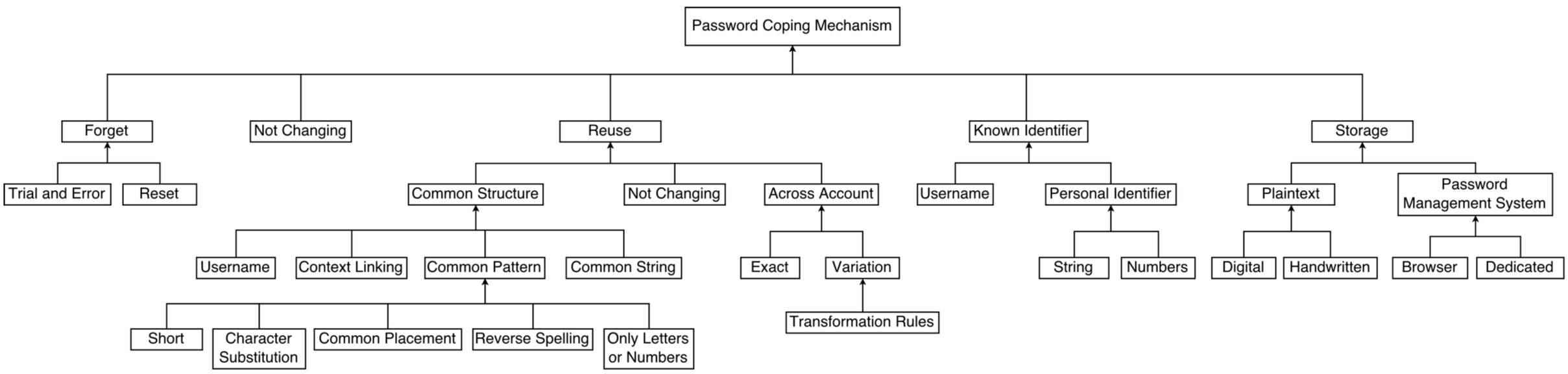
Password Coping Mechanisms

Austin Klasa

Passwords are the most common means of authenticating users, and the number of passwords a user must remember is increasing. This leads to the need to classify and study password coping mechanisms: any method used to cope with the large number of passwords a user must remember for multiple accounts. A user will choose the password coping mechanism that works best for them. Some users will create their own hybrid password coping mechanism: a combination of multiple different categories. After a literature review and analysis of eight research papers gathered from an online database, a pattern of password coping mechanisms emerged. These findings present a map of past research and were utilized to create the password coping mechanism taxonomy below.



User Story:
John Doe is overwhelmed by the number of passwords he must remember. He was recently required to change his Facebook password. His old password was DoeFacebook!2014 and his new password is JohnFacebook!2015. John Doe's hybrid password coping mechanism falls under the following categories:

- Known Identifier - Personal Identifier - String
- Reuse - Common Structure - Context Linking
- Reuse - Common Structure - Common String
- Reuse - Common Structure - Common Pattern - Common Placement
- Reuse - Across Account - Variation

Research Questions:

- How many users use password coping mechanisms?
  - Which password coping mechanism categories and subcategories are most frequently used?
  - Metric: Frequency count
- Which password coping mechanism subcategories are frequently combined to create hybrid password coping mechanisms?
  - Metric: Frequency count
- Which password coping mechanism subcategories present the most risk if exploited to gain unauthorized access to a user's account?
  - Metric: Password entropy
- Can social engineering be utilized to change a user's password coping mechanism so they can be exploited?

Special thanks to Dr. Melissa Dark

"INSuRE (http://insurehub.org) is training students in information security research with problems provided by the National Security Agency, Sandia National Labs, Pacific Northwest National Labs, and the Indiana Office of Technology. Any opinions, findings, and conclusions or recommendations expressed in this material are those of the author(s) and do not necessarily reflect the views of the aforementioned."