**PIN SELECTION POLICIES**

**SLIDE 14: introduction**

*Until now we discussed about different ways to exploit PINs information leakage in common real-life environments (like ATMs scenario) and now we focus on how PINs should be chosen to increase their strongness and so decreasing the probability of guessing.*

When a PIN is chosen there should be a compromised between usability (how easy to remember) and security (so, how randomness there is). 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 and this fact leads to an important problem in term of PIN security.

How can we reach the missed compromised between usability and security? We can do that with good PIN selection policies that can be applied to every real-life scenario where a user needs to select a PIN. Here are some tips, derived from different studies, that efficient PIN selection policies should follow to increase the security of chosen PINs *[read them]*.

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

Now let’s discuss about the main problem of PINs talking 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 ones. This means that from all PINs space selection which is available just a tiny portion is the most used from users.

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 PINs chosen under PIN selection policies a user study was conducted via an online survey where users were asked to choose lock/unlock smartphone PINs under 5 different PIN selection policies, if the user chooses 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**

1. Nothing really surprising but we need to remember that we haven’t to force users to remember something really complex;
2. And this is a factor that reduces the searching space;
3. Compared to the 332 people involved in this study.

🡺 **about 10 minutes of discussion**