

ABSTRACT:
Hardening the Linux Kernel
Mike Weller, BAE SYSTEMS

Computer security professionals have used the reference monitors to provide security enforcement since the early 1970's. This paper considers the Linux kernel as a reference monitor that enforces security policy upon external users as well as resident applications.

Many approach hardening an operating system or kernel by applying all the latest security patches that address all published vulnerabilities. While applying the latest patches is a good thing, this paper takes the view that security is first an architectural framework. Truly hardening the Linux kernel begins with the understanding that the kernel as primarily a security policy enforcement mechanism at the very center of our security architecture.

One concept for evaluating security mechanisms uses the NEAT principle:

- Non-bypassable
- Evaluatable
- Always invoked
- Tamper proof

Hardening the Linux kernel walks through each of the NEAT attributes as it may be applied to deploying and configuring the Linux kernel for the user's environment.