Intrusion detection using system calls monitoring

Daniel Băluță, Gabriel Sandu
Computer Science and Engineering Department
Politehnica University of Bucharest
{*daniel.baluta,gabrim.san*}*@gmail.com*

Abstract

One of the recent approaches of detecting a potentially dangerous application is monitoring the system calls it makes and denying them based on custom user enforced policies. We expand this method further by trying to solve the concurrency problems that arise from working in a multithreaded or multiprocessor environment. This paper will also discuss how static analysis of the system calls can be used to predict unusual application behaviour and some of the solutions to avoiding race condition exploits by compromised applications.

Keywords: intrusion detection, system calls, access policy, trace, attack, security, monitor.

References

[1] D. Wagner, D. Dean. *Intrusion Detection via Static Analysis*. IEEE Symp. on Security and Privacy, 2001.

[2] T. Garfinkel. Traps and pitfalls: *Practical problems in system call interposition based security tools*. Network and Distributed Systems Sec. Symp., 2003.

[3] R. Watson. *Exploiting Concurrency Vulnerabilities in System Call Wrappers*. WOOT'07 First USENIX Workshop on Offensive Technologies, 2007.

[4] M. Rajagopalan, M. Hiltunen, T. Jim, R. Schlichting. *System Call Monitoring Using Authenticated System Calls*. IEEE Transactions on Dependable and Secure Computing, Volume 3, 2006.