多重認證堵漏洞 網絡安全你要識

現今不少人都有網上服務戶口，每天都要使用不同形式密碼和賬號登入各種服務。不過，我們常常會接觸到一些特別專有名詞，例如：MFA、2FA、3FA、2SA、Token和OTP等。雖然每天在用，但卻搞不清楚這些名詞代表什麼、有什麼分別，甚至被弄得十分混淆。有見及此，本報請來前線信息安全專家及密碼學家龐博文，來解釋這些用在身份認證保安上的專有名詞。

傳統上所有網上電子服務都倚賴「賬號使用者名稱」（User Name）及「密碼或口令」（Password）作最基礎的登入認證手段，但由於此認證手段太薄弱，容易被盜取，再加上一般使用者的信息安全意識並不強，故可能在無意間洩漏使用者名稱及賬號給別人，又或使用弱口令等問題。

為提升網上服務戶口登入的安全性，傳統的認證手段實在有加強的必要。信息安全學借鑒了中國古代《六韜兵法》中《龍韜》的「兵符」概念，構建「多因素驗證」（Multi-factor authentication，簡稱MFA）來加強賬號認證。MFA驗證方法就是現在驗證流程的整個基礎。

MFA是一種基於賬號使用者名稱和密碼的加強認證安全機制，其通常會採取「三段式因素」，純粹使用賬號使用者名稱和密碼的登入認證稱為「單因素」（One Factor），單因素所指的是密碼。「雙因素」（Two Factors）就是除密碼外，再外加的第二重認證方法，例如平日使用銀行服務時，銀行會派發給客戶一個隨機生成密碼的電子令牌（Token），當客戶同時使用密碼和令牌來作認證，就構成「雙因素認證」（Two-factor authentication，簡稱2FA）。這方法比「單因素認證」可最大限度地降低因人為錯誤、密碼錯放或裝置遺失而導致的風險。

生物特徵認證 減被假冒風險

如涉及極端敏感的資料或賬號，信息安全專家或會在「雙因素認證」上再作加強，這方法稱為「三因素認證」（Three-factor authentication，簡稱3FA）。當使用者腦內記得密碼，同時手上拿着令牌，第三個可再加強的因素就是生物認證，亦即指眼球瞳孔辨識、聲紋和面容辨識，以及掌紋辨識等。

這種與生俱來的生物特徵因難以被複製和假冒，所以進行一些嚴謹的身份認證時，可作為第三個因素來加強認證方式。近年不少手機銀行軟件都加入了面容識別認證。

MFA會因資料的敏感性，在身份認證系統被設計時，由信息安全專家依據法例、法規或使用者體驗，作靈活配合來建立。學習信息安全的入門，通常都會背誦MFA口訣：Something you know（你知道的），Something you have（你擁有的），Something you are（你與生俱來的）。

MFA最常用的是「單因素」，特點是配置便宜且快速，但亦最不安全，所以專門針對大量使用者及非敏感資料的狀況下使用。一般合乎成本效益而又較安全的是2FA，亦是日常生活中處理財務及個人敏感資料時最常用到。

3FA是最安全，但因硬件設備成本高，所以通常極少數人被容許存取最敏感資料情況下使用。

不過，近年硬件開始普及，令價錢成本下降，所以可在消費者的智能電話加裝這些設備，令3FA更廣泛地使用。當然，3FA很大情況下亦會受制於硬件的規格、設計水平和辨識演算法的優劣，例如某些品牌的手機，其面容識別就曾被立體圖片欺騙。因此，使用3FA時會在產品和運作流程設計方面，要求較高技術水平。

一次性密碼 縮短時限防截取

雖2FA被認爲合乎成本效益，但亦有其本身弊病，如使用者忘記攜帶隨機生成密碼的電子令牌或銀行卡，就無法使用。爲方便使用者的同時又維持安全性，信息安全專家創造出使用電郵和短訊發放「動態認證碼」，這方法稱爲「兩步認證」（Two-step authentication，2SA）。

2SA的優勢在於使用者不用隨身攜帶電子令牌或銀行卡，只需使用手機就可接收「動態認證碼」。但需緊記這是「兩步認證」，而非「雙因素認證」，因認證過程中沒有增加一個新的認證因素，而是針對同一個認證因素的驗證過程作改進。

不管是2FA還是2SA，最重要的就是「動態認證碼」安全機制。這安全機制的構成主要倚賴「一次性密碼」（One-time password，簡稱OTP），OTP有效期爲一次登錄、會話或交易，可避免靜態密碼認證的安全缺點，甚至可設置OTP的存活時間長短，來抵擋認證碼被截取的可能。

龐博文小檔案

一個擁有接近半甲子經驗，由Apple IIe年代存活至今的前線信息安全專家及密碼學家。擅長有組織性網絡對抗、黑客術及電腦鑒證調查技能。口頭禪：「你今日畀人Hacked咗未呢？」