505/31/12/21

11

Abstract

Name: AKBER ALI KHAN
Supervisor: Prof. Musheer Ahmad
Department: Applied Sciences and Humanities, Faculty of Engineering and Technology
Title: A Study of Authentication Protocols using Elliptic Curve Cryptography

Keywords: Authentication, Key agreement, Elliptic curve cryptography, Internet of Things (IoT), Smart grid, Vehicle to grid, Security and privacy, Random oracle model, AVISPA, Biometric and fuzzy extractor, One way collision resistant hash function.

The objective of the thesis is to design secure communication protocols for cyber physical system. The performance of the proposed works is compared with existing works ensuring security through safe and reliable data transmission and mechanisms providing anonymous, secure communication.

The thesis is divided into seven Chapters and every Chapter details are as follows:

Chapter one gives a brief overview of authentication and discusses the security objectives behind our research work on authentication protocols. Further, we discuss the security attacks in authentication protocols. Chapter two discusses some mathematical preliminaries used in our work. Cryptographic prerequisites, symmetric-key vs public-key cryptography, one-way hash function, identity-based cryptosystem, One-way hash function has been discussed briefly. Elliptic Curve Cryptography (ECC) and a comparison of ECC and RSA are presented. ECC-based assumptions for the authentication protocol. Further, we discuss the biometric and fuzzy extractor with its properties, formal security model for authentication protocols. Finally, we discuss the formal security verification using broadly accepted Automated Validation of Internet Security Protocols and Applications (AVISPA) software tool. Chapter three deals with an elliptic curve cryptography based mutual authentication scheme for smart grid communications using biometric approach. In this chapter have used ECC and biometric based initialization phase, registration phase, login and authentication phase. The registration and login and authentication phase are between user and server. We discuss the security analysis of the proposed chapter. Further, we discuss performance analysis of the components such as comparison of functionality features, comparison of computation cost and comparison of communication cost. This chapter provides secure and efficient approach for smart grid. The content of this Chapter is published in Journal of King Saud University Computer and Information Sciences, Elsevier, (SCIE, ESCI and Scopus Indexed, IF: 13.473). Chapter four deals with a Password-based anonymous lightweight key agreement framework for smart grid in short we called PALK. There are ECC based three phases in this Chapter those are as initialization phase registration phase, login and key agreement phase and password change. The registration phase performs between user and trust authority, login and key agreement perform between two participants of this communication system. We discuss formal security analysis by random oracle model under the two different methods, simulation study using AVISPA tool and informal security analysis of this chapter. Further, we discuss performance analysis of the components such as comparison of functionality features, comparison of computation cost and comparison of communication cost. This Chapter provides secure and efficient authentication techniques in smart grid system. The content of this Chapter is

published in Journal of Electrical Power and Energy Systems, Elsevier (SCIE, Web of Science and Scopus Indexed, IF: 4.63). Chapter five, we propose a lightweight authentication and key agreement framework for smart grid network in short, we called LAKAF. To indicated that proposed Chapter ensure secure communication, we have proved the claim of security using formal security analysis in the random oracle model and using information security analysis. Moreover, we have used simulation tool ``AVISPA" to show the proposed protocol security against a replay attack and man-in-the-middle. We have evaluated the performance of the proposed framework and compared it with related schemes on desirable performance parameters. The proposed Chapter have achieved all desirable security attributes and supports efficient communication. The content of this Chapter is published in Journal of Systems Architecture, Elsevier (SCI, Web of Science and Scopus Indexed, IF: 3.777). Chapter six, we have proposed a secure and efficient key agreement framework for critical energy infrastructure using mobile device. In this Chapter registration of vehicle perform between vehicle user with its mobile device and trust authority, registration of grid server with trust authority. Finally, authentication and key agreement phase establish between vehicle and grid server. To indicated that proposed Chapter ensure secure communication, we have proved the claim of security using formal security analysis in the random oracle model and using information security analysis. Moreover, we have used simulation tool ``AVISPA" to show the proposed protocol security against a replay attack and man-in-the-middle. We have evaluated the performance of the proposed framework and compared it with related schemes on desirable performance parameters. The proposed Chapter have achieved all desirable security attributes and support efficient communication. Chapter seven, we discuss some future research directions.