My Stupid Simple Presentation:

Avoiding Shell Expansion Command Line Injection

Overview

- Background: Definition of the problem
- Further Exploration of the Programmatic Problem Space
- Solution in C
- Solution in Other Languages
- Gotchas

HUTCH TVS

Background

- Shell meta-characters like & && ; |
- System(3)
- system(“mail -s 'Thanks for signing up'” + user_email)

Programmatic Problem Space

- Programmers should be afraid of this
- Use library when you can (zlib anybody?)
- Robust programming should capture results and act on results
  - stdout (did it succeed)
  - Exit status
  - stderr (what was the error?)

Solution

Don't use the shell to launch programs!

DUH

Launching Outside Programs Effectively (in C)

- int pipe(file_descriptors[2]);
- int fork;
- int exec***(executable_path, args, …);
- int waitpid(pid_t pid, int *status-ptr, int options);
- Win32: http://msdn.microsoft.com/en-us/library/ms682499.aspx

Other Languages

- Python: exec***(); spawn***(); subprocess;
- Ruby:
  - 1.8 exec()
  - 1.9 exec([env],...); spawn([env],...)
  - Alternatives: Open3, Open4
- PHP: string escapeshellarg (string $arg)
- Java: exec() overloaded

Gotchas

- Flush Your Buffers!
- Env
- Know your command (tar --info-script F)

©Jeremiah McCann (2009)