The C-DAX Security Architecture for Smart Grids

Michael Hoefling∗, Florian Heimgaertner†, Barbara Vieira†, Erik Poll† and Michael Menth∗
∗University of Tuebingen, Tuebingen, Germany, Email: hoefling@uni-tuebingen.de
†Radboud University Nijmegen, Digital Security Group, Nijmegen, Netherlands

I. INTRODUCTION

Today, smart grid (SG) refers to the next-generation electrical power grid designed to enhance the resilience of the grid to power flow disruptions, improve energy efficiency, and reduce carbon emissions. To accomplish these goals, the modern electrical power grid will incorporate a wide variety of SG applications, e.g., synchrophasor-based real-time state estimation [1], electric vehicle charging, and future retail energy transactions [2]. However, one of the main obstacles in the way of the deployment of SG applications is the limited capabilities of today’s utility communication infrastructure in terms of scalability, reliability, and security.

The Cyber-secure Data and Control Cloud for power grids (C-DAX) project [3] develops an abstract representation of a unidirectional information channel; data transmitted within a topic is called topic data. C-DAX is composed of C-DAX clients and the C-DAX cloud. Publishers are C-DAX clients generating data for a specific topic; subscribers are C-DAX clients interested in certain topic data. C-DAX nodes form the C-DAX cloud, and provide a specific set of functions, e.g., forwarding topic data.

II. C-DAX SECURITY ARCHITECTURE

The security architecture of C-DAX provides topic access control, end-to-end integrity and end-to-end confidentiality of published data, and authentication of clients and nodes. In contrast to more innovative solutions for security in information-centric SG middleware presented in [4], the current C-DAX middleware uses authentication and encryption mechanisms based on standard cryptographic primitives. We presented a paper on this work at the IEEE IoT/CPS-Security Workshop [5].

A. Security Rationale

C-DAX nodes do not have to trust each other inside the C-DAX cloud, and clients do not have to trust the C-DAX cloud for guaranteed end-to-end security. Topic data transmission should be protected end-to-end because (1) only legitimate publishers may publish data for a certain topic, (2) only legitimate subscribers may receive data from a certain topic, and (3) third parties (e.g., forwarding nodes, and malicious clients) must not modify or spoof topic data. The actually required security properties for the topic data transmission may vary depending on the SG applications, and the C-DAX middleware must be capable of supporting them.

B. Security Properties

Source authentication is required for control plane messages and realized using digital signatures and access control lists (ACLs). Topic access control is required for all topics to prevent unauthorized clients from publishing data. Symmetric keys are shared among authorized publishers and involved forwarding nodes for the same topic, and used to compute hash message authentication codes (MACs). End-to-end integrity enables subscribers to verify the integrity of received topic data without having to trust intermediate forwarding nodes; it is realized similar to topic access control through MACs and shared keys among publishers and subscribers. End-to-end confidentiality guarantees that only the intended receivers of a message can read the message content, i.e., forwarding nodes cannot decrypt or alter topic data.

C. Key Updates

Key updates can be scheduled periodically by configuring a key lifetime and replacing it after expiration. Key updates can also be triggered by join or leave events and ACL changes. The advantage of periodical key updates is that there is no means to attack the C-DAX cloud by intentionally causing key updates. To make sure that messages for a topic originate from legitimate publishers and can only be read by legitimate subscribers, backward secrecy and forward secrecy are required for the topic keys [6].

ACKNOWLEDGMENT

The research leading to these results has received funding from the European Community’s Seventh Framework Programme FP7-ICT-2011-8 under grant agreement n° 318708 (C-DAX). The authors alone are responsible for the content of this paper.

REFERENCES