專 題 演 講

講 者： 楊竹星 教授（國立成功大學電機工程學系）

題 目： Multiple Data Source Network Attack Analysis System based on MITRE Framework

摘 要：

隨著網際網路技術進步，現代人對於網路的依賴亦日趨嚴重。在享受便利的網路同時，攻擊者也藉由網路，不留痕跡地進行犯罪。攻擊者的攻擊手法日益推陳出新，為了達到目的攻擊者往往會不擇手段，大到近年知名的勒索病毒 WannaCry 加密使用者資料求取贖金，小到網站遭駭個資外洩等，攻擊方式讓人防不勝防。現在的攻擊已跳脫鎖定單一目標的入侵行為轉變並升級為多層次多目標的攻擊，因此大多數網路攻擊無法使用單一防禦方式進行防範。 此外在描述同一網路攻擊事件時，各個廠商往往根據公司不同之經驗與作業流程而有產生不同之解讀方式，造成在同一事件的描述時，無法取得共識。因此 MITRE 提出 ATT&CK Framework，使用同一個 Framework 讓廠商在交換/討論同一攻擊事件，可以有一共通語言，以減少溝通上之誤差。

利用事件關聯性分析的方式找出有關聯之攻擊以進行整合並找尋潛在性的威脅。研究結合網路型入侵偵測及主機型入侵偵測之風險評估系統，並利用 MITRE ATT&CK 所提供之攻擊矩陣描述系統目前所遭受之攻擊。最後使用視覺化呈現讓系統管理者可更容易管理所屬之網路，提升整體網路安全之能量。