Knowledge-Based Support for Security Risk Analysis of Microgrid

Gang Yang, Puzhi Yao, (gang.yang, puzhi.yao)@student.Adelaide.edu.au, Master of Software Engineering
Supervised By Prof. M. Ali Babar, (ali.babar@Adelaide.edu.au)
School of Computer Science

Introduction

- Like any other networked system, a Microgrid system can be a prime target of cyber security attacks that need to be taken into consideration during the design and operations of a Microgrid.
- There is a lack of realisation of the potential risk of cyber attacks and lack of knowledge for analysing and addressing the risks that can be exploited to launch cyber attacks, which can result in a huge social and financial damages.

Research Problem

- Microgrid systems are a new breed of systems whose design, development, and operations may not be driven by security sensitive considerations.
- Key stakeholders (e.g., designers, developers, managers, and operators) may not have the required cyber security knowledge to analyse the threat landscape and the potential solutions.

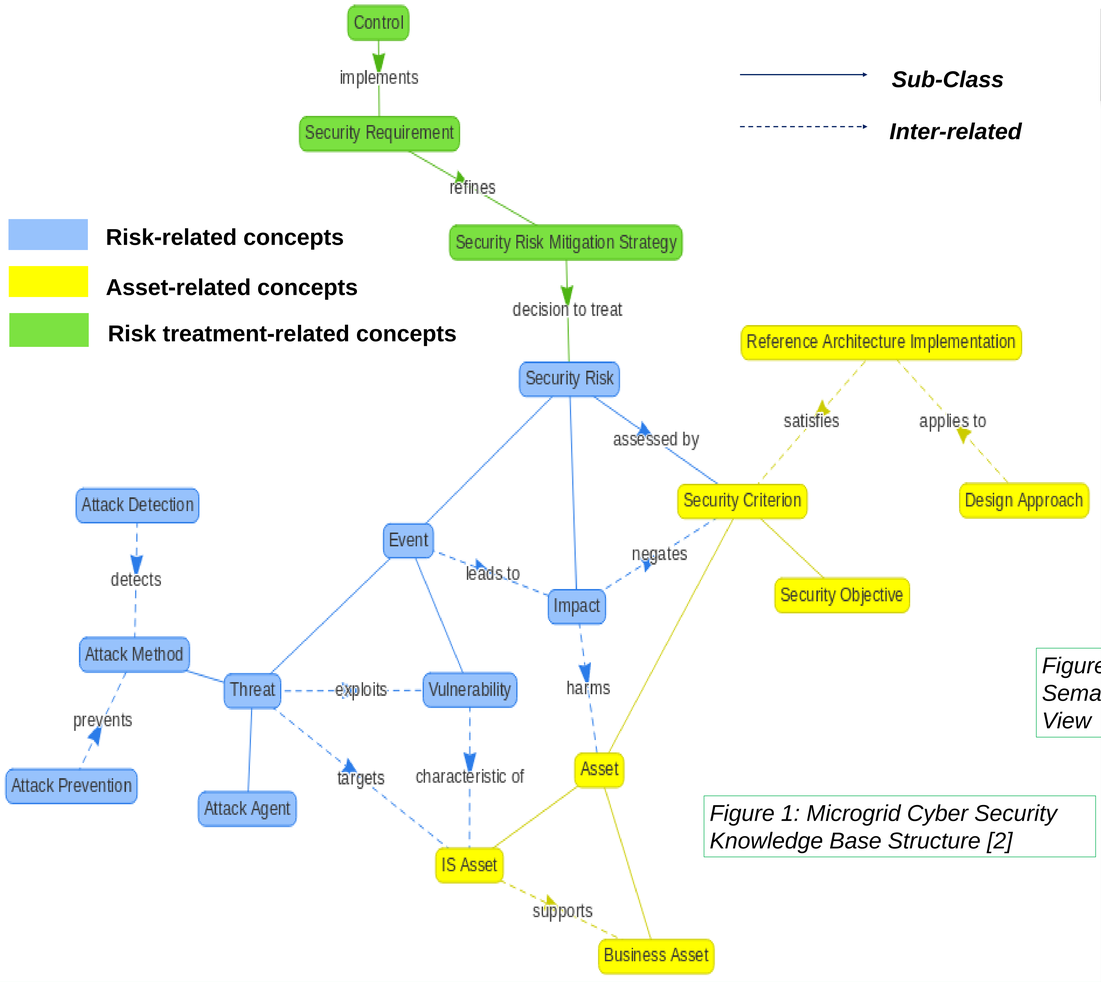

Figure 1: Microgrid Cyber Security Knowledge Base Structure [2]

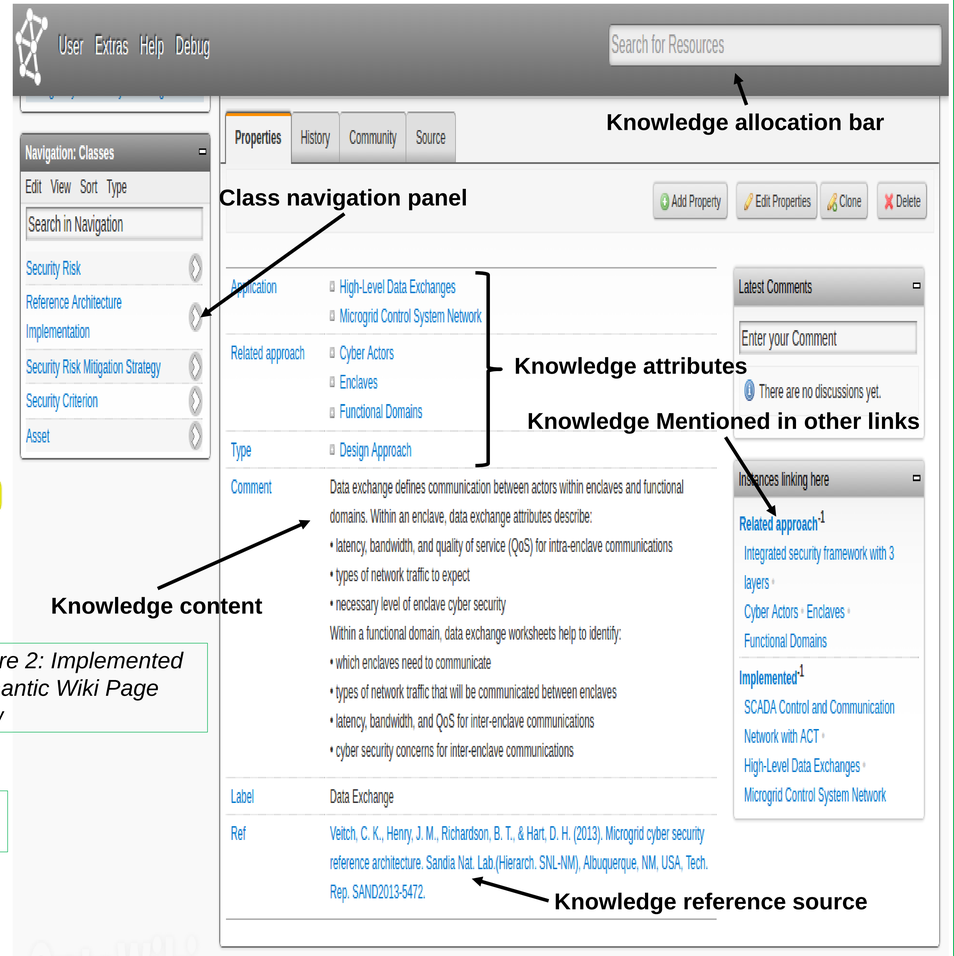

Figure 2: Implemented Semantic Wiki Page View

Project Objectives

- Determine the types of cyber security threats to and solutions for Microgrid systems for coalescing the available information in a readily usable form.
- Develop a knowledge-based approach that can support cyber security risk analysis of Microgrid.
- Leverage a semantic and extensible Wiki platform that can support our approach to capturing and sharing cyber security knowledge for analysing threats and devising solutions of Microgrid.

Key Milestones

- Reviewed a large amount of literature on cyber security threats to Smart Grid and Microgrid for identifying and categorising the reported cyber security threats, vulnerabilities, challenges, their potential impacts and proposed solutions for Microgrid systems.
- Built and evaluated an Ontological model to characterise a knowledge system which captures cyber security threats and solutions of Microgrid.
- Designed and Implemented a semantic Wiki (i.e., OntoWiki) based system for implementing the cyber security knowledge model for easy of capture and management of cyber security knowledge.

Future Work

- Carry out extensive evaluation of the developed approach and system with the real users of Microgrid systems.
- Refine and enhance the approach and the implemented systems for Microgrid cyber security decision making.
- Deploy the system in real-life setting for assessing it robustness and value.

Key References

[1] Wenye Wang and Zhuo Lu. Cyber security in the smart grid: Survey and challenges. *Computer Networks*, 57(5):1344–1371, 2013.
[2] Dubois, É., Heymans, P., Mayer, N., & Matulevičius, R. (2010). A systematic approach to define the domain ISSRM. In *Intentional Perspectives on Information Systems Engineering* (pp. 289-306). Springer Berlin Heidelberg.
[3] Veitch, C. K., Henry, J. M., Richardson, B. T., & Hart, D. H. (2013). Microgrid cyber security reference architecture. *Sandia Nat. Lab.(Hierarch. SNL-NM), Albuquerque, NM, USA, Tech. Rep. SAND2013-5472.*