Linux Plumbers Conference 2019

Contribution ID: **55**

Type: **not specified**

What does remote attestation buy you?

Monday 9 September 2019 15:00 (45 minutes)

TPM remote attestation (a mechanism allowing remote sites to ask a computer to prove what software it booted) was an object of fear in the open source community in the 2000s, a potential existential threat to Linux's ability to interact with the free internet. These concerns have largely not been realised, and now there's increasing interest in ways we can use remote attestation to improve security while avoiding privacy concerns or attacks on user freedom.

More modern uses of remote attestation include simplifying deployment of machines to remote locations, easy recovery of systems with nothing more than a network connection, automatic issuance of machine identity tokens, trust-based access control to sensitive resources and more. We've released a full implementation, so this presentation will discuss how it can be tied in to various layers of the Linux stack in ways that give us new functionality without sacrificing security or freedom.

I agree to abide by the anti-harassment policy

Yes

Primary author: GARRETT, Matthew (Google)

Presenter: GARRETT, Matthew (Google)

Session Classification: LPC Refereed Track