Openfind Software Engineered for Growth™

電子郵件社交工程的攻與防

台灣科技大學 資訊管理系/ 副教授 羅乃維

大綱

- 電子郵件社交工程
- 電子郵件社交工程演練
- 真正的市場需求在哪裡？
- 電子郵件社交工程自動化演練與教育系統
  - 設計、實作、展示
- 結論

電子郵件社交工程

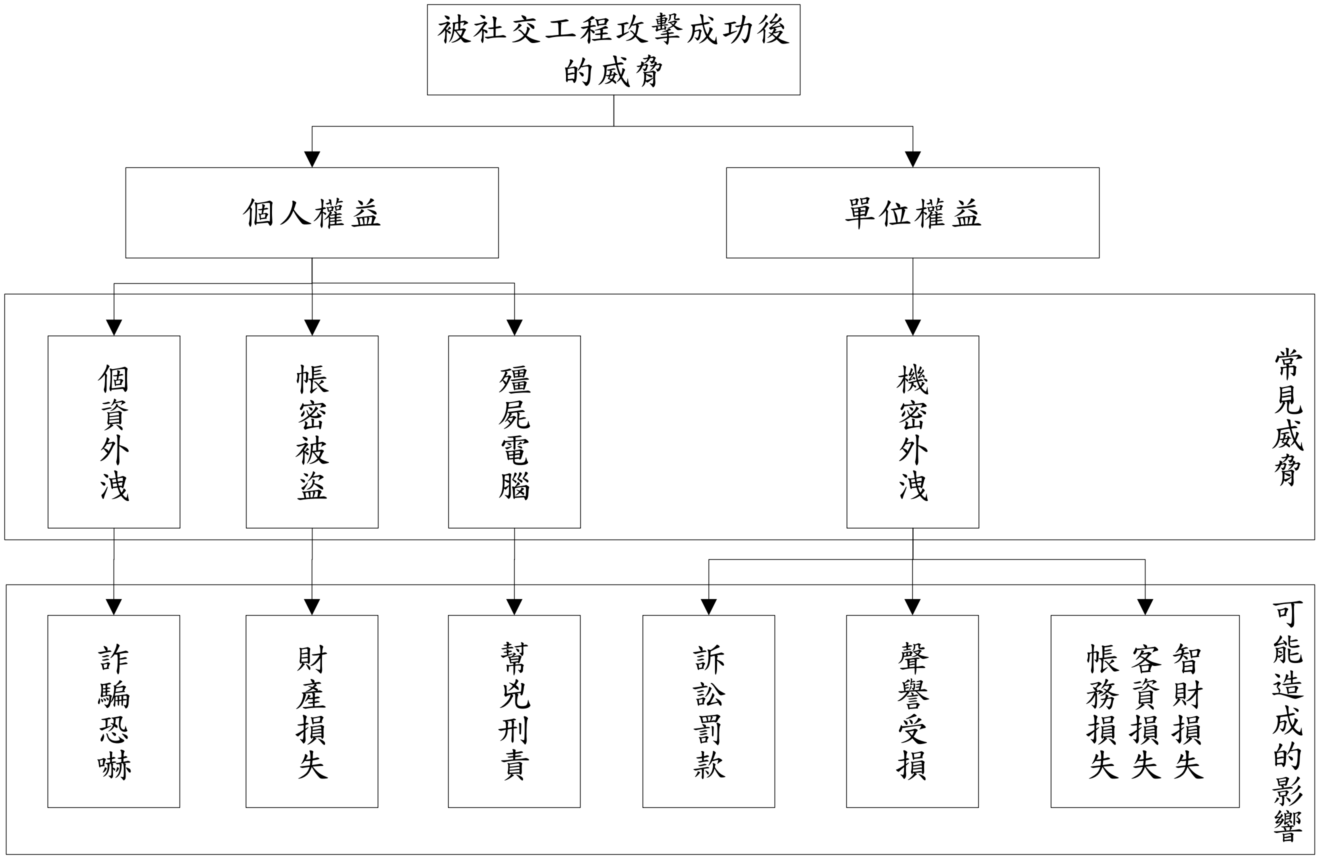
社交工程在資訊安全上的意義

- 社交工程
  - 操縱他人執行某些特定動作(例如ATM匯款)或吐露特定資訊的技巧
  - 無視電腦安全防護
  - 不需要專業的電腦技術
  - 早期社交工程使用「電話」當做工具
  - 目前社交工程大都是利用「電子郵件」或「偽造熱門網頁」來進行攻擊

資料來源：Google圖片，版權歸Google與該電影公司所有.

社交工程的安全威脅

- 被社交工程攻擊成功後的威脅



社交工程的攻擊方式

- 常見的社交工程攻擊方式
  - 網路釣魚
    - 透過電話、電子郵件、即時通訊或傳真嘗試取得被害人的個人資料或財務資訊的手段
  - 圖片中的惡意程式
    - 以知名明星或情色圖片誘使被害者開啟，導致觸發系統漏洞，例如微軟的JPEG 緩衝區滿溢弱點，故可能會執行圖片內的惡意遠端程式碼
  - 偽裝系統修補程式
    - 定時更新系統可防止因系統漏洞而遭受未知攻擊，故也衍生出以偽造的系統修補程式誘使被害者開啟的攻擊方式

社交工程的攻擊方式(續)

- 常見的社交工程攻擊方式(續)
  - 即時通訊軟體
    - 擁有廣大使用者的通訊軟體，如MSN、奇摩即時通等遭受病毒感染後，就會自動發送一段惡意網址的連結誘使被害者點選
  - 在電子郵件中隱藏未知陷阱
    - 將惡意程式、連結、附件隱藏於郵件中，再應用社交工程的概念使被害者開啟郵件

電子郵件社交工程

- 電子郵件是最適合做社交工程攻擊的工具
  - 可偽裝寄件者
  - 低成本且可大量發送
  - 容易使用，無技術門檻
  - 可輕易利用被害者協助攻擊他人的電子郵件
    - 轉寄電子郵件給親友、同事

電子郵件社交工程防護措施

- 實體層面
  - 開啟網路防火牆
  - 設定並定時更新電腦密碼
  - 機密資料使用加密保護
  - 定時執行最新的系統修補程式
  - 電子郵件軟體設定
    - 關閉「自動下載圖片」功能
    - 取消「郵件預覽」
    - 關閉「自動傳送回條」功能
    - 以「純文字格式」讀取郵件內容

電子郵件社交工程防護措施(續)

- 心理層面
  - 建立正確的個人資訊安全觀念
    - 檢查寄件者名稱與信箱
    - 以郵件主旨評估是否有必要開啟郵件
    - 檢查郵件內的連結是否正確

      例: www.google.com ⇨ www.goog1e.com
    - 檢查郵件附檔的副檔名是否為常見可含有病毒的檔案名稱(*.bat、*.pif、*.exe、*.zip、*.src、*.cmd、*.rar等等)
    - 轉寄郵件時刪除寄件者與收件者資料，並使用密件傳送

電子郵件社交工程演練

電子郵件社交工程演練

- 目前沒有任何產品或安全系統可以為電子郵件社交工程提供100%的防護並同時兼顧電子郵件使用者的個人需求

因為任何資安系統最薄弱的一環是「人」

唯有良好的資訊安全觀念才是投資報酬率最高的安全對策：

針對電子郵件使用者實施電子郵件社交工程演練

電子郵件社交工程演練(續)

- 根據行政院國家資通安全會報於2007年頒定的「防範惡意電子郵件社交工程施行方案」，各主管機關每年應至少辦理2次電子郵件社交工程演練
- MIC 於 2011 年 1 月的調查報告中指出
  - 2011~2013年台灣企業預計往雲端服務發展，而前2項服務為資訊安全與電子郵件
  - 當企業考慮走向雲端運算時，資訊安全與電子郵件服務即將成為企業擁抱雲端的關鍵起點
  - 思考：雲端化的電子郵件系統如何防護社交工程攻擊呢？

電子郵件社交工程演練(續)

- 96、97年度政府內部電子郵件社交工程演練資料

區分	平均		最高	最低
	開啟率	點閱率	開啟率	開啟率
96年度	18.02%	11.46%	58.57%	2.73%
97年度	30.57%	19.81%	100%	1.53%

資料來源：行政院國家資通安全會報技術服務中心

電子郵件社交工程演練(續)

- 教育部99年度電子郵件社交工程演練計畫
  - 本計畫主要分為兩個階段
    - 對所有人員進行社交工程演練
    - 對演練成績不佳的人員進行教育訓練
  - 訓練時間
    - 社交工程教育訓練所花費時間：一個月（演練前）
    - 社交工程演練所花費時間：一個月（演練中）
    - 再次教育訓練所花費時間：三個月（演練後）

電子郵件社交工程演練(續)

- 其他企業的教育訓練也跟政府進行的十分相似，但這樣的訓練方法也產生以下幾項問題：
  - 公司員工資料外洩
  - 演練花費龐大
  - 需要專業人員執行演練計畫

市面既有社交工程演練系統（舉例）

- 市面上的社交工程演練系統並不多，Google網站有關電子郵件社交工程演練排名最高的前兩家公司分別為(以下資訊來源為其公司網站)：
  - 定威科技
    - 可自行針對單位人員進行電
    - 軟體功能可模擬駭客寄送電
    - 可自行設計社交工程演
    - 可假冒寄件者
    - 自動收集收件者點選記錄
  - 漢昕科技
    - 委外採簽訂保密協定方式
    - 由漢昕科技執行社交工程演練
    - 演練結束後報送演練結果

無社交工程教育訓練功能

無法證明演練郵件的效果

＋ 教育訓練」流程的功能

真正的市場需求在哪裡？

真正的市場需求

- 電子郵件社交工程演練能隨時舉行
- 演練成本要低
- 需要即時、方便、省成本的電子郵件使用者教育訓練
- 實施演練時，避免任何組織資料外洩的疑慮
- 演練的工具或系統以及產生的資料，能掌握在組織手中

電子郵件社交工程自動化演練與教育系統

- 符合市場需求的電子郵件社交工程自動化演練與教育系統應有以下幾項特點：
  - 可人工自行設計社交工程電子郵件
  - 自動化製作含有社交工程訊號的社交工程電子郵件
  - 電子郵件社交工程演練與教育訓練全自動化

電子郵件社交工程自動化演練與教育系統

系統設計

- 名詞解釋
  - 社交工程電子郵件
    - 使用社交工程技巧於郵件內容上，誘使收件者情不自禁執行郵件功能，例如，開啟郵件、點閱郵件內連結、開啟附件
  - 社交工程訊號
    - 社交工程訊號指的是當收件者執行郵件功能時所觸發的訊號
      - 收件者開啟郵件的訊號
      - 收件者點閱郵件內連結的訊號
      - 收件者開啟郵件附件的訊號

系統設計(續)

- 本系統分成兩個部份，分別是
  - 應用程式端
    - 負責執行社交工程演練與教育訓練
  - 網頁資料庫端
    - 負責接收並儲存社交工程訊號

系統設計(續)

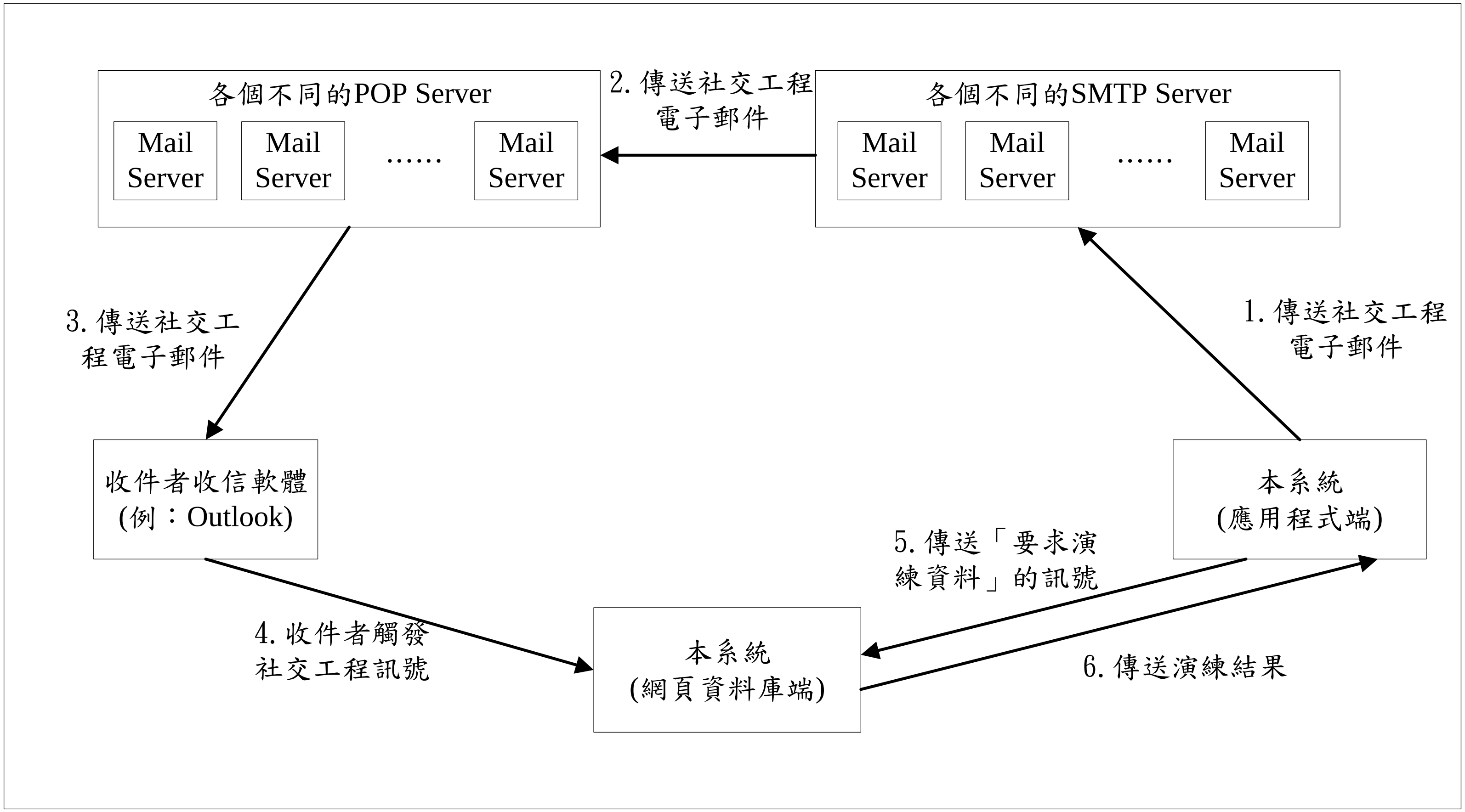
- 應用程式端功能
  - 可隨意更換不同Mail Server
  - 自動化製作社交工程電子郵件
  - 可自行設計社交工程電子郵件
  - 插入社交工程訊號於任意郵件中
  - 可設定郵件傳送頻率
  - 演練完成後自動執行教育訓練
  - 重覆進行社交工程演練與教育訓練
  - 資料庫查詢

系統設計(續)

- 網頁資料庫端功能
  - 處理社交工程訊號
  - 提供使用者欲查詢的演練資料

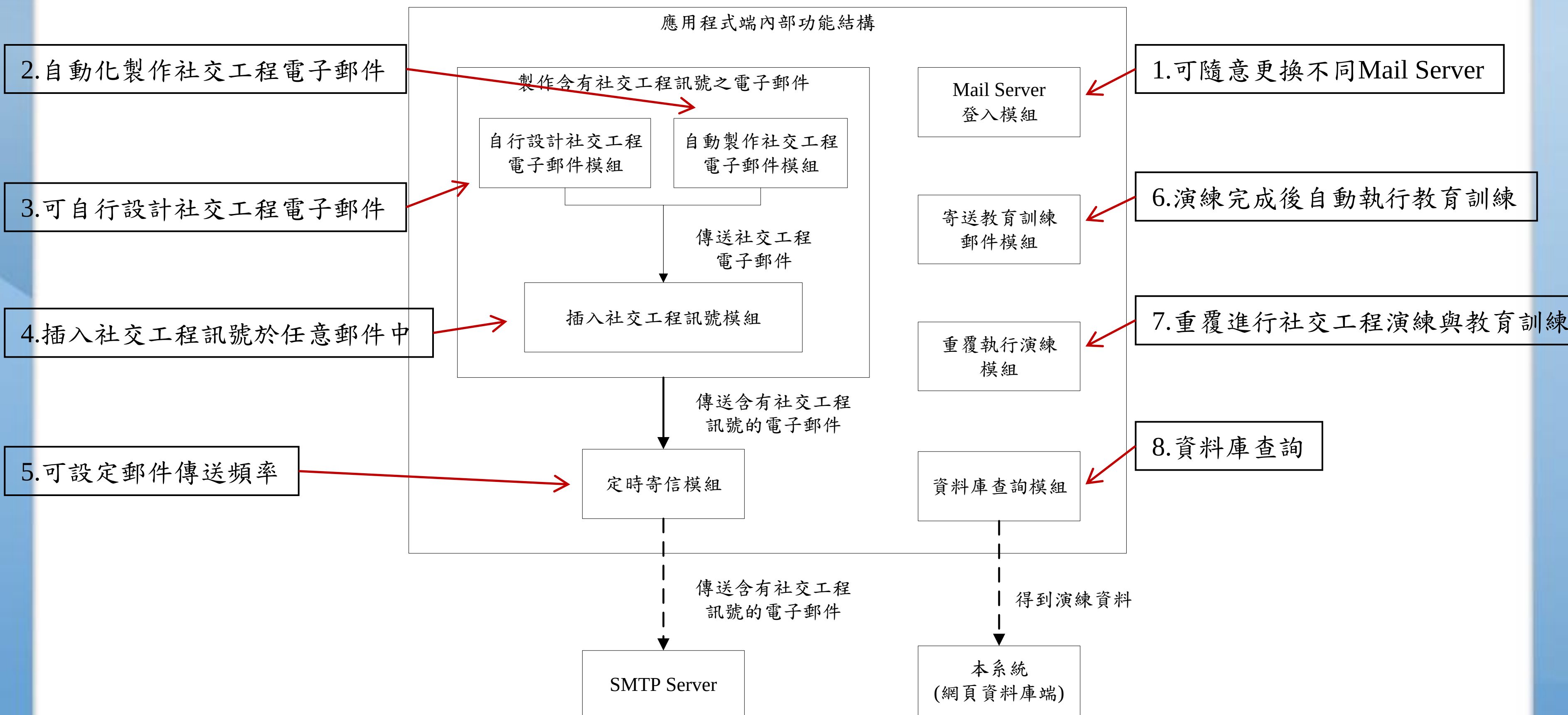
系統架構

- 完整系統架構圖



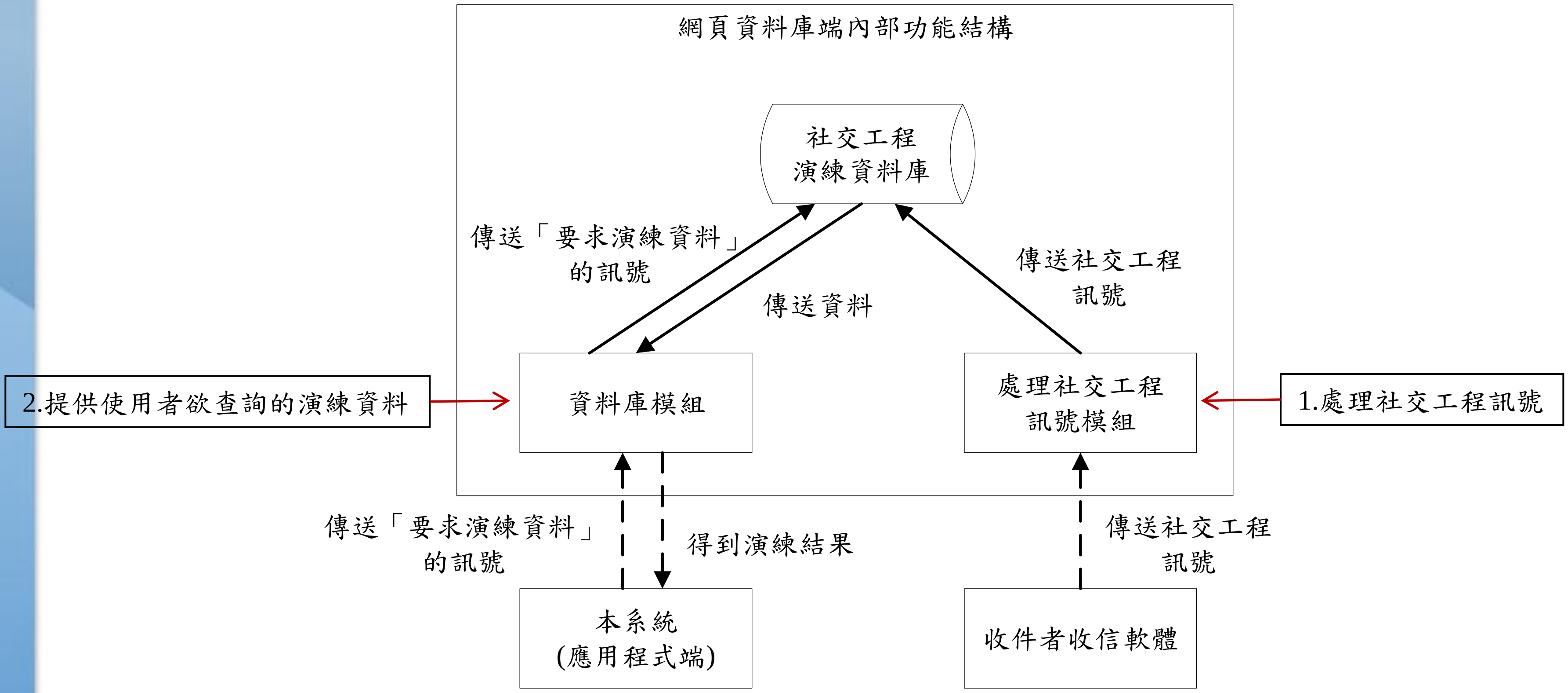
系統架構(續)

- 應用程式端內部功能結構

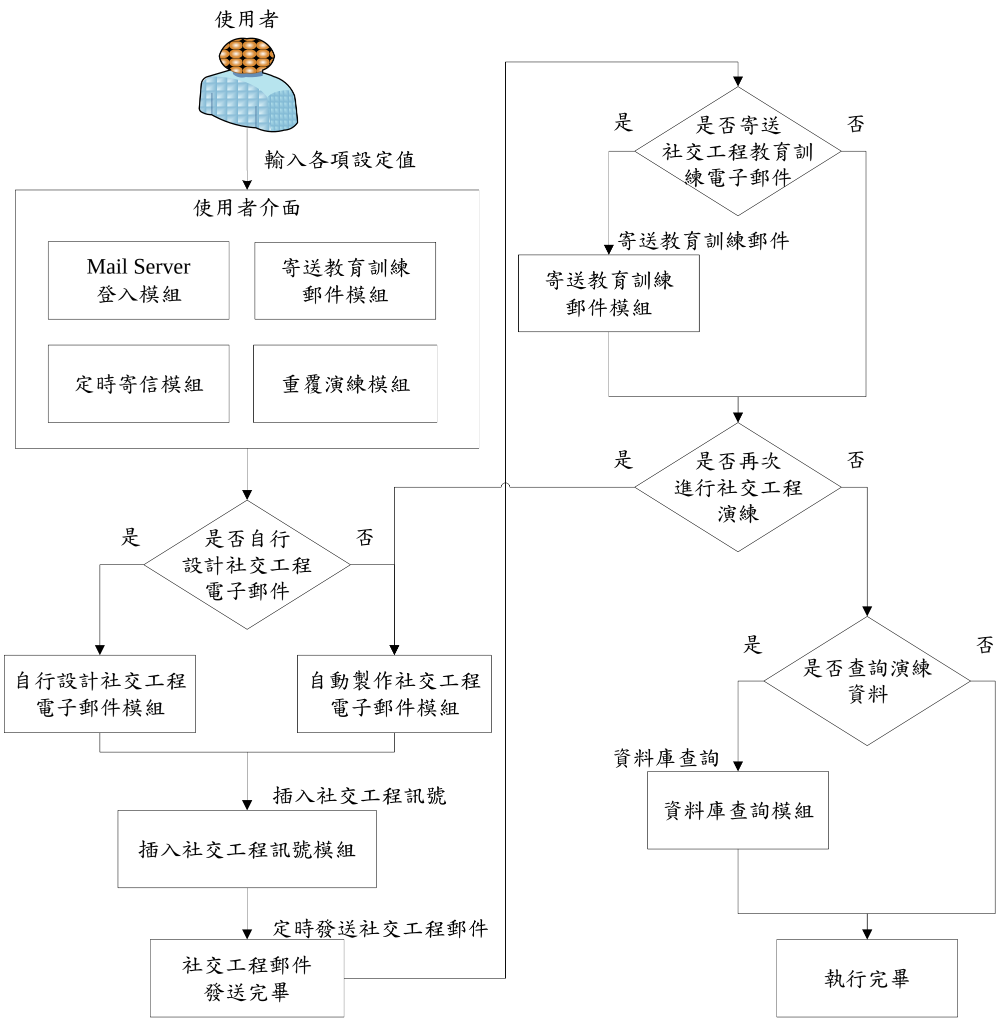


系統架構(續)

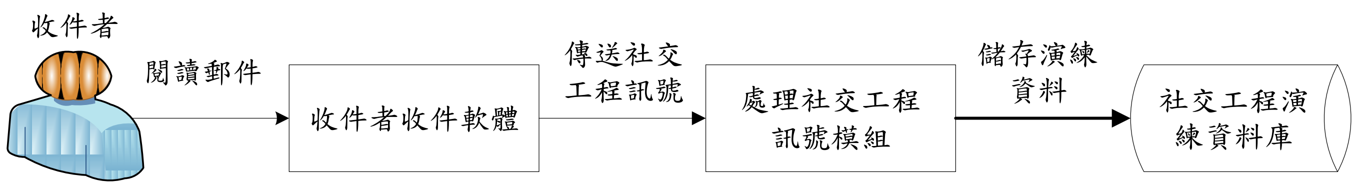
- 網頁資料庫端內部功能結構



系統流程(應用程式端)


使用者
輸入各項設定值
使用者介面
Mail Server
登入模組
寄送教育訓練
郵件模組
定時寄信模組
重覆演練模組
是
否
是否自行
設計社交工程
電子郵件
自行設計社交工程
電子郵件模組
自動製作社交工程
電子郵件模組
插入社交工程訊號
插入社交工程訊號模組
定時發送社交工程郵件
社交工程郵件
發送完畢
是否寄送
社交工程教育訓
練電子郵件
寄送教育訓練郵件
寄送教育訓練
郵件模組
是否再次
進行社交工程
演練
是否查詢演練
資料
資料庫查詢
資料庫查詢模組
執行完畢

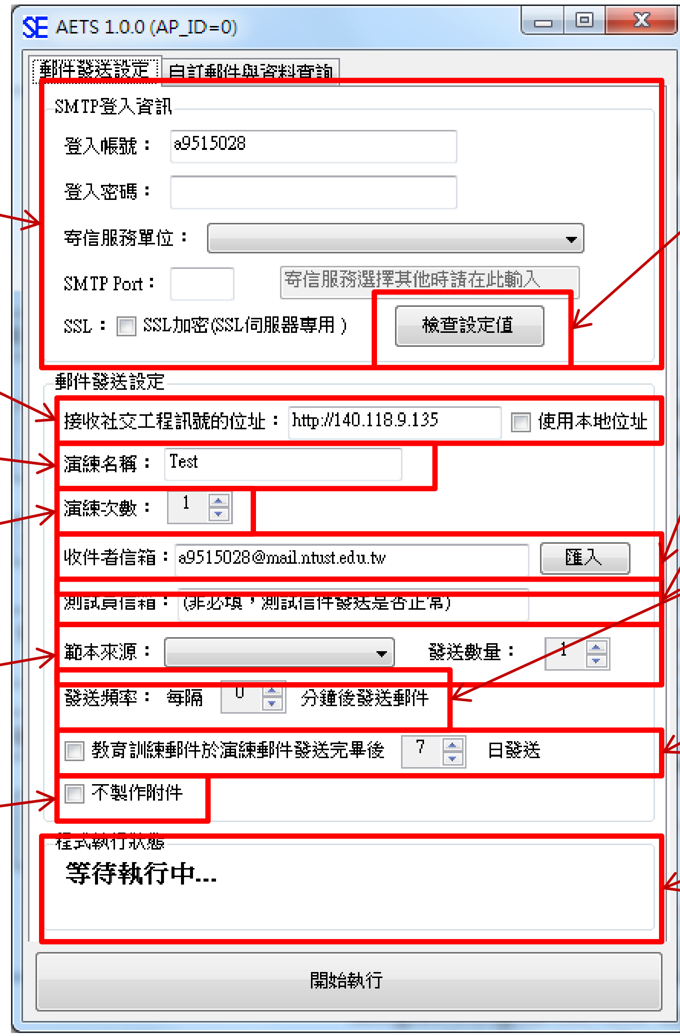
系統流程(網頁資料庫端)



系統實作

- 系統介面與功能介紹
- 系統執行流程
- 社交工程電子郵件解析
- 社交工程演練結果資料解析

系統介面與功能介紹



設定 Mail Server

設定網頁
資料庫端位址

設定演練名稱

設定重覆進行
演練的次數

設定郵件範本
來源及發送數量

可設定不自動
製作附件

驗證輸入資料

收件者郵件群組
批次輸入

設定測試員信箱

發送郵件頻率設定

教育訓練郵件
發送設定

顯示
程式執行狀態

系統介面與功能介紹(續)

自行設計
社交工程郵件介面

是否使用相同寄件者

加入郵件附加檔案

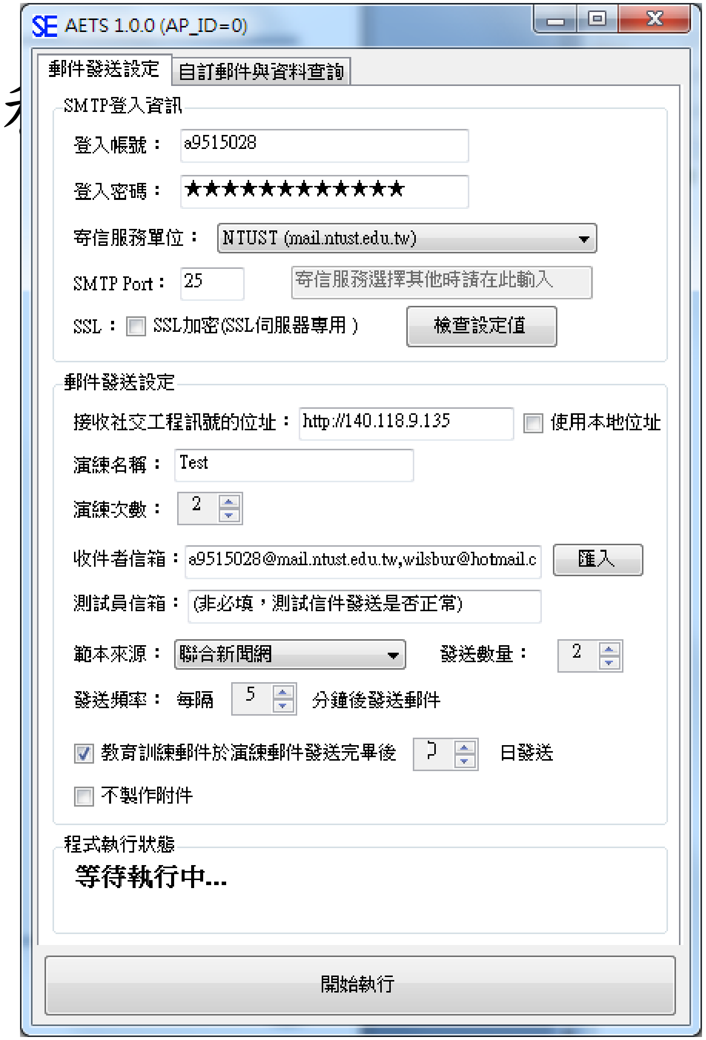
演練資料查詢

系統設定(範例)

控制項名稱	控制項內容
Mail Server	NTUST(mail.ntst.edu.tw)
Mail Server Port	25
SSL加密	不使用
演練名稱	Test
演練次數	2
收件者信箱	a9515028@mail.ntust.edu.tw, wilsbur@hotmail.com
測試員信箱	不使用
範本來源	聯合報
發送數量	2封
發送頻率	5分/1封
教育訓練郵件	於演練完畢後0天發送
自訂寄件者名稱	測試用
自訂寄件者信箱	test@gmail.com
自訂郵件內容	測試用 Google
自訂附加檔案	測試用.doc

系統執行流程(範例)

- 步驟一：開啟



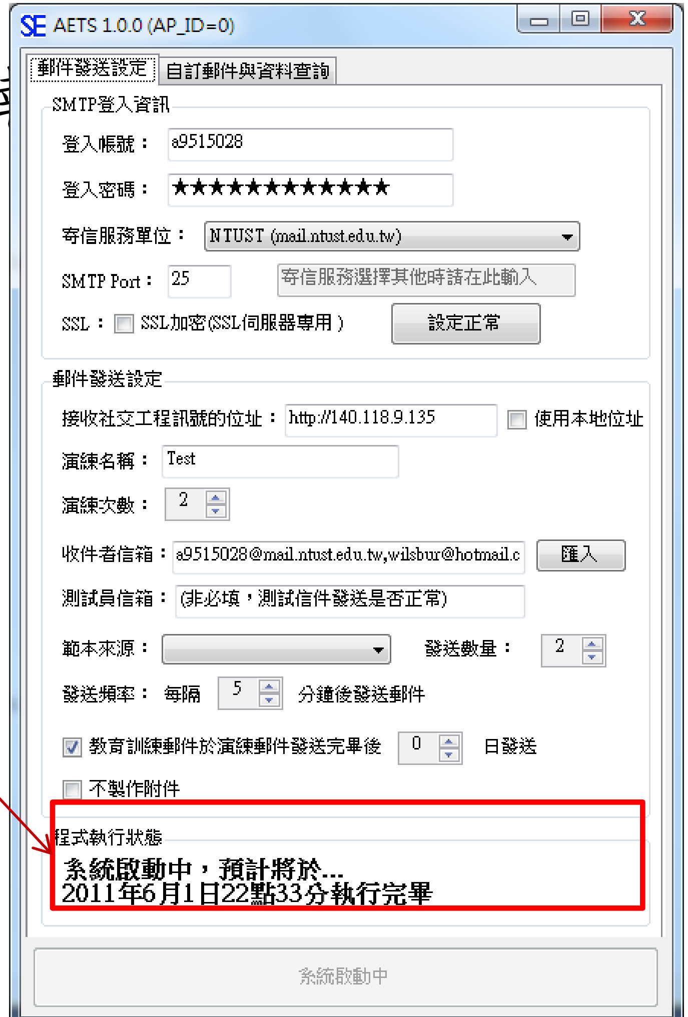
系統執行流程(範例)

- 步驟二：輸入

系統執行流程(範例)

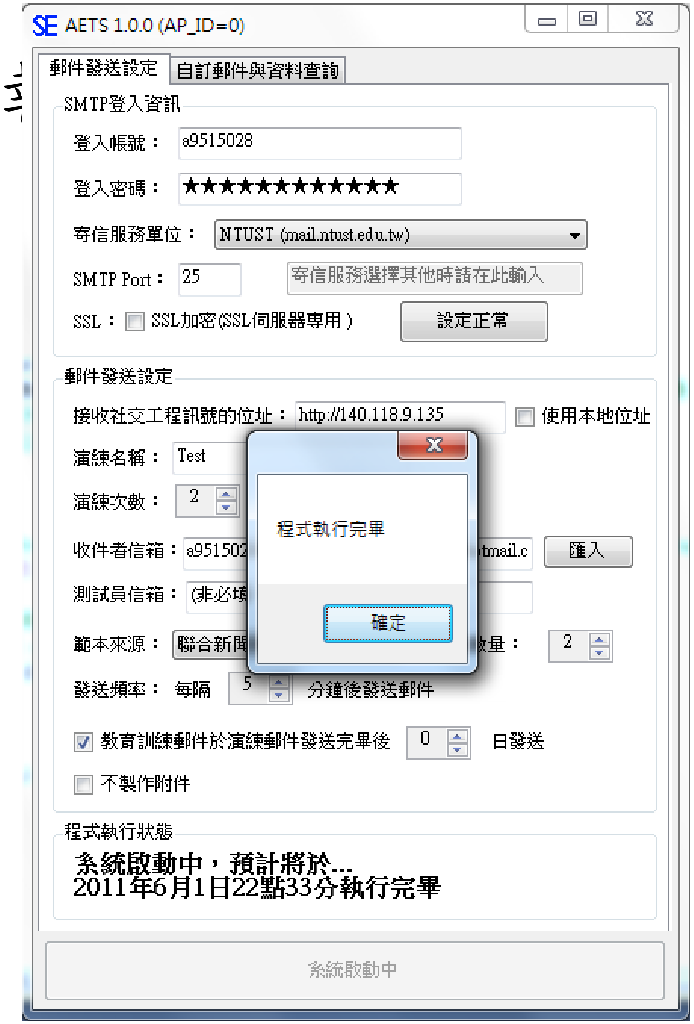
- 步驟三：開始

計算並顯示預計將執行完畢的時間



系統執行流程(範例)

- 步驟四：系統



社交工程電子郵件解析

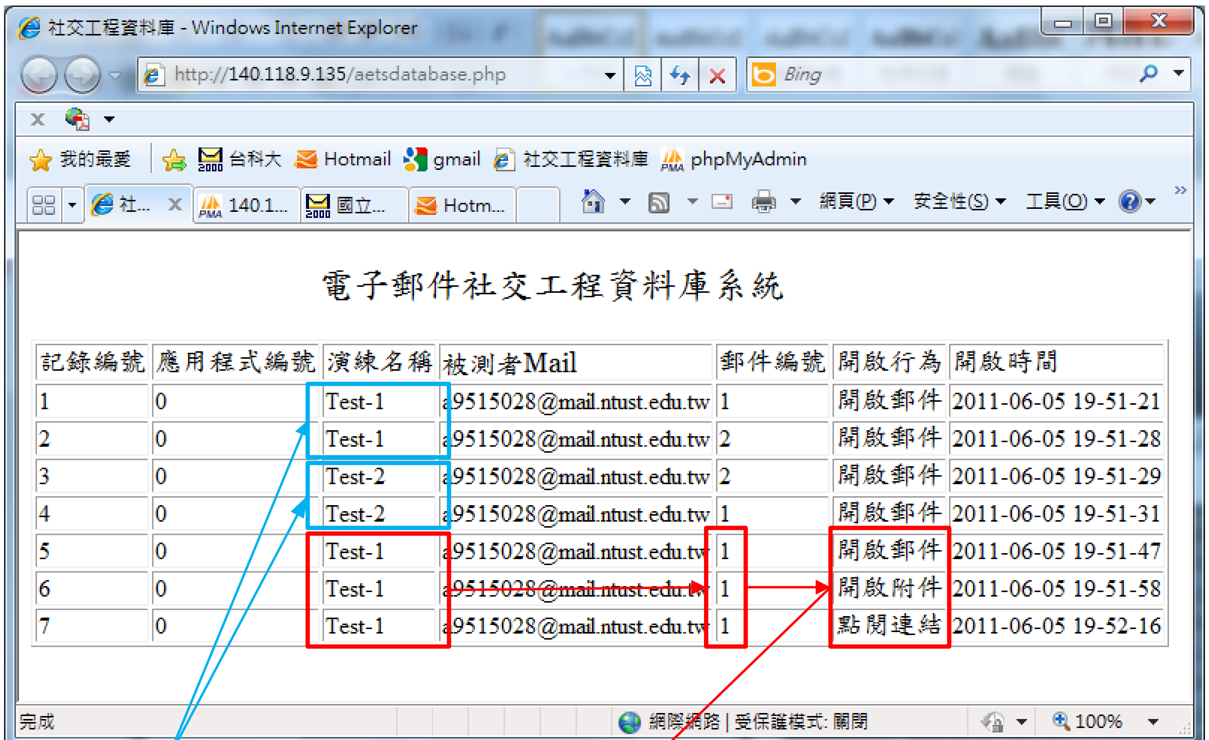
第二次演練郵件

第一次演練郵件

預覽視窗

社交工程演練結果資料解析

- 電子郵件社交工程資料庫系統



電子郵件社交工程資料庫系統

記錄編號	應用程式編號	演練名稱	被測者Mail	郵件編號	開啟行為	開啟時間
1	0	Test-1	a9515028@mail.ntust.edu.tw	1	開啟郵件	2011-06-05 19-51-21
2	0	Test-1	a9515028@mail.ntust.edu.tw	2	開啟郵件	2011-06-05 19-51-28
3	0	Test-2	a9515028@mail.ntust.edu.tw	2	開啟郵件	2011-06-05 19-51-29
4	0	Test-2	a9515028@mail.ntust.edu.tw	1	開啟郵件	2011-06-05 19-51-31
5	0	Test-1	a9515028@mail.ntust.edu.tw	1	開啟郵件	2011-06-05 19-51-47
6	0	Test-1	a9515028@mail.ntust.edu.tw	1	開啟附件	2011-06-05 19-51-58
7	0	Test-1	a9515028@mail.ntust.edu.tw	1	點閱連結	2011-06-05 19-52-16

第一次跟第二次演練

同一封社交工程郵件的三種觸發動作

結論

結論

- 社交工程是操縱他人執行某些特定動作(例如使用ATM匯款)或吐露特定資訊的人際技巧
- 在資訊安全議題上，運用電子郵件執行社交工程可能造成個人與組織的重大損失（名譽、商譽、財務等）
- 運用電子郵件社交工程自動化演練與教育系統可以達到在低成本、高安全性的前提下，組織提升人員在電子郵件方面的資安認知與警覺性

系統展示

Q&A

Email: nwlo@cs.ntust.edu.tw
URL: http://idsl.cs.ntust.edu.tw/index.html