Revisiting Fragment Marking Scheme

Ngo Tien Dung, Choong Seon Hong
Department of Computer Engineering, Kyung Hee University
dungnt@networking.khu.ac.kr, cshong@khu.ac.kr

Abstract

IP traceback is an solution for Defending against distributed denial-of-service attacks, the Fragment Marking Scheme is the famous method for IP traceback problem. In this paper, we are interested in understanding the reconstruction process at the victim of Fragment Marking Scheme deeply and make us more clearly about its limitation based on some papers mentioning it.

1. Introduction

In this paper we mainly base on [2] and [1] to make analysis clearly about Reconstruction process at the Victim of FMS in order to reveal its limitations.

2. Reconstruction process at the victim

2.1 Reconstruction process

Limitation of Fragment Marking Scheme (FMS) [2] is that it is unfeasible in the case of multiple attacks. Let m' and m be number of disjoint edges and number of attackers at distance d in the attack graph. There might be many attack paths from each attacker. As a result, $m' \geq m$.

In order to derive the reconstructed attack graph, first of all, victim classifies set of all collected unique edge fragments Ψ into Ψ_0, Ψ_1, …, $\Psi_{max(d)}$ based on values of their distance fields (See Fig. 1). Intuitively, $|\Psi_{d,f}| \leq m'$. In the case of multiple attacks, the victim cannot distinguish which eight fragments are marked by the same router, therefore the victim needs to consider all possible ordered combination of the eight sets $\Psi_{d,0}$, $\Psi_{d,1}$, …, $\Psi_{d,7}$ and check their validity. Each combination is a candidate edge-id. Let the set of these candidate edges as C_d

$$\Rightarrow |C_d| = \prod_{0 \leq f \leq 7} |\Psi_{d,f}| \leq (m')^k .$$

This research was supported by the MKE(The Ministry of Knowledge Economy), Korea, under the ITRC(Information Technology Research Center) support program supervised by the NIPA(National IT Industry Promotion Agency)(NIPA-2011-C1090-1131-0005). Dr. CS Hong is the corresponding author.

combination of the set C_d), to reconstruct the routers at distance d, the victim XORs each element x in C_d with each element y in S_{d-1}, where S_{d-1} is the set of distinct routers (each router is represented under the form of interleaving of router's address and its hash) at distance $d-1$ in the reconstructed attack graph, which is already derived in the prior phase. Hence, the set of the XOR results is $|\Gamma_d| = \prod_{i=1}^{|C_d|} |S_{d-1}| = |C_d|.|S_{d-1}|$, (convention: $|S_{-1}| = 1$).

2.2. Limitation of Fragment Marking Scheme

However, the reconstruction process at distance d has not finished yet, the victim must to check these results have the right format or not. The false positive event arises from this checking step. Each element in Γ_d, that satisfies the checking will be inserted to the set of reconstructed routers S_d. Clearly, $S_d \subseteq \Gamma_d$. There is a little difference in mentioning the false positive event between [2] and [1]. While [2] is interested in calculating *false positive of accepting an edge-id at particular distance* d, [1] calculates *false positive of accepting an router*. At any particular distance d, each candidate edge-id in C_d is accepted once there is at least one element in the corresponding result set of $|S_{d-1}|$ elements which satisfies the checking. Clearly, the maximum number of accepted edge-id at distance d is $|C_d|$.

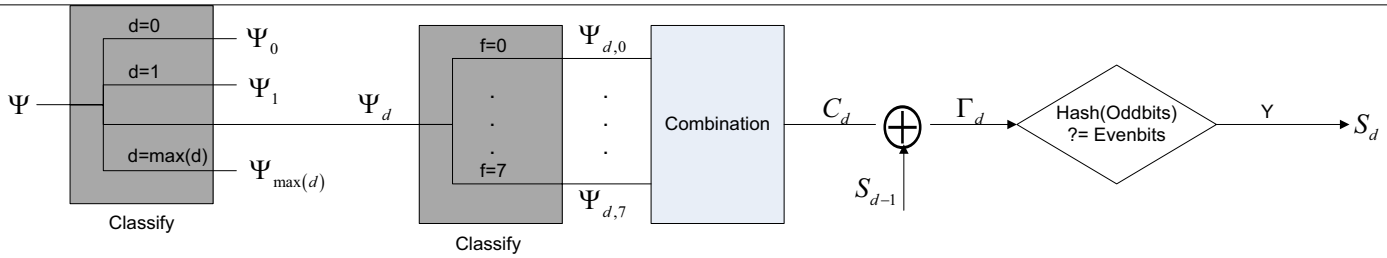

Figure 1. Reconstruction process at the victim.

$$p_f = \Pr(r_i \text{ is false positive}) \le \Pr\left(\left(Hash\left(OddBits\left(r_i\right)\right) = EvenBits\left(r_i\right)\right)\right) = \frac{1}{2^h} \quad (1)$$

$$\Pr(\text{an edge}-\text{id at distance } d \text{ is false positive}) = 1 - \prod_{i=1}^{|S_{d-1}|}\left(1 - \Pr(r_i \text{ is false positive})\right) \quad (2)$$

From (2) and (1), we derive:

$$\Pr(\text{an edge}-\text{id at distance } d \text{ is false positive}) \le 1 - \left(1 - \frac{1}{2^h}\right)^{|S_{d-1}|} \quad (3)$$

Because $S_{d-1} \subseteq \Gamma_{d-1}$

$$\Rightarrow |S_{d-1}| \le |\Gamma_{d-1}| = |C_{d-1}|.|S_{d-2}| \le (m')^k.|S_{d-2}|$$

…

$$\Rightarrow |S_0| \le (m')^k.|S_{-1}| = (m')^k$$

Therefore:

$$|S_{d-1}| \le (m')^{kd} \quad (4)$$

From (3) and (4), we have:

$$\Pr(\text{an edge}-\text{id at distance } d \text{ is false positive}) \le 1 - \left(1 - \frac{1}{2^h}\right)^{(m')^{kd}}$$

In the case that there is only one attack path from each attacker in the attack graph, that is, $m' = m$, and for $d-1$ we obtain the upper bound in [2] is:

$$\Pr(\text{an edge-id at distance } d = 1 \text{ is false positive}) \le 1 - \left(1 - \frac{1}{2^h}\right)^{m^k}$$

If $h = 32, k = 4, m = 100$, then $\Pr = 0.023 \Rightarrow$ low Error $\Rightarrow$ FMS is **feasible**. Thus, for $h = 32, k = 8$ (the values [2] uses for its implementation), FMS scheme is just feasible with the case of less than 10 attackers at the same distance $d = 1$.

Total number of combinations required to be checked for all distance is: $|\Gamma| = \sum_{d=0}^{\max(d)} |\Gamma_d|$

From (4) $\Rightarrow \Gamma$ is large $\Rightarrow$ FMS must check a a lot of time $\Rightarrow$ **High computation overhead** is a limitation of FMS.

Each checking is a trial with probability of false positive p, $|\Gamma|$ checkings are $|\Gamma|$ trials with the same probabilities p, i.e., Bernouli trials:

$$E[\text{Number of false positives}] = |\Gamma|.p_f \le \frac{|\Gamma|}{2^h}$$

Γ is large $\Rightarrow$ Another limitation of FMS is **large number of false positives**.

3. Conclusion

In this paper, We make analysis about limitation of FMS more clearly based on [2] and [1]. That is the first important work to find another scheme which is better than the Fragment Marking Scheme.

4. References

[1] Perrig A. Dawn Song. Advanced and authenticated marking schemes for ip traceback. INFOCOM, 2001.

[2] S. Savage, D. Wetherall, A. Karlin, and T. Anderson. Network support for ip traceback. Networking, IEEE/ACM Transactions on, 9(3):226 –237, June 2001.