Why Principles-Driven Forensic Analysis is a New Paradigm

Sean Peisert Matt Bishop Sid Karin Keith Marzullo

Successful forensic analysis requires the ability to re-create any event regardless of the intent of the user, the nature of the previous events, and whether the cause of the events was an illegitimate intruder or an authorized insider. Current tools fall short of these goals. The events they cannot accurately identify include anything that a program is reading or writing to memory. This covers a huge number of possible events and exploits, such as changes to the user environment, buffer overflows, race conditions, and covert information sharing in user space.

Current techniques to resolve these problems result in generation of too much information, leading to impractical performance slowdowns and high storage requirements. They also suffer from a disparity between the goals of system designers, administrators, and forensic analysts. Five principles address current failures. Any tool that does not follow all of these principles will fail to record actions or results in enough detail to understand their meaning. Some current tools use techniques that address part, but not all, of these principles. Thus, they fail to recognize and report many scenarios, or do so incorrectly.

Principle 1: *Consider the entire system. This includes the user space as well as the* entire *kernel space, filesystem, network stack, and other related subsystems.*

Principle 2: *Assumptions about expected failures, attacks, and attackers should not control what is logged and audited. Trust no user and trust no policy, as we may not know what we want in advance.*

Principle 3: *Consider the effects of events, not just the actions that caused them, and how those effects may be altered by context and environment.*

Principle 4: *Context assists in interpreting and understanding the meaning of an event.*

Principle 5: *Every action and every result must be processed and presented in a way that can be analyzed and understood by a human forensic analyst.*

In this paper, we identify gaps in existing tools and techniques and show how adherence to the five principles closes these gaps. We then suggest new techniques for logging and auditing that satisfy the five principles. Some of these techniques are already used, and some are adaptations from other disciplines. The idea of *synthesizing* these techniques into a single set of tools, and the method used to do so, is unique. Furthermore, by concentrating on which principles the tools need to meet, before addressing how they can do so efficiently, we show how a much more powerful and usable computer forensics analysis system can be created.