App Armor and SE Linux

Author: Stefan Alfeis, stefan.alfeis@quant-x-sec.com
Translation: Jeremias Bogomolec, jeremias.bogomolec@quant-x-sec.com

SE Linux and App Armor

The two systems SE Linux (System Enhanced Linux) and App Armor belong to the so-called MAC-Systems in Linux. MAC stands for Mandatory Access Control and it extends the so-called Discretionary Access Control (DAC). To shortly outline this, DAC grants access to resources on the basis of user roles and MAC expands on this principle by imposing rules on each respective resource instead of granting a specific user access rights. Both systems are part of the expanded Linux Security Modules (LSM), which have been anchored in the Linux-Kernel since 2003. LSM is a Security Framework that has been conceived for the Linux-Kernel with the goal of being a generic interface for the MAC.

SE Linux

SE Linux's development was pioneered by Red Hat, and even the NSA participated in its development significantly. SE Linux is a complex system of roles, identities, domains and contexts. Every object of a system is assigned a type. The sort of each respective type is appointed within the extended attributes of the file, which are appropriately named "Extended Attributes". This is where the limitation of SE Linux, to only be applicable on systems that support Extended Attributes, originates from. To summarize: Every admin should remind themselves that on systems with SE Linux the access control occurs per file and per user.
At every login on a system, each user automatically possesses their SE-Linux-Identity and a username. A role, which allows the user to move within an assigned domain, is automatically attached to this identity. So identity, role and domain are interconnected. SE Linux allows users to perform various roles. With every role the domain changes and all programs, that the user executes run in the respective domain of the role, which the user had during the program's initialization. Due to this everything can quickly become very confusing. SE Linux demands a high degree of settings from the administrator, in order to provide all users with the programs they need to use.

App Armor

App Armor was originally founded by SUSE, but is by now also being developed and improved by the Ubuntu developers. One of the reasons for App Armor was the great complexity of SE Linux. Just like SE Linux, App Armor is based on the LSM and also differentiates for every single file whether a demanded access is permitted or not. However, App Armor does not differentiate by users, roles and domains are also not incorporated. It also has no requirements for the file system since it does not utilize Extended Attributes. Therefore App Armor is less limited within the usage of file systems.
It grants access to an object using the file path within the system, the rules for this are defined

inside the so-called "Profiles". The App-Armor-Profile determines the access rules within the system. App Armor knows three modes for its Profiles:

complain: "learning mode" actions, that violate rules are only logged and not prohibited
enforce : "enforcement mode" actions, that violate rules are logged and prohibited
audit : "audit mode" all rule applications and rule violations are logged

App Armor brings a list of profiles with itself, but it is also possible to create one's own Profiles. If you choose to do this tread carefully though, since briefly created Profiles can make the execution of programs impossible or threaten the security.

Conclusion

Both SE Linux as well as App Armor raise the security level on their respective systems.
SE Linux is much more powerful, but has the drawback of its heightened complexity and being difficult to operate.
App Armor requires far less preparatory groundwork, but also has less setting possibilities than SE Linux.
Both systems should however be cleanly adjusted by the administrator, instead of deactivated, when an object access fails.

Sources:

https://wiki.ubuntuusers.de/AppArmor/
https://debian-handbook.info/browse/de-DE/stable/sect.apparmor.html https://apparmor.net/ https://de.opensuse.org/AppArmor https://www.linux-magazin.de/ausgaben/2018/02/app-armor-se-linux/ https://www.redhat.com/de/topics/linux/what-is-selinux https://debian-handbook.info/browse/de-DE/stable/sect.selinux.html https://www.admin-magazin.de/Online-Artikel/Mandatory-Access-Control-MAC-mit-SE-Linux