TOKEN: Trustable Keystroke-Based Authentication for Web-Based Applications on Smartphones

Mohammad Nauman\textsuperscript{1} and Tamleek Ali\textsuperscript{2}

\textsuperscript{1} Department of Computer Science, University of Peshawar, Pakistan
\textsuperscript{2} Institute of Management Sciences, Peshawar, Pakistan
recluze@gmail.com, tamleek@imsciences.edu.pk

Abstract. Smartphones are increasingly being used to store personal information as well as to access sensitive data from the Internet and the cloud. Establishment of the identity of a user requesting information from smartphones is a prerequisite for secure systems in such scenarios. In the past, keystroke-based user identification has been successfully deployed on production-level mobile devices to mitigate the risks associated with naïve username/password based authentication. However, these approaches have two major limitations: they are not applicable to services where authentication occurs outside the domain of the mobile device – such as web-based services; and they often overly tax the limited computational capabilities of mobile devices. In this paper, we propose a protocol for keystroke dynamics analysis which allows web-based applications to make use of remote attestation and delegated keystroke analysis. The end result is an efficient keystroke-based user identification mechanism that strengthens traditional password protected services while mitigating the risks of user profiling by collaborating malicious web services.

Keywords: Remote attestation, privacy, security, keystroke-based identification.

1 Introduction

The increasing popularity of both smartphones and web-based applications has given rise to the deployment of non-native web-based applications targeting these mobile devices. As in any application residing in the cloud, security is an important concern for this new breed of applications and within the scope of security, user authentication is a critical factor. Traditional approaches to authentication involving ‘strong passwords’ have several limitations in the context of mobile phones. Miniature keyboards (and in latest devices – on-screen touch keyboards) tend to motivate users to choose simpler, and thus weaker, passwords. A solution to this problem, proposed and implemented on desktop computers since more than two decades back, is keystroke-dynamics analysis\textsuperscript{[1,2]} that uses more sophisticated parameters, such as duration between each keystroke pressed, alongside password matching to strengthen authentication.
A recent extension to this approach has been to measure keystroke dynamics [3,4] of users on mobile platforms alongside password-based authentication to determine their authenticity. While this approach has been shown to be highly effective [5], existing techniques fail to be applicable on web-based services. The reason that existing keystroke-dynamics analysis approaches cannot be deployed as-is for web-based services is fairly straight-forward. Keystrokes are captured on the client end, while the authentication decision needs to take place on the remote web-application server platform. There is no way for the web application to trust the measurements of keystroke dynamics taken on the client platform. Moreover, if the keystroke dynamics patterns of a user are released to any requesting web site, collaborating malicious applications may profile a user’s usage pattern and lead to privacy concerns for the user. The recent hack [6] of the popular micro-blogging site Twitter, in which the hacker was able to access Twitter’s confidential documents using only their compromised passwords, is evidence of the need for enabling better authenticating mechanisms for web applications.

In this work, we propose an authentication framework based on two hot security research topics – keystroke-dynamics and remote attestation – that allows the extension of the former to web-based applications using the constructs of the latter.

Contributions: Our contributions in this paper are the following:

1. We extend keystroke-dynamics based user authentication to web-based applications targeting mobile devices,
2. We devise an infrastructure for establishing trust on keystroke patterns reported by the client platform and
3. We enable privacy protection against profiling attacks that may arise as a result of releasing keystroke patterns outside the user’s device.

Outline: The rest of the paper is organized as follows. Section 2 provides background knowledge about both keystroke-based authentication and Trusted Computing. The problem description is detailed in Section 3 along with the challenges in solving these problems. Our proposed architecture is presented in Section 4. The paper is concluded in Section 5.

2 Background Work

2.1 Keystroke-Dynamics Analysis

The concept of keystroke-dynamics based user authentication is not a new one. Card et al [1] first proposed this method of authenticating users based on the time span between each successive keystroke. This time duration is termed as digraph. Further studies added more parameters to this basic metric including overlapping combinations of keys due to different time spans between key press and key release events. Rick et al. [7] reported strong empirical evidence in support of keystroke latency-based verifier for desktop systems to successfully