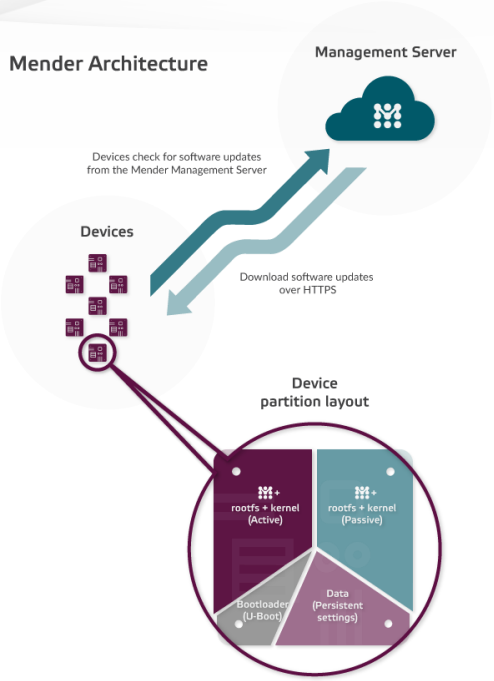
MENDER



Over-the-air (OTA) software updates for embedded Linux devices: an end-to-end open source updater

Why Mender?

1. Built from the ground up with security in mind, Mender enforces secure HTTPS connections and has zero open ports on the device
2. Avoid bricked devices with automated rollback support
3. No vendor lock-in with the only end-to-end open source OTA updater with both server and client licensed under Apache 2.0

A tangible threat to IoT

The growing connectivity of embedded systems is causing justified apprehension in bringing new devices online. Many malicious attackers specifically scan for recently published security vulnerabilities with the intent of seeking outdated and vulnerable systems and devices. Malware - such as Mirai, Hajime, BrickerBot, and Reaper - have successfully targeted insecure embedded Linux systems. The number of compromised devices are in the millions and growing. DDoS attacks have increased 91% in 2017 due to insecure IoT devices.

> At 40-60 days, the probability of a vulnerability being exploited reaches over 90%

A key finding by Kenna Security is at 40-60 days, the probability of a vulnerability being exploited reaches over 90%. If the vulnerability is remediated within 5-10 days after discovery, that number drops to under 10%.

Building a homegrown updater seems easy at first glance, but many custom updaters are built without security in mind. They also lack a robust update process where the devices are at risk of bricking if there is power failure or poor network connectivity during the update.

Solution

Mender is an open source project to deploy OTA software updates across your fleet of Linux devices:

- Open source without vendor lock-in for both the client and management server
- Device groupings for controlled rollouts
- Dual A/B root filesystem updates with rootfs compression to save bandwidth
- Full image atomic updates, avoiding the unmanageability of a package-based approach or complications from partial updates
- Scripting support for custom actions (e.g. custom sanity checks after the update is installed)
- eMMC, SD card, and raw NAND/NOR flash support
- OTA and standalone (without server) deployments

Security and Robustness

- Secure TLS client/server communication
- End-to-end signing and verification of image artifacts for authenticity and integrity
- Automated rollback support with a dual A/B partition setup if an update fails for any reason
- Root filesystem integrity check to avoid corruption

Operating System & Board Support

Mender currently supports Linux-based devices that use U-Boot and provides a feature layer for the Yocto Project for easy integration with Yocto-based projects. Mender can be integrated into other Linux distributions (e.g. OpenWRT, Buildroot, Debian) on demand – contact us for more details.

Mender has the Raspberry Pi 3 and the BeagleBone Black as reference devices. Support for a virtual device using QEMU is provided for development and testing purposes.

Contact us for further guidance on supporting other OS distributions and boards. Integrating Mender into additional Yocto-supported platforms is easy - requiring minimal updates to the meta-mender and platform layers.