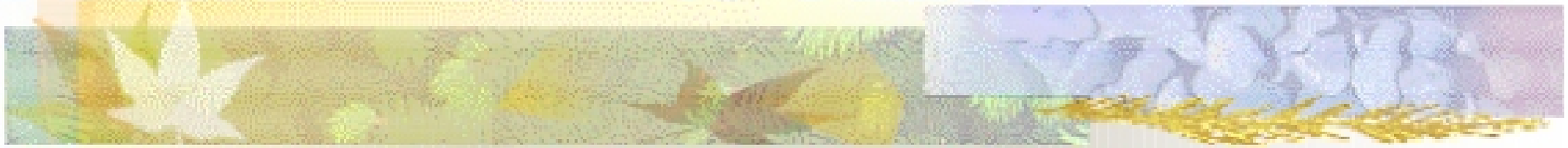
A Sense of Self for Unix Processes



Stepannie Forrest,Steven A. Hofmeyr,
Anil Somayaji, Thomas A. Longstaff

Presenter: Ge Ruan

Overview

- This paper presents an intrusion detection algorithm which is learned from mechanisms of natural immune systems.
- In natural immune system, pattern recognition is used to check whether a cell is normal or abnormal?
- So, how to define the pattern of normal or "Self" is the main focus of this paper.

Definition of Self

- What we mean self in computer system is more dynamic than in the case of natural immune systems.
  - Load updated software
  - Edit files
  - Run new programs
  - Change work habits

In these cases, the normal behavior of the system is changed, sometimes dramatically.