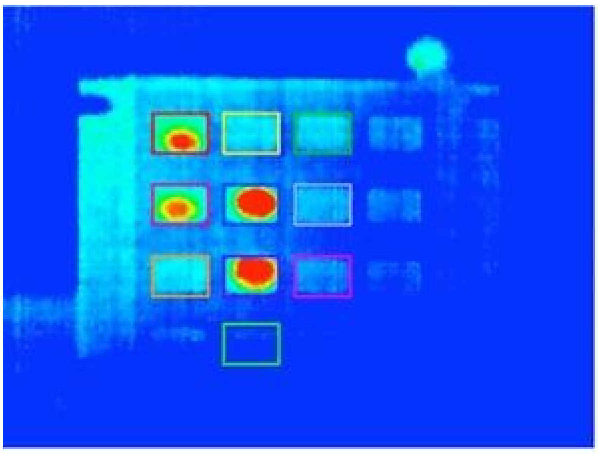
BANKING APPLICATIONS IN TILLS AND WEB – PROBLEMS WITH THE CURRENT DESIGN

There was a time when people used to withdraw money from the bank if they needed money for different usages. Now, the time is changed and thanks to the people who invented technologies to make it easy for billions of people around the world. With the new born technology there are people (Hackers) who are born to exploit the bugs in it. That's where testers can help find bugs and developers fix them before they can be exploited by bad guys out there. Let me stop the story here and talk about what are the problems in current implementation of banking applications; I am considering ATM machines and Internet Banking web applications.

ATM APPLICATION

My dad yesterday was telling me that nowadays, hackers use a technique of heat-maps for identifying the PIN for the debit card. So how does it work? The hacker enters the ATM location quickly once genuine end-user leaves after transaction. He / she get inside and can get the last 4 pressed keys from 0 to 9 based on the heat-map generation.

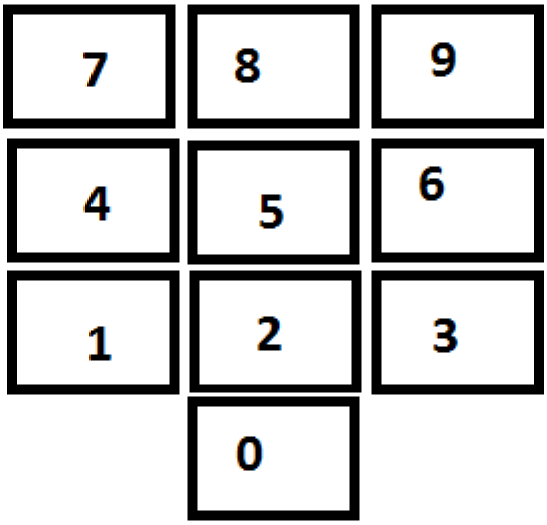
Heat-maps could look something like below on a number pad,



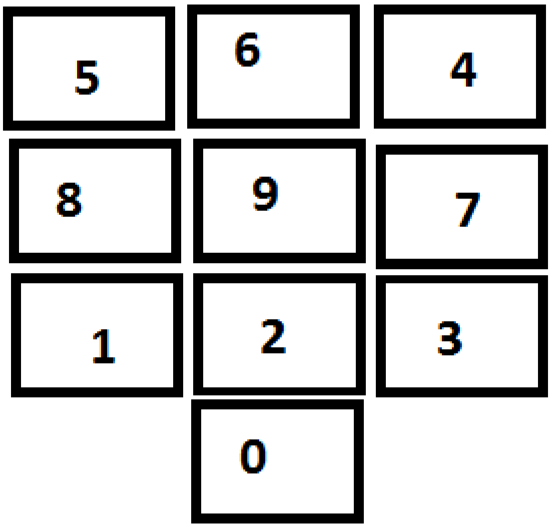
Now, my dad asked me how one could solve it? He said after entering the PIN he can rub with some material or else he could press all the buttons once so that equal intensity of heat-map is generated. Now, my answer to him was: That is something that you are doing by your awareness to avoid such instances. What about those people who are not aware about it and being victimized?

That's when I spoke about how technology could be helpful and what solution or the design should be thought of to avoid it from the technology perspective. After some thought going in my brain I thought of the below solution, Use touch screen based input at least for number pad which is used to enter PIN and once transaction is done, jumble up all the digits from 0 – 9 in a random fashion or in some proprietary algorithmic way. Now, heat-maps are static and do not move with the numbers LOL. And hacker is shown 4 digits which are wrong. Now, in place of 0 where heat-map is produced it is digit 9.

Example: During the start of transaction the number pad has the following numbers arranged. The end-user will input the PIN and collect the money.



Once the transaction is completed, the number pad should randomly re-arrange the numbers and show something like following for the next end-user.



However, a little care needs to be taken here so that algorithm or pattern is not cracked. Example: Whenever 9 are displayed in the first location in the first row, it is equivalent to 0 or some other digit. Hard-coding could be dangerous as it could be cracked by reverse-engineering.

I hope you got the idea. For those banking industries that do not have it yet, please think about this approach. I see that even touch-screen based ATM or tills do not have this rambling of number on number pad for every transaction. I hope you will care about your end-users privacy and security in the coming days / months / years.

INTERNET BANKING WEB APPLICATION

I hope most of you use online banking (Internet Banking) and you must have come across on-screen keyboard provided by the web application and they say that it is for security reasons where hacker should not get access to your account using keyloggers which records the keystrokes from your keyboard. Now, I am not sure if the solution architects of those kinds of applications knew that there are keyloggers which could take screenshot for every click that is done.

How would one get IPIN when end-user uses on-screen keyboard to enter the IPIN using mouse device by click operation?

1. Let us say IPIN is composed of 4 characters
2. It means 4 clicks have to be made on the on-screen keyboard
3. 4 clicks means 4 screenshots
4. Now, looking at the screenshots generated it is easy to know what are the 4 characters that were clicked which is IPIN
5. Now, you might say there are different combinations again for hacker to identify the sequential order of those 4 characters
6. It is simple, he / she need not bother about it as he / she can look into the date time of the file generated which will easily let him / her know about the sequential order of the IPIN characters

How secure do you feel now? Now, to make one more straightforward point; even script kiddies can do this and not core hacking skills is required however, we can still call it was hacked. Now, this is the current problem but, what is the solution for this.

Solution to the above problem is,

The attacker while looking at the screenshot uses the mouse pointer as the reference to get the character that was clicked. Now, there could be multiple solutions. Here are few examples which you would like to suggest your organization or use it in your product which you might be developing or you have already developed.

1. When click is made on any one of the character, at particular exact instance show dummy mouse pointers which look alike displayed on all the characters on the on-screen keyboard. Now, in the screenshot there is no clue about which character was clicked because there are mouse pointers on all the keys. Once the click is done the dummy mouse pointers should become disabled. You see how this solution serves both Usability and Security without compromising on any one of these. How is that?
2. You could also write an AJAX script which will show some picture of company logo in the space of on-screen keyboard when any character is clicked. Example: I click on “A” and when the click is made there should be an image which should be shown and once the click is done the on-screen keyboard must revert back. Now, attacker will see image in the screenshot rather than mouse pointer on the specific character.

Disclaimer

I request you all to give the credits for the author while you are sharing this idea. Initially, author thought about patenting this idea but, later decided on giving it as open-source to the community to use this idea in their product(s). This idea is being released under GPL while credits are given to author. Author is not sure if any idea exists as such but, in his opinion he has not seen this implementation in the existing design of product(s) which could be tills and online banking applications.