國 立 高 雄 師 範 大 學 教 學 綱 要 (106 學 年 度)

科目名稱：資訊安全　　□必修 ■選修　　教師：楊中皇

任課班級：軟體工程與管理學系

每學期開課學分數：上學期 3 學分　　下學期 ____ 學分

總學分數： 3 學分　每週上課時數： 3 小時

連繫電話： 8000　辦公地點：軟體工程與管理系　辦公時間（Office hour）：TBA

※※請遵守智慧財產權觀念、不得非法影印※※

一、教學目標： 本課程主要使學生瞭解資訊安全的基礎技術，並探討資訊系統安全通信協定設計與攻擊。內容包含理論上探討密碼系統、訊息認證與數位簽章等技術，並介紹現行網際網路與行動網路中所採用的安全架構及其安全通信協定。

二、課程核心能力及其配分：本課程內容包含：資訊安全導論、網路安全與管理等，亦將探討以開放原始碼為基礎的網路安全新技術的發展。課程內容包括

1. 網路安全簡介
2. 私密金鑰密碼系統
3. 公開金鑰密碼系統
4. 數位簽章
5. 金鑰管理技術
6. 網路安全應用實例

三、教材內容：課本與講義(參見 http://security.nknu.edu.tw/textbook/)。

四、實施方法：

1. 講授：依據教學進度講授教學單元之各項內容。
2. 提問與討論：每週課程前提出問題引導學生學習，另外也鼓勵學生針對授課內容提出問題進行討論。
3. 應用實例：配合教授單元，透過應用實例與文獻之研討，加強學生對網際網路與行動網路於實務應用之能力。每位同學需針對各別的資訊安全應用實例進行期中與期末報告。

五、評量方式：

1. 期中考（採 Open book）：佔總成績 30%
2. 期末考（採 Open book）：佔總成績 30%
3. 期中報告與期末報告：佔總成績 30%
4. 課堂參與：佔總成績 10%

六、主要讀本及參考書目：

（1）主要讀本：楊中皇，網路安全理論與實務，學貫行銷股份有限公司，2008 年 9 月出版。

（2）參考書目：(參考資料詳見 http:/security.nknu.edu.tw/infosec/)

- Nikolay Elenkov, *Android Security Internals: An In-Depth Guide to Android's Security Architecture*, No Starch Press, 2015.
- A.J. Menezes, et al, ***Handbook of Applied Cryptography***,CRC Press Series on Discrete Mathematics and Its Applications), 1996. 參閱 http://www.cacr.math.uwaterloo.ca/hac/有 PDF 電子檔。

七、教學進度：

週	別	內　　容	作　　業	參 考 資 料
（上學期）	1	資訊安全概論		
	2	私密金鑰密碼系統(一) 古典加密		
	3	私密金鑰密碼系統(二) DES/Triple-DES		
	4	私密金鑰密碼系統(三) AES		
	5	公開金鑰密碼系統(一) 概論		
	6	公開金鑰密碼系統(二) RSA		
	7	公開金鑰密碼系統(三) Diffie-Hellman		
	8	公開金鑰密碼系統(四) ElGamal		
	9	期中報告		
	10	期中考		
	11	單向雜湊函數、數位簽章		
	12	金鑰管理、密碼模組		
	13	IC 卡、Wireshark 封包分析軟體		
	14	Nessus、Snort 軟體介紹		
	15	Android 安全簡介		
	16	期末報告(一)		
	17	期末報告(二)		
	18	期末考		