Saeed Ullah Jan

An Improved Lightweight Privacy Preserving Authentication Scheme for SIP-Based-VoIP Using Smart Card

Anchor Academic Publishing

disseminate knowledge

Jan, Saeed Ullah: An Improved Lightweight Privacy Preserving Authentication Scheme for SIP-Based-VoIP Using Smart Card, Hamburg, Anchor Academic Publishing 2017

PDF-eBook-ISBN: 978-3-96067-628-7
Druck/Herstellung: Anchor Academic Publishing, Hamburg, 2017

Bibliografische Information der Deutschen Nationalbibliothek:
Die Deutsche Nationalbibliothek verzeichnet diese Publikation in der Deutschen Nationalbibliografie; detaillierte bibliografische Daten sind im Internet über http://dnb.d-nb.de abrufbar.

Bibliographical Information of the German National Library:
The German National Library lists this publication in the German National Bibliography. Detailed bibliographic data can be found at: http://dnb.d-nb.de

Hermannstal 119k, 22119 Hamburg
http://www.diplomica-verlag.de, Hamburg 2017
Printed in Germany

WITH THE NAME OF ALMIGHTY “ALLAH” THE MOST MERCIFUL AND THE GRACIOUS

ALL GLORY BE TO ALLAH,

THE CREATOR OF THE UNIVERSE,

THE MOST MERCIFUL AND MIGHTY,

THE LORD OF THE DAY OF JUDGMENT,

THE ONLY WE WORSHIP,

THE ONLY WE ASK FOR HELP,

GUIDE US (O LORD) TO THE PATH THAT IS STRAIGHT,

THE PATH OF THOSE YOU HAVE BLESSED, NOT OF THOSE WHO HAVE EARNED YOUR ANGER, NOR THOSE WHO HAVE GONE ASTRAY

“AMEEN”

Dedication

This thesis is dedicated:

To

The Holiest Man Ever Born,

***Prophet Muhammad* (صلی اللہ علیہ وسلم)**

&

To

MY Parents and Family

I am most appreciative of my parents, family and love of my life, whose affection has always been the source of encouragement for me, and whose prayers have always been a key to my success.

&

To

My Beloved colleagues

Who were always there for me and made my life at UOM easier and fun.

&

To

My Honorable Teachers

Whose are beacon of knowledge and a constant source of inspiration for my whole life span.

Acknowledgements

First of all I would like to thank ALMIGHTY ALLAH for his countless blessing to complete my studies. At the leading edge, I would like to thank my supervisor Dr. Fawad Qayum who shared a lot of his experience and ideas with me. I appreciate his professionalism, planning, and constant involvement in my research. I cherish the time we spent in discussions and in the laboratory hammering over problems. Working under him has sharpened my research skills and increased my enthusiasm to work in cryptography.

I am grateful to Dr. Sohail Abbas for his encouragement, advice, and help whenever needed. I am thankful to the Department of Computer Science Research Lab and the Software Engineering Department for offering me a fabulous environment to work and study. I would like to take this opportunity to acknowledge Dr Sohail Abbas and lab mates who made my stay at University of Malakand exciting and unforgettable. I acknowledge the help received from him on innumerable occasions. I would especially like to thank him for helping me out with various tool flows for the discussions that we had on technical as well as non- technical topics. I thank Dr Shakeel Arshad, Dr Siffat Ullah, Dr Sami Ur Rahman and Dr Sehat Ullah for working along with me on several courses and assignments.

I am grateful to Dr Ajab Khan and Dr Siffat Ullah Khan for giving me this opportunity to further my studies. I would like to acknowledge the help received from my colleague, Mr Aziz Ur Rahman, who took care of things while I was away. I would like to thank my brothers and my family for the love and encouragement I received. Without their support this thesis would not have been possible. I would like to thank my friend Mr Aziz Ur Rahman and Mr. Muhammad Salim for his prayers and for being my role model for hard work.

SAEED ULLAH JAN

Abstract

In the past few years, secure information sharing became very popular in the area of immigration, military applications, healthcare, education, foreign affairs, etc. As secure communication utilizes both wireless and wired communication mechanizations for exchanging sensitive information, so security and privacy of the information exchange cannot be easily compromised. To moderate the security, integrity, authenticity, and privacy issues related to information exchange, numerous authentication mechanisms have been recommended by different researcher in the literature in recent times, but are vulnerable to prospective security flaws such as masquerade, insider, replay, impersonation, password guessing, server spoofing, denial-of-service attacks and in addition failed to deliver mutual authentication.

In the past few years we have also seen a balanced growth in the acceptance of VoIP (Voice over IP) facilities, because the numerous Web and VoIP applications depend on huge and extremely distributed infrastructures to process requests from millions of users in an appropriate manner. Due to their extraordinary desires, these large-scale Internet applications have frequently surrendered security for other objectives such as performance, scalability and availability. As a result, these applications have characteristically favored weaker, but well-organized security mechanisms in their foundations. Session Initiation Protocol (SIP) is an application and presentation layers signaling protocol that initiates, modifies, and terminates IP-based multimedia sessions. Implementing SIP for secure communication has been a topic of study for the past decade, and several proposals are available in the research domain. However, security aspects are not addressed in most of these proposals, because SIP is exposed to several threats and faces security issue at these layers. Probes for SIP (Session Initiation Protocol) servers have been conveyed for many years, and to gather more details about these activities we simply design a scheme for SIP servers in a network and composed data about some popular attacks. What will follow is an explanation of our interpretations and guidance on how to prevent these attacks from being successful.

Biometrics a new field of research has also been materialized in this research, entitled “a three-factor authentication scheme" in which one factor is biometrics. In biometric cryptosystems the benefits of biometric confirmation are presented to basic cryptographic key supervisory systems to enhance security. Anyhow, this research delivers a general outline of the basics, permitting to biometrics as well as cryptography. This work also gives biometric cryptosystems based on iris biometrics and using smart card as well as a password for authentication.

Table of Contents

List of Figures

List of Tables