**University of Taipei**

**Computer Science**

**Homework 3**

**Student ID: U10916024**

**Student: Cheng-Hao, Zhang**

**張呈顥**

**2023**

1. **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.**

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  
- 行為差異性：聲音、筆跡、鍵盤、滑鼠  
• 通行密碼驗證(Something Known)

**11.**

二部份：使用者身分(Identity)及鑑別 (Authentication)。不但要能夠