Statistical Analysis of The Privilege Level of Vulnerability

Junmin Chen[1,2,a], Zhihong Tian[3, 4,b]

[1]Key Laboratory of Trustworthy Distributed Computing and Service (BUPT), Ministry of Education

Beijing, China

[2]School of Computer Science, BUPT, Beijing, China

[3]School of Computer Science and Technology, Harbin Institute of Technology Haerbin 150001, China

Haerbin 150001, China

[4]Beijing HIT Computer Network and Information Security Technology Research Center

Beijing, China

[a]cjmmjc7@gmail.com, [b] tianzhihong@hit.edu.cn

Abstract.

This paper gives a brief but comprehensive introduction of condition of attack state and how we analysis it from massive xml file. Multi-attribute-based classification method supports mining privilege level of vulnerability. Owing to associated analysis, it combined directly and indirectly of vulnerability threats which makes evaluation more convinced. Meanwhile, the method offers guidance and assistance to the vulnerability smart identification, multi-level quantitative attributes on the thin side vulnerabilities, and also highlights the impact of the vulnerability of the security attributes of system confidentiality and availability, etc. It is of significant importance for the further detection, description, evaluation of vulnerability.

Keywords: network security, vulnerability

Introduction

With the rapid development of information networks, attack techniques are varied and mutated against their original appearance, we ushered uninvited guests like denial of service, scanning probe, malicious software, and disguised spoofing attacks. When assessing the effect of attack techniques, the research values more on the field of its effects and capability in network environment. It will help improve the defense capabilities of network devices also the security class of information system. To establish a network attack effect evaluation model, the first thing to be analyzed is the quantities of typical attacks, then extracting the basic network attack effect.

What’s vulnerability? Wikipedia defines vulnerability as “a weakness which allows an attacker to reduce a system's information assurance in computer security”. Vulnerability is the intersection of three elements: a system susceptibility or flaw, attacker access to the flaw, and attacker capability to exploit the flaw. To exploit a vulnerability, an attacker must have at least one applicable tool or technique that can connect to a system weakness. In this frame, vulnerability is also known as the attack surface.

Vulnerability are uncovered constantly. This happens in part because of the un-bug-free characteristic of our software components, and unfortunately the programmer is unconscious of how fragile their masterpiece are. Besides, hackers have access to more and more resources thus gives a chance for attackers take advantages of vulnerabilities to exploit hosts, databases, your individual privacy.

The composition of vulnerabilities in attack scenarios can be traditionally performed based on detailed pre and post-conditions. Despite very precise, this approach relies on human analysis, that is time consuming and sometimes not much scalable. We investigate the NIST National Vulnerability Database (NVD) for three purpose:

Analysis association among vulnerability attributes connected to impact, privilege, exploitability, type of vulnerability and clues derived from natural linguistic description.

Model an assessing prototype.

Normalize the pre and post-condition of majority vulnerabilities.

Modeling network vulnerability using model checkers

To model the vulnerability of computer networks like showed in Fig. 1 and Fig. 2, in the research community, the initial approach was using model checking techniques. A model checker could assist engineers to identify individual design flaws in a model of a system. Using model checkers, the researchers could get away of custom special purpose tools for attack graph generation. To check if the system has a bug or side effect, the model is completed looked after whether it meets a correctness specification.

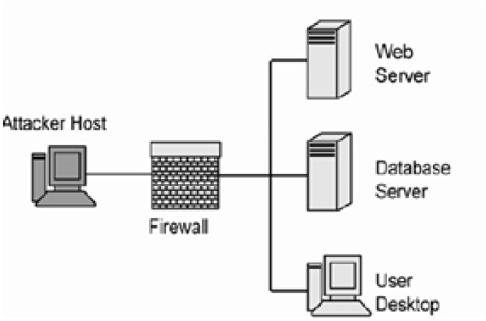

Fig. 1 Example of a simple network

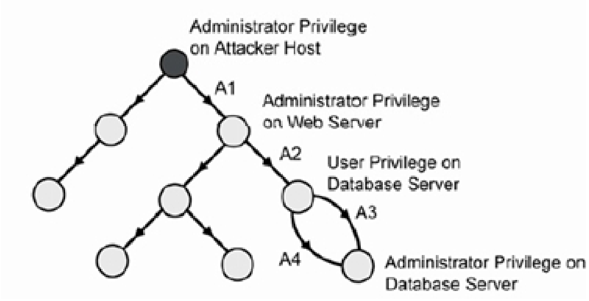

Fig. 2 shows a part of its attack graph. Each node in the attack graph stands for a state of the network or attacker; arcs represent exploits or attacks; and the attacker host is the black one.

The model is a state staff defined by variables, initial values for the variables and a description of the 15 conditions under which variables may change value. When the variables change value they cause a state transition. The sum of all possible states of a state machine is the state space. The model can be automatically checked by a model checker against a correctness specification if the model has any flaws. The correctness specifications are expressed in propositional temporal logic. The model checker performs an exhaustive search through the state space to determine that each state satisfies the correctness specification. If the correctness specification is not satisfied, the model checker will give a counterexample execution, showing the sequence of states that lead to the violation of the correctness specification.

Conditions

We build the prototype of privilege by a given set: {user, admin, DoS, obtainCred, runCode}. The value in this set is given by the level of violation on the CIA of information security from the illegal privilege level. Preconditions specify required privilege to launch attack actions, while the post-conditions show capabilities an attacker gains after exploiting vulnerabilities successfully. So we classify pre-condition by CIA vector, while post-condition the description tag.

Pre-condition. Formed of three metric groups: base, temporal, and environmental metrics, the CVSS has a numerical score and a text vector that indicates the severity of the vulnerability, and the way in which it was calculated. The vector maps the tag vector like (AV:N/AC:L/Au:N/C:P/I:N/A:N) in NVD XML files is a key to initialized our accessing model.

The result of CIA value for permutation and combination is 27 groups, we re-group them into 9 sets showed as Table 1.

Table 1.Group of CIA value

CIA impact	NVD attributes configuration
Complete CIA	<C:C/I:C/A:C>
Partial CIA	<C:N/I:N/A:N>
No CIA	<C:N/I:N/A:N>
Only-C	<C:C/I:N/A:N>, <C:P/I:N/A:N>
Only-I	<C:N/I:C/A:N>, <C:N/I:P/A:N>
Only-A	<C:N/I:N/A:C>, <C:N/I:N/A:P>
C & I	<C:C/I:C/A:N>, <C:P/I:C/A:N><C:P/I:P/A:N>, <C:P/I:P/A:N>
A & C	<C:C/I:N/A:C>, <C:P/I:N/A:C><C:P/I:N/A:P>, <C:C/I:N/A:P>
A & I	<C:N/I:C/A:P>, <C:N/I:C/A:C><C:N/I:P/A:C>, <C:N/I:P/A:P>

Through a large amount of data analysis and calculation, we cover some rules which can help us figure out privilege:

1. We found that there is a strong correlation between CIA impact level <C:N/I:N/A:C> and DoS. NVD database shows that all vulnerabilities with that CIA value pointed to a set of vulnerabilities whose description includes DoS effect.
2. <C:C/I:C/A:C> related to privilege level “admin”.
3. Especially, a vulnerability is classified with post-condition privilege level categories “user”, “admin”, “DoS” when find alike key word in its description instead of CIA impact.
4. When analyzing the description, we discovered two privilege levels “read credentials” and “change firewall rules”, their impact in the attack graph is serious since they give remote attacks a privilege escalation. So we assign the post-condition of these two as admin level.
5. Moreover, it also does impact heavily on availability (A in CIA vector), and 93.2% of only-A CVEs cause DoS effect.
6. runCode impoact CIA completely or partially(majority). So we set effect partial CIA as the runCode.

Only-C CVEs was group to no privilege. In fact, these are easily exploitable, with attributes like reqire network access, low complexity and no authentication, so we put only-C into remote sections.

1. We found that there is a strong correlation between CIA impact level <C:N/I:N/A:C> and DoS. NVD database shows that all vulnerabilities with that CIA value pointed to a set of vulnerabilities whose description includes DoS effect.
2. <C:C/I:C/A:C> related to privilege level “admin”.
3. Especially, a vulnerability is classified with post-condition privilege level categories “user”, “admin”, “DoS” when find alike key word in its description instead of CIA impact.
4. When analyzing the description, we discovered two privilege levels “read credentials” and “change firewall rules”, their impact in the attack graph is serious since they give remote attacks a privilege escalation. So we assign the post-condition of these two as admin level.
5. Moreover, it also does impact heavily on availability (A in CIA vector), and 93.2% of only-A CVEs cause DoS effect.
6. runCode impact CIA completely or partially(majority). So we set effect partial CIA as the runCode.

Post-condition. If a CVE number is not given, the classifier takes only the text description with categorical values provided by Nessus. In this situation, the classifier also pick categorical database fields from the NVD database when they are available same as text descriptions from the CVE dictionary. Make the best of both worlds, we choose to analysis linguistic text- the description. Phrases showed below are collected into parts for each privilege level:

1. The admin privilege category can be concluded by phrases including “gain system privileges”, “gain root”, “gain access to root”, etc.
2. DoS attacks may disable a service but cannot gain access. The description of attack DoS is usually composed of “denial of service”.
3. “Intercept transmission”, “intercept communication”, “obtain plain text”, “obtain clear text”, “read network traffic”, “unencrypted”, “sniff” are attack effect obtainCred’s common phrases.
4. Groups like “read”, “include”, “list” and “download” are pointed to gain confidential attacks, which could re-classify to obtainCred. And also “bypass access authentication” and “bypass authentication”.
5. Level runCode shows the ability of executing programs. Phrases like “execute arbitrary code”, “execute arbitrary programs” and so on.
6. Phrases like “modify”, “write”, “overwrite”, “upload” maps malicious actions, we remap them as runCode.

Summary

The two pictures blow shows the data distribution of each privilege level in two views: effect and impact.

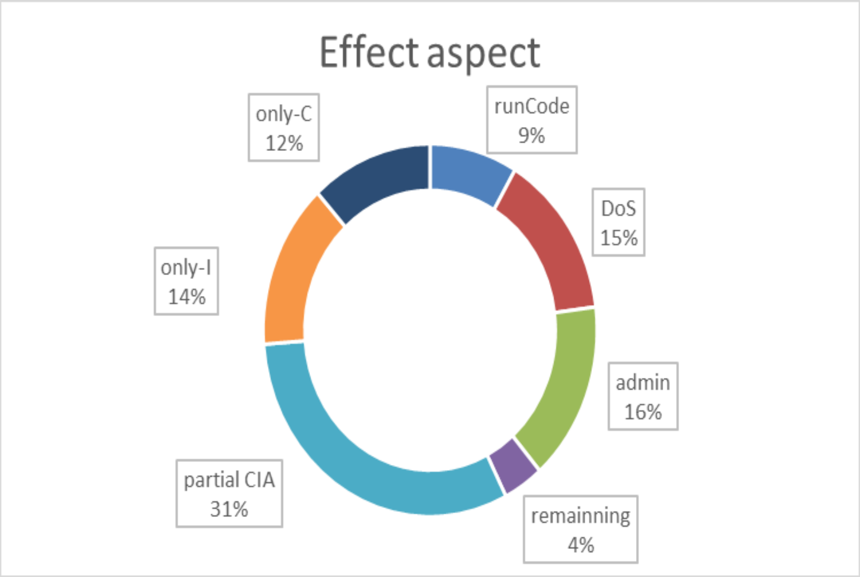

Fig.3 Effect Aspect Percentage

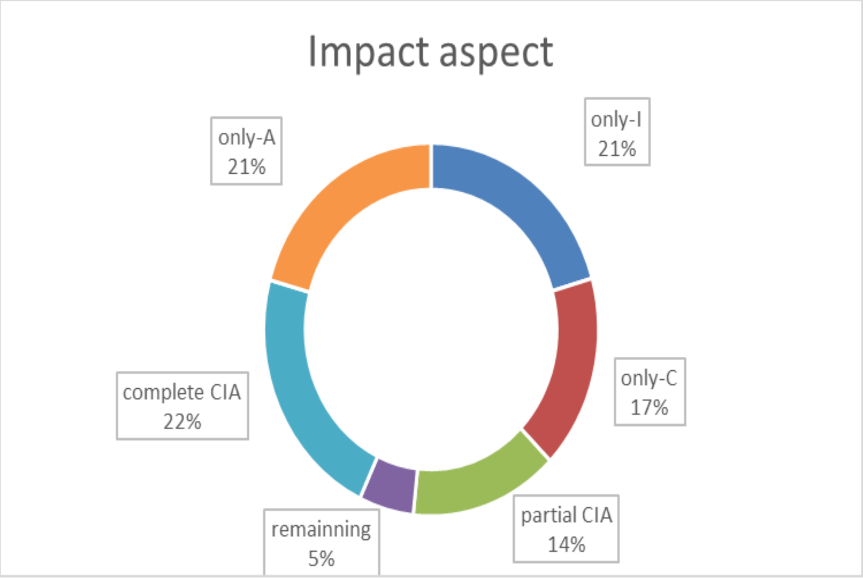

Fig. 4 Impact Aspect Percentage

References

[1] NVD: (National Vulnerability Database v2) http://nvd.nist.gov.

[2] Weka: (Data mining software) http://www.cs.waikato.ac.nz/ml/weka/

[3] Kap G, Ali D. Statistical Analysis of Computer Network[D]. KTH University, October 7, 2013.

[4] Lippmann, R.P., Ingols, K.W., Scott, C., Piwowarski, K., Kratkiewicz, K.J., Artz, M., Cunningham, R.K. : Evaluating and Strengthening Enterprise Network Security Using Attack Graphs. Technical Report ESC-TR-2005-064, Masschusetts Institute of Technology, Lincoln Laboratory, Masschusetts, USA (2005)

[5] Franqueira V N, Keulen M V. Analysis of the NIST database towards the composition of vulnerabilities in attack scenarios[D]. Enschede, The Netherlands:University of Twente, 2008.

[6] Hu Ying, Zheng Kangfeng, Yang Yixian. Mining network attacks effect with NVD vulnerability database[J]. computer sicence, 2008, 01(35N9． 3):55-57.