A LATTICE COMPANY

OpenPRoT in Action: PLDM Firmware Update

Open standards. Hardware-verified trust.

BMC firmware updates today still largely rely on vendor-specific tools and protocols, with no standard that works everywhere.

"Every platform is a custom integration."

Solution Overview

OpenPRoT runs on a Root of Trust hardware device, protecting the firmware of downstream devices (for example, BMC, CPU, GPU, and NIC). It verifies every update before it is applied, with automatic recovery built into the architecture.

Demo:

A real firmware update to a representative BMC target, leveraging a standards-based methodology using PLDM Type 5.

Key Benefits

- Standards-based: Interoperable across vendors
- Hardware protection: the Root of Trust verifies updates, not the downstream device
- Fail-safe by design: Automatic recovery built into the architecture
- Open source, fully auditable
- Built with industry collaboration (AMD, AMI, ASPEED, Google, Insyde, Jabil, 9elements, Nuvoton, and others)

Key Features

- PLDM Type 5 Firmware Device
- Verify-before-commit flash updates
- Fully configurable for different device types with support for:
  - Redundant flash devices or partitions
  - Recovery devices or partitions
  - Anti-rollback protection
  - Image transfer over PLDM interface or dedicated staging area
- Fully open source and customizable (Apache License v2.0)

For more information, visit **github.com/OpenPRoT/openprot**