Georgia Tech Research Corporation
Technologies Available for LICENSING
OFFICE OF TECHNOLOGY LICENSING
https://licensing.research.gatech.edu | techlicensing@gtrc.gatech.edu

Apparatus and Method for Protecting Log Information (#6327)

A combined approach that limits cyber intruders from altering systems logs, including those who have managed to obtain root access

The invention combines hardware and software to accomplish the goal of stopping or limiting the ability of computer system intruders from altering the existing logs. It limits intruders who are able to gain remote access to the server from modifying existing logs or removing the log data. It is able to limit intruder ability even if they gain root privileges. The intruder's history of accessing the system and gaining privileges will be recorded by this invention, even if the intruder stops the logging activities or modifies the logs subsequent to intrusion. Logging data prior to the intrusion will not be modifiable along with data regarding the origin of the attack. IT personnel can obtain valuable data of activities that occurred during and prior to the intruder gaining full privileges and modifying the system, as well as information on where the intrusion occurred.

Benefits/Advantages

- Hardware and software to prevent 'log' data tampering
- System logs impenetrable and non-modifiable
- Disables the ability to remove or tamper with trace data
- Attackers unable to delete log data stored in the Hard Disk Drive
- Program works in background without impacting performance

Potential Commercial Applications

- IT administrators
- Stand-alone computers
- Computer networks
- Telecommunication networks

Background/Context for This Invention

Computer system administrators use logs generated by the operating system kernel to check on various aspects of the computer, including potential attacks or unauthorized activity. System intruders frequently try to access the logs folder to cover their tracks or disguise any malevolent activity. Protecting the log data from this type of malicious activity helps hamper the ability of intruders to change the system operations in any manner and provides a reliable safeguard for IT (Information Technology) administrators.

Jongman Kim
Professor - Georgia Tech School of Electrical and Computer Engineering

Junghee Lee
Graduate Student - Georgia Tech School of Electrical and Computer Engineering

More Information

Publications

For more information about this technology, please visit:
https://licensing.research.gatech.edu/technology/apparatus-and-method-protecting-log-information

Images:

The automated sequential delivery of multiple fluids. A varying number of delay gates imprinted in the branches are shown in the figure.

COVID-19 and flu saliva test on paper: (A) The automatic sequential delivery of multiple reagents required for virus test; (B) Water pouring into the device triggers the virus assay, allowing the presence of SARS-CoV-2 and influenza A & B viruses to be visually identified by the color changes in the corresponding detection spot