University of Taipei

Computer Science

Homework 3

Student ID: U10916024

Student: Cheng-Hao, Zhang

張呈顥

2023

▸ User Authentication

使用者身分識別主要是要辨識某人是否為合法的系統使用者。

可分為二部份：使用者身分（Identity）及鑑別（Authentication）。不但要能夠唯一識別使用者身分，而且必須要有方法來預防歹徒冒充別人身分的能力。

Cybercriminals can gain access to a system and steal information when user authentication is not secure.

3.User Identity 不須加密

User Identity（UID）通常位於 DB 系統 Table 上，是屬於 Key value 的狀態；意即，UID 是具有唯一性的。針對 UID 辨識使用者的驗證，主要是要確認此人身分是否存在於本系統內，若有則進入驗證階段，若無直接拒絕存取（Access denied）。

誠如前段所述，UID 的主要功能是辨識使用者身分，且是使用者鑑別的 Key value，不須加密；需要保密的是鑑別（Authentication）的相關資料。

6.直接儲存密碼法之優缺

對於 Password 之直接儲存，其安全性**極度堪憂**，因此目前普遍不被學業界所接受與使用。直接儲存密碼如同字面上之解釋，在系統儲存密碼時，並未有任何的加密措施，即所謂的存 Password 的明文；若惡意人士有窺探系統 DB 的機會，則所有使用者之密碼將無所遁形，此系統之機密、完整性將不復存在。

雖說如此，直接儲存密碼法依舊有其優點。因為儲存時未有任何的加密措施，所以在進行使用者身分與其密碼之比對時，所需時間甚短、十分快速。也因此，其安全性低下；效率與安全性只能取其一，而大家選擇了安全。

8.辨識使用者身分之類型

- 證件驗證（Something Held）
  - 條碼卡、 磁卡、IC 卡、智慧卡（Smart Card）
- 生物特性驗證（Something Embodied）
  - 生理結構唯一性：指紋、手紋、眼紋，如：Face ID, Touch ID
  - 行為差異性：聲音、筆跡、鍵盤、滑鼠
- 通行密碼驗證（Something Known）
  - 現行眾多系統採用的驗證方式
- 多重要素驗證（Multi-factor authentication, MFA）
  - 實體金鑰（Physical key）：大多人同時擁有多個系統的帳號密碼，常常容易忘記或混淆，因此有所謂「密碼是拿來防自己人」的一類說法。另外，鑒於現今科技之發展迅速及量子電腦的誕生，相關加密演算法之安全性已可被挑戰；因此發展出實體金鑰的驗證方式。它透過晶片韌體的驗證，來確保金鑰未被竄改，進而保全驗證之安全性。
  - 2FA：不以單一要素為驗證標的，而是使用雙重驗證之方式來達成安全性的維護。例如同時使用 Password 配上 email、簡訊或 2FA 應用程式 e.g., Authy, google-authenticator[1]的 OTP。

[1] https://github.com/google/google-authenticator

11.Password 的威脅

- 字典攻擊法(Dictionary Attack)

  以字典中之單字來測試使用者之通行密碼，一般常見單字有二萬個，測試一組單字僅需 1 毫秒，因此以字典攻擊法 20 秒內即可得知使用者的通行密碼（假設使用者之通行密碼為字典中之單字）。

- 猜測攻擊法(Guessing Attack)

  以使用者相關之資料猜測使用者之通行密碼，如生日、身分證號碼、電話號碼及紀念日（如結婚紀念日）等。

- 窮舉攻擊法或暴力攻擊法(Brute-Force Attack)

  將所有可能之通行密碼一一測試，因此若使用者所選之通行密碼過短，很快就會被測出。

- 重送攻擊法(Replaying Attack)

  攔截使用者的通行密碼，重新輸入到主機系統，以通過系統驗證。

- 行騙法(Spoofing)

  類似金光黨的行騙手法。駭客模擬主機系統之登入 (Login)畫面及其處理步驟，以騙取使用者密碼。