

11/7/01

Data Forensics: Analyzing the Tracks of an Intruder

Tye Stallard

Applications are providing the functionality that was once the sole realm of operating systems. The evolution of the World Wide Web, distributed computing and peer-to-peer technologies are evidence of this. When flawed applications expose interfaces to domains of little or no trust, the role of the administrator is critical. The administrator must monitor application logs and perform appropriate actions when important events occur. This research investigates automated forensic techniques to detect productive administration or the lack thereof. The results can provide feedback, shorten the exposure of vulnerable software and improve security of critical or not so critical systems.