Project Proposal

Advanced Operating Systems

Intrusion detection using system calls analysis

Daniel Băluță
danie.baluta@gmail.com

Gabriel Sandu
gabrim.san@gmail.com

We propose an intrusion detection mechanism based on system calls analysis , currently emerging two possible approaches. First one is based on analyzing typical application behavior and recognize attacks by their unusual effect through constraining the system call trace of a program's execution to be consistent with program's source code. Second one assumes that between the program running and the kernel exists a monitor that logs all system calls and according to an internal policy it decides if the system call is allowed or denied.

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

References:

Intrusion Detection via Static Analysis – D. Wagner, D. Dean

Traps and Pitfalls: Practical Problems in System Call Interposition Based Security Tools – G. Tal

Exploiting Concurrency Vulnerabilities in System Call Wrappers – R. Watson

Authenticated System Calls – M. Rajagopalan