A Symptom-Based Taxonomy for an Early Detection of Network Attacks*

Ki-Yoon Kim and Hyoung-Kee Choi

The School of Information and Communication Engineering,
Sungkyunkwan University, Suwon, Korea, 440-746
{doogysp, hkchoi}@ece.skku.ac.kr

Abstract. We present a symptom-based taxonomy for an early detection of network attacks. Since this taxonomy uses symptoms in the network it is relatively easy to access the information to classify the attack. Accordingly it is quite early to detect an attack as the symptom always appears before the main stage of the attack. Furthermore, we are able to classify unknown attacks if the symptom of unknown attacks is correlated with the one of the already known attacks.

1 Introduction

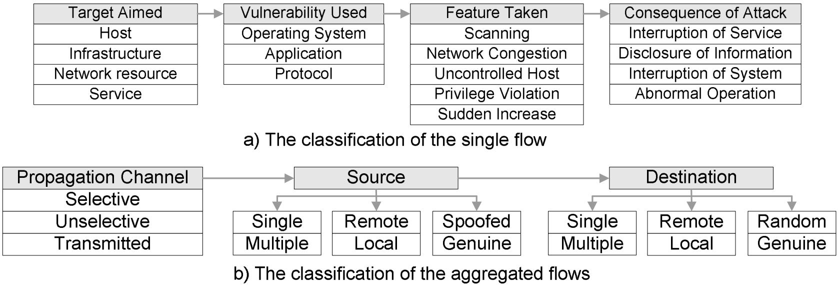
In order to protect the network against attacks effectively, the attacks must be classified by similar types and patterns, and a proper prevention and defense method for each type of attacks must be selected and applied. To classify attacks with similar patterns, taxonomies which classify attacks using their characteristics have been previously proposed. However, the previously proposed taxonomies show a few weaknesses; 1) taking excessive time to analyze information necessary to classify attacks and hence not being able to respond to newer attacks in a timely manner, 2) being able to trust the consequences of attack classification only when all normal system patterns are identified in advance. Since the weakness in the attack taxonomy directly influences on the selection of a defense method, they may also become the roadblock in the system defense. In order to setup the new taxonomy, we focus on the fact that a network shows symptoms when an attack is prepared and initiated [2][3], and that the variety of information in the network can be collected using the logs from different type of sensors [1]. Based on this fact, we propose the symptom-based taxonomy that uses symptoms in the network to classify attacks.

2 Symptom-Based Taxonomy

The symptom-based taxonomy classifies attacks in two stages; a single flow and aggregated flows. Fig. 1 shows the two-staged classification of the symptom-based

* This research was supported by the MIC (Ministry of Information and Communication), Korea, under the ITRC (Information Technology Research Center) support program supervised by the IITA (Institute of Information Technology Assessment).

C.C. Yang et al. (Eds.): PAISI 2007, LNCS 4430, pp. 327–328, 2007.



a) The classification of the single flow

b) The classification of the aggregated flows

Fig. 1. Two-staged classifications of symptom-based taxonomy

taxonomy. In the first stage, attacks in a single flow are of interest. A typical example of the first stage attack includes a DoS attack. The classification takes advantages of such information as target (victim) aimed, vulnerability used by attacks, phenomenon shown during attacks, and the consequence of attacks. In the second stage, the aggregated flows are used to judge whether attacks in the form of a single flow are independent to other attacks, and whether they are relevant to form a unified attack. Such an attack as DDoS is the unified attack and occurs simultaneously from various nodes in the aggregated flows. In this case, individual single flows from each node are classified as an attack in the first stage. Then, they are further considered, in the second stage, to check whether the individual attacks are a part of the unified attack. Information used in the second stage is the locations of the attacker and the target. In other words, if a number of attacks in the single flows comes from the same source or passes to the same target or both over a short period of time, then these are the unified attacks by definition. As a result, this taxonomy can resolve problems occurred due to the delayed response to new attack patterns as well as problems occurred due to registering all normal patterns.

3 Conclusion

We present a symptom-based taxonomy for an early detection of network attacks. Only information required to the proposed taxonomy is the distinct symptoms at the scene. The symptoms are available in the convenient and reliable logs from different sensors in the network. As a result, the proposed attack taxonomy is able to classify even unknown attacks without a delay.

References

1. Cristina Abad et al., "Log Correlation for Intrusion Detection: A Proof of Concept", Computer Security Applications Conference, Dec. 2003.
2. Nong Ye, Joseph Giordano and John Feldman, “A Process Control Approach to Cyber Attack Detection,” Communications of the ACM, Vol. 44 No 8, pp 76-82, Aug. 2001.
3. Akira Kanamaru et al., "A Simple Packet Aggregation Technique for Fault Detection", International Journal of Network Management 2000, Vol. 10, pp 215-228, Aug. 2000.