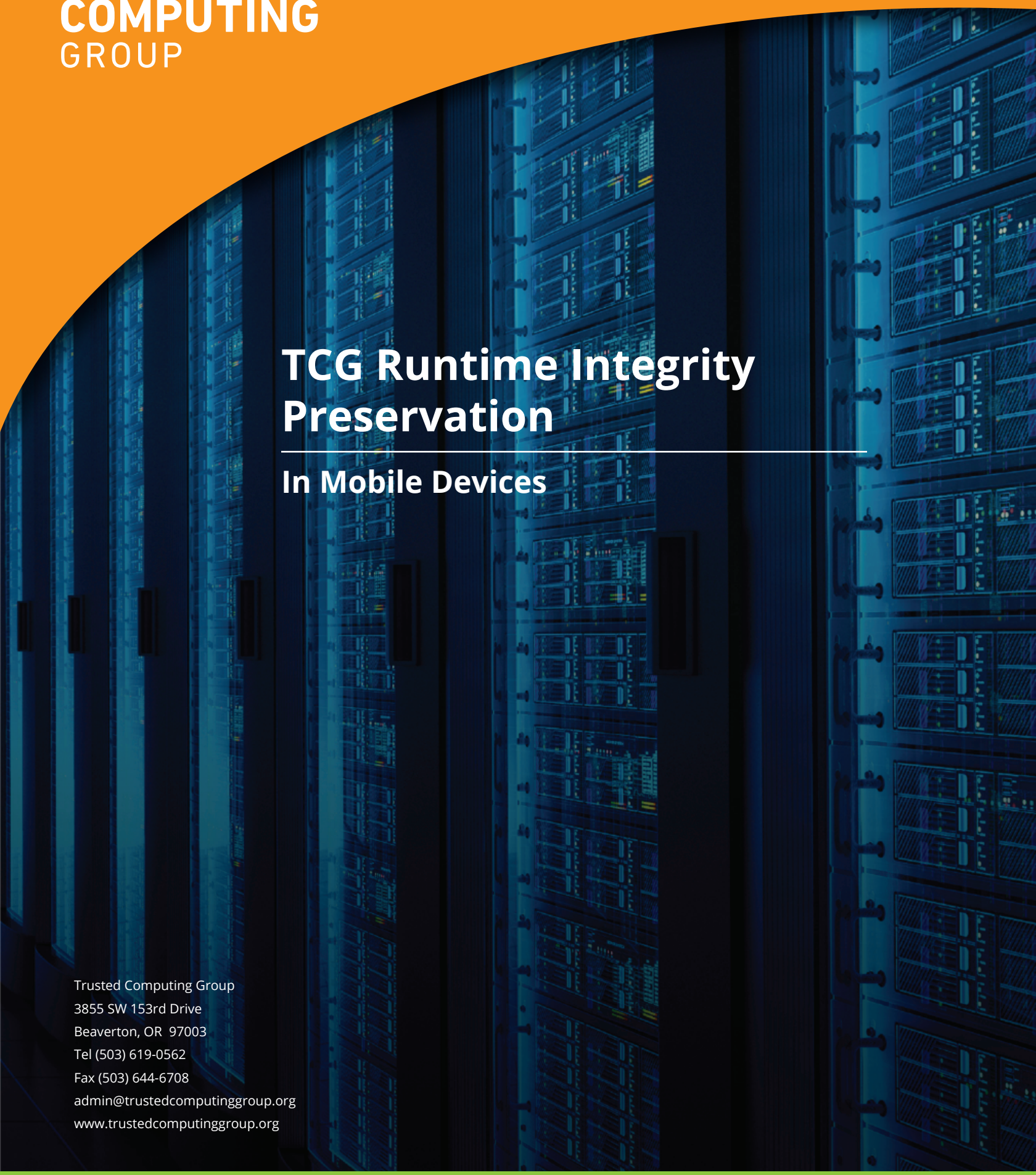
TRUSTED® COMPUTING GROUP

JANUARY 2020



TCG Runtime Integrity Preservation

In Mobile Devices

Trusted Computing Group
3855 SW 153rd Drive
Beaverton, OR 97003
Tel (503) 619-0562
Fax (503) 644-6708
admin@trustedcomputinggroup.org
www.trustedcomputinggroup.org

OVERVIEW

Most people today use their mobile phones as their primary computing device, conducting day-to-day business ranging from mundane to sensitive. People have come to rely on their devices to be secure and to behave as expected. At the same time, mobile devices represent valuable targets for malicious activity. The challenge for mobile security experts is to design and implement devices with secure architectures and protections commensurate with the mobile threat.

Platform integrity is a fundamental requirement for the security of mobile devices. The TCG Runtime Integrity Preservation in Mobile Devices (RIP) addresses the challenge of platform integrity by recommending best practices and mechanisms to preserve the critical portions of the runtime state of mobile devices.

RUNTIME INTEGRITY

Modern mobile devices use secure boot to ensure they startup in an expected state. Runtime integrity preservation ensures that the device continues to behave in an expected manner following a successful secure boot. This capability is particularly relevant because mobile devices operate for weeks or months after each secure boot. While mobile device state changes as the user installs and executes apps, some parts of the mobile device state can be evaluated with respect to their integrity. RIP provides recommendations for policies and mechanisms for the enforcement and assessment of platform integrity of mobile devices during operation. RIP also provides recommendations for the remediation of platform integrity compromises.

IMPLEMENTING RUNTIME INTEGRITY PRESERVATION

The recommendations in this document target designers, developers, implementers, and integrators of trusted computing technologies in mobile devices. The core recommendations address security policy, pre-boot considerations, platform integrity assessment, platform integrity enforcement, and platform integrity remediation as well as advanced control- and data-flow integrity solutions.

The document also describes static and dynamic runtime integrity preservation mechanisms as examples of valid implementations of the recommendations. The figure below provides an example of high-level architecture of a mobile device that implements RIP. There are numerous ways to implement the recommendations of RIP with this or alternate architectures. The figure highlights direct RIP components in blue. In the rich environment, the RIP Monitor initiates integrity measurement or remediation and can send platform posture reports via a Trusted Network Connect (TNC) client. The RIP Driver provides mechanisms for remediation, such as application restart or device reboot. A Hardware Security Module can provide hardware support for integrity measurement. The figure highlights components that support RIP in orange. These components provide mechanisms that support RIP, such as secure storage, integrity enforcement, and control- and data-flow integrity solutions.

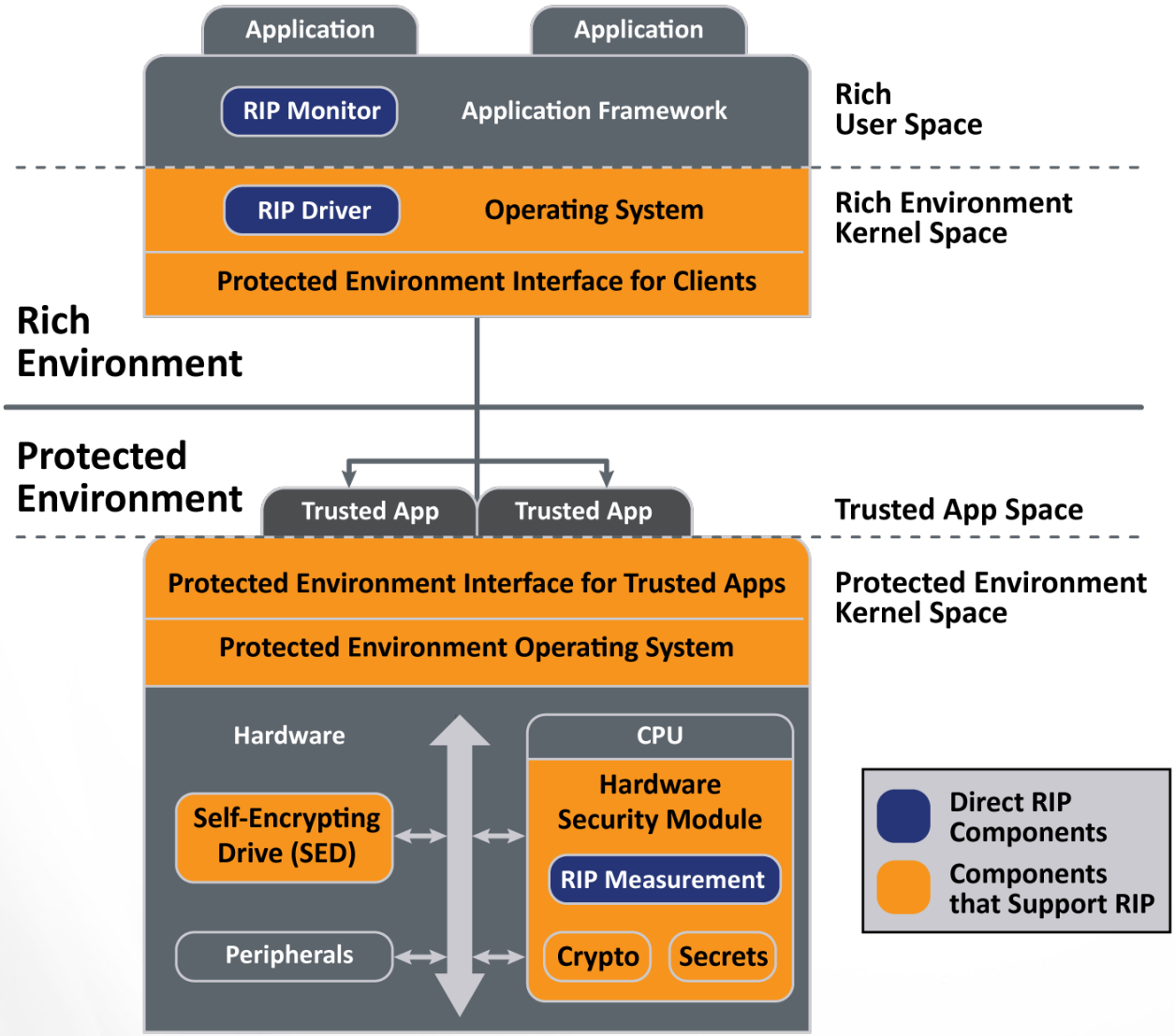


Fig 01: Example of high-level architecture of a mobile device that implements RIP

Mobile device stakeholders should consider the RIP recommendations in order to leverage them in secure architectures and applications. Mobile device manufacturers and enterprise administrators can establish security policies that identify the critical portions of a device's runtime state and the entities authorized to modify that state. Designers, developers, implementers, and integrators can provide RIP mechanisms on the mobile device that prevent or detect and remediate runtime state modifications made by unauthorized actors.

LEARN MORE:

Visit https://trustedcomputinggroup.org/ or email TCG Administration (admin@trustedcomputinggroup.org) for more information