Design and Implementation of a Zero-Knowledge Authentication Framework for Java Card

Ahmed Patel, Universiti Kebangsaan Malaysia, Malaysia and Kingston University, UK

Kenan Kalajdzic, Center for Computing Education, Bosnia and Herzegovina

Laleh Golafshan, Department of Computer Engineering and IT, Science and Research Branch, Islamic Azad University, Fars, Iran

Mona Taghavi, Department of Computer, Science and Research Branch, Islamic Azad University, Tehran, Iran

ABSTRACT

Zero-knowledge authentication protocols are an alternative to authentication protocols based on public key cryptography. Low processing and memory consumption make them especially suitable for implementation in smart card microprocessors, which are severely limited in processing power and memory space. This paper describes a design and implementation of a software library providing smart card application developers with a reliable authentication mechanism based on well-known zero-knowledge authentication schemes. Java Card is used as the target smart card platform implementation based on the evaluation of the Fiat-Shamir (F-S) and Guillou-Quisquater (G-Q) protocols under various performance criteria are presented to show the effectiveness of the implementation and that G-Q is a more efficient protocol.

Keywords: *Authentication, Cryptography, Fiat-Shamir Protocol, Guillou-Quisquater Protocol, Java Card, Security, Smart Cards, Zero-Knowledge Protocols*

1. INTRODUCTION

User authentication is essential in many networked and Internet applications. It is a process by which a user proves his/ her identity to the system, thus proving his/ her rights to use particular information and services. The essence of authentication is the demonstration of either the knowledge of a secret, the possession of a physical object, or the authenticity of a certain human body characteristic.

The most popular mechanism of user authentication is the use of passwords. It is cheap to deploy and easy to use. While suitable for many applications, password authentication is lacking many features necessary for security critical applications. Badly chosen passwords are easy to guess, can be intercepted in transmission and re-used later for impersonating legitimate users. Passwords cannot be used directly to sign digital documents.

DOI: 10.4018/jisp.2011070101

Cryptography offers better methods of authentication, but their use is connected with manipulating secret cryptographic keys, which are difficult to remember. For sensible use, cryptographic keys need to be stored in some well-protected computing devices. For people on the go, such a device has to be small enough to fit into a pocket. Smart cards are probably the most widespread device of this sort.

A Smart card is a credit card sized plastic card with an embedded single-chip microcomputer. The use of special manufacturing technology makes physical tampering or probing of the microcomputer circuitry difficult, although not completely impossible. Smart card microcomputers are characterized by low clock frequencies (around 1 MHz) and small memory capacity (1-16 KB of ROM and less than 1 KB of RAM). Thus, smart cards are portable and small computers with different types of memory. Java Card technology is used in order to enable smart cards for running small applications in secure mode for a variety of environments, such as telephone networks and banking industry (ORACLE, 2010; Chen, 2000) and mobile agent e-marketplaces (Wei & Patel, 2009; Patel, 2010). Typically, it is touched wherever authentication and security are essential to access valuable data.

The limitations of smartcards severely impact the choice of cryptographic techniques available for use in smartcard applications. Currently, only techniques based on symmetric cryptography are in wide use. Although asymmetric (public key) cryptography offers a richer range of functionality, it requires more memory space and processing power than is available in the majority of currently available smartcards.

In the domain of authentication protocols, an alternative to both symmetric and asymmetric cryptography is the use of zero-knowledge proof techniques. Zero-knowledge authentication protocols offer same level of convenience as authentication protocols based on asymmetric cryptography, but require less memory space and processing power. Zero-knowledge protocols consist of two essential parts, the *prover* and *verifier* (Kapron *et al*., 2007). For a more detailed account regarding the background and content of zero-knowledge protocol see published paper by Vadhan (2004).

To validate practical applicability of zero-knowledge techniques in smartcard environment, the authors developed a prototype software library that implements a well-known zero-knowledge authentication protocol. Java Card specification was used as the target smartcard platform. The results of this work are discussed in the rest of this paper.

Section 2 gives a brief overview of smartcard technology and related standards. Section 3 gives an introduction into zero-knowledge proofs and zero-knowledge authentication protocols. Thereafter, the design and implementation of a prototype library based on the evaluated zero-knowledge protocols are discussed in Section 4 and the conclusions given in Section 5.

2. SMARTCARDS

A smartcard looks like a normal credit card with a chip embedded in it. Smartcards can be divided into three main categories according to the capabilities of the chip:

- *Memory cards*, which can just store data and have no data processing capabilities.
- *Wired Logic Intelligent Memory cards,* which contain also some built-in logic, usually used to control the access to the memory of the card.
- *Processor cards,* which contain memory and processor and have data processing capabilities.

Smartcards have to communicate with some other devices to gain access to a network. Therefore, they can be plugged into a reader, commonly referred to as a card terminal, or they can operate using Radio Frequencies (RF). In the former type of card, the connection is made when the reader contacts a small golden chip on front of the card whilst the latter (*contactless card*) can communicate via an antenna,