TCG Specification.

Architecture Overview Specification

一、 動機

隨著科技不停發展，有越來越多事情得以透過電腦、手機甚至是穿戴式裝置完成，舉凡購物繳費、個人金融帳戶的操作、公司企業機密資訊的保全等等。但根據 AV-TEST 報告指出，惡意程式的數量正以指數的方式成長，相較於 2012 年已成長超過七倍，突破七億大關。換言之，我們的敏感機密資訊很可能暴露於危險之中。更何況或許因爲方便性、必要性或只是單存的好奇心，無可避免地，使用者的機敏資訊很可能與那些已知或未知的不安全應用共存於同一設備。

而爲了保護終端使用者在設備上行爲的安全性、免除遭惡意行爲侵害，於是 Trusted Computing 便因此而生，期望能利用此項技術給與使用者更安全可靠的使用環境。藉由軟體或硬體的整合，令使用行爲得以依據所預期的方式執行，又或可用於數位版權管理(DRM)，對智慧財產權加以保障。

二、 議題

Trusted Computing Group(TCG)透過標準與規範，以達到安全計算。TCG 技術得以保護重要業務的系統與資訊、達到安全認證並保護使用者身分並建立網路完整性。有了 Trusted hardware 與其 applications 便可以幫助企業降低成本且能夠遵循相關法律規範。其中，TCG 硬體部分可以自半導體廠商獲得，而軟體部分則可以自應用程式開發商獲得。

TCG 不論在智慧型手機、嵌入式裝置、伺服器、基礎建設、網路設備、儲存裝置或雲端等安全皆有投入，涵蓋超過十億台設備。幾近所有企業的電腦、伺服器、嵌入式系統皆會含有 TPM 元件，而其他網通裝置、驅動程式等需要網路安全或自我加解密的裝置，也皆有 TCG 相關規範在其中。

三、 研發方法

- Trusted Platform Module(TPM):

  利用完整性檢查或加密金鑰等機制，確保唯有在安全的記憶體、register 環境下才得以操作機敏資料，而存取此 shielded locations 需要進一步的特殊權限。

  藉由 TPM 認證機制，確保資料在操作過程的準確性、日誌保存的完整性、紀錄報告的過程完整性，而外部實體也得以驗證 **shielded locations** 與其保護能力。

- Root of Trust:

  信任所需要的最小單位，若有不正當行爲將會很難被發現，共可分爲三種常見的元件：RTM (Root of trust for measurement)、RTS (Root of trust for storage)、RTR (Root of trust for reporting)。RTM 可用來計算可靠度的完整性量測，RTS 可用來精確地保持摘要的完整性，RTR 可確保 RTS 報告的可靠度。

- Integrity Measurement:

  在測量事件方面可分爲兩類數據，其一爲測量值另一爲測量摘要。前者爲嵌入式數據或程式碼的表示法，儲存於 TPM 當中；後者爲測量值的 hash 值，基本上可儲存於任何地方。並導入 Stored Measurement Log (SML)機制，爲測量值的一串序列，而每個序列包含測量值與測量摘要的 hash 值。

- Protected Storage:

  由於 TPM 空間有限，只會儲存必要的 key 和暫存操作時用來加密或數位簽章的 key，而沒有頻繁使用的 key 則會由 TPM 加密後儲存在外部的儲存裝置，而 TPM 透過 Key Cache Management (KCM)來在需要的時候 load 回來使用。KCM 爲一介面允許外部程序可管理 TPM，也就是外部儲存裝置與 **TPM** 間的仲介，得以控制 **caching keys** 與 **storage keys**。

- Integrity Reporting:

  RTR 是用來揭露 shielded-locations 儲存完整性測量的結果，並證實儲存數據的正確性是基於「可信任平台身分」。完整性報告經數爲簽證後，透過 Attestation Identity Keys (AIK)來對 Platform Configuration Registers (PCR)進行身分驗證，以防止重放攻擊。

- Endpoint of Communication:

TPM 利用公開金鑰對訊息加密，確保訊息僅有具私鑰的接收端得以解開，同時亦導入簽章技術以確保訊息的完整性。此外，TPM 尚具有 Sealing 機制，sender 需先向 receiver 請求其 PCR 值，接著將要傳過去的訊息利用對稱式金鑰加密，並利用 receiver 的公鑰加密在傳給 receiver。而 receiver 接收到 sealed 訊息後，需先使用自己的私鑰解密，再減掉自己的 PCR 值，最後才得以使用對稱式金鑰來獲取明文。由此可見，若是非原本的 TPM 是無法解開密文的。

- Interface with Software Services:

TCG 軟體可分爲三個介面，主要是利用大多數計算平台的服務來進行分層。

TDDL(TCG Devices Driver Library) Interface: 爲一個 user mode 的介面，確保各 TCG 軟體的 stack 不同，使得與 TPM 溝通時能正確地傳遞，同時也爲 TPM 應用程式提供一個與系統操作無關的介面。

TCS(TSS Core Service) Interface: 做爲 user mode 中的 system process，管理欲提供給 TPM 的授權訊息。TCS 實作出對 TPM 的 threaded access、儲存與平台相關的重新認證密鑰、管理 event logs 並存取 PCR 相關的暫存器、負責序列化、同步與處理 TPM 相關指令。

TSP(TCG Service Provider) Interface: 提供針對 TPM 基於物件導向架構的 C 介面。其 Context Manager 提供 dynamic handle 能較有效率地利用應用程式與 TSP 資源。

四、 反思與展望

TCG 對 Trusted Computing 有極大的貢獻，並訂立相關標準措施，保護電腦不受病毒和攻擊者影響。但從另一個角度來說，同樣也就限制了使用者的行爲，甚至會有強制性壟斷的可能，從而傷害那些購買 trusted computing 的人們，這也就令「信賴」成爲最主要的爭論。TCG 對技術信任的描述爲「如果一個系統運算總是按照預期的方式和目標進行，那它就是可信的」。此段描述將 Trusted Computing 描述爲一個使用者「被迫信賴」的系統，而非是眞正值得信賴的，畢竟「可信賴」(Trusted)和「值得信賴」(Trustworthy)不同。雖然 TCG 聲稱 Trusted Computing 可增進安全性，但是否有可能使用者非但得不到更好的安全保障，還會被 Trusted Computing 強制限制使用 DRM，不僅會傷害隱私，也會受到其他限制。此外，Trusted Computing 也很可能會影響自由軟體市場、私有軟體開發和一般化的 IT 市場競爭。

但不管如何，隨著 **IoT** 的興起，Trusted Computing 勢必仍會持續受到重視，期望能在惡意程式充斥的世界中，能爲使用者提供更爲安全且可信賴的執行環境。