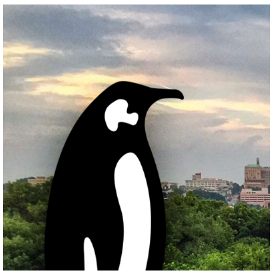

Contribution ID: **206**

Type: **not specified**

Securing build platforms

Tuesday, 14 November 2023 09:30 (40 minutes)

The software chain of trust —that source code, actors, and outputs all meet (often implicit) expectations when placed under scrutiny —is an area of growing concern. Accidental or malicious tampering with the chain of trust can result in security issues, failure to comply with software licences, inexplicable errors and more.

Linux distributions reduce the number of trust decisions consumers have to make, but how is trust in a distribution and its chain of trust evaluated such that consumers feel confident consuming otherwise opaque blobs?

npm have adopted SLSA and Sigstore to produce build provenance, which provides a non-falsifiable link from source code to built package. However, npm package builds are much simpler than many distribution builds (even before one considers bootstrapping toolchains). Further, the use of GitHub Actions and Sigstore in npm's architecture may not be technically or socially feasible in many established communities.

Can we map this technique to distribution build platforms? SUSE and Flatcar Linux have started down this path, but both have unsolved issues around verification which prevents consumer adoption for evaluating trust.

This topic would aim to introduce the motivations for securing build platforms, discuss approaches language ecosystem registries are taking, and explore how we might adapt and adopt these solutions for Linux distribution build platforms. Examples and demos will be focused on OpenEmbedded/Yocto Project through the submitters proof of concept experiments integrating these concepts in the yocto-autobuilder2 system.

Primary author: LOCK, Joshua (Verizon)

Presenter: LOCK, Joshua (Verizon)

Session Classification: Build Systems MC

Track Classification: LPC Microconference: Build Systems MC