植基於 Google 雲端訊息推播技術的行動認證機制 (Mobile Authentication Based on Google Cloud Messaging)

楊慶隆　　邱創昱　　蔡松叡
國立東華大學 資訊工程學系
cnyang@mail.ndhu.edu.tw

摘要

多數人習慣使用容易記的弱密碼當作自己帳號的通行碼，但是這些簡單的數字組合，容易遭破解。如果選擇數字與符號不具意義的長密碼，又容易遺忘。由於人對圖形的記憶比文字容易，很多點擊式的圖形密碼認證機制被提出，以代替文字密碼。但是圖形密碼需要大的資料庫容量來儲存圖片。本文以 Android 平台，結合 Google 雲端訊息推播技術 (Google Cloud Messaging; GCM)，設計完成一個行動認證機制。藉由智慧型手機以及一台具有視訊鏡頭的電腦，不需要記憶密碼就可以使用這套行動認證機制登入帳號。使用者登入時，會從 GCM Server 同步推播至手機一組亂數，再經具金鑰的雜湊函數，計算得雜湊值並轉換為 QR 碼。透過視覺通道(電腦的視訊鏡頭替代肉眼判斷影像內容稱之為視覺通道)，將雜湊值傳送到伺服器。最後使用者成功登入系統，而視覺通道讓我們不用手動輸入長串的雜湊值，也能防止側錄或偷窺攻擊。

關鍵詞：Google 雲端訊息推播技術、QR 碼、雜湊函數、認證、視覺通道。

Abstract

People often use weak passwords, such as the names, or combination of alphanumeric words, for their accounts. However, these weak passwords are easily cracked by malicious attackers. Choosing the strong password is secure, but it is not easy to remember. Since graphic picture is more memorable than text, graphical passwords are accordingly proposed. However, graphical password needs a large storage capacity to store the pictures. In this paper, we implement a mobile authentication scheme based on Google Cloud Messaging (GCM). Through the helps of smart phone and computer with a camera, one can login accounts without remembering password. Client's mobile device will receive a random number from GCM Server by push notification. By using the keyed hash function, a hashed value is determined from this random number and then transferred to QR code. Through the visual channel (composed of smart phone and computer with a camera), we can transmit this hashed value to the server. Finally, one can successfully login system. Meantime, the visual channel let users not keyin the long hashed value and meantime can avoid the peeping attack.

Keywords: Google Cloud Messaging (GCM), QR code, Hash function, Authentication, Visual channel.

1. 前言

網路服務千百種，現代人生活已經和網路脫不了關係，舉凡食衣住行都與網路有關，網路上使用者不計其數，就以 Facebook 來說，在 2012 年已超過十幾億名活躍用戶，為了要區別使用者，各大網站都有其登入系統，此類需要登入操作的網站本文稱作「登入網站」，目前主要登入方法為輸入一組帳號密碼[1]-[3]，但每天需使用到的服務繁多，帳號密碼不只一組，若註冊新帳號又須多記一組密碼，導致使用不便。一般而言，使用者會選擇短密碼，或者是自己的名字、生日、電話、寵物名字來當作密碼。若是這樣，惡意的攻擊者可使用密碼攻擊工具來破解。如果選擇數字與符號不具意義的長密碼增加安全強度，又容易遺忘。而且在不安全的環境中輸入密碼可能會被竊取，導致隱私暴露，為此若能有個統一且快速，安全性高又不需要記憶密碼的登入方法，必能有極多的應用場合。

如何讓使用者不需要記憶密碼就可以達到認證。當然可使用指紋、視網膜、聲音波型等個人的生物特徵，但是這增加了複雜度。或者是使用圖形密碼認證機制[4]-[5]，利用人對圖形的記憶比文字更容易，避免記憶長密碼。但是圖形密碼需要大的資料庫容量來儲存圖片。本文以 Android 平台，結合 Google 雲端訊息推播技術 (Google Cloud Messaging; GCM)，設計完成一個行動認證機制。藉由智慧型手機以及一台具有視訊鏡頭的電腦，不需要記憶密碼就可以使用這套行動認證機制登入帳號。由於智慧型手機的普及，幾乎人手一支，且有高度相容性。例如 Google 的 Android 手機智慧型手機以及一台具有視訊鏡頭的電腦平台，憑著完全開放原始碼免費的作業系統，任何人都能獲得及使用 Android 系統，越來越多的國內外開發工程師也競相投入 Android 手機開發行列，進而成為手機市占率最高的作業系統。使得現代人生活中擁有方便性絕佳的載具，讓我們的行動認證機更為可行。

綜合以上敘述，本文提供一種安全且方便的登入方式，使用者不再需要記憶密碼，且可快速的登入各個「登入網站」。使用者登入時，會從 GCM Server 同步推播至手機一組亂數，再經具金鑰的雜湊函數，計算得雜湊值並轉換為 QR 碼。透過視覺通道(電腦的視訊鏡頭替代肉眼判斷影像內容稱之

為視覺通道)，將雜湊值傳送到伺服器。最後使用者成功登入系統，而視覺通道讓我們不用手動輸入長串的雜湊值，也以能防止偷窺攻擊。

文章架構如下，第二部份是為相關背景，介紹 GCM 推播技術的使用方式及特色。第三部份為本文所提的植基於 Google 雲端訊息推播技術的行動認證機制。App 實作，則於第第部份說明，最後為本文結論。

2. 相關背景

GCM 為 Google 提供的一種訊息推播技術，可將伺服器上的資料推播給行動裝置(如手機、平板)上的 App。使用此技術的伺服器需向 Google 申請 API key，由 API key 可向 GCM Server 申請 Sender ID [6]。Android client 端的裝置要加入此推播的群組，只需將 Sender ID 傳送給 GCM 伺服器，並將收到的 Register ID (簡稱為 RegID) 傳送給應用程式伺服器，就完成加入此推播群組的工作。當應用程式伺服器要傳送訊息時，需將本身的 API Key 和使用者的 RegID 及欲發送的訊息傳送給 GCM 伺服器，就可由 GCM Server 推播給行動裝置上的 App[7]-[8]。

GCM 可幫第三方的伺服器端發送訊息，至該伺服器的使用者行動裝置上，且行動裝置不必維持運行狀態。當要傳送訊息時，伺服器會利用無線網路推播來喚醒行動裝置，再由手機中的 App 接收訊息資料。當行動裝置在無網路的環境下，無法收到訊息，這些通知訊息將會被存在伺服器中，而這些被暫存的訊息有數量上的限制，數量限值為一百則，當超過一百則時通知訊號將會被丟棄，直到行動裝置回到有網路的環境底下，行動裝置將會收到一條特殊的訊息通知，告知通知訊號的數量已達上限。

GCM 所傳輸的資料分為兩種，一種是輕量型的訊息，用來通知行動裝置上的 App 去擷取伺服器上的資料；另一種是含有裝載資料的訊息，訊息大小的限制為 4KB，大部分用在即時通訊上的簡單訊息交換。本機制採用第二種的方式，伺服器產生亂數後，藉由 GCM 的推播機制，將亂數推播給使用者，並由我們完成的 App 雜湊此亂數並產生 QR 碼。透過視覺通道，讓視訊裝置擷取 QR 碼，且送至伺服器端。

3. 植基於 GCM 的行動認證機制設計

使用者需要有智慧型手機，及擁有視訊鏡頭的電腦裝置。當使用者要登入一個「登入網站」時，可點選本機制提供的登入頁面，輸入完帳號後，本系統的認證伺服器會發送亂數，藉由 GCM Server 推播給使用者的手機，由手機中的 App，將亂數透過具金鑰的雜湊函數 (註: 此金鑰為使用者與登入網站所分享的秘密訊息)。產生的雜湊值則為此次登入的密碼，並轉成 QR 碼的形式在手機螢幕上呈現，使用視訊鏡頭擷取 QR 碼並傳回伺服器端。伺服器比對 QR 碼與亂數的雜湊值是否相同。若相同，使用者可以登入此網站。有別於傳統輸入密碼的方式，此種透過視訊鏡頭擷取畫面的方式，稱為視覺通道，不會有輸入密碼被側錄或偷窺的風險[9]-[10]。此亂數雜湊值為密碼，每次數值皆不相同，為一次性密碼，不需擔心密碼外洩或竊取的可能。透過 GCM 推播技術，使用者可以馬上取得此亂數，不需要記憶密碼。我們將此認證機制稱為行動認證，是因為過程中使用這需藉由行動裝置的幫忙。表 1 為行動認證機制與傳統登入方式的比較。

表 1. 本機制與傳統方式之比較

	本機制	傳統方法
安全性	採用亂數雜湊值為密碼，每次不同，只有該手機收到亂數。	每次密碼相同。需防止密碼被側錄或偷窺。
便利性	密碼被轉成 QR 碼後，透過視覺通道傳送雜湊值。	需手動輸入密碼，不同帳號密碼不同，有忘記密碼的疑慮

3.1 本機制架構

本機制架構如圖 1 所示，令 H，M，P，S，G 分別代表使用者，行動裝置(智慧型手機)，一台具有視訊鏡頭的電腦，認證伺服器，以及 GCM Server，詳細認證步驟說明如下:

(1) $H \rightarrow P \rightarrow S$: 輸入使用者帳號。
(2) S: 產生亂數 α。
(3) $S \rightarrow G$: 傳送{API key, RegID, α}至 GCM Serve。
(4) $G \rightarrow M$: 將 α 推播至使用者的智慧型手機。
(5) M: 計算 $\beta = H_K(\alpha)$，並用 β 產生 QR 碼，其中 $H_K(\cdot)$ 為具有金鑰的雜湊函數。H 與 S 分享金鑰 K。
(6) $M \rightarrow P \rightarrow S$: 透過視覺通道傳送 QR 碼。
(7) S: 從使用者帳號取得相對的金鑰 K 並由 QR 碼得 β，來確認 $\beta \stackrel{?}{=} H_K(\alpha)$。

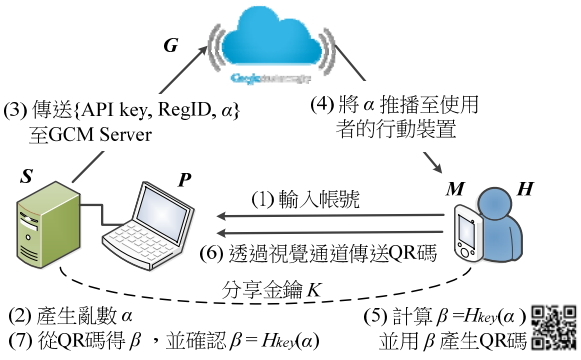

圖 1. 使用 GCM 推播技術的行動認證機制

一般的方法都是輸入帳號密碼，任何人只要有

密碼後即可登入。本方法的特色在於登入不需輸入任何密碼，藉由行動裝置(如智慧型手機)中的 App 接收由 GCM Server 傳送來的一組亂數 α。因為認證伺服器與使用者分享金鑰 K，當它由視覺通道收到 QR 碼後，驗證 $\beta \stackrel{?}{=} H_K(\alpha)$ 來決定是否為合法使用者。

3.2 伺服器端與行動裝置端之設計

本論文提供各種需要登入操作的網頁(如社群網站、信箱、...等)一種新的認證機制，採用此設計的網頁可在登入頁面提供連結，讓使用者選擇傳統的登入方式或此認證方式。本系統包含認證伺服器，及一個手機 App。該認證伺服器需先向 GCM 申請一組 API key，並擁有一個資料庫，記錄使用者的帳號，RegID，與雜湊時使用的金鑰 K。

當使用者從行動裝置中下載本系統的 App 後，App 會自動的向 GCM 申請一組 RegID，並傳送至認證伺服器端。認證伺服器收到後，產生一把雜湊用的金鑰，此金鑰需以“離線”方式通知使用者，並輸入至手機。完成後，App 會列出與本計畫合作的網頁，使用者可以選擇那些網頁要採取此方式登入，並進行綁定程序，因為當使用者在此網站採取本系統的認證登入方式，將不再需要輸入密碼，只需要使用者本人的手機。

在 App 中點選與本系統合作的「登入網站」後，會連結到該網站的綁定頁面中，過程中需填入此網頁使用者的帳號密碼，若為合法使用者，網頁會傳送帳號與 RegID 至本系統的認證伺服器。綁定過程是在網頁端處理，本 App 不會接觸到使用者在各網頁的密碼，確保使用者隱私。當使用者欲登入一採用此系統的網頁，可點選連結至本系統為此網頁設計的頁面，使用者輸入完帳號後，會進行圖 1 的認證過程，當認證伺服器確認是合法登入的使用者後，會向此「登入網站」發送使用者在此網頁的帳號與登入訊息，並由「登入網站」讓使用者轉跳至登入後的畫面，完成登入程序。

4. 系統實作

本部份介紹此行動認證系統的實作過程，包括以 Android 的環境下並配合 Eclipse 整合開發環境的 App，以認證伺服器的建置。

4.1 開發流程與技術

此系統分為兩個部分，認證伺服器與行動裝置上的 App。認證伺服器端需架設多個的認證服務網頁，提供每個需要登入網站的專屬頁面。認證伺服器需與各「登入網站」間有一個安全的 VPN 通道，並有傳送訊息給 GCM Server 的功能。所建置的網頁，可讓使用者填入帳號，藉由此帳號，在資料庫中尋找使用者的 RegID，並產生亂數，讓 GCM 推播至使用者的行動裝置中。當收到由視覺通道傳來之 QR 碼時，認證伺服器需解回 QR 碼並比對亂數雜湊值是否與 QR 碼的值相同。認證伺服器除需具備以上功能外，還需在新的使用者註冊時，需將對方的 RegID 寫入資料庫中，並產生一把金鑰，作為雜湊時共享的金鑰。上述，是我們開發一個認證伺服器所需的功能。

另一方面，手機端的 App 程式所需的功能說明如下。App 安裝完後，初次執行時要自動向 GCM 註冊一組 RegID，並傳送至認證伺服器中。之後，使用者可以選擇那些「登入網站」要啟用本系統的行動認證機制，點選後，程式要開啟連結至該網站的綁定頁面。當使用者填入帳號後，「登入網站」會將帳號與 RegID 發送至本系認證統伺服器，讓認證伺服器寫入資料庫中。Android 手機中具金鑰的雜湊函數，我們是使用 MD5，並採用 HMAC (Hash-based Message Authentication Code)方式，輸出雜湊值大小為 128 位元，並且轉換成 QR 碼的形式，在螢幕上呈現。

在認證網頁及手機 App 中，本文所需的 QR 碼編解碼程式，使用 ZXing 所提供的開放原始碼。ZXing 提供了多種不同一維及二維條碼的編解碼原始碼，如 Code 39、Code 93、Codabar...等，提供了各種語言所撰寫的開放原始碼，可以在不同的平台上執行。本文使用 Java 語言在網頁與 Android 平台上實作 QR 碼的編解碼，開發介面如圖 2，使用 Eclipse 撰寫程式碼，並匯入 ZXing 提供的 JAR 檔，以執行其提供的套件程式。

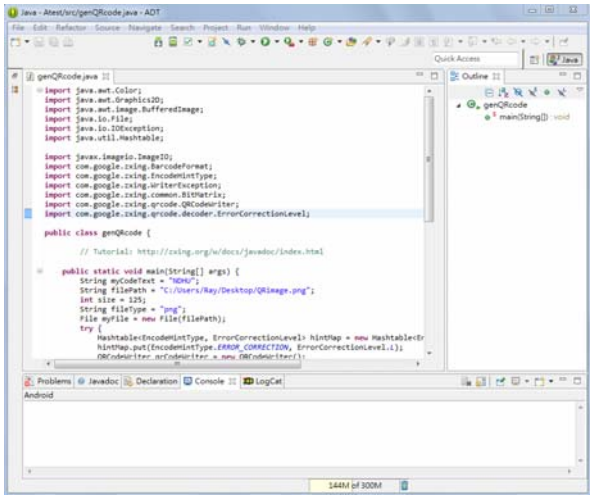

圖 2. QR 碼實作介面

圖 3 為 QR 碼產生器的部分指令，當亂數經過雜湊後，輸出為字串型態，大小為 128 位元，宣告參數 CodeText 及 Size 來儲存字串內容與大小，並產生錯誤控制碼編碼對應 ECCMap，以 QRCodeWriter 類別建立物件，輸入相關參數便可產生 QR 碼的二元矩陣，之後在由矩陣產生圖檔即完成 QR 碼。

```
String CodeText = hashValue;
int size = 128;
...
QRCodeWriter qrWriter = new QRCodeWriter();
BitMatrix matrix = qrWriter.encode (CodeText,
BarcodeFormat.QR_CODE, size, size, ECCMap);
...
```

圖 3. QR 碼部分程式

4.2 實作結果

實作本系統需撰寫一支手機 App 程式，以及架設一個進行認證伺服器，兩者皆須滿足上一節所提之功能。當使用者從 Android 平台中下載本系統的 App 後，初次執行時，系統會進入等待畫面，如圖 4(a)所示，此過程會向 GCM 註冊一組 RegID，當取得 RegID 後再發送給本系統認證伺服器。認證伺服器會產生一把雜湊時使用的金鑰，此金鑰需以“離線”方式通知使用者，以完成註冊程序。App 會進入主程式頁面，如圖 4(b)。使用者可以選擇那些「登入網站」要使用本系統的行動認證服務。

(a) (b)

圖 4. 本系統手機 App 執行畫面

當點選其中一個登入網站後，程式會自動開啟網頁，連結至該登入網站的綁定頁面，當登入網站與採用本系統的認證服務時，圖 5 為模擬的綁定頁面。連結此頁面時，程式會自動將 RegID 傳送至該登入網站。當使用者輸入完帳號密碼後，點選啟用，當網站確認帳號密碼無誤後，會將帳號與 RegID 一起發送至本系統伺服器，並完成綁定程序碼。

圖 5. 登入網站中啟用認證服務頁面

與本系統合作的「登入網站」，可以在原登入頁面放置連結，讓使用者可以進入本系統為此網站所架設的認證頁面。或是該網站直接採用本系統服務，作為該網站的登入方式。當一個經過綁定程序的使用者要登入網站時，會連結至本系統的認證網頁，如圖 6 所示。使用者輸入帳號後，按下確認鍵，伺服器端會在資料庫中查詢該帳號的 RegID，並產生亂數，由 GCM 推播至使用者的手機。

圖 6. 本系統認證服務網頁

手機端收到亂數後，App 透過金鑰將亂數雜湊，運算完的值以 QR 碼呈現在螢幕上，如圖 7 所示。

圖 7. 進行認證服務所需的 QR 碼

使用者將手機畫面對準視訊鏡頭，透過視覺通道掃描 QR 碼，如圖 8 所示。視訊畫面下方，會顯示發送訊息時間，當手機接收到後可以比對時間，確認是否為該次認證的 QR 碼。

圖 8. 透過視覺通道擷取 QR 碼

當伺服器取得 QR 碼中後，與亂數雜湊值比

對，確認使用者是否認證成功，並將結果回傳給「登入網站」，若使用者認證成功，網站便轉跳至登入後的畫面。若使用者在本系統認證網頁中，在收訊不好的情況下，輸入完帳號後，卻沒有收到由 GCM 推播來的亂數，無法產生 QR 碼時。使用者只需重新整理頁面，並再次輸入帳號，伺服器會重新發送亂數，不須擔心遺失封包而無法登入網頁的問題。傳送時，手機螢幕也會顯示發送時間，可以與網頁上顯示的比對，確認是否為該次認證的 QR 碼，以避免惡意第三者的重送攻擊。由於每次登入都會有不同的亂數，產生的 QR 碼也都不相同，所以手機 App 程式只會暫存顯示 QR 碼，當使用者掃描完按下確認後，會自動移除並將記憶體釋回給作業系統，使用者不需擔心使用本系統 App 造成儲存空間的負擔。

5. 結論

本論文採用 Android 開發，搭配智慧型手機及具視訊鏡頭的電腦，完成了能夠使建立在視覺通道的認證方法，登入過程無需記憶繁雜的密碼，也更有安全性保證。我們將此認證機制稱為行動認證，是因為過程中使用這需藉由行動裝置的幫忙。雖然本方法有硬體上的限制，但對於登入機制又多了一樣選擇。做這個專題開發此行動認證，我們學習了 JAVA 語言在 Android 平台的開發過程，及使用 Eclipse、模擬器等開發工具，並了解 QR 碼的轉換原理，透過 GCM 雲端推播技術，設計安全且方便的網站登入系統。

本行動認證機制，除了使用 GCM 訊息推播外，亦可自行架設推播伺服器，但此方法需要額外的硬體與通訊成本，另外，也可採用藍牙(Bluetooth)或其他通訊技術完成本機制。

參考文獻

[1] Morris, R., and Thompson, K. “Password security: a case history”, Commun. ACM, 1979, 22, (11), pp. 594–597.

[2] Seeley, D., “Password cracking: a game of wits”, Commun. ACM, 1989, 32, (6), pp. 700–703.

[3] Gait, J., “Easy entry: the password encryption problem”, ACM SIGOPS Oper. Syst. Rev., 1978, 12, (3), pp.54–60.

[4] J. Spitzer, C. Singh, and D. Schweitzer, “A security class project in graphical passwords,” Journal of Computing Sciences in Colleges archive, 2010, 26, pp. 7–13.

[5] S. Chiasson, E. Stobert, A. Forget, R. Biddle, and P.C. van Oorschot, “Persuasive Cued click-points: design, implementation, and evaluation of a knowledge-based authentication mechanism,” IEEE Tans. On Dependable and Secure Computing, 2012, 9, pp. 222–235.

[6] Google play,https://support.google.com/googleplay/android-developer/answer/2663269?hl=zh-Hant.

[7] Wikipedia, https://en.wikipedia.org/wiki/ISO/IEC_27001.

[8] Google Developers, https://developers.google.com/android/c2dm/?hl=zh-TW.

[9] McCune J., Perrig A., and Reiter M., “Seeing-is-believing: using camera phone for human-verifiable authentication,” IEEE Symposium on Security and Privacy, pp. 110-124, 8-11 May, 2005.

[10] Kao, Y.W., Zhang, X., Studer, A., and Perrig, A., “Mobile encryption for laptop data protection (MELP)”, IET Inf. Secur., 2012, 6, (4), pp. 291–298.