Blog: Hacking myself to prove a point

- https://www.macchaffee.com/blog/2023/hacking-myself/

Binary OS security (process with full user permissions OR root) is becoming a big problem. If you get execution on desktop OS as the user running it, it is all over.

Developers run lots of untrusted code during their work. While browsers sandbox untrusted code (with many security issues), developers run untrusted code directly.

OS design from 70' is not helping here.

If only we had Plan9 today, each application has it's own namespace (like docker on Linux), that can be arbitrarily nested without root privileges. Plan9 does not need root at all since there is no global namespace state to manage (all is per process); on Linux/UNIX you need root to manage namespaces (file systems/VFS, networks, processes etc.).

Another nice aspect of Plan9 in this context would be its ability to transparently run computation on separate computers over network. You can trivially run compilation on compilation farm, separated from your PC. This could be used to mitigate such vulnerability.

Revision #3
Created 2023-01-25 10:40:09 GMT by hxd
Updated 2023-01-25 11:27:48 GMT by hxd