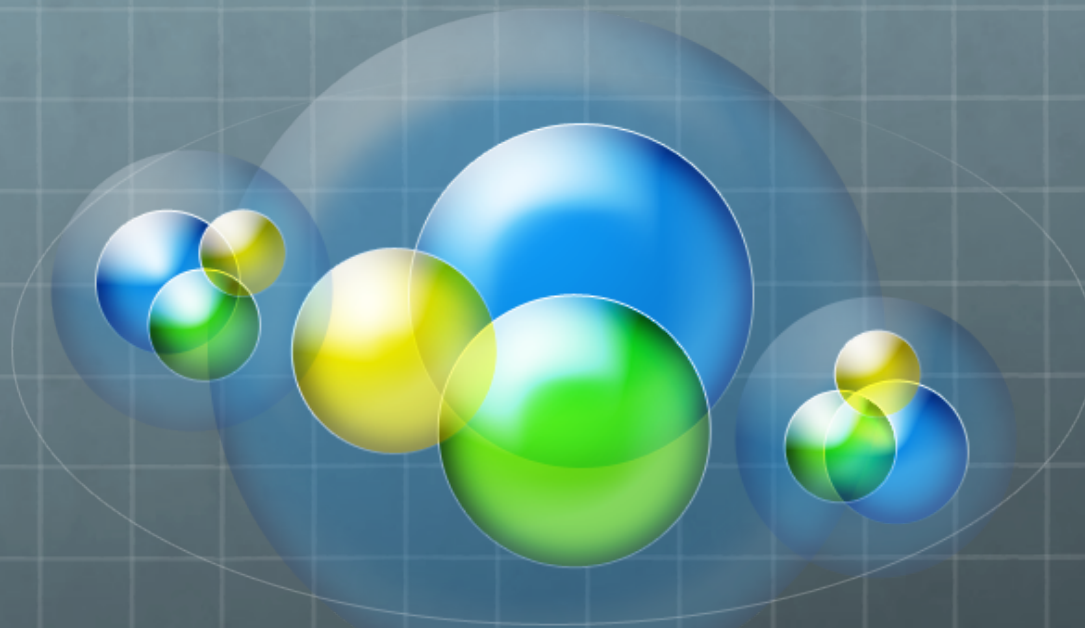




Advance Software Security

Fang Yu
Spring 2013



College of Commerce
National Chengchi University

Information

- Instructor: Fang Yu yuf@nccu.edu.tw
- Office: Health Center 4F 150409, ext.77457
- This is a 2 credit seminar-type course for graduate and undergraduate students
- Tuesday 2:10-4:00pm @ mis mac classroom (5F, Yi-Hsien Building)
- TAs: Shawn Lee and Steven Tai
- <http://sosl原因ab.nccu.edu.tw/Courses.html>

Objective

Give me some buzz words...

Cloud



Apps

SECURITY

Cloud can be compromised



Cloud Defense



White Hackers v.s. Black Hackers

- 🌐 We have implemented VIS, a Virtual Introspection System running on the KVM-based cloud system
- 🌐 The Black Team
 - 🌐 Collect and replay traditional attacks on VMs in a closed-environment guarded by the VIS system
- 🌐 The White Team
 - 🌐 Apply/Modify/Enhance VIS to detect abnormal behaviors of VMs, preventing system kernel and VMs from attacks

Catch the flag

- 🌐 Three round competition
 - 🌐 Black hackers present and replay attacks
 - 🌐 White hackers propose and implement defense with VIS
- 🌐 Winner gets extra 20% increase on the final grade



Apps may do more than
it appears



Analyze App Executable



From executable to system method calls

```
[ classRef_FBPageFansSet sel_stringWithFormat:]: 10  
[ classRef_FWLoadingOverlayView_0 sel_initWithFrame:]: 1  
[ classRef_TTMessageController_0 sel_initWithNibName:bundle:]: 1  
[ classRef_FWBaseWebViewController_0 sel_willAnimateRotationToInterfaceOrientation]: 1  
[ classRef_FBComposerTextView sel_initWithFrame:]: 1  
[ classRef_FBNotificationBar sel_initWithFrame:]: 1  
[ classRef_TTURLCache sel_cachePathWithName:create:]: 1  
[ classRef_FBAalytics sel_sharedInstance]: 41  
[ classRef_UIWindow sel_class]: 1  
[ classRef_NSMutableArray sel_allKeys]: 2  
[ classRef_FBTableLauncherNavigationBar sel_alloc]: 2  
[ classRef_TTStyledInline sel_alloc]: 2  
[ classRef_FBPhoto sel_photoWithPID:]: 7
```

White Hackers v.s. Black Hackers

- We have implemented AppBeach, the tool set that is able to resolve and count system calls of iOS executable
- The Black Team
 - Investigate and embed malicious behaviors in an iOS app
 - Collect online apps that may (or may not) have these behaviors
- The White Team
 - Apply/Modify/Enhance AppBeach to identify patterns of malicious behaviors
 - Reveal behaviors of online apps

Catch the flag

- 🌐 Three round competition
 - 🌐 Black hackers present malicious behaviors and online apps
 - 🌐 White hackers identify the patterns and analyze apps
- 🌐 Winner gets extra 20% increase on the final grade



To take this course

- 🌐 You need to join one team (white or black in cloud or app) before next week
- 🌐 Cloud Security: Shawn Lee (swlee@swlee.org)
 - 🌐 Cloud Black Team:
 - 🌐 Cloud White Team: T.B.A.
- 🌐 App Security: Steven Tai (100356023@nccu.edu.tw)
 - 🌐 App Black Team: T.B.A.
 - 🌐 App White Team: T.B.A.

Next week

- 🌐 Shawn will demo how to replay an attack in VMs and how VIS detects and prevents the attack
- 🌐 Steven will demo how to analyze an online app using AppBeach and reveal the behaviors of the app