LETTER
from the Foundation

Security

Information Security has a concept of "Defence in Depth," a strategy of applying multiple layers of security measures which work in concert to limit the impact of an attacker gaining unauthorized access to a system, for example, by exploiting a vulnerability. These layers include techniques applied to the design of a system or program, those applied during development, mitigations applied at run-time, and operational procedures and techniques.

The "Principle of Least Privilege" is a technique that can apply during design and operation. The principle states that a process should operate with only those privileges that are required. Tools like static analysis (automated source code analysis) are applied during development. Some tools operate on running software as part of the development process, such as code-coverage-guided automated fuzzing. American Fuzzy Lop (AFL) and Syzkaller are two such examples which have been used to good effect in FreeBSD. Runtime mitigations apply when software is used in production. Examples include address randomization and limitations on memory protection. Finally, operational procedures and techniques include those employed by the software author or provider, such as the FreeBSD security team's process for issuing security advisories, and by the user or sysadmin, such as setting and documenting configuration options.

Welcome to this security-focused *FreeBSD Journal* issue. We'll touch on a few different areas related to security, including ports, base system userland and kernel topics, and system configuration.

On behalf of the FreeBSD Foundation,
Ed Maste
Senior Director of Technology