

Statistical Fingerprinting for Malware Detection and Classification

Disclosure Number

201002422

Technology Summary

This invention is a novel method of identifying existing malware infections. The invention reliably detects malware and rootkit infections via monitoring of "symptoms." The invention identifies particular malware or malware families through statistical "fingerprinting" based on observed effects. Since malware must execute on the machine, it will necessarily cause a statistical deviation from the baseline that can be detected (a "symptom" of the infection). Further, it is anticipated that different classes of malware will cause different patterns of deviations, and these can be used to identify the class of malware, or even the particular malware itself.

Inventor

PROWELL, STACY J

Computational Sciences & Engineering Div

Licensing Contact

SIMS, DAVID L

UT-Battelle, LLC

Oak Ridge National Laboratory

Rm 124C, Bldg 4500N, MS: 6196

1 Bethel Valley Road

Oak Ridge, TN 37831

Office Phone: (865) 241-3808

E-mail: SIMSDL@ORNL.GOV

Note: The technology described above is an early stage opportunity. Licensing rights to this intellectual property may be limited or unavailable. Patent applications directed towards this invention may not have been filed with any patent office.