rebuilding builders instead of trusting trust ☆

.ical (/nixcon-2024/talk/AS373H.ics) (/nixcon-2024/talk/AS373H/feedback/)

2024-10-25 17:05–17:50, Arena

The key principles Nix is built on are great for supply chain security.
Those principles could take us much further, if we extended or replaced the signatures that provide transport security for binary caches today, in favor of a more powerful mechanism.
A mechanism that works end to end from builder to user, includes provenance data about the builder, and ideally makes that provenance data verifiable.

Adopting Trustix, or extending the existing signing scheme are both possible ways to add builder provenance data, but comparing those options is not the focus of my talk.
Instead I would like to focus on the kind of data that we might want to add, and the benefit we would obtain.
This starts simple with a boolean flag, which lets signers claim to have built a derivation themselves, all the way up to a source link and remote attestation, which make it possible to verify which software is running on the builder.

What level of experience in Nix is the talk addressed to? –
This session is aimed at more advanced Nix'ers, who are interested in security.

Do you allow your talk to be recorded? – yes
See also:

- Paper (https://www.digidow.eu/publications/2024-schwaighofer-scored/Schwaighofer_2024_SCORED24_CloudBuildSystemsTrust.pdf)
- Slides (385.3 KB) (https://talks.nixcon.org/media/nixcon-2024/submissions/AS373H/resources/nixcon2024-rebuilding-builders_KXEA1Ss.pdf)

(/nixcon-2024/speaker/HMYGKG/)

Martin Schwaighofer (/nixcon-2024/speaker/HMYGKG/)

Martin Schwaighofer is a PhD student at JKU in Austria, interested in proving the link between a running system and it's source code.

This speaker also appears in:

- hashes all the way down (/nixcon-2024/talk/RDZVFH/)