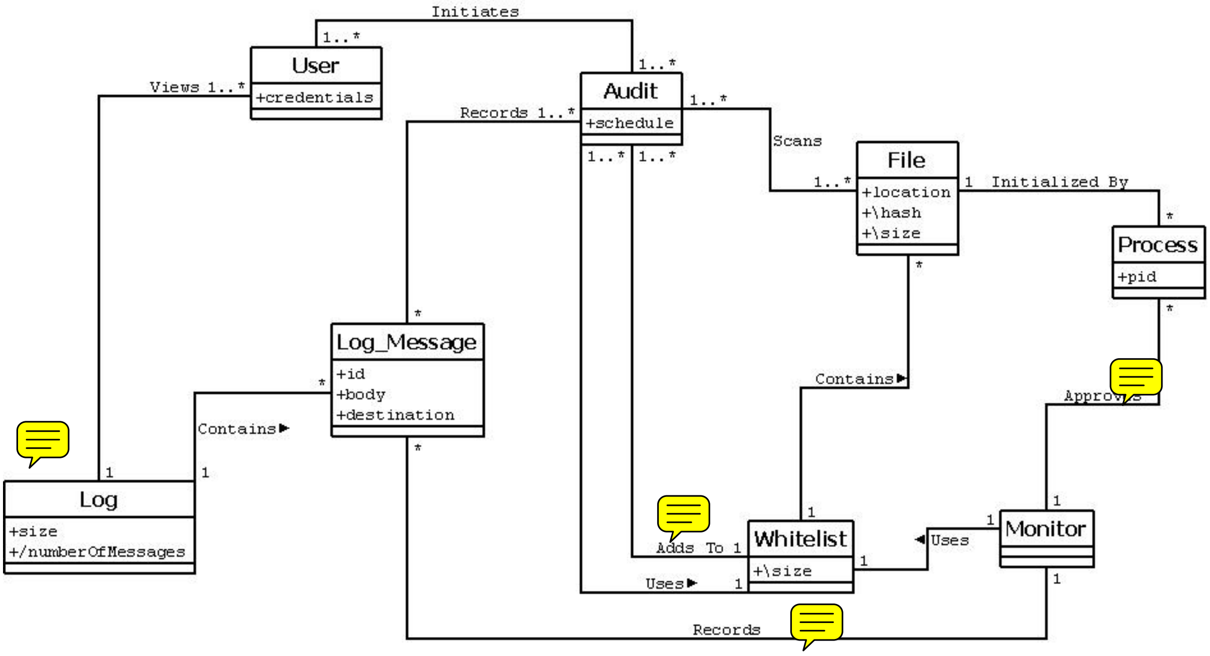
Software Security API
Eric Crockett
David Pick
Josh Dash

Domain Model Explanation



In this model, Users (Tempus employees) can initiate system Audits, or Audits may be scheduled to run regularly. Users must authenticate to the Audit system before they are allowed to initiate a system Audit. A system Audit scans the entire directory tree. It compares the hash of each scanned file to the Whitelist to see if the file has been previously detected. The system Audit may add files to the Whitelist and will also send Log_Messages back to Tempus. Users can later view all of the Log_Messages.

A separate part of the system is the Monitor. The Monitor detects when a new Process attempts to run, checks it against the Whitelist, and then either approves or denies the Process. Each Process is associated with the File which initiated it. The Monitor routine may also send Log_Messages which can be viewed later by Users.

Although Files and Processes may seem synonymous, they are distinct in our model because of what they symbolize. Files represent files in the hard drive which have been whitelisted; they are created by the Audit and persist as long as they are whitelisted. Processes on the other hand exist only in memory and represent a running program. A new Process is created when some executable is run. The Monitor can either approve or deny the Process. Even though Processes and Files exist in a 1-1 relationship, they are distinct because Audit operates on Files, while Monitor operates on Processes.