WebIDS: A Cooperative Bayesian Anomaly-Based Intrusion Detection System for Web Applications
(Extended Abstract)

Nathalie Dagorn

Laboratory of Algorithmics, Cryptology and Security (LACS), Luxembourg
& ICN Business School, France
nathalie.dagorn@icn-groupe.fr,
nathalie.dagorn@orange.fr
http://www.uni.lu/
http://www.icn-groupe.fr/

Abstract. This paper presents WebIDS, a learning-based anomaly detection system for Web applications aiming at improving the decision process, reducing the number of false positives, and achieving distributed detection.

Keywords: Anomaly detection, Correlation, Web application.

1 Introduction

Attacks on Web applications and services have been increasing dramatically for the last years. Related approaches in intrusion detection are still rare. The major challenges anomaly-based systems have to solve in the field are the improvement of the decision process, the reduction of the high number of (false) alarms caused by unusual activities, and the recent need of distributed intrusion detection. At the crossing of these research areas, the aim of our work is to propose an efficient distributed anomaly detection system dedicated to the security of Web applications.

2 Our Proposal: WebIDS

WebIDS analyzes HTTP GET requests as logged by Apache Web servers. The analysis process is based on a multi-model approach [5] implementing ten statistical algorithms: attribute length, attribute character distribution, structural inference, token finder, attribute presence or absence, attribute order, access frequency, inter-request delay, invocation order, and anomaly history (which allows, among others, keeping track of alarms). The system requires no special configuration (autonomous learning). A non-naive Bayesian network is used as a decision process [3], classifying the events more accurately and incorporating information about confidence in the models. At the root node, a specification of the event classification [6] distinguishes between a normal state and five Web attack states (authentication, XSS, command execution, denial of service, and other attack). The system is improved after each log analysis by filtering out false positives using an alarm clustering technique [2]. As part of the anomaly

R. Lippmann, E. Kirda, and A. Trachtenberg (Eds.): RAID 2008, LNCS 5230, pp. 392 – 393, 2008.

history model, a cooperation feature enables the system to achieve alarm and event correlation [4]. The Intrusion Detection Message Exchange Format (IDMEF) [1] is used for sharing alarm information between systems.

3 Experimental Results

WebIDS has been implemented in an IT company based in Luxembourg and showed good detection rates (sensitivity of 96.02 %, specificity of 99.99 %, and reliability of 99.94 %). The false positive rate (0.01422 %) is lower than the rates observed for similar systems. Nevertheless, these results must be mitigated because only a small number of anomalies could be observed by WebIDS over the experimental period, and the comparison with existing systems is not based on the same dataset.

4 Conclusion and Future Work

As a conclusion, we can state that the cooperative anomaly-based intrusion detection system proposed is both innovative and efficient. By improving the decision process, reducing the false positive rate and enabling cooperation between systems, it meets the defined challenges. As a follow-up to this research, the deployment of WebIDS in a more widely distributed environment is currently considered. Some functional and technical improvements are being carried out for that purpose.

References

1. Debar, H., Curry, D., Feinstein, B.: The Intrusion Detection Message Exchange Format. Internet Draft IETF (2005), http://www.ietf.org/internet-drafts/draft-ietf-idwg-idmef-xml-14.txt
2. Julisch, K.: Using Root Cause Analysis to Handle Intrusion Detection Alarms. PhD Thesis, University of Dortmund, Germany (2003)
3. Kruegel, C., Mutz, D., Robertson, W., Valeur, F.: Bayesian Event Classification for Intrusion Detection. In: 19th Annual Computer Security Applications Conference. IEEE Computer Society Press, New York (2003)
4. Kruegel, C., Valeur, F., Vigna, G.: Intrusion Detection and Correlation - Challenges and Solutions. In: Advances in Information Security, vol. 14. Springer, Heidelberg (2005)
5. Kruegel, C., Vigna, G., Robertson, W.: A Multi-Model Approach to the Detection of Web-Based Attacks. Computer Networks 48(5), 717–738 (2005)
6. Valdes, A., Skinner, K.: Adaptive, Model-Based Monitoring for Cyber Attack Detection. In: 3rd International Symposium on Recent Advances in Intrusion Detection, pp. 80–92. Springer, Heidelberg (2000)