Contribution ID: **193** Type: **not specified**

Improving SEPolicy Development Experience

Monday, 24 August 2020 10:15 (15 minutes)

Despite having capabilities to specify access control at a high level of granularity, SEPolicy is typically added in the development process as an afterthought; to accord the same permissions to a given set of processes that were developed with no regard to access restrictions. On Android - where SEPolicy operates in mandatory access control (MAC) mode - OEMs typically rely on tools such as audit2allow to help speed-up the development process and end up with scenarios where vendor and system applications are given more privileges than necessary for correctness. In these cases instead of utilizing SEPolicy to implement a security blueprint, rules are modified to pass restrictions. On Android, abuse due to vendors granting excessive permissions is prevented by neverallow checks and xTS requirements. However tests such as xTS are done at the end of the cycle versus at the beginning of vendor/OEM application design.

This talk focuses on the tools lacking for SEPolicy development, the approach with which such tools may be developed and shares our experience in developing tools to analyze and model SEPolicy.

I agree to abide by the anti-harassment policy

I agree

Primary author: CHALLAKERE, Nagaravind (Microsoft)

Presenters: CHALLAKERE, Nagaravind (Microsoft); CATTELL, Shaylin

Session Classification: Android MC

Track Classification: Android MC