arm

# 安全宣言

# 導言

一場系統安全戰役如火如荼展開，我們也在加緊腳步，希望能夠瞭解資料背後的真實意義及重大價值。在這場戰役中，科技公司除了供應產品之外，還肩負了更多社會責任。我們的宣言文件指出資料導向世界的威脅漸增，提供詳細的技術指南，以利因應相關風險。此外，我們探究資訊革命守護者的責任，並討論科技廠商應致力遵守的社會契約。

# 內容

# 宣言

## 共生合作：掌握人性因素，提升網路安全


### Mary Aiken博士

都柏林大學司法網路心理學家暨歐洲刑警組織歐洲網路犯罪中心(EC3)學術顧問(心理領域)


身為網路心理學家，我的工作是對人類和科技的交集分析並提出深層解釋，或是解釋人類和科技的互動。

對於實體犯罪和白領犯罪，我們發展出多種預防策略，但也日漸需要新的策略，來對抗網路犯罪。至今，針對重要基礎設施的攻擊，已耗費了我們的全副心力；不過，物聯網所帶來的連線能力，表示所有的基礎設施都將遭受攻擊。現在的駭客無孔不入，攻擊手法更加全面而複雜，所有使用者和企業都可能淪為目標，物聯網只會增加這類攻擊的機率。

每個人都是第一線的守護者，但不是所有人都認真看待自己的行為。我們也並非人人都是IT專家，且裝置和系統出廠時，也未必內建安全性。使用者對於網路安全過於胸有成竹，誤以為萬無一失，這就是虛假的安全性。許多攻擊發生的原因在於「數位衛生」習慣不良、設計缺乏安全性，且使用者的意識不足。年輕一代的使用者多是數位通，不過很矛盾的是，他們也更容易自滿於安全性的現況。我們身為學界專家、設計人員、開發人員和工程師，必須加強保護消費者，同時關注科技安全方面的網路心理學。我們必須採取以人為本的方法，仔細考量人類使用連網「物件」的真實情況，不能再以科技界先入為主的成見，來看待使用者的行為。

威脅者包括組織性犯罪集團、政府組織、跨國行為者或小型團體，他們也都是人類。因此，不論是針對消費者或網路罪犯，最重要的任務就是瞭解人類如何與技術互動。至今的努力方向，大多著重技術解決方案，然而創意和設計不能無中生有，因此，必須深入瞭解人類行為如何在網路領域中組合、變化、擴大或強化，並探討其中原因。

### 調查性思維

我們必須採用行為剖析專家的思考方式，考量方法、動機和機會。方法涉及工具和技術，但是生成動機和掌握機會則是人類獨有的能力。大多數安全事件通常帶有人為疏失，而外部攻擊者正是利用這種人性弱點發動攻擊。他們經常從高層下手：魚叉式網路釣魚攻擊的重心逐漸移往高價值目標（如執行長），一旦成功後，受攻擊的公司通常會遭受龐大損失。

那麼，該如何防範人為疏失，保護網路安全？我們必須深入解析網路上的行為。

要分析任何系統的人為因素，都是非常複雜的過程，必需對人類能力具備基本的認識。我們不能只關注認知層面，也要考量身體、行為、生理、社會、發展、情感和動機等面向。很少人會思考網路攻擊的社交和心理層面：到底哪些人會是攻擊者？他們為什麼要發動攻擊？

為了因應網路攻擊，安全解決方案設計者和廠商必需考量網路環境的動態特性，以及不斷演變的網路行為。值得注意的是，北大西洋公約組織（NATO）在2016年表示網路是「作戰領域」，也就是進行戰爭的空間，正式將現代化戰爭的範圍

從陸、海、空擴展至電腦網路。

「線上階級權威最小化」的概念是指在網路世界裡，沒有任何人負責統御，因為實際的情況就是如此。

因此，我們如何面對網路世界？是否可以採行司法管轄或治理權限？我考慮仿照聯合國憲章的架構，提出「網路憲法」，內容如下：

「我們人民，為建立更完善的網路社會，樹立正義，保障安寧，共同防衛，促進公共福利，並使自己和後代享有自由福祉，特制定本憲法。」

尋求解決方案時，我們可以向環保運動學習：這項倡議提出「預防原則」，要求產業承擔保護環境的責任，亦可視為網路世界的基本原則。雖然，保護關鍵基礎設施仍是私部門的責任，不過全球安全標準確實需要一套共識基準，確保重要產業系統(如電網和航空交通管制)的管理操作系統正常運作。

有鑑於威脅形勢快速演變且科技突飛猛進，我們的研發方法也必須更具靈活彈性，其中包括開拓資金來源，以利加速達成重要的預期結果。

### 邁向共生合作

科技的運用有利有弊，而業界的主要挑戰，就是趕上威脅者技術演進的腳步。網路攻擊案件數量龐大且持續演變，因此需要更精密的人類智能擴增（IA）解決方案，這是基於「以人為本」的考量，所開發並部署的科技解決方案，目的在於緩解技術安全威脅。

這表示人類的洞察及合作，搭配強大的機器學習和細心的設計工程，可形成堅實的防禦基礎，以減緩安全攻擊、駭入或入侵，維護網路世界安全，進而保障科技產業，並確保業界蓬勃發展。

透過這篇宣言，科技產業可從不同角度思考網路安全方面的注意義務 (duty of care)，擴大集思廣益的範圍和迫切性。

# 安全健康證書：免疫系統和醫療服務如何大規模提升物聯網的安全性

**Milosch Meriac**
Arm首席安全研究主管

不斷上演的系統安全保衛戰，大多處於被動防守態勢。我們總是先發現攻擊，再辨識來源，然後採取因應行動，並設法降低未來風險。這是我們數十年如一日的因應對策，從傳統運算技術到行動系統都是如此。但是，未來物聯網 (IoT) 極為複雜的互動方式，導致這種被動方式難以有效管理和擴充。

### 災情蔓延的危害

遏制惡意軟體的影響範圍至關重要，因為關閉整個系統造成的損害，可能比惡意軟體本身更嚴重。此外，找出安全漏洞並更新已驗證的韌體，可能要耗費大量時間。物聯網技術勢必具有廣泛部署型態，而且涵蓋了關鍵的基礎設施網路，因此完全關閉系統是絕不可行的作法。

這種情況類似人體免疫系統，會自動對目標發揮作用，藉此抵抗感染。人體感染可能會快速失控，不只影響感染器官，也可能波及周遭組織。此時，醫療服務就能發揮效用，治療患者並迅速處理感染部位，效果優於人體自行抵禦的機制。

因此，我們得出了一種理想模式：技術解決方案對於裝置攻擊的防護方式，就如同人體和醫療系統的合作。 我們也因此實現遍及整個網路的回應機制，並將已知安全漏洞特徵對應至裝置韌體，降低整個網路架構、系統和軟體的潛在安全風險，同時為產品團隊提供早期預防的方針。

### 預防接種

那麼，IoT的免疫系統和醫療服務如何運作？首先，我們先分析IoT免疫系統的可能型態。宏觀而言，這類系統會從邊緣節點開始，透過感應器偵測異常行為，這些邊緣節點可提供即時韌體執行追蹤記錄和效能計數器統計資料，可藉以掌握程式碼和資料存取模式。

如同生物的免疫系統，這項技術會主動觀察並監控系統網路流量，並且記錄、學習常見的行為。使用加密總帳技術的內外部測量經過時間戳記，可儲存於本機防竄改區域或網路內。流量-向量觀察資料封包經簽章加密後，會從主要應用收集，成為彙總測量數據，再向中央伺服器傳送回報。依據這些流量模式、節點互動和程式執行讀數，可以變更或撤銷存取金鑰，藉此分開或隔離節點，並將節點流量強制傳送到過濾主機。

不符合規定的應用，若無法及時證明訊息交付地位並以加密方式控制訊息，則可透過無線方式重置或重新閃存。這種方法與傳統的安全看門狗相同：要求加密密鑰來重置本機裝置看門狗，藉此強制潛在感染主機持續與中央控制器通訊。使用這類強制通訊通道，就可以強制安全看門狗和後端伺服器通訊，而不受網路堆疊影響。

實作現有的網路通訊協定，就可以獲得強制隔離節點的高階緩解功能。這表示，除了預防相鄰裝置遭受惡意存取，還能控制受影響裝置的網路流量和頻寬，緩解流入和流出的阻斷服務攻擊。

在最簡單的案例中，網路可透過虛擬網路辨識碼 (VLAN ID)

進行切割，而這類辨識碼一般可由受管交換器和路由器支援。VLAN的概念亦可延伸至網狀網路，使用安全通道通訊協定，就能以端對端方式，在網狀路由器和雲端架構之間延伸這類虛擬網路。

### 韌體「到府診治」

在不受限於特定廠商的環境中，標準化的無線韌體更新(FOTA)檔案格式和網路通訊協定，將成為不可或缺的要件。Arm Mbed 最新推出的Firmware Manifest Format已可滿足FOTA要求（包括規則執行、降級防護），而目前也在著手實現IETF的標準化。往後，「安全即服務」供應商僅能提供節點和廠商簽章韌體，無法進行韌體簽章。本機管理員也可以要求他們提出加密簽章，然後再允許韌體更新。

### 健康檢查

現在，我們來看看IoT「健康服務」的可能樣貌。可以針對系統擷取的行為模式進行巨量資料分析，藉以即時、持續監測系統健全度。如此一來，就能在感染之前，使用許多統計分析資料辨識漏洞，例如裝置類型、韌體版本、系統事件、事件流量模式等。接著，系統會使用中央規則和封鎖清單，在網路邊界封鎖已知的惡意特徵和流量模式。

此外，這類「健康服務」也能夠：

- 參照大量設施的裝置互動模式資料集，計算感染機率，據以觸發網路免疫反應。
- 在使用者授權下採取措施(如觸發韌體更新、隔離節點等)，同時對本機裝置實施明確的加密規則，徹底避免濫用權限。
- 人類操作員可針對高階使用者釐清安全警告(可能性低的事件)；必要時也能透過延伸手動操作卸載使用者。
- 執行規則，限制未修補的裝置僅能經由過濾流量進行存取，以較高的延遲維持裝置功能，同時確保安全。這可以視為一種遠端中間人防火牆，類似深度封包檢測(DPI)。
- 在受信任的邊界或網狀路由器套用流量過濾器，以保護使用者隱私。

健康服務也提供受信任的「霧運算」(fog computing)設備，可部署於本地網路，提升恢復能力和信任度。這類設備構造可以非常簡單，例如使用安全性經過強化的低成本WiFi路由器，來執行幾項精簡、受信任的軟體流程；但它們也可以非常複雜，例如高端防竄改19吋機架伺服器，可用於處理多項受信任的高端流程，並維持強大的隔離、記憶體加密和驗證功能。

如果是負載繁重的應用，則可透過雲端環境(或由使用者視需要進行)，以遠端方式佈建既有的可信任執行環境(TEE)空間。TEE語意可以延伸至網路，提供互不信任且隔離的運算環境，網路擁有者無需信任雲端供應商程式碼，即可遷移至本機網路。如此，雲端供應商就能仰賴這些應用 (已遷入遠端網路TEE設備空間) 的完整性和機密性。

雲端服務可運用這些受信任的設備來推動低延遲工作、運算任務、機器學習、或在本地網路套用機器學習模式，理論上也能夠將資料鏡像至本地網路 （反向亦可），提高網路停機的恢復能力、減少延遲並加強保護使用者資料隱私。

為了達成這個目標，針對在相同網路/裝置上運行的多種應用和虛擬機器，設備平台必須確實加以隔離並保障其安全。另一方面，必須防止使用者或本機攻擊者竄改裝置來外洩資料/智慧財產，或是插入不受信任程式碼，以不恰當的方式變更裝置行為。

本地網路有了這些受信任的運算節點，就能將電池供電節點上的高功耗運算作業遷移至市電供電裝置。大幅增加電池續航力，同時提升關鍵資料的安全性。

### 總結

預計再過3到5年，上述的IoT免疫系統和健康服務，就能夠普遍地保護各種技術。參考、採用人體抵抗感染的方法並加以調整，我們可為IoT網路實現更快速、更有效率的攻擊防護能力。有鑑於IoT的部署規模，我們必須具備這類全方位的對策，才能維護系統的信任度，而這項目標已非遙不可及。

# 裝置型安全模式


## Rob Elliott

Arm視覺架構總監


如果行動裝置學會辨識我們，從而保護我們避免駭客和竊賊的攻擊，那該有多好？運用這種熟悉度（familiarity）的技術，將可創造一種前所未有的驗證環境。其實，這並不是幻想，機器學習和人工智慧都已具備這項能力。

機器學習演算法已經投入工業機器人、無人機、汽車應用和新一波智慧居家裝置等產品功能，這些演算法運行於發展成熟的IP和矽晶上，在各種行動裝置中默默發揮效用，將流程和應用程式最佳化，同時提升元件執行速度，加強可靠度和安全性。機器學習部署在越來越多的行動裝置中，也逐漸以深入且獨特的方式，掌握這些裝置的使用方式。如此一來，所有裝置將會更熟悉使用者，並且基於這樣的熟悉度，創造出真正穩固的驗證和安全環境。

### 全新好友

裝置的行為模式記錄，可供我們深刻瞭解裝置的互動對象。實體感應器（如加速度計）或與軟體的細緻互動，都有助於取得身分辨識資訊。這些資訊包括使用者使用觸控螢幕的方式，或用來開啟應用程式的指令。 舉例來說，使用裝置執行近場通訊（NFC）支付功能時，若裝置上下顛倒或環境照明不佳 (如在口袋中)，就會發出警示。同樣的，警告也可以來自:

- 優先系統呼叫
- 罕見的大量CPU活動且優先層級較高
- 作業流程的異常高頻率活動

模式辨識能力可讓更多系統受惠，這類功能已經常用來防範電腦病毒、演算法適應行為和迴避偵測的偽裝技術。包含在安全套件的機器學習功能，可用於偵測異常行為，協助工程師辨識安全問題。若要辨識已知攻擊，可運用日誌來訓練類神經網路，再將網路部署於邊緣裝置。日誌是防範已知問題的實用工具，可加以擴充，使其自動反覆訓練，以因應新興

攻擊手法。完成上述準備之後，裝置偵測到入侵事件時，將可快速重新訓練並部署網路，以因應新的威脅。

所有相關「症狀」可用於擷取攻擊向量的重要資訊，並回報至安全鏈上游，同時藉以判定異常行為是否與特定應用或裝置相關。這些症狀也可用於提升支付交易安全性，例如先要求額外生物辨識輸入 (如聲音或指紋辨識)，才允許繼續支付程序。

### 學會自主學習

為何裝置尚未內建這些措施？就應用領域的各方面而言，機器學習仍處於早期發展階段，而我們著手部署解決方案時，也必須徹底重新思考，如何將運算資料從雲端散佈到邊緣，實現最佳化的機器學習演算法。目前，機器學習的焦點是雲端系統，伺服器在這類環境篩選從邊緣收集的大量資料和資訊，運用類神經網路執行訓練流程，來尋找有意義的模式。這些訓練不只針對資料，更強調仔細判定資料是否為有待辨識的問題，並同時蒐集正面和負面的範例。

訓練完成後，學習功能就能依據系統中(類神經網路進行訓練的環境)的不同輸入資料，推導出有用的資訊。工作內容可以非常簡單，例如從介於0-1的五個輸入值判定一個建議輸出值；也可以十分複雜，例如接收來自多個攝影機和其他感應器的輸入資訊，並制定複雜的決策，以實現駕駛汽車的功能。隨著使用案例益趨廣泛，推導流程需要更高的運算能力和更低的延遲特性。

在邊緣應用機器學習以提升安全性

這種學習流程最適合用在運算能力幾乎沒有限制的雲端，但是使用者仍須付出一定代價。不過，將機器學習推廣至物聯網邊緣的同時，我們將協助降低雲端運算相關的頻寬、成本和延遲。提高運算資源的分佈效率，也有助於改善行動裝置使用者的隱私保障，因為他們可能不希望讓所有資料都在雲端接受分析。(上述範例包括儲存於本機的指紋辨識學習流程。) Arm 贊助的調查《人工智慧的今日與未來》(AI Today, AI Tomorrow) 探討民眾對於人工智慧的態度，一項重要的發現為：人們希望能在本機掌控機密資料。

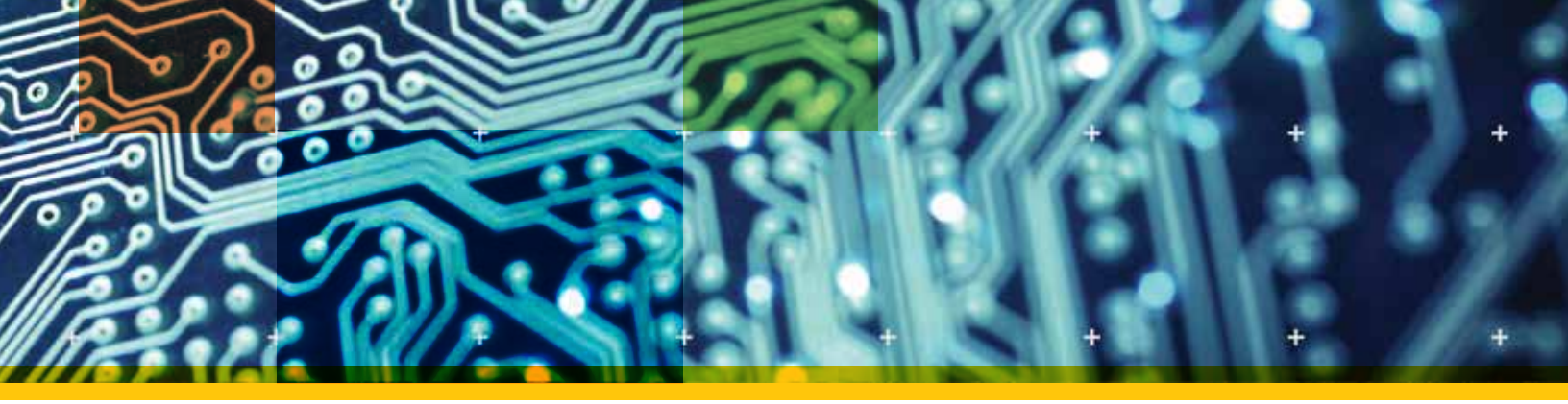
隨著感應器愈加普遍，今日已掌握大量資料的裝置，明日將能夠獲得更多資料。隨著裝置擁有的資料量增加，邊緣需要更強大的運算能力。至此，資料將化約為一種新型態的運算權重。這些新型態的權重將由雲端系統共用，藉此在裝置間分享資訊，並針對資料執行不同的運算任務。機器學習將利用各種裝置資源，而這樣的協作方法將促使學習更為強大、有效率。對效能和低延遲的強烈需求，將促使硬體、軟體和工具進一步升級。這些都是Arm致力改善使用者體驗的領域，接下來讓我們檢視其中之一項：軟體。

> **熟悉度是真正堅實驗證的基礎...**

### 理解軟體

對於機器學習而言，軟體的環境可能十分混亂。許多ML框架在不同效能層級受到多個程式庫支援；許多裝置各有不同的部署方式，可執行完整框架或者自訂轉換工具。為了釐清這些「紛擾」，Arm正致力於提供軟體和工具平台，讓整個體驗更為簡單一致。更好的是，我們試圖確保Tensorflow和Caffe 等現有工具，都不需要針對新產品進行修改。

為了簡化流程，關鍵在於透過穩定可靠的軟體平台，來提供簡便的ML部署路徑，如此一來，隨著新裝置數量增加，不需要大幅修改，即可寫入軟體。平台若採用最佳化的程式庫，硬體將能夠視需要進行創新，同時讓軟體無縫部署於Arm平台上。



# 改善程式碼安全性的架構指南


## Richard Grisenthwaite

Arm首席架構師暨研究員


無論是駭客或潛在的攻擊目標，雙方都在不斷精進攻防能力，而CPU架構面對已知攻擊的因應方法是，採用新設備來防範這些攻擊。於是，攻擊者發動更複雜的攻擊，從此雙方陷入無止盡的循環。不過，打破這個循環(或至少大幅延長循環週期) 的新時代就在眼前，硬體和軟體開發人員必須團結起來，以前所未有的合作方式來改善安全性。

### 戰勝「假資料」

現在，攻擊者會透過處理器所使用的資料，來破壞正常執行作業。一般而言，處理器使用的資料會寫入堆疊上的緩衝區，因此，攻擊者會將放置於堆疊的資料排列成可執行的程式碼序列，藉由破壞函數返回 (如緩衝區溢位)，處理器可能會受騙，進而執行這串任意且潛在的惡意程式碼。

為了因應此問題，處理器架構在大約2000年開始推出新功能，讓記憶體區域 (包括堆疊) 可標記為「非執行」。Arm針對這個問題，在Armv6中推出了執行禁用 (XN) 位元技術。這個問題一度貌似已經解決，不過，攻擊者也做出回應，開發出「return-to-libc」及「return-oriented programming」等技術，再次利用緩衝區溢位弱點進行攻擊。這兩種方法均透過緩衝區溢位，在初始階段破壞處理器執行作業，使其執行合法安裝於記憶體內、標記為可執行的程式碼。如此一來，攻擊者即可隨時使用非預期資料來執行此合法程式碼。至於return-to-libc攻擊，破壞行動會使用「假」資料來呼叫一組標準程式庫函數，使攻擊者得以利用原程式預期外的資料，進而掌控其功能。返回導向程式設計技術則更進一步，攻擊者藉由串連標準程式庫片段來建立「gadget」，可隨機發動貌似返回位址的惡意程式。軟體對於這類攻擊的反制措施，是在記憶體內隨機配置程式庫，使攻擊者難以建立這串位址。不過，攻擊者又發現一種機制，得以刺探位址配置，進而將實際配置納入該串返回位址。

### 使用指針驗證防範惡意執行

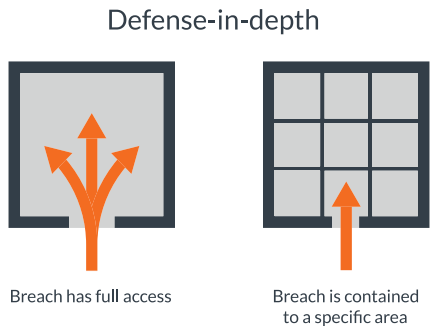
Arm的Armv8.3產品推出全新機制，進一步加強防堵這類攻擊手法。指針驗證 (Pointer Authentication) 採用64位元目標位址的部分較高位元，藉此持有加密產生的指針驗證程式碼(PAC)，位址使用之前，可先透過這類程式碼加以驗證。舉例來說，處理器新增PAC之後，當返回位址來到函數入口，處理器即能檢查PAC是否正確，再進行返回。

新增的屬性使得這項方法更為健全，例如，每一執行階段都使用獨特金鑰和加密強函數來產生PAC，攻擊者將無法針對特定返回位址猜測PAC。為了防範針對PAC值進行增量猜測，作業系統可變更金鑰，藉此因應大量的錯誤PAC。

### 深度防禦及隔離

身為CPU架構師，我們的設計不能抱持僥倖心態，以為沒有機制可以損害處理程序安全性和完整性，即使是正確寫入的軟體也不能大意。我們需要進一步的機制來提供「深度防禦」，為周邊安全防火牆提供額外保護。要強化深度防禦，一項實用的方法就是改善軟體「隔離」的方式，如此即可加強現有攻擊防禦機制，即使執行作業已遭受初步損害，仍可有效防範攻擊者造成嚴重破壞。為了建立這些屏障或防火牆，我們必須強化現有大多數的處理器，延伸其20多年未曾變更的典型權限和安全模式。這種典型的模式為：處理器提供單一位址空間，對映至一組分頁表，並且通常會給予統一

的權限。對於應用程式寫入人員來說，這種模式十分方便，但對於攻擊者也一樣便利。一旦處理程序遭受損害，任何開放存取的記憶體，攻擊者也將能自由存取。為了預防這種情況，我們將應用隔離成數個區域 (有時稱為「沙箱」)。執行於每個區域內的程式碼，僅可存取該應用記憶體的子集，用以運行該程式碼的功能。這表示一個區域內的損害，將限制在該區域的記憶體內。




目前的處理器幾乎未提供這類隔離所需的特定硬體支援；必要時通常僅將處理程序變成作業系統層級的隔離區域。因此，我們選用作業系統處理模式的現有設備，以提供隔離功能，同時執行標準行程間通訊機制，使隔離區域得以通訊。另一方面，也將存取範圍限制在應用中所有轉譯表的一個子集，來保護各隔離區域中程式碼所使用的記憶體。雖然部分商用作業系統缺少處理器架構的特定支援，但也都不惜承擔額外的複雜度而採用這項方法，這也說明了安全性的重要程度。未來的處理器架構應簡化隔離區域的使用方式，使其完全限縮在單一處理程序和位址空間內。

## 監視軟體的挑戰

多數處理器的標準權限控管模式，是採用權限分級的方法(或稱保護環)，每一環的權限逐漸遞增。在這種模式中，執行於特定權限層級的程式碼能夠存取較低層級的所有設備，但是屬於這項權限層級的設備 (至少一部分)，則不可從較低層級存取。如此即可打造真正的權限分層，成為監視軟體的堅實基礎，例如作業系統和Hypervisor負責管理資源及執行於較低層級的軟體。然而，這也導致監視軟體成為攻擊者顯而易見的誘人目標，尤其是，大多數監視軟體的用途，是為了管理不同應用或虛擬機器硬體之間的資源。依照現行運算模式，監視軟體因此必須能夠讀寫應用或虛擬機器的資料。這雖然是很正常的作法，但也表示一旦監視軟體受到損害，執行應用或虛擬機器的所有資料也將一同受損，而且幾乎無法加以保護。上述的隔離區域策略或許有用，不過未來的系統必須在應用或虛擬機器內保護資料，不但要避免監視軟體成為入侵途徑，同時不減損監視軟體管理系統的成效。

## 其他管道的崛起

架構定義了處理器所需的功能行為，不過很少有人討論如何實作這些行為。對於軟體來說，這通常不是很重要，處理器的微架構和實體實作，同時決定了行為的實作方式，這種抽象型態，讓架構合規範軟體得以執行於不同的實作環境。然而，這種抽象太過簡單，微架構和實體實作可能遭到通稱「其他管道」的機制利用，因而損害安全性。而且，由於這類攻擊仰賴的屬性並非由架構定義，導致架構本身也無法因應這些問題。不過，我們仍有解決的辦法。舉例來說，我們都知道，存取模式和金鑰加密演算法的執行時間必須不受金鑰影響。架構可透過這項特性帶來助益，例如提供指令來加速通用加密演算法，如此即無需使用獨立於資料的資料存取途徑。Arm在Armv8.4中推出一項機制，可讓軟體用來指示現行程式碼，要求執行時間不受處理資料的影響。

長久以來，將裝置和系統設計分門別類的「孤島型」專業，目前正受到檢視。若要扭轉我們與駭客之間的「被駭-修補漏洞」這種無止盡戰役，就必須這麼做，重新整合軟硬體團隊的努力，將安全防護標準繼續向上提升。

# Arm 宣言

## 履行IoT數位社會契約

**Simon Segars**
Arm執行長

Lloyd's of London預估網路犯罪每年在全球造成的損失高達5000 億美元，因為各產業的系統和裝置安全性通常不足。

在本宣言中，我們已提出多種科技進展的構想來協助降低網路攻擊，不過創意本身不足以解決問題。如同 Mary Aiken 博士在序言中所述，使用者是自己的第一線守護者，這表示民眾可以遠離可疑網站、注意下載內容、變更預設密碼，並將裝置更新至最新狀態來修補安全性問題。

然而，儘管使用者應擔負自身安全的更多責任，但我們也知道民眾常常因為意外、衝動或分心，而作出損害網路安全的行為。因此，我們作為科技廠商，必須承擔所謂「數位社會契約」(社會契約)的責任，並致力於在任何情況保護使用者。

### 安全社會契約

依據社會契約，所有科技公司日漸承擔更重大的責任，因為連網裝置越來越普遍。網路攻擊者的手法益趨縝密，因此必須將安全性作為設計考量的第一要務，確保安全防禦措施涵蓋所有威脅範圍。這項社會契約，將成為科技業和使用者之間的信任基礎。

### 違背社會契約

Mirai殭屍網路在2016年發動的攻擊中，駭客尋找小量日常IoT裝置的安全弱點，透過大量資料請求來轟炸網路，導致重要視訊串流和社群媒體網站被迫關閉。當時攻擊集中在美國網域名稱伺服器(DNS)公司Dyn，將主機服務轉換至外部網域，後果就是他們立即損失14,500名客戶[1]。

我身為科技公司執行長，深知Arm必須堅守社會契約，讓企業或個人安心使用我們的技術。這表示，我們必須投入心力解決問題，甚至提供更多選擇，例如我們最新發佈的平台安全架構PSA (Platform Security Architecture)，以利引導安全的裝置實作。我們同時也在考慮透過更多方式與產業生態系統合作，藉此提高攻擊和漏洞資訊的流通性和透明度，確保問題不再重複發生。

### 對安全高度敏感的產業所產生的衝擊

履行社會契約的挑戰，依公司的類別而有所不同，以汽車市場為例，這個擁有100年歷史的產業，正處於劃時代的顛覆過程，所有人的目光都轉向電力、混合動力車款和全自動駕駛。

在過去，汽車公司從產品設計到交付階段，需要花費7-10年。如今，由於科技公司產品上市時間縮短至少一半，這樣的競爭也讓汽車公司加速創新周期。這樣新的競爭情勢可能會損害社會契約，帶來更多風險。不過，汽車業者都必須達到功能安全標準，確保車輛符合嚴格的安全目標。在這類案例中，社會契約是以法律上的注意義務 (duty of care) 作為基礎，因此，當汽車製造商努力趕工的同時，相互競爭的科技公司則在學習，如何在高度管制的安全環境下營運。

聯網汽車的競爭，確實已經面臨挑戰，使 (非法律意義的) 社會契約受到威脅，最可怕的莫過於駭入汽車，進而劫持安全系統[2]。雖然這並未違法，但已導致信任受損，因此，這方面引發了更多關注。

## 快速上市的IoT模式

社會契約面臨的更大風險在於產品上市速度過快。這對所有市場都有影響，不過在商業市場和關鍵基礎設施方面的傷害更大，因為這些領域遭受攻擊的損失可能更高。威脅日益增加的證據來自美國能源部，該部會今年針對電力系統提出網路攻擊警告，「危險正逐漸逼近」[3]，且威脅的「複雜性、規模、頻率」都在增加。此外，英國新成立的國家網路安全中心報告指出，去年共出現約600起「重大」攻擊[4]，另也預防了數千起攻擊。

因此，隨著連網技術不斷擴張，我們也必須重新思考。若要在快速上市的產業中取得成功，就必須奠基於設計、出貨、分析、轉型 － 加速學習及反覆練習的腳步，但是這些模式卻有損害安全之虞，因為產品部署之後，內部弱點可能無法在現場修正，導致系統更容易遭受攻擊。在講求設計和反覆速度的市場改進這種模式十分困難，因為要建立堅實的安全性並不容易，不但可能提高成本，更將拖累進度和利潤。因此，唯一可能的改善方法，就是思考如何提出更具恢復能力的全新商業模式，且不影響上市時間，這對於IoT等熱門市場尤其重要。達成的作法則如上面的章節所述，亦即為開發人員提供「始於安全設計」(secure-by-design)的技術，如此將能實現專為IoT建置的全新商業模式，而這樣的模式也符合社會契約的責任。

## 設計、出貨、分析、調整或隔離和處理：IoT的全新商業模式

全新模式將進一步提升晶片的安全性，同時讓系統防禦有更充裕的時間來回應，我進一步統整這些模式為：安全設計、出貨、分析、自我修復或隔離，最後則是處理 (如有需要)。對於IoT這類可能需要在單一系統部署大量連網裝置的市場，這種模式將成為一大關鍵。它將提供更精密的模式來保護系統完整性，同時確保科技業對產品生命週期負起責任。

上述模式亦可提供同時修補大量裝置的能力，如同修理手機故障一般，而這不是新的技術。另一項進展則是能夠如同手術治療般管理單一裝置，使得單一裝置能夠自行隔離並進行處理，直到能夠恢復原狀。這類全新商業模式的關鍵就是分散式智慧，這表示將現行主要位於雲端的強大運算能力，推廣至裝置網路的邊緣。如此一來將能打破僵化的「指揮-控制」結構，提供更靈活的分散式安全模式。這種作法與Milosch的想法一致，增強免疫系統並管理醫療服務。在這個生物學的類比中，免疫系統可處理大部分問題，但有醫療服務的適時介入會更好，其中包括推動大規模免疫計畫、臨床醫生的個人治療，或者是現在越來越普遍的DNA層級的治療，給予客製化的精準醫療 (precision medicine)。

## 缺乏標準

您可能已經注意到，我們全新的IoT安全模式沒有談到標準。我不是要排除標準，我認為業界公司和政府將貫徹這些標準，聯合國甚至也可能介入，因為此機構已將網路世界視為戰區。

對Arm來說，我們確實認為標準和政府規定通常都是過去式，而對於如IoT如此快速演變的世界，我們需要的是展望未來。駭客動作通常也較產品製造還快，因此我們的手法必須具備前瞻性、靈活和彈性。讓我們回到免疫系統的類比：此系統將需要對前所未見的威脅作出回應，就如同白血球如何攻擊視為威脅的異物。

## 目標

根據Gartner分析師的研究指出，截至2017年底為止，全球將有84億台聯網裝置[5]，預計在未來三年內這個數字就會成嘗到超過200億台，成長率高達150%。因此，網路犯罪相關的金額達到超過4,000億美元現在看來很驚人，相較於未來我們將面對一個將有依照台聯網裝置的世界來說，這個金額可能只會是口袋裡的零錢而已。

在本宣言中我們所陳述的策略與思維將有所改變，我也預期將看到我們成功的將駭客阻隔於我們的企業之外的世界。

社會契約理論：這是哲學史之初就開始探究的理論，將個人道德和/或政治義務視為相互訂定的契約或協議，來形成彼此共處的社會。
資料來源：: http://www.iep.utm.edu/soc-cont/

1. https://securityledger.com/2017/02/mirai-attack-was-costly-for-dyn-data-suggests/
2. https://www.wired.com/story/car-hack-shut-down-safety-features/
3. https://www.bloomberg.com/news/articles/2017-01-06/grid-in-imminent-danger-from-cyber-threats-energy-report-says
4. http://www.bbc.com/news/uk-41478608
5. https://www.gartner.com/newsroom/id/3598917

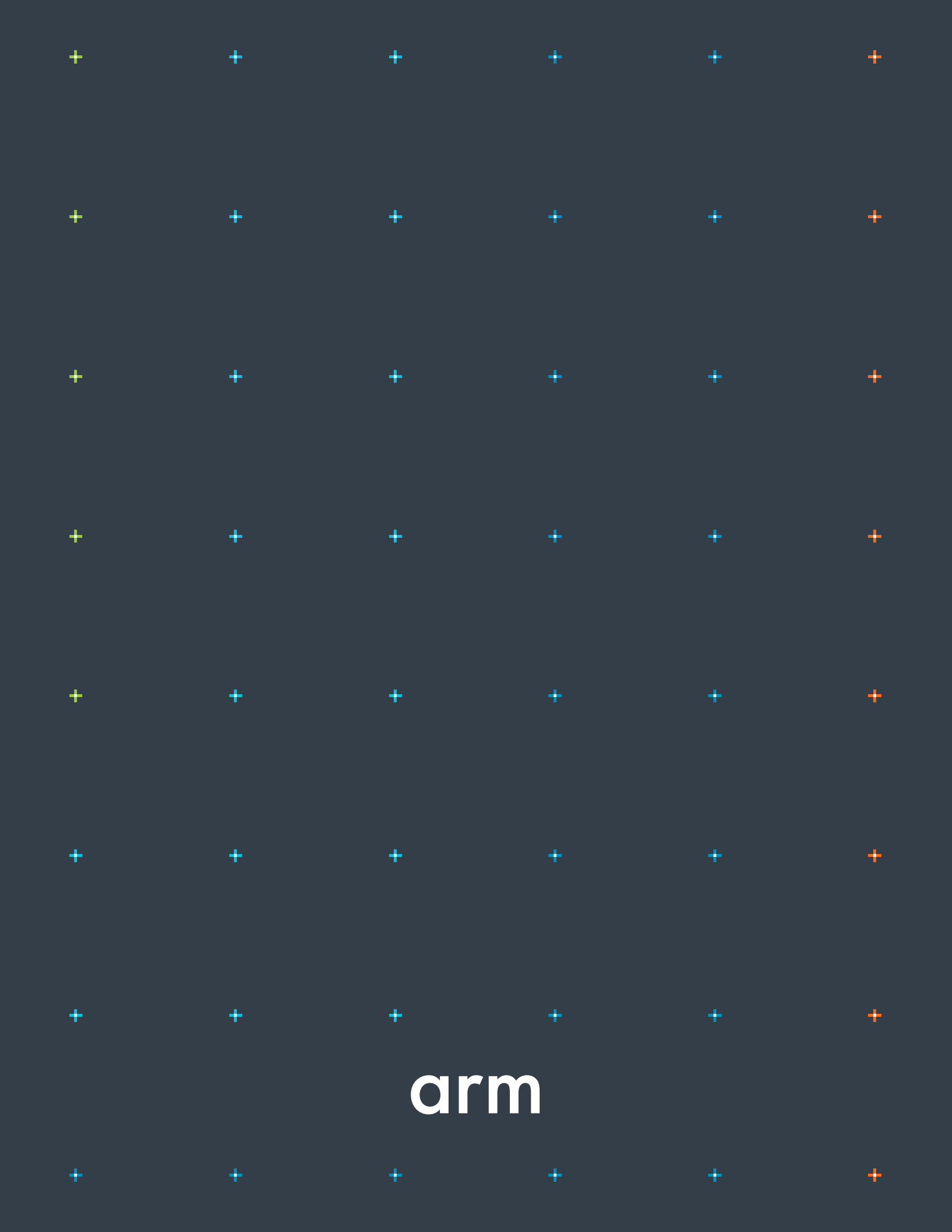
arm

我們見證了重要的基礎設施、醫療服務系統遭受勒索網路攻擊，以及作為網路閘道的家用電子裝置受到駭客侵襲。身處業界的我們，正站在命運的十字路口。一個方向有著許多同樣混亂且成本高昂的貓捉老鼠遊戲，科技快速進展，隨之而來的則是漏洞和修補。我們提出的另一個方向，則受到一系列共同信念所指引：

# 安全宣言

- 隨著連網世界逐步擴張，我們必須增加信任感
- 沒有公司可自外於與使用者共同遵守的社會契約
- 安全是業界的集體責任，創造機會卻也帶來挑戰
- 先進安全智慧應遍部在整個物聯網內
- 安全性必須是設計考量的第一要務，並關注產品的終身防護
- 我們必須建置安全系統，以因應潛在的人為疏失

**下載Arm 物聯網安全宣言:**
http://pages.arm.com/iot-security-manifesto.html


arm