11
Dec
2009

A FOSS Perspective On Richard Schaeffer's Three Tactics For Computer Security

Federal Computer Week published a great, succinct quote from Richard Schaeffer Jr., the NSA's (National Security Agency) information assurance director, on three approaches that are effective in protecting systems from security attacks:

> We believe that if one institutes best practices, proper configurations [and] good network monitoring that a system ought to be able to withstand about 80 percent of the commonly known attack mechanisms against systems today, Schaeffer said in his testimony. You can actually harden your network environment to raise the bar such that the adversary has to resort to much, much more sophisticated means, thereby raising the risk of detection."

Taking Schaeffer's three tactics as our lead, here is a FOSS perspective on these protection mechanisms:

Best practices implies community effort: discussing, sharing and collectively building understanding and techniques for managing systems and their software components. FOSS (Free and Open Source Software) communities develop, discuss and share these best practices in their project support and development forums. Debian's package management system implements some of these best practices in the operating system itself thereby allowing users who do not participate in the development and support communities to realize the benefits of best practices without understanding or even knowing that they exist. This is one of the important benefits of policy- and package-based operating systems like Debian and Ubuntu.

Proper configuration is the tactical implementation of best practices. Audit is a critical element here. Debian packages can use their *postinst* scripts (which are run after a package is installed, upgraded, or re-installed) to audit and sometimes even automatically fix configuration problems. Right now, attentive, diligent systems administrators, i.e., *human beings*, are required to ensure proper configuration as no vendor — not even Debian — has managed to automate the validation let alone automatically fix bad configurations. I think this is an area where the FOSS community can lead by considering and adopting innovations for ensuring proper configuration of software.

Good network monitoring invokes the discipline of knowing what services are running and investigating when service interruptions occur. Monitoring can contribute to configuration auditing and can help focus one's efforts on any best practices that should be considered. That is, monitoring helps by engaging critical thinking and building a tactile awareness of the network — what it does and what is exposed to the activities of a frequently malicious Internet. So, like proper configurations, monitoring requires diligent, attentive systems administrators to maintain security. LinuxForce's Remote Responder℠ services builds best practices around three essential FOSS tools for good network monitoring: Nagios, Munin, and Logcheck.

Posted by CJ Fearnley *in* Security, Systems Management, *0 comments*