Improving SEAndroid policies: SELint

Filippo Bonazzi, Elena Reshetova, N. Asokan

Aalto University

Collaborative Research Institute for Secure Computing

Android OEMs make mistakes when writing SEAndroid policies

Tools needed to help spot errors, misconfigurations

SELint makes suggestions to improve a source policy

SELint can simplify and speed up analyst workflow


The Register®
Biting the hand that feeds IT

DATA CENTRE SOFTWARE NETWORKS SECURITY INFRASTRUCTURE DEVOPS BUSINESS HARDWARE

Security

OEMs still the Achilles heel of Android security, say boffins

Mobe-makers just can't be bothered keeping Google-spawn up to date

http://www.theregister.co.uk/2015/10/26/oems_still_the_achilles_heel_of_android_security_say_boffins/

OEM SEAndroid policies

- significantly modify default AOSP policy
- include results from automatic tools (e.g. *audit2allow)*

This results in several mistakes:

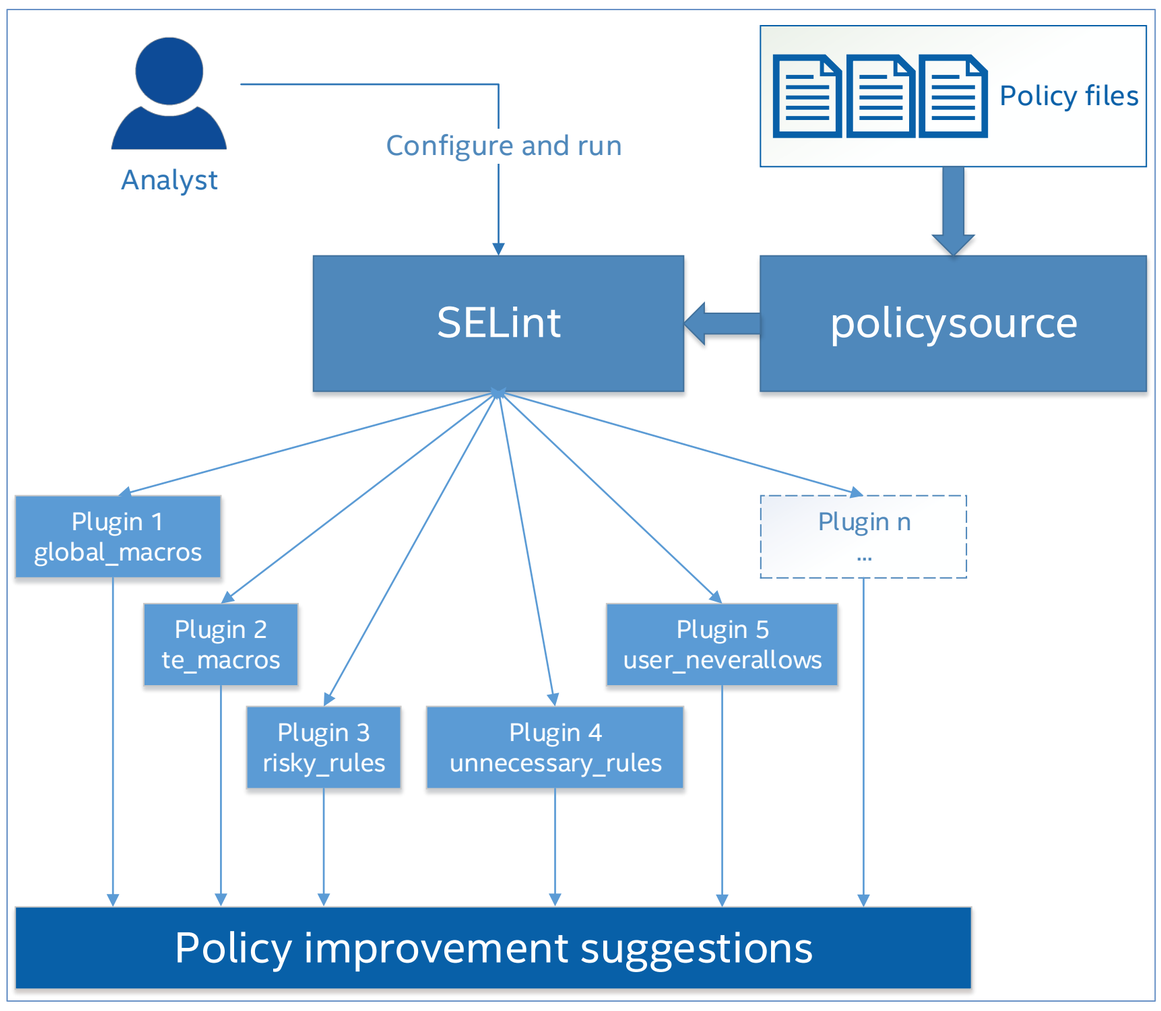
- Unnecessary/leftover rules
- Potentially dangerous rules
- Overuse of default domains/types

Also due to lack of relevant tools that

- work on source policy
- incorporate knowledge of common flaws
- do not require expert knowledge

Goal: A tool to help OEMs develop better SEAndroid policies

- **SELint**



SELint: source policy improvement suggestions

Our idea: develop semi-automated tool to simplify and speed up analyst workflow.

- Realize plugin architecture to support custom 3rd-party analysis requirements
- Develop "core" set of plugins to provide generally useful functionality
- Enable community contribution of new plugins and extended knowledge base

SELint performs checks on a source policy by loading analysis plugins:

- Suggest using M4 macros where applicable
- Report potentially dangerous rules
- Report unnecessary or ineffective rules
- Assert custom neverallow rules
- ...

https://ssg.aalto.fi/projects/selint/

Intel CRI for Secure Computing