

IMPLEMENTATION AND PENETRATION TESTING OF IT SECURITY
FUNCTIONS FOR SMART GRID CLUSTER CONTROLLERS

By

Patricia Hamdoyo
11802005

BACHELOR'S DEGREE
in

INFORMATION TECHNOLOGY
FACULTY ENGINEERING OF INFORMATION TECHNOLOGY

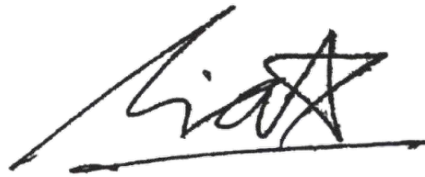


SWISS GERMAN UNIVERSITY
The Prominence Tower
Jalan Jalur Sutera Barat No. 15, Alam Sutera
Tangerang, Banten 15143 - Indonesia

June 2022

STATEMENT BY THE AUTHOR

I hereby declare that this submission is my own work and to the best of my knowledge, it contains no material previously published or written by another person, nor material which to a substantial extent has been accepted for the award of any other degree or diploma at any educational institution, except where due acknowledgement is made in the thesis.



Patricia Hamdoyo, CEH

12 June 2022

Student

Date

Approved by:



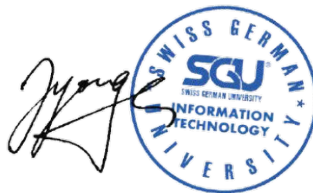
Prof. Dr.-Ing. Egon Ortjohann

12 June 2022

Thesis Advisor

Date

Dipl.-Inf I Eng Kho



12 June 2022

Thesis Co-Advisor

Date

Dr. Maulahikmah Galinium, S.Kom., M.Sc.

12 June 2022

Dean

Date

Patricia Hamdoyo

ABSTRACT

IMPLEMENTATION AND PENETRATION TESTING OF IT SECURITY FUNCTIONS FOR SMART GRID CLUSTER CONTROLLERS

By

Patricia Hamdoyo
Prof. Dr.-Ing. Egon Ortjohann, Advisor
Dipl.-Inf I Eng Kho, Co-Advisor

**SOUTH WESTPHALIA UNIVERSITY OF APPLIED SCIENCE
SWISS GERMAN UNIVERSITY**

In today's world, electricity is one of the essential aspects of daily life, especially with renewable energy technology. This work was done in the Department of Energy Supply under Prof. Dr.-Ing. Egon Ortjohann at Soest University of Applied Sciences, Germany. In this work, security functions were implemented using intelligent grid technology based on the Clustering Power System Approach (CPSA) in the Smart Grid Cluster Controller (SGCC) system. The security requirements in the field of power systems are very high due to the critical infrastructure. A smart grid is a modern power grid that uses information technology (IT). Security breaches have a threatening effect on the power grid infrastructure. The security aspect of modern networked systems is necessary to avoid threats. Recommendations about security features are based on the well-known BDEW White Paper and the 270xx series of standards for security recommendations in critical infrastructures in Germany. Some security configurations are carried out based on the security recommendations. Finally, penetration tests showed that several security vulnerabilities existed. As a result, some security

adjustments were made. This work can serve as a basis for further development of the SGCC's security function.

Keywords: International Electrotechnical Commission (IEC), Information Security Management System (ISMS), International Organization for Standard (ISO 270xx series), Penetration Testing, Smart Grid Cluster Controller.

© Writing Copyright 2022
by Patricia Hamdoyo

All rights owned by the South Westphalia University of Applied Sciences,
Institute for Electrical Power Systems,
Under the law of research projects from the
“Ministry of Education and Research”,
Federal Republic of Germany

DEDICATION

I dedicate this work to the institution Fachhochschule Südwestfalen and/or to myself.
To see how far I can work through and the things that I need to improve the most as
an engineer, a programmer, and a person.

ACKNOWLEDGEMENTS

First and foremost, I would like to express my deepest gratitude to God for always finding a way through my hardships.

Second, I would like to express my gratitude also to Prof. Dr.-Ing. Egon Ortjohann for giving me the opportunity to do my thesis work in his laboratory. I am also very thankful to Dipl.-Ing. Andreas Schmelter guided me since my internship period and encouraged me to finish this thesis work. Without his patience and guidance, this work may not be there now. I am also thankful to Shashank Damodar Varada, Joseph Andreas, and Nabila Gina Nastiti for their guidance and encouragement alongside other laboratory members.

Third, I would like to thank my family and my best friends, especially Kayla Widjaja and Livinia Tjandra for supporting me and encouraging me wherever they are since high school.

To Kennemann, I would like to thank him for welcoming me to his home like his own granddaughter and to my house roommates that welcomed me like a family. Then, to the entire SGU batch 2018 for the last 4 years of learning in SGU with awesome life experiences and an uncountable amount of fun.

Last, but not least, I would like to thank Yoshua Paradigma Situmorang who accompanied and comforted me unconditionally since the beginning of my university life.

TABLE OF CONTENTS

	Page
ABSTRACT	3
DEDICATION	6
ACKNOWLEDGEMENTS	7
TABLE OF CONTENTS	8
LIST OF FIGURES	10
LIST OF TABLES	11
CHAPTER 1 – INTRODUCTION	12
1.1. Background.....	12
1.2. Research Problems.....	13
1.3. Objectives	13
1.4. Significance of Study.....	14
1.5. Research Questions.....	14
1.6. Hypothesis	15
1.7. Thesis Scope	15
1.8. Thesis Limitation.....	16
CHAPTER 2 – LITERATURE REVIEW	17
2.1. Smart Grid.....	17
2.1. Clustering Power System Approach.....	18
2.2. Smart Grid Cluster Controller.....	19
2.3. Computer Network	20
2.4. Cybersecurity	20
2.5. Federal Association of Energy and Water Management	20
2.6. International Organization for Standardization (ISO)	23
2.7. Cluster Controller Operating System.....	23
2.8. Transmission Control Protocol and Transport Layer Security connection....	24
2.9. Secure Socket Layer	25
2.9.1 Secure Socket Layer in Port.....	26
2.10. Security Tools.....	26
2.10.1. Uncomplicated Firewall.....	26
2.10.2. OpenSSL	27

2.10.3.	TheHarvester	27
2.10.4.	Maltego	27
2.10.5.	Shodan.....	28
2.10.6.	Nmap	28
2.10.7.	Dirb	28
2.10.8.	Nikto.....	29
2.10.9.	Wireshark.....	29
CHAPTER 3 – RESEARCH METHODOLOGY		30
3.1.	Requirements Based on BDEW.....	31
3.1.1	Checklist Analysis	31
3.2.	Virtual Machine.....	33
3.3.	Uncomplicated Firewall.....	33
3.4.	OpenSSL	33
3.5.	Penetration Testing Tools.....	35
3.5.1.	Information Gathering	35
3.5.2.	Scanning the Smart Grid Cluster Controller.....	37
3.6.	Vulnerability Report	40
CHAPTER 4 – RESULTS AND DISCUSSIONS.....		41
4.1.	Initial Evaluation (Preliminary Result).....	42
4.2.	Securing Frontend page	47
4.3.	Penetration Testing Results	50
4.3.1.	Vulnerability Scanning with Maltego.....	51
4.3.2.	Vulnerability Scanning with Shodan.....	52
4.3.3.	Vulnerability Scanning with TheHarvester	53
4.3.4.	Vulnerability Scanning with Nmap	53
4.3.5.	Vulnerability Scanning with Nikto.....	58
4.3.6.	Vulnerability Scanning with Dirb.....	58
4.3.7.	Comparison HTTP and HTTPS	60
CHAPTER 5 – CONCLUSIONS AND RECOMMENDATIONS		63
5.1.	Conclusion.....	63
5.2.	Future Recommendation.....	64
GLOSSARY		65
REFERENCES		67
APPENDIX.....		72
CURRICULUM VITAE		95

LIST OF FIGURES

Figures	Page
Figure 2.1: Overall Architecture for Smart Grid (Trilliant Holdings Inc. (n.d.))	18
Figure 2.2: CPSA Implementation (Prof. Dr.-Ing. Egon Ortjohann and Wirasanti, 2014)	19
Figure 2.3: SGCC Logo (Power Supply Department at Fachhochschule Südwestfalen, 2020)	19
Figure 2.4: Example of TCP and TLS Handshake diagram (Cloudflare, 2019).....	24
Figure 2.5: Example diagram of SSL Handshake (Rijn, 2017).....	25
Figure 3.1: Thesis Workflow diagram.....	30
Figure 3.2: Generate SSL Certificate with OpenSSL tool.....	34
Figure 3.3: Example of TheHarvester Usage.....	36
Figure 3.4: Example Screenshot of Nmap scanning Facebook	38
Figure 3.5: Example usage of Dirb inside Debian VM.....	39
Figure 4.1: Port communications controlled by Docker and UFW	45
Figure 4.2: Generate SSL Certificate.....	48
Figure 4.3: Warning page after HTTPS Configuration.....	49
Figure 4.4: Login page after HTTPS Configuration.....	49
Figure 4.5: Configuration test with wget	50
Figure 4.6: Simple architecture of penetration testing environment.....	50
Figure 4.7: Information gathering result with Maltego.....	51
Figure 4.8: Information gathering with Shodan.....	52
Figure 4.9: Information gathering result with TheHarvester	53
Figure 4.10: Scanning result by Nmap using Kali Linux part 1	54
Figure 4.11: Scanning result by Nmap using Kali Linux part 2	55
Figure 4.12: Scanning result by Nmap using Kali Linux part 3	56
Figure 4.13: Nmap scan result for Heartbleed	57
Figure 4.14: Nikto scanning result.....	58
Figure 4.15: Dirb scanning result.....	59
Figure 4.16: Wireshark sniffing result through HTTP communication.....	60
Figure 4.17: Wireshark sniffing result after HTTPS configuration	61
Figure 4.18: Nmap result scan after port localization part 1.....	62
Figure 4.19: Nmap result scan after port localization part 2.....	62

LIST OF TABLES

Table	Page
Table 1: Checklist of priority for SGCC security based on BDEW Whitepaper.....	72
Table 2.1: Part of BDEW Checklist Table (E-wirtschaft, 2018)	21
Table 3.1: Legend for checklist based on BDEW	31
Table 3.2: Table Header Description Based on BDEW Whitepaper	32
Table 4.1: Overview of chapter 4.....	41
Table 4.2: Checklist of highest priority for SGCC security features	42
Table 4.3: Commands for SSL key generation.....	47