電腦的記憶體變成臨時 Wi-Fi
敏感資料不保

Reported: 台北工程部

Date: Aug 3rd 2021

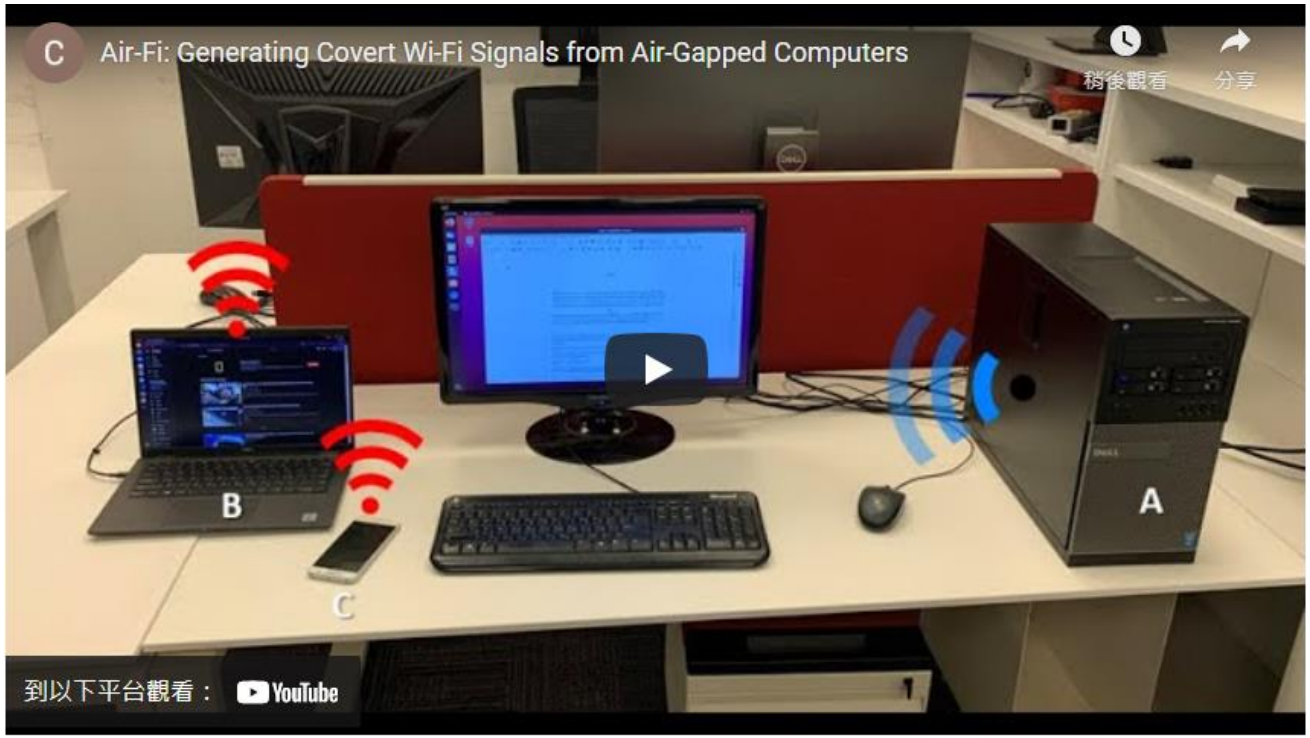
AIR-FI 的工作原理

AIR-FI 技術的核心理論是：任何電子元件在電流通過時，都會產生電磁波。

由於 Wi-Fi 訊號就是無線電波的一種，無線電基本上就是電磁波。

所以推論，攻擊者如果能將惡意程式碼植入完全隔離的電腦，就可控制流過記憶體模組的電流，進而產生電磁波，接下來就是調整到與 Wi-Fi 訊號頻譜一致（2.4GHz）。

研究員示範影片展示，他們成功在左邊這台完全隔離的電腦植入程式，然後發送訊號給右邊有 Wi-Fi 的電腦接收。



AIR-FI 是最容易的洩密攻擊!

AENEAS

怎樣讓記憶體產生電磁波的？

研究說明，只要透過讀入及寫出電腦記憶卡，在完美精準的時間點操作，就可讓記憶體匯流排產生出與微弱的 Wi-Fi 訊號一致的電磁波。

之後訊號就可被任何有 Wi-Fi 功能的裝置接收，包括智慧手機、筆記型電腦、物聯網裝置、智慧手錶等等，都成為接收的工具。

研究人員表示，他在不同的隔離電腦裝置嘗試此技術，沒有安裝 Wi-Fi 網卡的情況下，可用 100b/s 速度向數公尺外的裝置傳輸資料。

研究測試對於目前各種針對如何從一台置於隔離環境（沒有網路線、無線網卡）的電腦，盜取其中資料的攻擊方式研究，研究顯示 AIR-FI 攻擊是最容易成功的攻擊之一。

AIR-FI攻擊適用任何作業系統!

AENEAS

過去任何攻擊多半透過取得漏洞的方式，而取得漏洞前可能還要獲得 root / admin 許可權。

「（AIR-FI）只需一般使用者，只要他能接觸到這台電腦就可發起。且這種攻擊適用任何作業系統，甚至從虛擬機器（VM）內部進行。」

此外，雖然主要只有最新的記憶體模組才能在 2.4GHz 範圍內發出訊號，但研究人員表示，如果遇到舊記憶體模組，可透過超頻以達到所需輸出。

Thank You

AENEAS