Project Presentation

Authentication Using Zero Knowledge Proof

BY

MITU22BTCS0293	**GAURANG SHARMA**
MITU22BTCS1037	**YOGESH THAKUR**
MITU22BTCS0381	**KAUSHAL CHORDIYA**
MITU22BTCS056	**PRADNYA KHORE**

Guided By

Prof. Smita Gumaste

Department of Computer Science & Engineering, MITSoC, Loni Kalbhor

Index

1. Introduction

Traditional authentication systems rely on users' passwords to verify identity. While widely used, this approach has significant security risks, including vulnerability to password theft, phishing attacks, and database breaches.

Zero Knowledge Proof (ZKP) authentication offers a more secure alternative by enabling users to prove their identity without revealing their password or any other sensitive information. In a ZKP system, the user demonstrates knowledge of a secret to the verifier without disclosing the secret itself. This method drastically reduces the risk of sensitive data exposure and enhances overall security.

Problem Statement

Traditional authentication methods, such as passwords and biometrics, expose sensitive information, making them vulnerable to attacks.
Zero-Knowledge Proof (ZKP) offers a secure alternative by allowing a user to prove knowledge of a secret without revealing the secret itself.
This project aims to develop an authentication system using ZKP, ensuring that no sensitive data is transmitted during the authentication process.

Domain – Cyber Security
Technology – Python

Literature Survey

Volume 5, Issue 1, January 2015 ISSN: 2277 128X

International Journal of Advanced Research in Computer Science and Software Engineering

Research Paper

Available online at: www.ijarcsse.com

A Survey of Zero-Knowledge Proof for Authentication

Jitendra Kurmi
Scholar
Department of Computer Science & Engg.
Lovely Professional University
Phagwara, Punjab, India

Ankur Sodhi
Assistant Professor
Department of Computer Science & Engg.
Lovely Professional University
Phagwara, Punjab, India

Abstract - Zero-knowledge proofs are cryptographic protocols which do not disclose the information or secret itself during the protocol. Zero-knowledge proofs plays an important role in the design of cryptographic protocols. The application of Zero-knowledge protocols can be in authentication, identification, key exchange and other basic cryptographic operations. Zero-knowledge proof has been implemented without expose any secret information during the conversation and with smaller computational requirement than using comparable public key protocols. The most cryptographic problems can be solved with the help of zero-knowledge protocols, as well as with cryptography. Zero-knowledge protocols can be a best solution in many occasions. The Zero-knowledge proof protocols are very lightweight, due to which it requires less amount of memory. Thus Zero-knowledge protocols widely used especially in authentication. This paper presents an overview of zero-knowledge protocol used for authentication, identification and key exchange.

Keywords - Proof of knowledge, Zero knowledge, Digital identification, Password Authentication, P2P Identity Authentication, key exchange, RFID, public key encryption, pseudo random number generator.

The paper discusses various implementations of ZKPs that enhance security in cryptographic protocols, including methods to prevent common attacks like replay and man-in-the-middle attacks and passive attacks.

ZKPs are implemented to ensure security without revealing secrets, often requiring less computational power than public key protocols and promotes user privacy and also helps to prevent many cyber attacks.

Literature Survey

Extending Web Applications with a Lightweight Zero Knowledge Proof Authentication

Sławomir Grzonkowski
DERI Galway, NUIG
IDA Business Park
Galway, Ireland
slawomir.grzonkowski@deri.org

Wojciech Zaremba
DERI Galway, NUIG
IDA Business Park
Galway, Ireland
wojciech.zaremba@deri.org

Maciej Zaremba
DERI Galway, NUIG
IDA Business Park
Galway, Ireland
maciej.zaremba@deri.org

Bill McDaniel
DERI Galway, NUIG
IDA Business Park
Galway, Ireland
bill.mcdaniel@deri.org

ABSTRACT

User authentication is a crucial requirement for secure transactions and access to the sensitive resources on the Web. We propose, implement and evaluate a Zero-Knowledge Proof Authentication (ZKP) algorithm based on isomorphic graphs. The proposed mechanism allows for authentication with varying confidence and security levels.

We suggest that most of the computations should be carried out by the user's web browser without revealing password or login at any point in time; instead generated random isomorphic graphs and permutation functions based on the user login/password can be exchanged.

Our experimental evaluation shows that by combining the asynchronous web with ZKP protocols, it is feasible to satisfy existing usability standards on the web.

Each time a web-application provides authentication, both login and password details are sent. In most cases the credentials are transferred from a client to a server using HTTP[1]. Although for security reasons in most of the existing solutions, the credentials are not stored on the servers in plaintext form, they are given to the servers in a readable form during the authentication procedure. The other approach is to use HTTP Digest mode [2], but the drawback of this approach is that the server can impersonate the user to a third party. This is a serious privacy problem. Developers of non-commercial web applications often ignore this issue. For commercial software, including banking and on-line shopping, developers use asymmetric cryptography communication protocols, for instance, HTTPS[3]. This protocol sets up a secure connection but the credentials are still sent. Public key solves the problem partially because users are required to provide public and private key-pairs or digital certificates.

One of the primary challenges identified in the paper is the variability in performance across different web browsers and hardware configurations.

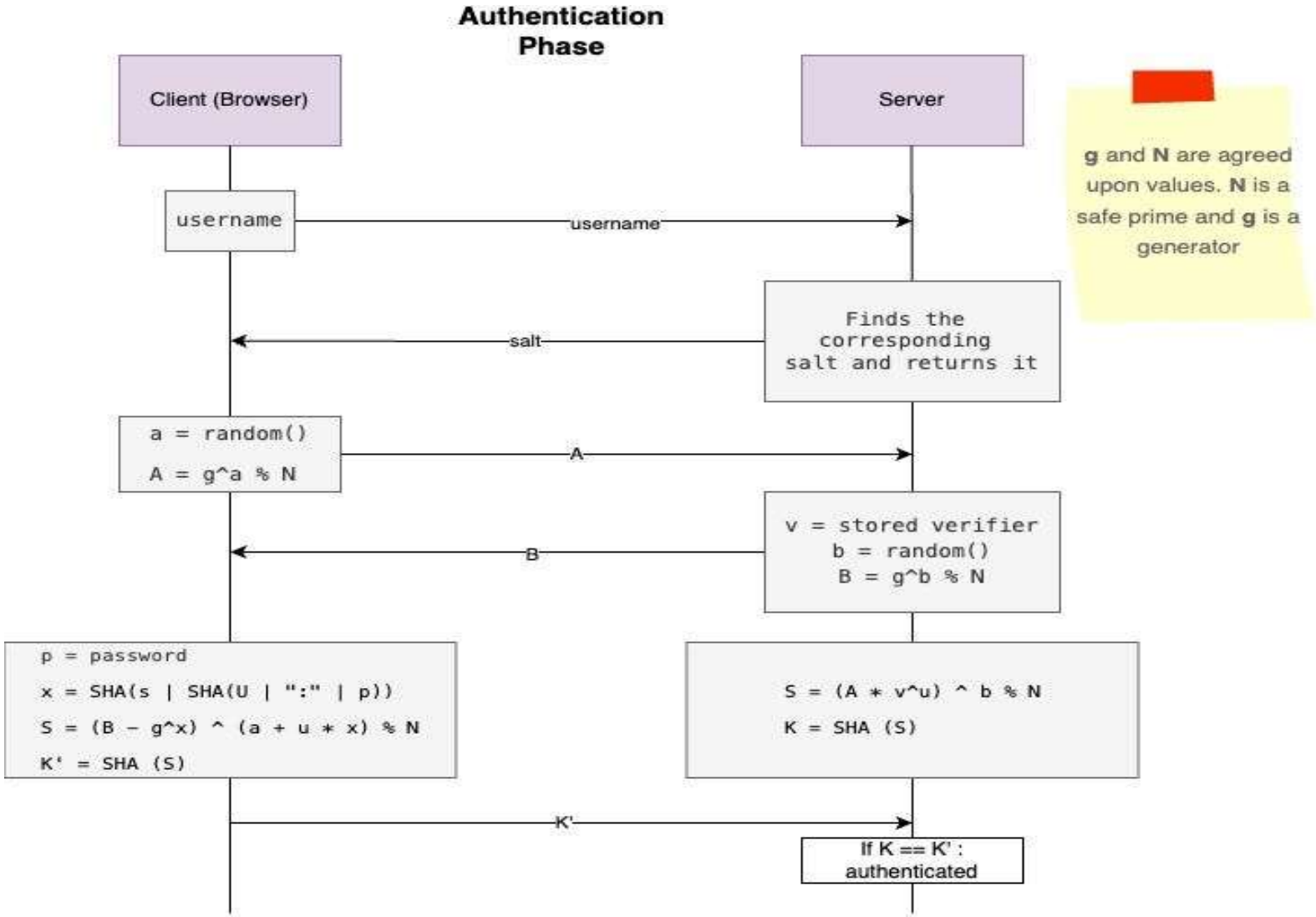
For example, the authentication process takes longer on some browsers (like Opera) and may even fail if the process exceeds certain time thresholds.

Due to compatibility issues not every device is able to implement this authentication process

Objectives

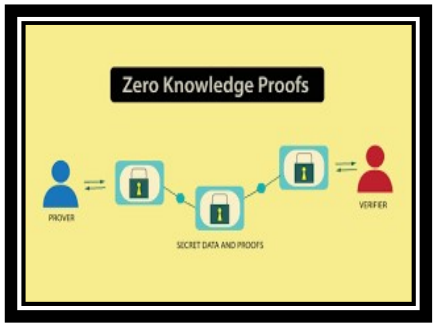
1. To provide the user a more secure way of authentication
2. To deal with the privacy concerns of the user
3. To make this method compatible with all kinds of devices

Concepts and Methods



Implementation

We are going to implement ZKP in an environment to improve security and enhance out understanding about different algorithms and encryption techniques.



Our Team

Pradnya Khore

Yogesh Thakur

Gaurang Sharma

Kaushal Chordiya