Saal: Project 16:00 01:00 Day: 1 Track: Security & Hacking nA 2501

Title: **How to make your software build reproducibly**

Subtitle: Get a verifiable path from source to binary

Speaker: **Lunar**

Short: *Auditing source code is not enough when build tools are themselves a target. When software can be built reproducibly, anyone is enabled to verify that binaries have actually been made from the source code they claim to be made from. The lecture will present several tricks learned while trying to make Debian the largest collection of free software build reproducibly.*

Long: Free software gives us the possibility to verify its behavior by looking at the source code. However, what we use most often are distributed binaries. How can we make sure they have actually been made from the source code they claim to be made from? When builds are deterministic or reproducible, anyone can recreate a byte-for-byte identical result, preventing hard to detect compromises. Reproducible builds require a way to record and recreate the build environment, and then build processes themselves need to be made deterministic. An effort to make Debian packages build reproducibly has been on-going for the past two years. Several lessons were learned from these experiments that will be shared with the audience.