SCIENCE CHINA
Information Sciences

• LETTER •

December 2021, Vol. 64 229304:1–229304:2
https://doi.org/10.1007/s11432-020-3008-1

A comprehensive evaluation of diversity systems based on mimic defense

Qing TONG & Yunfei GUO*

National Digital Switching System Engineering and Technological R&D Center, Zhengzhou 450002*, China*

Received 26 February 2020/Revised 22 April 2020/Accepted 21 July 2020/Published online 9 November 2021

Citation Tong Q, Guo Y F. A comprehensive evaluation of diversity systems based on mimic defense. Sci China Inf Sci, 2021, 64(12): 229304, https://doi.org/10.1007/s11432-020-3008-1

Dear editor,

Diversity systems increase attacking challenges through mechanisms such as system diversification design, redundancy, or dynamic rotation. They resist various external threats, including the unknown attacks on the system. Several research studies have been conducted to analyze and validate the security and effectiveness of diversity systems, which are classified into three categories: theoretical analysis [1], simulation analysis [2], and experimental evaluation [3]. Although previous research studies have been proposed, they focus only on whether the software diversity can provide security and how to improve the security of diversity systems. Only a few studies discuss the differences between the various types of diversity technologies. In this study, we propose a diversity system evaluation method based on the attack and defense experiment.

Diversity systems classification. Here, we classify the diversity systems into spatial, temporal, and hybrid diversity systems.

The temporal diversity systems are those that rotate different executors or attributes over time, making the systems behave differently in some aspects or present different attributes in each period. The difference is shown over time; therefore, we refer to this type of diversity as temporal diversity. For example, the MTD systems [4], which dynamically change the attack surface and show different characteristics in different periods, are typical temporal diversity systems.

The spatial diversity systems make use of multiple executions at the same time for one request and vote on the results of the multiple executions to get a final output. As different executions exist at the same time, we refer to this type of diversity as spatial diversity. Typical representatives of spatial diversity systems are voting-based heterogeneous redundant systems, such as the SITAR [5].

The hybrid diversity system incorporates both spatial and temporal diversity features. It is first used in the design of mimic defense dynamic heterogeneous redundancy (DHR) architecture [6] based on our knowledge. As shown in Figure 3 of [7], the system is implemented based on the DHR architecture votes on the outputs of the redundant executors. Also, it uses a dynamic selecting algorithm to change the composition of the online executors over time. The system is transformed into a temporal diversity system if there is only one executor online. When the dynamic selecting algorithm is not used, the system is transformed into a spatial diversity system, which relies solely on redundant executions and voting. The system is transformed into a static and single-node normal system when both kinds of diversity are not available.

Owing to the flexibility of the DHR architecture, we propose different diversity systems for experimental evaluation based on the DHR and deploy the same web service on each system. The essential components of these web server systems include a proxy and several executors. For the temporal diversity web server system, which is abbreviated as D-S, only one executor is working online in each time while the proxy rotates other executors to replace the online executor in turn. For the spatial diversity web server system, which is abbreviated as R-S, the proxy copies the request from the client and dispatches the requests to different executors simultaneously. Each executor processes the same request and sends the response back to the proxy. Then, the proxy votes on the responses and sends the final response back to the client. In the hybrid strategy diversity system, which is abbreviated as H-S, there are two sets of executors, including the online and offline executors. The H-S runs as an R-S basically, except that executors online will be replaced with the executors in the offline set, based on the rotating strategy.

Indicators. Compared with the traditional single-node static system, the diversity system has both redundant and dynamic characteristics. We propose the attack step length and attack tolerant ability as the security indicators.

The interaction between an attacker and a system is considered as an attack step. When a specific attack succeeds, the accumulated minimum number of attack step is the attack step length, which is denoted as AL. The ability of diversity systems to survive attacks is regarded as attack tolerant ability, which is represented as AT. Assuming that the total test time is T and the total surviving time of the system is t_{survive}, then $\text{AT} = t_{\text{survive}}/T$.

* Corresponding author (email: gyf@ndsc.com.cn)

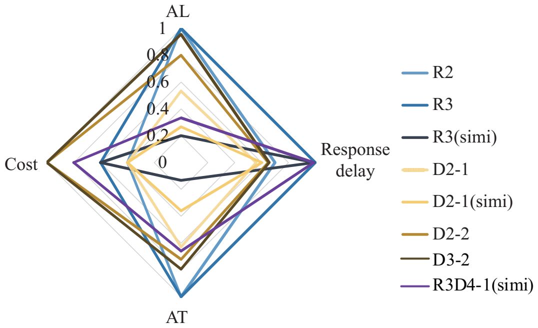

Figure 1 (Color online) The comprehensive comparison of AL, AT, response delay, and cost for the tested systems.

Furthermore, we also quantify the diversity of executors and running costs. The diversity value of executors suggests the differences in the executor set. Inspired by the Shannon-Wiener index [8], the diversity of executors is calculated as diversity $= -\sum_{i=1}^{n} p_i \log p_i / \log n$, for an executor set composed of n executors. As for the cost, we focus on the runtime cost C_{flow} in the evaluation. C_{flow} can be calculated as $C_{\text{flow}} = \int_{t=0}^{T} f(t) \cdot c_{\text{mov}} + \int_{t=0}^{T} r(t) \cdot c_{\text{online}}$, where c_{mov} represents the cost of one dynamic change of an executor, and c_{online} is the cost of working online per unit time for an executor.

Experiments and analysis. The Trojan horse is one of the typical attacks on web applications that reflects sufficient details of attack and defense processes. In our experiments, the attacker uses the Trojan horse to achieve remote access and modify the home page. Then, only the fragile executor can be attacked successfully. To ensure the system is possible to be attacked successfully, we included the fragile executor in each tested diversity system.

Taking the fragile executor as an example, a successful attack includes three steps, (1) uploading the Trojan horse, (2) connecting the Trojan horse, and (3) modifying the home page. From the attack case, we tested eight different diversity systems and the AL, AT, response delay, and cost results. Figure 1 shows their comparison.

To make it easier to indicate a diversity system, we gave a short name for each system. Taking “R3D4-1(simi)” as an example, “R” denotes R-S, “3” means that there are three online executors work simultaneously, “D” represents D-S, “4” means that the total number of executors used is four, “-1” denotes that the online executors’ combination rotates once per minute, and “(simi)” indicates the existence of executors of the same type in the system executor set.

As shown in Figure 1, the general value performance of R2 is the best, while the values of R3(simi) are the worst among all the systems. Compared with R2, R3 has significant response delay and cost. Therefore, for the R-Ses, the response delay and cost are determined by the online voting executors’ number. Still, the diversity of these executors is the dominant factor of the defense ability.

For the D-Ses, the response delay values are almost the same. The cost values of the D-Ses demonstrate a positive association with the rotation frequency. In addition, the comparison between the D2-1 and D2-2 indicates that a higher rotation frequency leads to a higher defense ability and the diversity, executor number, and rotation frequency all play a role in improving the defense ability of the D-Ses.

Results of R3(simi), D2-1(simi), and R3D4-1(simi) suggest that the combination of the two kinds of diversity plays a complementary role in defense ability; however, it also increases the cost and response delay.

Conclusion. In this study, we propose the diversity system as the research to grasp the difference between temporal and spatial diversity. Moreover, with the Trojan horse attack experiments, the defense ability, cost, and response delay of the diversity systems with different configurations are evaluated and compared with each other.

Acknowledgements This work was supported by Foundation for Innovative Research Groups of National Natural Science Foundation of China (Grant No. 61521003) and National Key Research and Development Program of China (Grant No. 2018YFB0804004).

References

1 Zhuang R, Deloach S A, Ou X. A model for analyzing the effect of moving target defenses on enterprise networks. In: Proceedings of the 9th Annual Cyber and Information Security Research Conference, Oak Ridge, 2014. 73–76

2 Eskridge T C, Carvalho M M, Stoner E, et al. VINE: a cyber emulation environment for MTD experimentation. In: Proceedings of the 2nd ACM Workshop on Moving Target Defense, Denver, 2015. 43–47

3 Gallagher M, Biernacki L, Chen S, et al. Morpheus: a vulnerability-tolerant secure architecture based on ensembles of moving target defenses with churn. In: Proceedings of the 24th International Conference on Architectural Support for Programming Languages and Operating Systems, Providence, 2019. 469–484

4 Okhravi H, Hobson T, Bigelow D, et al. Finding focus in the blur of moving-target techniques. IEEE Secur Privacy, 2014, 12: 16–26

5 Wang F, Gong F, Sargor C, et al. SITAR: a scalable intrusion-tolerant architecture for distributed services. In: Proceedings of Workshop on Information Assurance and Security, Niagra Falls, 2003. 153–155

6 Hu H C, Chen F C, Wang Z P. Performance evaluations on DHR for cyberspace mimic defense. J Cyber Secur, 2016, 1: 40–51

7 Tong Q, Zhang Z, Zhang W H. Design and implementation of mimic defense web server. J Softw, 2017, 28: 883–897

8 Yong W, Qiang D, Dick S. Security evaluation using software diversity measurement: an ecological approach. In: Proceedings of the 2016 International Conference on Software Engineering Research and Practice, Monte Carlo Resor, 2016. 95–101