Computers and Electrical Engineering 000 (2017) 1–14

Contents lists available at ScienceDirect

Computers and Electrical Engineering

journal homepage: www.elsevier.com/locate/compeleceng

Network security assessment using a semantic reasoning and graph based approach[☆]

Songyang Wu, Yong Zhang[*], Wei Cao

The Third Research Institute of Ministry of Public Security, Shanghai 201204, China

ARTICLE INFO

Article history:
Received 11 July 2016
Revised 1 February 2017
Accepted 1 February 2017
Available online xxx

Keywords:
Network security
Security ontology
Attack graph
Semantic reasoning

ABSTRACT

Owing to the high value of business data, sophisticated cyber-attacks targeting enterprise networks have become more prominent, with attackers trying to penetrate deeper into and reach wider from the compromised machines. An important security requirement is that domain experts and network administrators have a common vocabulary to share security knowledge and quickly help each other respond to new threats. We propose an innovative ontology and graph-based approach for security assessment. An ontology is designed to represent security knowledge such as that of assets, vulnerabilities, and attacks in a common form. Using the inference abilities of the ontological model, an efficient system framework is proposed to generate attack graphs and assess network security. The performance of the proposed system is evaluated on test networks of differing sizes and topologies.

1. Introduction

Enterprise networks that employ various IT (Information Technology) services are becoming more and more important for achieving business objectives. Owing to the high value of business related data, sophisticated attacks targeting enterprise networks have become more prominent in recent years. The attackers will no longer stop after a single successful attack, but try to penetrate deeper into and reach wider from the compromised machines. A security administrator for an enterprise network has to combat these multistage and multi-host attack scenarios [1,2]. As the combination of machines and services deployed on enterprise networks become increasingly complex, assessing the overall security of an enterprise network becomes a daunting task for human administrators. To maintain the security and availability of a productive IT infrastructure, a common vocabulary and automated solutions are important for exchanging security knowledge and analysing potential attacks on an enterprise network.

Attack graphs [3] are useful tools that help facilitate scalable security analysis of enterprise networks by illustrating complicated-potentially multistage-attack paths to network administrators. Many security management schemes based on attack graphs have been proposed [2,4–7], these enable analysts to understand the cause and consequences of security risks, and help to determine appropriate countermeasures. In general, security assessment of a network through attack graphs requires the several steps. Firstly, collecting the attributes of the network including topology, services, vulnerabilities, and configurations. Secondly, mapping each attack action to different vulnerabilities using certain formal language (such as Datalog used in MulVAL [4]). Thirdly, generating attack graphs to illustrate the threat of various attack scenarios to critical

[☆] Reviews processed and recommended for publication to the Editor-in-Chief by Area Editor Dr. G. Martinez.

[*] Corresponding author.
E-mail address: zhangyonglab@yeah.net (Y. Zhang).

http://dx.doi.org/10.1016/j.compeleceng.2017.02.001
0045-7906/© 2017 Elsevier Ltd. All rights reserved.

assets. Finally, to recommend damage mitigation measures. However, one major drawback of attack graphs is the lack of a common vocabulary to share security knowledge between security domain experts and network administrators. Because of the large volume of information collected from various devices on enterprise networks, administrators face obstacles in effectively modelling security problems, and making correct decisions based on limited security assessment experience.

In this paper, we propose an innovative security assessment approach that uses ontology [8] to share attack knowledge between multiple parties and infer logic-based attack graphs. The ontology serves as a common vocabulary, which is designed to represent security knowledge such as that of vulnerabilities, attacks, and the relationships between them. This ontological model also adopts SWRL (Semantic Web Rule Language) rules to help express the cause-consequence relationships of all known attack scenarios. Using a reasoning engine such as JESS (Java Expert System Shell) [9], potential threats to critical IT assets can be inferred using the predefined SWRL rules. A full attack graph may be constructed depending on the inference abilities of the ontological model. The ontology and SWRL use the Open World Assumption [10], whereby the semantic ontology is extended to incorporate knowledge of new vulnerabilities and threats. Such an approach facilitates information exchange and enables administrators to accomplish security assessment tasks with the help of domain experts. Our major contributions include:

- An enhanced security ontology based upon previous works [11,12] is designed for modelling central concepts and relationships, as well as inferring rules about vulnerabilities, threats, and attacks. This serves as the basis for sharing security knowledge among various agents.
- Based on the inference ability of the security ontology, we propose an efficient and scalable system framework and algorithm to compute a full attack graph.
- Our attack graph model can be easily transformed into a MulVAL attack graph, which supports application of various sophisticated approaches for quantifying attacks risk and developing optimal mitigation plans.
- To clarify discussion, we illustrate the generation of an attack graph with a case study, and the performance of our system is evaluated on test networks of varying sizes and topologies.

The remainder of the paper proceeds in the following manner. Section 2 is a discussion of existing related works. Section 3 presents the design of the architecture. In Section 4, we present the design of an ontological security model. Section 5 describes a scheme for security assessment using semantic reasoning and attack graphs. Section 6 describes performance analysis for attack graph generation on varying networks sizes and topologies. Finally, we outline our conclusions in Section 7.

2. Related works

The issue of information security assessment for enterprise networks has long attracted attention in literature. In the last decade, attack graphs have emerged as a mainstream technique for security analysis on enterprise networks [6].

An attack graph models the interdependencies between network topology, vulnerabilities, and attacks. Various risk metrics can be extracted from attack graphs. Literatures [2,4] constructed the reasoning engine MulVAL, and built an attack graph generation tool based on it. The key idea of MulVAL is the usage of Datalog rules to specify attack techniques and system security semantics. The attack simulation traces computed by the MulVAL reasoning engine are utilized to construct a logical attack graph. Homer et al. [6] presented a model that can be used to produce quantitative security metrics that measure the likelihood of breaches occurring within a given enterprise network. They utilize existing tools [2] for generating attack graphs, and then apply probabilistic reasoning to produce a vulnerability metrics aggregation that is computationally sound and has clear semantics. Poolsappasit et al. [5] proposed a Bayesian network-based risk management framework to quantify the likelihood of attacks on a network using metrics defined in the Common Vulnerability Scoring System (CVSS) [13]. Furthermore, they utilize a genetic algorithm to recommend optimal mitigation plans according to a cost model specified by the user. The structure of Poolsappasit et al.'s Bayesian attack graph is similar to the MulVAL attack graph. NetSecuritas [7] is a security management tool that integrates an open-source scanner, as well as exploit databases and methodologies available in the public domain to facilitate security assessment. It aggregates network and vulnerability information to generate attack graphs for security assessment and mitigation actions.

Although existing graph-based schemes have made significant contributions to enterprise network security analysis , we argue that one major drawback is the lack of a common vocabulary to precisely define and share security knowledge between domain experts and network administrators. The aforementioned proposals generally store attack knowledge and network configurations in Datalog tuples or databases. The relationships of network attack knowledge are concealed within complex data structure definitions. Because of the large volume of information collected from enterprise networks, administrators may find it difficult to effectively model security problems considering their often limited experience with security risk assessment.

Development of a security ontology is one possible solution for this problem, because it allows for a clear and precise definition of all entities and their relationships to each other. The security ontology creates a common, unambiguous semantic language for representing knowledge in the security domain, and serves as a basis for information sharing between people or various other agents [14].

Ontology has many applications in the security domain. Vorobiev et al. [11] argued that collaboration between distributive components is a better way to withstand security attacks. They developed several ontologies including a security attack

Please cite this article as: S. Wu et al., Network security assessment using a semantic reasoning and graph based approach, Computers and Electrical Engineering (2017), http://dx.doi.org/10.1016/j.compeleceng.2017.02.001