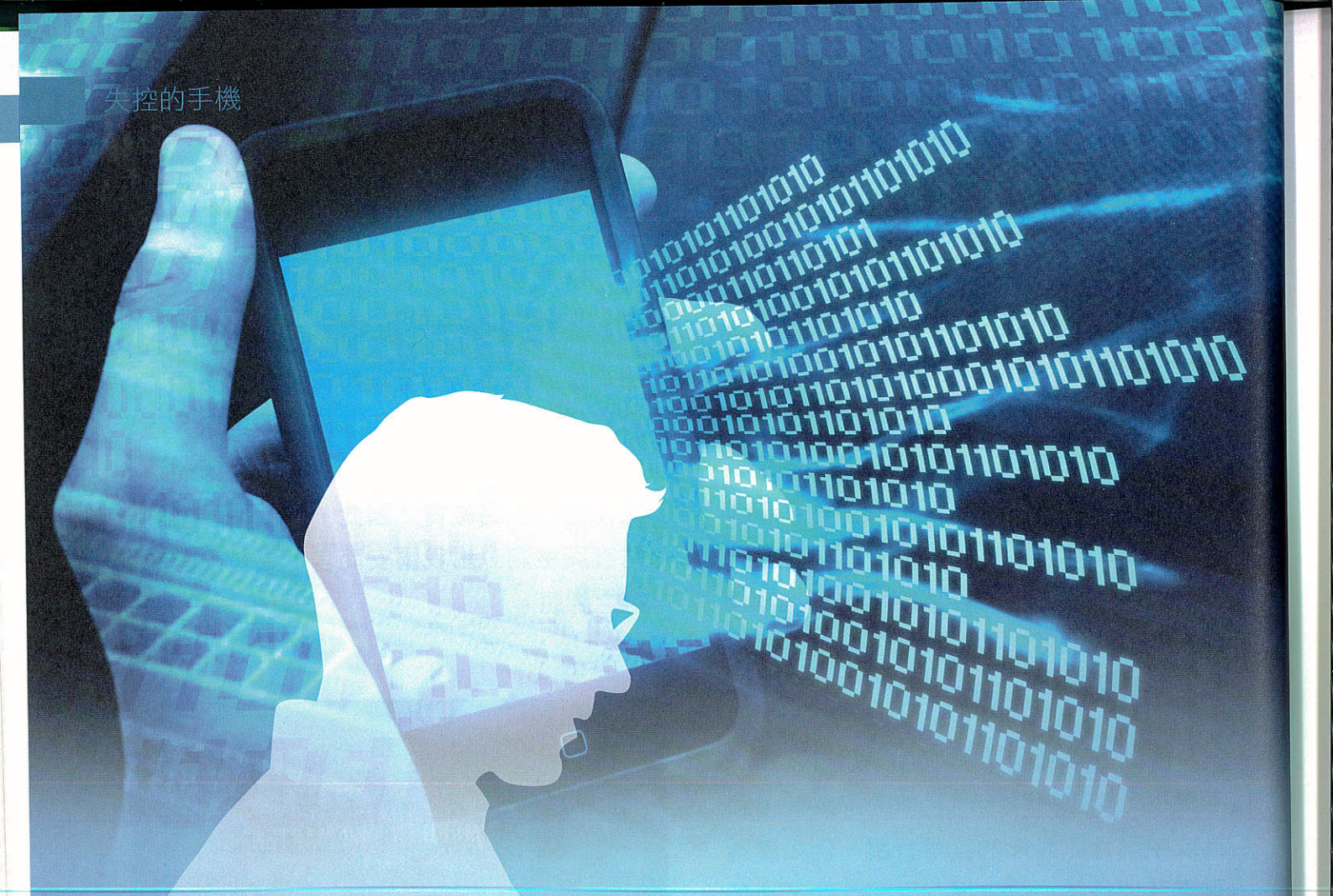
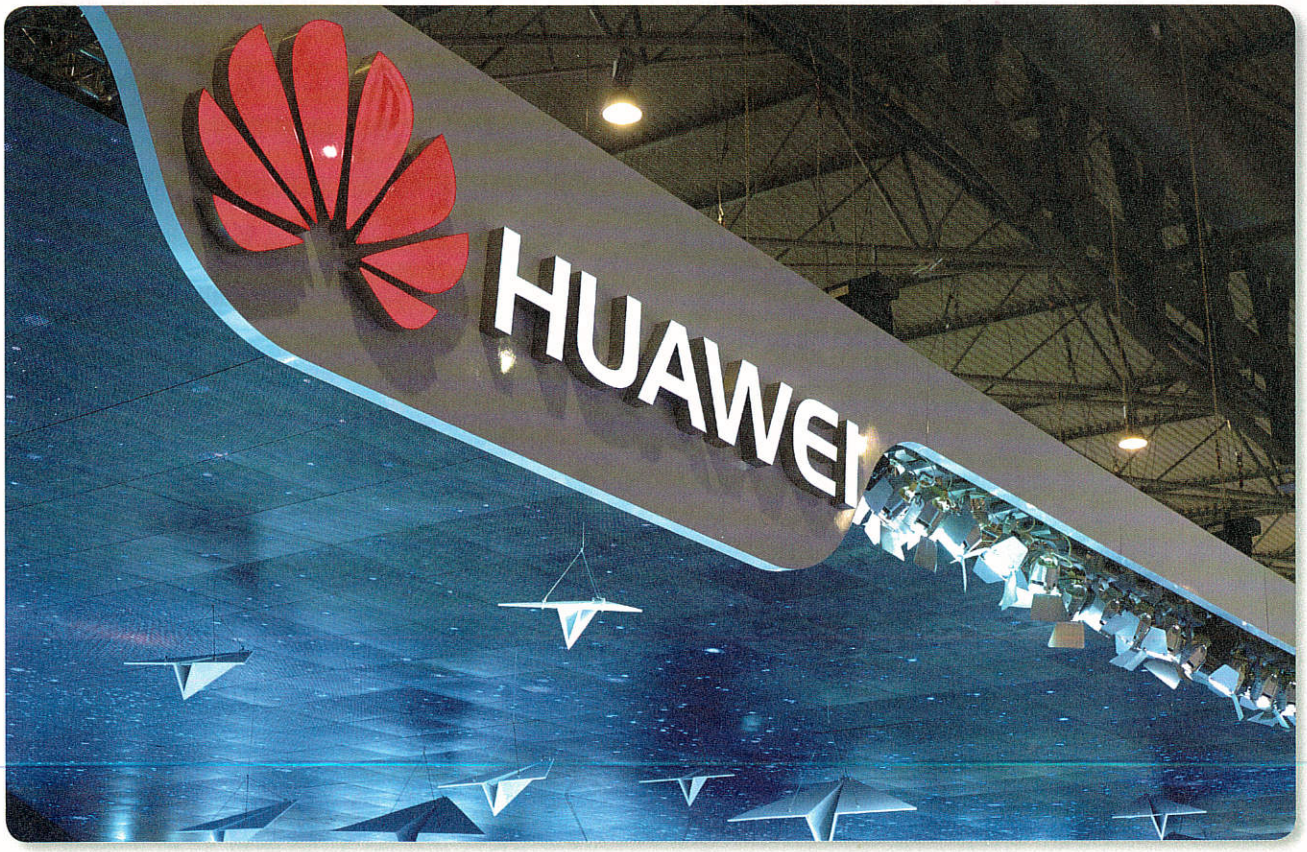


手機個資如何被竊取？

／法務部調查局資通安全處　雷喻翔

美國眾議院情報委員會數年前就曾公布調查報告，指「中國大陸廠商華為通訊所生產的設備，存在追蹤郵件、擾亂美國通訊系統的可能性」，此後阻止華為向美國通訊企業供應相關設備。



華為的通訊電子設備，可能被蓄意設計開後門漏洞，屢遭各國以國家安全考量拒絕採購。（Photo Credit: Kārlis Dambrāns, https://www.flickr.com/photos/janitors/16103977343/in/album-72157650786478488）

延燒國際的資安新聞

華為（Huawei）總部位於中國大陸深圳，以網路通訊設備起家，後來跨足智慧手機市場而闖出名號，近期卻屢遭各國以國家安全考量拒絕採購，指華為的通訊電子設備，可能被蓄意設計開後門漏洞，懷疑北京可能藉此非法收集境外國家用戶的通話內容；去年 10 月彭博社（Bloomberg News）報導，亞馬遜（Amazon）在 2015 年曾打算收購一家串流視訊伺服器業者，但在評估其產品安全中發現其上游的伺服器供應商超微電腦（Super Micro），疑似在組裝過程中遭植入中國間諜晶片，此外蘋果（Apple Inc.）也曾發現相似情形而終止和超微電腦的合約。

究竟我們所使用的通訊設備是否能夠守住使用者的隱私？高舉資訊安全大旗而拒某些通訊品牌於門外是否合理？

什麼是通訊設備？

通訊設備是個廣泛的名詞，從最上游的基地台、路由器、交換器，到使用者終端設備—也就是手機，都是通訊設備的

範疇。每個設備都是由極為精密的硬體（Hardware）晶片、使用者應用程式的軟體（Software）以及中介軟硬體的韌體（Firmware）所組成，任何一個環節都需要數十名至上百名的工程師通力合作才得以使其功能正常運作。正因為其複雜度之高，若在系統埋入具有特殊用途的系統模組，不正如在樹林中藏起一片落葉般難以察覺？

什麼是除錯模組？

程式開發階段由於系統還未穩定，研發工程師 RD（Research & Development）通常需要在原本的功能模組中另外加入除錯模組（debug module），當系統發生問題時能夠蒐集當下的資訊以便日後的分析。以智慧型手機為例，相信讀者一定有這樣的經驗：原本正常使用的手機卻突然毫無預警的關機、總是無法正常啟用某一個應用程式等，因此每間系統商都需要專門進行測試的人員，品質保證工程師 QA（Quality Assurance）應運而生。

除錯模組所扮演的角色就是在問題發生的當下盡可能地蒐集手機系統內的資訊，從手機 IMEI 識別碼、作業系統版號、系統時間、當下系統的記憶體快照等等全部蒐羅，藉由這些資訊讓 RD 可以詳細判讀系統狀態。除錯模組會將所蒐集的資訊存放在手機的內存空間中，等到 QA 完成了所有檢測項目後一次擷取在這過程中所產生的除錯資訊，再將這些重要的資訊傳遞予 RD。為加快軟體開發進程，通常 QA

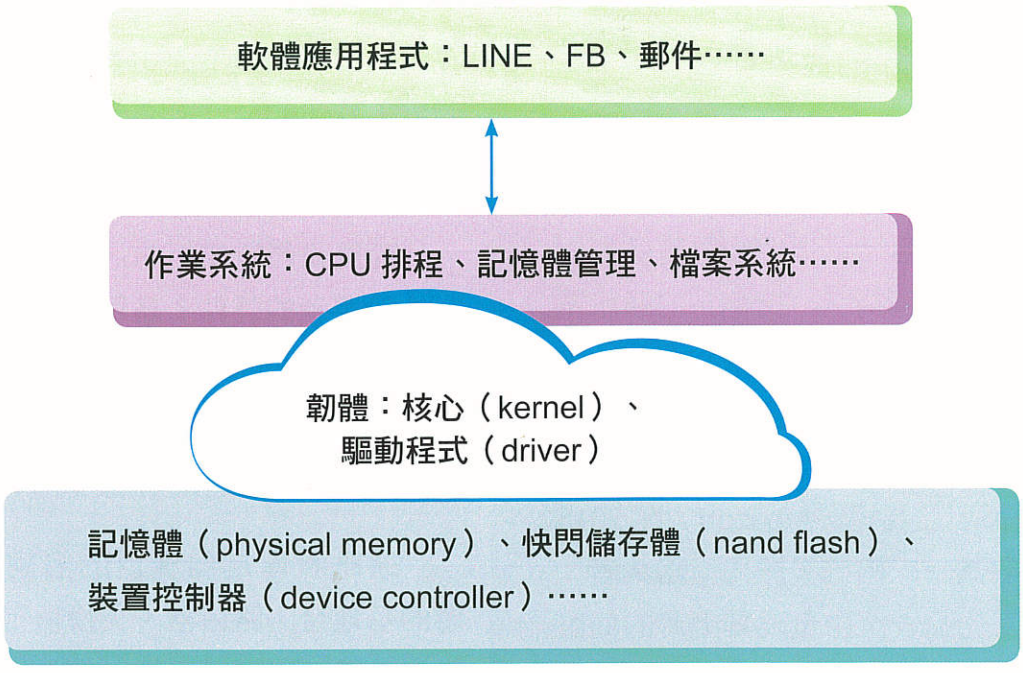
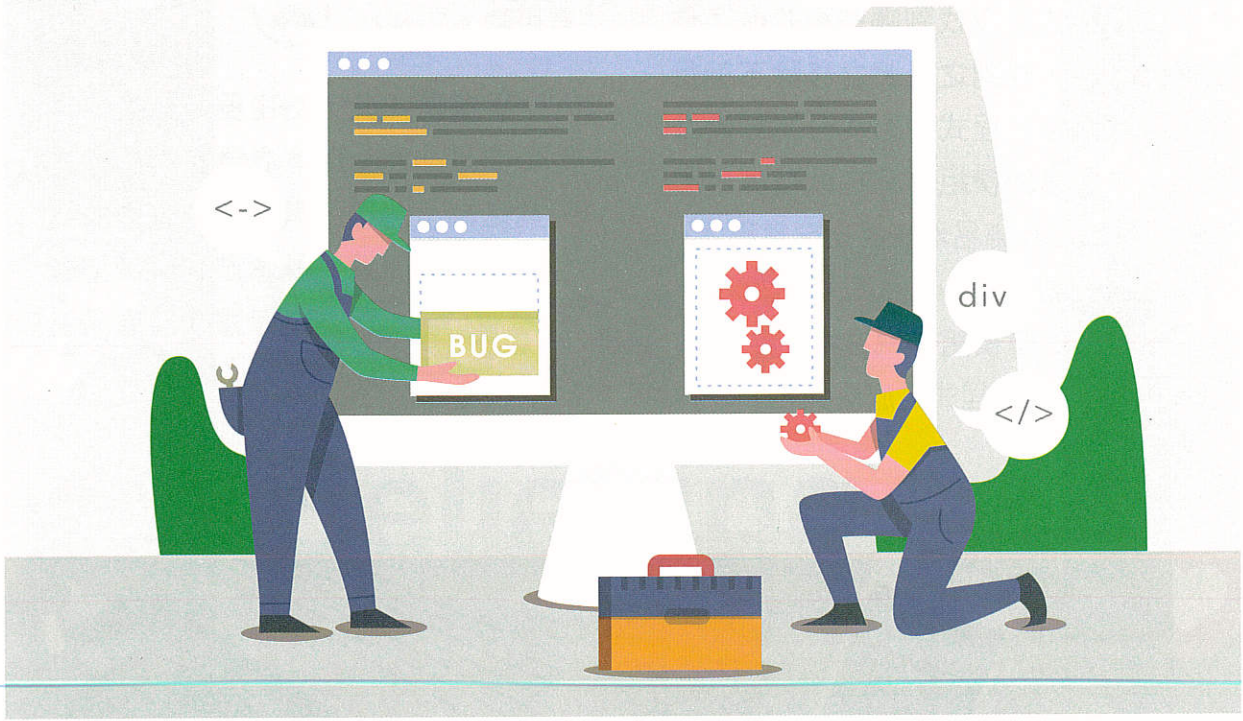


圖 1　通訊設備的基本組成



智慧型手機的系統開發，會經由 QA 檢測完項目後一次擷取除錯資訊，傳送給 RD 掌握問題並解決。

所測試的手機會配載網路 SIM 卡。網路狀況隨著位置的不同各有所異，有時候臺北、高雄兩地所產生的問題就是不同，所以 QA 必須機動性地全臺移動甚至全世界移動。進階版的除錯模組可以在問題發生的當下馬上將資料傳回某一台伺服器，RD 得以第一時間便掌握到系統發生的問題。

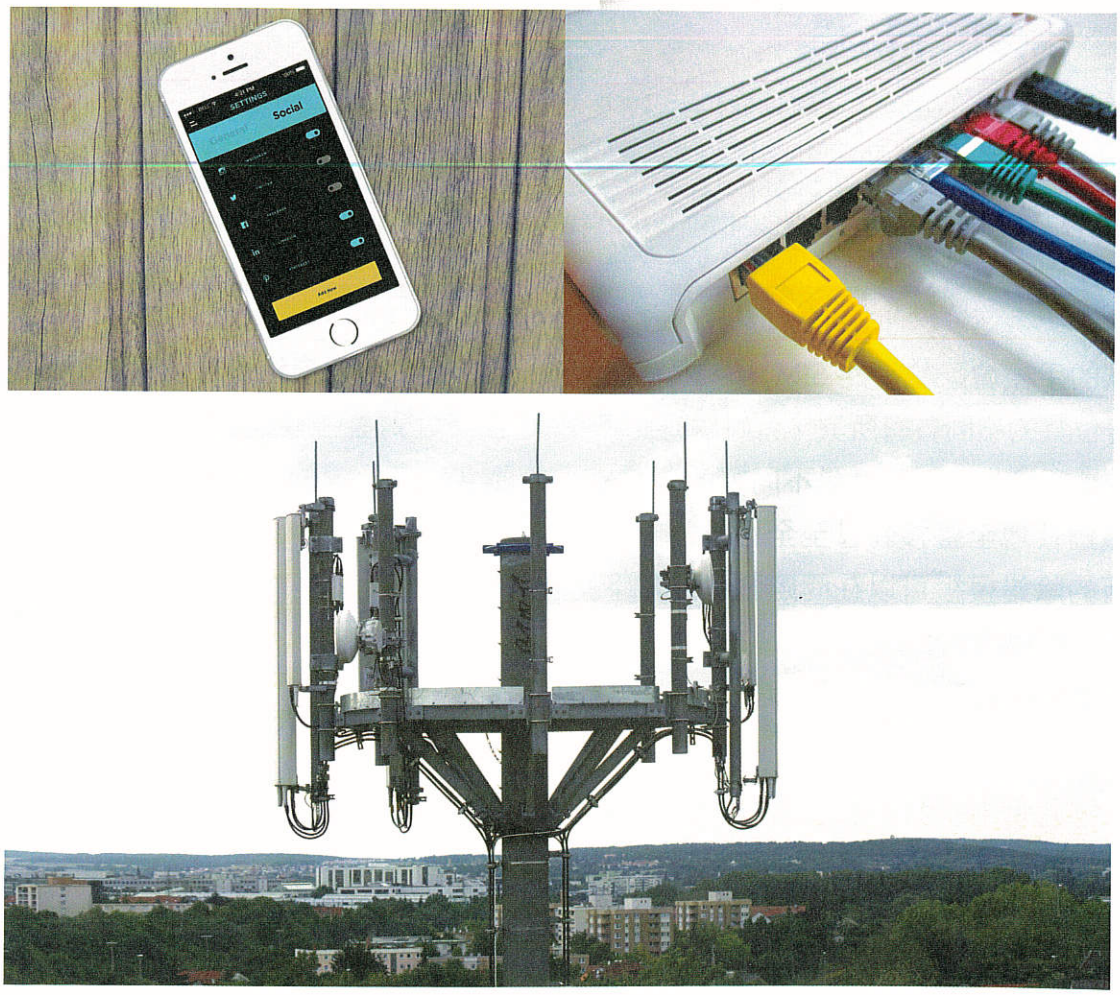
當除錯模組化身惡意模組

敘述至此，您是否已聯想到前述的行為跟惡意的駭客在手機中所埋入的後門程式有何分別？其實兩者本質相同，都是將系統中的資訊回傳至特定伺服器的程式碼，差別在於寫程式碼的工程師其主觀意念，究竟這個模組是為了幫助產品的開發，讓其達到盡善盡美的地步？抑或是藉以竊取手機使用者的個人資訊？

正常情況下，除錯模組只限定於開發階段，一旦產品達到上市的品質其將被移除，此模組將不再自動回報相關系統資訊。試著想像一個情境，如果某手機開發商收到一批訂單，從而知道該批下單的手機將用於其他國家的機敏機關，若該手機開發商所處的國家有意從中打探其他國家的內部訊息，那麼在開發過程中於動輒十幾萬行的程式碼中埋入一組惡意模組，似乎也不那麼令人意外。

或許讀者心中有所疑惑：「現在市面有許多應用程式可以找到哪些程式做了你不預期的行為，找到之後將之移除不就行了嗎？」然而系統程式的組成分為韌體及軟體，如果惡意的模組是寫在軟體應用程式層級，可以較為容易地發掘出惡意程式，但如果是寫在韌體之中，那麼事情就不是那麼簡單了。除錯模組是寫在韌體中的核心（kernel），即為程式最底層與晶片介接的部分，無法單獨分離出來，其隱密性不言可喻。

手機是如此，路由器、交換器甚至基地台亦是如此，原本立意良善的除錯模組究竟是為了開發所需或是別有用心僅在一念之間，然而只要是牽涉到機敏議題，為了資訊安全起見，在考慮購置通訊設備的過程中宜三思而後行。



手機、路由器、交換器甚至基地台，都可能因為植入惡意程式的除錯模組而導致資安危機。