Using Conference Styles with LaTeX

Dr. Milaan Parmar

Abstract

This is some abstract text. This has been included for demonstration only. This is why it's being kept brief.

1 Introduction

Introduction text here. 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 naive 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. We present a prototype implementation of our protocol using the popular Android operating system for smartphones.

2 Background

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 naive 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[1] 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 [2]collaborating malicious web services. We present a prototype implementation of our protocol using the popular Android operating system for smartphones.[3]

2.1 Some Related Work

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 naive 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.

3 Conclusions

In the past, keystroke-based user identification has been successfully deployed on production-level mobile devices to mitigate the risks associated with naive 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.

References

[1] M. Nauman, T. Ali, and A. Rauf. Using trusted computing for privacy preserving keystroke-based authentication in smartphones. *Telecommunication Systems*, pages 1–13, 2011.

[2] M. Nauman and M. Uzair. Se and cs collaboration: Training students for engineering large, complex systems. In *Proceedings of the 20th Conference on Software Engineering Education & Training*, pages 167–174, Washington, DC, USA, 2007. IEEE Computer Society.

[3] H. Seo and H. Kim. User input pattern-based authentication method to prevent mobile e-financial incidents. In *Parallel and Distributed Processing with Applications Workshops (ISPAW), 2011 Ninth IEEE International Symposium on*, pages 382–387. IEEE, 2011.