Private Computing on Open Infrastructure: Zero-Knowledge Proofs and the Aleo Platform

- **Speaker**: Michael Venema
- **Room**: CC 203
- **Time**: Sat 2:00 pm – 2:30 pm

- **Format**: Lecture (30 Min + Q&A)
- **Difficulty**: Some experience required
- **Track**: Security / Privacy
- **Presenter Location**: In-person
- **Experience**: first time speaking
- **At**: at lfnw

Description:

Privacy and decentralization are core to the free/libre and open-source philosophy, but implementing them securely at scale remains a major challenge. This session introduces how **zero-knowledge proofs (ZKPs)** enable private computation on public systems, using the **Aleo platform** as an open-source example.

Attendees will learn how ZKPs allow verification of computations without revealing underlying data, how Aleo integrates these proofs at the protocol level, and what developers can take away from its architecture—even if they never touch a blockchain. The talk focuses on practical privacy-engineering concepts, open-source tooling (including the **Leo** programming language), and how these techniques can enhance user trust in distributed and Linux-based environments.

Participants will leave with a solid understanding of ZKP fundamentals, privacy-preserving design patterns, and how to apply Aleo’s open-source components to build secure applications—no token speculation required.

Target Audience:

- Developers
- Sysadmins
- Open-source enthusiasts interested in privacy-preserving computation, cryptography, or distributed systems