Future Internet Security Services Enabled by Sharing of Anonymized Logs

Jianqing Zhang[1], Nikita Borisov[1], William Yurcik[2], Adam J. Slagell[2], and Matthew Smith[3]

[1] University of Illinois at Urbana-Champaign {jzhang24, nikita}@uiuc.edu,
[2] National Center for Supercomputing Applications {byurcik, slagell}@ncsa.uiuc.edu
[3] University of Marburg matthew@informatik.uni-marburg.de

Abstract. As security monitoring grows more complicated, there is an increased demand for outsourcing these tasks for to Managed Security Service Providers (MSSPs). However, the core problem of sharing private data creates a barrier to the widespread adoption of this business model. In this position paper we propose an anonymization solution that promotes sharing logs with MSSPs while simultaneously protecting privacy.

1 Introduction

MSSPs follow a long trend of outsourcing organizational functions. They leverage economies of scale by assembling skilled security professionals and a security support infrastructure that can be shared across multiple organizations [6]. MSSPs can also correlate attacks across organizational boundaries to provide a more effective response [1]. This is particularly relevant for the field of Grid computing where computing and resource usage spans organizational boundaries but security analysis cannot "see" beyond their local organizational boundary.

However, MSSPs must handle sensitive data that is either protected by privacy laws, such as employee and customer data, or highly valuable to competitors, such as volumes, applications, etc. This data also includes technical details that, if they were to fall into the wrong hands, could be used to more effectively attack the organization. For this reason, many organizations are reluctant to form such a close and high-risk connection with an outside security provider and have to either hire expensive security professionals or sacrifice the level of security protection. This concern over data privacy is a barrier to the growth of the MSSP market. We propose a new approach that can address this problem — a privacy-preserving technique for sharing security data between organizations and MSSPs.

2 Anonymized Logs for Attack Analysis

Logs are the essential unit for system administration and security analysts. Our solution is to anonymize private information within logs to prevent sensitive information from being leaked to the MSSP while still providing enough information for the MSSP to analyze for actionable security information. While log anonymization is a well-studied topic [2, 5], the problem of using shared log data for attack analysis is relatively unexplored. Existing work on privacy-preserving sharing of logs [4, 3] falls short of describing a sufficient set of techniques to replace on-site monitoring.

Figure 1 shows the architecture for future privacy-preserving MSSPs. Anonymized logs from different organizations are sent in real-time to MSSPs for monitoring and analysis. When the MSSP detects any unusual activity, such as flows that would suggest a potential denial-of-service attack, it can send an alert back to an organization who can then take an appropriate corrective action. blocking the source IP address of the attack. This IP address may not be visible to the MSSP due to log anonymization; however, the MSSP can supply enough information with its alert such that the organization can cross-reference it with its own unmodified logs and discover the correct address.

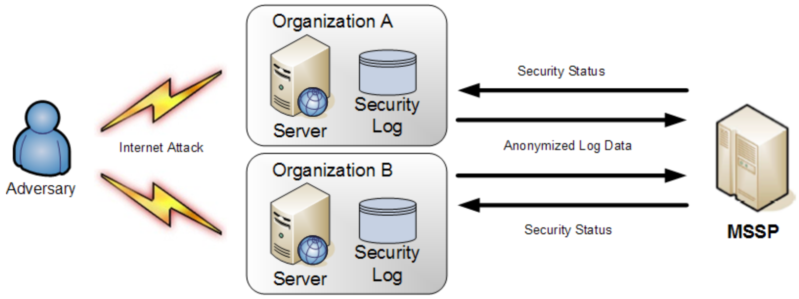

Fig. 1: Future Privacy-Preserving MSSP Architecture

3 Research Challenges

The use of anonymized logs in this context presents a trade-off: the more information is anonymized, the less information is available to the MSSP. The key challenge is to identify which points in this trade-off are reasonable for providing outsourced security management while adequately protecting privacy. We would like to take advantage of the fact that while legitimate traffic has high privacy value, attack traffic is only private in so far as it reveals information about the characteristics of the internal network. Therefore, an adaptive solution may be appropriate, where most log entries are highly anonymized, but a limited number of entries deemed suspicious are described in more detail, and entries corresponding to verified attacks may be shared with other organizations.

Another challenge is to deal with arbitrarily malicious MSSPs. It has been shown that active probing may be used violate the anonymity of data logs [7]. We plan to investigate whether there are better anonymization techniques that are resistant to such probing, while at the same time leaving enough information to still be useful to detect attacks. We also are interested whether an honest-but-curious or similar attack model is a reasonable way to represent a semi-trusted relationship with MSSPs.

Our plan is to identify several techniques for monitoring logs for attacks that are used by security professionals and translate them into the domain of anonymized security logs. We believe that concrete applications (including large scale Grid applications) will help guide decisions about the trade-offs between privacy and fidelity of information. We also plan to make the solution adaptable so that MSSPs can experiment with and apply new monitoring techniques without modifying the log sharing infrastructure. We are at an early stage in our research, but we believe that a solution to this problem will represent a paradigm shift in the future security services, expanding the MSSP market and providing better overall protection on the Internet.

References

1. Slagell, A., and Yurcik, W. “Sharing Computer Network Logs for Security and Privacy: A Motivation for New Methodologies of Anonymization,” *IEEE/CREATENET SecureComm*, 2005.
2. Li, Y., Slagell, A., Luo, K., and Yurcik, W., “CANINE: A Combined Conversion and Anonymization Tool for Processing NetFlows for Security,” *Intl. Conf. on Telecom. Sys.*, 2005.
3. Xu, D., and Ning, P., “Privacy-Preserving Alert Correlation: A Concept Hierachy Based Approach,” *21st Comp. Sec. App. Conf.*, 2005.
4. Lincoln, P., Porras, P., and Shmatikov, V., “Privacy-Preserving Sharing and Correlation of Security Alerts,” *13th USENIX Sec. Symp.*, 2004.
5. Flegel, U. “Pseudonymizing Unix Log Files,” *Infra. Sec. Conf.*, 2002.
6. Ding, W., Yurcik, W., and Yin, X, “Outsourcing Internet Security: Economic Analysis of Incentives for Managed Security Service Providers,” *Workshop on Internet and Network Economics (WINE)*, 2005.
7. Bethencourt, J., Franklin, J., and Vernon, M., “Mapping Internet Sensors with Probe Response Attacks,” *USENIX Security*, 2005