The 33rd Annual Conference of the Japanese Society for Artificial Intelligence, 2019

An Autonomous Cooperative Randomization Approach to Prevent Attacks Based on Traffic Trends in the Communication Destination Anonymization Problem

Keita Sugiyama*1 Naoki Fukuta*2

*1 Faculty of Informatics, Shizuoka University
*2 College of Informatics, Academic Institute, Shizuoka University

The communication destination anonymization problem is one of the problems to be resolved under some trade-offs in the cyber security field. Several approaches have been proposed for the communication destination anonymization problem such as Wang's U-TRI. However, due to the trade-offs that the user cannot take too expensive costs to make the network performance improved while keeping its security level, there remains the issues to make anonymization even over a short period of time while giving a good throughput. In this paper, we present an overview of the approach to solve this issue by introducing autonomously coordinating multiple end-hosts and a simulation environment to analyze it.

1. Introduction

When defending facilities with the camera network or patrolling ponds for avoiding illegal disposals by drones, the networks constituting them also need to be protected at the same time in order to operate them properly. It is mentioned that the anonymity of communication destination in such network is often implemented for this purpose [Wang 17]. U-TRI [Wang 17] has been proposed by Wang et al as one of the approaches for that purpose. However, it is mentioned that U-TRI still suffers from an issue when attackers are allowed to utilize their observed traffic trends [Wang 17]. In this paper, we present an overview of the approach to solve this issue by introducing autonomously coordinating multiple end-hosts and a simulation environment to analyze it.

2. Background and Related Work

2.1 Communication Destination Anonymization

It is one of the security problems on enterprise local networks that attackers are able to gather intelligence such as which end-hosts are online and which end-hosts are important by sniffing traffic in the networks. In order to prevent this problem, identifiers appear in network traffic need to be anonymized. PHEAR [Skowyra 16] and U-TRI [Wang 17] are methods to anonymize addresses in the local network. U-TRI implement anonymity by updating identifiers representing the communication destination and source in VIRO, which is a method of efficiently routing packets using the Software Defined Network, at random intervals based on idea of Moving Target Defense [Jajodia 11].

Contact: Keita Sugiyama, Faculty of Informatics, Shizuoka University, 3-5-1 Johoku, Naka-ku, Hamamatsu-shi, Shizuoka 432-8011 Japan, cs15050@s.inf.shizuoka.ac.jp

2.2 Attacks Based on Traffic Trends

As mentioned in the original Wang's U-TRI paper [Wang 17], U-TRI leaves the problem to allow attackers to attack based on traffic trends. Although the detail is not clearly mentioned there, the following cases can happen. For example, on the system where multiple clients are managed by a server, it is expected that packets whose destination address or source address is the address of the server appear frequently since multiple clients communicate with the server. In such a case, even if the address of each end-host is updated in a certain period, it is not difficult for the attacker to identify the address of the server by investigating the appearance situation of the address in a shorter period than the address-update interval. The primary factor of that is that, U-TRI implements anonymity in the medium to long term, but anonymity is not implemented in the short term. It is possible to make that hard by making the address-update interval very short for the purpose of implementing anonymity. However, shortening the address-update interval disorderly is not a practical solution since it is expected that the network performance will be greatly impaired by increasing the packet loss rate.

In this way, U-TRI leaves the possibility of traffic analysis utilizing the fact that it is difficult to implement short-term communication destination anonymity and that the tendency of traffic tends to be biased due to the nature of the system. In this paper, we will proceed with the necessary discussion to propose a method to effectively implement short-term anonymity.

3. Overview of Proposed Approach

The aim of our proposed approach is to implement a short-term anonymity in consideration of the trade-offs with the network performance while implementing the communication destination anonymity in the medium to long term like the U-TRI does. In addition, it is also required to

	Address	The First Observed Time	The Last Observed Time
1	~~f0:00:38:4e:8f:29~~	00:00:12	00:08:12
2	~~5e:11:59:50:df:30~~	00:00:12	00:04:12
3	~~ef:fe:27:b7:3d:10~~	00:04:12	00:08:12
4	~~a0:50:88:8a:5f:33~~	00:08:12	00:12:12
5	~~bf:2c:f8:9d:db:48~~	00:08:12	00:13:30
6	**be:9a:70:5b:9f:54**	00:12:12	00:13:30

Figure 1: The recently updated addresses estimated by the attacker.

change the strategy automatically and autonomously in consideration of the current traffic trends since network traffic changes over time.

Regarding the former requirement, the approach that each end-host determines the address-update frequency according to its own importance level is considered as one of the ways of satisfying the requirements.

Regarding the latter requirement, the approach that each end-host determines the address-update frequency according to its own packet transmission/reception status and packet loss is considered as one of the methods satisfying the requirements.

Therefore, it is possible for each end-host to determine its own address-update frequency in consideration of its own importance level, packet transmission/reception status, and its potential or current level of packet losses. Here, an issue is found using this approach. The issue of this approach is that the attackers are able to predict the most recently updated address, that is, the address likely to be the address pointing to the end-host whose address is being updated frequently, by excluding addresses that have not been observed for a long time and addresses that have been observed for a long time among the observed addresses. Figure 2 shows how an attacker predicts the most recently updated address from the observed addresses. Entries 1 to 4 are the addresses that have not been observed for a long period of time. Entry 5 is an address that is being observed for a long period of time. The attacker predicts that entry 6 is the address that was most recently updated.

In this way, it becomes an issue when attackers are able to gain much profit by attacking the end-host with high frequency of address-updates if the address-update frequency can be predicted by attackers. In order to solve this issue, we also require the ability that allows each end-host to cooperate with other end-hosts for giving attackers uncertainty about their own importance level.

4. Calculation of Attack-Success Rate by Simulator

In this work, we are preparing a prototype simulator to evaluate effectiveness our approach. The prototype of simulator has a mechanism to analyze the differences among the original U-TRI and our approach regarding their abilities to prevent an attack which utilizes its poor implementation of anonymity of communication destination (Attacker A) and an attack which predicts an end-host whose update frequency of the addresses is high (Attacker B).

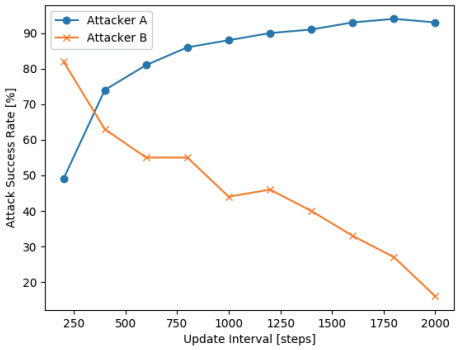

Figure 2: Attack-success rate of each attacker against the address-update interval of the server. The number of end-hosts except for the server = 6, the address-update interval of end-host except for the server = 2000 [steps].

On a situation with a network which has one server and six cameras where each camera communicates with the server, we analyze the attack-success rate of each attacker in the case where the attack-success condition is to attack the server. Figure 2 shows the results on that condition. It shows the attack-success rate when only the address-update interval of the server is changed while the address-update interval of end-hosts are fixed except for the server.

5. Conclusion

In this paper, we presented an overview of the approach to prevent attacks based on the traffic trends which is unavoidable in the original U-TRI, which provides the communication destination anonymization problem in the cyber security field by autonomously coordinating multiple end-hosts. In addition, we presented a prototype simulator to analyze differences among the original U-TRI and our approach.

References

[Jain 11] Jain, S., Chen, Y., and Zhang, Z.-L.: VIRO: A scalable, robust and namespace independent virtual Id routing for future networks, *2011 Proceedings IEEE INFOCOM*, pp. 2381–2389 (2011)

[Jajodia 11] Jajodia, S., Ghosh, A. K., Swarup, V., Wang, C., and Wang, X. S.: *Moving Target Defense: Creating Asymmetric Uncertainty for Cyber Threats*, Springer Publishing Company, Incorporated (2011)

[Skowyra 16] Skowyra, R., Bauer, K., Dedhia, V., and Okhravi, H.: Have No PHEAR: Networks Without Identifiers, in *Proceedings of the 2016 ACM Workshop on Moving Target Defense*, pp. 3–14 (2016)

[Wang 17] Wang, Y., Chen, Q., Yi, J., and Guo, J.: U-TRI: Unlinkability Through Random Identifier for SDN Network, in *Proceedings of the 2017 Workshop on Moving Target Defense*, pp. 3–15 (2017)