Unified Authentication with Smart Cards via Near Field Communication

Lucas Pinheiro Cinelli, Otto Carlos M. B. Duarte
Universidade Federal do Rio de Janeiro - GTA/COPPE - Rio de Janeiro, Brazil

Abstract—**We discuss an authentication scheme with Smart Cards using the OpenID standard. This mechanism is a more secure alternative to the usual password only method. The project implements OpenID unified authentication to maintain minimum the number of cards necessary for a user. We also argue that NFC is essential to a fast and simple identification process.**

I. Introduction

The most common authentication technique is based on the usual identificator scheme, namely username/password. However, this method has already well known weaknesses to many attacks such as phishing and keylogging and, also, it is very prone to user error. Another source of problems is the need for many authentication identificators, for the various Service Providers, causing users to choose easy, memorable and repeated passwords.

A way to avoid part of these problems is removing the possible troubles caused by the need for the innumerous different passwords, so we implemented an authentication protocol using the OpenID standard which enables a unified validation through Identities Providers. We have also tackled other major security issues by implementing the verification process with Smart Card instead of usual username password pair. Besides, we also propose a contactless communication through Near Field Communication (NFC) between the card and the reader as an alternative to the present physical contact implementation for user identification.

II. The Smart Card Alternative

Newer smart cards, which present secure cryptoprocessors, are inherently secure, at least when compared to other technologies already in usage or to the ones in development. Furthermore, it accounts for possible theft and misuse in it‘s conception since it is possible to replace the cards, as opposed to the also current biometry which is unstrustworthy for the impossibility of altering ones fingerprints once it has been digitally stolen.

Java Card is a subset of the Java language intented for the memory constraints of smart cards. The abstraction proportioned by the Java Virtual Machine (JVM) together with multi-application support and the broad range of development environments offers a real possibility for the smart card market to expand. Nevertheless, such features requires additional security mesures to avoid applications interchanging confidential informantion. Therefore, it is crucial to guarantee applet isolation and the three main mechanisms [1] are prohibition of dynamic class loading during execution, applet firewalls, and applet multithreading incompatibility. However, it is fundamental for security that Java Card Runtime Environment (JCRE) is correctly implemented otherwise the firewalls will not function properly and it will be possible to illegal references to objects.

III. Multiple Authentication with OpenID

The OpenID standard is a set of specifications which defines a protocol of authentication between the Service Providers (SP), Identity Provider (IdP) and users. The process occurs by exchange of HTTP messages to validate the user together with the Idp and then to redirect him to the SP of interest.

The great advantage of OpenID is its unified identification method that transfers the authentication responsibility from the SPs to an IdP. Consequently, all SPs will be obligated to verify the autencity of a user by requesting it to an Idp making unnecessary the vast number of passwords a user must memorize because an Idp can support many distinct SPs.

IV. Secure Contactless with NFC

Near Field Communication is a subset of RFID standards, which establishes a short range wireless communication that relies on Radio Frequency (RF) modulation, operating at 13.56MHz with a working distance up to 10 cm supporting a maximum data rate of 424 kbps.

A smart card characterizes a passive device, since it retrieves the power from the RF field generated by the card reader, and therefore can only be active when submitted to such electromagnetic field.

The implementation of contactless authentication does not necessarily jeopardize the security of the process [2], although it requires greater attention to possible attacks such as eavesdropping and man-in-the-middle. Nonetheless, the proximity necessity of NFC design offers more security to the data transfer and cryptography can evade those issues when correctly implemented.

V. Conclusion

In this scenario, contactless smart cards shall represent a significant amount of authentication devices in the future for its user convenience and security supremacy over the typical password only method. Although it is of uttermost importance that applications developed in Java Card be cautiously implemented in order to avoid the already known attacks to the weaknesses of this technology. Nevertheless, a protocol similar to OpenID is mandatory to a real pratical project since users cannot carry as many cards as services they may use.

Acknowledgments

This work was supported by FINEP, FUNTTEL, CNPq, CAPES, and FAPERJ.

References

[1] A. K. Ghosh, “Security risks of java cards,” in *CardTech/SecurTech*, vol. 98, 1999, pp. 465–470.

[2] A. Kundarap, A. Chhajlani, R. Singla, M. Sawant, M. Dere, and P. Mahalle, “Security for contactless smart cards using cryptography,” in *Recent Trends in Network Security and Applications*. Springer, 2010, pp. 558–566.