AppArmor Beginner's Workshop

György Demarcsek

https://tiny.cc/apparmor-bsideslux

@gdemarcsek

PGP: 5033679CB2DBB024

IBM

Setup (USB) – With Vagrant

1. Make sure that port 8080 is free to bind to on your host machine
2. Copy all the files to a directory
3. Install VirtualBox and Vagrant from tools/ if you do not have them
4. `cd workshop && vagrant box add --force --name bsideslux18/apparmor virtualbox-gdemarcs-bsideslux18.box`
5. `cd bsideslux18 && vagrant up && vagrant ssh`

https://tiny.cc/apparmor-bsideslux

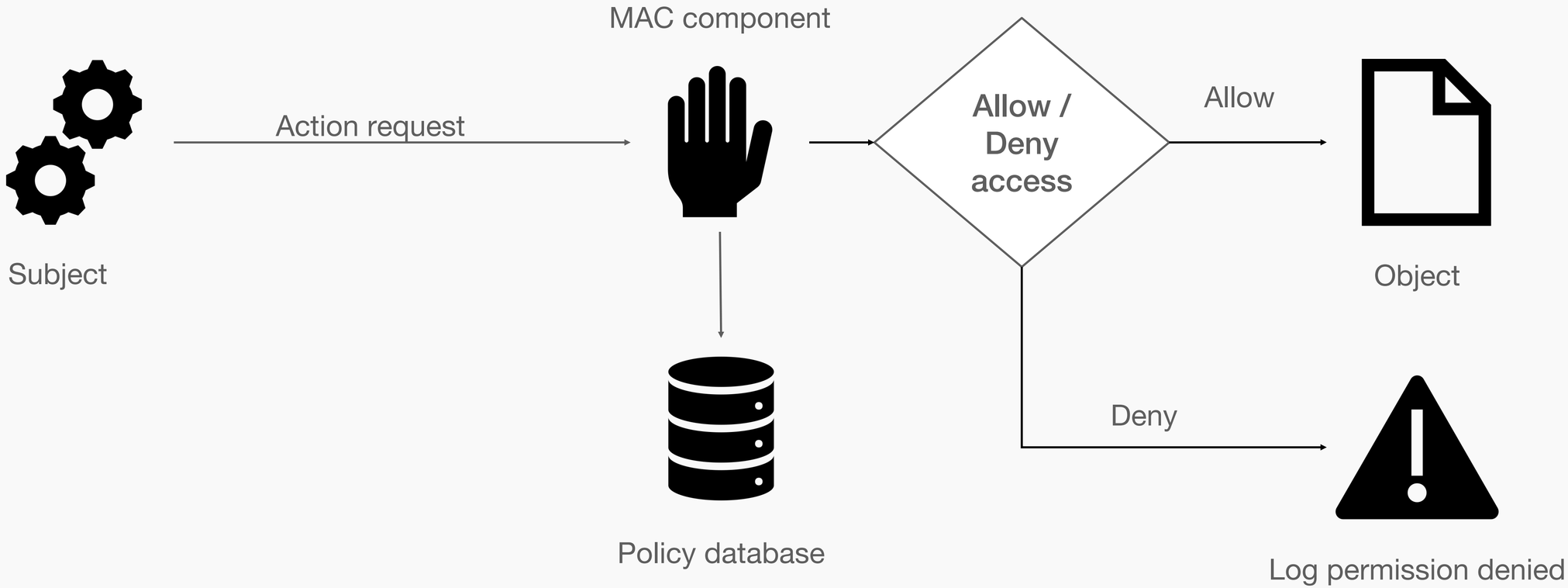
Setup (USB) – Without Vagrant

1. Copy all the files to a directory
2. Install VirtualBox if you do not have it already
3. Import the OVF file from the workshop directory (double click) & start the VM
4. Show the VM in VirtualBox and log in with username **vagrant** and password **vagrant** to Gnome Shell
5. Open Gnome Terminal

https://tiny.cc/apparmor-bsideslux

IBM

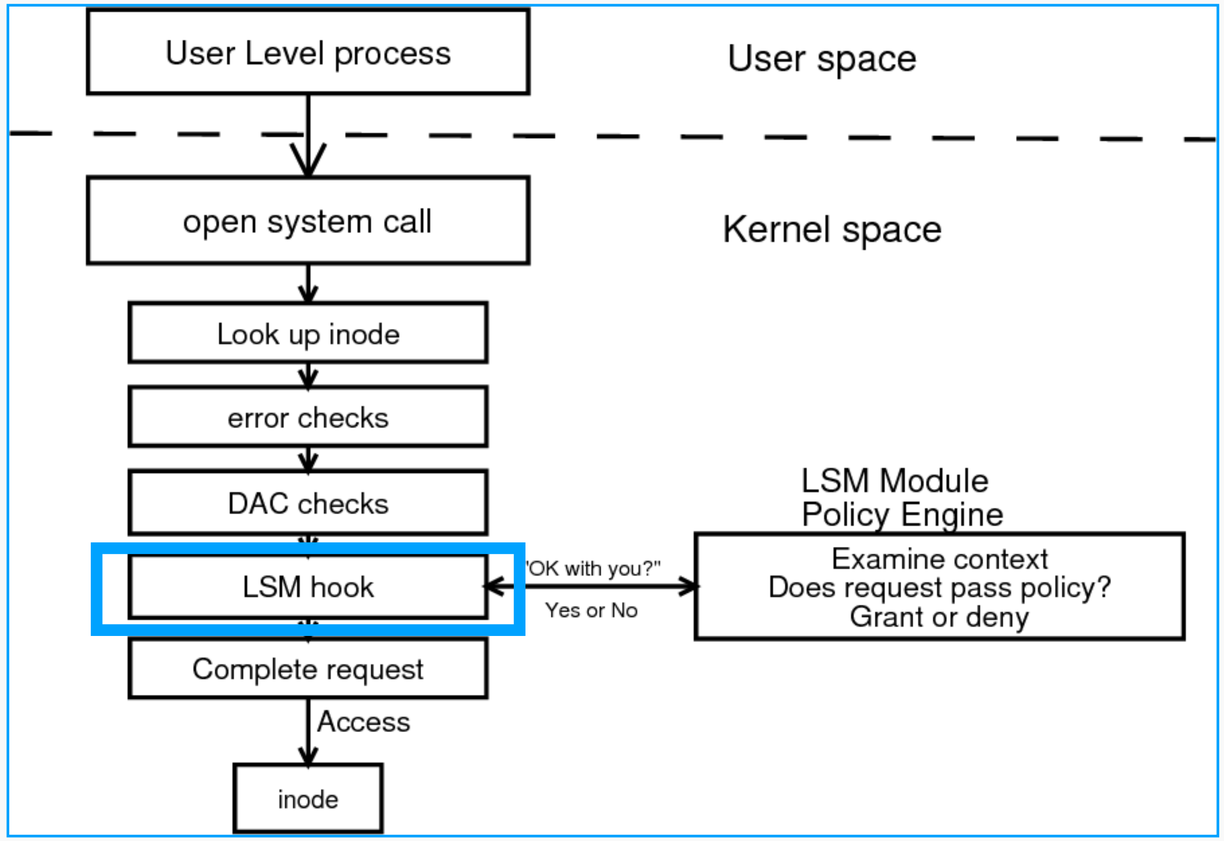
Mandatory Access Control



https://tiny.cc/apparmor-bsideslux

IBM

Linux Security Modules



- Framework designed to enable additional mediation of access to kernel resources
- Hooks in syscall impl
- Stop & fail / propagate execution
- Examples: AppArmor, SELinux, TOMOYO

https://tiny.cc/apparmor-bsideslux

IBM

AppArmor Confinement Model

- Targeted
- Path-based policies
- Default deny
- Complain and enforce modes
- Profile language: files, network access, capabilities, IPC, resource limit

Use cases

- Reduce attack surface (pre and post exploitation)
- Detect intrusion attempts or otherwise anomalous behaviour
- Understand what your processes do (especially your third-party dependencies...)

https://tiny.cc/apparmor-bsideslux

Lab work

Let’s start experimenting with AppArmor together!

Just as good as your profiles

- /etc/cron.d/** w,
- **capability sys_module, # caveats/sys_module.c**
- capability sys_ptrace,
- File descriptor leakage on exec (O_CLOEXEC)
- **Rename problem (https://bugs.chromium.org/p/project-zero/issues/detail?id=1676) # caveats/rename.c**

IBM

Thank you!

Questions?