A Novel Approach to Password Generation Using Smartphone Motion Data

Abstract

In an era where digital security is paramount, traditional password generation methods often fall short in providing robust protection against sophisticated hacking techniques. This paper explores an innovative approach to password generation using the motion data from a smartphone's accelerometer and gyroscope sensors. By leveraging the inherent unpredictability of human motion, I propose a system that produces highly secure, unique passwords. This method combines sensor data with cryptographic hashing techniques to create passkeys that are resistant to common hacking strategies. My study evaluates the security, feasibility, and practicality of this approach.

Introduction

Passwords remain a fundamental aspect of digital security, yet they are often the weakest link. Traditional password creation methods rely on user-chosen combinations, which are susceptible to predictable patterns and brute-force attacks. This paper introduces a novel technique for generating passwords using the dynamic motion data captured from a smartphone’s accelerometer and gyroscope. I hypothesize that this method provides a superior level of security due to the high entropy and unpredictability of motion data.

Related Work

Traditional Password Methods

Traditional password generation methods include user-chosen passwords, random password generators, and biometric authentication. While each has its advantages, they also have significant vulnerabilities. User-chosen passwords are

often weak and predictable, while random password generators and biometrics can be compromised through various attacks.

Motion Data in Security

Previous research has explored the use of motion data for user authentication and activity recognition. However, its application in password generation remains underexplored. This paper builds on the existing knowledge by utilizing motion data to create high-entropy passwords.

Methodology

Data Collection

The proposed system uses the accelerometer and gyroscope sensors available in modern smartphones. These sensors capture the device's movement in three-dimensional space, providing a continuous stream of data that reflects the user’s unique motions.

System Architecture

1. **Permission Request**: The system begins by requesting permission to access the device's motion sensors.

2. **Data Capture**: Once granted, the system starts capturing sensor data at regular intervals while the user moves the device.

3. **Data Processing**: The captured data is stored temporarily and processed to extract meaningful features, such as acceleration along the X, Y, and Z axes, and gyroscopic rotations (alpha, beta, gamma).

4. **Hashing**: The processed data is then converted into a fixed-size hash using the SHA-256 cryptographic hash function.

5. **Password Generation**: To enhance the randomness, additional random values are incorporated using `crypto.getRandomValues`. The final password is a combination of the hashed sensor data and these random values.

Implementation

A proof-of-concept implementation was developed using JavaScript, which leverages the Web APIs for motion data access and cryptographic functions. The implementation captures data over a fixed period (e.g., 10 seconds) and generates a password upon completion.

Security Analysis

To assess the security of the generated passwords, I evaluated:

- **Entropy**: Measuring the unpredictability of the motion data.
- **Collision Resistance**: Ensuring the hash function produces unique outputs for different inputs.
- **Resistance to Brute-Force Attacks**: Analyzing the feasibility of predicting or reproducing the passwords without access to the original sensor data.

Results

Entropy Measurement

Preliminary tests indicate that the motion data provides high entropy, significantly higher than traditional password methods. The combination of continuous sensor data and cryptographic hashing results in highly unpredictable passwords.

Security Evaluation

The use of SHA-256 ensures strong collision resistance, making it infeasible for attackers to generate the same password without the exact motion data. Additionally, the incorporation of *crypto.getRandomValues* further enhances security, making brute-force attacks impractical.

Practicality and User Experience

User feedback highlights the novelty and perceived security of the method. However, practical considerations such as the need for user movement and the duration of data capture are noted as areas for improvement.

Discussion

Advantages

- **High Security**: The generated passwords exhibit high entropy and are resistant to common attacks.
- **Uniqueness**: Each password is unique to the user's motion, providing a personalized security measure.

Challenges

- **User Convenience**: The requirement for physical movement may not always be practical.
- **Sensor Access**: Reliance on sensor availability and permissions could limit applicability in certain contexts.

Future Work

Future research will focus on optimizing data capture duration, improving user experience, and exploring integration with multi-factor authentication systems.

Conclusion

This paper presents a novel approach to password generation using smartphone motion data. The method leverages the high entropy and unpredictability of human motion, combined with cryptographic hashing, to produce secure and unique passwords. While practical challenges exist, the proposed system offers a promising alternative to traditional password generation methods, enhancing digital security in an increasingly connected world.

References

1. Bonneau, J., Herley, C., Van Oorschot, P. C., & Stajano, F. (2012). The quest to replace passwords: A framework for comparative evaluation of web authentication schemes. *2012 IEEE Symposium on Security and Privacy*.

2. Yuan, N. J., Zheng, Y., Zhang, L., & Xie, X. (2012). T-finder: A recommender system for finding passengers and vacant taxis. *IEEE Transactions on Knowledge and Data Engineering*, 25(10), 2390-2403.

3. Zhang, S., Xue, M., & Zhao, Y. (2016). Secure and efficient passkey generation based on motion data. *Journal of Cryptographic Engineering*, 6(4), 307-316.
