以網頁驗證碼為基礎的側錄程式密碼防禦機制

許玉芳[1] 沈慧宇[2] 金馳[3]
建國科技大學[1,3]電子工程系 [2]資訊與網路通訊系
[1]yfshi@cc.ctu.edu.tw , [2]wyshen@ctu.edu.tw, [3]robinpig46@yahoo.com.tw

摘要

傳統上，為防制駭客以側錄程式攻擊原使用者的帳號密碼登入，大部分多採用 OTP – One-Time Password 一次性密碼的保護機制，或軟體式動態鍵盤的輸入方式，以避免攻擊者有效攔截使用者的帳號密碼資料。但是 OTP 的缺點必須在使用者端的電腦內安裝相關的硬體讀卡設備；而動態鍵盤的程式仍存在被攻擊的風險，且往往需要另申請合法憑證。

本文嘗試提出一種全新的密碼登入方式，使用者無須再記住密碼的明文資料，相反的，使用者需記住的是密碼的產生方式，並利用登入驗證碼的亂數產生機制與圖形辨識難度，以防禦本地電腦的側錄程式攻擊，這樣的防禦機制完全不需要額外安裝任何硬體設備或軟體程式，而且每次登入的密碼也會完全不同，換言之，本文所提出的防護方式是更便捷且仍具有 OTP 所擁有一次性密碼的功能。

關鍵詞：側錄程式、動態鍵盤、一次性密碼

Abstract

Traditionally, in order to protect user password from eavesdropping program such as keylogger, One-Time Password (OTP) or software dynamic keyboard is always adopted to prevent password and user name from being intercepted. However, OTP solution needs additional hardware reader installation and software dynamic keyboard exist some exploit risks. Moreover, dynamic keyboard should still need additional requirement for valid certificate.

In this paper, we try to propose a new authentication approach. It is not necessary for user to remember his password context. Instead, user should only keep in mind how password is created. Additionally, in order to enhance the password hacking complexity, the graphical authentication code which varies with login times is inserted to mix with the password generation. In other words, the real password will be dependent on the authentication code. Therefore, the login password must be valid for only one time. Since the login password changes each time automatically, we are convinced that this approach will provide sufficient security for one-time password solution without any software package or hardware device involved.

Keywords: keylogger, dynamic keyboard, one-time password

1. 研究動機與目的

目前網際網路所存在的惡意程式 (Malware) 中，木馬程式可能是最為普遍，因為它可以輕易透過釣魚 (Phishing) 的方式就下載到使用者電腦。很多木馬程式 (Trojan) 往往會包裝側錄程式 (Keylogger) ，側錄程式可以在背景過程讀取使用者所輸入的鍵盤資料，使用者將因此在不知不覺中輸入被攔截的帳號與密碼等相關重要資訊，攻擊者再將所攔截到帳號與密碼等資訊傳送到遠端駭客網站，而這也正是許多網路帳號被盜用日益嚴重的重要原因。

為能解決帳號密碼被盜用的問題，許多網站會提供動態鍵盤的軟體模擬方式以避免觸發敲打實體鍵盤，這個方式確實可以應付許多側錄程式，但是點選動態鍵盤的行為資訊仍可能在網路中被攔截，相關的密碼明文資料還是很可能會被分析出來，因此大部分的動態鍵盤網頁都會搭配 HTTPS [1][2][3]的通訊協定，以建立傳送端與接收端雙方的加密通道。

HTTPS 通訊協定可以建立瀏覽器與伺服器之間的加密通道，主要的基本原理是利用伺服器憑證 (Certificate) 內的公鑰 (Public Key)[4] 來傳遞後續加密與解密所需要的對稱鑰匙 (Session Key)，由於瀏覽器會主動透過憑證授權中心 (CA-Certificate Authority) 來驗證伺服器憑證是否合法，因此透過公鑰所加密傳送的對稱鑰匙將具備合法使用的有效性，換言之，瀏覽器可以依據對稱鑰匙將網路封包轉換為密文，而伺服器則可以利用該對稱鑰匙將相關的密文還原為明文資料，反之亦然。

由於上述 HTTPS 運作原理具有非常完備的理論基礎，而且破解其加解密過程需要很高成本與時間的代價，因此 HTTPS 不僅適用於帳號密碼的登入網頁或會員帳號的申請網頁，也普遍應用於金融銀行或電子商務的資金交易，但是，使用 HTTPS 通訊協定必須申請合法的憑證，若是沒有合法的憑證，瀏覽器會出現伺服器網站可能是偽造的警告網頁，事實上，許多網站基於成本考量，往往都不會申請合法的憑證。

OTP (One-Time Password) [5]是一次性的密碼的技術，密碼使用一次後立即失效，因此也可以用來防禦側錄程式的攻擊，然而，由於使用者需要再加裝相關的讀卡機才可以利用 OTP 的功能，因此，可能也無法全面性推廣。

本文所提出的方法完全異於動態鍵盤與 OTP 的防禦機制，第二節將說明本方法的設計理念；第三節則舉例說明系統運作細節；第四節說明本方法的相關重要特色；最後，本文會針對本論文做一簡要的結論。

2. 設計理念

本文的設計理念與 HTTPS 相近，如下圖 1，HTTPS 主要功能就是建立瀏覽器與伺服器的加密通道，因此，攻擊者無法從網路中攔劫任何有效的資料。一樣的道理，若是使用者與瀏覽器之間存在隨機組合的資料變化，攻擊者自然也無法執行任何側錄的動作。

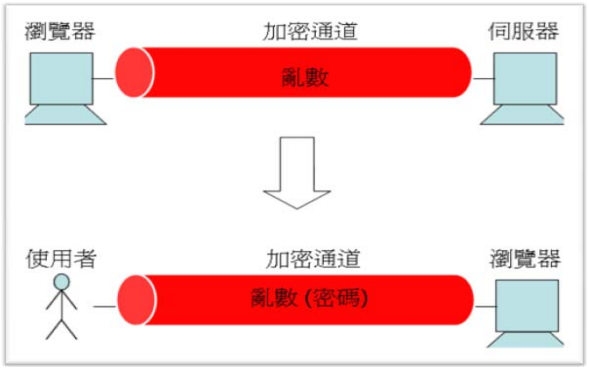

圖 1 可以避免被側錄的加密通道

本文設計方式就是利用網頁驗證碼的隨機明文資料，再透過適當的計算規則，產生密碼的隨機明文資料，密碼內容本身雖然是以明文的方式呈現，其內容卻是數字與文字的隨機組合，下圖 2 代表密碼產生方式運作的示意圖，其中，網頁驗證碼是一隨機的亂數字元，使用者只需要記住適當的計算規則，就可以產生各種不同的密碼。

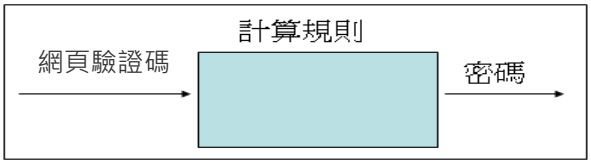

圖 2 登入密碼產生方式

網頁驗證碼主要是以圖形來顯示文字與數字的隨機組合 (如下圖 3 所示)，大部分是應用在帳號密碼的登入網頁或會員帳號的申請網頁，主要目的是用以防止機器程式將大量資料直接輸入網頁的相關欄位，來增加驗證的複雜性，由於大部分機器程式無法判讀以圖形所表示的文字或數字，(除非機器程式本身具備類似 OCR-Optical Character Recognition 光學字元辨識能力)，因此，網頁驗證碼確實可以在前端瀏覽器有效阻擋惡意的機器程式。

圖 3 網頁驗證碼範例

3. 本系統運作

伺服器依據使用者的帳號基本資料決定所要列舉的計算規則，使用者在申請帳號時就必須決定所使用的計算規則，一旦決定相關的計算規則，使用者就必須記住該規則的計算方式。如下圖 4 所示，使用者如果選擇替換式規則，他可以決定右起第 4 個位置要替換為 Z，第 6 個位置要替換為 9；使用者如果選擇循環式規則，他可以決定左移 3 個位置，然後右補 A5C。

在本系統架構中，使用者不再需要記住密碼，使用者只需要記住登入演算法所產生的計算規則，當使用者連線到登入網頁時，登入網頁一樣會出現帳號密碼的輸入欄位，同時也會出現一驗證碼圖示。它與傳統驗證碼不同的是本系統架構的密碼與驗證碼存在一定的計算規則，使用者必須依照記憶中的計算規則與驗證碼一同運算，才可以得出密碼的內容，換言之，使用者不再需要記住密碼，使用者只需要記住登入演算法的計算規則即可。

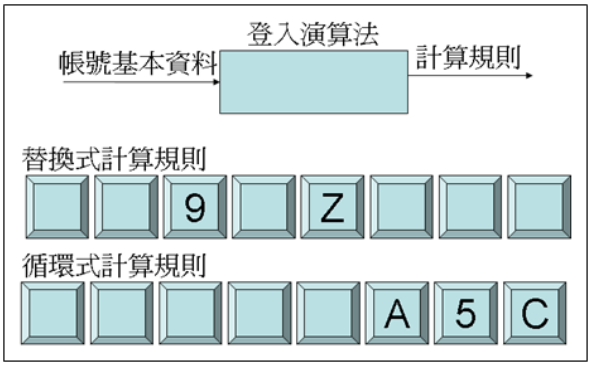

圖 4 計算規則範例

所謂計算規則可能是乘以 2 [*2], 加上 3 [+3], 右起第 3 個字元改為 p [p?3], 右移 2 位且左補 9k [9k>2], 或是左移 1 位且右補 m [1<m] 等類似的規則。

舉例來說，若是登入網頁所出現的驗證碼為 1234，那麼上述計算規則所換算出來的密碼如下。

[*2]	所對應的密碼為 2468，
[+3]	所對應的密碼為 1237，
[p?3]	所對應的密碼為 1p34，
[9k>2]	所對應的密碼為 9k12，
[1<m]	所對應的密碼為 234m。

由於計算規則並沒有任何特別的限制，而且計算規則不會提示於任何網頁內容 (但是使用者與伺服器會記住計算規則)，所以所對應的密碼不僅每一次登入都不相同，而且所對應的密碼也可以展現相當高的亂度 (因為驗證碼本身就是亂數產生器所建立)。

由於伺服器會記住使用者自由定義的驗證碼與計算規則，因此雙方一定都可以驗證密碼的正確性。

本系統實作範例介面如下圖所示，其中圖 5 代表系統登入畫面，每次登入的密碼內容都與驗證碼有關聯性，因此，密碼內容只有一次有效性。

圖 5 系統登入介面

另外，圖 6 是申請新帳號時所定義的密碼產生方式，使用者必須記住自己所勾選的密碼產生方式，依據驗證碼字元內容執行位移、取代或交換的字元操作運算以產生動態的密碼內容。由於每次登入系統時驗證碼都不會一樣，密碼的明碼內容也會隨之改變，因此，使用者無須記住密碼的明碼內容 ，僅須記住密碼的產生方式。

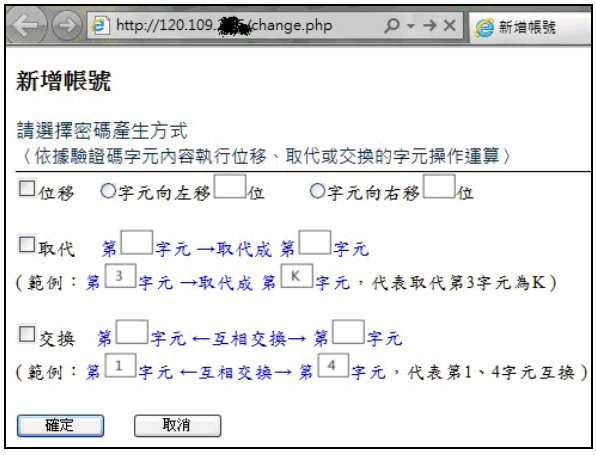

圖 6 密碼產生方式操作介面

4. 本系統特色

(1) 網路攔截密碼的安全強度高

本文提出的方法所產生的密碼是以明文的方式在網路上傳送，由於每次登入的密碼都不相同，所以即便攻擊者攔截相關的密碼資料也無法使用。但是，以明文方式表現的密碼可以被進一步分析，因為攻擊者會希望了解登入演算法的計算規則，然而，這一部份的分析過程還需要再搭配使用者的驗證碼規則，而驗證碼是以圖形的方式隨機呈現數字與文字的組合，因此破解的難度將大幅提高，而這也正是本文採用驗證碼的主要原因。

(2) 密碼方便性

本文所提出的密碼運作機制有別於傳統的密碼記憶方式，傳統上，使用者所背記的是密碼明文資料，然而，在本文所介紹的方式中，使用者需要記憶的卻是密碼明文的產生方式，密碼長度越長，就越能顯示出我們所提供的方法的方便性，事實上，以 15 個字元長度的密碼明文資料為例，若是採用 [+3] 的計算規則，使用者僅需記住 +3 這樣的規則即可。

(3) 本地攔截密碼的防禦入侵度高

即便攻擊者以側錄程式攔截使用者與瀏覽器之間所輸入的密碼資料，甚至以類似 OCR 的方式判讀驗證碼的內容，攻擊者依然無法入侵使用者的登入網頁，因為輸入演算法所產生的每一種計算規則都具有很高的變化性，入侵難度相對非常高。

(4) 一次性有效的密碼

本方式所提出的登入方式具有非常特殊的意義，尤其當伺服器主機受到某種程度的入侵時 (例如攻擊者可以利用 injection 的方式取得網頁內容的控制權，但是由於存取管控的機制，卻仍無法取得 root 管理者的密碼)，使用者瀏覽器所呈現的動態鍵盤網頁有可能是攻擊者所偽造的，攻擊者處心積慮希望能在伺服器端攔截到使用者的帳號密碼資料 ，但是，就如同前文所述，攻擊者所取得的仍屬一次性有效的密碼，因而無法以使用者的帳號執行入侵動作。

5. 結論

本文所建議的驗證系統方式不僅不需要額外安裝任何軟體或硬體，每次所產生的登入密碼也完全不同。此外，計算規則雖然簡易，卻容易記憶，如果再將日期或特殊紀念日等相關變數考慮進去，不僅依然有方便記憶的特性，同時也大幅提高其複雜度。

本系統的使用最大的改變是在於密碼的記憶方式，如果不必去記憶密碼的明文，改而從原始基礎去記憶密碼的產生方式，瀏覽器與使用者之間所傳遞的輸入資料就可以呈現亂數的組合，因此可以免除被攻擊者側錄到原始密碼的明文資料。

參考文獻

[1] RFC 2818, “HTTP over TLS”.

[2] Rescorla, E. SSL and TLS: Designing and Building Secure System. Reading, MA: Addison-Wesley, 2001.

[3] Cormen, T; Leiserson, C; Rivest, R; and Stein, C, “Introduction to Algorithm”, Cambridge, MA: MIT Press, 2001.

[4] RFC 2459, “Internet X.509 Public Key Infrastructure Certificate and CRL Profile”.

[5] RFC 2289, “A One-Time Password System”.