為行動裝置安全性提供「深度防衛」

作者：Ian Smythe，Arm 市場行銷副總裁 2020-09-22

在機殼之下，消費性裝置由硬體元件、運作這些硬體元件的韌體，以及數十萬個軟體程式碼行列組成；這些都很容易遭受不同種類的駭客攻擊，需要確保它們的安全性。

為了在次世代裝置上達成無縫數位沉浸體驗的願景，需要一種橫跨整個系統單晶片、聚焦各種體驗與使用場景，以解決方案為基礎的方法。這些體驗與場景隨著每天的任務有所不同，例如通訊、購物與金融，一路到更為複雜與先進的作業負載，如影像串流、遊戲、擴展實境(XR)、虛擬實境(VR)與擴增實境(AR)。

Arm 的「全面運算」(Total Compute)就是一種實現以上願景的方案，包含兩項特色：運算效能與(compute performance)開發人員存取(developer access)。除此之外，我們也需要安全地完成這些體驗──不僅是在裝置本身，還要橫跨整個行動生態系。「全面運算」從終端解決方案到貫穿整個 Arm 生態系對消費裝置的支援，力求將安全置入所有層面。

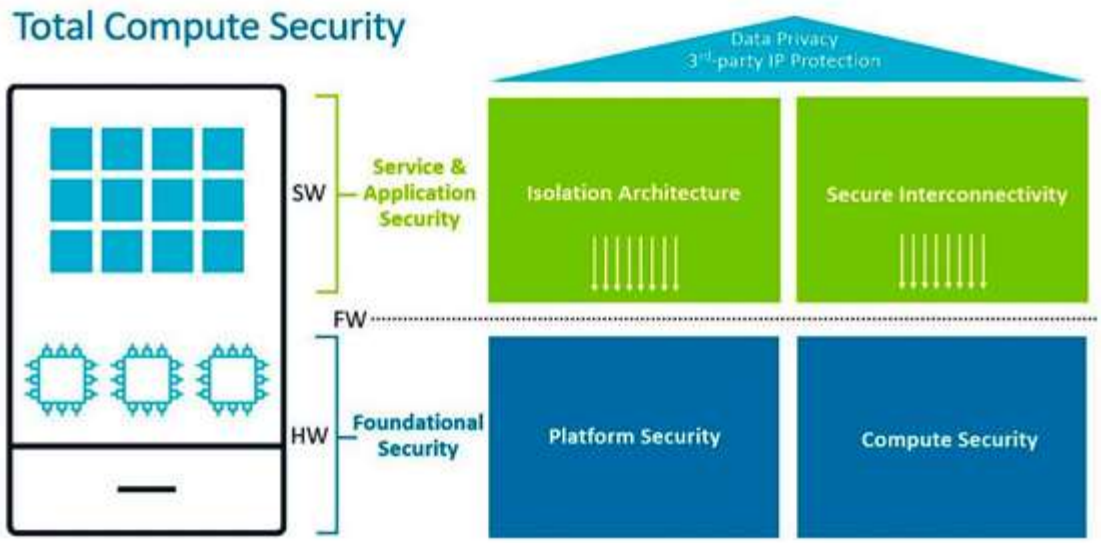
過去 20 年來，Arm 致力扮演行動科技安全先鋒，其 TrustZone 技術今日已經用在全世界數十億個行動裝置上，也進一步擴展到智慧手錶、數位電視、連網家庭裝置，以及次世

代筆電。這項技術是這類消費性行動裝置運算處理器的核心。因此，Arm 處在最好的位置，可以因應橫跨整個裝置與應用生態系全新的安全威脅。

打造安全必須從頭開始，也就是每個裝置的核心。全面運算讓確保終端裝置的承諾，再向前推進一步，為硬體、韌體、軟體、作業系統、應用與服務，提供「深度防衛」的安全性。

全面運算安全的兩面

在機殼之下，消費性裝置由硬體元件、運作這些硬體元件的韌體，以及數十萬個軟體程式碼行列組成；這些都很容易遭受不同種類的駭客攻擊，需要確保它們的安全性。組合與實作的數量很多，也可能出現碎片化，這會讓快速與廣泛實施安全補丁的挑戰性變高，進而形成一個找出漏洞與修補漏洞的無限循環。因此，打破這個循環需要不同的方法。



透過全面運算的安全性方法。

Arm 的全面運算安全願景，是藉由從頭開始確保裝置的安全性來保護個資。這意味著從架構開始，這也是所有運算的基本設計。Arm 的目標是在大量生產前減輕裝置的脆弱性，並大幅降低消費裝置的攻擊向量。實際上看，這個方法可以拆解為安全性的兩個關鍵面向：

- 硬體(HW)與韌體(FW)的基礎安全；
- 軟體(SW)的應用與服務安全。

隨著次世代消費性裝置的複雜性持續提升，安全也必須超越只保護裝置單層的分立式解決方案。從裝置的硬體，到利用存在裝置上許多個資的雲端服務，我們需要包括系統合作在內的多層解決方案。

基礎安全

基礎安全可拆解成兩個安全元素：平台安全與運算安全。

平台安全

今日多元的實作與安全的作業系統，讓應用開發人員與學習演算法的開發人員，很難相信他們的 IP 以及用戶的數據，在其使用的裝置上可以獲得保護。

平台安全包含在五個由英文單字 C 代表的層面與業界合作。這五個 C，就是建立協作(Collaboration)、合作(Cooperation)、通用性(Commonality)、一致性(Consistency)，以及商品化(Commoditization)。我們已經與晶片廠商、OEM 廠商、作業系統廠商(OSV)、獨立軟體廠商(ISV)與開發人員展開公開協作，以便為次世代的消費裝置帶來平台安全性。

Arm 針對共同的安全架構與一致的硬體與軟體實作標準，與這些夥伴協同合作。標準化的平台安全可以協助加速裝置的上市。更重要的是，它可以為應用與雲端服務建立對裝置平台的信任。

最佳的協作範例，是針對基礎系統架構(BSA)與平台安全架構(PSA)規格草案所作的努力。Arm 藉由與矽晶圓廠家及例如 Android 等 OSV 夥伴，合作開發安全分區客戶介面(SPCI)規格，目前已有顯著進展。SPCI 的目標，是在真實世界中，於安全服務的客戶與安全分區中服務提供者之間，打造一套標準化的 API。這是一個通用的介面，真實世界的虛擬機器監視器並不需要安全的作業系統驅動程式。Arm 期待與所有夥伴持續進行這些公開協作，以便為次世代的終端裝置促成平台安全。

運算安全

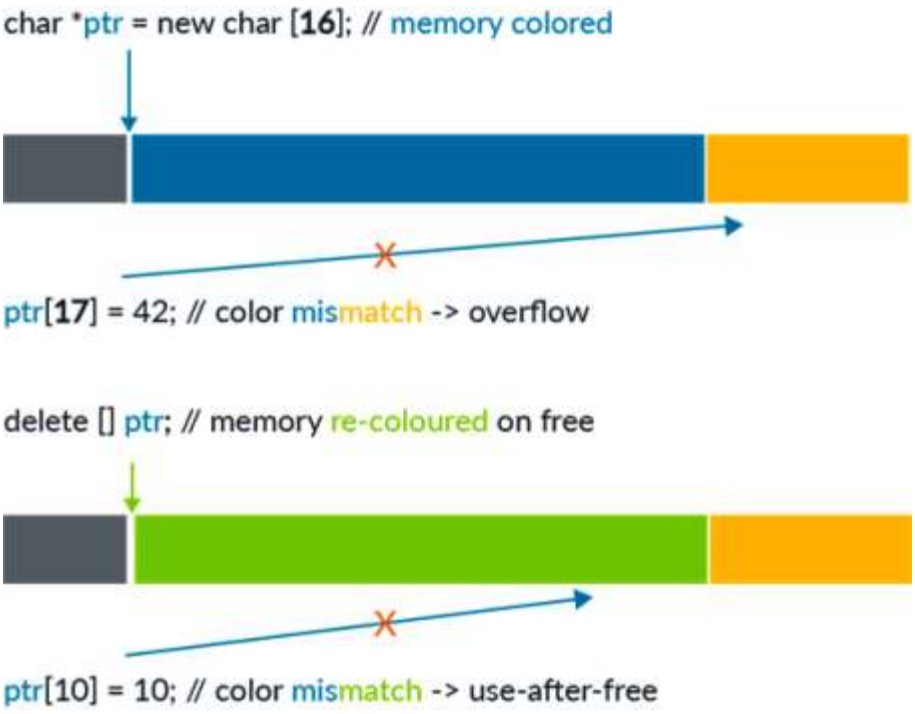
標準雖然需要花時間開發與導入，運算安全卻聚焦在透過今日的架構提升基礎安全。這些解決方案包括：64 位元、指標鑑別碼(PAC)、分支目標識別(BTI)，以及最近剛推出的記憶體標籤延伸(MTE)。首先，它們靠著強化軟體對攻擊的韌性提高門檻；其次在攻擊造成傷害前，從源頭堵住軟體漏洞。

記憶體標記擴展(Memory Tagging Extension，MTE)，是 Arm 為全面運算增添的新力軍。記憶體的安全錯誤，是駭客攻擊向量最大的單一類別。簡單地說，MTE 讓橫跨整個

生態系的記憶體安全違規的檢測，變得更加簡單且更有效率。他們在把系統單晶片供貨給 OEM 代工廠商之前，馬上可以應對這種病毒類型。

其次，OEM 代工廠商也能因此受益，因為 MTE 在裝置大量生產前，也能檢測其他的記憶體安全錯誤。在硬體上市可用前，像 HWASAN 等工具也可以在 Android 系統內存取，以支援程式碼檢查。一旦上市後，OSV 與應用開發人員可以使用具備 MTE 功能的裝置，尋找他們程式碼中自己的緩衝器溢位與堆已損壞。

對於各種 C/C++ 程式碼，MTE 已經證實具有許多好處，未來更可能為生態系帶來更大的價值。例如，我們已經在研究中看到 MTE 獨特的應用，它也可能對如 Javascript 等其他程式語言帶來好處。



透過 MTE 的記憶體鎖鍵的存取範例。

儘管 Arm 的基礎安全解決方案已有相當基礎，但全面運算還會加速應用與服務安全的解決方案。

應用與服務安全

我們從兩方面投入應用與服務安全：

- 可信任應用的強健沙盒使用的隔離架構，例如在虛擬機器容器內運行的應用。
- 網路間連結的安全性，以確保 CPU、GPU 與 NPU 的並行處理。

在深入探討這兩個面向之前，應先思考現有的與應用及服務安全有關的安全挑戰。

TrustZone 架構的作業系統運行在行動裝置已有十多年。它們透過數位版權管理(DRM)，保護電影產業的產出內容、保護用戶的個人生物特徵量測數據，甚至於透過電子錢包進行的付款。

不過，就在高階作業系統(HLOS)應用數量成長的同時，保護個資與企業智慧財產的需求，同樣與日俱增。因此，能夠擴充今日可被信任的作業系統、以服務上百個、甚至成千個應用、程式庫與模型開發人員的需求，可能是個挑戰。開發人員必須創造自己的安全應用，但是他們並沒有與每個裝置 OEM 代工廠商及矽晶圓廠商合作所需的資源。反過來說，OEM 代工廠商與矽晶圓廠商也沒有與眾多開發人員合作的資源，並測試其中的變數。

隨著開發人員把更多的機器學習(ML)能力與他們的應用結合，ML 持續增加的使用場景，也已彰顯深度保護 IP 的必要性。我們在購物推薦、自然語言處理、司機與乘客的匹配、處理來自智慧手錶的數據，以及進行診斷評估等方面，都看到 ML 的使用。這些模型本身成為某些公司的商業核心資產，因此需要被保護、免於遭受競爭對手與駭客的傷害。

隔離架構

藉由改進隔離架構，應用與服務安全得以因應這些挑戰。想像一下，倘若硬體製造商與 HLOS 可以建立可信任的隔離，意味著他們得以確保開發人員的安全程式碼與用戶的資料，能夠與裝置硬體、韌體、HLOS 及其它的應用妥善隔離開來。把惡毒的程式碼帶進應用的駭客以及應用意外導入的漏洞，在這種環境下因為造成的傷害比較小，可能就不那麼令人擔憂。它可以顯著降低事件的風險，並且可能透過知名的 App 商店，以較易擴充的方式部署安全的程式碼。

隔離架構也能協助業界達成需要的規模。A 級韌體框架(FF-A)為機密運算所需的可擴充的安全性，跨出了第一步。

在 BSD-3 條款授權下，最近 Google 的 Hafnium 專案轉型 Trusted Firmware，可說朝這個方向跨出意義非凡的一步。它為 Arm 的安全 EL2 虛擬化進行延伸，促成參考級安全分區管理器(SPM)的公開與協作開發。Trusted Firmware 專案是公開治理社群專案，致力於開發值得信任與透明的參考級韌體堆疊。它可以重複使用，設計用意在於為裝置生態系減少移植與整合的工作。

所有 Arm 夥伴目前在自己的 FF-A 實作中，都可以利用參考級的 S-EL2 SPM。由 Trusted Firmware 提供的 FF-A 規格以及 EL3 與 S-EL2 的參考實作，提供一個共同的框架。這意味 OEM 代工廠商與矽晶圓廠商可以提供一個可擴充規模的共同程式模型，以便與任何開發人員合作打造安全的應用。

網路間連結安全

應用與服務安全的另一個層面，就是網路間連結的安全性。目前已在市面上販售以及未來即將上市的消費性裝置，說明了確保同步處理的需求。不管是透過電視、平板電腦或智慧手機，觀賞運動賽事的現場直播是很好的例子。

今日的消費性裝置可以安全地呈現受到 DRM 保護的 4K 直播串流，但如果賽事直播秀出選手球衣的購買連結呢？點擊這個連結，會跳出比較小的「畫中畫」視窗，並詢問觀眾是否要看看自己穿上球衣的樣子。裝置此時必須保護直播賽事的串流、用來在觀眾的照片上呈現球衣的 AR 模型、購物 app 用以展示球隊商品的智慧財產，以及這筆交易的個資。此時最多可能同步出現四個處理，在需要保護的不同 CPU、GPU 與 NPU 上執行。

這一類在網路間連結的安全使用場景，正在挑戰今日終端處理安全需求的極限。利用全面運算提升運算效能的同時，Arm 也在研究新方法，以確保在不同處理器運行越來越複雜的作業負載的安全。若只專注在最佳化個別 IP 區塊，將限制在整個系統上有效且安全進行網路間連結的能力。全面運算針對整個系統單晶片採取系統層級的解決方案觀點，也將幫助網路間連結的安全性。

結語

透過全面運算在安全上促成的各項好處，可為整個生態系提供更好的保護，也讓所有層面相對地不易受到攻擊。這些好處超越硬體、軟體、作業系統、應用與服務，帶來「深度防衛」與保護。它將聚焦於未來在終端或雲端上、重要的安全性使用場景，同時移除生態系內的產品碎片化。隨著邁入一個更廣的終端數據處理與數據創新社會，全面運算將使一切將更為安全無虞。

本文由 Arm 供稿；責譯：Judith Cheng

文章來源: https://www.eettaiwan.com/20200922nt71-delivering-security-defense-in-depth-through-total-compute/