Object Capabilities, ACLs & Sandboxing

Capabilities

- Public keys are capability to send you a message that you can grand by giving the key
- Capabilities can be forwarded - external system like trust needs to be used
- Capabilities needs to be revocable - single key per capability granted

Confused deputy problem

UNIX security

- https://wiki.alopex.li/LetsBeRealAboutDependencies

> what we actually want for robust, reliable infrastructure is an environment and API that deals with all the above stuff one way or another, and provides explicit, deny-by-default control of everything programs are allowed to do, a la a capability system. Linux is not this, but people keep trying to turn Linux into that with tools like Docker. I think that if an API like WASI or such ever gets popular, that has these properties designed in from the start, life will become much better. Making such a system that is actually nice for humans to use interactively is still a problem, but a different problem.)

- https://github.com/netblue30/firejail/wiki/Frequently-Asked-Questions

Implementations

- https://forgefed.org/blog/stabilizing-ocaps/

Revision #4
Created 2023-05-09 21:05:09 IST by hxd

Updated 2023-06-12 19:06:41 IST by hxd