

Master Thesis Project Plan

Kyrre M Begnum

27. mai 2002

pH (Process Homeostasis) is a patch for the 2.2.x GNU/Linux kernel, that enables the kernel to track system calls generated by all processes and analyse these traces using a pattern matching algorithm. It also generates a profile of every binary that is being executed. Should a process generate system call patterns that do not correspond to the profile, the process will be delayed using a time-delay algorithm. This is meant to sabotage attacks which are based on executing alien code (buffer overflow). Using a special system call, pH's reaction sensitivity can be adjusted in runtime.

This is a process based anomaly detection system (ADS) with a reaction pattern. Today we have other anomaly detection systems that base their detection on overall system signatures based a set of system variables. One example is *Cfengine* - A autonomous agent and a middle to high level policy language for building expert systems which administrate and configure large computer networks. Cfengine has a module for detecting anomalies based on system variables and the ability to define a reaction pattern to a given anomaly event.

1. **How does a system using pH differ from a normal one on a overall system perspective?**
 - (a) How do two apparent similar computer systems differ with regard to overall system variables like memory, CPU and disk usage?
 - (b) Would this difference increase if one of the systems should run a pH-patched kernel?
2. **How could a process based anomaly detection system be incorporated into a more generic configuration engine like cfengine?**
 - (a) In what way does cfengine offer an interface for communicating with pH?
 - (b) How could a pH-based eventhandling approach enable a system administrator to define higher level reaction patterns for the system?