Chapter 29
Denial of Service Attack on Protocols for Smart Grid Communications

Swapnoneel Roy
University of North Florida, USA

ABSTRACT

In this work, a denial of service (DoS) attack known as the clogging attack has been performed on three different modern protocols for smart grid (SG) communications. The first protocol provides authentication between smart meters (SM) and a security and authentication server (SAS). The second protocol facilitates secure and private communications between electric vehicles (EV) and the smart grid. The third protocol is a secure and efficient key distribution protocol for the smart grid. The protocols differ in either their applications (authentication, key distribution), or their ways of communications (usage of encryption, hashes, timestamps etc.). But they are similar in their purpose of design (for the smart grid) and their usage of computationally intensive mathematical operations (modular exponentiation, ECC) to implement security. Solutions to protect these protocols against this attack are then illustrated along with identifying the causes behind the occurrence of this vulnerability in SG communication protocols in general.

INTRODUCTION

The collective nature of a smart grid (SG) with many subsystems and networks, working together as a system of systems makes its components vulnerable to various kinds of attacks most of which can be performed remotely. Therefore, security has become a first class parameter in the development of SG, and many authentication and key management protocols have been designed and are continually being designed. Security protocols for the smart grid can be broadly classified into two major classes according to their functions:

DOI: 10.4018/978-1-7998-5348-0.ch029

1. Authentication, and
2. Key Management.

User authentication can enable a perimeter device (e.g., a firewall, proxy server, VPN server, or remote access server) to decide whether or not to approve a specific access request to gain entry to a computer network. It is necessary to be able to identify and authenticate any user with a high level of certainty, so that the user may be held accountable should his/her actions threaten the security and productivity of the network. The more confidence a network administrator has regarding the user's identity, the more confidence the administrator will have in allowing that user specific privileges, and the more faith the administrator will have in the internal records regarding that user.

Multi-factor authentication is an approach to cyber-security in which the user is required to provide more than one form of verification in order to prove his/her identity and gain access to the system. It takes advantage of a combination of several authentication factors. Commonly used factors include verification by:

1. Something a user knows (such as a password),
2. Something the user has (such as a smart card or a security token), and
3. Something the user is (such as the use of biometrics) (Stallings & Brown, 2008).

Due to their increased complexity, multi-factor authentication systems are harder to breach than those using any single factor.

Multiple factor authentication is needed to provide high-level security. But with the introduction of more factors, there are possibilities to introduce more vulnerability in the protocols that an attacker can exploit to launch an attack on them. Vulnerabilities are detected by static analysis before they are exploited. The root causes of CPU, stack, and other resource-exhaustion vulnerabilities (DoS) are often design flaws rather than programming errors. Several multi-factor authentication protocols in the literature involving smart cards, RFIDs, wireless networks, or digital signatures, rely on the usage of complex mathematical operations (e.g. ECC) for their security. Hence some level of protection should be added to them to guarantee total security against various kinds of attacks.

Key management is the management of cryptographic keys in a cryptosystem. This includes dealing with the generation, exchange, storage, use, and replacement of keys. It includes cryptographic protocol design, key servers, user procedures, and other relevant protocols. Key management concerns keys at the user level, either between users or systems. This is in contrast to key scheduling; key scheduling typically refers to the internal handling of key material within the operation of a cipher. Successful key management is critical to the security of a cryptosystem. In practice it is arguably the most difficult aspect of cryptography because it involves system policy, user training, organizational and departmental interactions, and coordination between all of these elements.

The nodes are all non-interactive in distributed key management protocols that are conventional. Every node is assumed to be able to independently learn about the keys shared with other nodes, without the assistance or intervention of any trusted third parties. The memory cost of each node in a non-interactive network has been proved to be N-1, where N is the total number of nodes in the network. This number does not depend on the kind of algorithms used to determine the pairwise keys. The pairwise key model, the Blom model and the Blundo model are optimum as non-interactive schemes in terms of their memory cost. However, as N grows, the memory requirement of non-interactive schemes grows exponentially.