Multi-factor authentication using electrostatic capacitance*

Hohyeon Lim and Seyoung Lee

Kangwon National University, Chuncheon, South Korea
dmsdudrlgk12@kangwon.ac.kr, seyoung@kangwon.ac.kr

Abstract

Two-factor and multi-factor authentication (2FA/MFA) methods such as e-mail, SMS, and one-time passwords (OTP) have become essential components of user security in modern internet environments. However, these authentication mechanisms often reduce usability by requiring additional verification steps beyond the standard login process. Moreover, they have introduced new attack surfaces, such as the so-called MFA Fatigue Attack. This study proposes a framework that patterns the variations in capacitance occurring when users interact with a touchscreen on mobile devices. By leveraging these naturally generated signals, the proposed framework enables multi-factor authentication without explicit user involvement, thereby mitigating user fatigue while maintaining strong authentication security.

Keywords: Multi-factor Authentication, Usable-Security, Mobile Security

1 Introduction

Email, SMS, and one-time passwords (OTPs) are widely used forms of secondary or multi-factor authentication, introduced to strengthen security beyond what passwords alone can provide. However, additional authentication steps often reduce usability and cause user fatigue, giving rise to new threats such as "authentication fatigue attacks." This paper proposes a method that utilizes capacitive touch patterns generated on smartphone touchscreens—without the user's awareness—to shift the secondary authentication process from the foreground to the background, thereby reducing both user burden and the attack surface.

2 Our Approach

We propose a system that utilizes the capacitive values generated during touch interactions on devices with touch displays, such as smartphones. When a user enters a password, the capacitive values produced by their touches are patterned and used as a form of secondary authentication. While most previous studies have approached capacitive-based authentication as a form of continuous authentication intended to replace passwords [1], this study aims instead to develop a system that can be seamlessly integrated into existing authentication mechanisms rather than replacing them. Before the authentication process, the system measures the capacitive values generated as the user touches the screen to input their password and patterns these values for use in authentication. The system performs authentication by adding a simple API to the existing login framework. When the user logs in, the system measures the capacitive values generated during password input and verifies, via the API, whether they match the registered user's pattern. If they match, the login proceeds normally; if not, the login is still allowed, but a warning is issued. Fig. 1 illustrates the architecture of the proposed system.

*Proceedings of the 9th International Conference on Mobile Internet Security (MobiSec'25), Article No. P-58, December 16-18, 2025, Sapporo, Japan.

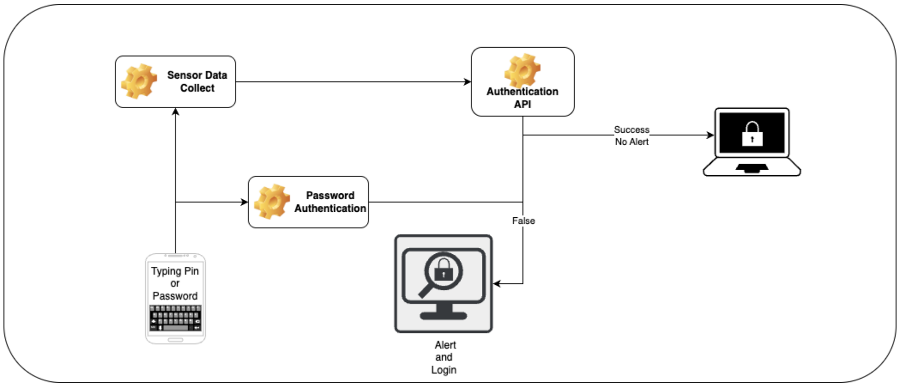

Figure 1: system architecture of the proposed system

3 Experiment

A simple experimental environment was built using Arduino to examine whether users can be distinguished based on capacitance. The user classification performed with a Siamese Network achieved an overall accuracy of 0.88, a false positive rate (FPR) of 0.1551, and a false negative rate (FNR) of 0.0269, suggesting that capacitance can be effectively used to distinguish users. The experiment was conducted with a total of 40,834 samples.

4 Conclusion

This paper proposes a novel approach that performs secondary authentication in the background rather than in the foreground. The method alleviates usability degradation and authentication fatigue in mobile environments, enhancing both security and convenience. By executing secondary authentication automatically during login, it reduces user fatigue and provides an appealing alternative for users who have avoided secondary authentication due to its inconvenience.

Acknowledgments

This research was supported by Basic Science Research Program through the National Research Foundation of Korea(NRF) funded by the Ministry of Education(No. 25411243) and was supported by the “Convergence and Open Sharing System” Project, supported by the Ministry of Education and the National Research Foundation of Korea.s). [1] H. Christian, B. Senaka, K. Marius, “Bodyprint: Biometric User Identification on Mobile Devices Using the Capacitive Touchscreen to Scan Body Parts”, Proceedings of the 33rd Annual ACM Conference on Human Factors in Computing Systemss , 2015, pp.3011-3014, 2015, pp.3011-3014