Accepted Manuscript

Design and hardware implementation of a security-enhanced elliptic curve cryptography based lightweight authentication scheme for smart grid communications

Dariush Abbasinezhad-Mood, Morteza Nikooghadam

PII: S0167-739X(17)31537-6
DOI: https://doi.org/10.1016/j.future.2018.02.034
Reference: FUTURE 4005

To appear in: *Future Generation Computer Systems*

Received date : 13 July 2017
Revised date : 5 January 2018
Accepted date : 20 February 2018

Please cite this article as: D. Abbasinezhad-Mood, M. Nikooghadam, Design and hardware implementation of a security-enhanced elliptic curve cryptography based lightweight authentication scheme for smart grid communications, *Future Generation Computer Systems* (2018), https://doi.org/10.1016/j.future.2018.02.034

Design and hardware implementation of a security-enhanced elliptic curve cryptography based lightweight authentication scheme for smart grid communications

Dariush Abbasinezhad-Mood, Morteza Nikooghadam*

Department of Computer Engineering and Information Technology, Imam Reza International University, Mashhad, Iran.
(Email: dariush.abbasinezhad@imamreza.ac.ir, * *corresponding author*: m.nikooghadam@imamreza.ac.ir)

Abstract

Security and privacy are among the main concerns in the smart grid adoption. The different parties of smart grid can communicate securely by means of symmetric key algorithms. However, in order to utilize the symmetric key encryption methods, the parties need to establish a common key beforehand. To do so, several key management schemes have been presented during the last decade to be employed in the context of smart grid. Quite recently, Mahmood et al. have proposed an interesting elliptic curve cryptography-based authentication and key agreement scheme for smart grid communications. They have said that their presented scheme can withstand several known attacks and can provide the perfect forward secrecy. After careful deliberation, we found that their scheme cannot provide the perfect forward secrecy. Furthermore, their scheme is vulnerable under the commonly accepted Canetti-Krawczyk adversarial model. That is to say, the private key of users and shared session keys can be easily compromised in case of ephemeral secrets leakage. As a result, to remedy the existing challenges, in this paper, an authentication scheme is proposed that can both provide the desired security features and offer better efficiency in communication and computational costs than several recently-published schemes. Finally yet importantly, the security of our proposed scheme has been validated using the widely-accepted ProVerif tool and the cryptographic elements have been implemented on a suitable hardware for smart meters. The results are indicative of the betterment of the proposed scheme for real-world applications. We hope that the obtained results be useful for other researches in this field.

Keywords: Authentication, elliptic curve cryptography, ephemeral secret leakage, ProVerif, smart grid security.

1. Introduction

The current power grid can no longer manage the ever-rising needs and expectations of the 21th century [1]. For that reason, smart grid (SG), the innovative digitally-enabled power grid, has been developed that is envisioned to replace the aging infrastructure of the current electrical grid [2]. Because of the miscellaneous stupendous features that SG will offer, such as bidirectional digital communications, distributed supervision and control, self-recovery capabilities, remote check, and more consumer options [3], it has attracted appreciable attention from both academia and industry [4]. In SG, several new technologies are integrated with some existing ones to provide a more efficient, reliable, sustainable, and economical electricity delivery [5].

Contrary to the existing power grid that only the one-way transmission of electricity is practicable, the emergence of SG paves the way to bidirectional digital communications between the electric utility and consumers [6]. These two-way communications are the main achievement of SG [1] that not only make the monitoring, management, and control of SG easier [7], but also in near at hand, the consumers can send their excessive electrical energy back to the grid [8]. Nonetheless, SG is exposed to numerous security threats by the integration of new technologies and the bidirectional communications [9].

In SG, real-time information of customers, like their usage reports, are sent to the energy supplier at regular time intervals of fifteen minutes [10]. Moreover, some command messages are sent vice versa in order to be executed by the measurement devices. To provide a secure channel for these communications, several key management schemes have been proposed during the last decade. Different stakeholders of SG can first share a common key by the employment of a key establishment method; afterwards, using the generated shared key and a symmetric encryption algorithm, fast and secure communications of these entities become possible.