When is logging sufficient?

Johannes Olegård, Stefan Axelsson
Department of Computer and Systems Sciences, Stockholm University

It is generally agreed that logs are necessary to understand cyberattacks after they have happened. However, little is known about what such logs should contain to be forensically helpful. Conventional logs are typically not designed for security purposes, which creates correlation difficulties and results in logs with too little or too much information. Related work has mainly focused on filtering such conventional logs rather than determining the correct information to log in the first place.

In this work, we discuss what it means for logging to be sufficient in relation to forensic readiness. We then propose a bookkeeping-inspired logging system that minimally captures attacker movements and does so despite log tampering. We implement a proof-of-concept of this system based on distributed tracing, using the Linux kernel Function Tracer (ftrace) and OpenTelemetry.