【後量子電腦時代的網安資安問題與解決】
以電子身分證及數位簽章為例

❖ **課程介紹：**

網安資安問題即國安問題，故網安資安則國安；而危機包含危險及機會，無知則危險，智慧則機會來臨，後量子電腦時代的來臨，你是看到機會還是危險？

量子電腦時代的來臨，代表著只要是軟體加密，在足夠經濟利益的吸引下，駭客就會想方設法去破解密鑰，盜取資料資訊錢財，並勒索廠商，讓個人資訊資料公開，引起社會的恐慌。近年國際上資安事件層出不窮：yahoo、Facebook、eBay、Uber、Equifax、Target、JP Morgan、OPM、TJX、Heartland Payment…資安都出問題,包含我國銓敘部的個資全部外洩。而銀行及加密貨幣，是最能直接衡量經濟利益的駭客事件：Bitfinx 被盜 12 萬枚比特幣，價值 7,200 萬美元、日本 Coincheck 被盜價值約 4 億美金的數位貨幣、全球最大加密貨幣交易所 Binance 被盜 7000 枚比特幣，價值 4,000 萬美元、日本 Mt. Gox 公司的 85 萬枚比特幣不翼而飛，至今下落不明。

聯合國安理會 2019 年 3 月的調查報告指出，北韓駭客竊取了至少 6.7 億美元的數位貨幣。並依據 2018 年 10 月美國資安機構”火眼”(FireEye) 調查報告指出，北韓 APT38 駭客團體事件，全球十一國有十六家銀行受害,共竊取了至少 11 億美金,包含我國第一銀行 2016.07 被盜領 8,237 萬台幣、2017.10 遠東銀行遭竊 18 億元。這些都是號稱世界最嚴密的銀行軟體加密，在量子電腦時代還未來臨前就已是不堪一擊，問題重重，顯然現在的密碼學基礎上有其疏漏之處。

所以 21 世紀 Alfred Principle 提出，密鑰一定會遺失或洩漏，如何能在察覺密鑰遺失或洩漏的情況下，讓系統迅速地在使用者最小負擔甚至無負擔的前提下，恢復安全狀態並正常運作才是重點。而要達到縱使密鑰洩漏依然安全，其關鍵在如何運用新式電子身分證及新式電子簽名方法。

簡單來說，電子身分證是國家內事，無關國際標準，其重點是安全，若因安全限縮其功能，與紙本身分證無差別，為何換發？而且採用國外廠商 IC，安全是否有保障？難道只為消耗預算？所以最好的方法是秘鑰由硬體 IC 內部自行產生，其 IC 的製程規格及加密方法是公開的，也就是說沒有人能夠複製這秘鑰，達到 CC 安全規範 EAL5+以上的安全等級，是目前 e ID 世界上加密等級最高的，同時 CA 認證中心也要達到 CC 安全規範 EAL5+以上的安全等級。

新式數位簽章，則綁定人事時地物，每次都是新的簽章用於特定用途，保證無法增減竄改，取代以往數位簽章只綁定人，如同印章，一旦被盜取竄改，則後果不堪設想；新式數位簽章也利用認證中心的確認，並執行所核准的指令，也就是說利用自行生成的數位簽章，由認證中心代執行個人隱私權命令，而不是用已被破解的自然人憑證的方法來保護，則個資及隱私權得以保障。

網路安全及資料資訊安全是二十一世紀的顯學，新式電子身分證及新式電子簽名方法，不只是在本次討論的 e ID, FINTEC, Healthcare 基礎關鍵，也是未來 AI、IOT、數位貨幣錢包、區塊鏈、金融卡、儲值卡、員工卡、無人駕駛車船飛機、身分證、護照、健保卡…的基礎關鍵，各位是不是你們的機會來臨了？

日期/時間	2019 年 9 月 24 日(二)，9:30~16:30，共 6 小時
地點	科技大樓 4 樓 4002 教室(台北市大安區和平東路二段 106 號)
主辦單位	工研院產業學院
協辦單位	安悅科技股份有限公司、台灣隱私權顧問協會

❖ **課程大綱：**

時間	講題	主講者
09:00-09:30	報到	
09:30~09:50	貴賓致詞	工研院產業學院 王本耀 訓練長 台灣隱私權顧問協會 陳柏文 執行長
09:50~10:30	淺談量子電腦的資安問題與策進	前國安局副局長 郭崇信
10:30~11:10	區塊鏈與密碼貨幣之安全	國立台灣大學 陳君明 兼任助理教授
11:10~11:30	休息交流	
11:30~12:10	歐盟與台灣個資法對 AI 時代資訊安全之要求	達文西法律事務所 葉奇鑫 所長
12:10~13:10	午餐	
13:10~13:50	簡介 CC EAL 安全認證 （以晶片及系統安全說明）	財團法人電信技術中心 黃嘉章 經理
13:50~14:30	初探解決問題之專利及管理方法	安悅科技 黃音凱 董事長
14:30~15:20	1. 一種密碼可選的挑戰響應身份認證方法及其應用 2. 一種靠加密算法綁定設備和用途的電子簽名方法	安悅科技 張英輝 董事總經理
15:20~15:40	休息交流	
15:40~16:30	純網銀 FinTech 商品如何獲利探討與客戶電子身份認證解決方案	前合作金庫銀行協理 吳文正

*主辦單位得保留活動議程及講師之變更權利 The Meetup agenda is subject to change

❖ **講者介紹：**

	**郭崇信** 現職：中華民國資訊軟體協會 特聘顧問 經歷：前國家安全局 副局長 電訊科技中心 主任
	**陳君明** 現職：國立臺灣大學數學系 兼任助理教授 Wisecure Technology Chairman 銓安智慧科技 研發長 學歷：美國普渡大學數學系 博士
	**葉奇鑫** 現職：達文西個資暨高科技法律事務所 所長 東吳大學法律研究所 兼任助理教授 國發會 個資法諮詢委員 臺灣網路暨電子商務產業發展協會(TIEA) 監事 台灣數位安全聯盟(TWCSA) 理事
	**黃嘉章** 現職：財團法人電信技術中心 經理 經歷：財團法人電信技術中心 工程師
	**黃音凱** 現職：安悅科技 董事長 經歷：鴻海精密董事長 特別助理 典通科技 總經理 偉詮電子 副總經理
	**張英輝** 現職：安悅科技 董事總經理 經歷：Pictologic USA Director 富晶半導體 創辦人 印通科技 協理 學歷：交通大學 電子工程 博士
	**吳文正** 經歷：歷任合作金庫 業務部/資訊部/信託部/信用卡部/電子金融部 協理

【課程費用資訊】

- **課程費用：免費**
- **報名方式：**線上報名http://college.itri.org.tw，或請將報名表傳真 02-2381-1000
- **課程聯絡人：**(02)2370-1111，分機 316 李小姐、分機 309 徐小姐

報 名 表

FAXTO：(02)2381-1000 李小姐收

課程名稱：後量子電腦時代的網安資安問題與解決以電子身分證及數位簽章為例				
公司全銜			統一編號	
發票地址			傳　　真	
參加者姓名	部　門	電　話	手機	E-mail
		(　　)		
		(　　)		
聯絡人		(　　)		

☐ 信用卡（線上報名）：繳費方式選「信用卡」，直到顯示「您已完成報名手續」為止，才確實完成繳費。
☐ ATM 轉帳（線上報名）：繳費方式選擇「ATM 轉帳」者，系統將給您一組轉帳帳號「銀行代號、轉帳帳號」，但此帳號只提供本課程轉帳使用,各別學員轉帳請使用不同轉帳帳號！！轉帳後，寫上您的「公司全銜、課程名稱、姓名、聯絡電話」與「收據」回傳。
☐ 銀行匯款(公司逕行電匯付款)：土地銀行 工研院分行，帳號 156-005-00002-5（土銀代碼：005）。戶名「財團法人工業技術研究院」，請填具「報名表」與「收據」回傳。
☐ 即期支票：抬頭「財團法人工業技術研究院」，郵寄至：100 台北市中正區館前路 65 號 7 樓 704 室，李小姐收
☐ 計畫代號扣款(工研院同仁)：工研院員工報名請網路點選「工研人報名」填寫計畫代號後，經主管簽核同意即可

1、請註明服務機關之完整抬頭，以利開立收據；未註明者，一律開立個人抬頭，恕不接受更換發票之要求。
2、若報名者不克參加者，可指派其他人參加，並於開課前一日通知。
3、如需取消報名，請於開課前三日以書面傳真至主辦單位並電話確認申請退費事宜。逾期將郵寄講義，恕不退費。