Large Scale Kernel Logging for System Recovery Purposes
LIA Project Proposal

Yonne de Bruijn
yonne.debruijn@os3.nl

Alexandros Stavroulakis
alexandros.stavroulakis@os3.nl

February 20, 2015

Version: 1.0

Introduction

Rapid restoration of systems to their original state has thus far usually been facilitated by reflashing
system images or performing clean installs. A different approach will be presented without reinstalling
the operating system. By intercepting disk writes on a kernel level and storing these in a centralized
manner, it might be possible to restore the system state by taking the inverse of every command stored.
In this way, the hypothesis is that the strain put on the network should be lower than traditional methods,
as no full disk images are being communicated. Time will be spent on implementing such a technique
and evaluating the scalability and feasibility.

Motivation

The main motivation for this project is to see if it is possible to log and use the kernel calls in a large
infrastructure. If so, the researchers would like to see if this would put a smaller load on the network
when compared to usual ways of restoring systems. There might be a tipping point regarding the amount
of users, or amount of actual work being performed, where it is more beneficial to simply reflash the
system. Investigating if this approach is feasible and/or might be useful is what drives this project.

Research question

Is it feasible to develop a centralized manner to log disk writes for recovery purposes? And if it is
feasible, how would it scale in a large infrastructure?

Approach

Research time will be spent on creating a Linux kernel which is able to log the disk writes back to a
centralized server. The centralized server will be developed in such a way that it is able to store the
information being passed by several of these linux kernels, which are being run on the local systems. After this, a theoretical research will be performed on how to restore the systems to their original state. If time permits, this will be implemented in a proof-of-concept. When this proves unreachable within the time limit, the end product will encompass the kernel combined with the back-end to perform large scale logging.

Ethical concerns

Logging disk writes in a shared computer environment can, of course, involve certain ethical concerns. However, the research team does not see any particular privacy issues arising, as tracing user actions back to actual users would be a very difficult task to accomplish.

Related work

System recovery in an automated manner along with Kernel and System Call logging are widely researched areas. The following papers are related to the idea behind this project and will be taken into account when completing the research and writing the final report.
