Dandan WU, Jie CHEN, Ruiyun XIE, Ke CHEN, 2024. OntoCSD: an ontology-based security model for an integrated solution of cyberspace defense. *Frontiers of Information Technology & Electronic Engineering*, 25(9):1209-1225. https://doi.org/10.1631/FITEE.2300662

OntoCSD: an ontology-based security model for an integrated solution of cyberspace defense

Key words: Cyberspace defense; Integrated solution; Ontology; Case-based reasoning (CBR); Computer network defense (CND)

Corresponding author: Dandan WU
E-mail: wudd_2023@163.com
ORCID: https://orcid.org/0000-0001-5214-387X

Introduction

The construction of an integrated solution for cyberspace defense with dynamic, flexible, and intelligent features is a new idea.

To solve the problem whereby traditional static protection methods cannot respond to various network attacks or security demands in an adversarial network environment in time, and to form a complete integrated solution from “threat discovery” to “decision-making generation,” we propose an ontology-based security model, OntoCSD, for an integrated solution of cyberspace defense that uses Web ontology language (OWL) to represent the ontology classes and relationships of threat monitoring, decision-making, response, and defense in cyberspace, and uses semantic Web rule language (SWRL) to design the defensive reasoning rules. Further, the case-based reasoning (CBR) is used to quickly generate a detailed and comprehensive decision-making scheme.

OntoCSD can discover potential relationships among network attacks, vulnerabilities, the security state, and defense strategies.

Hightlight

1. OntoCSD integrates ontology classes, relationships, and reasoning rules, which can provide a dynamic, flexible, and intelligent defense mechanism. We have also designed a double-layer knowledge reasoning model. OntoCSD is different from other models that can reason only some simple point-to-point risks and defensive measures. This standardized design expression is conducive to realizing integrated solutions quickly, accurately, and intelligently.
2. We are committed to relying on the Protégé platform and its compatibility with multiple reasoning engines to form integrated solutions, from ontology modeling and threat reasoning to decision-making scheme generation.
3. The consistency and feasibility of OntoCSD are validated by Kendall's coefficient of concordance (*W*) and four experimental cases in a typical computer network defense (CND) system. It is proved that OntoCSD can support automatic association and reasoning, and provide an integrated solution framework for cyberspace defense.

Research methods

1. we propose an ontology-based security model, OntoCSD, for an integrated solution for cyberspace defense that uses Web ontology language (OWL) to represent the ontology classes and relationships of threat monitoring, decision-making, response, and defense in cyberspace.

The definition of OntoCSD based on ontology is: $O = (C, R, I, D, A)$

2. To simulate the attack scene, the corresponding reasoning rules are designed by using SWRL (semantic Web rule language).

The form of the SWRL rule is as follows: $A_1, A_2, \cdots, A_m \rightarrow B_1, B_2, \cdots, B_n$

So, different kinds of reasoning rules such as finding a potential risk in entities based on actual needs can be designed. For example, reasoning rules for entity security vulnerabilities in systems can be designed in Fig. 1.

{
ISComponents (?ISC)
^hasVulnerability(?ISC, ?vul)
^Vulnerability(?vul)
^Attacker(?attacker)
^Uses(?vul, ?Network)
->CompromisedBy (?ISC, ?attacker)
}

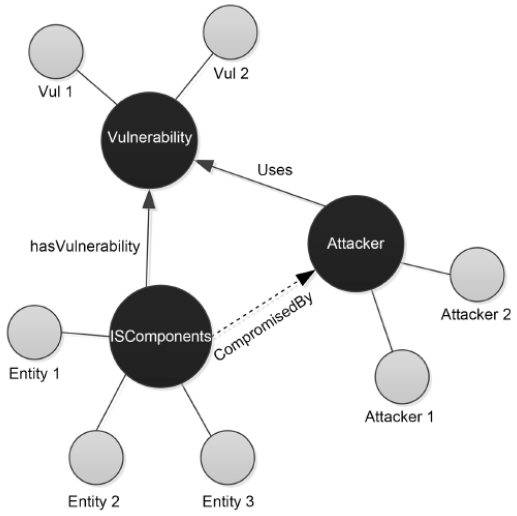


Fig. 1 A graphical example of a reasoning rule

Research methods

3. We bulid the framework for an integrated solution in Fig. 2. OntoCSD focuses on the double-layer reasoning process for an integrated solution based on ontology, including network threat reasoning (rule reasoning) and decision-making reasoning (case reasoning).

Step 1: According to the input of network threat information, the implicit security risk data will be obtained by threat reasoning rules.

Step 2: The output of threat reasoning is applied to the generation of a decision-making scheme as the input data; the best scheme will be obtained by calculating the similarity value. Moreover, the administrator can make local adjustments to this scheme.

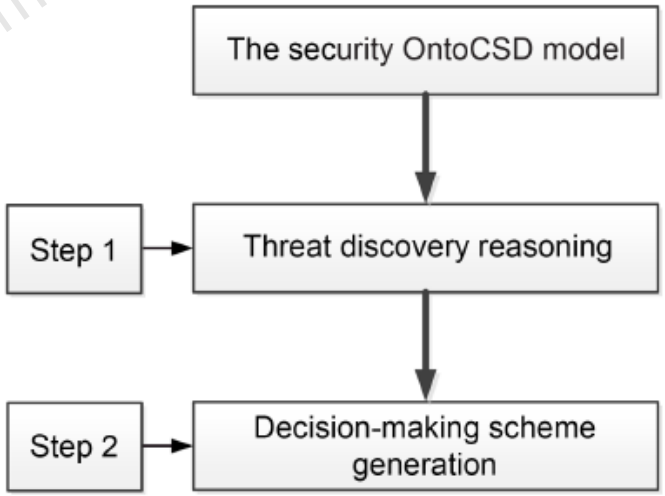


Fig. 2 The double-layer reasoning framework for an integrated solution

Research methods

We take the existing network attacks and vulnerabilities data as the main threat database to design different experiments to test the performance of OntoCSD. The consistency of the ontology-based security model is validated by Kendall's coefficient of concordance (*W*). Furthermore, in order to evaluate the consistency and feasibility of reasoning about the problem of cyberspace defense, four security threat cases in a typical CND system are selected for representation and reasoning experiments.

Protégé (version 5.5.0), developed by Stanford University, is used as an ontology platform that can provide a graphical and interactive knowledge ontology development environment. The OWL class is used to establish the ontology model. In our experiment, the HermiT (Version1.4.3.456) engine is selected as a threat reasoning tool to verify the consistency of the knowledge. The implicit knowledge and correlation can be deduced correctly with SWRL rules. The myCBR workbench is selected as the decision-making reasoning engine to provide task-oriented configuration, knowledge modeling, case base processing, and case similarity comparison.

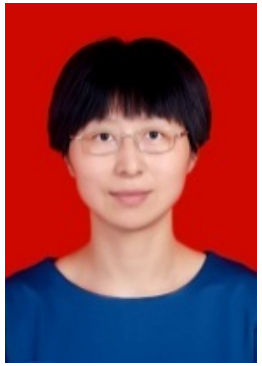
Research methods

The knowledge area coverage and problem-solving capacities of OntoCSD and other ontology models in the domain of cyberspace defense are compared.
OntoCSD is more comprehensive and valuable than the other ontology models in the field of cyberspace security in four dimensions: system entity, reasoning rules, consistency verification, and whether to generate defense decision-making scheme. Furthermore, the scalability of OntoCSD can adapt to the changing environment, such as power networks, task networks, service networks, supply chain networks, and other complex networks. Network managers can design reasoning rules according to the actual environment and security requirements. Different reasoning rules that meet different defense needs can significantly improve the reasoning capabilities of OntoCSD and meet the adaptability in virtual network adversarial environments.

Future directions

1. It should be made clear that the research into constructing an integrated solution with dynamic, flexible, and intelligent characteristics is also a new challenge.
2. The OntoCSD model is still in its initial stage for an integrated solution. The mentionable thing is that the defensive scheme generated using a similarity-based CBR method is currently used for only small-scale CND systems, while network topology security schemes targeting large-scale nodes (such as hundreds of nodes or more) require further analysis and argumentation. The established defense case base needs to be updated in real time and evaluated for defense performance based on the latest developments and changes in network threats, which should be conducted from multiple dimensions such as the efficiency, robustness, availability, security, and reliability of system security operation. These issues will be the main focus of our research in the future.

Dandan WU received the Postgraduate degree in School of Mechano-Electronic Engineering of Xidian University, Xi'an, China in 2014. Her current research interests include cyberspace security, and deep learning.



Jie CHEN received the B.S. degree in Computer Science and Technology from the Chongqing University of Computer Science, China in 1999, and received the M.S. degree from the Sichuan University of Electronic and Communication Engineering, China in 2006. She is currently pursuing the Ph.D. degree in School of Cybersecurity of Northwestern Polytechnical University. Her current research interests include cyberspace security, network defense architecture, and AI algorithms.

Ruiyun XIE is an Associate professor and doctoral supervisor at the Northwestern Polytechnical University. His current research interests include cyberspace security and network confrontation.