International Journal of Digital Crime and Forensics
Volume 15 • Issue 1

Key Node Identification Based on Vulnerability Life Cycle and the Importance of Network Topology

Yuwen Zhu, State Key Laboratory of Mathematical Engineering and Advanced Computing, China*
Lei Yu, Chinese Academy of Sciences, China

ABSTRACT

The key network node identification technology plays an important role in comprehending unknown terrains and rapid action planning in network attack and defense confrontation. The conventional key node identification algorithm only takes one type of relationship into consideration; therefore, it is incapable of representing the characteristics of multiple relationships between nodes. Additionally, it typically disregards the periodic change law of network node vulnerability over time. In order to solve the above problems, this paper proposes a network key node identification method based on the vulnerability life cycle and the significance of the network topology. Based on the CVSS score, this paper proposes the calculation method of the vulnerability life cycle risk value, and identifies the key nodes of the network based on the importance of the network topology. Finally, it demonstrates the effectiveness of the method in the selection of key nodes through network instance analysis.

KEYWORDS

Importance of Topology, Key Network Nodes, Risk Value, Vulnerability Life Cycle

INTRODUCTION

With the highly complex nature of a network structure, the identification of key network nodes is an important method to analyze and master the complex network structure and function. The key nodes of the network refer to the nodes that play a decisive role in the structure and stability of the network. If a defender loses the authority of such nodes in the process of an attack and defense, it will lead to a rapid decline in network performance and even disrupt the connectivity of the entire network structure.

One of the important topics in network scientific research is how one can identify the influence of each node accurately and efficiently in a complex network. At present, network key node identification technology mainly refers to key node identification based on network topology and key node identification based on network node vulnerability.

DOI: 10.4018/IJDCF.317100 *Corresponding Author

However, the existing methods generally measure the influence of nodes from a single angle or a certain aspect, which is not comprehensive enough to consider all the problems. The traditional methods do not consider the aspect of attack and defense and ignore the impact of the network node's vulnerabilities in terms of network security and the difficulty of network attack and defense. Most of the key network nodes are identified by using static methods and the distribution law of the vulnerability utilization probability is not taken into consideration in the time dimension of vulnerability generation.

In order to provide a solution to the aforementioned problems, this paper studies the network key node identification method based on the vulnerability life cycle and the significance of the network topology. The network topology structure and the change of node vulnerability life cycle over time are comprehensively explained, thus dynamically reflect the changes of key network nodes in real-time.

The contributions of this paper are as follows:

- The authors propose a formal description of network key nodes based on vulnerability life cycle.
- The authors propose a calculation method of vulnerability life cycle risk value based on common vulnerability scoring system (CVSS) score.
- The authors propose a method for identifying key network nodes based on the vulnerability life cycle and the importance of network topology.
- The authors designed an example and perform a security analysis on a network abstract model, thereby proving rapid modeling, quantitative calculation, and the final key node identification of the target network.

The rest of this paper is structured as follows. The second section discusses the related work. The third section details the formal description of network key nodes based on the vulnerability life cycle. The fourth section calculates the vulnerability lifecycle risk based on CVSS score. The fifth section proposes the key node identification method based on the vulnerability life cycle and importance of network topology. The sixth section gives an example to illustrate the effectiveness of the method of identification of key network nodes. The seventh section gives a comparison of related work. Finally, the eighth section summarizes the paper and proposes future work.

RELATED WORK

Although a lot of research has been conducted in the fields of vulnerability life cycle, key network nodes, and multi-attribute analysis, a systematic theoretical method has not yet been proposed to incorporate the vulnerability life cycle into the analysis of key network nodes.

The concept of the vulnerability life cycle was first proposed by Arbaugh et al. (2000) of CERT (the Computer Emergency Response Team) in the United States. They analyzed several states that a vulnerability may experience from production to extinction. Combined with the security report issued by the coordination center of CERT, they reported the distribution of a number of vulnerabilities in different states over the years. Frei (200) used system dynamics to model and analyze the vulnerability life cycle, but the dataset used in the experiment was small, and the impact of software vendors was not analyzed. Combined with the open-source OSVDB vulnerability database, Kaaniche et al. (2013) analyzed the distribution of time length of Windows, Unix, and Mobile OS operating system vulnerabilities in different life cycle stages. The results show that the time distribution is related to specific operating system types. Mingqiu et al. (2011) calculated the vulnerability security risk value based on the Mamdani model by quantifying the attack frequency and technology of the time dimension of the vulnerability life cycle.

The most widely used methods for network key node identification based on network topology includes: degree centrality, betweenness centrality, proximity centrality, etc. Although the degree centrality (Freeman, 1977) algorithm is simple and efficient, it does not take the global structure