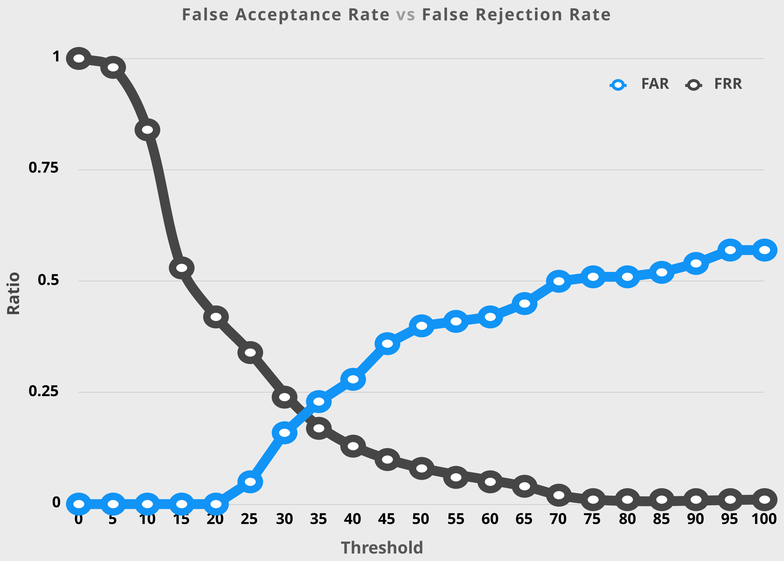
TAPPED-BASED AUTHENTICATION FOR MOBILE DEVICE SECURITY

Lukasz Brodowski, Cameron Dziurgot and Donald Moretz.

Faculty Advisor: **Stan Kurkovsky, Ph.D.**
Professor and Chair of Computer Science

INTRODUCTION

- Passkeys have been around since personal phones existed.
- A tap sequence used as a passkey offers infinite unique combinations.
- Our results show that it is possible to authenticate using a unique tap sequence, and convenient enough to be used every day to unlock a personal device.



PROBLEM

- Current devices have only a four-digit passkey which isn't very secure.
- A tap sequence is a much more complex passkey.
- Every tap sequence can be unique for each user, unlike a traditional four-digit passkey.
- Tap sequence is practically impossible to brute force because their are infinite possibilities.

BACKGROUND

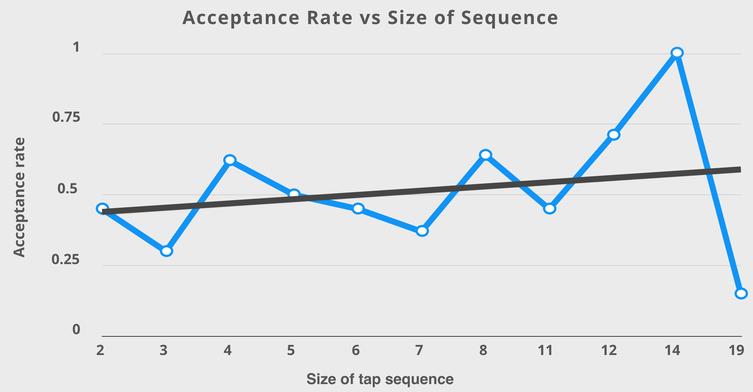
- TapSongs [2] first introduced the idea of a tap sequence being used for authentication in 2009.
- A tap sequence is a set of timestamps recorded by an application.
- Minimum requirements for tap authentication include the relative timestamps of the up/down presses [1].
- The sequence can be made more complex by adding coordinates, pressure or area.
- To compare the tap sequence vectors the Hamming distance can be used.
- Hamming distances measures the minimum number of substations required to change one vector to another [3].
- We used a variation of the Euclidean distance which is the sum of squares of data sets for each vector.
- Our algorithm also took into account standard deviation which allows for margin of error when entering a passkey.
- Based on a calculated dissimilarity score, we can decide whether the correct sequence was entered.

APPROACH

- A prototype on Android was implemented.
- The application let us test the capability of mobile devices and their ability to run the algorithm quickly.
- This prototype allowed us to verify the practicality and usability of this approach of authentication.
- Since only two tap sequences need to be compared (key and attempt), this is a very fast feedback loop.
- The approach is unique because every single passkey is distinct due to micro variations.

RESULTS

- Tap sequences are extremely hard to replicate.
- Can be made easier by only comparing intervals of presses.
- This allows us to match the sequences reliably while keeping a reasonable acceptance rate.
- The algorithm returns a dissimilarity score which indicates how close the master and trial sequences are.
- It was found that more complex patterns were more secure while still being relatively easy for the user to replicate.
- The next step was to start recording statistics to better improve acceptance rate by tweaking the algorithm or the acceptance score.
- After many tweaks, a tap sequence proves to be a reliable way of verification for the average user.



REFERENCES

[1] Marques, D., Guerreiro, T., Duarte, L., Carriço, L. (2013). Under the table: tap authentication for smartphones. In Proc. of BCS HCI '13, Swinton, UK

[2] Wobbrock, J.O. (2009). TapSongs: tapping rhythm-based passwords on a single binary sensor. In: Proc. UIST '09. ACM Press. 93-96.

[3] Norouzi, M., Fleet, D. J., & Salakhutdinov, R. (2012). Hamming Distance Metric Learning. Advances in Neural Information Processing Systems 25, 1-9.