Exploiting & Ranking Vulnerabilities in Computer Network

Akshay Aparadh, Nikhil Adap, Ninad Bodke, Pranav Ambre

Abstract— A network security metric is desirable in evaluating the effectiveness of security solutions in distributed systems. Aggregating CVSS scores of individual vulnerabilities provides a practical approach to network security metric. However, existing approaches to aggregating CVSS scores usually cause useful semantics of individual scores to be lost in the aggregated result. In this paper, we address this issues through novel security metrics. In this project we have defined some Attack graph and CVSS-based security metrics that can help us to prioritize vulnerabilities in the network by measuring the probability of exploiting them and also the amount of damage they will impose on the network. Proposed security metrics are defined by considering interaction between all vulnerabilities of the network. So our method can rank vulnerabilities based on the network they exist in. Results of applying these security metrics on one well-known network example are also demonstrates effectiveness of our approach.

Index Terms— ***Network hardening, Vulnerability, Exploit, CVSS, Attack Graph, Security Metric***

1 Introduction

Today's critical infrastructures and enterprises are increasingly dependant on the reliable functioning of distributed systems. In securing such systems, a network security metric is desirable since you cannot improve what you cannot measure. By applying a security metric immediately before, and after, deploying security solutions, we can judge those solutions' relative effectiveness in a direct and precise manner. Such a capability will make securing networks a science, rather than an art. The Common Vulnerability Scoring System (CVSS) is a widely adopted standard [10], which allows security analysts and vendors to assign numerical scores to vulnerabilities based on their relative severity. CVSS scores of known vulnerabilities are already available through public vulnerability databases. CVSS thus provides a practical foundation for developing network security metrics. On the other hand, CVSS is mainly intended for ranking individual vulnerabilities. It does not directly provide a way for aggregating individual scores into an overall metric of network security. Naive ways for aggregating scores (e.g., taking the average or maximum value) usually lead to misleading results, whereas existing attack graph-based approaches can achieve improved results.

In this paper we have proposed some CVSS and Attack graph based security metrics for ranking and prioritizing vulnerabilities in the network based on their danger for the network by considering their relationship with other vulnerabilities. Proposed security metrics can provide us with below benefits:

• We can measure the probability of appearing each multi-step attack in the network.
• The danger of multi-step attacks or their effects on security parameters of the network (Confidentiality, Integrity and Availability) can be calculated.
• Vulnerabilities can be scored based on each network they exist in.
• We can prioritize vulnerabilities based on their calculated danger and choose the most perilous vulnerabilities for patching.

Features:

1. Creating a vitrualized network.
2. Detection of Vulnerablities.
3. Generating an Attack Graph.
4. Ranking & Scoring of vulnerabilities.

2 Procedure for Paper Submission

2.1 Review Stage

Detailed submission guidelines can be found on the author resources Web pages. Author resource guidelines are specific to each journal, so please be sure to refer to the correct journal when seeking information. All authors are responsible for understanding these guidelines before submitting their manuscript. For further information on both submission guidelines, authors are strongly encouraged to refer to http://www.ijser.org.

2.2 Final Stage

For papers accepted for publication, it is essential that the electronic version of the manuscript and artwork match the hardcopy exactly! The quality and accuracy of the content of the electronic material submitted is crucial since the content is not recreated, but rather converted into the final published version.

All papers in IJSER Transactions are edited electronically. A final submission materials check list, transmission and compression information, and general publication materials can be found at: http://www.ijser.org.

2.3 Figures

All tables and figures will be processed as images. You need to embed the images in the paper itself. Please don't send the images as separate files.

2.4 Copyright Form

For any questions about initial or final submission requirements, please contact one of our staff members. Contact information can be found at: http://www.ijser.org.

3 Sections

As demonstrated in this document, the numbering for sections upper case Arabic numerals, then upper case Arabic numerals, separated by periods. Initial paragraphs after the section title are not indented. Only the initial, introductory paragraph has a drop cap.

4 Citations

IJSER style is to not citations in individual brackets, followed by a comma, e.g. "[1], [5]" (as opposed to the more common "[1, 5]" form.) Citation ranges should be formatted as follows: [1], [2], [3], [4] (as opposed to [1]-[4], which is not IJSER style). When citing a section in a book, please give the relevant page numbers [2]. In sentences, refer simply to the reference number, as in [3]. Do not use "Ref. [3]" or "reference [3]" At the beginning of a sentence use the author names instead of "Reference [3]," e.g., "Smith and Smith [3] show ... ." Please note that references will be formatted by IJSER production staff in the same order provided by the author.

5 Equations

In order to help improving the above problems with two mentioned security metrics, we defined below security metrics for assessing the probability of exploiting vulnerabilities in the network.

For solving the problem with the Number of attack paths metric, we defined new metric named weighted number of attack paths as (3). As we described before, Exploitability Score of CVSS determines the exploitability level that is needed for the attacker to exploit the vulnerability so, the more this parameter higher the probability of exploiting it. Therefore we can define the probability of exploiting each individual vulnerability as (1). Division by 10 is because of the maximum value of exploitability in CVSS is 10.

$$Probability(Vul_K) = \frac{Exp(Vul_K)}{10}$$

In (1), Exp(VulK) is the Exploitability Score of CVSS for individual vulnerability VulK. By using this parameter, we defined the probability of each attack path in (2).On the other hand, this probability is computed by multiplying its involved individual vulnera-

$$Probability(AP_i) = \prod_{k=1}^{Attack\ Path_i\ length} \frac{Exp(Vul_K)}{10} \quad (2)$$

As we said the main problem with the Number of Attack Paths security metric is that, it ignores the difficulty degree of exploiting vulnerabilities. So using (2), ... nber of

$$WNAP(Vul_i) = \sum_{j=1}^{Number\ Of\ Attack\ Paths} Probability(AP_j) \quad (3)$$

Now the aim is to find the probability of exploiting each vulnerability. As more than one attack path can enable the attacker to exploit each individual vulnerability, we can claim relation in (4). We can say (4) is true because, for each vulnerability, the shorter the length of the shortest path and the higher the number of shortest paths, it is more probable to be exploited by the attacker.

$$Prob_{Vul_i} \propto \frac{Number\ of\ Shortest\ Paths}{Shortest\ Path\ Length} \quad (4)$$

Relation in (3) is a good means to improve the idea of using number of attack paths security metric for security evaluation. Number of attack paths is a good metric but, in one network, there may be vulnerabilities with the highest number of attack paths but, these attack paths are so long that cannot be exploited by the attacker. So in this paper instead of using number of attack paths metric we used percentage of number of shortest paths that is defined in (5) as another indicator of the simplicity degree of exploiting each vulnerability beside (3).

$$NSP\ Percentage = \frac{Number\ of\ Shortest\ Paths}{Number\ of\ Attack\ Paths} \quad (5)$$

Now based on (3), (4) we can propose a security metric for measuring the probability of exploiting each vulnerability in the network. This security metric is ...ge ...l-

$$\overline{WNAP(Vul_i)} = \frac{WNAP(Vul_i)}{Number\ Of\ Attack\ Paths} \quad (6)$$

$$Prob_{Vul_i} = \overline{WNAP(Vul_i)} \times \frac{NSP\ Percentage}{Shortest\ Path\ Length} \quad (7)$$

Now we introduce our proposed security metric for measuring the danger degree of each multi-step attack in the network. As we said CVSS contains a parameter called Impact that for each individual vulnerability, can calculate the impact of attack occurring on security parameters of the network. So for each attack path, we should define a danger degree that can estimate the overall impact of attack path exploiting on security parameters of the network. We found this Impact estimation by (8).

$$Impact_{AP_i} = \frac{\sum_{j=1}^{Attack\ Path\ length} Impact_{Vul_j}}{Attack\ Path\ length} \quad (8)$$

As we said more than one attack path may exist in the network that can enable the attacker to exploit each vulnerability. On the other hand, for defining security metrics, we had a simple assumption that, only one attacker exists in the network by the aim of attacking one special goal in the network. Note that one attacker can traverse only one path at the same time. So for estimating the damage of exploiting each vulnerability in the network, we defined security metric in (9). Among all the attack paths that help the attacker to reach his goal, security metric in (9), specifies the attack path with the highest as indication of damage degree.

$$Impact_{vul_i} = \max\left(Impact_{AP_k}\right)_{k=1,2,\ldots\ldots Number\ of\ Attack\ Paths} \quad (9)$$

Now we can prioritize vulnerabilities in the network by calculating (10) for them.

$$Emergency\ Degree_{vul_i} = Prob_{Vul_i} \times Impact_{vul_i} \quad (10)$$

By applying (10) on the attack graph of each network, the most emergent vulnerabilities for elimination can be found. Because by doing that, we can find the most probable and dangerous vulnerabilities in the network.

6 Helpful Hints

6.1 Figures and Tables

Because IJSER staff will do the final formatting of your paper, some figures may have to be moved from where they appeared in the original submission. Figures and tables should be sized as they are to appear in print. Figures or tables not correctly sized will be returned to the author for reformatting.

Detailed information about the creation and submission of images for articles can be found at: http://www.ijser.org. We strongly encourage authors to carefully review the material posted here to avoid problems with incorrect files or poorly formatted graphics.

Place figure captions below the figures; place table titles above the tables. If your figure has two parts, include the labels "(a)" and "(b)" as part of the artwork. Please verify that the figures and tables you mention in the text actually exist. Figures and tables should be called out in the order they are to appear in the paper. For example, avoid referring to figure "8" in the first paragraph of the article unless figure 8 will again be referred to after the reference to figure 7. **Please do not include figure captions as part of the figure. Do not put captions in "text boxes" linked to the figures. Do not put borders around the outside of your figures.** Per IJSER, please use the abbreviation "Fig." even at the beginning of a sentence. Do not abbreviate "Table." Tables are numbered numerically.

Figures may only appear in color for certain journals. Please verify with IJSER that the journal you are submitting to does indeed accept color before submitting final materials. **Do not use color unless it is necessary for the proper interpretation of your figures.**

Figures (graphs, charts, drawing or tables) should be named fig1.eps, fig2.ps, etc. If your figure has multiple parts, please submit as a single figure. Please do not give them descriptive names. Author photograph files should be named after the author's LAST name. Please avoid naming files with the author's first name or an abbreviated version of either name to avoid confusion. If a graphic is to appear in print as black and white, it should be saved and submitted as a black and white file (grayscale or bitmap.) If a graphic is to appear in color, it should be submitted as an RGB color file.

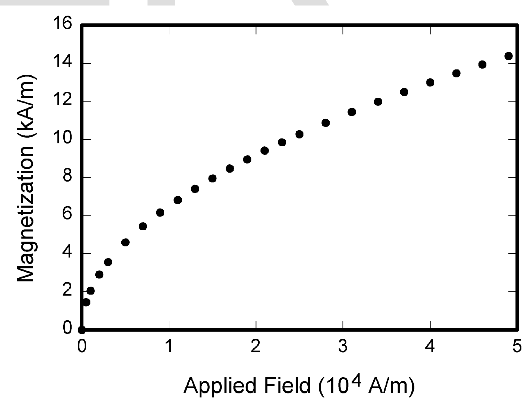

Fig. 1. Magnetization as a function of applied field. Note that "Fig." is abbreviated. There is a period after the figure number, followed by one space. It is good practice to briefly explain the significance of the figure in the caption.

Figure axis labels are often a source of confusion. Use words rather than symbols. As an example, write the quantity "Magnetization," or "Magnetization M," not just "M." Put units in parentheses. Do not label axes only with units. As in Fig. 1, for example, write "Magnetization (A/m)" or "Magnetization ($A \cdot m^{-1}$)," not just "A/m." Do not label axes with a ratio of quantities and units. For example, write "Temperature (K)," not "Temperature/K." Table 1 shows some examples of

ISSN 2229-5518

units of measure.

Multipliers can be especially confusing. Write “Magnetization (kA/m)” or “Magnetization (103 A/m).” Do not write “Magnetization (A/m) × 1,000” because the reader would not know whether the top axis label in Fig. 1 meant 16,000 A/m or 0.016 A/m. Figure labels should be legible, approximately 8 to 12 point type. When creating your graphics, especially in complex graphs and charts, please ensure that line weights are thick enough that when reproduced at print size, they will still be legible. We suggest at least 1 point.

6.3 Footnotes

Number footnotes separately in superscripts (Insert | Footnote)1. Place the actual footnote at the bottom of the column in which it is cited; do not put footnotes in the reference list (endnotes). Use letters for table footnotes (see Table 1). Please do not include footnotes in the abstract and avoid using a footnote in the first column of the article. This will cause it to appear of the affiliation box, making the layout look confusing.

6.4 Lists

The IJSER style is to create displayed lists if the number of items in the list is longer than three. For example, within the text lists would appear 1) using a number, 2) followed by a close parenthesis. However, longer lists will be formatted so that:

1. Items will be set outside of the paragraphs.
2. Items will be punctuated as sentences where it is appropriate.
3. Items will be numbered, followed by a period.

6.5 Theorems and Proofs

7 End Sections

7.1 Appendices

Network Hardening:

Network hardening is usually the process of securing a system by reducing its surface of vulnerability.

FreeBSD:

Free Berkeley Software Distribution.

GNU:

GeneralPublicLicense.

7.2 Acknowledgments

The preferred spelling of the word “acknowledgment” in American English is without an “e” after the “g.” Use the singular heading even if you have many acknowledgments. Avoid expressions such as “One of us (S.B.A.) would like to thank ... .” Instead, write “F. A. Author thanks ... .” Sponsor and financial support acknowledgments are included in the acknowledgment section. For example: This work was supported in part by the US Department of Commerce under Grant BS123456 (sponsor and financial support acknowledgment goes here). Researchers that contributed information or assistance to the article should also be acknowledged in this section.

7.3 References

7.3 Additional Formatting and Style Resources

Additional information on formatting and style issues can be obtained in the IJSER Style Guide, which is posted online at: http://www.ijser.org/. Click on the appropriate topic under the Special Sections link.

4 Conclusion

THE ATTACKS ON THE VIRTUAL NETWORK HAVE BEEN CARRIED OUT SUCCESSFULLY. THE ATTACK GRAPH REPRESENTING THE FLOW AND RESULTS OF ATTACKS IS DISPLAYED MANUALLY. THE NUMBER OF ATTACKS CARRIED OUT HELPS IN RANKING THE VULNERABILITIES BY USING THE FORMULA COUNTER=COMPLEXITY*SEVERITY.

Acknowledgment

The authors wish to thank A, B, C. This work was supported in part by a grant from XYZ.

References

[1] Chunlu Wang, Yu Bao, Xuesen Liang, Tianle Zhang,” Vulnerability Evaluating based on attack graph”, International Conference, ISCTCS 2012,2012, pp 555-563.
[2] Feng, Chen, and Su Jin-Shu. "A Flexible Approach to Measuring Network Security Using Attack Graphs."International Symposium on Electronic Commerce and Security.IEEE Computer Society, 2008.426--431.
[3] Sheyner, Oleg Mikhail. “Scenario Graphs and Attack Graphs.”PhD Thesis Submitted to School of Computer Science, Computer Science Department, Carnegie Mellon University, 2007.
[4] Sheyner, O., Wing, J.: Tools for Generating and Analyzing Attack Graphs. In: Proc. ofWorkshop on Formal Methods for Comp. and Objects, pp. 344–371 (2004).
[5] A. Jaquith, “Security Metrics: Replacing Fear, Uncertainty, and Doubt”, Addison Wesley Publication, 2007.
[6] S.Wang, Z.Zhang, Y Kadobayashi, “Exploring attack graph for cost benefit security hardening: A probabilistic approach”, Computers & Security, Vol. 32, No. 0. 2013, pp. 158-169,2013.
[7] Albanese, M., Jajodia, S., & Noel, S. (2012). Time efficient and cost effective network hardening using attack graphs.In Proc. of IEEE/IFIP International Conference on Dependable Systems and Network.
[8] Chen, Feng, Dehui Liu, and Jinshu Su Yi Zhang. "A Scalable Approach to Analyzing Network Security using

ISSN 2229-5518

Compact Attack Graphs." Journal of Networks (Journal of Networks) 5 (2010): 543-550.
[9] M. Keramati, A.Akbari, "An attack graph based metric for security evaluation of computer networks", 6'th