109【上】硬體安全導論 期末書面報告

系 級：__電 機 21__ 姓 名： __林 俊 曄__ 學 號： 106011206

課程內容：

- 請依自己的理解，總結本學期所學內容，包含課堂與期中、期末專題。

1. 課程所學:

在上這堂課之前，看到課名前其實有點疑惑，因為當時在資工系其實也有開了一門課程，叫做「**密碼與網路安全概論」**，由於當時我接觸過一些加密演算法的概念(EX: RSA、ENIGAMA)，以為資訊安全的範疇大多與軟體較相關，但整整上完一學期的硬體安全導論後，才發現事實並不是如此!

雖然我們可以透過**高深且複雜度極高的演算法**去加密我們不想被駭客竊取的資料，但道高一尺、魔高一丈，駭客根本不用和這些演算法硬碰硬，只要想辦法用其他**旁門左道的攻擊**方式，例如: **觀察電路在機密資料傳輸時的變化情形**、透過**不正常的操作方式(GLICH)**去嘗試又或者更進一步直接用**逆向工程**直接去看你 LAYOUT 的設計方式，攻擊手法多到根本防不慎防。

我覺得只用**軟體上的加密手法**就像是想用**超高級且安全的電子鎖**去保護寶藏，但一但小偷把電源切斷後，那個電子鎖便立即失效，小偷能輕鬆突破防護。所以我們在設置這樣的環境時，就要考量到不論小偷在何種情形下，運用何種方式(可能是一個笨小偷、一群聰明的小偷或甚至是一大群有組織計畫的小偷集團)，都無法輕易的突破防線。此外，隨著科技進步，計算機的計算能力日益增長，若單單只靠運算的複雜度來防範攻擊，在不久的未來這些我們曾經**認為不可能被破解的加密方式**再也不安全了。因此，產品需要從**硬體層面就具有防護能力**，而如何**高效且低成本的生產出安全的晶片**，在未來絕對是學界和業界都十分關注的議題!

2. 期中專題:

在期中專題中，我負責的是 **ARDUINO 板的資料蒐集**和**軟硬體整合**。雖然我之前有接觸過**嵌入式硬體的課程**，但我發現不同的板子的特性及使用方式還是有蠻大的差異，所以我剛開始其實處處碰壁，在大量的尋找相關資料和不斷嘗試與錯誤後，才大致了解 ARDUINO 板的習性，遇到特定問題時知道該如何解決。

在資料蒐集方面，我使用的是比較簡單直覺的 **polling**，在期中作業中只蒐集數量少的資料(512 筆 byte)來說，不太容易出現問題，所以就當時就沒有特別留意可能會產生的問題，而先前沒設計好的資料蒐集方式也讓我在往後的期末報告中吃盡苦頭，因為要蒐集的資料量高達數十 GB，用原本的方式不但慢且容易產生 bug，導致我剛開始蒐集資料的前幾天其實都是徒勞無功，直到我最後才改成 **interrupt** 的手法去收集，這告訴我們身為工程師真的不要怕麻煩，不要貪圖一時的方便而讓往後的自己欲哭無淚，不論軟體或硬體的設計，都是寧願仔細一點，一次就完成到位。

3. 期末專題:

在期末專題中，我負責 **ARDUINO 資料蒐集**、**NIST SP800 的測試**、**script 的撰寫**、**資料整理分析與視覺化**、**PPT 設計**和**前半部分的報告**，在整個過程中學習到非常多東西，我也很慶幸我以前在其他課程專題中有學習過如何獨立解決問題，所以在整個流程當中少走許多冤枉路。舉例來說，這次 NIST SP-800 的總共需要用到 100files 進行測試，但原本在 github 上的 source code 並不支援不同筆資料排程測試，還好我之前有碰過一些關於**.sp script 的教學**，**才順利的設計出能讓 NIST SP800 一次就跑完 100file 並且每個檔案都有順利設定參數以及儲存 final report**，真的節省許多時間!

至於在 Paper 方面的內容，我真的花了很多時間反覆看了好幾遍，基本的運算方式跟例子我是都有理解，但是在最後特定的數學部分(像是每種測設到最後總是可以通過一些奇怪的計算，弄出 p-value<0.01 就視為不是理想隨機數)，我還是無法完全參透其中的概念，雖然到最後可以就 pass rate 去分析他們的好壞，但我覺得這樣的理解還不夠透徹，光頻一個數字來判斷好壞似乎有點單薄，因此我會在下學期找**統計相關課程**來學習，希望能讓我了解原本困惑的地方。

修課心得：

- 請回顧本學期在課堂學習上遇到的問題、解決方式、組員間互動分工狀況，亦可寫下關於授課方式、內容之建議。

1. 課堂學習與解決方式:

我這學期在課程比較艱深的地方，會有許多不能理解的地方，**像是 Elliptic Curve Cryptography(ECC)的那單元**，老實說我幾乎都不太懂，只覺得可以光靠圖形上面的映射或做切線去做運算十分的有趣，不過在之後也沒有特別去。但在其他部分，像是**關於 GF 的觀念**我就有自己去查資料理解，因為我自己比較有興趣。我還蠻喜歡這樣的學習方式，因為在學習的過程中，並不會要求你全盤接受，或是要你完全學會所有跟這課程相關的所有內容，而是我們可以依照自己的興趣去針對特定的部分做更深入的研究學習，透過這樣的方式所學習的知識才真正是自己的，不像是為了考試而一股腦死記硬背的公式題型，往往過了一個週末就全部還老師了。

2. 組員間互動分工狀況:

我覺得組員間互動分工可能是這門課比較大的問題，也是這種大學分組作業的常見的通病，就是組內的**分工情形其實非常的不平衡**，老實說在我們這組或其他組都可以明顯到類似情況，有些組員非常被動，常常都只坐等其他人找到的解答，坐享其成。像是我們**第三組的陳同學**在**兩次的回家作業和期中期末報告**其實都沒有什麼貢獻，只在報告前的一兩天出現，對於作業整個流程架構都不了解，只要在下半場**上台照唸打好的 PPT 就完成他的期末報告**，而我多少心裡會不平衡。由於我們這組大家原本就都認識，所以沒有在當面都沒有說什麼，不過正好在這次的期末報告中有提到這部分，所以我認為還是該說出來，這樣對於其他認真對待課程的人才公平。

3. 授課方式與內容建議：

在內容方面我覺得其實都很不錯，而讓同學來上台報告的方式也能讓該組同學對整體內容有一定程度的了解，我也在整個課程中學到蠻多東西。而我想到的建議大概有兩點: 第一是可以增加有一個**大家上傳問題或討論的平台**，因為大家可能都會有類似問題，如果助教在討論區上直接回應的話，大家就不用一一寄信詢問助教同樣的問題，會比較有效率。第二點，就是在期初就先說明會有**小組互評機制**，讓少部分的人較不會有搭便車的想法。最後**很感謝助教大大們每次都很耐心回答我的問題 QQ**，愚蠢的我還不小心洗

掉兩次 TEST BOARD code，但助教都很好，馬上就回應我並給予協助，非常感謝 QQ!

參考文獻：

在我的紀錄中，只有這四個比較有用的資料，其他的沒有特別紀錄。

1. AES:

   https://www.youtube.com/watch?v=gP4PqVGudtg

   https://zhuanlan.zhihu.com/p/78913397

2. Auduino:

   https://hugheschung.blogspot.com/2018/05/arduino-putty-arduino-serial-port.html

   https://www.arduino.cc/reference/en/