# A short introduction to System Transparency

Fredrik Stromberg,
Mullvad VPN, mullvad.net.

**Abstract.** Computer security exists to facilitate trust, and a fundamental part of security is system integrity. Unfortunately, computer systems are rife with vulnerabilities, and the endless stream of patches serve both as immunization as well as recipes for exploitation. Administrators are in recurring races to patch before attackers exploit.

Even with a good patching story, a system, once compromised, is often costly to get back to a secure state. A lack of trustworthy audit trails may prevent discovering the initial cause of the breach resulting in inadequate mitigations. Unfortunately, systems also offer places to hide and gain malware persistence. The technical challenges involved in maintaining system integrity with a relatively high assurance prevent most organizations from doing so.

This lightning talk introduces a novel design approach for computer systems intended to offer deterrence, prevention, and detection of attacks as well as a possibility to prove to the owner, system administrator, user, or a third party exactly what is currently running on the system and what it has been permitted to run in the past.

System Transparency facilitates trust in the hardware and initial state of the system through a provisioning ritual and tamper detection which together with a TPM and firmware write-protection establishes the root-of-trust as well as prevents malware persistence. It requires reproducible builds in combination with immutable infrastructure which help deter and prevent malicious modification during the build stage as well as during runtime. It furthermore requires remote attestation of the boot chain in combination with a transparency log which provide assurances of the current system configuration, as well as an audit trail of previous configurations. If a machine using System Transparency is compromised due to an unpatched application, it can reboot, load an updated system image, and attest its new, patched, and uncompromised boot chain to its users.

**Keywords:** system transparency, privacy, trusted computing, provisioning ritual, tamper detection, tpm, reproducible builds, immutable infrastructure, remote attestation, certificate transparency