

作品集

大學專題作品

作品名稱	使用技術	頁碼
Dark Killer	Android SDK、Java Multithreading、Java Socket	1
Random It	Visual Basic、MySQL	2
彩色泡泡	Java Multithreading	3







研究所系統開發專案

作品名稱	使用技術	頁碼
Packet Mangling	Linux Kernel Module、Kernel Netfilter Framework	3
Optimized Qemu	C、linked list、IBTC hash table、shadow stack	4
分散式惡意軟體分析系統	Java、Cuckoo Sandbox	4
碩士論文	QEMU+KVM、Windows API hooking、x64 Assembly	5

作品集說明

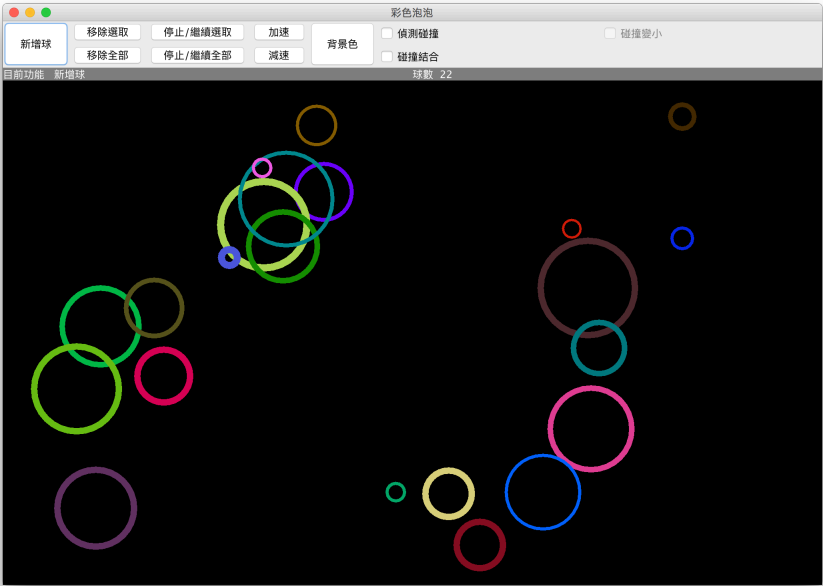
Android Game – Dark Killer

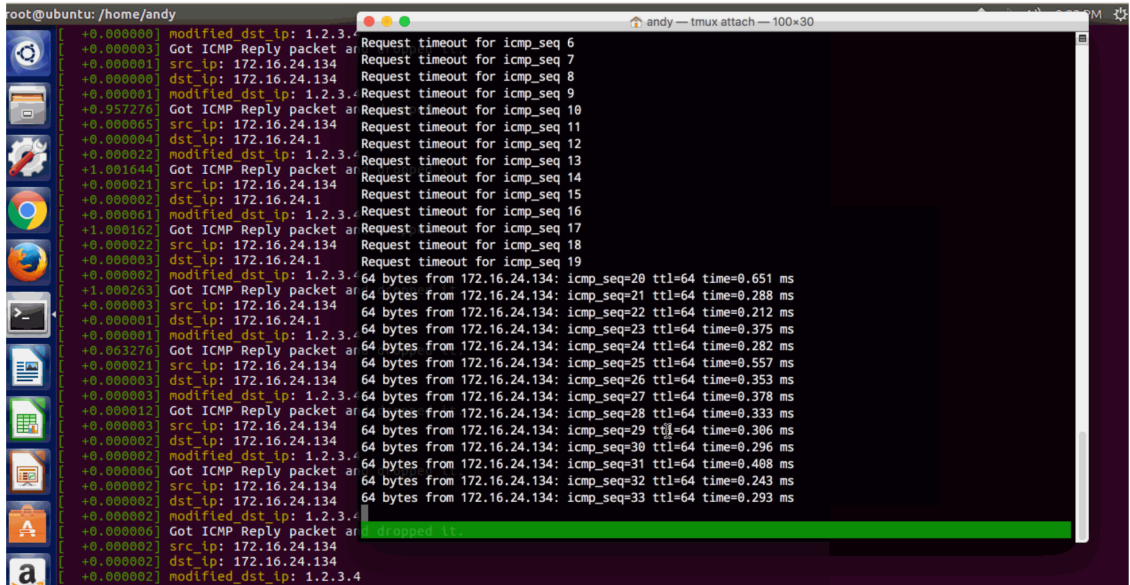
開發目標	目前市面上的手機 APP 遊戲，種類偏向於單機遊戲或是網路連線遊戲，較少桌遊類型的互動性遊戲，我們創造出擁有極高互動性，且舒適使用、容易上手的桌遊手機 APP 遊戲。使用者互動性高、簡單易用，容易上手，不須倚靠 3G 網路，以行動基地台與 Wifi 連結方式進行遊戲，身歷其境的音效及動畫效果		
使用技術	Android SDK、Java Multithreading、Java Server & Client Socket		
Github	https://github.com/a110605/darkkiller		
Slides	https://www.slideshare.net/andy149/dark-killer-app-presentation-slides		
系統截圖	 <p>Figure 1 遊戲進入畫面</p>	 <p>Figure 2 開始畫面</p>	 <p>Figure 3 人物說明</p>

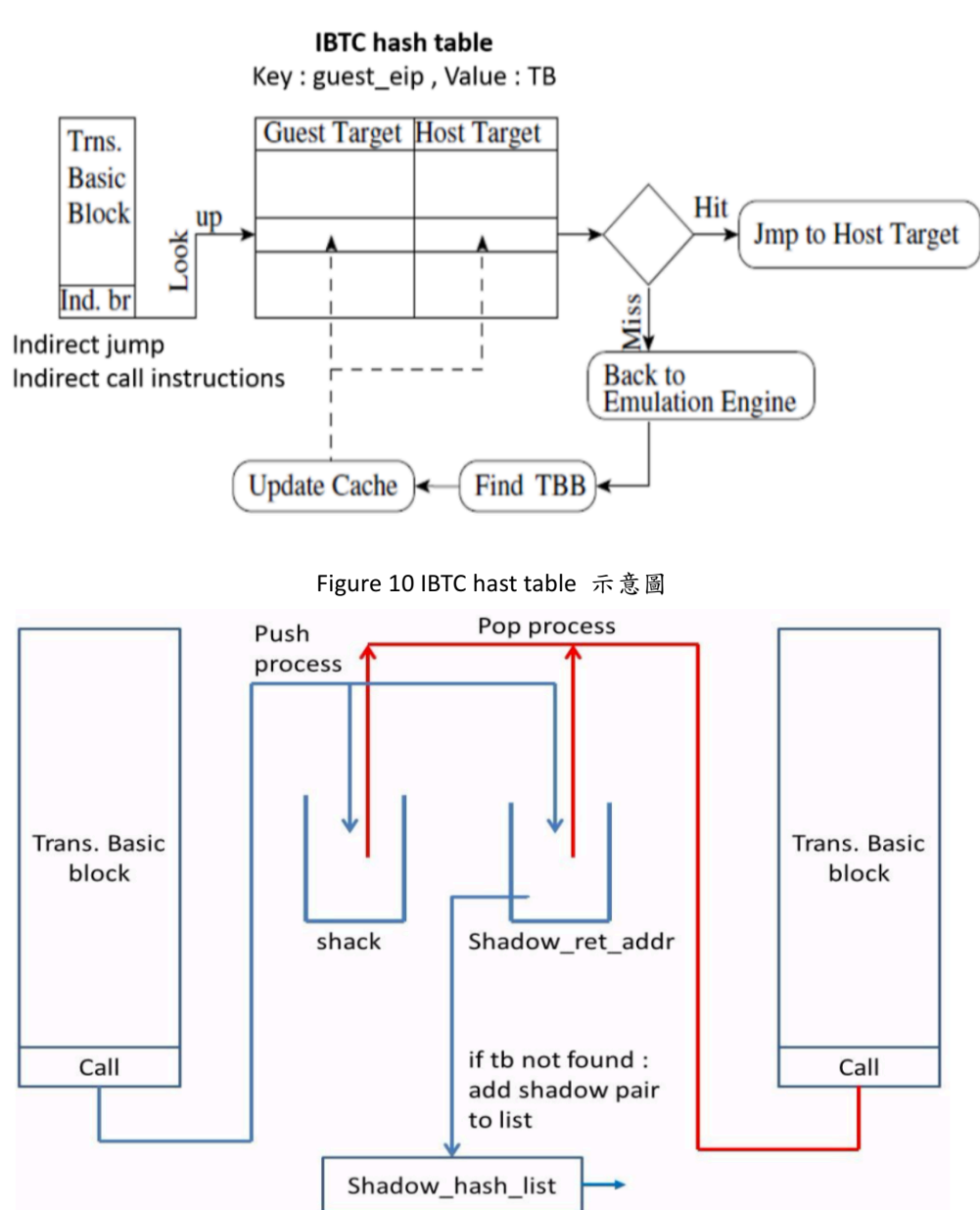
			
			

Random It – 自動點餐推薦系統

開發目標	鑒於中大學生每天面臨不知道要吃什麼的困擾，我們運用 VB 語言打造中大校園食物目錄統合，解決同學不知道要吃什麼的煩惱。功能包含隨機推薦早餐午晚餐店家與菜色，同時提供價格比對與查詢，再加上有趣的【菜餚格鬥小遊戲】增加使用者趣味性。
使用技術	MySQL、Visual Basic
系統截圖	

彩色泡泡 - Color Bubbles	
開發目標	模擬 Windows 螢幕保護程式可產生多種顏色大小的泡泡，並可選擇【碰撞結合】、【碰撞縮小】、【加速】、【減速】等功能。
使用技術	JAVA Multithreading
Github	https://github.com/a110605/colorbubble
系統截圖	

Packet Mangling – A self-made linux kernel module	
開發目標	撰寫 kernel module 採用 netfilter framework 攔截網路封包並竄改其內容
Github	https://github.com/a110605/packet_mangling
使用技術	Linux Kernel Module、Kernel Netfilter Framework
系統截圖	

Optimized Qemu	
系統目標	修改 qemu-0.13.0 source code 實作 indirect branch handling optimization methods 以增進 instruction branch 效能
Github	https://github.com/a110605/optimized-qemu
使用技術	C、linked list、IBTC hash table、shadow stack
系統截圖	 <p>The diagram illustrates the IBTC hash table and shadow stack mechanisms. The top part shows the IBTC hash table with keys as guest_eip and values as TB. It details the lookup process for indirect jump and call instructions, leading to a hit (jump to host target) or a miss (back to emulation engine, then find TBB and update cache). The bottom part shows the shadow stack mechanism, including push and pop processes, a shadow return address, and a shadow hash list for handling cases where a TB is not found.</p> <p>Figure 10 IBTC hash table 示意圖</p> <p>Figure 11 shadow stack 示意圖</p>

Cuckoo Sandbox - A Distributed Malware Analysis System	
系統目標	將現有 cuckoo framework 做成分散式系統以減少惡意軟體分析時間，當使用者於網頁上提交惡意軟體樣本後，透過 master agent 將樣本分散給不同的 slave 上進行樣本分析，產出 sample report 後由 slave agent 回傳給 master
Github	https://github.com/a110605/cuckoo_agent

使用技術	Java Socket 、 Cuckoo Sandbox
系統截圖	<div><p style="text-align: center;">Distributed System of Cuckoo Sandbox</p><p style="text-align: center;">Figure 15 分散式 Cuckoo 系統架構圖</p></div>

碩論 Enabling VMI-based Memory Inspection for Runtime Protection in KVM	
目標	在 QEMU+KVM 中實作虛擬機器內省側錄技術(VMI)，實現對 VM 內程式呼叫的 Windows API 進行 Profiling，使用者透過 QEMU 命令列指定一執行中 process name，開始側錄其所呼叫 Windows APIs 的參數值與回傳值，並將其紀錄成檔案，以供後續分析之用
Slides	https://www.slideshare.net/secret/xgnVDtUz5sHdgl
使用技術	C、QEMU+KVM、Windows API hooking、x64 Assembly
系統截圖	<div><p style="text-align: center;">System Architecture</p><p style="text-align: center;">Figure 16 論文系統架構圖</p></div>