TALLINNA TEHNIKAÜLIKOOL
ELEKTROENERGEETIKA INSTITUUT

Centralized User Account Management Process in Substation Automation

Faculty of Power Engineering

Department of Electrical Power Engineering

Master of Science

Head of Chair	Juhan Valtin
Supervisors	Paul Taklaja
	Omar Velasco
Student	Kaspar Müül

Tallinn 2015

Declaration of authorship

I hereby declare that this thesis is the result of my own independent work and it has been presented to the department of Electrical Power Engineering of Tallinn University of Technology in order to claim a master's diploma in Electrical Power Engineering. This thesis has not been presented before to claim a degree in engineering sciences or engineering.

Student (date and signature) _____

Lõputöö kokkuvõte

Autor: Kaspar Müül *Lõputöö liik:* Magistritöö

Töö pealkiri: TSENTRALISEERITUD KASUTAJAKONTODE HALDAMISE PROTSESS ALAJAAMADE AUTOMAATIKA SÜSTEEMIDES

Kuupäev: 07.01.2015 *65 lk*

Ülikool: Tallinna Tehnikaülikool

Teaduskond: Energeetikateaduskond

Instituut: Elektroenergeetika instituut

Õppetool: Kõrgepingetehnika õppetool

Töö juhendajad: Paul Taklaja, Omar Velasco (ABB)

Töö konsultandid: Arve Sollie (ABB), Krister Hagman (ABB)

Sisu kirjeldus: Magistritöö kirjutamise tingis energiasektori vajadus töökindla ja turvalise tsentraaliseeritud kasutajakontode haldamise süsteemi järele, millega oleks võimalik hallata kasutajakontosid ning autentimist alajaamade automaatikasüsteemides kasutatavates intelligentsetes elektroonilistes seadmetes (IED-s). Käesoleva töö eesmärgiks on hinnata rakendatava tsentraliseeritud kasutajakontode haldamise süsteemi ja lahendada turvalisust puudutavad probleemid.

Töö sisaldab kokkuvõtet tsentraliseeritud autentimise vajaduse kujunemisest ja põhilistest süsteemi puudutavatest probleemidest. Magistritöö selguse huvides on üks peatükk pühendatud krüpteerimise ja avaliku võtme infrastruktuuri (PKI) tutvustamisele. Järgnevalt on tutvustatud rakendatavat tsentraliseeritud kasutajakontode haldamise süsteemi, mis põhineb LDAP protokollil, ning kirjeldatud ohte, mis töökindlust ja turvalisust võivad mõjutada. Tsentraliseeritud kasutajakontode haldamise süsteemi turvalisuse tõstmiseks on soovitatud andmevahetus krüpteerida. Erinevate osapoolte tuvastamiseks on soovitatud digitaalseid sertifikaate, mis on väljastatud tunnustatud kolmanda osapoole, sertifitseerimiskeskuse poolt. Lõpuks on lahendatud IED ja ühendatava kliendi platvormi vaheline tuvastusprobleem sertifikaatide määramisega ja andmevahetuse krüpteerimisega. Et IED-l oleks võimalik uus serveri sertifikaat väljastada kui interneti protokolli (IP) aadressi muudetakse, siis lahenduseks on toodud sertifitseerimiskeskuse (CA) salvestamine IED sisemisele mälule kuid salajane sertifitseerimiskeskuse signeerimisvõti turvalisuse tõstmiseks on salvestatud TPM turvakiibile. Krüpteerimisvõtmete turvaliseks salvestamiseks on soovitatud kasutada TPM turvakiipi.

Kokkuvõtteks, pakutav süsteem võimaldab võrgu omanikul hallata oma süsteemi kuuluvate IED-e kasutajaid lihtsamalt, kasutades tsentraalset süsteemi kasutajakonto lisamiseks, muutmiseks või kustutamiseks, vähendades süsteemi haldamisele kuluvat aega ja ressurssi. Lahendatud on turvalisust puudutavad probleemid, kaitstes andmevahetust ja autentides erinevaid osapooli ning lahendatud salajaste krüpteerimis võtmete turvalise salvestamise probleem TPM kiibi lisamisega IED emaplaadile.

Märksõnad: alajaamade turvalisus, automaatika, intelligentne elektrooniline seade (IED), krüptograafia, rollipõhine ligipääsu kontroll (RBAC), sertifitseerimiskeskus (CA), TPM turvakiip.

Summary of the diploma work

Author: Kaspar Müül *Type of work:* Master thesis

Title: CENTRALIZED USER ACCOUNT MANAGEMENT PROCESS IN SUBSTATION AUTOMATION

Date: 07.01.2015 *65 pages*

University: Tallinn University of Technology

Faculty: The faculty of Power Engineering

Department: The department of Electrical Power Engineering

Chair: The chair of High Voltage Engineering

Tutors: Paul Taklaja, Omar Velasco (ABB)

Consultants: Arve Sollie (ABB), Krister Hagman (ABB)

Abstract: The thesis in hand was motivated primarily because of the electrical industry's need for a reliable and secure centralized user account verification system that handles the user authentication process in Intelligent Electronic Devices (IEDs) in substation automation systems. The purpose of this study is to evaluate the proposed system, define the security status and propose solutions for security problems.

The work explains the need for a centralized authentication system, defines the problems with the existing solution and the proposed one. It includes a short introduction to cryptography. The thesis identifies the dangers of adding an authentication server, which is based on Lightweight Directory Access Protocol (LDAP), into a substation environment and analyzes the most common attacks a particular system may encounter. As a result of the study, in order to provide security in the network between two connecting entities, third party trusted certificates and encryption are recommended. During the analysis, two new obstacles were identified, and solutions were presented. First, when changes are done to the IED that affect the information in the Server Certificate (SC), a Certificate Authority (CA) should be installed onto the IED in order to create a new SC. Second, due to the unsecure nature of the internal storage options on the IED, a Trusted Platform Module (TPM) is recommended in order to safely secure the CAs signing private key, the symmetric key, and the asymmetric private key. Evaluation indicates that using digital certificates for identification and encryption to provide safety while the data is in transit or stored, can significantly improve the safety of the centralized user authentication system in the substation automation environment.

The proposed system has the ability to make the handling of user accounts in multiple IEDs easier by giving the responsible entity the possibility to modify, delete and add user information centrally, using a centralized server and interface, rather than modifying user accounts in each separate device. The security problems have been solved by using encryption while the data is in transit or stored, TPM chips will be used to safely store encryption keys, and digital certificates will be used for identification.

Key words: Certificate Authority (CA), cryptography, Intelligent Electronic Device (IED), Role Based Access Control (RBAC), substation security, automation, Transport Platform Module (TPM).

Contents

Assignment

Topic of thesis:	**Centralized User Account Management Process in Substation Automation**
Student:	**Kaspar Müül, 111324**
Supervisors:	**Paul Taklaja, Omar Velasco (ABB)**
Chair:	**High Voltage Engineering**
Head of chair:	**Juhan Valtin**
Due date for thesis:	**07 January 2015**

_____	_____	_____
Student (signature)	Supervisor (signature)	Head of chair (signature)

Justification of Topic

It is necessary to research this topic due to the increasing market demand for a reliable and secure centralized user account management system which can handle the administration of user accounts in a substation automation environment by giving the utility the possibility to change, add, delete, or modify user accounts in their Intelligent Electronic Devices (IEDs) centrally rather than modifying each device separately. Due to the standard requirements and customer focus on this topic, substation automation product manufacturers have started to look into this subject. The thesis in hand tries to answer and to give a proposal on how to improve the security between the IED and the centralized authentication server. It also focuses on the security and the authentication between the IED and the connecting client. Current IEDs lack the secure storage that is needed to store encryption keys safely, and this thesis gives a recommendation on the best solution for this particular problem.

This thesis may be of interest to anybody whose work or interest is related to substation security and critical infrastructure protection.

Purpose of Work

The purpose is to study the implications of adding a proposed system to a substation environment and develop a proposal to improve security.

List of Problems

- What dangers can arise when introducing a centralized authentication server into a substation environment?
- How to transfer user information over the network securely and to identify each entity?
- How to store encryption keys safely on the IED?

Initial Data

The data used in this work is obtained from IEC and NERC standards, from the ‘’Information Security Management Handbook’’ and relevant whitepapers.

Preface

This thesis is the result of the collaboration between ABB AB Substation Automation Products business unit located in Västerås, Sweden and myself, Kaspar Müül, during the fall of 2014.

I would like to thank my supervisors Omar Velasco, Krister Hagman and Arve Sollie from ABB for their continuous support while tackling this assignment. I would also like to thank my supervisor from the Tallinn University of Technology, Paul Taklaja, who supported the process from the beginning and helped me to edit the thesis.

I would like to thank the colleagues and personnel at ABB SA Products for a pleasant and supportive atmosphere. I am especially grateful to Mr. Kjell I. Westberg, manager of TPPA at ABB for organizing accommodation and everything else necessary for my stay in Sweden.

This research was supported by ABB and by the Estonian scholarship program Kristjan Jaak, which is funded and managed by Archimedes Foundation in collaboration with the Estonian Ministry of Education and Research.

Kaspar Müül

Abbreviations

CA- Certificate Authority

CC- Client Certificate

CCA- Critical Cyber Assets

CRL- Certificate Revocation List

DoS- Denial of Service

HMI- Human Machine Interface

IC- Integrated Circuit

I-CA- Intermediate Certificate Authority

IED- Intelligent Electronic Device

IP- Internet Protocol

LDAP- Lightweight Directory Access Protocol

OCSP- Online Certificate Status Protocol

PKI- Public Key Infrastructure

RAM- Random Access Memory

RBAC- Role Based Access Control

RBACMNT- Role-Based Access Control Manager

R-CA- Root Certificate Authority

SC- Server Certificate

S-CA- Subordinate Certificate Authority

SECADM- Security Administrator

SECAUD- Security Auditor

SPOF- Single Point of Failure

TLS- Transport Layer Security

TPM- Trusted Platform Module

VPN- Virtual Private Network

WAN- Wide Area Network

Introduction

Recent shifts in technology have created security problems as the electrical industry moved from closed proprietary networks to more standardized communication and protocols. The industry has benefitted from the operational side, because now it is easier to control its automation systems, but this has created several vulnerabilities and requires substation automation to address cyber-security issues that haven't been addressed in this industry before. This means that substation automation devices are getting connected to external networks where anyone with the knowledge and expertise can access them. As the energy grid is considered a critical infrastructure for a nation's well-being, focus is needed for access control. In most utilities and enterprises, network security and access control have already been implemented by the local IT department, and users have login access to their files, e-mails, and corporate networks. As the modern enterprise infrastructure has used centralized authentication for years, it's finally time to bring that knowledge down to the Intelligent Electronic Device (IED) level and implement similar control in substation environments.

The thesis in hand was motivated primarily because of the electrical industry's need for a reliable and secure centralized user account verification system that handles the user authentication process in IEDs. The proposed system has the ability to make the handling of user accounts in multiple IEDs easier by giving the responsible entity the possibility to modify, delete, and add user information centrally, using a centralized server and interface, rather than modifying user accounts in each separate device.

The advantage of centralized authentication is that the user list is managed in a single central location, by a responsible entity who, therefore, has full control over who can access its IEDs. There are still technical challenges extending that solution to the substation automation systems. Currently, IEC62351 standards define the need for a centralized user authentication system giving an overview on how it could be implemented and which models can be used, but it does not focus on the security between the IED and the connecting entity. Therefore to fill the gap and implement a fully controlled system more research is necessary. In order to implement a centralized authentication system, its safety and security requirements have to be analyzed. The purpose of this study is to evaluate the proposed system, define the security status, and propose solutions for security problems. This thesis is focused on the security between the authentication server and the IED and also between the client platform and the IED. The main task is to solve the authentication problem between devices in the network and to protect data while it is in

transit and when it is stored on the IED. One key question that the author hopes to answer is to find a secure storage option for encryption keys as the current IEDs lack that function. The goal is to propose a solution where every step is monitored and a fully controlled centralized user authentication process is achieved.

This thesis uses information from IEC62351 and NERC CIP standards. An important source for information has been the "Information Security Management Handbook'' [1] and relevant whitepapers, for example ''Making the most out of substation IEDs in a secure, NERC compliant manner'' [2], ''Efficient Public-Key Certificate Revocation Schemes for Smart Grid'' [3] and ''Best Practices in LDAP Security'' [4]. According to the author's findings, no specific research has been done on implementing secure storage on the IED level, the author hopes to fill the gap on this issue and to raise awareness on this possibility.

The first chapter explains the need for a centralized authentication system and explains Role-Based Access Control (RBAC) and the difference and problems with both decentralized and centralized authentication.

The second chapter is dedicated to explaining symmetric/asymmetric encryption, certificates, third party trust with Certificate Authorities (CAs) and the Transport Layer Security (TLS) in order to better understand the third and fourth chapter.

The third chapter is dedicated to the centralized user authentication management system, explaining Lightweight Directory Access Protocol (LDAP), and compares PUSH and PULL models. Based on the PULL model, a possible user authentication process is created between the authentication server and the IED. Possible failure modes and dangers are discussed including Single Point of Failure (SPOF), Denial of Service (DoS) and fake client/server situations. Possible solutions include encrypted connections to provide security for data while it is in transit, and for improved authentication, third party trusted certificates are recommended for each entity in the network.

The fourth chapter is dedicated to the security between the IED and the connecting client. Currently, there is no security for transferred data and authentication between the connecting client and the IED. Therefore, encryption during transit and certificates for each entity is recommended. In case the IEDs Internet Protocol (IP) address is changed a new Server Certificate (SC) is required. In order to get a new SC, it has to be manually installed on the IED or transferred over the network. In order to save resources, time and to improve security, a CA is installed on the IED so that the IED can create a new SC when needed. This created a problem

where the secret signing key can be stolen from the IEDs internal memory, so to avoid the secret key from being leaked, a secure storage option is recommended for storing encryption keys. A Trusted Platform Module (TPM) can provide the necessary security for storing the signing private key of the CA, the symmetric key, and the asymmetric private key on the IED. In order to handle certificates in the substation automation system, a possible combination of Certificate Revocation List (CRL) and Online Certificate Status Protocol (OCSP) has been introduced.

It must be noted that in this thesis, an IED is a protective relay. The centralized authentication server in this thesis is called the LDAP server. In most documents and standards SSL/TLS encryption is written together, but in this thesis, only the term TLS is used.