# A sense of self for Unix processes



4 Author(s)

Forrest, S. ; Dept. of Comput. Sci., New Mexico Univ., Albuquerque, NM, USA ; Hofmeyr, S.A. ; Somayaji, A. ; Longstaff, T.A.

Abstract | Authors | References | Cited By | Keywords | Metrics | Similar

A method for anomaly detection is introduced in which “normal” is defined by short-range correlations in a process' system calls. Initial experiments suggest that the definition is stable during normal behaviour for standard UNIX programs. Further; it is able to detect several common intrusions involving sendmail and 1pr. This work is part of a research program aimed at building computer security systems that incorporate the mechanisms and algorithms used by natural immune systems

**Published in:**
Security and Privacy, 1996. Proceedings., 1996 IEEE Symposium on

**Date of Conference:**
6-8 May 1996

**Page(s):**
120 - 128

**Conference Location :**
Oakland, CA

**Meeting Date :**
06 May 1996-08 May 1996

**DOI:**
10.1109/SECPRI.1996.502675

**ISSN :**
1081-6011

**Publisher:**
IEEE

**Print ISBN:**
0-8186-7417-2

**INSPEC Accession Number:**
5310802