電子投票安全嗎？

法務部調查局資通安全處　雷喻翔

電子投票系統簡介

傳統投票方式所需耗費的人、物力資源，隨著選舉規模不斷擴大而逐漸攀升，為了減低資源浪費，電子投票（e-voting）在過去的十幾年受到了電腦科學家廣泛地研究，許多可行的機制也被提出討論。

好的電子投票系統必須滿足以下幾點特性：

一、**全體驗證能力**：所有參與投票的角色，諸如投票人或監票人等，可以驗證整個投票的過程以及最終結果。

二、**個人驗證能力**：每位投票者可以確認他的選票是否已經投出、是否已經成功地被紀錄以及是否被算進最終的計票結果。

三、**可靠性**：投票的過程是否可以有效偵測惡意投票行為。

四、**一致性**：無論是由誰來觀看投票流程，都會得到相同的選舉結果。

五、**匿名性**：只有投票者本人知道他自己選票的內容，也就是要達到無記名投票的目的。

好的電子投票系統除了可減低資源浪費，提高開票效率，更可增加民眾政治參與度。

六、**透明度**：為了確保公平及有效原則，整個投票過程必須是公諸於大眾。

為了達成上述的條件，從而設計出有效的 e-voting，專家學者們採用了兩項有用的工具：密碼學中的盲簽章（Blind Signature）以及區塊鏈技術。

盲簽章

個人可驗證性、可靠性及匿名性可以視為投票者對於是否達成秘密投票程度的指標，盲簽章這項技術的優點可符合以上三項特性。在講盲簽章的流程前先了解何謂數位簽章：電子世界中要如何證明某一個文件的內容沒有被竄改過呢？這時候便可以用數位簽章來確保此事，首先將文件內容透過 MD5（一種雜湊函數）計算後得到一組值，接著同時傳送文件內容以及計算後的值，這時候任何人都可以針對該文件藉由 MD5 的演算法算出另一組值，當這兩組值的內容相等時，我們便可以放心地說所收到的文件內容與原始的內容是相同的。

這種可受驗證的數位簽章確實可以保證傳遞的內容不會經過修改，但是若放到 e-voting 中，那將會違反無記名投票原則，因為如果必須一併送出原始內容方可驗證，那麼自己的投票意向不就暴露於第三人了嗎？因此盲簽章的精神便是：驗證方不需要對原始內容簽章，驗證方所簽章的內容可以是傳送方加密過的內容，只要這個加密的內容使用者可以復原即可。

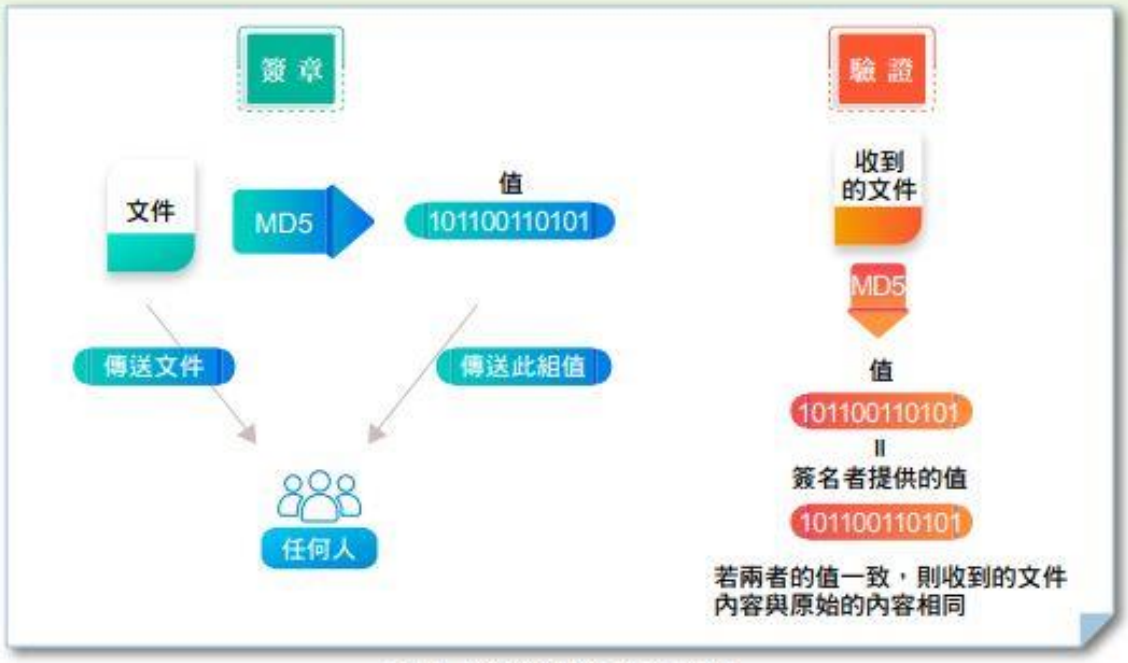


圖 1　簡單的數位簽章原理

我們用以下一個簡單的例子來描述盲簽章的過程：甲是一位擁有投票權的合格選民，乙是選委會，甲如何獲得具有選委會簽章的合格選票呢？甲有自己的加密模組 $E_{甲}$及解密模組 $E'_{甲}$，還有一張選票 V，乙則有 $S_{乙}$簽章模組。

流程如下所示（參考圖 2）：

一、甲先用自己的加密模組將已經有圈選結果的選票加密，接著將加密結果傳給乙。

二、乙收到甲傳來的訊息，由於乙無從得知甲的解密模組，因此無須擔心乙會知道甲秘密投票的內容。乙用自己的簽章模組對甲送過來的訊息進行簽章，然後便將這個資訊再回傳給甲。

三、甲在得到了乙所傳遞過來的訊息後，用解密模組 $E'_{甲}$解出 $S_{乙}(V)$，這便是乙對於甲的投票內容所做的簽章。

根據上述的步驟，甲在無須揭露自己投票內容的前提之下順利地獲取了乙方對於甲方投票內容的簽章。個人可驗證性、可靠性及匿名性在這個簡單流程中都得以確保。

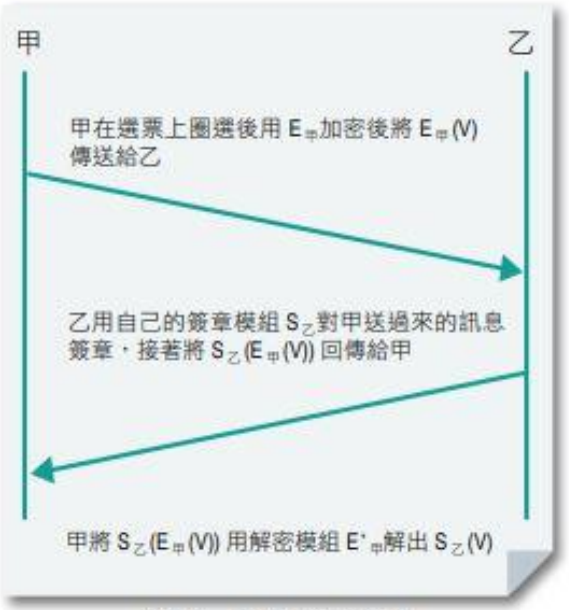


圖 2　盲簽章的過程

區塊鏈擁有不易竄改、高共享性、以及去中心化的特性。

區塊鏈

相較於盲簽章較著重在於「秘密投票」這個目的，區塊鏈則是著重於 e-voting 在「公眾使用」上的透明度。區塊鏈是一項源自於比特幣的技術，它是一種資料結構的概念，區塊鏈中的所有資料都是以區塊（block）的方式呈現，區塊和區塊間彼此連結成串，我們可以抽象地將之想像成為鏈狀結構，這也是區塊鏈之所以會如此命名的原因。

要在區塊鏈上建立一個新的區塊節點，必須遵守區塊鏈對等（Peer-to-Peer, P2P）網路上的相關規則，任何違反建立規則的區塊將不被區塊鏈所接受。為了達到去中心化及達到共享性的目標，每一個區塊鏈上的資料都是分散地儲存在雲端上，任何人都可以存取。經由使用區塊鏈，所有的資料傳送不再是單純的點對點擁有資料，而是將資料傳至公開的 P2P 對等網路上，一切的資訊都可透明接受檢驗。

接續上個章節，投票人取得選委會簽章，投票內容也獲得選委會的確認；接下來的實際投票動作，投票人用另一組非對稱金鑰，將本身的選票以及從選委會獲得的簽章一併傳送至區塊鏈網路，由於這一組非對稱金鑰僅個人知道，因此這一動作可以實踐秘密投票的要求；最後一個步驟是投票後整理階段，選委會從區塊鏈網路上驗證每一張選票是否符合選票格式、是否具有選委會發出的簽章、是否於投票截止日前投出及該張選票是否已經計算過。由於區塊鏈的性質，整個過程可由所有參

與人以及可存取區塊鏈的第三方共同進行計票以及稽核。

相關議題

在前述所介紹的盲簽章及區塊鏈技術，的確可以建立起一套可運作的基本電子投票系統，然而在實際的運作及更嚴謹的安全性上仍有一些議題需要考量。第一是身分識別的問題，資料透過 P2P 區塊鏈網路來溝通傳遞，有了公開透明的好處，但是也帶來了暴露投票者 IP 的風險，進而透過網路封包分析，勾稽出投票者與投票結果的關聯。

為了避免暴露 IP，經由洋蔥網路（TOR）隱藏個人的 IP 成為一種可能的解決方式；第二點是資料的保密及中立性。P2P 區塊鏈網路雖公開透明，但反面來看是在投票的過程中，投票進度也揭露於公眾，這多少也會影響選舉的最終結果。一種最直接的解決方式是不採用誰都可存取的公眾 P2P 區塊鏈網路，而是採用具一定程度權限控管且須經過授權的區塊鏈網路。然而要提高保密程度，公開透明就會遭受到質疑，這也是系統設計過程中需要取捨之處。

隨著資訊科技的進步，電子投票技術時至今日已算略具雛形，然而投票本身無論是政治性的選舉或是公投，其結果都是社會大眾矚目的焦點，只要投票過程稍有爭議，主事者難免遭受非議，因此在尚未百分之百處理潛在性風險之前，應持續提升相關的技術研究。

一些法國城市會使用投票機，但在 2017 年，法國外交部宣布總統選舉為完全紙本作業，避免資訊安全的隱憂。（Photo Credit: Wikimedia Commons, https://commons.wikimedia.org/wiki/File:IVotronic_img_3452.jpg#/media/File:IVotronic_img_3452.jpg）

本文摘自清流雙月刊中華民國109年1月 號P47-P51

無煙硝的5G戰爭

法務部調查局資通安全處　雷喻翔

／法務部調查局資通安全處　雷喻翔

美、澳、歐洲已有不少電信業者搶先推出5G（The fifth generation mobile communication）服務，其餘各國將相繼在2020年走入5G時代。

從1G到5G

早期8、90年代的電影中，常會看到重量級人士帶著一隻又大又重，俗稱「黑金剛」的手機，這便是第一代行動通訊—1G，也就是手機的濫觴，當時手機通話僅限於單純的類比式語音通話傳輸，有如行動版的家中電話；2G相較於上一代則是從原本的類比式語音改成數位化方式傳輸，除具有通話功能外，另外加入簡訊功能，逐漸具目前熟知的手機雛形；除了藉由行動通訊來傳輸文字資料，通訊專家開始著手讓手機可以快速地傳送大量資料（包含語音、文字、影像及圖片等），第三代行動通訊3G於焉誕生。

第一代行動通訊因外型巨大，被稱為「磚頭」或是「黑金剛」，功能僅限於單純的語音通話傳輸（左 1）；後來則加入簡訊功能，發展為第二代行動通訊（右 1）。

第三代行動通訊則為大眾熟知的智慧型手機通訊，已可快速且大量的傳送各種資料。

圖一　第一代至第五代行動通訊特性

第五代行動通訊的超可靠度和低延遲通訊使無人車駕駛這類對時間有嚴格要求的技術不再是未知數。

雖然 3G 已可經由行動傳輸達到近乎家用型電腦的功能，然而在傳送即時串流（real-time streaming）的影音資料時，仍無法滿足對於此類型資料的服務品質（Quality of Service）需求，於是 4G 做為一種解決方案被提出。4G 摒棄了傳統電話語音所使用的電路交換技術（circuit switch），轉而採用與網際網路（Internet）相同的封包交換技術（packet switch），進而達到全 IP（all-IP based）的行動通訊機制，大大提升傳輸性能及速率；4G 看似滿足了消費者對於行動傳輸的需求，但隨著 IC 晶片技術的發展，晶片尺寸愈發縮小，從原本的筆記型電腦到手機，甚至隨身手錶、眼鏡等都可內建 IC 晶片，在這種條件下，研究人員開始想像一種可能性：是否能讓所有可見的裝置都內建晶片，讓這些裝置彼此溝通傳遞訊息，達到資訊共享的境界，這就是物聯網（Internet of Things, IoT）的構想。為了達成萬物皆可連的目標，原本的 4G 技術已無法完全滿足，因此 5G 規格的訂定及相關研究如火如荼地開展。國際行動通訊組織定義出 5G 三大具體目標（圖二）：

一、增強型行動寬頻通訊（Enhanced Mobile Broadband, eMBB）

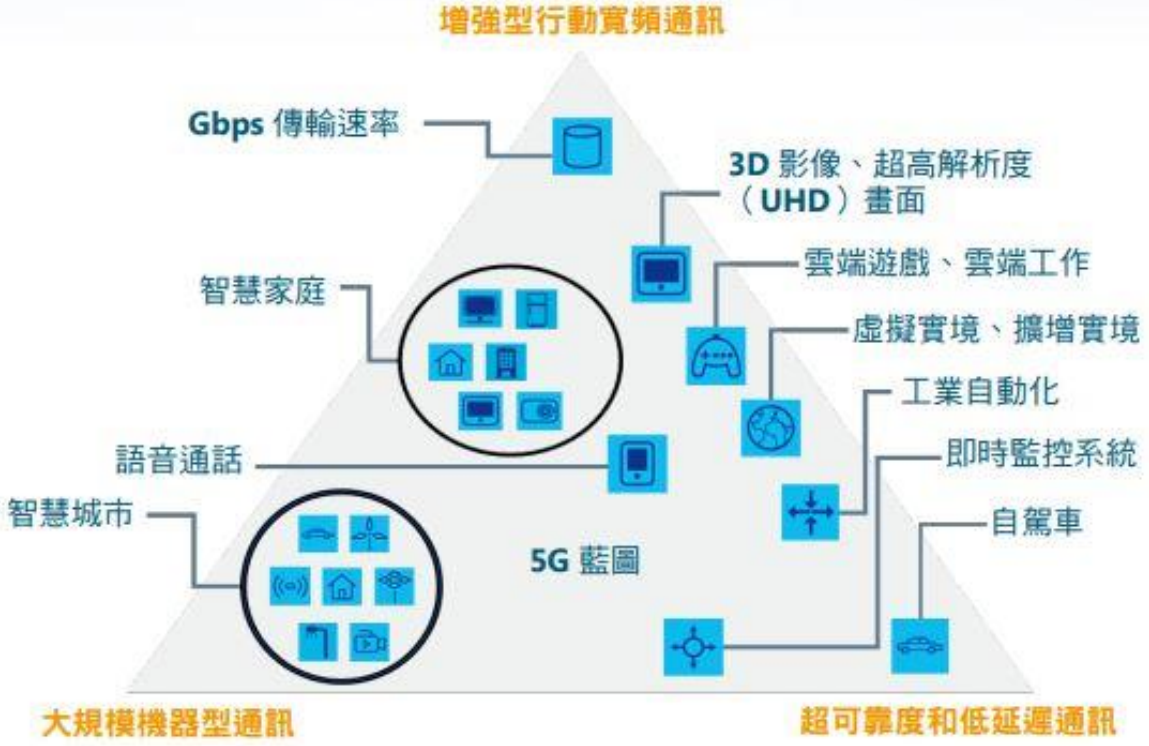
4G 擁有可提供靜態傳輸速率 1Gbps、高速移動下傳輸速率 100Mbps 的能力，5G 技術進一步提升傳輸速率達到 10Gbps（光看數字可能無感，讀者可以想像往後下載一部 8K 的 3D 影片只需 1 秒鐘的時間），有了高傳輸速率的 5G 便可以提供更多樣的行動應用。

二、超可靠度和低延遲通訊（Ultra-reliable and Low Latency Communications, URLLC）

物聯網的情境下，以往電影中的場景都將搬到現實生活，例如工廠生產過程的監控、智慧城市的交通控制樞紐、無人車駕駛以及遠端醫療等都不再是不可能。然而這類型的應用對於通訊的可靠度以及通訊間的回應時間都有高度且嚴格的需求，延遲時間依照標準需低於 1 毫秒。

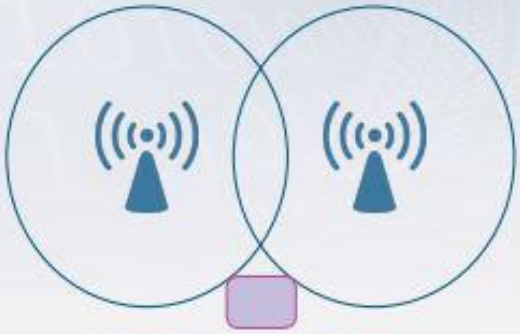
三、大規模機器型通訊（Massive Machine Type Communications, mMTC）

所想像到的物品都可連上網路，彼此之間傳遞訊息，新的 5G 規格必須能夠支援上述場景。平均而言，可能在每平方公里內將會有上百萬的裝置同時發送資料。



圖二　5G 三大具體目標

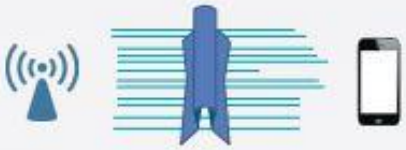
資料來源：節錄修改自 https://www.itu.int



圖三

圖四

圖五



圖六

要達成上述三大目標的關鍵通訊技術有下列四項：

一、小型基地臺（Small Cell）

以往由大型基地臺覆蓋手機通訊區域的做法將不足以應付物聯網時代的來臨。考慮圖三及圖四的場景，圖三中沒有在兩個大型基地臺所覆蓋區域的裝置將無法接收到基地臺的訊號，若在這個區域中想要建構物聯網，則這些裝置無法發揮資料傳遞之效；圖四中原本無訊號覆蓋的區域現在加入了小型基地臺，則物聯網裝置可以連至網際網路，成為大雲端的一分子。

二、大量多天線技術（Massive Multiple-Input Multiple-Output, Massive MIMO）

多天線技術（MIMO）在4G已被提出，但為了提升傳輸速率，基地臺及使用者裝置都必須要有更大量的 MIMO。終端裝置跟基地臺的溝通是藉由天線接收與傳送達成，直覺想法是藉由大量的天線來達成目

在物聯網中資料連結有可能是手機跟手錶、家電跟眼鏡等，之間的通訊協定不一定是透過語音資料，也可以經由藍牙、近端無線通訊、紫蜂感測網路或是 Wi-Fi 等協定進行通訊傳輸。（Photo Credit: AGCO-Fendt, https://commons.wikimedia.org/wiki/File:Standort_Jackson.jpg）

的，拜 IC 晶片進步之賜，Massive MIMO 已然成真。

三、波束成型（Beamforming）

無線通訊是藉由電磁波傳輸。電磁波發送的特性是向四周 360 度散開，但基地臺跟終端裝置之前的資料傳輸卻是單方向的，因此會造成電磁波的浪費。波束成型的提出就是為了解決電磁波浪費，將原本會四散開來的電磁波裝束成一把，針對固定的方向指向性傳送，如此一來能量變強，可傳輸的距離也更遠，大幅提升傳輸的效率，如圖五及圖六。

四、網路切片（Network Slicing）

以大規模機器型通訊而論，5G 網路的架構將不再只是單純基地臺與手機之間的通訊模式，物聯網世界裡，資料連結有可能是手機跟手錶、家電跟眼鏡等，之間的通訊協定不一定是透過傳統的語音資料通訊協定，也可以經由藍牙（Bluetooth）、近端無線通訊（Near Field

Communication, NFC）、紫蜂（ZigBee）感測網路或是 Wi-Fi 等協定以提高使用者體驗。但在這種多協定的異質網路底下，如果要進行系統建置與變更極為困難。

為了克服此種情境，網路切片就成為關鍵技術。所謂網路切片其實是軟體定義網路（Software Defined Network, SDN）及網路功能虛擬化（Network Function Virtualization, NFV）兩種技術的集合。前者就是把原屬於網路硬體的功能以軟體來取代，用以增加管理者修改及維護的彈性。後者是將原本的核心網路設備，例如防火牆（firewall）、路由器等，藉由軟體實作其功能，並將這些功能部署於通用規格的硬體中，當管理者想要更換其中某一項設備時，僅需在該臺通用硬體中，以軟體更新的方式替換掉對應的功能即可。

5G 安全性議題

承襲前幾代的行動網路發展而來，5G 可能的資安威脅也繼承了原有架構可能遇到的資安問題。

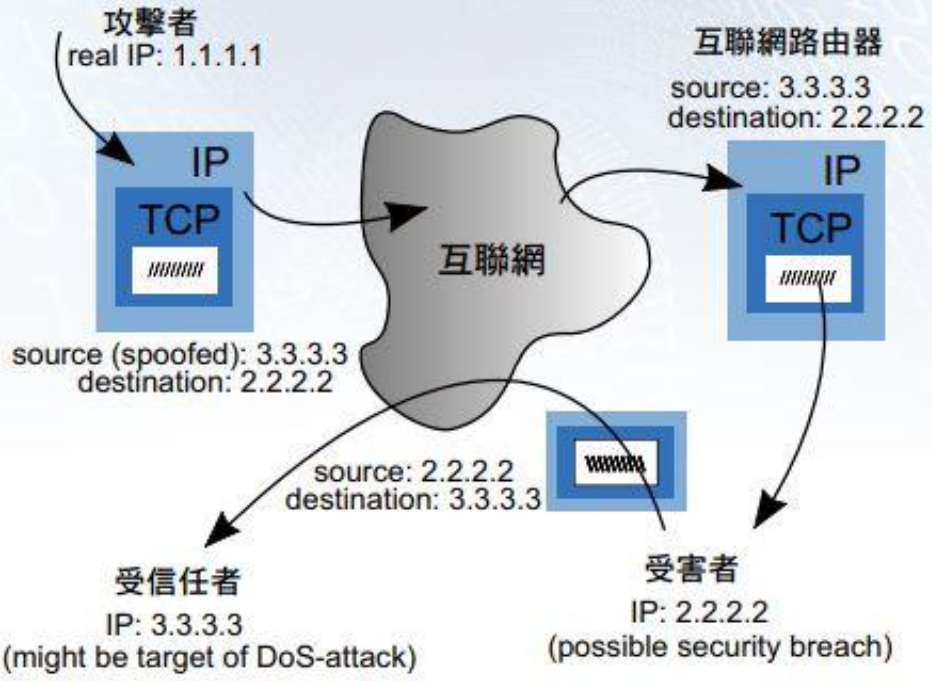
一、行動雲端計算

5G 架構下的雲端計算可以分成用戶端（client）及伺服器（server），用戶端最常遇到的資安風險就是潛藏手機中的惡意程式或間諜程式，透過使用者不經意的下載，植入到用戶端的裝置中，潛伏蒐集個人敏感資料或是破壞整體系統效能。雲端伺服器常見的攻擊則有 XML DoS（Extensible Markup Language Denial of Service），藉由產生大量的 XML 訊息來迅速耗盡伺服器的儲存空間進而導致伺服器癱瘓。另外由於網路傳輸的特性，使得 Wi-Fi 偵測（Wi-Fi sniffing）、IP 位址欺騙（IP Spoofing）及會話劫持（session hijacking）等仍是潛在的資安威脅。

二、軟體定義網路與網路功能虛擬化

軟體定義網路將原本部分屬於網路硬體的功能抽離出來，改由程式來控制，方便了網路管理者，同時也增加駭客攻擊的機會。由於軟體定義網路的控制器修改了原本資料傳輸的規則，因此屬於該控制器發送出來的封包在網路中很容易被辨識出來，這也增加了該控制器被鎖定使用 DoS（Denial of Service）攻擊的可能性。

網路功能虛擬化將分散的硬體裝置，以軟體的方式集中至一臺通用規格的硬體中，所以該臺通用規格硬體的使用者權限管理將成為最重要的議題，必須要嚴格地將所有使用者區分為一般使用者及系統管理者，兩者之間在伺服器中所能執行的功



IP 位址欺騙的示例情景。（Photo Credit: original by Nuno Tavares, this version by GGShinobi, https://commons.wikimedia.org/wiki/File:IP_spoofing_en.svg）

能及角色完全不同，系統管理者可以進行系統層面的參數修改，而一般使用者僅能使用系統管理者授權的權限進行操作。在通用規格硬體中的帳號稽核若是沒有落實，不該擁有管理權限的使用者有可能惡意或不經意地調整了網路底層應有的行為，進而導致系統崩壞。

最後，這兩者都大量仰賴軟體，然而如此龐雜的軟體工程，沒有人能完全保證軟體系統沒有任何錯誤（bug），一旦有了軟體錯誤，便為駭客提供了一扇入侵的門。

細究上述所列舉的 5G 安全議題，其根本原因是無線通訊架構的先天性所造成。此外，亦有人為刻意附加惡意程式之風險，則基地臺可利用後門程式，監聽或轉送所有經過該基地臺的封包。在關注 5G 所帶來的便利性的同時，亦須重視資訊安全的面向，以免得了便利卻失了隱私。

本文摘自清流雙月刊中華民國108年9月 號P66-P73