投稿類別：資訊類

篇名：

從應用程式淺談資訊安全

作者：
劉懿陞。曉明女中。高二丁班
劉思旻。曉明女中。高二戊班

指導老師：
賴維真老師

壹、前言

一、研究動機

近年來，資訊科技快速成長，雖帶給人們很大的方便，同時卻也產生資訊安全（以下簡稱資安）的隱憂。丹麥 TV2 電視台於 2015 年拍攝一部紀錄片〈手機不設防〉，其中揭露人們常忽略應用程式（Application，以下簡稱 App）的權限須知，而不假思索地間接同意 App 侵犯個人隱私，這已充分顯現出資訊科技進步之發達所隨之帶來的危險性。當人們享受著這些 App 帶來的方便時，是否想過其相對的代價呢？這些 App 究竟存取了多少權限？是否為一安全的應用程式呢？我們想要一探究竟。

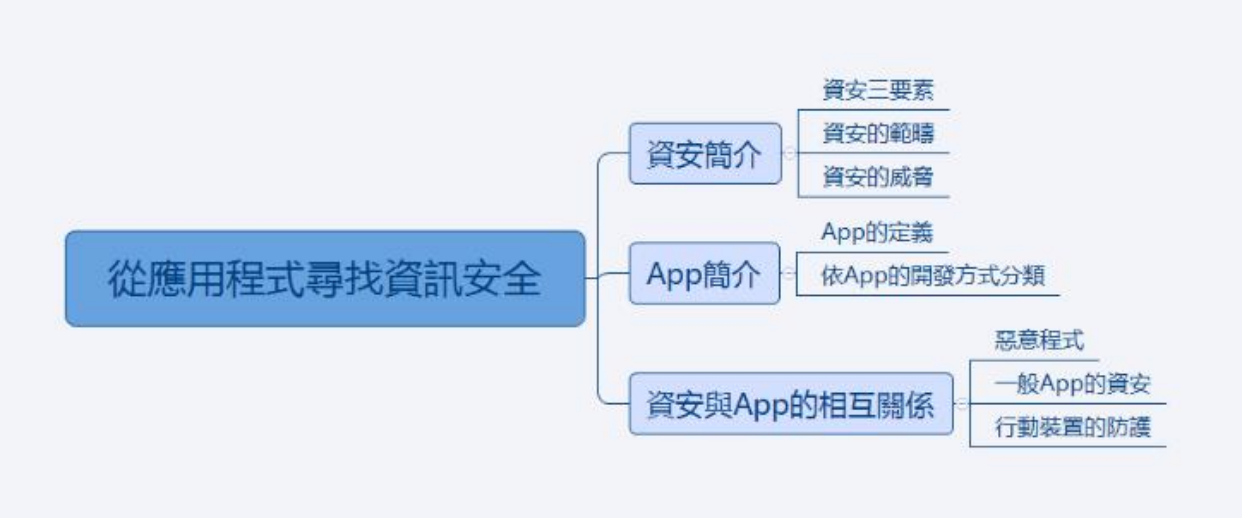
二、研究目的

希望藉由此次小論文，深入了解資安的重要性，並統整諸多資訊相關資料，探討與我們生活脫不了干係的 App 下載、其運作方法及牽涉的資安問題，經過嚴密的整理及思考後，尋找可行之解決方法。

三、研究方法

我們將利用網路上的論文、刊物，以及相關書籍，歸納出 App 與資安的相關性，討論並尋求兩者之間的平衡點。

四、研究架構



圖一：研究架構
（圖一資料來源：研究者繪製）

貳、正文

一、「資安」簡介

如何維護個人的資安，以免於遭人非法使用，近年來已成為一大熱門議題。當資安遭受威脅時，將會遭到重大損失，例如，在 2002 年，Yahoo 與 ebay 等著名網站遭分散式阻斷服務攻擊（Distributed Denial of Service，簡稱 DDoS），造成網路癱瘓，損失高達數十億美金。面對這樣的難題，我們不只應購買軟、硬體資安防護措施，資訊管理也不能掉以輕心。

（一）資安三要素

1、機密性：採取安全措施，以避免資料被無授權人員存取、使用或竄改。大部分的網路攻擊皆以破壞資訊的機密性為主。

2、完整性：維持資料的狀態，並確認資料內外的一致性，唯擁有權限的使用者可修改資料內容。

3、可用性：確保資料能夠正常運作，並在合法使用者的要求下，使資訊系統在適當時間下回應。

這三項要素稱為資訊安全三原則（Confidentiality，Integrity，Avalability，簡稱 CIA）。三者的關係相輔相成，缺一不可。例如，若只考慮資安的機密性，將資料加密，導致使用者無法執行行動，則將缺乏可用性。如今網際網路進步迅速，資安方面也隨之更顯重要，經由資安三要素的密切配合，並互相協調，如此一來資訊便可得到安全的保護。

另外，在資訊安全控管方面需要擁有以下列舉之特性：不可否認性，是為防止使用者否認以往執行過的動作；身分認證，確認使用者的身分；權限，依照使用者的職務及階級身分來做適當的權限劃分；可歸責性，將重要資料交由一位負責人管理，其管理紀錄可以被追究。

（二）資安範疇

「資安」一詞的範圍廣泛，包含許多面向，下表一為資安的 8 個範疇及其相關介紹。

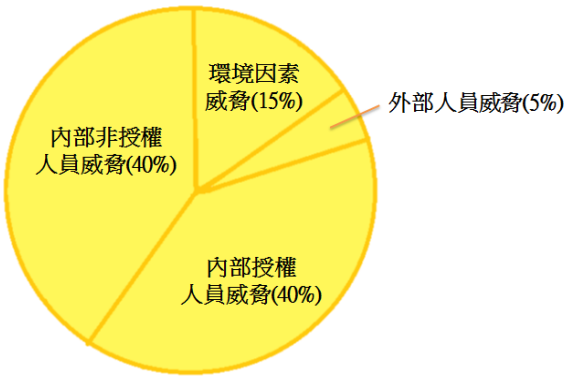
表一：資安的範疇與意涵

資安範疇	意涵
安全暨風險管理	藉由管理資訊安全及其風險，使其系統更加完善無漏洞，不讓駭客因此侵入系統。
資產安全	資產，能為個人或是企業帶來收益。近年來駭客喜歡侵入使用者的電腦進而獲取資產，資產安全也因此更顯重要。
安全工程	安全工程可協助聯繫各層面的資訊安全，並使其系統化。
通訊及網路安全	現今駭客會開放一組網路供人免費上網，而那組網路正是惡意程式之一，用以竊取使用者通訊等資訊。
身分識別暨存取管理	使用者的身分之於資料使用上非常重要，加強身分識別的嚴密性和嚴格管理存取資料，可預防駭客侵入。
安全性評估與測試	安全性的評估與測試需定期執行，以防止有意人士的破壞。
作業安全	駭客常利用作業過程中侵入系統，以獲取其想要的資訊，這時作業安全就顯得重要。
軟體開發安全	由於駭客可將開發人員誘至惡意網頁，因而取得新軟體的控制權，因此軟體開發安全的重要性也不容小覷。

（表一資料來源：研究者整理）

（三）資安威脅來源

近年來隨著科技的日新月異，資安的地位顯得越來越重要，資安所要面臨的威脅也日益增多。根據來源以及種類，我們將資安威脅略分為下面四大類：環境因素威脅，指天然災害，例如地震、颱風、火災等等；外部人員威脅，例如駭客、病毒；內部授權人員威脅，指作業疏忽或惡意竊取資源；內部非授權人員威脅，指非授權人員企圖竊取公司資源。而根據《資訊安全概論》（第二版）調查，我們整理出以下的關係圖（圖二）。



圖二：資安威脅來源比例關係圖
（圖二資料來源：研究者繪製）

二、App 的簡介

（一）App 的定義

近年來手機和平板電腦蔚為風尚，人們誤會行動手持裝置上下載的程式稱為 App，而電腦上下載的程式則是稱為軟體。其實從電腦上下載的程式也是 App，只是人們習慣稱 App 為從手機和平板電腦上下載而來的應用程式。

（二） 依 App 的開發方式分類

平常我們在應用程式商店所見的 App 種類繁多，常使我們看的眼花撩亂，其實 App 也可以依開發方式分類，如下表二，當中我們可以比較三種不同軟體之間的優缺點。

表二：App 的種類及其相關資訊

App 種類	定義	開發方式	優點	缺點
原生應用程式	作業系統廠商建議或是本身提供 SDK（軟體發展工具包）。	使用 Object-C 、Swift、Java、C、C++和 C#等程式語言開發程式。	1、執行快。 2、效能佳。 3、支援硬體裝置能力佳。 4、可上架於應用程式商店，並藉以賺取費用。 5、使用時不需打開瀏覽器及輸入網址。	1、需用指定程式語言或 SDK 開發。 2、開發測試過程中皆須程式編譯及部屬安裝的複雜過程，極為不便。 3、上架 App 需經官方審核程序。 4、部分開發者須繳年費至官方。 5、付費 App 官方需抽成。 6、App 更新後須重新上架及審核，而使用者也須更新或重新下再採可使用其新功能。
網頁應用程式	即網頁應用程式，因主要以行動裝置上的瀏覽器應用為主，又稱	使用 HTML、XHTML、HTML5 +、CSS +、Java Script 等。	1、針對不同裝置可用相同前端網頁技術開發。 2、測試時只需用用瀏覽器輸入網址或重新	1、執行速度不佳。 2、因對硬體支援度不佳，部分硬體功能便不敷使用。 3、需打開瀏覽器及輸入網址才能執行，部分功能需針對不同瀏覽器做不同的處理。

	行動網頁App。		整理網頁即可。 3、不須上架、審核，也不需繳年費至官方、抽成給官方。 4、更新時只需於後端網站主機修改，而使用者可隨時享用新功能。	4、執行 Flash 時有限制。 5、網路斷線時部分 App 將無法繼續操作。
混合式應用程式	以 Web App 開發用戶端程式，最終包裝成原生 App 上架至應用程式商店。	同 Web App 方式開發方式，並用框架工具和行動裝置硬體設備互動或加上部分原生程式，最後以原生 App 的名義上架。	1、可用統一的網頁技術開發。 2、於官方商店上架後可賺取費用。 3、使用時不須打開瀏覽器及輸入網址。	1、開發時於不同裝置時須用不同開發工具。 2、功能測試前需分開編譯並且包裝。 3、如需複雜運算之功能或遊戲，效能不如原生 App。 4、硬體支援度不及原生 App。 5、更新時需重新上架和審核，而使用者也須更新或是重新下載才可使用新功能。

（表二資料來源：研究者整理）

三、資安與 App 的相互關係

（一）惡意程式

1、惡意程式如何侵入

若下載應用程式後，手機的耗電量大增，速度變慢，甚至有點當機，那麼所下載的 App 則可能淺藏著惡意程式。惡意程式跟所有官方 App 一樣，會向用戶要求許多權限，有些更是偽裝成常見的安全 App，讓用戶疏忽。

而當使用者正愉悅地使用這些應用程式時，網路犯罪份子也正利用惡意程式，默默竊取使用者的資料。任何使用者的資料都可能被作為非法買賣的商品，就算只是留一通電話或一支 Email 都可能造成問題。網路犯罪份子可能會寄送偽裝官方電子郵件的惡意連結給使用者，一旦使用者點開，可能就讓網路犯罪份子往其個資開了一條康莊大道。

2、惡意程式如何獲取個資

惡意程式可存取擷圖、拍照、錄影、錄音，甚至側錄通話內容及獲取簡訊內容，例如 DENDROID。此一惡意程式可以將合法的 App 木馬化（變成木馬程式），從而監控用戶手機所有的動向。

網路上下載而來的來路不明的應用程式常夾帶惡意病毒或是木馬程式。木馬程式的傳播者就會成為裝置的另一個主人，它可以任意竊取、變更或損毀所有的資料，包含任何極隱私的資料。而在下載此類不明來源的應用程式時，硬體設備通常會提出警訊，但用戶經常忽略這些警訊，因為這些 App 看似安全。木馬程式可以隱蔽自己，並且破壞、傳輸資料，對於用戶的個資保障有極大的威脅。

3、外洩的資料流向

通常被竊取的資料將會被輸往木馬程式或惡意病毒所指定的電腦，任由電腦主人做任何非法的資訊買賣。

而這些網路犯罪份子往往比想像中的更難捉摸，他們利用洋蔥路由器（Onion Router，TOR），在網路的世界隱藏行蹤。因此，即使資料被他們從惡意程式竊取，也無從得知他們的流向。他們常常假扮朋友的身分，發簡訊或是傳送連結至用戶，因為 TOR 使其幕後操縱伺服器 (C&C server)更難被追蹤到。

（二）一般 App 的資安

1、應用程式存取的權限

大多數的使用者在下載 App 時，不清楚自己的資料被軟體存取了多少。一個安全的 App 對於個資的威脅將減少許多，但是當這些 App 本身以外的安全性，比如在資料運輸上的安全性、惡意病毒不斷試圖駭入等等。舉例來說，若 App 獲取你的手機的「控制震動」權限，則如字面上的意思，此應用程式將可以控制你的設備震動功能。若惡意程式侵入，它將可以藉此控制使用者裝置的震動功能，而通常通訊應用程式及遊戲

軟體皆有此功能。它可以停止震動功能，因此使用者無法確認訊息或是收到通知，讓惡意程式加以攔截，取得資訊。

修改／刪除 SD 卡內容，此功能允許應用程式寫入外部儲存設備，如 SD 卡、照相應用程式、音樂和影片應用程式及檔案管理應用程式皆擁有此功能。網路犯罪分子可因此備份所竊取的資料，亦可發送至指揮中心前將資訊儲存至使用者的 SD 卡，甚至可以刪除 SD 卡上的照片以及個人檔案。

2、應用程式資料運輸問題

另一個 App 造成的資安隱憂為傳輸資料時的安全漏洞。如去年台北市推行的「Hello Taipei 單一陳情系統」App 即出現嚴重的資安外洩問題。此 App 使用的為未加密的 HTTP（Hyper Text Transfer Protocol）而非加密的 HTTPS（Hyper Text Transfer Protocol over Secure Socket Layer），導致駭客可輕易獲取資訊。

HTTP，超文本傳輸協議，是一種藉由網際網路傳送全球資訊網文檔的數據傳送協議，並詳細規定瀏覽器和全球資訊網伺服器互通訊息的規則；而 HTTPS 是以安全為目標的 HTTP 的通道，為一種具安全性的安全套接字層（Secure Socket Layer，簡稱 SSL）加密傳輸協議。

HTTP 與 HTTPS 最大的不同點為安全性的大小。HTTP 以明文傳輸訊息，然而 HTTPS 則須至 CA（Computer Associates Inc.，一家美國軟體公司）申請證書，並使用 SSL 交換信息，兩者的連接方式也大為不同。

SSL 是一個常被運用在網際網路的資料加密上的協定。而 SSL 憑證則是網際網路上證明自己身份的工具。有效的憑證須由有公信力的憑證簽署單位信任簽署過。CA 在簽發之前會對申請人做身份的核對以預防網路詐騙。SSL 的目的是保障兩個通訊間的機密性和完整性並驗證伺服器的身分。SSL 被廣泛的運用在連線上，若以「https://」的方式連上網站瀏覽器出現一金鑰，則表示那個網站有支援 SSL。而 SSL 的主要運作是在應用層與傳輸層。

（三）行動裝置的防護

對於惡意的攻擊，用戶並非無解決之道。許多軟體可提供行動裝置一個更安全的使用空間。而以下為數個能夠保護個資的行為：高偵測惡意 App、防止用戶進入不安全連結、及時封鎖詐騙網站、Wi-fi 安全性檢查、應用程式安全漏洞掃描等等。

舉例來說，防火牆即是一種確保資訊安全的裝置，他能夠控制資料是否通過。防火牆存在的目的為防止網路攻擊，他能夠偵測與防止非經授權者存取網路資源，並將不安全的連線阻隔在外。

網路應用程式常常是攻擊的目標，網路應用程式防火牆（Web Application Firewall，簡稱 WAF）則是一項具閘道功能的應用程式。而集中式網路應用程式防火牆可協助簡化安全性管理的作業，以讓應用程式管理員更能夠對抗惡意入侵。WAF 可修補已知弱點以更快地遠離威脅。並提供安全性增強功能包括 SSL 原則管理和端對端 SSL 支援。WAF 有一個優點，他不需要修改後端程式碼即可進行保護行為，使網路不受威脅。

參、結論

在這個資訊極度發達的時代，各種跨時間、跨空間的交流都不成問題。而人手一台手機，每台手機又承載著數個 App，這些 App 同樣與這個世界無接縫的隨時交流著，但大多數的 App 使用者並沒有認真思考過 App 是什麼，未深入了解 App 便毫不猶豫地下載。

資訊科技雖帶來人類文明一大進步，其背後卻有資訊安全的隱憂。許多人認為網路科技方便，不管在何時何地，皆可使用應用程式，例如：玩遊戲、自拍、通訊等等，殊不知自己可能已經被監控了，就因為自己下載了惡意軟體。可能很多人對資安不以為然，認為只要安裝防毒軟體就可對惡意程式及病毒完全免疫。其實防毒軟體不全然能預防所有駭客侵入，它只是替我們的行動裝置上多加了一層防護而已，即使是定期更新抑或是掃描，也只有系統中毒的機率降低。最根本的預防方法就是將資安的 8 個範疇一一實踐嚴謹的檢查，並且規定一個時段要定期執行，任何一個地方疏忽將會造成極大的損失，不只個人，國家也將遭受牽連。

在方便之餘，用戶的個資可能已經被無限度地散播出去了。對於個資外洩，人人聞之喪膽，但當它換一個表達方式，人們卻變得相當安閒，像是不會有任何危險一般。App 都會要求許多權限，而每一項都是緊緊牽扯著資訊的流通。若今日用戶不幸下載到惡意程式，則相對於官方應用程式，資料外洩的機率又高上更多倍。若是一般官方應用程式，主要個資外洩都是因為駭客入侵；惡意程式則不然，惡意程式本身對於個人資料的侵害強度更高，速度更快，幾乎是在用戶下載的那瞬間即蓄勢待發，等著充分利用用戶的個資，而且是在此用戶不知情的狀況下。即使是官方的 App 都存在躲安全把關的惡意程式，更何況是不明來源的 App。所以，在下載 App 以前，必須確保幾件事，確定開發方是可以信賴的，且非來路不明，並且存取的權限並非莫名其妙無緣由的。

資安與我們息息相關，正當我們享受網路的方便性時，同時也別忽略了資安的重要性。下載程式時，使用者應留意應用程式所要求的權限，而非因貪圖便利一味地按下載鍵，隱私也因此被竊取，更甚者整台裝置無法使用。人們常常遺忘資安的重要，駭客就是看準這點，趁機駭入裝置中，若是是稍微的留心，並且正視資安的重要性，相信受害者將會減少。

肆、引註資料

林祝興、張明信（2016）。**資訊安全概論**（第二版）。台灣：旗標。

翁浩正（2016）。《手機不設防》：小心享受著便利，洩漏了隱私。關鍵評論網。2017 年 11 月 28 日，取自 https://hk.thenewslens.com/article/55290

App 應用程式開發簡介。博全科技有限公司。2017 年 9 月 11 日，取自 http://www.phd.com.tw/knowledge/app-dev/

鐘心怡（2011）。App 簡介。2017 年 8 月 6 日，取自 http://ba.tchcvs.tc.edu.tw/epapers/course/1001125_01.pdf

智慧家庭連網裝置漏洞多 趨勢科技發布 2017 年上半年智慧家庭網路安全摘要報告。資安趨勢部落格。2017 年 8 月 17 日，取自 https://blog.trendmicro.com.tw/

12 個最常被濫用的 Android 應用程式權限。資安趨勢部落格。2017 年 10 月 17 日，取自 https://blog.trendmicro.com.tw/?p=10121

GSS 資安電子報 0112 期【2014 年行動裝置（App）安全調查】。叡揚資訊。2017 年 9 月 18 日，取自 http://www.gss.com.tw/index.php/security/1353-112

何世昌（2017）。〈台北都會〉資安漏洞 智慧支付也曾中鏢。自由時報，2017 年 7 月 23 日，取自 http://news.ltn.com.tw/news/local/paper/1118763

HTTP 與 HTTPS 比較。壹讀。2017 年 8 月 31 日，取自 https://read01.com/Po237y.html#.WZbfCD4jHIV

幫你理解 HTTP 和 HTTPS 的區別。每日頭條。2017 年 9 月 7 日，取自 https://kknews.cc/tech/v9rkj9y.html

趨勢行動安全防護 產品特色。網路安全軟體 PC-cillin。2017 年 8 月 19 日，取自 http://www.pccillin.com.tw/product-tmms.html

Web 應用防火牆（WAF）。Microsoft Azure。2017 年 8 月 8 日，取自 https://docs.microsoft.com/zh-tw/azure/application-gateway/application-gateway-web-application-firewall-overview

網站 SSL 加密原理簡介。網管人。2017 年 8 月 26 日，取自 http://www.netadmin.com.tw/article_content.aspx?sn=1106140008

SSL 與 TLS 功能啟用以及憑證建立。EVO。2017 年 9 月 4 日，取自 https://www.evo-mailserver.com.tw/support/ssl_certificate.php

巫宗翰。DDoS 攻擊介紹。國立臺灣大學計算機及資訊網路中心電子報。2017 年 9 月 4 日，取自 http://www.cc.ntu.edu.tw/chinese/epaper/0026/20130920_2606.html