TPM2.0 在RPi2 上的效能測試

指導老師：鄭仁亮教授
組員：陳韋諭、吳岱燁、張迺湘

動機與目的

動機：

近年來資安的議題備受矚目，在PCI DSS、電腦中毒、智慧財產權各方面，可信平台模組(Trusted Platform Module ,TPM)提供系統化的解決，陸續微軟及IBM也不斷推動，可見TPM的發展前景多麼可觀。

相關研究：

論文*Emulation of TPM on Raspberry Pi*在Raspberry Pi上安裝TPM1.2模擬器，為計算機安全開發TPM學習環境及實驗手冊。

效能測試報告*fTPM: A Firmware-based TPM 2.0 Implementation*中將fTPM(韌體TPM)及dTPM(硬體TPM)做五種基準命令的TPM2.0的效能測試。

目的：

將TPM2.0模擬器安裝在Raspberry Pi 2上執行，並進行五種基準命令效能測試，將結果與fTPM(韌體TPM)及dTPM(硬體TPM)做比較。在安裝及指令測試過程中可以藉由此架構去分析位元組流和硬體TPM去做驗證，以利未來TPM2.0系統晶片的開發。

實驗環境

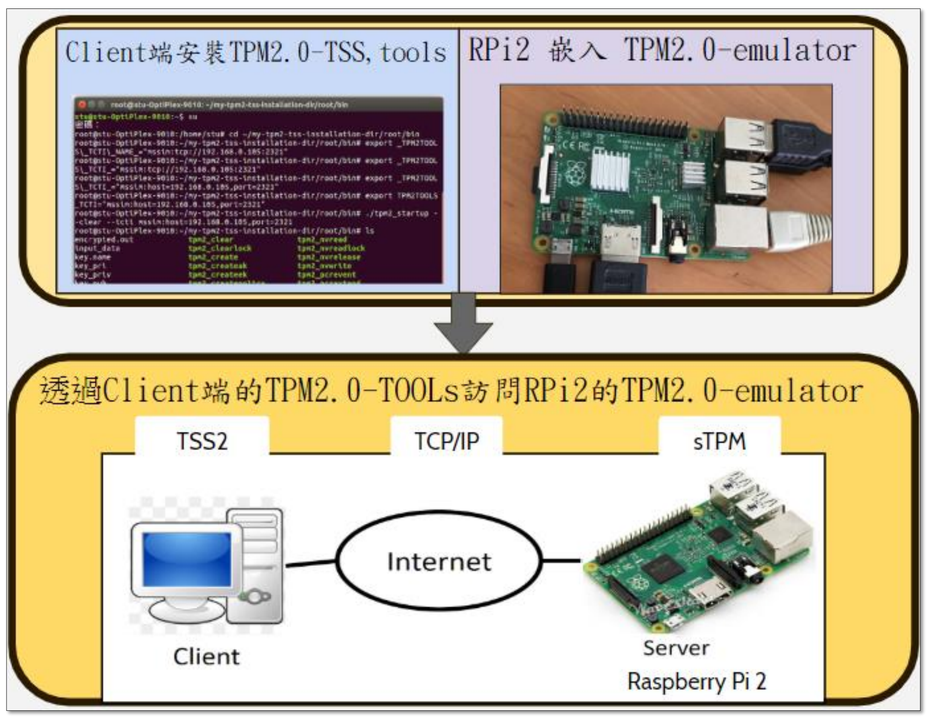

圖1 sTPM實驗環境

測試的比較裝置

TPM2.0不同類型的實現：

- Discrete TPMs (dTPM)：
  是專用晶片，最值得信賴的TPM類型。在硬體中實現規範功能，可防止軟體中的錯誤及竄改。

- Firmware TPMs (fTPM)：
  韌體TPM，在可信執行環境中運行的軟體模塊中，需特殊處理器及硬體支援。

- Software TPMs (sTPM)：
  軟體TPM，也稱TPM模擬器，依賴其運行環境，因此其提供的安全性較不會超過環境所提供的安全性，也易受到軟體層的漏洞或攻擊，適用於開發。

表1：測試的TPM2.0設備處理器型號

Device	Processor Type
Device # fTPM1	1.2 GHz Cortex-A7
Device # fTPM2	1.3 GHz Cortex-A9
Device # fTPM3	2 GHz Cortex-A57
Device # fTPM4	2.2 GHz Cortex-A57
Device # dTPM1	無提供
Device # dTPM2	無提供
Device # dTPM3	無提供
Device # sTPM	0.9 GHz Cortex-A7

測試報告*fTPM: A Firmware-based TPM 2.0 Implementation*中fTPM1~fTPM4為四台市售配有fTPM的現成移動設備，提供其處理器型號，dTPM為市售的TPM晶片，對其產品保密，sTPM為本專題使用之RPi2。

將本專題實驗環境用五種基準命令去做效能測試，與其他七種TPM裝置做效能比較。

TPM2.0 在RPi2 上的效能測試

慈濟大學
指導老師：鄭仁亮教授
組員：陳韋諭、吳岱燁、張迺湘

測試結果比較

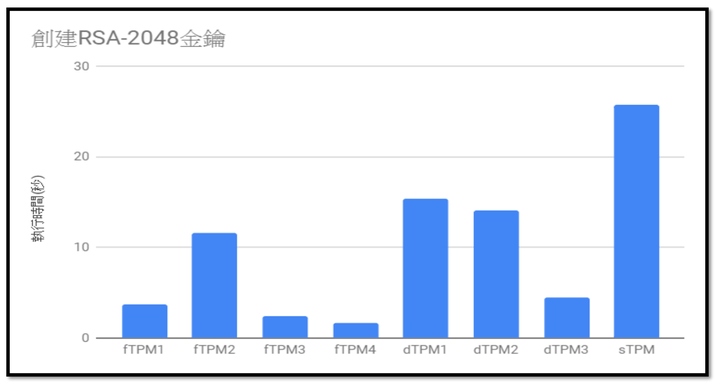

圖2-1 效能比較-創建RSA金鑰：創建2048位元的RSA密鑰。

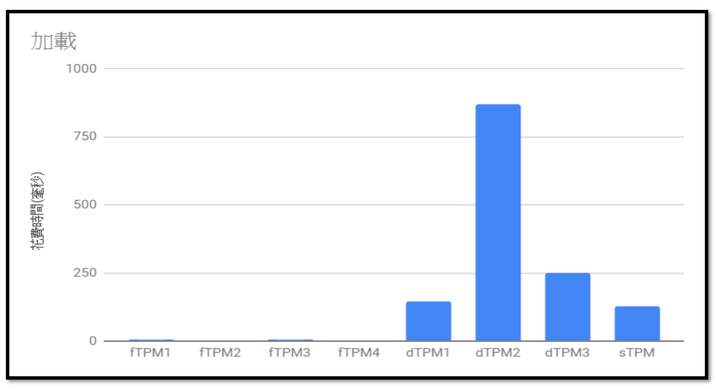

圖2-2 效能比較-加載：將2048位元密鑰加載到TPM2.0中。

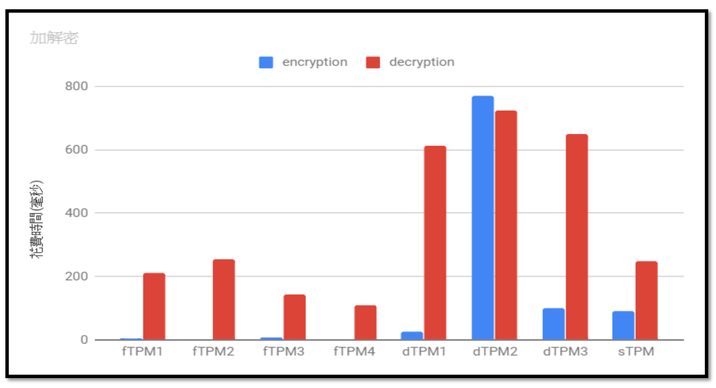

圖2-3 效能比較-加解密：用2048位元密鑰對資料進行RSA加解密。

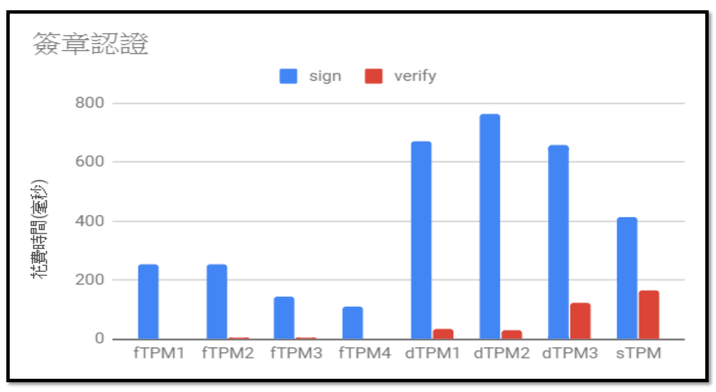

圖2-4 效能比較-簽章認證：用2048位RSA密鑰進行簽名驗證。

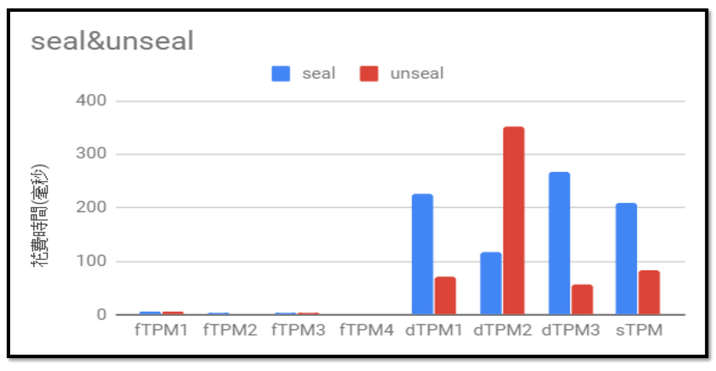

圖2-5 效能比較- Seal&Unseal：將10位元組信息密封至TPM，再解開密封看信息。

測試結果討論

兩點結果：

1. 在創建RSA密鑰的效能比較中，sTPM的效能較fTPM及dTPM差。
2. 除創建RSA密鑰的命令測試外sTPM的效能都介在fTPM及dTPM之間。

結果討論第一點：

在fTPM 的設計中使用合作檢查點，讓費時間的命令在作業系統中執行，不會因為缺乏虛擬化支持而導致長期運行而離開操作系統。

dTPM在沒有發出TPM的命令時，已在後台搜索質數，並維護質數緩存，供TPM需要時可以直接使用。

結果討論第二點：

fTPM較dTPM快，TPM晶片的微控制器本身執行較慢。 而sTPM和fTPM 的命令是在完全成熟的ARM Cortex內核上執行。

而fTPM使用硬體本身分配好的安全區域和普通區域，安全區域不與軟體層和設備連接，因此在fTPM不需要額外使用安全區域及普通區域的記憶體配置而較sTPM節省時間。

本專題特色與未來展望

本專題首次將TPM2.0成功安裝在RPi2上，並進行五種基準命令測試，與fTPM及dTPM去做比較。另外在實驗環境的安裝及指令測試過程中可以藉由本專題的實驗架構去分析bytestream和硬體TPM去做驗證，利於未來TPM2.0系統晶片的開發。