Abstract

The Self-Sovereign Identity (SSI) model is a cutting-edge approach to identity management that empowers individuals with complete control and sovereignty over their digital identities. This is achieved through the utilization of distributed ledger technology, allowing for autonomous administration without the need for central authorities. A system that implements the key architecture and features defined by the SSI model is commonly referred to as an SSI management system. As a personal information processing system, it is imperative that SSI management systems are designed with sufficient security and privacy measures to ensure the protection of personal information.

In SSI management systems, various security and privacy considerations can be evaluated and enhanced. The process of analyzing security weaknesses is an effective method for identifying the presence of common weaknesses in the target system. Similar to other domain software systems, SSI management systems may have specific weaknesses that require attention. The governance of the SSI management system serves as a framework for enforcing the principles and system properties defined by the SSI model, which are critical to protecting the operation of digital identities in various contexts. However, it has been noted that the current principles and system properties may not address necessary security and privacy aspects. Data sharing events within the SSI management system are unique situations in which data objects are made available with other actors. These events should be aligned with the SSI governance to ensure adequate protection.

This dissertation presents an approach to evaluating the security and privacy of the SSI management system by integrating domain expertise with information retrieval and system modeling techniques. The proposed approach consists of three solutions: mitigating SSI-specific weaknesses, improving SSI system properties, and modeling SSI data sharing events.

The first solution for enhancing security in the SSI management system is to mitigate the unique security weaknesses specific to this system. Currently, there has been limited research on SSI-specific weaknesses, making it challenging to identify them directly from the design of the SSI management sys-

tem. This dissertation aims to overcome this challenge by utilizing language correlations between descriptions of common security weaknesses published in the well-respected Common Weakness Enumeration (CWE) database and the functional requirements of the SSI management system. The goal is to infer the presence of SSI-specific weaknesses and initiate further analysis and mitigation efforts. To accomplish this, the SSI Weakness Identification Framework (SWIF) is proposed. This framework combines natural language processing and information retrieval techniques with the creation of a cross-domain transfer knowledge graph to identify SSI-specific weaknesses. The results of this study indicate that a recommender system implementing the SWIF is capable of accurately identifying language correlations and inferring valid SSI-specific weaknesses with optimal efficiency.

The second solution of the proposed approach is to improve the security and privacy of SSI system properties. This dissertation leverages laws, regulations, and standards as source documents to achieve this improvement. The principles and system properties of the SSI management system must adhere to these source documents in order to ensure proper governance of the system in terms of security and privacy. However, the definitions of laws, regulations, and standards differ from the SSI model concept, making it challenging to directly align source documents with SSI system properties. To address this challenge, this dissertation presents a systematic analysis method and an improved set of SSI system properties. The analysis method is used to assess the compatibility of security and privacy controls from source documents with existing SSI system properties, and to revise or introduce new properties as necessary. The improved SSI system properties are more globally consistent with source documents than the current set and are applicable to actual scenarios.

The final solution of the proposed approach involves a method for modeling SSI data-sharing events. This dissertation aims to comprehensively analyze these events by extracting the unique types and constraints from the SSI model concept. The events are modeled as a state transition system to provide a foundation for security and privacy analysis. The transformed SSI system properties serve as security and privacy specifications in the context of data sharing. The proposed method involves modeling the SSI data sharing state transition system using the Alloy specification language. The result could report a secure and privacy-preserving data sharing system within a specified scope.

Keywords: self-sovereign identity, weakness identification, compliance property, software modeling, security and privacy