**PIN SELECTION POLICIES**

**SLIDE 14: introduction**

*Until now we discussed about different ways to exploit PINs information leakage in common real-life environments and now we put our attention on how PINs should be chosen to increase the strongness of PIN itself and make harder the probability of guessing.*

When a user chooses a PIN there should be a compromised between usability (so, easy to remember) and security (so, the randomness of the PIN) and this is reachable with an efficient PIN selection policy. Usually, users prefer the usability over the security, this because the computational effort requested to remember an easy PIN is much lower than a complex alternative.

Here are some tips that efficient PIN selection policies should follow to increase the security of chosen PINs *[read them]*.

The goal of this part of the presentation is to show that PIN selection policies increase the security of the PINs decreasing the percentual of PIN guessed.

**SLIDE 15: how PINs are distributed in the real world**

Let’s discuss about how PINs are distributed in the real world. The set of global PINs follows a power law distribution where a small number of commonly used PINs have higher frequencies of usage than the majority. For instance, a study proved that the first digits of keypad (1,2,3) are more pressed than the others so, for an attacker should be easy to guess these digits.

Other commonly PINs used and derived from this fact are PIN generated:

* from dates and years
* from arithmetic operations
* PINs with close proximity

**SLIDE 16: how PINs can be more effectively chosen**

Looking at the real word distribution of PINs we noted that simpler PINs are the most commonly used. So, in order to avoid that we need to increase the security of the PINs, and this can be done enforcing PIN selection policies in every real-life usage (for instance, for lock/unlock smartphones).

To prove the strongness of PIN chosen under PIN selection policies a user study was conducted. In this study users were asked to choose smartphone PINs under 5 different PIN selection policies, if the user chose a PIN which was not allowed by the policy he were asked to select another PIN.

*[read the policies]*

Also, it was asked to rate how the chosen PIN was simple to remember with a scale from 1 to 5, 1 stands for “very easy” and 5 stands for “very difficult”.

**SLIDE 17: how PINs can be chosen and selected pt1**

*[read the slide]*

**SLIDE 18: how PINs can be chosen and selected pt2**

*[read the slide]*