SP Lab 1: Environment Variable and SETUID programs

School of Informatics, University of Edinburgh

Checkpoint 1. What is the usage of environment variables?

Checkpoint 2. How does a child process handle environment variables?

Checkpoint 3. How does `execve` handle environment varaibles when executing an external binary?

Checkpoint 4. What is the difference between `execve()` and `system()` with respect to environment variables handling?

Checkpoint 5. Why is your change of `LD_LIBRARY_PATH` ignored?

Checkpoint 6. How could you avoid these kinds of path attack?

Checkpoint 7. Your setting of `LD_PRELOAD` will fail in some cases, please list them and make a conclusion concerning when the linker ignores your environment variable settings.

Checkpoint 8. What is the difference between `execve()` and `system()` on handling external command usage? Which one is safer and why? Are there any attacks that can only succeed in the weaker one?

Checkpoint 9. Why does the file access still succeed even if the root privilege has been removed. What are the potential risks with this?