Deloitte.
勤業眾信

行動應用App資安檢測服務說明

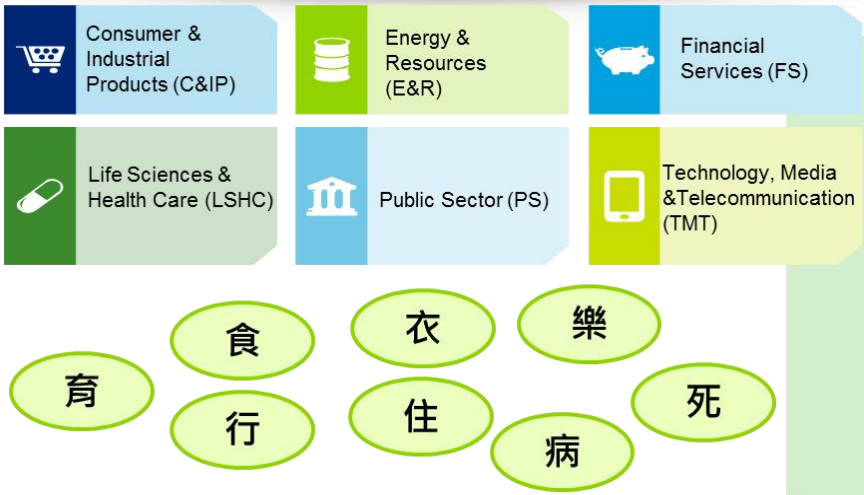
勤業眾信聯合會計師事務所
企業風險管理
2016.08.11

簡報大綱

- **App資安檢測背景說明**
- 勤業眾信資安檢測服務說明
- 意見交流

因應新興科技發展及數位化轉型
- 行動應用APP安全性議題備受關注

伴隨新興科技發展及數位化轉型，如雲端/大數據、物聯網、行動電商、行動醫療、工業4.0及金融科技FinTech，都可看到行動應用APP在數位化與業務模式改變中所產生的深遠影響



精準行銷

多通路

用戶體驗

O2O

社群品牌

行動戰情室

大數據分析

No	App類別	說明
1	社交通訊	含社交平台、部落格或論壇、即時通訊、視訊聊天
2	婚戀交友	含網路交友、婚戀媒合服務
3	影音媒體	含音樂廣播、影視戲劇、動畫、媒體播放器、行動直播
4	新聞雜誌	含新聞雜誌App和閱讀器
5	書籍漫畫	含小說、漫畫、一般書籍
6	學習與參考資源	含語言學習、字典和翻譯、百科全書、教科書等
7	網路購物	含C2C拍賣、團購、各類商品等的網路銷售平台
8	健康醫療	如運動健身、生理和體重飲水等紀錄工具、醫院診所
9	商業辦公	可提升工作效率和生產力之軟體服務，如辦公軟體、名片建檔、雲端儲存等
10	應用工具	含防毒軟體、瀏覽器、個人化桌布、計算機、QR Code、鍵盤輸入法、電子信箱等
11	生活服務和資訊	含食衣住行相關的搜尋和預訂服務、政府便民服務，如飲食餐廳、交通、旅遊、電影、地圖導航、天氣等
12	金融支付	含財經證券、理財記帳、網路銀行、電子錢包、行動支付

金融業行動應用APP資安常面臨的風險


網銀App漏洞 金管會關注

分享 G+ 分享 留言 列印 存新聞

2016-04-07 03:01 經濟日報 記者韓化宇／台北報導 分享 238 傳送 G+1 0

- 事件時間：2016/04/07
- 事件說明：行動金融時代來臨，民眾能透過行動銀行 App 隨時隨地取得金融服務。金管會對此相當重視，特地抽測幾家公民營銀行的App，結果發現對資安保護，仍存有被駭客入侵的風險。因此指示銀行公會，修訂「金融機構辦理電子銀行業務安全控管作業基準」，要求所有銀行，都要再度進行資安檢測，提升抵禦駭客入侵的防護能力。

金融業行動應用APP資安常面臨的風險

01 行動應用程式發布安全
- 未檢視行動應用App所需執行權限，如：GPS定位
- 未提供安全性問題回報管道

02 敏感性資料保護
- 儲存過多的個人資料於暫存檔案中，容易遭惡意程式使用或傳遞，如：信用卡資料
- 傳輸個人資料時未進行安全加密傳輸

03 身分認證、授權與連線管理安全
- 後端連線伺服器未進行資安檢測或驗證
- 缺乏交易資料完整性驗證與防護

04 行動應用程式碼安全
- 所使用套件程式內容含已知的安全弱點存在
- 未對使用者輸入欄位地方進行相關的安全驗證。
- 未有效保護App，導致可解析程式碼內容及進行修改動作。

國內針對行動應用APP安全職責分工

依「行政院國家資通安全會報第26次委員會議」決議辦理 (103年6月24日)

- 依據行動裝置軟硬體、App類型及犯罪防治，分別由主管機關各司其職
- 使用者自行下載 App，依其應用類型由各目的事業主管機關負責管理

Layer 1	手機硬體安全	國家通訊傳播委員會(NCC)
Layer 2	手機作業系統安全	國家通訊傳播委員會(NCC)
Layer 3	手機預載App安全	國家通訊傳播委員會(NCC)
Layer 4	使用者自行下載之App安全	經濟部工業局
4.1	共通性及非特定領域App基礎安全要求 • 「行動應用App基本資安規範」 • 「行動應用App基本資安檢測基準」	經濟部工業局
4.2	特定領域應用App安全 (例：網路銀行App、健康照護App...) • 「金融機構提供行動裝置應用程式注意事項」 • 「壽險業提供行動裝置應用程式作業原則」	**各目的事業主管機關**
Layer 5	手機詐騙行為防範	內政部警政署

簡報大綱

- App資安檢測背景說明
- **勤業眾信資安檢測服務說明**
- 意見交流

Deloitte行動應用APP資安檢測框架

行動應用APP資安檢測

依據經濟部工業局行動應用App基本資安自主檢測推動制度

行動應用 App 基本資安檢測基準

金融機構提供行動裝置應用程式注意事項
壽險業提供行動裝置應用程式作業原則

- **國際最佳實務**
  - ✓ OWASP Top Ten Mobile Risks
  - ✓ CSA Mobile Application Security Testing
  - ✓ NIST SP800-163

發布安全	敏感性資料保護	付費資源控管安全	身分認證、授權、與連線管理安全	行動應用程式碼安全	進階檢測項目
· 行動應用程式發布 · 行動應用程式更新 · 行動應用程式安全性問題回報	· 敏感性資料蒐集 · 敏感性資料利用 · 敏感性資料儲存 · 敏感性資料傳輸 · 敏感性資料分享 · 敏感性資料刪除	· 付費資源使用 · 付費資源控管	· 使用者身分認證與授權 · 連線管理機制	· 防範惡意程式碼與避免資訊安全漏洞 · 行動應用程式完整性 · 函式庫引用安全 · 使用者輸入驗證	· 各主管機關要求項目 · 伺服器端滲透測試 · 程式碼混淆機制 · 模擬器偵測機制 · 程式碼防竄改機制 · 防止動態偵錯機制

嚴謹檢測工序

案件承接階段

- 受測件取件與聲明資訊蒐集
- 受測件基本資訊核對

工具檢測階段

- 二個系統平台(iOS & Android)檢測過程超過**20項工具使用**

人工檢測階段

- 檢測項目超過**67項檢測基準**(依據不同APP等級進行檢測)

報告彙整階段

- 品質與技術面須符合**22個**內部作業程序及使用**64份**表單紀錄
- 製作檢測報告書

合格證明核發階段

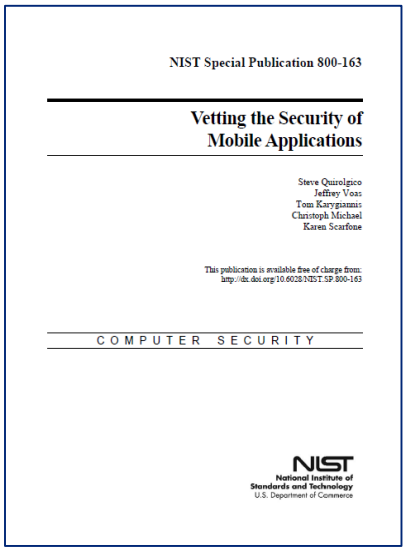
- 顧客滿意度調查與回饋
- 檢測報告書
- 授權代發予合格證明

行動應用基本資安檢測方法與參照最佳實務

勤業眾信將依專案之需求，針對客戶行動應用 App 進行資訊安全檢測，檢測手法遵循多項國際資安指引，符合經濟部工業局「行動應用App基本資安檢測基準」要求

行動應用 App 基本資安規範

行動應用 App 基本資安檢測基準


NIST Special Publication 800-163

Vetting the Security of Mobile Applications

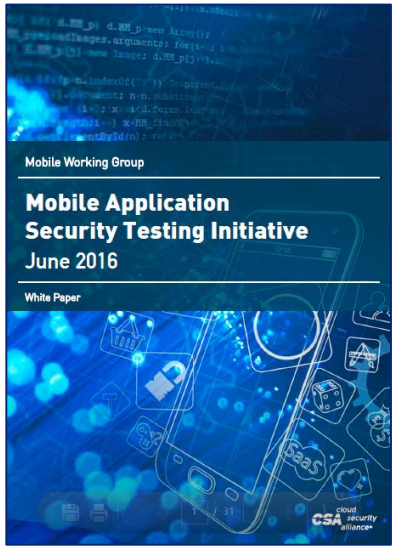
Steve Quirolgico
Jeffrey Voas
Tom Karygiannis
Christoph Michael
Karen Scarfone

This publication is available free of charge from:
http://dx.doi.org/10.6028/NIST.SP.800-163

COMPUTER SECURITY

NIST
National Institute of Standards and Technology
U.S. Department of Commerce

NIST SP800-163 Vetting the Security of Mobile Applications



CSA Mobile App Security Testing

OWASP Mobile Security Project

OWASP Top Ten Mobile Risks

行動應用App基本資安檢測項目

第一類 純功能性、第二類 具認證功能與連網行為、第三類 具交易功能（包括認證功能與連網行為）

編號	五大面向	資訊安全技術要求事項	第一類	第二類	第三類
1	4.1.1 行動應用程式發布安全	行動應用程式發布		V	V
2		行動應用程式更新		參考項目	
3		行動應用程式安全性問題回報		V	V
4	4.1.2 敏感性資料保護	敏感性資料蒐集		V	V
5		敏感性資料利用		參考項目	
6		敏感性資料儲存	V	V	V
7		敏感性資料傳輸		V	V
8		敏感性資料分享		V	V
9		敏感性資料刪除		參考項目	
10	4.1.3 付費資源控管安全	付費資源使用			V
11		付費資源控管			V
12	4.1.4 身分認證、授權、與連線管理安全	使用者身分認證與授權		V	V
13		連線管理機制		V	V
14	4.1.5 行動應用程式碼安全	防範惡意程式碼與避免資訊安全漏洞	V	V	V
15		行動應用程式完整性		參考項目	
16		函式庫引用安全		V	V
17		使用者輸入驗證	V	V	V

2016 OWASP Top 10 Mobile Risks

項目	風險	說明
M1	作業系統平臺使用不當	包含行動作業系統平臺功能的濫用或未能有效使用平臺所提供的安全控制措施。
M2	不安全的資料儲存	包含敏感性資料儲存未進行加密、暫存資料含有敏感訊息及非故意的資訊洩漏。
M3	不安全的傳輸	於資料傳輸過程中，未施以合適的傳輸保護機制，如使用有弱點的SSL版本或敏感資訊用明文進行傳送。
M4	不安全的身份驗證	包含使用者身份驗證問題及應用程式session管理。
M5	加密失效	加密失效可能分為兩種情況，如使用強度高的加密演算法卻遭到破解或使用過於簡單的加密演算法遭到破解。
M6	不安全的授權	對未經授權的使用者授予存取的權限，可執行原本不能執行操作或服務使用。
M7	用戶端程式碼品質問題	包括用戶端程式碼所開發問題，如行動應用APP存有緩衝區溢位弱點或XSS問題。
M8	程式碼篡改	包括可針對二進位檔案修補、資源修改和動態記憶體修改等
M9	逆向工程	透過逆向工程方式，針對二進位檔案進行分析，以確定原始程式碼、函式庫、使用資源及演算法內容。
M10	無關的功能	於發佈時，在行動應用APP中啟用原先不打算發佈之相關功能。

行動應用APP檢測設備與工具

資安科技暨鑑識分析中心目前用於行動應用App基本資安檢測服務之設備及工具如下表所示

工具軟體名稱	功能簡述
Android Debug Bridge(ADB)	Android系統開發與除錯工具
SQLite Database Browser	資料庫檢視工具
Dex2jar	逆向工程工具-將Dex (Dalvik Executable)執行檔反編譯成Java編譯的*.jar執行檔
Java Decompiler-GUI (JD-GUI)	逆向工程工具-靜態分析程式原始碼
APKTool	逆向工程工具-反編譯行動軟體之後，查看AndroidManifest.xml與smali文件
Burp Suite	代理伺服器工具-檢視與攔截行動軟體之網路行為，用於驗證伺服器憑證
WireShark	側錄與分析網路封包工具-檢視是否有採用安全的加密傳輸通道(例如SSL/TLS)和敏感性資訊

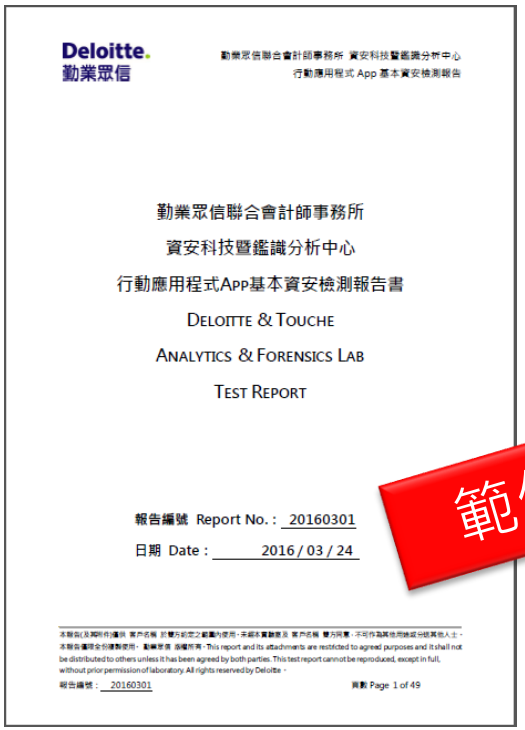
工具軟體名稱	功能簡述
iNalyer	應用程序分析工具
iFunbox	IOS 作業系統檔案存取工具
SQLite Database Browser	資料庫檢視工具
Class-dump-z	類別函數分析工具
Clutch	執行緒安全分析
Snoop-it	IOS動態分析黑和工具
IDA PRO	逆向工程分析工具
Burp Suite	代理伺服器工具(檢視與攔截行動軟體之網路行為，用於驗證伺服器憑證)
WireShark	側錄與分析網路封包工具(檢視是否有採用安全的加密傳輸通道(例如SSL/TLS)和敏感性資訊)

國際級認證實驗室出具之行動應用安全檢測報告

- 採用標準化且一致性之檢測技術，評估行動應用APP安全性，並以公正第三方的角色出具符合國際級品質且經工業具認可之檢測報告。

  - 檢測報告書內容
    - *實驗室資訊*
    - *委託方資訊*
    - *受測程式資訊*
    - *服務資訊*
    - *檢測資訊摘要*
    - *檢測結果說明*
    - *檢測結果擷圖*

  - 附件與備考
    - *檢測人員簡歷*
    - *檢測軟體工具*
    - *檢測環境說明*



範例

Deloitte行動應用App資安檢測團隊

- 勤業眾信擁有**專業的資安技術團隊”Tiger Team”**，包含了前國家安全局資訊安全顧問，美國空軍歐洲指揮部資訊系統安全官及英國Cyber Security Centre資訊安全專家、國家資通安全會報技術服務中心、警政署刑事警察局科技研發科

CISSP Certified Information Systems Security Professional | CISM Certified Information Security Manager | CEH Certified Ethical Hacker | ECSA EC-Council Certified Security Analyst | CHFI Computer Hacking Forensic Investigator | ECIH EC-Council Certified Incident Handler | CISA Certified Information Systems Auditor

2016 HITB（Hack in the Box）CTF國際安全攻防競賽荷蘭Deloitte ERS團隊取得第2名好成績

Deloitte’ brand at BlackHat 2016 in Las Vegas

惡意程分析(阿根廷)、Red Team演練(賽普勒斯)、人因工程與資安(荷蘭)

- CODEXGIGAS MALWARE DNA PROFILING SEARCH ENGINE
- Arsenal Theater Demo: WarBerryPi Troops Deployment in Red Teaming Scenarios
- SECURITY THROUGH DESIGN - MAKING SECURITY BETTER BY DESIGNING FOR PEOPLE

國內第一批合格行動應用APP資安檢測實驗室

通過經濟部工業局及財團法人全國認證基金會
「行動應用APP基本資安檢測實驗室認證服務計畫」

Deloitte.
勤業眾信

陳威棋 協理
CFE/CEH/CHFI/CISA

企業風險管理

行動：0921-174-299
ikewchen@deloitte.com.tw

勤業眾信聯合會計師事務所
10596台北市民生東路三段156號12樓
統一編號: 94998251

電話:(02)2545-9988 分機 7807
傳真:(02)2545-9966 分機 7807
www.deloitte.com.tw

Member of
Deloitte Touche Tohmatsu

意見交流

外部使用

Deloitte.
勤業眾信

關於德勤全球
Deloitte（"德勤")泛指德勤有限公司（一家根據英國法律組成的私人擔保有限公司，以下稱德勤有限公司("DTTL")），以及其一家或多家會員所。每一個會員所均為具有獨立法律地位之法律實體。德勤有限公司（亦稱"德勤全球"）並不向客戶提供服務。請參閱 www.deloitte.com/about 中有關德勤有限公司及其會員所法律結構的詳細描述。

德勤為各行各業之上市及非上市客戶提供審計、稅務、企業風險、管理顧問及財務顧問服務。德勤聯盟遍及全球逾150個國家，憑藉其世界一流和優質專業服務，為客戶提供應對其最複雜業務挑戰所需之深入見解。德勤約210,000 名專業人士致力於追求卓越，樹立典範。

關於德勤大中華
作為其中一所具領導地位的專業服務事務所，德勤大中華區設有22個辦事處分佈於北京、香港、上海、臺北、成都、重慶、大連、廣州、杭州、哈爾濱、新竹、濟南、高雄、澳門、南京、深圳、蘇州、台中、台南、天津、武漢和廈門。德勤大中華擁有近13,500名員工，按照當地適用法規以合作方式服務客戶。

關於勤業眾信
勤業眾信係指勤業眾信聯合會計師事務所(Deloitte & Touche)及其關係機構，為德勤有限公司(Deloitte Touche Tohmatsu Limited)之會員。集團成員包括勤業眾信聯合會計師事務所、勤業眾信管理顧問股份有限公司、勤業眾信財稅顧問股份有限公司、德勤財務顧問股份有限公司，及德勤商務法律事務所。

勤業眾信以卓越的客戶服務、優秀的人才、完善的訓練及嚴謹的查核於業界有著良好聲譽。透過德勤有限公司之資源，提供客戶全球化的服務，包括赴海外上市或籌集資金、海外企業回台掛牌、中國大陸投資等。