Regular Paper

Communications of the CCISA
Vol. 29 No. 1 Feb. 2023

以一次性密碼為基礎的雙因素身份驗證應用程式之即時網路釣魚攻擊防禦能力的分析與強化

吳星旻[1]、顧維祺[2*]、余傳欣[3]
[1,2,3]國立臺中教育大學資訊工程學系
[1]acs106106@gm.ntcu.edu.tw、[2]wcku@mail.ntcu.edu.tw、[3]a0910415754@gmail.com

摘要

由於傳統使用單一固定密碼的身份驗證系統難以防禦字典攻擊、肩窺攻擊、竊聽攻擊、間諜程式攻擊以及網路釣魚攻擊，所以有許多以一次性密碼為基礎的雙因素驗證(2FA) 系統被提出。然而，雖然這些以一次性密碼為基礎的 2FA 驗證系統對於一般的網路釣魚攻擊有基本的防禦能力，但是對於進階的即時網路釣魚攻擊之防禦能力則仍有所不足。近年來，即時網路釣魚攻擊對於以一次性密碼為基礎的 2FA 驗證系統的威脅與日俱增，網路釣魚攻擊相關的資安事件頻傳，攻擊者可使用各類型的即時網路釣魚攻擊工具突破以一次性密碼為基礎的 2FA 驗證系統的防線。在本論文中，我們首先評析包括 Aegis Authenticator、Google Authenticator、Microsoft Authenticator、andOTP 與 Bitwarden 等五套目前較常見的以一次性密碼為基礎之 2FA 應用程式，除了分析其一般安全性與使用性之外，並特別分析其對於即時網路釣魚攻擊的防禦力。接著，我們根據綜合評析結果選擇其中整體安全性較高的 Bitwarden 為基底，植入我們所提出的 URI 設定之安全檢查機制以及 URI 即時比對機制，以強化系統對於即時網路釣魚攻擊的防禦能力。

關鍵詞：身份驗證、一次性密碼、即時網路釣魚攻擊、雙因素驗證

* 通訊作者 (Corresponding author.)

Regular Paper

Communications of the CCISA
Vol. 29 No. 1 Feb. 2023

Analysis and Improvements of Real-Time Phishing Resilience for Two-Factor Authentication Apps Based on One-Time Passwords

Xing-Min Wu[1], Wei-Chi Ku[2*], Chuan-Hsin Yu[3]
[1,2,3]Department of Computer Science, National Taichung University of Education
[1]acs106106@gm.ntcu.edu.tw, [2] wcku@mail.ntcu.edu.tw, [3]a0910415754@gmail.com

Abstract

Traditional authentication systems based on fixed passwords are vulnerable to dictionary attacks, shoulder surfing attacks, eavesdropping attacks, spyware attacks, and phishing attacks. Therefore, many two-factor authentication (2FA) systems based on one-time passwords have been proposed. Although these 2FA systems based on one-time passwords can resist common phishing attacks, they still lack strong defensive capabilities against real-time phishing attacks, in which attackers can use various types of real-time phishing tools to break through the defenses of 2FA systems based on one-time passwords. In recent years, as the threats of real-time phishing attacks against 2FA systems based on one-time passwords increase significantly, security events related to real-time phishing attacks occur frequently. In this paper, we first analyze the general security strength and usability of the five most popular 2FA apps based on one-time passwords, including Aegis Authenticator, Google Authenticator, Microsoft Authenticator, andOTP, and Bitwarden. In particular, we also analyze their resiliencies to real-time phishing attacks. According to the comprehensive comparison results, we select Bitwarden, which has higher overall security, as the base app to embed our proposed security improvement mechanisms, including the security check mechanism for URI setting and the instant URI comparison mechanism, to enhance the system's resilience to real-time phishing attacks.

Keywords: Authentication, One-Time Password, Real-Time Phishing Attack, Two-Factor Authentication

壹、前言

用戶身份驗證 (User Authentication) 作為多數資訊系統在安全性上的第一道防線，其重要性不言而喻。用戶身份驗證程序通常藉由驗證用戶所知道的事、所持有之物或是本身所具備之特徵以確認其身份的真實性，因此用戶身份驗證技術依其運用之身份驗證因素 (Authentication Factor) 可區分為以下三種類型：

- 知識 (Knowledge) 因素：用戶所知之資訊，例如：用戶帳號 (Account) 及密碼 (Password)、通行密碼片語 (Passphrase)、PIN (Personal Identification Number) 等。
- 持有 (Ownership) 因素：用戶所持有之物品，例如：銀行卡、智慧卡、晶片卡、USB 鑰匙、動態密碼產生器、智慧型手機等。
- 固有 (Inherence) 因素：用戶與生俱來的之生物特徵或行為 (Biometrics)，例如：指紋 (Fingerprint)、虹膜 (Iris)、臉型 (Face)、掌紋 (Hand Geometry)、語音 (Voice) 等生物辨識 (Biometrics)。

在諸多身份驗證因素中，密碼 (Password；或稱作 “通行碼”) 具有易於部屬、低成本及方便使用等優點且無生物特徵有侵犯隱私之疑慮與不易更換等缺點，因此至今仍是大多數用戶身份驗證系統普遍採用的身份驗證因素。然而，一般的用戶密碼對於字典攻擊的防禦能力較弱，而且傳統的密碼驗證系統多無法防禦肩窺攻擊 (Shoulder-Surfing Attack)、竊聽攻擊 (Wiretapping Attack) 與間諜程式攻擊 (Spyware Attack) 等擷取攻擊 (Capture Attacks) [23] 以及網路釣魚攻擊 (Phishing Attacks) 攻擊 [3][6][19]。攻擊者一旦藉由字典攻擊、擷取攻擊或網路釣魚攻擊得到用戶的密碼後便可假冒用戶登入網站，並可能藉以進行更複雜且影響更廣泛的攻擊。另一方面，由於一般用戶為了使用上的方便而習慣在多個網站使用相同的密碼，若其中一個網站的密碼洩漏，則可能導致該用戶在其它網站的帳號也有被盜用的風險。

有鑑於使用單一固定密碼作為身份驗證因素有上述的安全問題，因此有許多不同類型的身份驗證方法被提出，例如結合了任意兩種身份驗證因素的雙因素驗證 (2FA；Two-Factor Authentication) 機制以及無密碼驗證 (Passwordless Authentication) 機制。2FA 機制提供用戶較強的帳號安全防護，攻擊者除了須得到帳號密碼以通過第一階段的身份驗證之外，還須設法通過第二階段的身份驗證才能駭入該帳戶，因此 2FA 可提高對字典攻擊、擷取攻擊以及網路釣魚攻擊的防禦能力 [22]。無密碼驗證機制則可以 FIDO (Fast IDentity Online) 聯盟與全球資訊網協會 (World Wide Web Consortium；W3C) 共同制定的 FIDO2 標準 [14] 為代表，FIDO2 運用公鑰密碼學 (Public-Key Cryptography) 技術為基礎以避免傳統密碼身份驗證系統所遭遇的各種風險並大幅提升對於網路釣魚攻擊的防禦能力，而 Google、Microsoft 與 Apple 並於 2022 年 5 月 5 日共同宣布 [13] 未來將積極擴大支援 FIDO2。然而，由於目前並非所有平台與裝置都支援 FIDO2，部分設備可能無法使用，意即用戶可能需要購買特定的設備或軟體，從而增加了使用成本，FIDO2 無密碼驗證系統在短期內仍難以普及。此外，即使在未來 FIDO2 無密碼驗證系統逐漸普

及之後，2FA 機制仍可作為不適用 FIDO2 無密碼驗證系統的環境或特定應用之另一個身份驗證機制的選項，2FA 機制未來仍有其實用價值。

在眾多 2FA 驗證系統中 [30]，以一次性密碼 (One-Time Password；OTP) [21][26][27] 為基礎的 2FA 驗證系統因其較低的硬體需求與易用性，已成為現今最常見與廣泛使用的 2FA 驗證系統，目前市面上已有許多以一次性密碼為基礎的 2FA 應用程式，例如：Aegis Authenticator [2]、LastPass Authenticator [24]、Google Authenticator [17]、andOTP [5]、Twilio Authy [7]、Duo Mobile [12]、2FA Authenticator [1]、FreeOTP [15]、TOTP Authenticator [33]、Microsoft Authenticator [25]、SAASPASS [29] 以及 Bitwarden [8] 等。然而，雖然以一次性密碼為基礎的 2FA 驗證系統對於一般的網路釣魚攻擊具備基本的防禦能力 [22]，但是對於進階的即時網路釣魚攻擊 (Real-Time Phishing Attacks) 之防禦能力則仍有所不足，攻擊者可藉由即時網路釣魚攻擊偽裝合法用戶繞過系統的 2FA 驗證機制，誘騙用戶在釣魚網站上輸入帳號密碼與 OTP 等身份驗證訊息後即時利用此捕獲的資訊非法登入網站。近年來，即時網路釣魚攻擊對於以一次性密碼為基礎的 2FA 驗證系統的威脅與日俱增，直接或間接相關的資安事件頻傳，因此，以一次性密碼為基礎的 2FA 驗證系統之即時網路釣魚攻擊防禦能力的強化仍有其必要性。

在本論文中，我們首先評析 Google Authenticator、Aegis Authenticator、andOTP、Microsoft Authenticator 與 Bitwarden 等五套目前較常見的以一次性密碼為基礎的 2FA 應用程式，除了分析其一般安全性與使用性之外，並特別分析其即時網路釣魚攻擊的防禦力。接著，我們根據綜合評析結果選擇其中整體安全性較強的 Bitwarden 為 2FA 應用程式基底，植入我們所提出的 URI 設定之安全檢查機制以及 URI 即時比對機制等兩項強化機制，以強化系統對於即時網路釣魚攻擊的防禦能力。

貳、相關研究

在本節中，我們將分別簡介與本論文相關的研究—以一次性密碼 (One-Time Password；OTP) 為基礎的雙因素身份驗證 (Two-Factor Authentication) 以及即時網路釣魚攻擊 (Real-Time Phishing Attacks)。

2.1 以一次性密碼為基礎的雙因素驗證

雙因素驗證 (2FA；Two-Factor Authentication) 為結合任兩種身份驗證因素的身份驗證機制，可提供用戶較強的帳號安全防護，降低字典攻擊、擷取攻擊以及網路釣魚攻擊的威脅。如前一節所述，以一次性密碼 (One-Time Password；OTP) [21][26][27] 為基礎的 2FA 驗證系統為目前最普遍、最常見的 2FA 驗證系統。以一次性密碼為基礎的 2FA 驗證系統用戶除了需要輸入一般固定密碼之外，還需要輸入一次性密碼。因此，即使攻

擊者竊取了用戶的固定密碼也無法登入。常見的以一次性密碼為基礎之 2FA 機制主要是利用簡訊、電子郵件或 2FA 驗證器 (Authenticator) 讓合法用戶取得並輸入一次性密碼 (One-Time Password；OTP) 來通過第二階段的驗證。早期的 2FA 驗證器多使用專門的 2FA 硬體 Token 儲存金鑰以產生 OTP 供用戶通過 2FA 驗證，成本較高且較不方便。近年來，由於智慧型行動裝置的普及，軟體 Token 型式的 2FA 應用程式 (2FA App) 逐漸成為 2FA 驗證器的主流，用戶只需在智慧型行動裝置上安裝 2FA 應用程式並設定金鑰便可隨時隨地產生 OTP 供用戶通過 2FA 驗證。現今，大部分的大型服務提供商 (包括 Google、Microsoft 和 Facebook 等) 都支援使用 2FA 應用程式作為登入系統時的身份驗證方式以強化帳號的安全性。

2.2 即時網路釣魚攻擊

即時網路釣魚攻擊 (Real-Time Phishing Attacks) 為一種運用中間人攻擊 (Man-in-the-Middle Attack ; MITM) 模式的進階型網路釣魚攻擊，攻擊者藉由各種手段誘騙用戶在釣魚網站上輸入帳號密碼與 OTP 等用戶身份驗證訊息後即時利用此身份驗證訊息於 OTP 有效期限內假冒用戶登入合法網站 [11]。傳統的以簡訊或電子郵件傳遞的 OTP 有效期限通常設定為 3 至 10 分鐘，若用戶被誘騙至釣魚網站上輸入包含 OTP 在內的身份驗證資訊，則攻擊者通常有充足的時間運用此身份驗證資訊假冒該用戶登入合法網站，意即以簡訊或電子郵件傳遞 OTP 的方法對於即時網路釣魚攻擊的防禦力不足。雖然現有以一次性密碼為基礎的 2FA 應用程式藉由大幅縮減 OTP 的有效期限 (通常為 30 秒) 以降低一般網路釣魚攻擊的成功機會，但攻擊者仍可輕易地藉由具有即時功能的網路釣魚工具 (例如：Evilginx2 與 Modlishka) [16] 讓釣魚網站成為攻擊者與合法網站之間的中繼站以進行即時性的網路釣魚攻擊，用戶一旦在釣魚網站上輸入包含 OTP 在內的身份驗證資訊後，此類網路釣魚工具可擷取身份驗證資訊與 Session Cookie 以讓攻擊者假冒用戶登入合法網站，意即此類網路釣魚工具可有效增加即時網路釣魚攻擊對於現有以一次性密碼為基礎之 2FA 應用程式的攻擊成功率。根據 O'Reilly [28] 在 2021 年於 SlashNext 所發表的研究報告指出，目前已經有多種類型的即時性網路釣魚技術與工具被發展出來，使得即時網路釣魚攻擊對於以一次性密碼為基礎的 2FA 應用程式的威脅與日俱增，所產生的資安問題比過去更為嚴重 [10][20][31][32][34]。

參、以一次性密碼為基礎的 2FA 應用程式之評析與比較

現有以一次性密碼為基礎的 2FA 應用程式大致上可分為兩類 [35]：(1) 獨立的 2FA 應用程式 (Standalone 2FA Apps)；(2) 整合 2FA 與密碼管理器 (Password Managers) 的應用程式。在獨立的 2FA 應用程式中，用戶必需額外安裝獨立的應用程式，將所有的

OTP 金鑰保存其中，當用戶送出帳號密碼並收到驗證請求後，至 2FA 應用程式查看並輸入對應的 OTP 後即完成驗證程序，這類型的應用程式包含 Aegis Authenticator [2]、LastPass Authenticator [24]、Google Authenticator [17]、andOTP [5]、Twilio Authy [7]、Duo Mobile [12]、2FA Authenticator [1]、FreeOTP [15] 以及 TOTP Authenticator [33]。而對於有使用密碼管理器的用戶來說，為了方便管理，整合 2FA 功能的密碼管理器無疑是最佳選擇，不需安裝額外的應用程式即可使用兩種功能，這類型的應用程式包含 Microsoft Authenticator [25]、SAASPASS [29] 以及 Bitwarden [8]。根據 AlternativateTo [4] 網站上之 2FA 應用程式的排名結果，我們從中挑選出較常見且綜合評比較高的五套以一次性密碼為基礎的 2FA 應用程式 — Aegis Authenticator [2]、Google Authenticator [17]、Microsoft Authenticator [25]、andOTP [5] 與 Bitwarden [8] 做安全性與使用性的評析並作綜合比較。

3.1 Aegis Authenticator 的評析

Aegis Authenticator [2] 是一套免費且開源的以一次性密碼為基礎之 2FA 應用程式 (操作畫面請參見 (圖 1))，支援密碼和指紋保護應用程式、自定義圖示、OTP 分組、匯入匯出和本地備份。Aegis 有三種添加雙因素驗證的方式，包括 QR-code (Quick Response code)、圖片及手動輸入。在手動輸入雙因素驗證時，可以選擇 OTP 的類型 (TOTP [27]、HOTP [26]、Steam)、雜湊函數類型 (SHA1、SHA256、SHA512)、OTP 有效週期及 OTP 位數。Aegis 的設置頁面還包含其它功能，包括外觀設定、群組分類、防止螢幕截圖、隱藏驗證碼、加密資料庫、自動鎖定應用程式，可從其它 Authenticator 匯入 OTP (需 root) 以及設定在緊急狀況時可刪除資料庫。不過，Aegis Authenticator 並沒有支援 Android 以外平臺的版本。此外，針對即時網路釣魚攻擊的防禦力方面，由於系統不提供登入網站的網址設定與安全性檢查，也未提供網址的即時安全性比對，難以防止攻擊者藉由網路釣魚攻擊竊取 OTP，故 Aegis Authenticator 不具備良好的即時網路釣魚攻擊防禦能力。

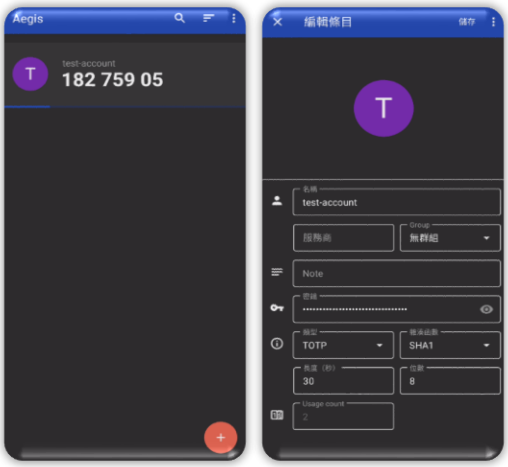

圖 1：Aegis Authenticator 的操作畫面

3.2 Google Authenticator 的評析

Google Authenticator [17] 是 Google 提供的以一次性密碼為基礎之 2FA 應用程式 (操作畫面請參見 (圖 2))，支援 Android、iOS 系統以及瀏覽器擴充套件，但僅限在 iOS 上可以 Face ID 保護應用程式。Google Authenticator 使用簡易的介面及功能讓一般用戶也能快速上手，提供 QR-code 及手動輸入兩種添加雙因素驗證的方式與兩種 OTP 類型 (TOTP、HOTP)，還提供方便的資料轉移功能，用戶可將舊裝置中的資料以 QR-code 的方式匯出並使用新裝置掃描後匯入。不過，其方便簡單的特性也降低了本身的安全性。此外，針對即時網路釣魚攻擊的防禦力方面，由於 Google Authenticator 不提供登入網站的網址設定與安全性檢查，也未提供網址的即時安全性比對，難以防止攻擊者藉由網路釣魚攻擊竊取 OTP，故 Google Authenticator 不具備良好的即時網路釣魚攻擊防禦能力。

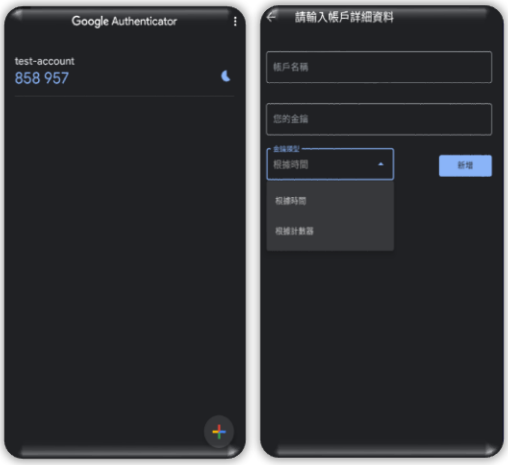

圖 2：Google Authenticator 的操作畫面

3.3 Microsoft Authenticator 的評析

Microsoft Authenticator [25] 為微軟提供的一套免費且整合以一次性密碼為基礎的 2FA 與密碼管理器的應用程式 (操作畫面請參見 (圖 3))，提供密碼和指紋保護應用程式，並支援 Android 及 iOS 平臺，除了具備產生 OTP 的功能之外，也能管理密碼。另外，微軟的無密碼 (Passwordless) 登入，讓用戶可以完全移除傳統密碼，透過 Microsoft Authenticator 來登入微軟帳戶，幫助用戶省去設定、更改密碼的步驟，並避免可能發生的密碼問題，增強安全性。Microsoft Authenticator 還內建雲端備份功能，未來在轉移或復原資料時會更方便，也能避免更換裝置後沒有驗證碼無法登入或必須重新建立帳戶的問題。然而，針對即時網路釣魚攻擊的防禦力方面，由於 Microsoft Authenticator 不提供登入網站的網址設定與安全性檢查，也未提供網址的即時安全性比對，難以防止攻擊者藉網路釣魚攻擊竊取 OTP，故 Microsoft Authenticator 並不具備良好的即時網路釣魚攻

擊防禦能力。

圖 3：Microsoft Authenticator 的操作畫面

3.4 andOTP 的評析

andOTP [5] 是一套免費且開源的以一次性密碼為基礎之 2FA 應用程式 (操作畫面請參見 (圖 4))，支援密碼和指紋保護應用程式、自定圖示、標籤分組和本地備份，andOTP 可以使用 QR-code、圖片及手動輸入作為添加雙因素驗證的方式。手動輸入時，可以選擇 OTP 的類型 (TOTP、HOTP、MOTP、Steam)、雜湊函數類型 (SHA1、SHA256、SHA512)、OTP 有效週期及 OTP 的位數。andOTP 的設置頁面還包含其它功能，包括介面設置、自動鎖定、防止螢幕截圖，以及設定在緊急狀況時可以刪除資料庫。不過，與 Aegis 相似，andOTP 除了 Android 之外目前並沒有提供支援其它系統的版本。此外，針對即時網路釣魚攻擊的防禦力方面，由於 andOTP 不提供登入網站的網址設定與安全性檢查，也未提供網址的即時安全性比對，難以防止攻擊者藉由網路釣魚攻擊竊取 OTP，故 andOTP 並不具備良好的即時網路釣魚攻擊防禦能力。

圖 4：andOTP 的操作畫面

3.5 Bitwarden 的評析

Bitwarden [8] 是一套免費、開源且整合以一次性密碼為基礎的 2FA 與密碼管理器的應用程式 (操作畫面請參見 (圖 5))，用戶可在加密資料庫中保存各種重要資訊 (例如：密碼、信用卡及個人資料)，提供多平臺的應用程式，支援密碼和指紋保護應用程式，並支援包括 Android、iOS、網頁版及瀏覽器擴充套件。Bitwarden 還支援自動填入 (Autofill) 功能，用戶可以對每一組帳密設定多組自定的 URI (Uniform Resource Identifier；統一資源標識符)，用戶在新增密碼時，可以決定這組密碼在自動填入時登入網站的網址必須符合設定的 URI 比對規則 [9]，藉此降低網路釣魚攻擊 (Phishing Attacks) 的成功機會。另外，在付費版本中，Bitwarden 還提供了 OTP 自動填入的功能，用戶在新增密碼時，可針對支援 2FA 的網站設定一組對應的金鑰。用戶在登入時，系統會利用此金鑰產生 OTP 以供用戶用以通過網站的 2FA 驗證。針對即時網路釣魚攻擊的防禦力方面，當用戶啟用 OTP 自動填入功能時，系統會先自動檢查登入網站的網址，只有當此網址符合所設定 URI 及其比對規則時，系統才會即時自動填入 OTP。除了可減少 OTP 遭遇擷取攻擊 [23] 而洩漏的風險，並具備一定程度的即時網路釣魚攻擊防禦能力。然而，在 URI 設定時未做安全性檢查，可能導致用戶將釣魚網站設為信任網址而不自知，而讓攻擊者得逞。此外，若用戶跨平台使用 OTP 或未啟用 OTP 自動填入功能時，Bitwarden 將不能防禦針對竊取 OTP 的擷取攻擊與即時網路釣魚攻擊。因此，Bitwarden 整體的即時網路釣魚攻擊防禦能力仍有改進的空間。

圖 5：Bitwarden 的操作畫面

3.6 綜合比較

我們將 Google Authenticator、Aegis Authenticator、andOTP、Microsoft Authenticator 與 Bitwarden 等五套常見的以一次性密碼為基礎之 2FA 應用程式的綜合比較結果彙整於

(表 1)。其中，除了 Google Authenticator 外，都提供 2FA 應用程式保護機制，並且都禁止螢幕截圖，提供用戶第一層的保護。Google Authenticator [17] 功能較少、操作簡單，即使是不熟悉雙因素驗證的用戶也能夠快速上手，應用程式支援 Android 及 iOS 兩大平臺，也可以在瀏覽器中的擴充套件中使用此功能。Aegis Authenticator [2] 與 andOTP [5] 功能相近，兩者較 Google Authenticator 有更高的自由度及更完整的功能，包含每個 OTP 的自定義圖示、OTP 的標籤分類及排序方式，還提供多種介面設置，且在資料匯出時可讓用戶選擇是否加密資料以防外洩，功能較為複雜，適合熟悉基本 2FA 操作且需要 2FA 進階功能的用戶使用，不過應用程式目前只提供 Android 用戶使用。Microsoft Authenticator [25] 與 Bitwarden [8] 的自由度雖然比不上前三套以一次性密碼為基礎的 2FA 應用程式，但由於結合密碼管理器，除了具備原本的雙因素驗證功能外，還能夠管理各種密碼、付款資訊以及用戶資料，並且可以透過雲端進行資料同步，即使隨身裝置遺失了也能夠復原，除了支援 Android 及 iOS 兩大平臺，也可以在瀏覽器中的擴充套件中使用。不過，Microsoft Authenticator 在 Android 及 iOS 的備份/同步系統是不兼容的，轉換平臺必須重新輸入所有資料。而 Bitwarden 除了可以讓用戶設置多組 URI 及多種比對模式外，在付費版中還提供 OTP 自動填入的功能，與另外四套 2FA 應用程式相比，Bitwarden 有較好的即時網路釣魚攻擊防禦能力，不過，若用戶跨平台使用 OTP 或未啟用 OTP 自動填入功能時則失去即時網路釣魚攻擊的防禦能力。

表 1：五套較常見的以一次性密碼為基礎之 2FA 應用程式的綜合比較表

2FA Apps / 功能比較		Aegis Authenticator	Google Authenticator	Microsoft Authenticator	andOTP	Bitwarden
應用程式保護		✓	✓	✓	✓	✓
禁止截圖		✓	✓	✓	✓	✓
備份	本地	✓	✓	×	✓	×
	雲端	×	×	✓	×	✓
自定OTP模式		✓	✓	×	✓	×
結合 Password Manager		×	×	✓	×	✓
平台		Android	Android、iOS、Browser	Android、iOS、Browser	Android	Android、iOS、Browser
開源		✓	✓(舊版)	×	✓	✓(OTP為付費版)
即時網路釣魚抵擋能力		低	低	低	低	中

肆、2FA 應用程式之網路釣魚攻擊防禦能力的強化

在本節中，我們將針對現有以一次性密碼為基礎的 2FA 應用程式中整體安全性較強的 Bitwarden [8] 作為改進對象，增加兩項安全機制—URI 設定之安全檢查機制與 URI 即時比對機制，藉以進一步強化其即時網路釣魚攻擊的防禦能力。

4.1 URI 設定之安全檢查機制

由於 Bitwarden 用戶在一開始設定 URI (Uniform Resource Identifier；統一資源標識符) 時並未對其進行安全性檢測，若用戶誤將釣魚網站的網址設定為信任網址則後果不堪設想。因此，我們增加用戶在設定 URI 時的安全性檢查以確保其為安全網址。我們使用的方法為透過 Google Safe Browsing [18]，在用戶添加 URI 時進行安全性檢查並顯示網址是否安全，再由用戶自行決定是否設置此 URI。此安全檢查機制搭配 URI 即時比對機制可有效提升對即時網路釣魚攻擊的防禦能力。

4.2 URI 即時比對機制

當以一次性密碼為基礎的 2FA 應用程式所在的裝置即為登入裝置時，則無論用戶是否開啟 OTP 自動填入功能，均強制根據用戶所設置之 URI 並依照 Bitwarden 的三種 URI 比對模式 [8][9] (包括：[Exact] Mode、[Start With] Mode 以及[Host] Mode) 判斷登入網站 URI 的可信賴等級 (Trust Level)，依序處理：(T1) 若符合 [Exact] Mode 的比對，則系統顯示 “高可信賴度”；(T2) 若符合 [Start With] Mode 的比對，則系統顯示 “中可信賴度”；(T3) 若符合 [Host] Mode 的比對，則系統顯示 “低可信賴度”； (T4) 其它情形則系統顯示 “不可信賴”。若符合 T1 或 T2 或 T3 時，當 OTP 自動填入功能為開啟時，系統將提示用戶是否送出 OTP 並執行其回應的命令；否則當 OTP 自動填入功能為關閉時，系統將顯示 OTP 並由用戶自行決定是否在登入網站手動輸入 OTP。當以一次性密碼為基礎的 2FA 應用程式所在的裝置與登入裝置不相同時，則此跨裝置身份驗證不提供 OTP 自動填入功能，用戶需先將跨裝置瀏覽器中登入頁面網址轉換成二維條碼 (Quick Response code；QR-code)，並使用內建的二維碼掃描器將此 QR-code 轉換成登入網站 URI。接著，系統同樣將強制根據用戶所設置之 URI 並根據 Bitwarden 的三種 URI 比對模式 [8][9] 來判斷登入網站 URI 的可信賴等級 (Trust Level)，依序處理：(T1) 若符合 [Exact] Mode 的比對，則系統顯示 “高可信賴度”；(T2) 若符合 [Start With] Mode 的比

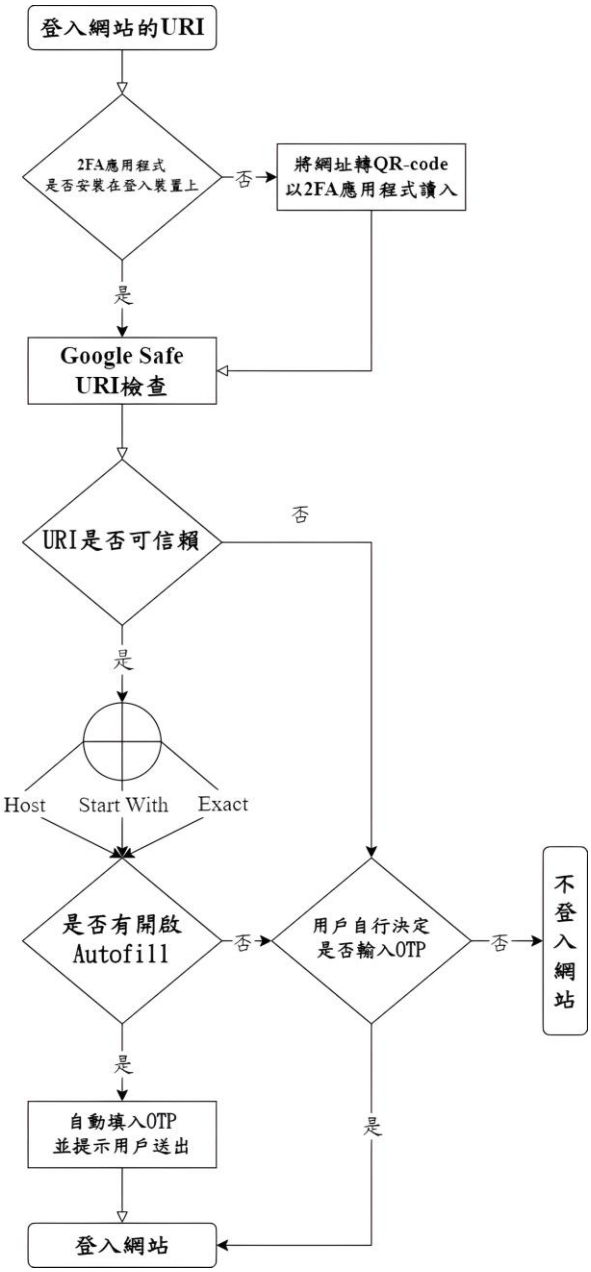

圖 6：URI 即時比對機制的處理流程

對，則系統顯示 “中可信賴度”；(T3) 若符合 [Host] Mode 的比對，則系統顯示 “低可信賴度”； (T4) 其它情形則系統顯示 “不可信賴”。若符合 T1 或 T2 或 T3，系統將顯示 OTP 並由用戶自行決定是否在登入網站手動輸入 OTP，URI 即時比對機制的處理流程請參見 (圖 6)。

伍、結論

即時網路釣魚攻擊對於以一次性密碼為基礎的 2FA 驗證機制的威脅與日俱增，攻擊者可使用現成的即時網路釣魚攻擊工具輕易突破以一次性密碼為基礎的 2FA 驗證機制的防禦。在本論文中，我們首先評析 Google Authenticator、Aegis Authenticator、andOTP、Microsoft Authenticator 與 Bitwarden 等五套目前較常見的以一次性密碼為基礎之 2FA 應用程式，並特別針對即時網路釣魚攻擊的防禦力作分析與綜合比較。接著，我們挑選其中具備較強即時網路釣魚攻擊防禦力的 Bitwarden 作進一步的安全性強化，我們提出設定 URI 時之安全性檢測機制以及 URI 即時比對機制。其中，在用戶設定 URI 時即利用 Google Safe Browsing 對網址進行安全性檢查，確保該網站為合法網站。而在用戶需要以 OTP 登入網站時，系統根據先前設定之 URI 自動判斷目前擬登入網站的可信賴等級並作對應的 OTP 控管，可降低用戶被釣魚網站騙取 OTP 的機會。我們所提出的強化機制可有效提升以一次性密碼為基礎的 2FA 應用程式對於即時網路釣魚攻擊的防禦能力。

參考文獻

[1] 2FA Authenticator. <https://2fas.com/> (Accessed: Jan. 15, 2023)

[2] Aegis Authenticator. <https://github.com/beemdevelopment/Aegis> (Accessed: Jan. 15, 2023)

[3] A. Aleroud and L. Zhou, “Phishing Environments, Techniques, and Countermeasures: A Survey,” *Computers & Security*, Vol. 68, pp. 160-196, 2017.

[4] AlternativateTo Authenticator APP. <https://alternativeto.net/tag/authenticator-app> (Accessed: Jan. 15, 2023)

[5] andOTP. <https://github.com/andOTP/andOTP> (Accessed: Jan. 15, 2023)

[6] APWG: Phishing Activity Trends Report, 4th Quarter 2021, Technical Report, Feb.2022.

[7] Twilio Authy. <https://authy.com/features/> (Accessed: Jan. 15, 2023)

[8] Bitwarden. <https://bitwarden.com> (Accessed: Jan. 15, 2023)

[9] Bitwarden: Using URIs. <https://bitwarden.com/help/uri-match-detection/> (Accessed: Jan. 15, 2023)

[10] B. Kondracki, B. A. Azad, O. Starov, and N. Nikiforakis, “Catching Transparent Phish: Analyzing and Detecting MITM Phishing Toolkits,” *Proceedings of the 2021 ACM SIGSAC Conference on Computer and Communications Security*, pp. 36-50, 2021.

[11] M. Boodaei, “Real-Time Phishing Takes Off,” Security Intelligence, Nov. 2010. <https://securityintelligence.com/real-time-phishing-takes-off/> (Accessed: Jan. 15, 2023)

[12] Duo Mobile. <https://duo.com/product/multi-factor-authentication-mfa/duo-mobile-app> (Accessed: Jan. 15, 2023)

[13] FIDO Alliance: Apple, Google and Microsoft Commit to Expanded Support for FIDO Standard to Accelerate Availability of Passwordless Sign-Ins. <https://fidoalliance.org/-apple-google-and-microsoft-commit-to-expanded-support-for-fido-standard-to-accelera-te-availability-of-passwordless-sign-ins/> (Accessed: Jan. 15, 2023)

[14] FIDO Alliance: FIDO Authentication. <https://fidoalliance.org/fido2/> (Accessed: Jan. 15, 2023)

[15] FreeOTP. <https://freeotp.github.io> (Accessed: Jan. 15, 2023)

[16] P. Gadient, P. Gerig, O. Nierstrasz, and M. Ghafari, "Phish What You Wish," *2021 IEEE 21st International Conference on Software Quality, Reliability and Security (QRS)*, 2021, pp. 1048-1059.

[17] Google Authenticator. <https://play.google.com/store/apps/details?id=com.google.android.apps.authenticator2> (Accessed: Jan. 15, 2023)

[18] Google Safe Browsing. <https://safebrowsing.google.com> (Accessed: Jan. 15, 2023)

[19] B. B. Gupta, N. A. G. Arachchilage, and K. E. Psannis, "Defending against Phishing Attack: Taxonomy of Methods, Current Issues and Future Directions," *Telecommunication Systems,* Vol. 67, pp. 247-267, 2018.

[20] S. D. Gutppa, K. T. Shahriar, H. Alqahtani, D. Alsalman, and I. H. Sarker, "Modeling Hybrid Feature-Based Phishing Websites Detection Using Machine Learning Techniques," *Annals of Data Science,* pp.1-26, March 2022.

[21] N. Haller, C. Metz, P. Nesser, and M. Straw, "A One-Time Password System," IETF RFC 2289, Feb. 1998.

[22] C. Y. Huang, S. P. Ma, and K. T. Chen, "Using One-Time Passwords to Prevent Password Phishing Attacks," *Journal of Network and Computer Applications*, Vol. 34, No. 4, pp.1292-1301, 2011.

[23] W. C. Ku, D. M. Liao, C. J. Chang, and P. J. Qiu, "An Enhanced Capture Attacks Resistant Text-Based Graphical Password Scheme," *Proceedings of the 2014 IEEE/CIC International Conference on Communications in China: Privacy and Security in Commutations*, pp.204-208, 2014.

[24] LassPass Authenticator. <https://www.lastpass.-com/solutions/authentication> (Accessed: Jan. 15, 2023)

[25] Microsoft Authenticator. <https://www.microsoft.com/zh-tw/security/mobile-authenticator-app> (Accessed: Jan. 15, 2023)

[26] D. M'Raihi, M. Bellare, F. Hoornaert, D. Naccache, and O. Ranen, "HOTP: An HMAC-Based One-Time Password Algorithm," IETF RFC 4226, December 2005.

[27] D. M'Raihi, S. Machani, M. Pei, and J. Rydell, "TOTP: Time-Based One-Time Password Algorithm," IETF RFC 6238, May 2011.

[28] L. O'Reilly, "Phishing Attacks that Defeat 2FA Every Time," Security Boulevard, March 2021. <https://www.slashnext.com/blog/phishing-attacks-that-defeat-2fa-every-time>

[29] SAASPASS. <https://saaspass.com> (Accessed: Jan. 15, 2023)

[30] Sabarinath, "Introduction to Two Factor Authentication and Different Types of 2FA," TechLog360, April. 2020. <https://techlog360.com/two-factor-authentication-2fa/> (Accessed: Jan. 15, 2023)

[31] M. Sameen, K. Han, and S. O. Hwang, "PhishHaven − An Efficient Real-Time AI Phishing URLs Detection System," *IEEE Access*, Vol.8, pp.83425-83443, 2020.

[32] Y. Sun, S. Zhu, Y. Zhao, and P. Sun, "Let Your Camera See for You: A Novel Two-Factor Authentication Method against Real-Time Phishing Attacks," *arXiv preprint, arXiv. 2109.00132*, 2021.

[33] TOTP Authenticator. <https://www.binaryboot.com/totp-authenticator> (Accessed: Jan. 15, 2023)

[34] J. Umawing, "Has Two-Factor Authentication Been Defeated? A Spotlight on 2FA's Latest Challenge," Malwarebytes Labs, June 2019. <https://www.malwarebytes.com/blog/news/2019/01/two-factor-authentication-defeated-spotlight-2fas-latest-challenge>

[35] M. Vonau, "The 5 Best 2FA Apps on Android," Android Police, Dec. 2022. <https://www.androidpolice.com/best-2fa-apps-on-android/> (Accessed: Jan. 15, 2023)

[作者簡介]

吳星旻，國立臺中教育大學資訊工程學系研究生
顧維祺，國立臺中教育大學資訊工程學系教授
余傳欣，國立臺中教育大學資訊工程學系研究生