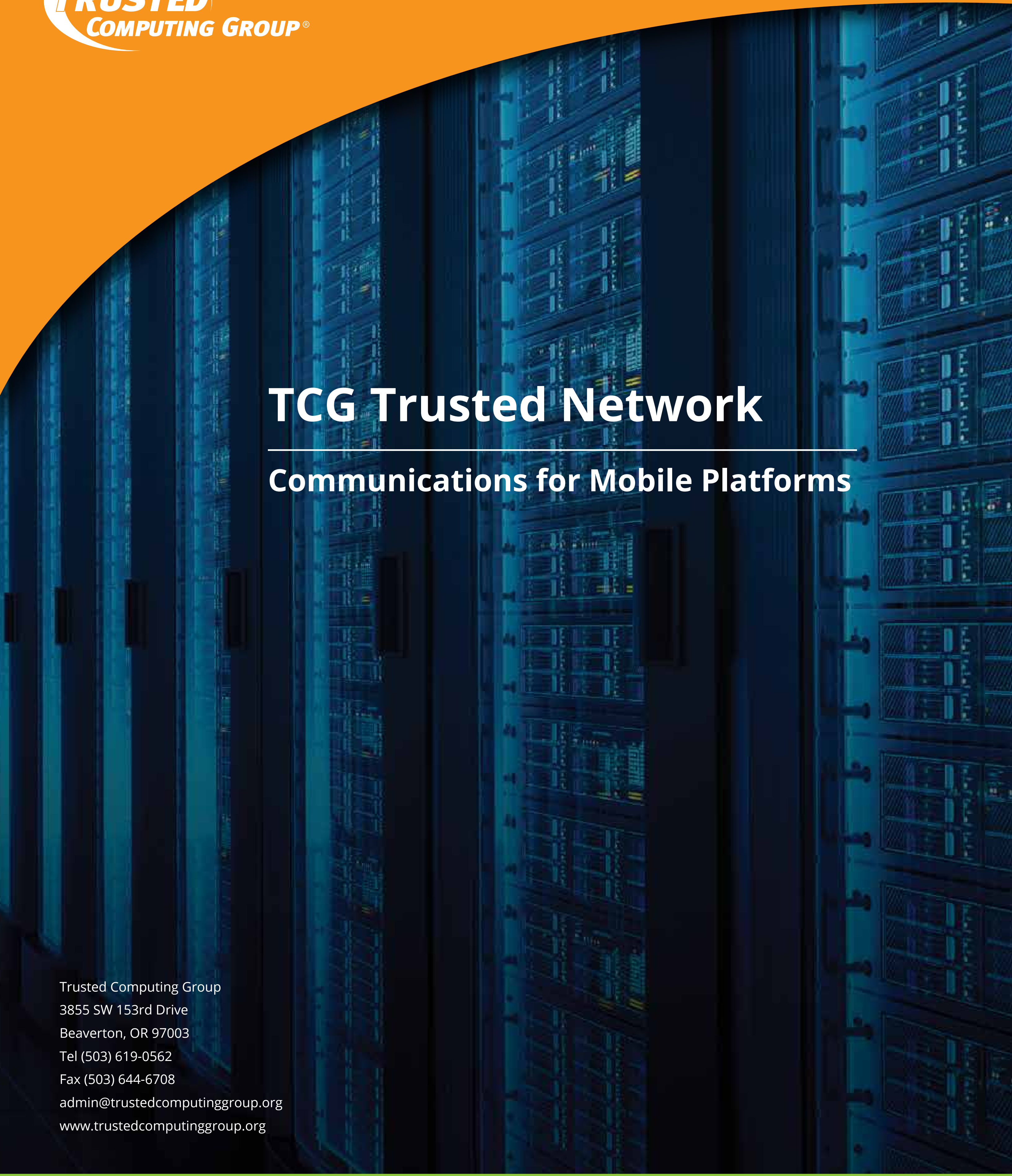
JUNE 2018



TCG Trusted Network

Communications for Mobile Platforms

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

INTRODUCTION

Wireless mobile devices face many of the same threats that target traditional endpoints and their software is subject to similar types of vulnerabilities that attract malicious activity. Insecure devices are a threat to the security and privacy of device owner/users. In addition, insecure devices can also be vectors for attacks against the mobile networks to which they are connected. Thus, both for the protection of their users and for the protection of their own services, mobile network and service providers need to be able to detect and respond to insecure and compromised devices. To offer the desired convenience without sacrificing the security and privacy of their users, network and service providers need some level of assurance that a mobile device is healthy (uncompromised) and can be trusted before allowing access to their services. This requires a way to measure the health of a mobile device and a means to convey the measurements to authorized parties. To address these and other challenges, the Trusted Computing Group (TCG) is developing standards-based solutions to mobile device trust and security issues.

MOBILE PLATFORM ARCHITECTURE

FOUR IMPORTANT CONCEPTS FOR SECURING MOBILE DEVICES INCLUDE:

1. MOBILE ROOTS OF TRUST (RoT)
2. SECURE BOOT
3. MEASURED BOOT
4. PROTECTED ENVIRONMENT

TCG's solutions are based, in part, on the expertise of members and their insight into the hardware and software aspects of targeted systems. The Mobile Platform Work Group (MPWG) has published multiple specifications focused on improving the trustworthiness of mobile devices. In particular, the MPWG has advanced four important concepts for securing mobile devices:

- Mobile Roots of Trust: A Root of Trust (RoT) is a component that performs one or more security-specific functions, such as measurement, storage, reporting, verification, and/or updates.

- Secure Boot: Secure Boot **[2]** is a process in which every software image is validated before execution.

- Measured Boot: In Measured Boot **[2]**, the TPM securely stores and protects the measurements of each code module after they are loaded and measured.

- Protected Environment: A Protected Environment is a functional element that has execution and memory resources that are isolated from other components of a mobile device in order to host sensitive applications that require security and privacy properties **[2]**.

Together, these capabilities are critical to the security of mobile devices because they support important security functions, including device integrity, attestation, isolation, and confidentiality.

TRUSTED NETWORK COMMUNICATION (TNC) ARCHITECTURE

TCG's TNC is an open architecture to support network access control and security automation. TNC standards integrate security tools across endpoints, networks, and servers into an intelligent, responsive, coordinated defense. The TNC Architecture offers capabilities in three distinct security areas:

- **Compliance** evaluates an endpoint's adherence to network policy both at the time of connection and on an ongoing basis while it is connected to the network;
- **Orchestration** provides a dynamic repository and notification service for real-time state and events; and
- **Access Control** manages the use of protected resources and networks based on endpoint posture and other factors.

These capabilities can be used for many purposes, including security automation, continuous monitoring, asset management, endpoint compliance assessment and enforcement, protection of critical resources, leveraging of shared information, and event correlation and assessment. Application of these capabilities enables trusted network communications - the ability to understand the trustworthiness of an endpoint before and while it is allowed to communicate on the network.

The combination of TCG's Mobile and TNC technologies provides a powerful set of tools to those interested in better securing mobile networks. The following examples identify some mobile network challenges and potential solutions that can be achieved through the use of TCG technologies.

USE CASE 1: DEVICE HEALTH REPORTING IN MOBILE NETWORKS

When a mobile device connects to a cellular base station, the base station establishes (or refreshes) a device-specific Security Context for that mobile device. The Security Context identifies and tracks security characteristics of a mobile device that is connected to a mobile network. This Security Context is transferred to a new base station every time there is a handoff.

Currently, the information in the Security Context is limited to descriptions of the mobile platform of the device, with no useful health reporting. As such, this Security Context is of little use for determining whether the device is compromised or at risk of compromise. The ability to support more detailed health assessment of mobile devices, similar to what is common today on traditional workstations, would be a powerful tool for tracking and managing unhealthy mobile devices.

USE CASE 2: STREAMING SERVICES FOR MOBILE DEVICES

Increasingly, mobile devices are the means by which users consume streaming services (i.e., Netflix, HBO, etc.). Since many of the providers of these services operate on a paid subscription model, providers of streaming services wish to ensure that content is only provided to authorized devices (i.e., devices whose owners have paid for the content.) To do this, keys are provisioned on mobile devices and used as the basis for device identification and encrypted delivery of content.

Content providers would like to have some assurance that the device to which they give a content key is healthy, and that safeguards to protect the confidentiality of this key are intact. This requires some level of health and configuration assessment of the endpoint. This assessment needs to be robust enough to make useful determinations about device health, while not violating the privacy of the device owner.

TNC APPLIED TO MOBILE NETWORKS

Today, TNC is primarily employed in traditional networking environments. However, the capabilities TNC provides align well to the challenges facing mobile environments. TCG Mobile standards provide for protection of critical processes on the mobile device. These processes could include TNC components responsible for collecting and delivering device assessment information. Since TNC assessments are designed to be modular, network and service providers would be able to add components to collect the specific information they need to be confident in the mobile device's health.

For mobile device assessment, TNC could facilitate fine-grained measurement and evaluation of mobile device health when connecting to a cellular network. The TNC measurement agents would be protected by the device's Protected Environment and other mobile security features. Access could be allocated based on what measurements, if any, a device provided.

These technologies could also support more secure streaming services. The state of keys and the security features that protect those keys can be monitored by TNC modules and reported when the device seeks a new content key. As with health assessments, mobile security features, such as the Protected Environment, could ensure these TNC modules can run securely and free from interference. This allows content providers not only to verify that the device possesses the requisite key, but that the device is protecting the key against unauthorized duplication.

CONCLUSION

The examples noted above represent just a few of the challenges in the field of mobile communication and computing to which TCG technologies can be applied. As part of its ongoing efforts to address trust issues, TCG continues to develop and expand on these standards-based technologies to better align them with the unique constraints and needs of the mobile environment. Interested parties are invited to join TCG and contribute their perspectives and expertise to further develop these solutions.

REFERENCES

[1] Trusted Computing Group, *TNC Architecture for Interoperability*, Version 2.0, October 2017

[2] Trusted Computing Group, *TPM 2.0 Mobile Reference Architecture*, Rev 142, December 2014

[3] Trusted Computing Group, *Trusted Platform Module Library*, Part 1: Architecture, Rev 1.38, September 2016

[4] Global Platform, *TEE System Architecture*, Version 1.1, January 2017, available through the Global Platform Document Library