

**CYBERSECURITY RISK AND PRIVACY RISK IDENTIFICATION
ON RDAP RISK ASSESSMENT:
Case study PANDL.ID**

By

Andi Budimansyah

2-1951-025

MASTER'S DEGREE

in

MASTER OF INFORMATION TECHNOLOGY

FACULTY OF ENGINEERING AND INFORMATION TECHNOLOGY

SWISS GERMAN UNIVERSITY


SWISS GERMAN UNIVERSITY

The Prominence Tower

Jalan Jalur Sutera Barat No. 15, Alam Sutera

Tangerang, Banten 15143 - Indonesia

11 January 2021

Revision after thesis defense on 27 January 2021

ABSTRACT

**CYBERSECURITY AND PRIVACY RISK IDENTIFICATION ON RDAP
RISK MANAGEMENT: CASE STUDY PANDI.ID**

By

Andi Budimansyah

Dr. Ir. Moh. A. Amin Soetomo, M.Sc, Advisor

Dr. Charles Lim, BSc., MSc., Co-Advisor

SWISS GERMAN UNIVERSITY

The Registration Data Access Protocol (RDAP) is a WHOIS replacement protocol to find-out Domain Name registration information with one of its features, "user differentiated access," with limited Registrant data for anonymous and complete for authenticated users. It requires the placement of a complete Registrant Data in the Data Store, containing personal data protected by law. Previous papers guide Digital Forensic Investigators to collect digital evidence related to the domain and IP registrations and recommend getting complete Registration data. Another paper provides RDAP with the system, device, and method to improve mitigation from abnormal request analysis patterns. This research Explains RDAP system design and conducts a Risk Assessment using ISO / IEC 27 005 as a general guide and at the stage of risk identification, using LINDDUN for Privacy risk and STRIDE for cybersecurity risk. Furthermore, the mitigation suggestions at the Strategic, Tactical, and Operational level in the People, Process, and Technology. Finally, some institutions recommended having the complete Registrant data directly through Access Rights or indirectly through Request Rights.

Keywords: Registration Data Access Protocol, RDAP, Risk Assessment, ISO 27005, STRIDE, LINDDUN, Cybersecurity Risk, Privacy Risk, Risk Assessment, PANDI, .ID Registry.

Andi Budimansyah



© Copyright 2021

by Andi Budimansyah

All rights reserved

SWISS GERMAN UNIVERSITY

DEDICATION

I dedicate this works for the future of the country I loved: Indonesia



ACKNOWLEDGEMENTS

I wish to thank, Dr. Ir. Moh. A. Amin Soetomo, M.Sc, as Thesis Advisor, and Dr. Charles Lim, BSc., MSc. Thesis Co-Advisor has patiently guided the author extraordinarily in the preparation of this research.

I also thank the Chancellor, Dean and all lecturers, and Administration, Library from SGU, fellow SGU MIT Batch 25 students who help each other, work hand in hand, and continue to encourage and discuss.

All PANDI Management for the 2019-2023 Period has provided the opportunity to conduct RDAP research at PANDI and Diky Proyogo, Maskat, who is very helpful in its implementation.

Thank you also to Prof. Yudho Giri Sucahyo, S.Kom, M.Kom, Ph.D., CISA, CISM, ISO 27001 LA, Ir. Isnawan, Shidiq Purnama, S.Kom, MM, ISO 27001 LI, NSA, Basuki Suhardiman, Shita Laksmi, SIKom, MA, MA, Riki Arif Gunawan, Teguh Arifyadi, SH, MH, CEH, CHFI for providing time in evaluating, providing valuable suggestions and input in writing this research. Also, to DR. Bisyron Wahyudi, Ruby Alamsyah, Hasto Prastowo, Achmad Yahya Sjarifuddin, MBA. who took the time to validate this research.

Finally, I also thank my beloved wife Astuty Mahmud and my dear children Imam Wicaksono, Andi Thasya Barlian, Andi Intan Anjani, and Andi M. Alghifari for their support and enthusiasm.

Hopefully, all the support, guidance, input, direction, enthusiasm, and motivation will be good deeds that will get more rewards from Allah SWT.

TABLE OF CONTENTS

| | Page |
|------------------------------------------------|-----------|
| STATEMENT BY THE AUTHOR | 2 |
| ABSTRACT | 3 |
| DEDICATION..... | 5 |
| ACKNOWLEDGEMENTS | 6 |
| TABLE OF CONTENTS | 7 |
| LIST OF FIGURES | 11 |
| LIST OF TABLES | 13 |
| CHAPTER 1 – INTRODUCTION | 14 |
| 1.1. Background | 14 |
| 1.2. Problem statement | 17 |
| 1.2.1 The Problem with WHOIS Protocol..... | 17 |
| 1.2.2. The Challenge of implementing RDAP..... | 18 |
| 1.3. Research objective..... | 19 |
| 1.4. Research Question | 20 |
| 1.5. Scope and limitation | 20 |
| 1.6. Significance of study | 20 |
| 1.7. Hypothesis..... | 21 |
| 1.8. Thesis structure | 21 |
| CHAPTER 2 – LITERATURE RIVIEW | 22 |
| 2.1. Theoretical Perspectives | 22 |
| 2.2. Technology standard | 23 |
| 2.2.1. WHOIS RFC | 23 |

| | |
|-----------------------------------------------------------------------------------------------------|-----------|
| 2.2.2. Registration Data Access Protocol (RDAP) RFCs | 25 |
| 2.3. Regulation..... | 26 |
| 2.3.1. Law of the Republic of Indonesia concerning Electronic Information and Transactions | 26 |
| 2.3.2. Republic of Indonesia draft Law on Personal Data Protection | 27 |
| 2.3.3. General Data Protection Regulation (GDPR) | 28 |
| 2.4. The Risk Management in PANDI.ID | 29 |
| 2.5. The RDAP RISK..... | 33 |
| 2.5.1. Cyber security Risk | 33 |
| 2.5.2. Privacy Risk | 33 |
| 2.6. Frame work for Risk Management | 35 |
| 2.6.1 NIST 800:30 r1 | 35 |
| 2.6.2 ISO/IEC 31000 – Risk Management Guidelines | 38 |
| 2.6.3 ISO/IEC 27005 Information security risk management | 40 |
| 2.6.4 NIST Privacy Framework | 41 |
| 2.7. Threat Modeling Method (TMM) | 42 |
| 2.7.1 Overview | 42 |
| 2.7.2. STRIDE..... | 43 |
| 2.7.3. LINDDUN | 45 |
| 2.8. Papers on RDAP, Risk Management, Data Privacy | 48 |
| 2.9. Related Work..... | 51 |
| CHAPTER 3 – RESEARCH METHODS | 61 |
| 3.1. Research Methodology | 61 |
| 3.2. Research Frame work..... | 61 |
| 3.2.1. Context Establishment | 62 |
| 3.2.2. Risk Identification..... | 62 |

| | |
|--------------------------------------------------------------------------------------------------------|-----------|
| 3.2.3. Risk Analysis | 63 |
| 3.2.4. Risk Evaluation..... | 63 |
| 3.2.5. Research Evaluation and Validation..... | 63 |
| CHAPTER 4 – RESULTS AND DISCUSSIONS | 67 |
| 4.1. Context Establishment..... | 67 |
| 4.1.1. Data Flow Diagram model for the RDAP..... | 68 |
| 4.2. Risk Identification..... | 71 |
| 4.2.1. The RDAP Assets | 71 |
| 4.2.2. RDAP Security Assumptions..... | 73 |
| 4.2.3. Mapping the threat | 76 |
| 4.2.4. Identify Threat Scenario (and assessment of consequences) using Misuse case (MUC) table..... | 83 |
| 4.3. Risk Analysis | 83 |
| 4.3.1 Assessment of Consequences | 86 |
| 4.3.2. Assessment of incident likelihood | 86 |
| 4.3.3. Level of Risk Determination..... | 86 |
| 4.4. Risk Evaluation | 86 |
| 4.4.1. Evaluation of levels of risk base on risk evaluation criteria | 86 |
| 4.4.2. RDAP Suggestions..... | 87 |
| 4.5. Research Evaluation and Validation..... | 92 |
| 4.5.1. Research Evaluation by Expert Judgment | 92 |
| 4.5.2. Research Validation | 93 |
| 4.6. Some challenge on implementing RDAP in PANDI | 95 |
| 4.7. Research Summary | 96 |
| CHAPTER 5 – CONCLUSION AND RECCOMENDATIONS | 97 |
| 5.1. Conclusion | 97 |

| | |
|----------------------------------------------------------------------------------|------------|
| 5.2 Recommendations | 98 |
| 5.3. Future work | 99 |
| GLOSSARY..... | 100 |
| APPENDIX..... | 105 |
| A. Chronology of RDAP implementation (ICANN, n.d.) | 105 |
| B. Full data and limited data in Domain data display | 106 |
| C. Definition of Personal Data | 108 |
| D. OWASP API Security Top 10 – 2019 | 114 |
| E. Risk Evaluation from LINDDUN to Identify Privacy threat scenarios .. | 116 |
| F. Risk evaluation from STRIDE to identify Cybersecurity threats scenario | 120 |
| G. Detail RDAP risk from LINDDUN and STRIDE and Suggested | |
| Mitigation..... | 131 |
| H. Likelihood and Impact risk determination using PANDI Policy and | |
| SOP. 132 | |
| I. Example of STRIDE Classification Model Spoofing | 133 |
| J. Research Evaluation | 134 |
| K. Research Validation..... | 137 |
| L. RDAP Use case & Activity Diagram | 141 |
| M. Some screen capture of the RDAP application..... | 151 |
| REFERENCES | 155 |
| CURRICULUM VITAE..... | 161 |

LIST OF FIGURES

| Figures | Page |
|----------------------------------------------------------------------------------------------------------------------|------|
| Figure 1-1 Domain Name Registry Basic Services | 14 |
| Figure 1-2 PANDI Request WHOIS 2020 | 14 |
| Figure 1-3 RDAP response for different type of user | 18 |
| Figure 2-1 RDAP Authentication (ICANN) | 23 |
| Figure 2-2 The requirement of PIA identification in GDPR (Wei et al, 2020) | 29 |
| Figure 2-3 Risk Management Concept (PANDI, 2020) | 30 |
| Figure 2-4 A Taxonomy of Privacy (Solove, 2006) | 34 |
| Figure 2-5 Risk Assessment in the risk management (NIST 800-30 Rev 1, 2012) | 36 |
| Figure 2-6 Risk Management Hierarchy (NIST 800-30 Rev 1, 2012) | 37 |
| Figure 2-7 Risk Assessment Process. (NIST 800-30 Rev 1, 2012) | 38 |
| Figure 2-8 Principles, framework and process (ISO 31000 - Risk Management Guidelines, 2018) | 39 |
| Figure 2-9 The Process (ISO 31000 - Risk Management Guidelines, 2018) | 40 |
| Figure 2-10 The risk management process (ISO / IEC 27005 Information Security Risk Management, 2018) | 41 |
| Figure 2-11 Cybersecurity and Privacy Risk Relationship (National Institute of Standards and Technology, 2020) | 42 |
| Figure 2-12 LINDDUN Methodology steps (Wuyts & Joosen, 2015b) | 46 |
| Figure 2-13 First 3 LINDDUN steps (Problem space) (Wuyts & Joosen, 2015b) | 47 |
| Figure 2-14 Final 3 LINDDUN steps (Solution space) (Wuyts & Joosen, 2015b) | 48 |
| Figure 2-15 Mapping of ISO 27005, LINDDUN and STRIDE | 60 |
| Figure 3-1 Research Framework | 62 |
| Figure 4-1 RDAP & WHOIS configuration module | 68 |
| Figure 4-2 RDAP Data Flow Diagram | 69 |
| Figure 4-3 The RDAP Assets | 72 |
| Figure 4-4 Entity Relationship Diagram | 73 |
| Figure 4-5 Level of Risk Determination | 86 |

Figure 4-6 Risk Evaluation87



LIST OF TABLES

| Tables | Page |
|------------------------------------------------------------------------|------|
| Table 1-1 ccTLD Whois and RDAP Server Tables..... | 16 |
| Table 2-1 RDAP & WHOIS comparisons..... | 22 |
| Table 2-2 Impact level assessment criteria (PANDI, 2020) | 32 |
| Table 2-3 likelihood level assessment criteria (PANDI, 2020) | 32 |
| Table 2-4 TMM Strengths and Weaknesses (Shevchenko et al., 2018) | 43 |
| Table 2-5 The STRIDE Threats (Adam Shostack, 2014) | 44 |
| Table 2-6 STRIDE-per-Element (Adam Shostack, 2014) | 44 |
| Table 2-7 LINDDUN Mapping Template (Wuyts & Joosen, 2015a) | 46 |
| Table 2-8 Related work..... | 54 |
| Table 2-9 Mapping ISO 27005-LINDDUN-STRIDE | 58 |
| Table 3-1 IPO Methodology | 64 |
| Table 3-2 LINDDUN per element | 65 |
| Table 3-3 STRIDE Per-element | 66 |
| Table 3-4 Misuse case..... | 66 |
| Table 4-1 Detail Process - Extended to DFD..... | 70 |
| Table 4-2 Assumption..... | 74 |
| Table 4-3 LINDDUN Mapping Table | 76 |
| Table 4-4 STRIDE per-element | 78 |
| Table 4-5 Summary misuse case..... | 84 |
| Table 4-6 PPT Suggested mitigations | 87 |
| Table 4-7 Authenticated user recommendations..... | 91 |