二、研究計畫中英文摘要：請就本計畫要點作一概述，並依本計畫性質自訂關鍵詞。

計畫中文關鍵詞	智慧型手機；使用者驗證；行為生物識別；資訊安全；對抗式攻擊；假冒攻擊；弱特徵；特徵篩選
計畫英文關鍵詞	Smartphone; User Authentication; Behavioral Biometric; Information Security; Adversarial Attack; Impersonation Attack; Weak Features; Feature Selection
計畫中文摘要	近年來，智慧型手機上的應用軟體功能變得越加廣泛，像是行動支付這種富含個人隱私資訊的應用。根據eMarketer的調查，其預測2027年在美國使用行動支付的人數，將從2020年所有手機用戶中的35.4%上升到49.4%。然而，目前智慧型手機裝置上的身分驗證系統，如圖形密碼、文字密碼鎖等等，在開放環境下操作時容易遭受到惡意人士透過肩窺(Shoulder Surfing)的方式竊取密碼，導致使用者的行動支付遭到盜用，造成重大損失，因此，團隊所研發的基於行為之非侵入式連續身分驗證系統，可以減少打擾使用者的日常使用，避免使用者因為貪圖方便而選擇關閉身分驗證系統，此外，其會在手機系統後台持續驗證使用者的身分，確保手機在使用過程中的任一時刻皆為合法使用者。但基於行為的身分驗證系統作為機學習中的一環，勢必會受到對抗式攻擊(Adversarial Attack)的影響，惡意人士可以透過假冒攻擊(Impersonation Attack)，也就是模仿使用者的行為來破解身分驗證系統，因此，研究團隊預計在本計畫二年的研究中，針對假冒攻擊議題做研究，以提升模型的可用性與穩健性。在研究團隊的初步研究中已針對一位受害者與一位攻擊者進行實驗，並已證實受害者存在容易被攻擊者模仿的特徵，我們稱之為弱特徵(Weak Feature)，在將資料集移除弱特徵後，所訓練的抵禦模型也能有效抵禦攻擊者，然而此模型要在實際應用中仍存在某些限制，因此在第一年度中，我們將研究情境擴增至一位受害者與多位攻擊者，預期找到當前受害者容易被所有攻擊者模仿的特徵，並建立一個能夠為當前受害者抵禦多位攻擊者的模型，接著在第二年度中，研究將基於第一年度的研究結果，並將研究情境擴增至多位受害者與多位攻擊者，預期找到適用於所有受害者的弱特徵，使模型能夠為多位受害者抵禦多位攻擊者的假冒攻擊，以提升模型的穩健性。
計畫英文摘要	In recent years, the functionalities of applications on smartphones have become increasingly widespread, such as mobile payment applications that contain personal privacy information. According to eMarketer's survey, it is predicted that by 2027, the percentage of people using mobile payments in the United States will rise from 35.4% of all mobile users in 2020 to 49.4%. However, current identity authentication systems on smartphones, such as pattern passwords, text password, etc., are susceptible to malicious individuals stealing passwords through shoulder surfing when operated in open environments. This can lead to significant losses due to the unauthorized use of users' mobile payments. Therefore, the team has developed a behavior-based, non-intrusive continuous authentication system that minimizes disruption to users' daily activities. This system aims to prevent users from choosing to disable identity authentication systems for the sake of convenience. Additionally, it continuously verifies the user's identity in the background of the mobile system, ensuring that the phone is in the hands of an authorized user at any given moment. However, as a part of machine learning, behavior-based authentication systems are prone to adversarial attacks. Malicious individuals can use impersonation attacks to mimic user behavior and potentially attack the authentication system. Consequently, the team plans to focus on the issue of impersonation attacks in this two-year project to enhance the model's robustness. In the initial research, experiments involving one victim and one attacker were conducted. It was confirmed that the victim had weak features that were easily mimicked by the attacker. After removing these weak features from the dataset, the trained defense model could effectively resist

	the attacker. However, the model still has certain limitations in practical scenario. Therefore, in the first year, we will expand the scenarios to include one victim and multiple attackers, aiming to find weak features that the current victim easily mimicked by all attackers. Subsequently, we will build a model capable of defending the current victim against multiple attackers. In the second year, building upon the findings of the first year, the research will extend to multiple victims and multiple attackers, with the goal of finding weak features applicable to all victims. This approach aims to enable the model to resist impersonation attacks from multiple attackers targeting multiple victims, thereby enhancing the model's robustness.
計畫概述	請概述執行本計畫之目的及可能產生對人文、社會、經濟、學術發展等面向的預期影響性(三百字以內)。 ※此部分內容於獲核定補助後將逕予公開
	本研究計畫所提的增強智慧型手機行為身分驗證抵禦假冒攻擊能力以提升系統穩健性之研究，對於社會方面，可預防使用者因智慧型手機傳統身分驗證機制的安全漏洞造成為害，也能同時預防對本驗證機制的對抗式攻擊，強化行動裝置的安全性；在學術發展方面，就團隊所知目前尚無其他研究針對行為身分驗證之對抗式攻擊提出防禦方法，因此本研究將為學術界帶來新的指標，為後續研究者提供一個防禦對抗式攻擊的可能性方向。