# Human Factors in Webserver Log File Analysis: A Controlled Experiment on Investigating Malicious Activity



| | |
|---|---|
| Title | Human Factors in Webserver Log File Analysis: A Controlled Experiment on Investigating Malicious Activity |
| Publication Type | Conference Paper |
| Year of Publication | 2014 |
| Authors | Layman, Lucas, Diffo, Sylvain David, Zazworka, Nico |
| Conference Name | Proceedings of the 2014 Symposium and Bootcamp on the Science of Security |
| Publisher | ACM |
| Conference Location | Raleigh, NC, USA |
| ISBN Number | 978-1-4503-2907-1 |
| Keywords | ACM CCS, Foundations, Human and Societal Aspects of Security and Privacy, human factors, Intrusion Detection Systems, Intrusion/Anomaly Detection and Malware Mitigation, log files, Quantitative Verification, science of security, security, Social Aspects of Security and Privacy, Validation and Verification |

Abstract

While automated methods are the first line of defense for detecting attacks on webservers, a human agent is required to understand the attacker's intent and the attack process. The goal of this research is to understand the value of various log fields and the cognitive processes by which log information is grouped, searched, and correlated. Such knowledge will enable the development of human-focused log file investigation technologies. We performed controlled experiments with 65 subjects (IT professionals and novices) who investigated excerpts from six webserver log files. Quantitative and qualitative data were gathered to: 1) analyze subject accuracy in identifying malicious activity; 2) identify the most useful pieces of log file information; and 3) understand the techniques and strategies used by subjects to process the information. Statistically significant effects were observed in the accuracy of identifying attacks and time taken depending on the type of attack. Systematic differences were also observed in the log fields used by high-performing and low-performing groups. The findings include: 1) new insights into how specific log data fields are used to effectively assess potentially malicious activity; 2) obfuscating factors in log data from a human cognitive perspective; and 3) practical implications for tools to support log file investigations.

URL http://doi.acm.org/10.1145/2600176.2600185
DOI 10.1145/2600176.2600185
Citation Key Layman:2014:HFW:2600176.2600185

Quantitative Verification Science of Security Validation and Verification Foundations ACM CCS foundations Human and Societal Aspects of Security and Privacy Human Factors Intrusion Detection Systems Intrusion/Anomaly Detection and Malware Mitigation log files Quantitative Verification Science of Security security Social Aspects of Security and Privacy validation and verification Intrusion Detection Systems Social Aspects of Security and Privacy Human and Societal Aspects of Security and Privacy Intrusion/Anomaly Detection and Malware Mitigation ACM CCS