CWMP 模糊測試的實作與研究

系所／資訊工程學系
指導老師／徐武孝
組員／林庭卉、黃于恬、黃詠元、林銀峰

網路帶給人類便利的生活，但網路通訊協定的安全如果暴露在危險中，可能會導致企業的內部資料外流，造成企業一定程度的損失。

模糊測試(Fuzz Testing)是一種發掘漏洞的軟體測試技術，概念為隨機產生大量數據傳送至被測試系統，執行過程由自動、半自動化的工具來進行測試，在此情況下嘗試擷取 Server 端和 Client 端之間的通訊數據，藉由得到的數據來分析網路通訊協定是否存在可能的安全漏洞。

本次專題使用模糊測試來檢測 CPE WAN Management Protocol（CWMP）這個網路通訊協定中的可能漏洞及弱點。實作平台以 Linux 的 Ubuntu 16.04 版為主，使用 Python 作為發展 CWMP 前端模糊測試程式，Server 的部分則使用 ACS(Auto-Configuration Server)。

CWMP 模糊測試程式先使用 TCP 與 ACS 建立三方交握連線，然後 CWMP 模糊測試程式會傳送連線請求給 ACS；當 ACS 收到連線請求後會發送回應封包給 CWMP 端模糊測試程式以確認雙方已建立連結。當雙方沒有資料要傳輸時，CWMP 模糊測試程式會發送空內容的 HTTP 封包並結束連線。

CWMP 的協定堆疊（Protocol Stack）如

圖 1 所示，本專研主要為對 Simple Object Access Protocol（SOAP）封包的內容(Payload)做修改(模糊測試)，然後將修改後的封包傳到 ACS；我們使用 Wireshark 來觀察 ACS 所回應的封包是否有異常或是沒回應。

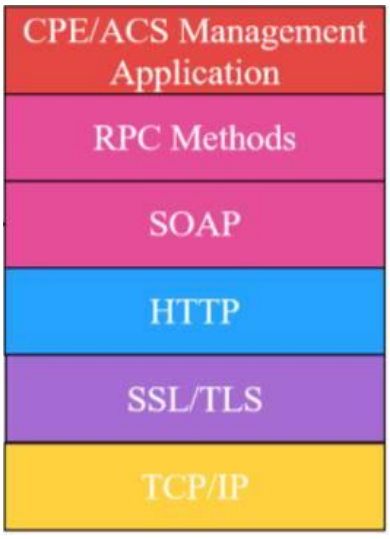

圖 1： CWMP 的協定堆疊