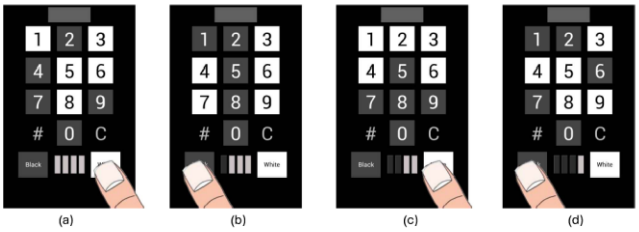


Figure 9. The IOC BW PIN entry scheme. The digit 1 is being submitted by the user in this example of a 4-round procedure

The basic BW method presents the decimal digit keypad to the user, in the standard layout, with random half of the keys colored in black and the other half colored in white, and the user must indicate the color of his PIN by pressing a separate black or white button. A 4-round procedure identifies each PIN digit, so that the 4-digit PIN entry requires 16 rounds to complete. Each single round operation is quite simple and intuitive to the user, but the large number of rounds causes practical usability issues.

Review of BW Scheme

Immediate Oracle choice: Fig 9 illustrates the entry of a single PIN digit through a set of 4 rounds of the IOC BW scheme. The user input is received by the system at each round, immediately after the display of the colored numeric keypad.

Delayed Oracle choice: One could understand Fig 9 as a DOC procedure if the bottom input buttons are removed and the delayed user inputs are illustrated after the 4-th box. However this version requires higher mental effort from the user, such as remembering a sequence of colors.

RR(Recording Resilience) Variants of BW scheme: The RR variant of the BW method attempts to provide security against adversaries that are equipped with camera-based recording devices. The approach was to remove one round from the 4-round process required for each PIN digit entry. This creates ambiguity in the PIN digits to the observer, and the adversary is forced to guess the correct 4-digit PIN from a pool of possible PIN.[1]

Disadvantages: Round redundancy, restrict to length 4, security up to few camera-based recording.

4. Tictocpin: Colored Pin Entry, Strengthened Through A Hidden Auxiliary Channel

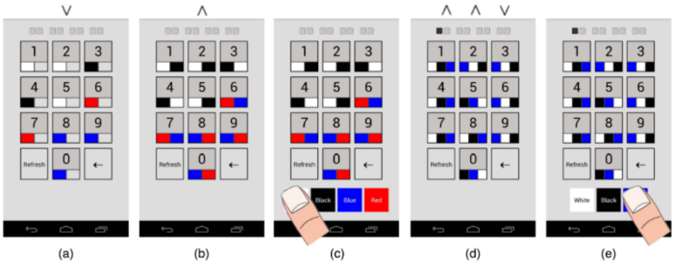


Figure 10. TictocPIN scheme — A running example of submitting the digit 1 through a 2-round procedure.

Description of TictocPIN

The ingenuity of the BW method was in assigning colors to numeric keys and opting to receive each PIN digit through a *multi*-round challenge-response procedure. In particular, the colored challenges allowed for *intuitive* user responses. In our improved scheme a smaller number of rounds is used and the user is informed through a vibrotactile channel as to which of multiple displayed challenges is to be taken as valid.[1]

PIN Entry Example

Let us explain the execution example given by Fig 10, which illustrates the entry of the single PIN digit 1 through the TictocPIN system. Fig 10(a) is first displayed with a short 30 msec vibration. The left box under the 1-key is colored in white and the right box is left empty. Note that there is no color keypad at the bottom. After a 500 msec pause, which includes the 30 msec vibration, the right boxes under the digits are additionally colored as in Fig 10(b), and a simulated sound of vibration is produced. This display is maintained for 500 msec, after which the display changes to Fig 10(c). The color pad has appeared below the numeric keypad to serve as the user input interface. The first round of the key entry ends with the user pressing white. The displays for the subsequent three 500ms intervals, which form the challenge presented by the second round, is compressed into Fig 10(d). The left, middle, and right boxes under each of the ten digits are incrementally filled with colors, with each display lasting 500 msec. The first two phases are accompanied by simulated vibration sounds and the third phase arrives with a real short vibration. Finally, the input color pad appears as in Fig 10(e), and the user presses the blue key, the color under the 1-key that appeared with the vibration, to completes the second round of the key entry. The PIN digit 1 was successfully entered to the system through these two rounds. Further PIN digits may be entered through similar processes.[1]

III. RESULTS AND DISCUSSION

Comparison of Methods

No.	Method Name	Method Type	Security	Usability	Time
1	Mod 10 method	Textual	Secure	Math Oriented	Less login time than Mod 10 Table Method
2	Mod 10 Table Method	Textual	Secure	Easy To Use	Login time high
3	Color Pass Method	Textual	Quite Robust	User Friendly	Takes less time for login
4	Randomized Square Matrix Virtual Keyboard	Textual	Effectively Prevent Attack	Easy To Use	Take less time
5	Secure Pattern Based Authentication	Graphical	Resilient To Theft, Unlinkable, Robust	Easy To Learn	Moderate
6	Puzzle Authentication Method	Graphical	Robust	Easy To Learn	Moderate
7	BW Method	Graphical	Moderate	Because of 16 rounds, practical usability issue	Slower compared to other methods
8	TicToc Pin Entry Method	Graphical	Resilient To Camera Recording, Robust	Moderate	Slower compared to other methods

Table III: Comparison of various methods

IV. CONCLUSION

In this paper we had studied different textual and graphical methods of preventing shoulder surfing attack. From Table III, it is seen that the time required to enter the PIN using this Textual methods is little more as compared to the time required to enter the graphical methods. Because textual methods is based on computations, where Mod 10 method takes more time for login than Mod 10 table method and Color pass method because Mod 10 is fully math oriented but Mod 10 table and Color pass method are user friendly and takes less login time for login compared to Mod 10 method. Graphical methods, BW method have several drawbacks, such as round redundancy, unbalanced key press, recording non- resilience the more strengthened TictocPIN method requires smaller number of rounds than original BW method.

V. REFERENCES

[1] Taekyoung Kwon, *Member, IEEE, and Jin Hong* *"*Analysis and Improvement of a PIN-Entry Method Resilient to Shoulder-Surfing and Recording Attacks*"*

[2] Hyungjun Shin, Daeyoung Kim "Secure Pattern-based Authentication Against Shoulder Surfing Attack in Smart Devices"

[3] Pradyumn Nand, Prashast Kumar Singh" Prevention of Shoulder Surfing Attack using Randomized Square Matrix Virtual Keyboard"

[4] Nilesh Chakraborty, Samrat Mondal "Color Pass: An Intelligent User Interface to Resist Shoulder Surfing Attack"

[5] Mirang Park, Yoshihiro Kita, Kentaro Aburada, Naonobu Okazaki " Proposal of Puzzle Authentication Method with Shoulder-Surfing Attack Resistance