A Review on Network Attack Graph Technology

Bin-tao YUAN*, Zu-lie PAN and Fan SHI

College of Electronic Engineering, National University of Defense Technology, Hefei, China

*Corresponding author

Keywords: Cyber security, Vulnerabilities, Attack graph, Risk analysis.

Abstract. The computer network has been an essential part of people’s life. However, with the development and popularization of the information technology, various cyber security vulnerabilities have been emerging. Because of the high price of repairing, troublesome hysteresis is inevitable when repairing the vulnerabilities. Furthermore, 0-day vulnerabilities are still unfamiliar to large number of manufacturers. Therefore, researchers come up with the attack graph technology, helping with locating important vulnerabilities and key nodes, to better analyze the state of the cyber security and reduce the strengthening costs. The attack graph technology mainly focuses on helping the administrator with network defense strategies, through making risk analysis in the network by assessing the vulnerable relationship among nodes. The attack generation technology shows the inefficiency of the present technology in application to large-scale network, but we can expect the proper development by combining with the artificial intelligence in the future.

Introduction

With the rapid development of the information technology and the popularization of the network, more and more network attacks focus on the government, enterprises, scientific research institutions and some infrastructures. Means of attacking are constantly changing. Cyber security of governments and enterprises is facing threats. According to the 2017 Report of Cyber Security in China issued by the National Internet Emergency Center(CNCERT/CC) in August, 2018 [1], CNCERT/CC received 103400 reports of cyber security incidents both in domestic and over abroad in 2017. The top three cyber security incidents were vulnerabilities, web page counterfeiting and malware. China National Vulnerability Database (CNVD) has indicated the constantly increasing numbers of network vulnerabilities in recent years [2].

In order to deal with the more and more severe cyber security problems, how to predict the danger and protect the target system or node has become a problem that governments and enterprises must consider when designing cyber security protection strategies. In view of this problem, the attack graph technology emerged. In 1998, PHILLIPS put forward the concept of attack graphs for the first time, which can analyze the external and internal attacks of a network, so as to understand the vulnerability of a particular network [3]. The attack graph is a kind of directed graph which is a graph theory principle to analyze the nodes and the interactive relationship among nodes on the Internet. Furthermore, it intuitively illustrates the possible paths that an attacker used in network attack which provides a basis for making protection strategies. At present, the attack graph technology plays a role in risk assessment, dynamic detection, alarm correlation and even medical field [4,5,6,7].

This paper is organized as follows. In section 1 we introduce the concept and application of attack graph. In section 2 we make classifications on the attack graph. In section 3 we introduce the existing technology and tools to generate the attack graph. In section 4 we introduce making using of custom algorithm to generate attack graph. Finally, we make a conclusion in section 5.

Classifications of the Attack Graph

There are different types of the attack graph while considering the different information it represented according to nodes and edges in it, including first-raised the state-based attack graph and the widely
used attribute-based attack graph. Besides, there are Bayesian attack graph and other different types of attack graph.

**State-based Attack Graph**

SHEYNER first proposed the concept of state-based attack graph [8]. The nodes of the state-based attack graph represent the state information of network, such as the target host, attacker's privileges and vulnerabilities. Directed edge represents the transition of network state because of the atomic attack (Figure 1). Because each node is on behalf of the globe state of the network, the efficiency of generation state-based attack graph is fairly low, and it is difficult to apply to large-scale network.

![Figure 1. state-based attack graph.](image)

**Attribute-based Attack Graph**

The attribute-based attack graph generally contains two types of nodes and two types of edges [9]. The two types of nodes are representative for the atomic attack and the attribute condition respectively. The attribute condition is the condition of the target network and the attacker's privileges. The two types of directed edges respectively refer to the preconditions and the consequences of the atomic attack (figure 2).

![Figure 2. Attribute-based attack graph.](image)

**Attribute-based Attack Graph Development**

Via attribute-based attack graph, developments of two new attack graphs are produced by simplifying the information of nodes. They are penetration dependency attack graph and attribute dependency attack graph.

RITCHEY raised osmotic dependence attack graph, deleting the attribute node while preserving the atomic node only [10]. The simplified attribute-based attack graph unveils the interdependent relationship between atomic attacks.

![Figure 3. Attribute-based attack graph.](image)

AMANN introduced attribute dependency attack graph, remaining attribute nodes and transforming atomic attacks to edges [11]. The Attribute Dependency Attack Graph makes a description about the interdependent relationship of attribute changes after the target network attacked by the atomic attack.

![Figure 4. Attribute-based attack graph.](image)
Bayesian Attack Graph

PEARL introduced Bayesian network in 1988 which is a fairly effective probabilistic model [12]. In order to determine which paths are popular with attackers, Bayesian attack graph came out based on Bayesian network [13]. At present, the Bayesian attack graph is useful in the aspect of calculating the probability of the adoption of each attack path and the probability of network nodes captured. To assign probability figure to the initial node of the network, and the directed edge represents the causal relationship among nodes. The conditional probability of other nodes can be calculated, referring to the probability figure of the initial node and the causal relationship among nodes. FRIGAULT adds temporal aspects to the Bayesian attack graph to dynamically update the probability of vulnerabilities exploited in the attack graph [14].

Other Attack Graphs

RITCHEY proposes a host attack graph in which nodes represent the host and edges represent the highest privileges which refer to the user and the admin between hosts [15]. In 2010, WANG introduced an attack graph technology combining 0-day vulnerabilities [16]. Assuming that all remote services in the network have 0-day vulnerabilities, the cyber security assessment is available based on the minimum number of 0-day vulnerabilities that an attacker exploits to attack the target node.

Existing Technologies and Tools

The existing attack graph generation techniques are mainly based on model checking and logic deduction, and some tools to generate the attack graph automatically [17,18].

Model Checking

Model checking technology (figure 5) uses model checkers to detect all states in the network. Once a security strategy disobeyed, a graph of all possible attacks on the network will be generated, in which the security strategy encodes with CTL (Computation Tree Logic). The main open source tools for model checking are SMV and NuSMV [19,20]. Because of the generation of model checking technology is the state-based attack graph, it tends to get problems like state explosion, etc.

MulVAL

MulVAL (Multi-host Multi-stage Vulnerability Analysis) is a typical logical detection technology, using Datalog rules to describe the network information, such as attacker’s remote elevated privilege and Vulnerability [21]. As shown in Table 1, the first line is the result of attacks, and the rest are conditions.

Table 1. Datalog rule.

```
execCode(Attacker, Host, User) :-
    networkService(Host, Program, Protocol, Port, User),
    vulExists(Host, Vuld, Program, remoteExploit, privEscalation),
    netAccess(Attacker, Host, Protocol, Port).
```

The MuVAL model (figure 6) shows the reasoning engine of MulVAL is based on the XSB, which records all the rules that do not meet the security strategy, and synthesizes the logical attack graph through the graph builder [22].

TVA and Cauldron

TVA (Topological Vulnerability Analysis) is a tool to automatically analyze the vulnerabilities in the network to generate the attack graph [23]. It provides a monotonic assumption about attacks, “The set
of atomic attacks that an attacker initiate will not decrease with new atomic attacks interpreting”, so it has a better scalability and will short the scale of attack graph to a polynomial level.

Cauldron is a commercial cyber security analysis tool based on TVA, automatically analyzing all potential attack paths of a network, from the network to the application level [24]. It absorbs vulnerability data from scanners, aggregating and correlating that data with vulnerability databases.

**NetSPA and FireMon**

Lincoln Laboratory of MIT innovates NetSPA (A Network Security Planning Architecture) in 2008 [25]. Via the result of Nessus scanning, the tool gets the vulnerability information of the host, and then extracts the vulnerability in NVD (national vulnerability database) to generate the attack graph [26]. The attack graph generated by the NetSPA system is a multiple-prerequisite attack graph to demonstrates the potential path for an opponent to embark an attack with the help of known vulnerabilities. FireMon is the commercial version of network security manager platform tool NetSPA [27].

Except for the classical tools mentioned above, researchers have innovated new tools in recent years, such as Naggen and A2G2V [28,29]. For a brief summary and comparison of the classic techniques and tools described above, referring to Table 2, where H in complexity is on behalf of the number of hosts in the network.

<table>
<thead>
<tr>
<th>Tools</th>
<th>Open source</th>
<th>Accessible</th>
<th>complexity</th>
</tr>
</thead>
<tbody>
<tr>
<td>NuSMV</td>
<td>Yes</td>
<td>Free</td>
<td>exponential</td>
</tr>
<tr>
<td>MuVAL</td>
<td>Yes</td>
<td>Free</td>
<td>$O(</td>
</tr>
<tr>
<td>TVA</td>
<td>No</td>
<td>Not open</td>
<td>$O(</td>
</tr>
<tr>
<td>Cauldron</td>
<td>Commercial</td>
<td>Pay</td>
<td>$O(</td>
</tr>
<tr>
<td>NetSPA</td>
<td>No</td>
<td>Not open</td>
<td>$O(Hlg H)$</td>
</tr>
<tr>
<td>FireMon</td>
<td>Commercial</td>
<td>Pay</td>
<td>$O(Hlg H)$</td>
</tr>
</tbody>
</table>

**The Algorithms of Customized Attack Graph Generation**

The purpose of the algorithms of customized attack graph generation is to optimize the efficiency of the attack graph generation for specific scenarios and to narrow the scale of attack graph generation. BAO proposes an attack graph backward search algorithm [30]. The main idea of the algorithm is to backward search all the attacks related to the target from the attack target and generate attribute-based attack graph. The time complexity is between $O(|H|^2)$ and $O(|H|^3)$.

A specially designed search algorithm from artificial intelligence technology by GHOSH, called Planner, is used to generate attack graphs in order to alleviate the effects of the scalability problem [31]. KAYNAR introduces a parallel and distributed memory-based algorithm that builds attack graphs with vulnerabilities on a distributed multi-agent platform [32]. POLATIDIS presents an algorithm that builds attack graphs, using data supplied from the infrastructure [33]. The algorithm...
delivers all possible paths that can be exploited to access. Then, a recommendation system is utilized to make predictions about future attack steps in the network.

**Conclusion**

Starting with the birth and application of the attack graph, this paper introduces the main attack graph classification, classical or recent attack graph generation technology and tools, cyber security measurements and the defense technology by using attack graph. So far, the attack graph technology still faces many problems and challenges: with the constantly increasing number of Internet users and the expanding scales, although there are many technologies such as the proposal of distributed attack graph generation, there is not a particularly efficient algorithm production; vulnerability information in attack graph is an important indicator. Although there are some available vulnerabilities information in common vulnerability scoring system (CVSS) of NVD, the detailed vulnerability information is extracted manually by researchers, and the evaluation of vulnerability in CVSS is only divided into high, middle and low three levels, which is not specific and qualified enough. A closed-circle problem may occur in the process of generating an attack graph, and dealing with the closed-circle problem is a key challenge to the attack graph technology.

Since it was issued in 1998, the attack graph technology has been developing for 20 years with new technologies emerging, and it removes from the academic field to the industrial field. At present, the attack graph technology still needs more human resources. With the rapid development of the artificial intelligence technology, it will be an interesting research direction to combine artificial intelligence with the attack graph technology. The attack graph generation and analysis technology, which is highly automatic and intelligent, will be widely made use of in the future.

**References**


[26] NVD( national vulnerability database) on https://nvd.nist.gov/


