IGI PUBLISHING **ITB14878**

701 E. Chocolate Avenue, Suite 200, Hershey PA 17033-1240, USA
Tel: 717/533-8845; Fax 717/533-8661; URL-http://www.igi-pub.com

This paper appears in the publication, **Web Services Security and E-Business**
edited by **G. Radhaman & G. S. V. Radha Krishna Rao**

Chapter VIII

Node Authentication in Networks Using Zero-Knowledge Proofs

Richard S. Norville, Wichita State University, USA

Kamesh Namuduri, Wichita State University, USA

Ravi Pendse, Wichita State University, USA

Abstract

Zero-knowledge proof (ZKP) based authentication protocols provide a smart way to prove an identity of a node without giving away any information about the secret of that identity. There are many advantages as well as disadvantages to using this protocol over other authentication schemes, and challenges to overcome in order to make it practical for general use. This chapter examines the viability of ZKPs for use in authentication protocols in networks. It is concluded that nodes in a network can achieve a desired level of security by trading off key size, interactivity, and other parameters of the authentication protocol. This chapter also provides data analysis that can be useful in determining expected authentication times based on device capabilities. Pseudocode is provided for implementing a graph-based ZKP on small or limited processing devices.

Introduction

The concept of zero-knowledge proof was introduced by Goldwasser, Micali, and Rackoff (1991). Node authentication methods based on ZKPs were investigated in the past. However, their suitability for small computing devices, as well their implementation mechanisms, received less attention (Aronsson, 1995). With the advent of small wireless computing devices such as PDAs and smart sensors, the importance of authentication schemes that can provide high levels of confidence with less computational power has tremendously increased. This chapter contributes to this field of research by investigating the suitability of ZKP-based authentication schemes for small computing devices and provides their complexity analysis. It also provides implementation details needed for a practitioner.

Several authentication protocols are available in the literature. Examples include timed efficient stream loss-tolerant authentication (TESLA) (Perrig, Canetti, Song, & Tygar, 2001), authentication schemes based on polynomial rings (Hoffstein, Lieman, & Silverman, 1999), and elliptic curve cryptography (ECC) (Aydos, Sunar, & Koc, 1998) among several others. The reader is referred to text books on cryptography (Menezes, Oorschot, & Vanstone, 1997; Stinson, 2002) for a survey of authentication protocols based on hash functions and symmetric encryption algorithms.

ZKP-based authentication protocols provide a smart way to prove an identity of a node without giving away any information on the secret of that identity. There are many advantages as well as disadvantages in using this protocol over other authentication schemes such as challenges to overcome in order to make it practical for general use.

One advantage of ZKPs is that their computational requirements can be minimized based on the nature of the underlying problem. This makes them appealing for devices that are limited by processor speed.

The most noteworthy benefit in using a ZKP is that during the entire authentication process, no hints about the secret are ever given. This is important when one considers how effective hackers have been at infiltrating and stealing personal information from databases. Since keys are usually publicly available there is no need to store secrets.

Networks can also benefit from the ZKP protocol for two reasons. The transactions that take place during the authentication process are relatively light. Trust is gained through repeated interaction, not necessarily by the key size alone. The main benefit to network users is that no secure channel or encryption is needed to authenticate. Hackers listening in during the exchange of information gain no knowledge that they could not have already gathered on their own.

Challenges to overcome include the high memory requirements needed for ZKPs. Since the protocol uses public keys, they must be large enough to be difficult to solve in a timely manner. Also the amount of traffic generated by ZKPs is larger than other authentication schemes due to its interactive nature.