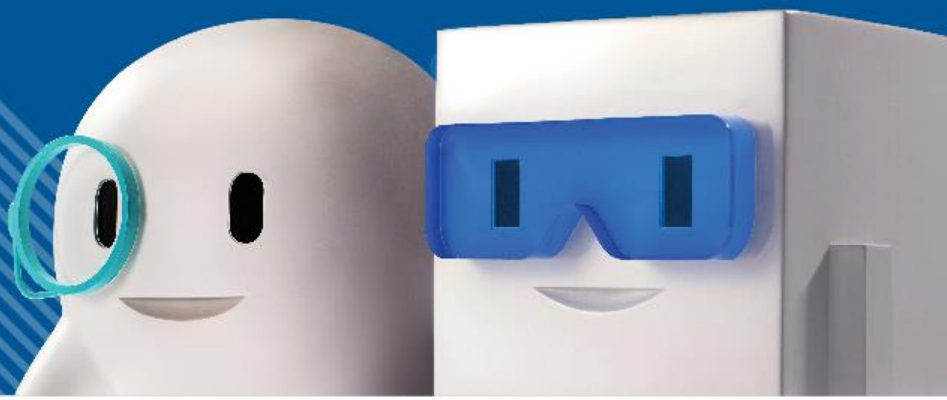
流動應用程式交易保安

Frankie Wong (HKCERT)



All-round Productivity Partner
全方位企業伙伴

議程

- HKCERT 簡介
- 流動應用程式交易保安研究
- 研究目的
- 交易保安測試
- 研究結果
- 保安建議

HKCERT 簡介

HKCERT 簡介

- 香港電腦保安事故協調中心 (HKCERT)
  Hong Kong Computer Emergency Response Team Coordination Centre

- 成立於 2001 年
- 100% 由香港特區政府資助
- 由香港生產力促進局 (HKPC) 管理

HKPC
Hong Kong Productivity Council
香港生產力促進局

HKCERT 簡介

- 服務範圍
  - 電腦保安警報監測及預警
  - 保安事故報告及求助
  - 出版資訊保安指引和資訊
  - 提高資訊保安意識

- 維持一個良好電腦保安協調網絡，包括本地及海外的機構，確保能有效地作出回應和處理

HKCERT 簡介

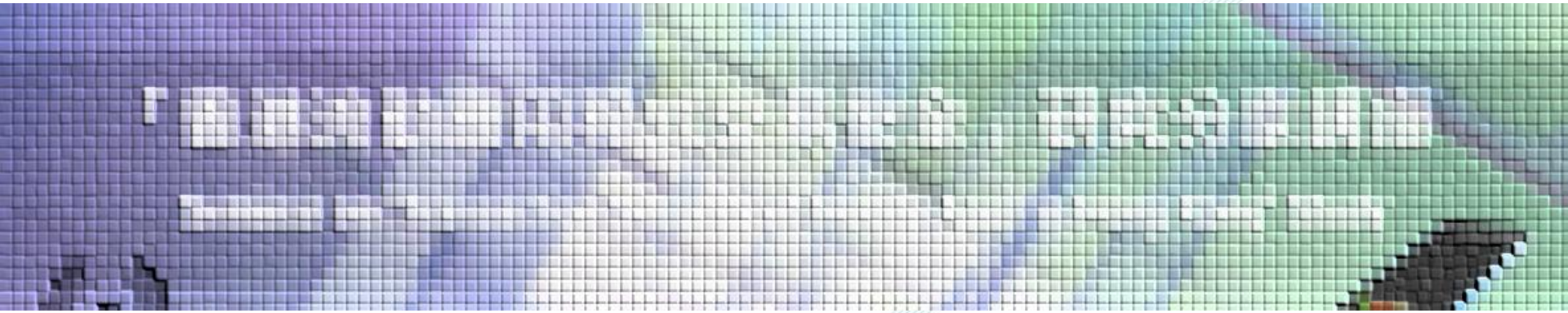
- 提供資訊
  - 資訊保安報 (每月)
  - Google Play 商店應用程式保安風險報告 (每月)
  - 香港保安觀察報告 (每季)
  - 殭屍網絡偵測及清理 (不定期)
  - 保安指南 (不定期)

訂閱資訊保安警報

網站： https://www.hkcert.org/

訂閱資訊保安警報： https://www.hkcert.org/subscription

流動應用程式交易保安研究



研究簡介

14-Sep-2015 HKPC 記者會

- 「香港流動應用程式交易安全研究」發佈會

HKCERT 及 PISA 合作進行
流動應用程式 SSL 保安測試

- Apr-Jul 2015
- 130 Apps
  (66 iOS + 64 Android)

研究簡介

- 本地新聞


34%交易Apps保安差易被
網上消費愈來愈流行
式（App）進行證券
易。惟有研究發現，
時，通訊加密保安不
資料外洩甚至有經濟
遊訂位服務Apps的
應避免使用公共Wi-
能顯示網站數碼證書
1/3無
（App）
香港電腦
地130個
驗證數碼
程式，
應用程式
告，並
家指市民
用不知名
34%網上
擊
(明報) 2015年
Level di
130
19%
網上商店App
研究的流動應用程式
應用程式的通訊加密
實落單服務的交易安
應用程式屬於「存有
服務及流動銀
及「最安全」
要聞港聞
2015年09月15日
1/3 Apps加密差易被黑
1/3 Apps加密差易被黑
30,102
極危險！
1/3網上交易App加密不足
44
分享
0
Tweet
0
44
A A
【本報訊】香港電腦保安事故協調中心今年4至7月測試130個本地常用、含網上交易服務的手機應用程式（Apps），66個屬iOS Apps，64個是Android Apps，發現超過三分一在處理個人及交易資料時，通訊加密保安不足，易被黑客盜取資料。
測試發現，34% Apps沒採用通訊加密技術，或沒驗證數碼證書，其中超過一半金融證券、網上商店及旅遊訂位服務Apps，屬於有使用通訊加密技術但無驗證數碼證書真偽的「存有漏洞」級別，甚至是沒使用通訊加密技術的「最重」級別。至於電子錢包、付費服務及流動銀行服務Apps保安較好，87%以上屬「安全」及「最安全」級別。
■測試發現34%手機應用程式通訊加密保安不足，用戶資料或會被黑客盜取。資料圖片
民使用App購物時，宜選用瀏覽
圖片）
安協會主席范健文（右）表示，黑
pp的漏洞，取得用戶信用卡號碼。
）

研究目的

從一個問題...

- 敏感資訊應該應用加密通訊 (SSL)
- 一個安全的 SSL 應使用有效的證書 (由信任的CA簽署)
- 可是，如果證書不是有效的 (例如：自我簽署的證書)...

研究目的

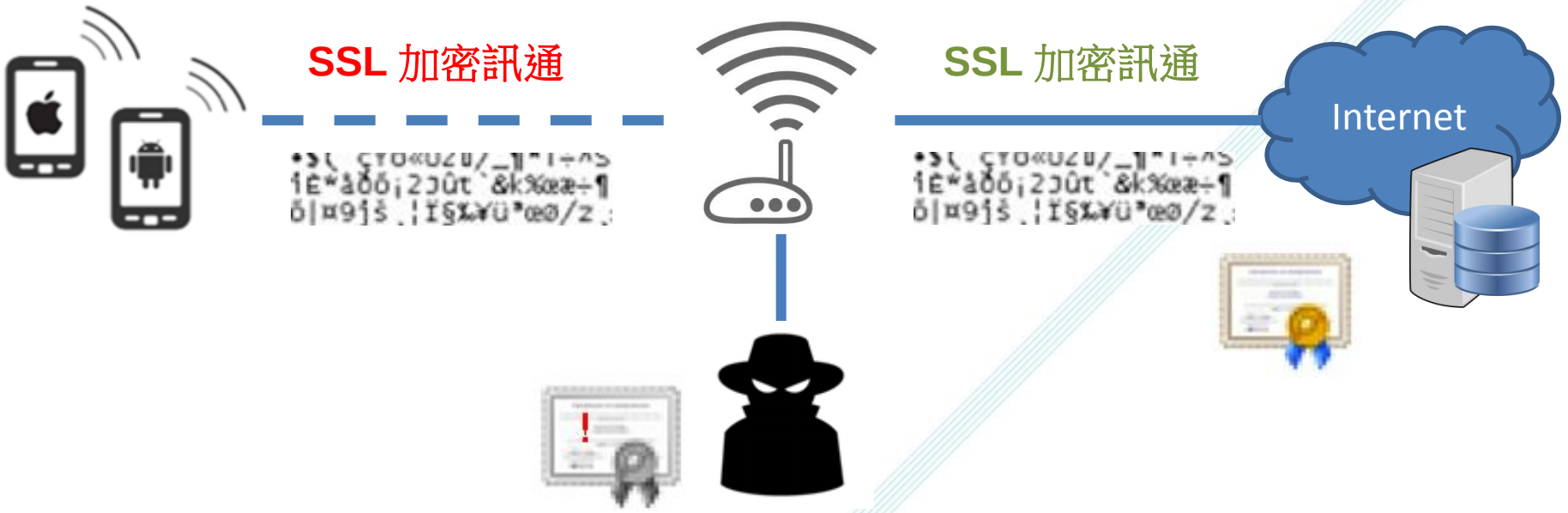
從一個問題...

- 若同樣情況在流動應用程式(App)上...？

- 若 App 沒有驗証 SSL 加密證書，
- SSL 通訊將變得**不安全**，App 將變得**存有漏洞**。

保安威脅 – 中間人攻擊 (MITM)

保安威脅 – 中間人攻擊 (MITM)



保安威脅 – 中間人攻擊 (MITM)

影響

- 在不為人知的情況下，通訊的數據將可**被截取**或**篡改**


Image: Movie - Overheard

- 可導致**資料外洩**或**金錢上損失**

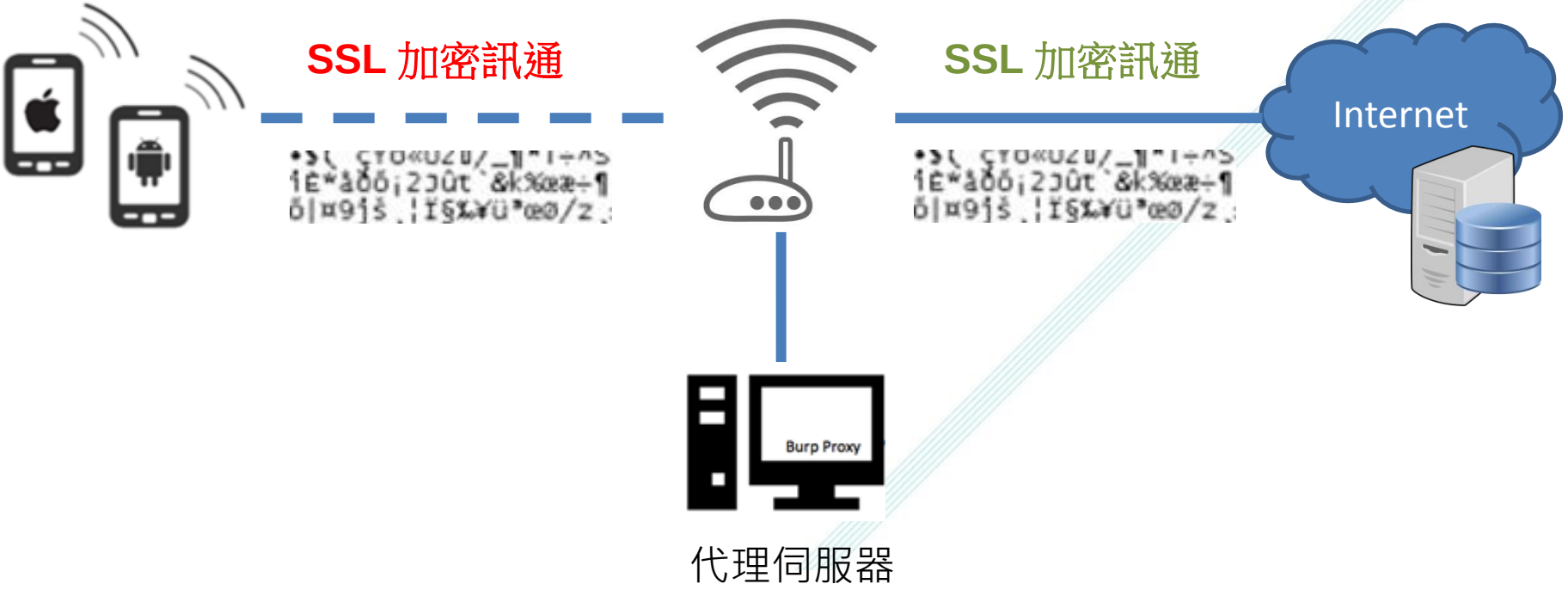
研究目的

- 在香港常用的 Apps 當中，**辨認**在SSL實行上存有**漏洞**
- 幫助香港的流動用戶在Wi-Fi網絡**防止中間人攻擊**
- **提高**香港大眾、Apps擁有者及開發者對SSL實行的**意識**

交易保安測試

交易保安測試

- 模擬中間人攻擊



交易保安測試

- 測試1：
  - App 在數據傳輸有沒有使用 SSL 加密通訊？
- 測試2：
  - 若使用 SSL 加密通訊
  - App 有沒有正確驗証加密證書？
- 進階測試3：
  - 若裝置被插入代理伺服器的證書 (Proxy CA's cert)，App 能否進階防止中間人攻擊？

測試評級

級別	內容
最安全	使用 SSL 加密，及 **進階的證書驗證技術**
安全	使用 SSL 加密，及 **正確驗證**
在有漏洞	使用 SSL 加密，但 **沒有正確驗證**
嚴重	**沒有 SSL 加密**，當中涉及敏感資料

研究結果

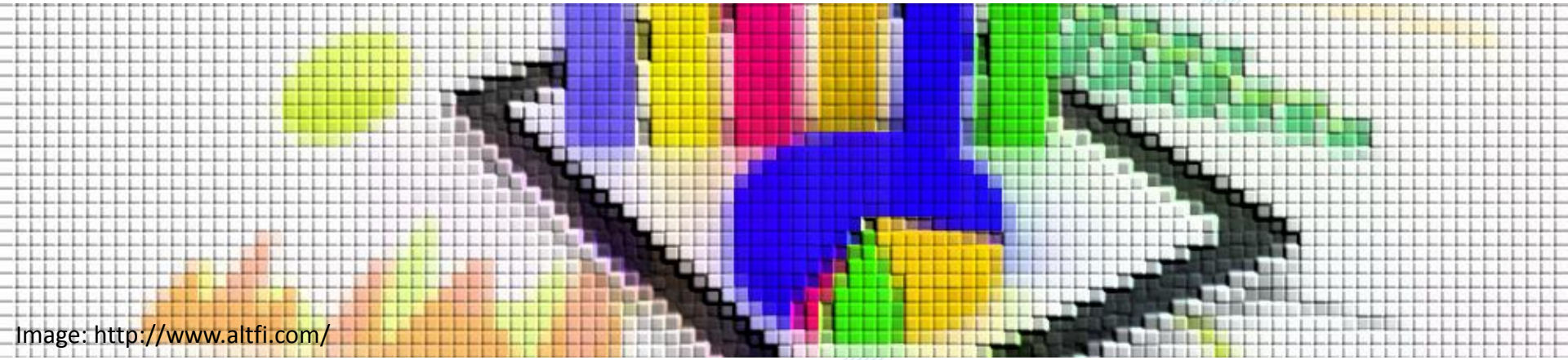


Image: http://www.altfi.com/

研究範圍

流動平台

及

香港公司開發/擁有的流行應用程式

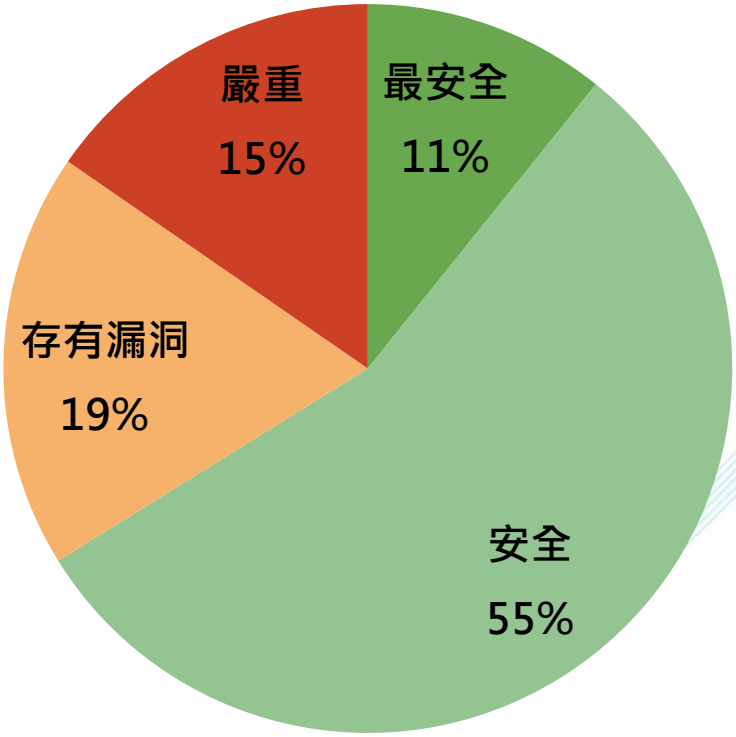
- 服務本地用戶
- 處理個人資料或網上交易
- 使用網頁協定 (http / https)

研究範圍

服務	數量
流動銀行服務 (Mobile Banking Service)	32
戲院訂票 (Cinema Ticketing)	26
金融證券 (Financial Securities)	24
網上商店/團購 (Online Shopping / Group Buy)	16
旅遊訂位服務 (Travel Booking Service)	13
外賣落單 (Online Food Ordering)	11
電子錢包/付費服務 (Digital Wallet / Payment Service)	8
總共	**130**

研究結果

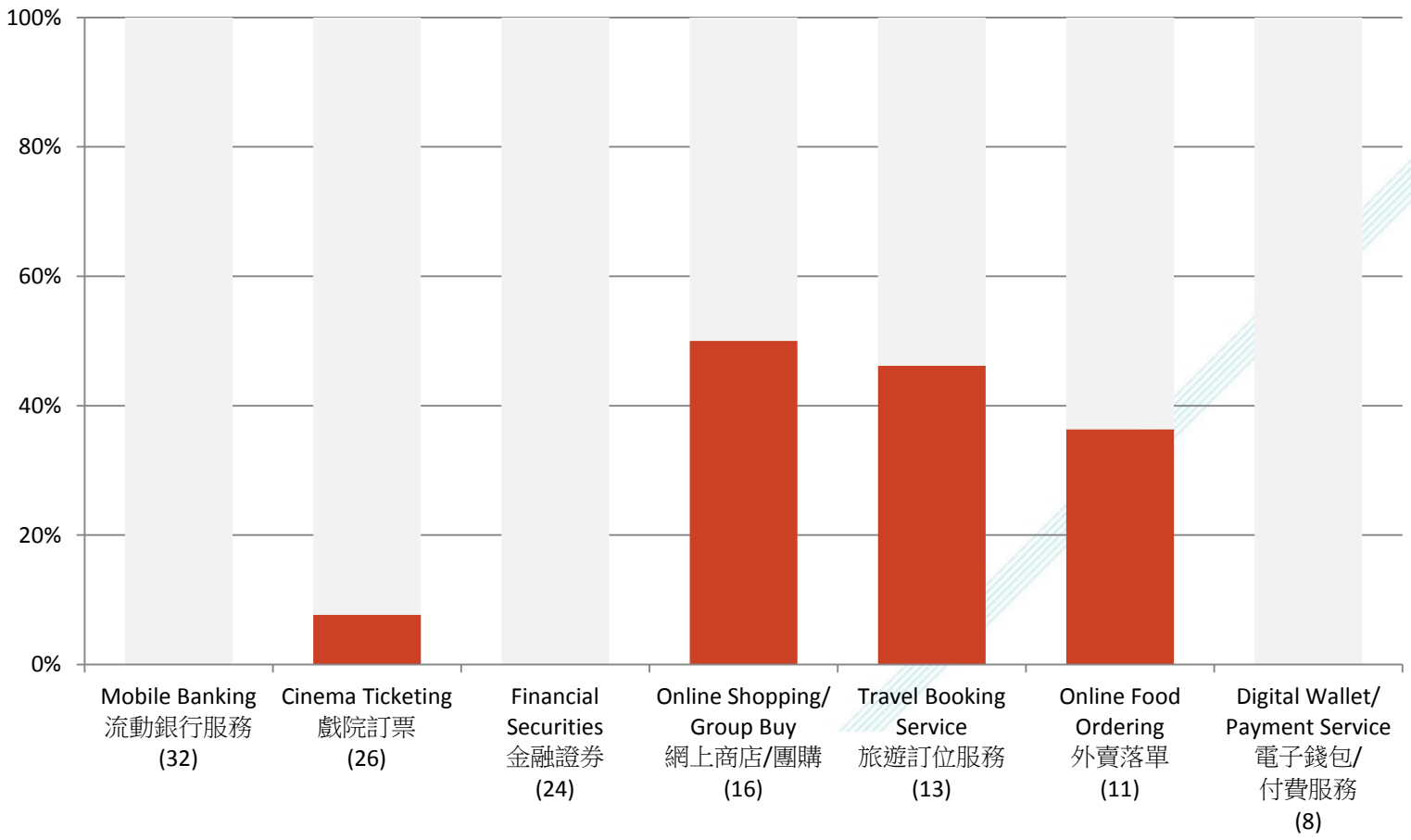
130 款應用程式的評級分佈

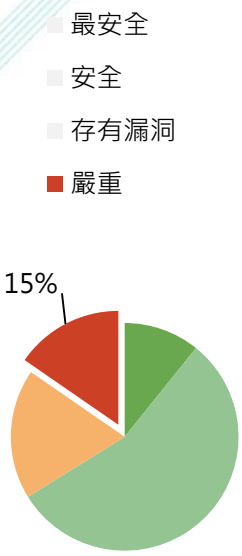


評級	數量
最安全	14
安全	72
存有漏洞	24
嚴重	20

研究結果

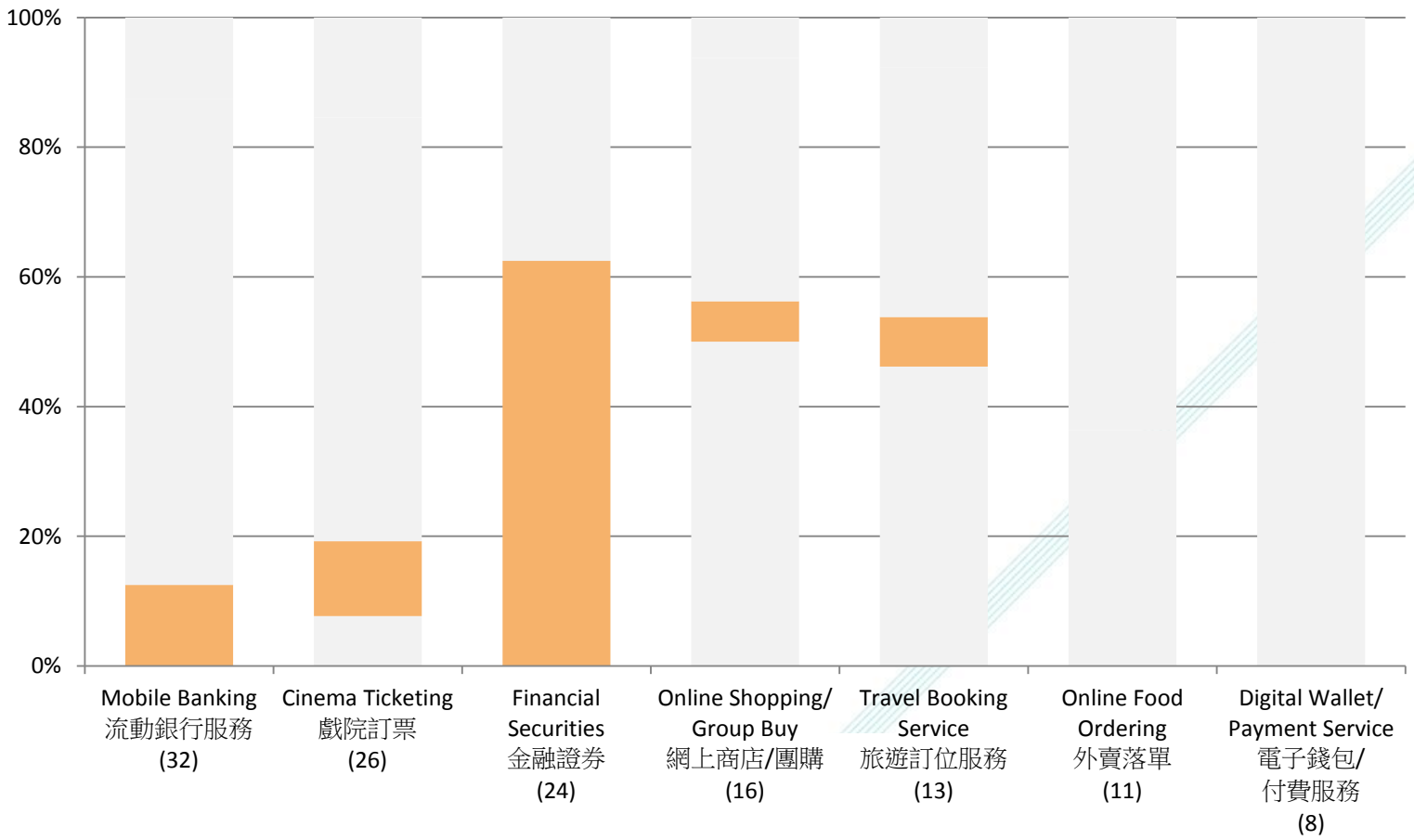
流動應用程式分佈 – 嚴重

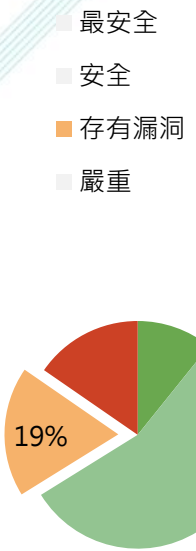




研究結果

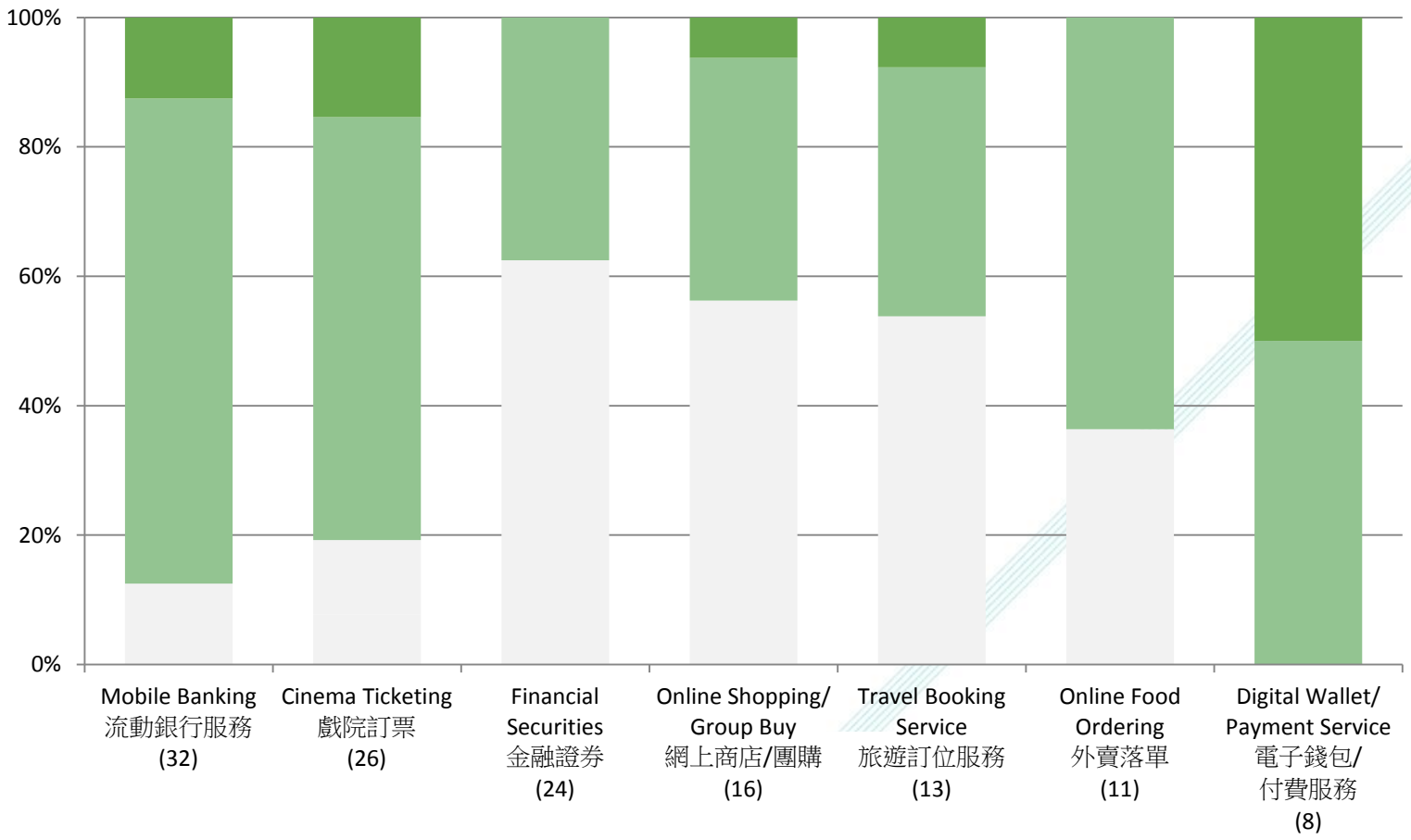
流動應用程式分佈 – 存有漏洞

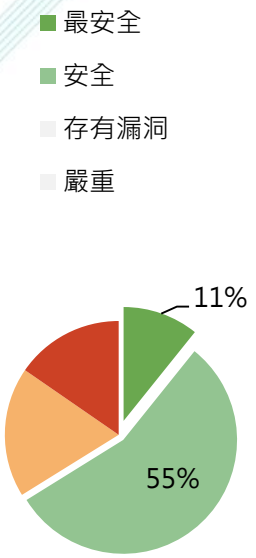




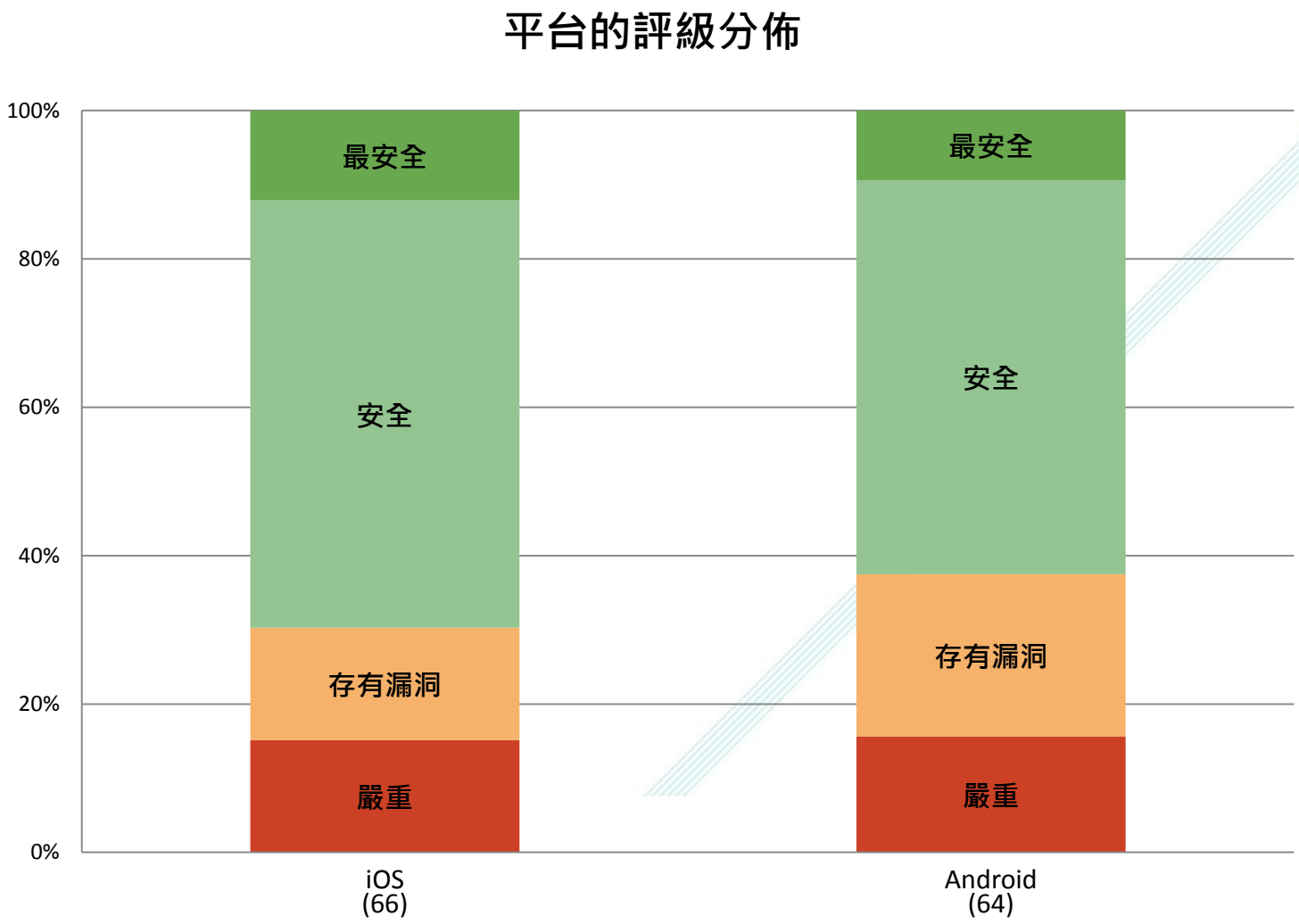
研究結果

流動應用程式分佈 – 安全/最安全





研究結果


平台的評級分佈
100%
80%
60%
40%
20%
0%
最安全
安全
存有漏洞
嚴重
最安全
安全
存有漏洞
嚴重
iOS
(66)
Android
(64)

研究發現

個案 1

- 服務：戲院訂票
- 評級：嚴重 / 存有漏洞
- 資料涉及：信用咭號碼 及 CVV碼

個案 2

- 服務：團購
- 評級：**嚴重**
- 資料涉及：登入帳號、個人資料、已購買的換領券

研究發現

個案 3

- 服務：旅遊訂位服務
- 評級：嚴重
- 資料涉及：個人資料，包括 HKID 及護照號碼

個案 4

- 服務：外賣落單
- 評級：**嚴重**
- 資料涉及：個人資料，包括真實地址、信用咭資料及CVV碼

保安建議

Image: http://www.tiib.com/

保安建議

- 建議應用程式開發者
  - 提高 SSL 加密通訊正確驗証的意識
  - 程式設計過程，建議擁有者使用 SSL 加密

- 建議應用程式擁有者
  - 使用外判應用程式開發公司時，應在標書清楚要求使用 SSL 加密通訊及正確驗証
  - 當應用程式推出時，可尋求第三方公司做安全驗証

保安建議

HKCERT 及 PISA 共同發佈

- 研究報告
- 流動應用程式(SSL實施)最佳行事指引

(https://www.hkcert.org/my_url/blog/15092402)

保安建議

建議應用程式用戶

- 當處理敏感數據時，
  - 使用**流動數據網絡** (3G/LTE) 取代連接公共 Wi-Fi
  - 或使用**手機瀏覽器** (例如: Chrome, Safari) 取代應用程式

- 不要從**非官方**應用商店安裝程式
  - 防止安裝惡意程式及不信任證書

謝謝

Frankie Wong (HKCERT)

hkcert.org / pisa.org.hk