**Introduction Chapter**

**PIN Selection Policies and User Behavior**

* Numerous studies have been conducted to examine the impact of password and PIN selection policies on users. These studies have looked at theoretical estimates, small-scale laboratory studies, and large-scale surveys.
* Some studies have shown that users often do not change their passwords regularly, despite knowing the importance of doing so.
* Password and PIN selection policies can affect the usability and security of passwords. Stringent policies can lead to users writing down their passwords, compromising their confidentiality.
* User training has limited impact on improving users' security awareness.
* Automated password-cracking tools are generally less effective against mnemonic passwords compared to control passwords.
* Transitioning from a less-constrained password policy to a stricter one can be challenging for users, leading to longer password creation times and difficulty in remembering passwords.
* A 16-character password policy has been recommended as a balance between strong passwords and user burden.

**Effectiveness of PIN Selection Policies**

* PIN selection policies for mobile phones have been studied through an online survey.
* The survey collected data on the number of participants who had to change their PINs to conform to stricter policies, the impact of the policy changes on remembrance difficulty, and participants' feelings about their changed PINs.
* For 4-short PINs, about 39.5% of participants had to change their PINs as they were among the blacklisted, 200 most popular PINs. The remembrance difficulty increased by about 0.36 on average.
* For 4-long PINs, about 52.7% of participants had to change their PINs that satisfied 4-short. The remembrance difficulty increased by about 0.74 on average.
* The stricter policies led to changes in the distribution and randomness of selected PINs.

**Real-World PIN Distribution**

* The distribution of real-world PINs, generated without any PIN selection policy, differs from the ideal uniform distribution.
* A large sample of PINs collected from an iPhone application showed variations in PIN selection patterns.
* The occurrence frequency of popular PIN subsequences of length 2 and 3 was analyzed.

**User Study on PIN Selection Behaviors**

* A user study was conducted to observe changes in PIN selection behaviors before and after introducing stricter selection policies.
* The study focused on authentication for mobile phones, and participants were asked to choose PINs for locking their phones.
* The study used a within-subject design to examine changes in pretest and posttest performances.
* Participants were encouraged to try the same PIN on stricter policies, and the questions were ordered based on policy strictness.
* The study ensured consistency in participants' perception of PIN complexity/strength by narrowing the application scope to mobile phone authentication.
* The survey was anonymous, and no identification information was collected.

**Related Work Chapter**

The related work chapter discusses various user authentication technologies, including passwords and PINs. It highlights the dominance of passwords and PINs as the preferred authentication method due to their low implementation and deployment costs. The chapter also mentions the need for PIN selection policies to help users choose stronger PINs and improve security. Additionally, it references studies that analyze the effectiveness of different selection policies and the impact of user behavior on password and PIN security.

Key points

* User authentication technologies include passwords, PINs, digital certificates, physical tokens, one-time passwords, transaction profile scripts, and biometric identification.
* Passwords and PINs are still the dominant authentication technology due to their low costs.
* PIN selection policies can help users choose stronger PINs and improve security.
* Studies have shown that mnemonic phrase-based passwords are more resistant to brute-force attacks.
* The effectiveness of selection policies can be influenced by user behavior and the tendency to choose substitute passwords that are easy to remember.
* PINs with close proximity, such as '0000' or '1111', are popular but vulnerable to attacks.
* Demographics of participants in the user study include a majority of males in the age group of 18-49 with at least some college education.
* The user study involved participants choosing PINs under different PIN selection policies, including 4-free, 4-short, 4-long, and 6-free policies.

**What real world PINs look like Chapter**

**Occurrence frequency of PINs** The occurrence frequency of PINs follows a power law distribution, meaning that a small number of commonly used PINs are heavily favored. This is evident from the histogram of PIN occurrence frequency, which shows a dramatic decrease after the 10th PIN. The distribution patterns of PINs are similar to those of passwords collected from another study.

**PIN selection practices** Many users choose PINs that are easy to remember but may not be secure. Common PINs like '1234' or '0000', as well as users' birthdays or telephone numbers, are often used. A study found that 15% of recorded PINs were part of the top 10 most commonly used PINs. This trend reduces the actual space of PINs used and increases the likelihood of an attacker guessing a PIN through brute-force attacks.

**PIN selection policies** To help users choose stronger PINs, devices and applications may enforce PIN selection policies. These policies capture security requirements and can restrict the use of certain PINs. For example, a policy may prohibit the use of duplicating numbers in a PIN. By implementing such policies, the aim is to increase the security of PINs and reduce the likelihood of successful attacks.

**Methodology Chapter**

Overview

The methodology chapter of the document discusses the PIN selection policy design and the user study conducted to evaluate the effectiveness of different policies. It also covers the measurement of PIN distribution and entropy calculation. The chapter provides insights into the impact of PIN selection policies on PIN distribution and user experience.

Key points

* The user study consisted of five different parts, where participants were instructed to choose a PIN under different PIN selection policies.
* PIN selection policies included 4-free, 4-short, 4-long, 6-free, and 6-long, each with specific restrictions on PIN selection.
* Participants were asked to rate the difficulty of remembering their selected PINs.
* The entropy of the collected PINs was calculated using Shannon's method and Massey's method.
* The results showed that stricter PIN selection policies led to changes in selected PINs and increased difficulty in remembering them.
* The study aimed to improve the randomness and security of PIN selection for mobile phones.

**Results and Recommendations Chapter**

The document provides an analysis of PIN selection policies based on a user study. It includes information on the occurrence frequency of different PINs, the difficulty of remembering PINs, and the demographics of the participants. The study also explores the impact of consecutive numbers and proximity on PIN selection. Based on the findings, recommendations can be made for designing effective PIN selection policies.

Key points

* The occurrence frequency of PINs was analyzed, showing the popularity of certain PINs and subsequences.
* The difficulty of remembering PINs was assessed, with participants rating the memorability of selected PINs.
* The study found that PINs with consecutive numbers and close proximity were commonly chosen by users.
* Recommendations can be made for PIN selection policies, such as disallowing popular PINs and considering the impact of consecutive numbers and proximity.

**Conclusions Chapter**

The conclusions and future work chapter of the document discusses the analysis of PIN selection policies and their effectiveness in improving PIN security and usability. The study focused on PINs used for locking mobile phones. The chapter also explores the characteristics of PINs used on mobile phones and evaluates the distribution of a sample PIN dataset. The effectiveness of different PIN selection policies is evaluated, and suggestions are made on how the policies should be designed.

Key points

* The study analyzed the characteristics of PINs used on mobile phones and evaluated the distribution of a sample PIN dataset.
* PIN selection policies were designed and evaluated for their effectiveness in improving PIN security and usability.
* The study focused on PINs used for locking mobile phones and aimed to provide consistent guidelines for choosing PINs.
* The conclusions highlight the need for carefully designed PIN selection policies and suggest improvements for future research in this area.