[A set of semantic data flow diagrams and its security analysis based on ontologies and knowledge graphs]

- **Autor:** Brazhuk, Andrei
- **Descrição:** For a long time threat modeling was treated as a manual, complicated process. However modern agile development methodologies and cloud computing technologies require adding automatic threat modeling approaches. This work considers two challenges: creating a set of machine-readable data flow diagrams that represent real cloud based applications; and usage domain specific knowledge for automatic analysis of the security aspects of such applications. The set of 180 semantic diagrams (ontologies and knowledge graphs) is created based on cloud configurations (Docker Compose); the set includes a manual taxonomy that allows to define the design and functional aspects of the web based and data processing applications; the set can be used for various research in the threat modeling field. This work also evaluates how ontologies and knowledge graphs can be used to automatically recognize patterns (mapped to security threats) in diagrams. A pattern represents features of a diagram in form of a request to a knowledge base, what enables its recognition in a semantic representation of a diagram. In an experiment four groups of the patterns are created (web applications, data processing, network, and docker specific), and the diagrams are examined by the patterns. Automatic results, received for the web applications and data processing patterns, are compared with the manual taxonomy in order to study challenges of automatic threat modeling.
- **Data de Criação:** 2023
- **Idioma:** Inglês
- **Identificador:** DOI: 10.48550/arxiv.2303.11198
- **Fonte:** arXiv.org

[A set of semantic data flow diagrams and its security analysis based on ontologies and knowledge graphs]

- **Autor:** Brazhuk, Andrei
- **Assuntos:** Applications programs ; Cloud computing ; Computer security ; Data processing ; Graphs ; Knowledge bases (artificial intelligence) ; Knowledge representation ; Ontology ; Pattern recognition ; Security aspects ; Semantics ; Taxonomy ; Threat models
- **É parte de:** arXiv.org, 2023
- **Descrição:** For a long time threat modeling was treated as a manual, complicated process. However modern agile development methodologies and cloud computing technologies require adding automatic threat modeling approaches. This work considers two challenges: creating a set of machine-readable data flow diagrams that represent real cloud based applications; and usage domain specific knowledge for automatic analysis of the security aspects of such applications. The set of 180 semantic diagrams (ontologies and knowledge graphs) is created based on cloud configurations (Docker Compose); the set includes a manual taxonomy that allows to define the design and functional aspects of the web based and data processing applications; the set can be used for various research in the threat modeling field. This work also evaluates how ontologies and knowledge graphs can be used to automatically recognize patterns (mapped to security threats) in diagrams. A pattern represents features of a diagram in form of a request to a knowledge base, what enables its recognition in a semantic representation of a diagram. In an experiment four groups of the patterns are created (web applications, data processing, network, and docker specific), and the diagrams are examined by the patterns. Automatic results, received for the web applications and data processing patterns, are compared with the manual taxonomy in order to study challenges of automatic threat modeling.
- **Editor:** Ithaca: Cornell University Library, arXiv.org
- **Idioma:** Inglês
- **Identificador:** EISSN: 2331-8422
- **Fonte:** Free E- Journals