

Qualification Statement for participation of: Fourth Information Survivability Workshop (ISW-2001)

Nadine Hanebutte

PhD student at the University of Idaho

Phone: 1-(208)885-4077

Fax: 1-(208)885-9052

For the last 2 semesters I have been working with Axel Krings at the University of Idaho conducting research in the area of survivability. We developed the kernel-based attack signature detection engine that uses an instrumented linux kernel to extract the kernel activity in real-time as well matching the extracted kernel profile against a signature database. The goal of the project is to use the output of this engine to implement survivability features.

My Master Thesis discussed how to measure software quality in terms of its likelihood to fail. The internal measures were extracted from software design documents before a single line of code was written and than mapped onto one external measure using Factor Analysis. The idea was to take what you can measure and quantify (e.g. Lines of Code, number of variables, number of functions called) and relate them to an external measure that cannot be quantified directly. I am trying to apply this idea from the software engineering area in the field of survivability. Instead of accessing survivability of a specific system on a case by case base it should be possible to identify a preliminary measure that allows to quantify or at least scale a system according to a survivability index. Maybe in terms of a system being in certain compromised state or in terms is how much survivability does the system need and the strength of threads to be expected.

QUESTIONS:

The same way security policies describe what is allowed, survivability policies can be used say what to do when a particular thing went wrong or a particular part of the system got compromised. How can existing security policies be mapped onto survivability (policies)? Security, safety and survivability go hand in hand. Survivability matters after prevention measures failed. One reason why these measures fail is that security is often ignored or applied incompletely because of the complexity of the security system itself. Is there a way to avoid this to happen to survivability systems? Can survivability approaches be implemented or even created in a way that minimizes human interference so that they will be applied and not seen as a burden?