●行政院國家資通安全會報資安技術交流小組第 4 次交流會議報告

行政院國家資通安全會報爲建立產官學研資通安全技術交流平台，掌握資通安全技術發展趨勢，充實資通安全作業能量，特設資通安全技術交流小組(以下簡稱本小組)。本小組於去(101)年 8 月 8 日召開成立會議，並置召集人 1 人，副召集人 1 人至 2 人，由資安會報召集人指派適當層級人員兼任。委員 10 人至 15 人，除召集人及副召集人爲當然委員外，其餘委員，由資安會報召集人就推動資通安全有關之機關(單位)代表、學者專家及民間諮詢廠商代表派(聘)兼之。

本小組於本(102)年 3 月 11 日召開第 4 次交流會議，邀請國內資安相關廠商，就近期發現之駭客手法進行交流。會中數聯資安股份有限公司發現駭客可利用手機錄音並將錄下之語音檔回傳駭客中繼站；關貿網路股份有限公司提出偵測系統共用管理帳號密碼之網芳攻擊；宏碁電子化資訊管理中心發現駭客透過 WEB 寫入木馬，置換登入畫面程式，進而達到竊取檔案的目的；臺灣微軟股份有限公司特別針對 AD Server 提出資安強化的建議；趨勢科技股份有限公司發現新型態的惡意程式，會跳過內部 DNS，轉而使用外部 Web DNS 查詢中繼站，藉以規避現有之防堵機制；行政院資通安全會報技術服務中心針對趨勢科技的報告，提出相關因應方案說明；中華電信則報告近期發現之零時差攻擊案例。上述相關簡報下載網址如下：

一、數聯資安股份有限公司「手機病毒感染電腦案例」：
http://www.icst.org.tw/docs/Fup/手機病毒感染電腦案例.pdf

二、關貿網路股份有限公司「偵測系統共用管理帳號密碼之網芳攻擊」：
http://www.icst.org.tw/docs/Fup/3_偵測系統共用管理帳號密碼之網芳攻擊.pdf

三、宏碁電子化資訊管理中心「Web Mail 安全問題」：
http://www.icst.org.tw/docs/Fup/Web%20Mail%20 安全問題.pdf

四、臺灣微軟股份有限公司「微軟產品安全強度、如何強化的公開資訊，以及資安強化服務之建議說明」：

1.http://www.icst.org.tw/docs/Fup/0%E5%BE%AE%E8%BB%9F_ESAE%20-%20short.pdf

2.http://www.icst.org.tw/docs/Fup/資安強化服務建議說明.pdf

五、趨勢科技股份有限公司「新型態攻擊手法-遮日行動」：
http://www.icst.org.tw/docs/Fup/新 APT 中繼站連線報到手法介紹.pdf

六、行政院資通安全會報技術服務中心「新 APT 中繼站連線報到手法因應方式」：
http://www.icst.org.tw/docs/Fup/新 APT 中繼站連線報到手法因應方式.pdf

七、中華電信「近期發現之零時差攻擊案例」：
http://www.icst.org.tw/docs/Fup/近期事件使用手法.pdf