個別課程英文授課大綱

表單編號：QP-T02-07-11
保存年限：10 年

課程名稱 Course Title	(中文) 進階軟體安全 (英文) Advance Software Security		
授課教師 Instructor	郁方老師	開課單位 Departments	資管系
學分數 Credit(s)	2	修課對象 Target Students	學士班、碩士班
課程目標 Course Objectives	Could and Apps have rapidly replaced conventional computing in recent years. They are known to be fraught with security risks. In this course, we will discuss modern risks of cloud computing and apps, and discuss techniques that address these risks. In addition, as multimedia becomes the dominant content presentation, we are also interested in multimedia security. We will study many selected papers, as well as implement practical tools. At the end of this course, students shall understand the basic security concepts of multimedia, cloud computing and mobile apps, and are familiar with techniques that can embed/extract/execute patterns/code in digital contents, detect (embedded) attacks of apps and alleviate potential risks of cloud computing. Students will also gain experience on doing research via rigorous paper study, as well as experience on practical tool development.		
課程大綱 Course Description	We are particularly interested in (but are not limited to) the following techniques: 1. Classify apps on their system method calls 2. Attack KVM/VMware kernel□via systematic monitoring and dynamic resource allocation and dispatching of the cloud□ 3. Hiding data in multimedia with encoding and decoding signatures and executable.		
上課進度 Weekly Course Schedule	Three topics will be covered in this course: Cloud security (C-team), App security (A-team), and Multimedia security (V-team). Students will be asked to select one topic and join the team based on their interests. **Schedule** (subject to change) • Week1: Course and Project Introduction • Week2: [Paper Study] "A Survey of Mobile Malware in the Wild" by A-team • Week3:		

	[Paper Study] "Addressing cloud security issues" and "Virtualization under attack: Breaking out of KVM" by C-team • Week4: [Paper Study] "User-centric Adaptation of Web Information for Small Screens" and the Visualizing Data Book Chapter 8 "Networks and Graphs" by V-team • Week5: [Project Discussion] "The Web Vulnerability Patcher" by V-team • Week6: [Paper Study] "PiOS: Detecting Privacy Leaks in iOS Applications" by A-team [Project Discussion] "AppBeAch" by A-team • Week7: [Paper Study] "Secure Virtualization for Cloud Computing" and "An Architecture for Providing Security to Cloud Resources"[Project Discussion] Detecting Malicious Behaviors of VMs by C-team • Week8: [Happy Spring Break] [Proposal Due (extended to Apr. 15)] • Week9: [Paper Study] "Visualizing the Execution of Java Programs" and "Software Visualization for Object-Oriented Program Comprehension" [Project Discussion] *3D-rize* XML graphics, and Patcher online (presented in English) • Week10: [Paper Study] "Crowdroid: Behavior-Based Malware Detection System for Android" [Project Discussion] Identifying Arguments of Obj_MsgSend in assembly by A-team • Week11: [Paper Study] "Hey, You, Get Off of My Cloud: Exploring Information Leakages in Third-Party Compute Clouds" by C-team [Project Discussion] Auditing and path tracking of VMs by C-team • Week12: [Paper Study] "Graphiz" and "Dinah: An Interface to Assist Non-Programmers with Selecting Program Code Causing Graphical Output" by V-team [Project Discussion] Visualizing Vulnerabilities in 3D and Mobile Devices • Week13: [Paper Study] "Vision: Automated Security Validation of Mobile Apps at App Markets" and "Hey, You, Get Off of My Market: Detecting Malicious Apps in Official and Alternative Android

	Markets" by A-team [Project Discussion] Decoding and decryption by A-team • Week14: [Paper Study] "SecVisor: A Tiny Hypervisor to Provide Lifetime Kernel Code Integrity for Commodity OSes", "All Your Clouds are Belong to us-Security Analysis of Cloud Management Interfaces" and "CUDACS: Securing the Cloud with CUDA-Enabled Secure Virtualization" by C-team [Project Discussion] VIS by C-team • Week15: [Paper Study] "Visualization of Test Information to Assist Fault Localization" and "Using Task Context to Improve Programmer Productivity" by V-team [Project Discussion] Stranger with the all new interface by V-team • Week16: [System Demo and Discussion] A-team demo and C-team demo • Week17: [System Demo and Discussion] V-team demo and discussion • Week18: [Final Report Due] Individual Study by V-, A-, C- team used in Section B.
教學方式 Instructional Method	Paper Study, Project Discussion.
課程要求 Course Requirements	1. Graduate students will be asked to present and lead the discussion of research papers in their field. 2. We also expect the graduate students lead a team to develop related systems/tools. Undergraduate students will be asked to join one team to help tool development.
評量方式 Evaluation	1. Participation (20%) 2. Paper Study(40%) --Each team will present 6-8 papers. --For each one, the team needs to turn in one page review in English, including the summary, advantages, disadvantages, and the comparison against your work 3. System Development (40%) --Each team needs to present its progress biweekly --Each team needs to turn in the proposal (in the middle of the class) and the final report (at the end of the class)
教材及參考書目 Textbooks & Suggested Materials	Cloud Security -CISE Research [article] -Top cloud security risks by [Gartner][ComputerWeekly]

-An open cloud project [slides]

-Books:

- C. Hoff, R. Mogull, and C. Balding, Hacking Exposed: Virtualization and Cloud Computing: Secrets and Solutions. [amazon]

-Technical papers:

- B.D. Payne, M. Carbone, M. Sharif, W. Lee. "Lares: An Architecture for Secure Active Monitoring Using Virtualization" [paper]
- J. Somorovsky, M. Heiderich, M. Jensen, J. Schwenk, N. Gruschka, L. Lo lacono. "All Your Clouds are Belong to us-Security Analysis of Cloud Management Interfaces" [paper]
- A. Seshadri, M. Luk, N. Qu, A. Perrig. "SecVisor: A Tiny Hypervisor to Provide Lifetime Kernel Code Integrity for Commodity OSes" [paper]□
- P. Sharma, S. K. Sood, and S, Kaur, Security Issues in Cloud Computing. [paper]
- F. Lombardi and R. D. Pietro, CUDACS: Securing the Cloud with CUDA-Enabled Secure Virtualization. [paper]
- N. Padmanabhan and B. Edwin, An Architecture for Providing Security to Cloud Resources. [paper]
- T. Ormandy, An Empirical Study into the Security Exposure to Hosts of Hostile Virtualized Environments. [paper]
- F. Lombardi, R. D. Pietro, Secure Virtualization for Cloud Computing, Journal of Network and Computer Applications. [paper]
- D. Zissis and D. Lekkas, Addressing Cloud Computing Security Issues, Future Generation Computer Systems. [report]□
- G. Anthens, Security in the Cloud. Comm. ACM. [paper]
- T. Ristenpart, E. Tromer, H. Shacham, S. Savage, Hey, You, Get Off of My Cloud: Exploring Information Leakages in Third-Party Compute Clouds. [paper]
- N. Elhage, Virtualization under attack: Breaking out of KVM. [paper][slides][video]

App Security

-News and Report□

- Hottest IT Skills? Cybersecurity [networkworld]
- Android programmers shifting toward Web apps [cnet]
- Apps could be overtaking the Web [technolog]
- Including Ads in Mobile Apps poses privacy, security risks [newsroom]
- iOS App downloads from Apple store achieve 25 billions [applestore]
- Mobile Apps take data without permission [bits]

" While Apple says it prohibits and rejects any app that collects or transmits users' personal data without their permission, that has not stopped some of the most popular applications for the

iPhone, iPad and iPod — like Yelp, Gowalla, Hipster and Foodspotting — from taking users' contacts and transmitting it without their knowledge."

- Apple Loophole gives developers access to photo [bits]

"After a user allows an application on an iPhone, iPad or iPod Touch to have access to location information, the app can copy the user's entire photo library, without any further notification or warning, according to app developers."

-Sites/Books:

- iPhone Hacks [site][book by O'Reilly]□

-Technical papers

- M. Bscher, F. C. Freiling, J. Hoffmann, T. Holz, S. Uellenbeck, C. Wolf. Mobile Security Catching Up? Revealing the Nuts and Bolts of the Security of Mobile Devices. [paper]
- Y. Zhou, Z. Wang, W. Zhou, X. Jiang. Hey, You, Get Off of My Market: Detecting Malicious Apps in Official and Alternative Android Markets. [paper]
- Y. Zhou, X. Zhang, X. Jiang, and V. W. Freeh. Taming Information-Stealing Smartphone Applications (on Android). [paper]
- W. Enck, D. Octeau, P. McDaniel, and S. Chaudhuri, A Study of Android Application Security. [slides][paper]
- D. Wetherall, D. Coffnes, B. Greensten, S. Han, P. Hornyack, J. Jung, S. Schechter, and X. Wang. Privacy Revelations for Web and Mobile Apps. [paper]
- M. Grace, W. Zhou, X. Jiang, A. Sadeghi, Unsafe Exposure Analysis of Mobile In-App Advertisements. [paper]
- Sans Institute, Mac Malware Analysis. [paper]
- A. P. Felt, M. Finifter, E. Chin, S, Hanna, D. Wagner, A Survey of Mobile Malware in the Wild. [paper][slides]
- M. Egele, C, Kruegel, E. Kirda, G. Vigna, PiOS: Detecting Privacy Leaks in iOS Applications. [paper] (Mac)
- P. Gilbert, B.-G. Chun, L. P. Cox, J. Jung, Vision: Automated Security Validation of Mobile Apps at App Markets [paper] (AppInspector-Android)
- A. P. Felt, E. Chin, S. Hanna, D. Song and D. Wagner, Android Permissions Demystified. CCS 2011. [paper] [slides]
- K. Rieck, P. Trinius, C. Willems, and T. Holz, Automatic Analysis of Malware Behavior using Machine Learning. [paper]□
- I. Burguera, U. Zurutuza, S. Nadjm-Tehrani, Crowdroid: Behavior-Based Malware Detection System for Android. [paper]
- A.-D. Chmidt, R. Bye, H.-G. Schmidt, J. Clausen, O. Kiraz, K. A. Yuksel, S. A. Camtepe, and S. Albayrak, Static Analysis of Executables for Collaborative Malware Detection on Android. [paper]

Multimedia Security and Data hiding

-Books

- Visualizing Data by Ben Fry, O'Reilly Media, Dec. 2007

-Links

- 29 Sexy iPhone App Design [link]
- A Graph Visualization Software [Graphviz: dot]

-Technical papers

- J. K. Paruchuri and S.-C. S. Cheung. Joint Optimization of Data Hiding and Video Compression. [paper]
- A. K. Bhaumik, M. Choi, R. J. Robles, and M. O. Balitanas. Data Hiding in Video. [paper]
- X. Quan and H. Zhang, Data Hiding in MPEG Compressed Audio Using Wet Paper Codes. [acmdl]
- B.-Y. Lei, K.-T. Lo, J. Feng. Digital Watermarking Techniques for AVS Audio. [paper]
- M. Wu and Bede Liu. Multimedia Data Hiding. [book]
- N. Memon and P.W. Wong, Protecting Digital Media Contents. [paper]
- C.-S. Lu and H.-Y. Mark Liao, Multipurpose Watermarking for Image Authentication and Protection. [paper]
- J. J. Chae and B. S. Manjunath, Data Hiding in Video. [paper]□
- M. Wu and B. Liu. Data Hiding in Image and Video: Part I-Fundamental Issues and Solutions. [paper]
- M. Wu and B. Liu. Data Hiding in Image and Video: Part II-Designs and Applications. [paper][summary][slides]
- D. Mukherjee, J. J. Chae, S. K. Mitra. A Source and Channel-coding Framework for Vector-Based Data Hiding in Video. [paper]
- A. S. Abbass, E. A. Soleit, and S. A. Ghoniemy. Blind Video Data Hiding Using Integer Wavelet TRansforms. [paper]□
- E. T. Lin, A. M. Eskicioglu, R. L. Lagendijk, E. J. Delp. Advances in Digital Video Content Protection. [paper]
- W. D. Pauw, E. Jensen, N, Mitchell, Visualizing the Execution of Java Programs. [paper]
- M. Kersten, G. C. Murphy, Using Task Context to Improve Programmer Productivity. [paper]
- A. Bragdon, S. P. Reiss, R. Zeleznik, S. Karumuri, W. Cheung, J. Kaplan, C. Coleman, F. Adeputra, and J. J. LaViola, Code Bubbles: Rethinking the User Interface Paradigm of Integrated Development Environments. [paper]
- M. J. Pacione, Software Visualization for Object-Oriented Program Comprehension, [paper] [full report]
- J. A. Jones, M. J. Harrold, J. Stasko, Visualization of Test Information to Assist Fault Localization. [paper] [slides]
- H. Ahmadi, J. Kong, User-centric Adaptation of Web Information for Small Screens. [paper]
- P. Gross, J. Yang, and C. Kelleher, Dinah: An Interface to

	Assist Non-Programmers with Selecting Program Code Causing Graphical Output. [paper] •P. Gross and C. Kelleher, Non-programmers Identifying Functionality in Unfamiliar Code: Strategies and Barriers. [paper] •T.-H. Chang, T. Yeh, R. Miller, Associating the Visual Representation of User Interfaces with their Internal Structures and Metadata. [paper] •P. Dragicevic, S. Huot, F. Chevalier, Animating from Markup Code to Rendered Documents and Vice Versa. [paper] •T. Karrer, J.-P. Kramer, J. Diehl, B. Hartmann, J. Borchers, Stacksplorer: Call Graph Navigation Helps Increasing Code Maintenance Efficiency. [paper]
課程相關 連結網址 Course Website	http://soslab.nccu.edu.tw
備註 Remarks	**Teams** *Cloud Security (C-Team)* ● You will be familiar with Cloud Architecture/Implementation, Linux, KVMs, VMware, Shell script, Python, System breaches, VM Monitoring *App Security (A-Team)* ● You will be familiar with iOS, Android, Objective C, Java, Reverse Engineering, Binary Analysis, Bytecode Analysis, Hardoop/Distributed Computation, *Multimedia Security and Visualization (V-Team)* ● You will be familiar with multimedia encryption and decryption techniques, water marking techniques, open puff, Java, Python, Unity and etc.