The Case for Turning on Trusted Platform Modules

In 2005, the Trusted Computing Group (TCG) published guidance to preserve user privacy as well as user control of their computing platform environment, among other things. The TCG recommended vendors deliver trusted computing technologies in a state such that platform users must choose to turn them on, a policy they called opt-in[1]. Vendors implemented opt-in for Trusted Platform Modules (TPMs) in a variety of ways, with several major vendors delivering platforms to end users with Trusted Platform Modules (TPMs) turned off. At best, vendors left the TPM in inconsistent states from vendor to vendor, and even across product lines of the same vendor. This inconsistency discouraged application developers from taking advantage of the TPM to enhance security in their products and systems. The opt-in policy has inadvertently hindered the integration into global enterprise IT infrastructures of over 400 million TPMs that platform vendors have shipped over the past eight years.

In implementing TCG's 2005 guidance, some vendors' concept of user may have been more narrow than necessary. As the guidance points out, users of Trusted Computing technologies may include traditional administrators and end users as well as platform vendors and service providers. Some platform vendors assumed a responsibility to ensure the integrity of the firmware and software they design, create, and deploy on their platforms. The TCG has designed the TPM with several controls that allows the end users (to include administrators) to control private information as well as control how the TPM should be used in their applications. However, end actor should take care to exercise this control in a way which avoids conflict with the roles of other actors who have responsibilities to preserve the integrity of the platform and software installed on the same.

The US, UK and EU follow internationally recognized agreements for protecting privacy. [2] However, despite the fact they share the same goals, sometimes they approach and implement solutions a little differently. With help from privacy advocates, the TCG identified and mitigated several concerns with privacy and user control in TPM features.

The US advocates allowing platform vendors to deliver TPMs in a state in which physical presence opt-in of the TPM is not necessary, and furthermore, to present a predictable TPM configuration to security-aware applications. The TCG recently approved a new interface[3] which allows vendors to configure the TPM and satisfy a variety of requirements with respect to privacy and user control. The US endorses this interface, which gives platform vendors flexibility to enable platform and service provider roles that provide integrity and other security features rooted in hardware, namely the TPM, while at the same time provide options to the other users, namely administrators and end users, to use the TPM to manage their own private information.

[1] TCG Best Practices Committee, "Design, Implementation, and Usage Principles Version 2.0", Trusted Computing Group, December 2005

[2] OECD Guidelines, the Fair Information Practices, and the European Union Data Protection Directive (95/46/EC)

[3] TCG PC Client Workgroup, "Physical Presence Interface Specification Version 1.20", February 15, 2011