以動態認證模組反制MMORPG機器人程式

陳凱嶸

et3w503@yahoo.com

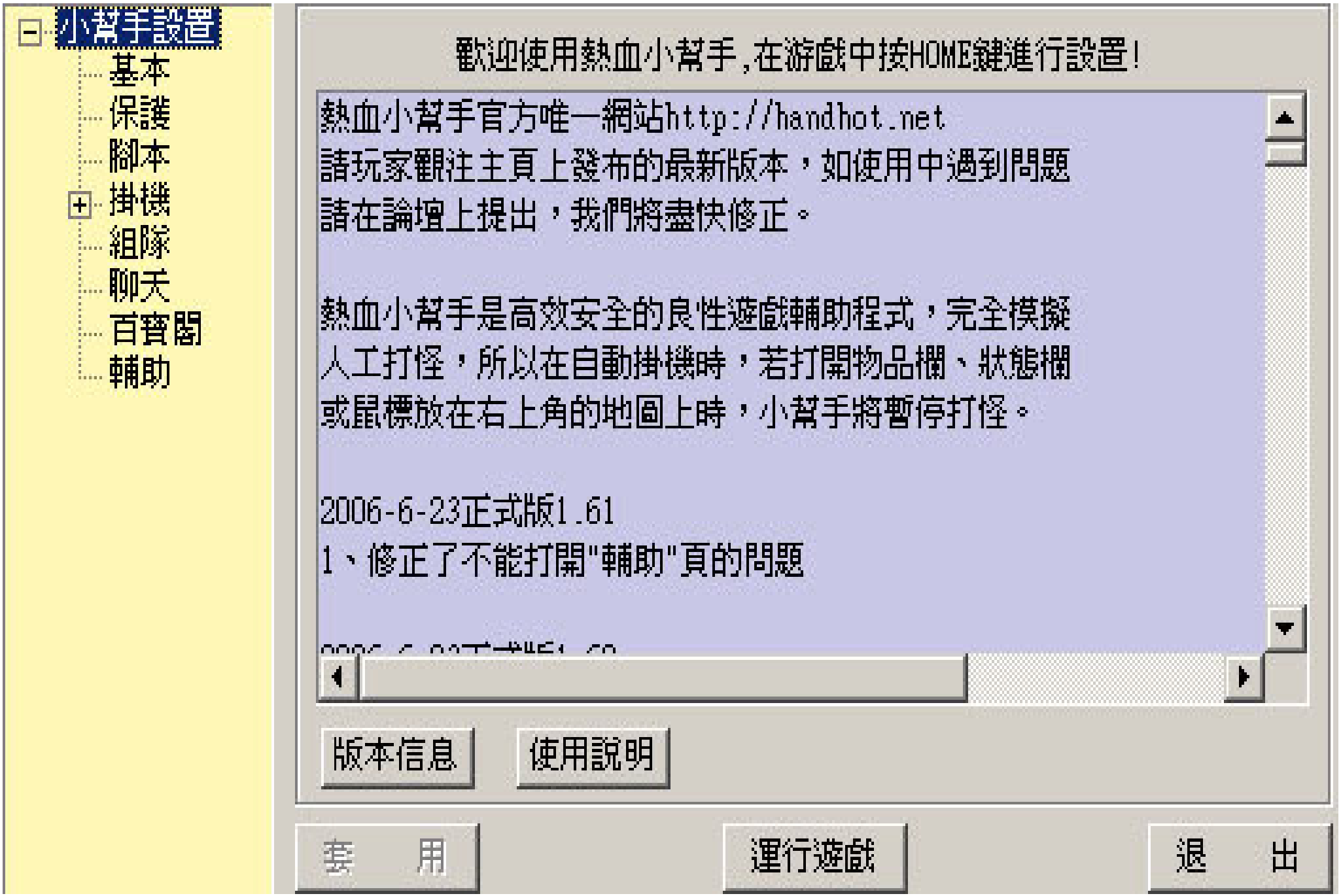
WAYI INTERNATIONAL DIGITAL ENTERTAINMENT CO., LTD.

HIT Conference 2007


玩家可以在一般頻道輸入/喜 /怒 /哀 /樂 即可變換表情
可快速升等
飛雲：請問有什麼門主說沒修練風功不能接lv10任務
公告：23:00-24:00華義國際3d人員在中原5及中原6線上限時玩家
逍遙聖神：野豬快開謝阿
公告：玩家可以在一般頻道輸入/喜 /怒 /哀 /樂 即可變換表情
F2
F3
F4
F5
F6
F7
F8
F9
F10

機器人程式(Bots)的分類

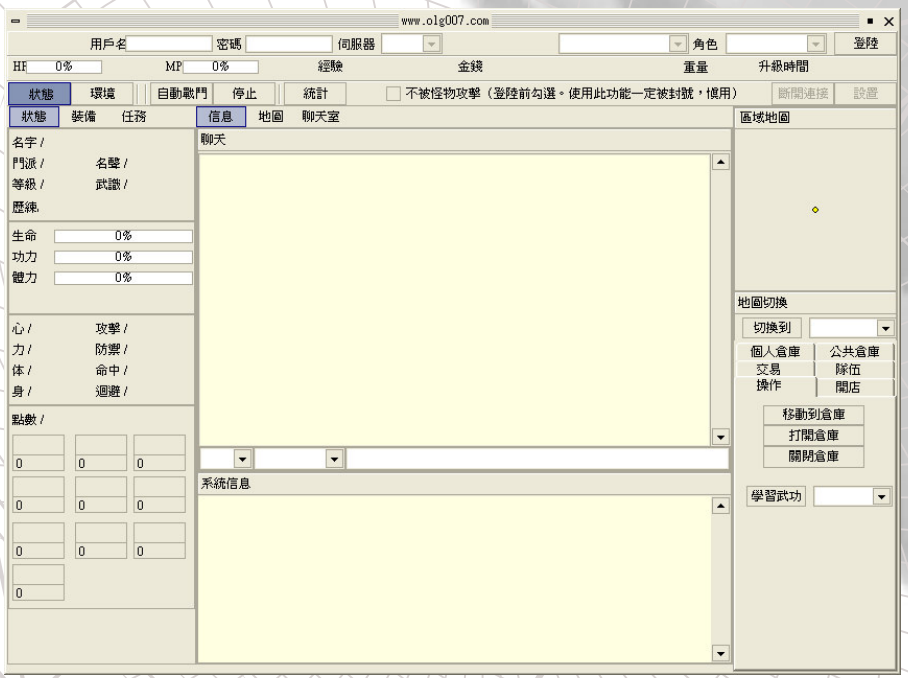
- Hook Bots(內輔，外掛)
  - 業餘高手即興創作
    - Windows Hooks: EzScript,QMACRO
    - API/Socket Hooks: WPE
  - 專業開發團隊
    - 小幫手


小幫手設置
基本
保護
腳本
掛機
組隊
聊天
百寶閣
輔助
歡迎使用熱血小幫手,在游戲中按HOME鍵進行設置!
熱血小幫手官方唯一網站http://handhot.net
請玩家觀注主頁上發布的最新版本，如使用中過到問題
請在論壇上提出，我們將盡快修正。
熱血小幫手是高效安全的良性遊戲輔助程式，完全模擬
人工打怪，所以在自動掛機時，若打開物品欄、狀態欄
或鼠標放在右上角的地圖上時，小幫手將暫停打怪。
2006-6-23正式版1.61
1、修正了不能打開"輔助"頁的問題
版本信息
使用說明
套　用
運行遊戲
退　出

機器人程式(Bots)的分類

- Standalone Packet Bots(脫機版外掛)
  - 專業開發團隊
    - 熱血特工　2005/10/05 ~ 2007/01/05
    - 熱血八方　2005/10/22 ~ 2006/07/03
    - 熱血戰神　2005-11-11 ~
    - 熱血征服者 2006/03/24 ~
    - 熱血幽靈

熱血特工

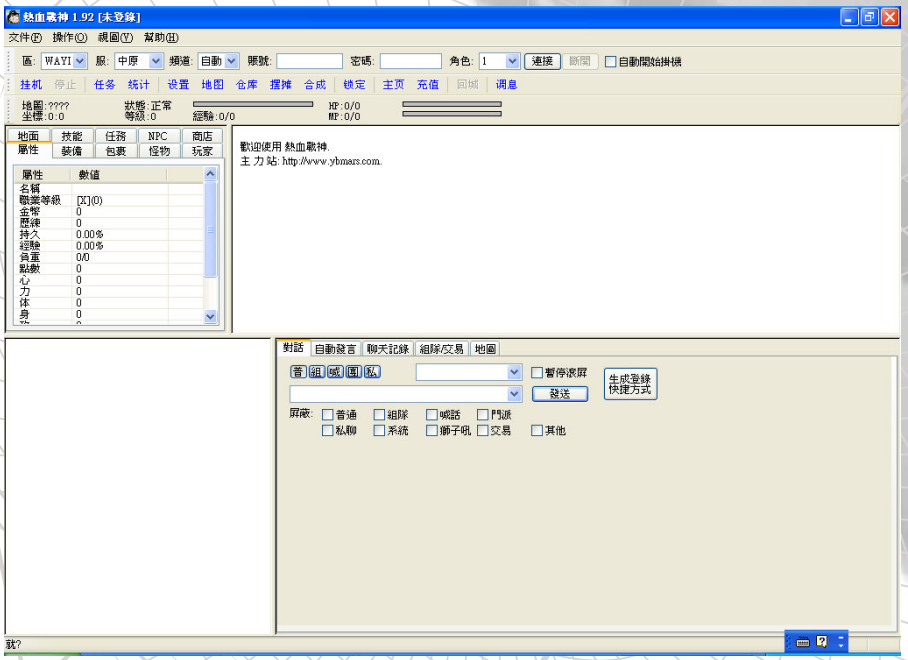


- 第一個進行收費的脫機版外掛
- 停止更新
- 目前尚可以順利進入遊戲

熱血八方

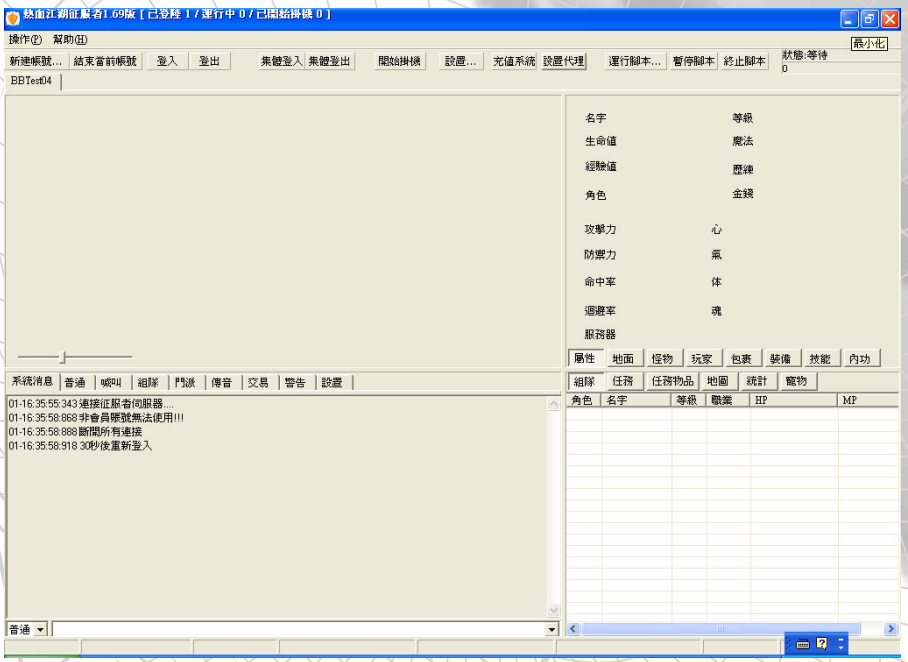
- 臺灣網咖到大陸進行『投資』
- 曾經親自跑到臺灣代理商提『合作案』
- 已經退出市場

熱血戰神



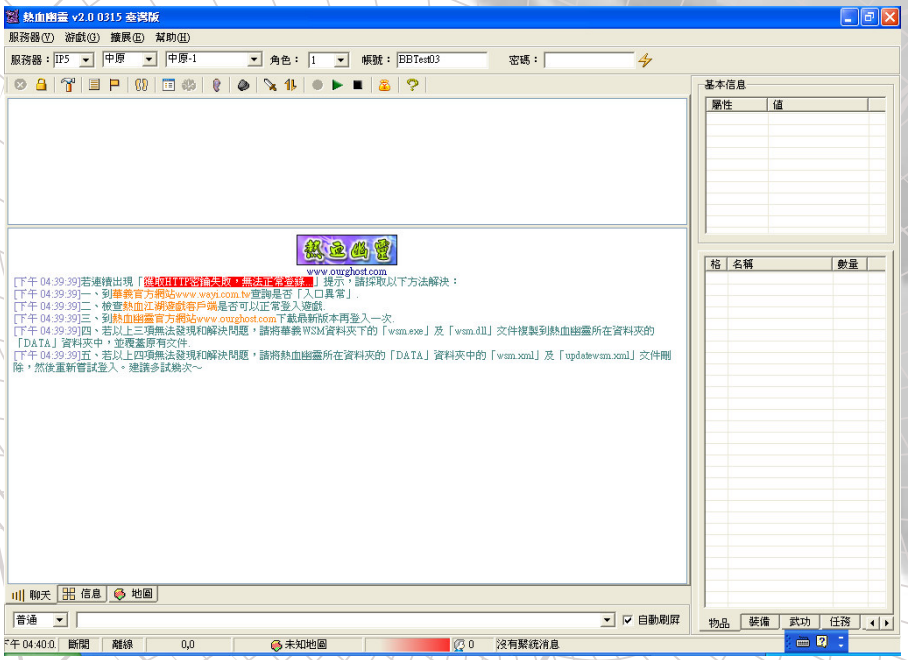
- 市佔率第一的脫機版外掛
- 72小時內一定破解
- 客戶服務周到
- 無法掛機會補償天數
- 目前已提出法律訴訟

熱血征服者



- 市佔率第二的脫機版外掛
- 2006/3/24投入市場
- 投入多種遊戲的脫機版外掛研發

熱血幽靈



- 曇花一現
- 臺灣外掛代理商與大陸外掛研發商有所爭議

各種Bots的比較

	針對熱血江湖開發	使用技術	每台電腦最大用戶數	反制方式
EzScript	NO	Windows Hooks	<5	Windows Hooks
QMACRO	NO	Windows Hooks	<5	Windows Hooks
WPE	NO	Socket/API Hooks	<5	Kernel Network Entry
小幫手	YES	Windows Hooks & Socket/API Hooks	<5	Signature Based Detection
熱血特工	YES	Packet Analysis	>20	動態認證模組
熱血八方	YES	Packet Analysis	>20	動態認證模組
熱血戰神	YES	Packet Analysis	>20	動態認證模組
熱血征服者	YES	Packet Analysis	>20	動態認證模組
熱血幽靈	YES	Packet Analysis	>20	動態認證模組

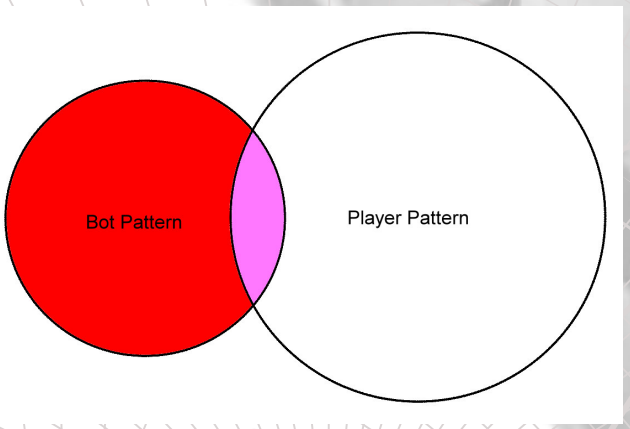
Bots反制方法-CAPATCHA

Microsoft Passport

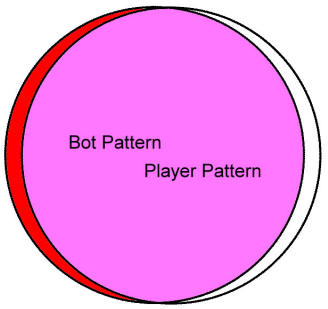
Yahoo

- 優點
  - Web目前大量使用
- 缺點
  - 干擾正常玩家
  - 圖型不容易辨識
- 破解
  - 影像辨識

Bots反制方法-Traffic Analysis



反制前



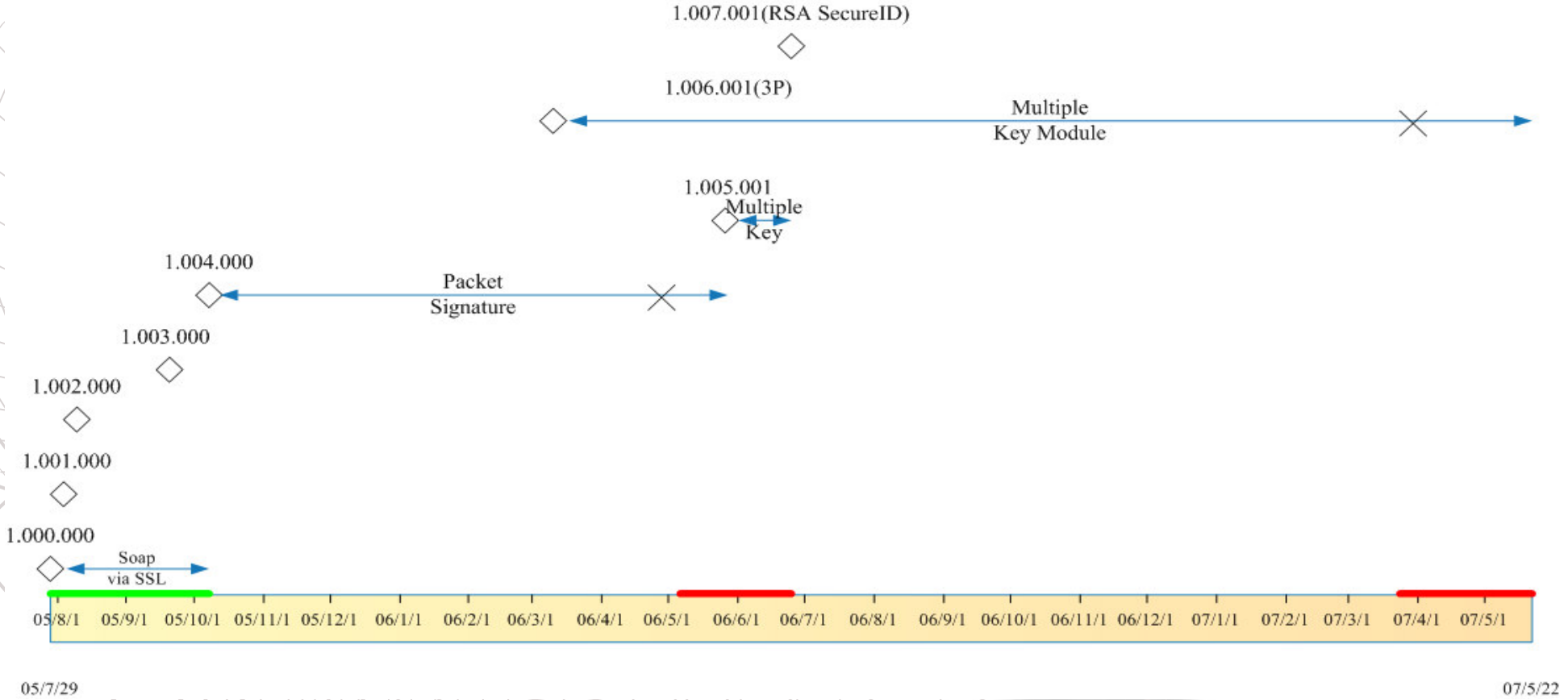
反制後

- 優點
  - Identifying MMORPG Bots: A Traffic Analysis Approach
- 缺點
  - 難以舉證
  - 無法對抗專業Bots
- 破解
  - 模仿使用者的行為

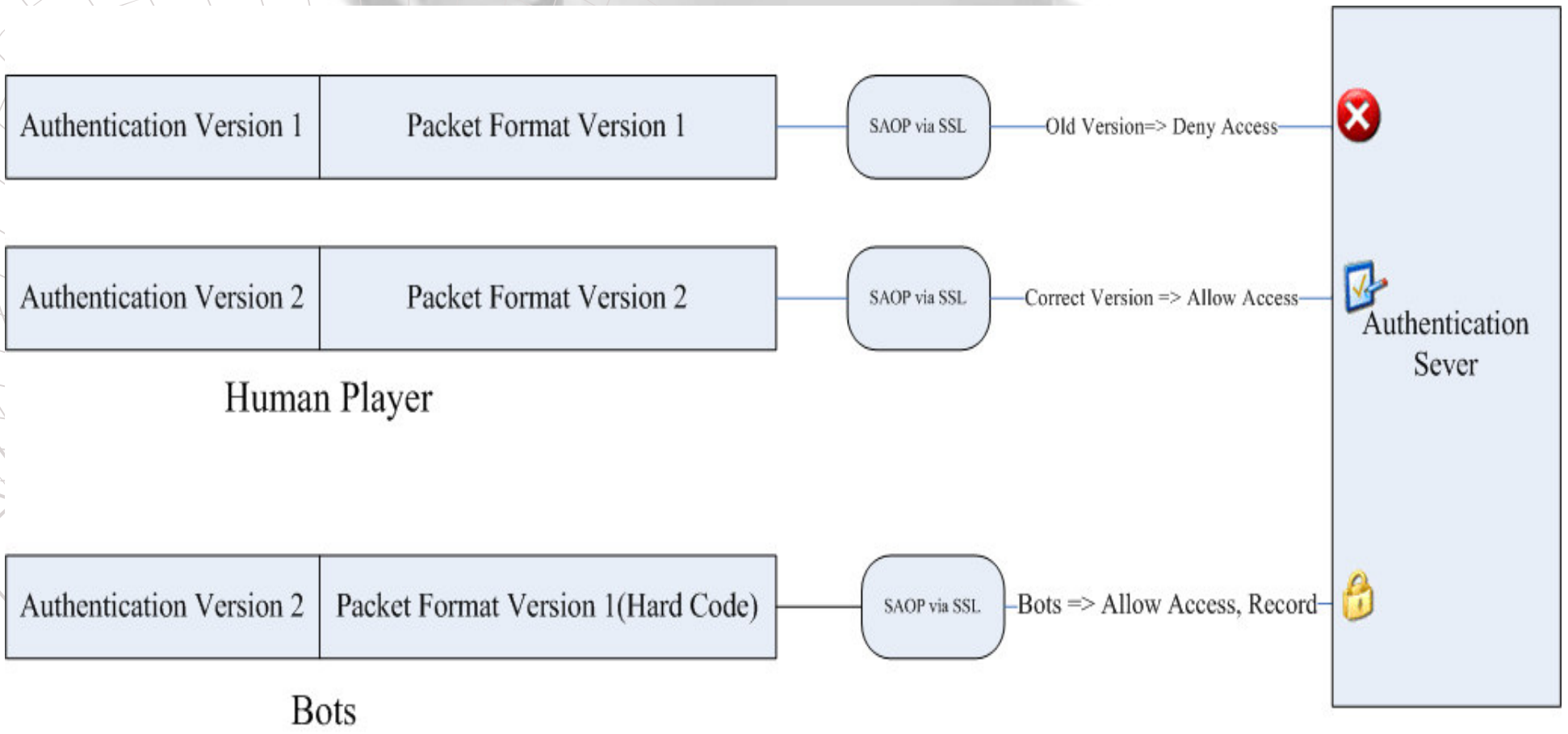
Bots反制方法-Signature Based Detection

- 與主流防毒軟體(Anti-Virus)方法相同
- 優點
  - 有專業的廠商提供服務
- 缺點
  - 必需緊盯著Bots更新
  - 對於脫機版無效
- 破解
  - 加殼與改變特徵

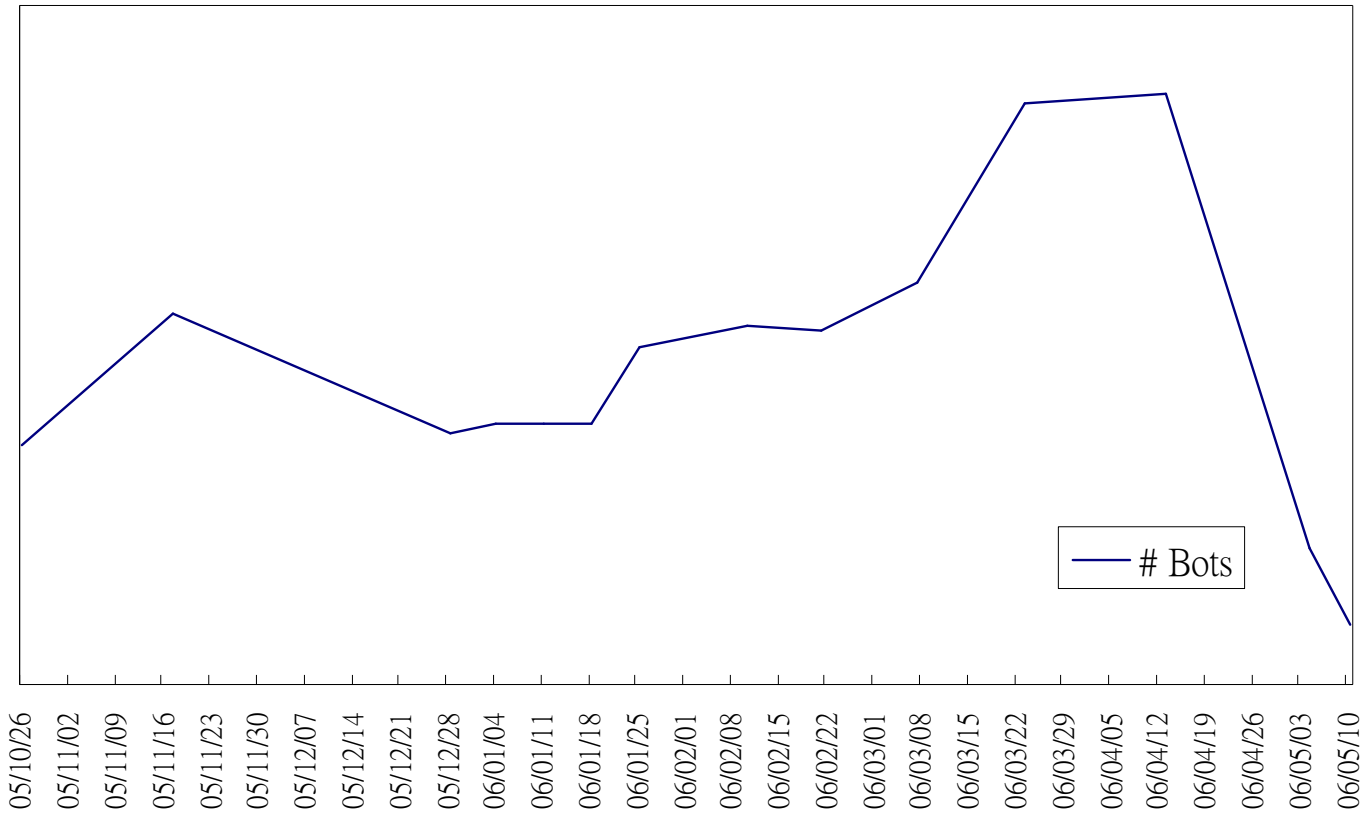
對抗Bots的Roadmap



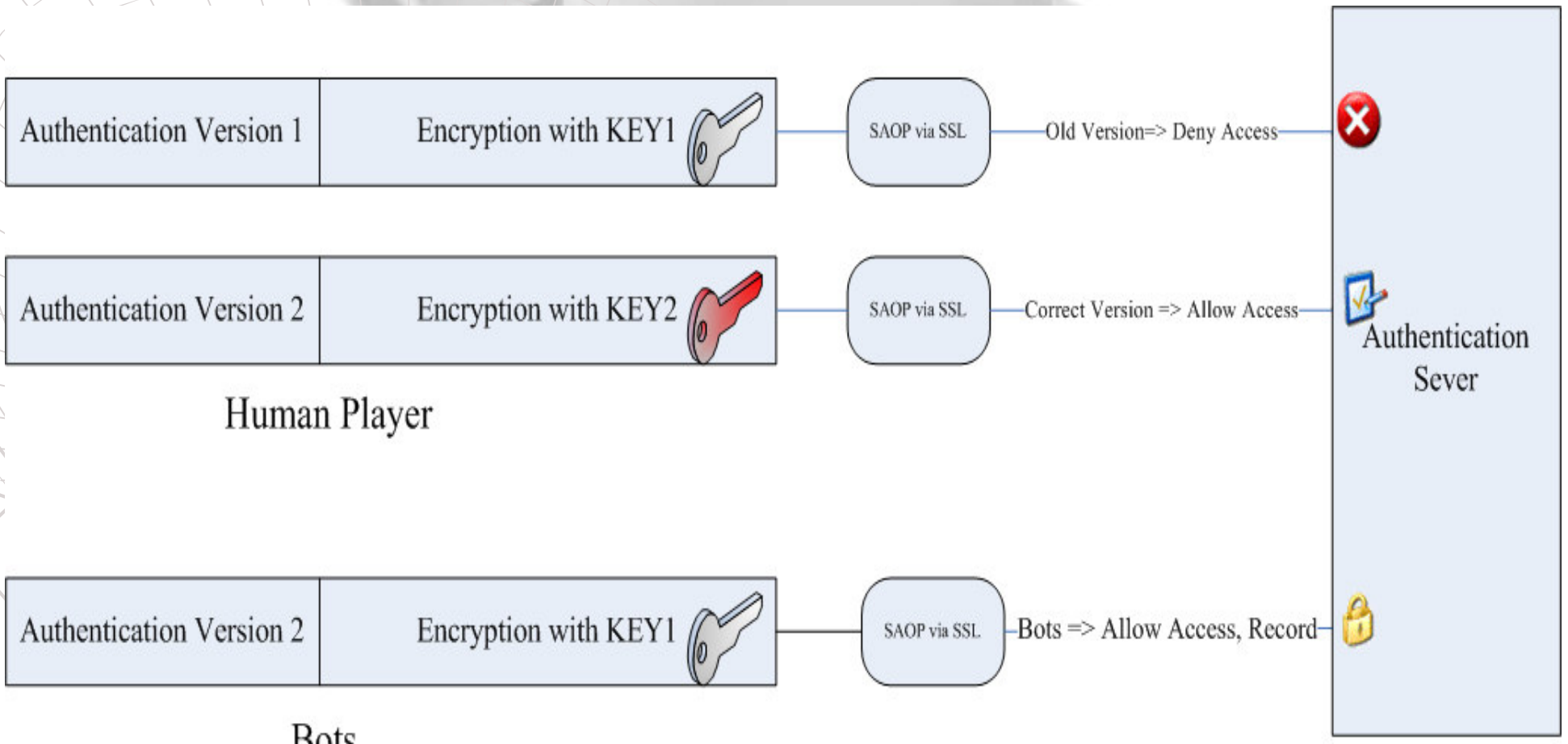
以封包特徵來辨識MMORPG機器人程式



以封包特徵辨識機器人程式使用者數量的歷史記錄



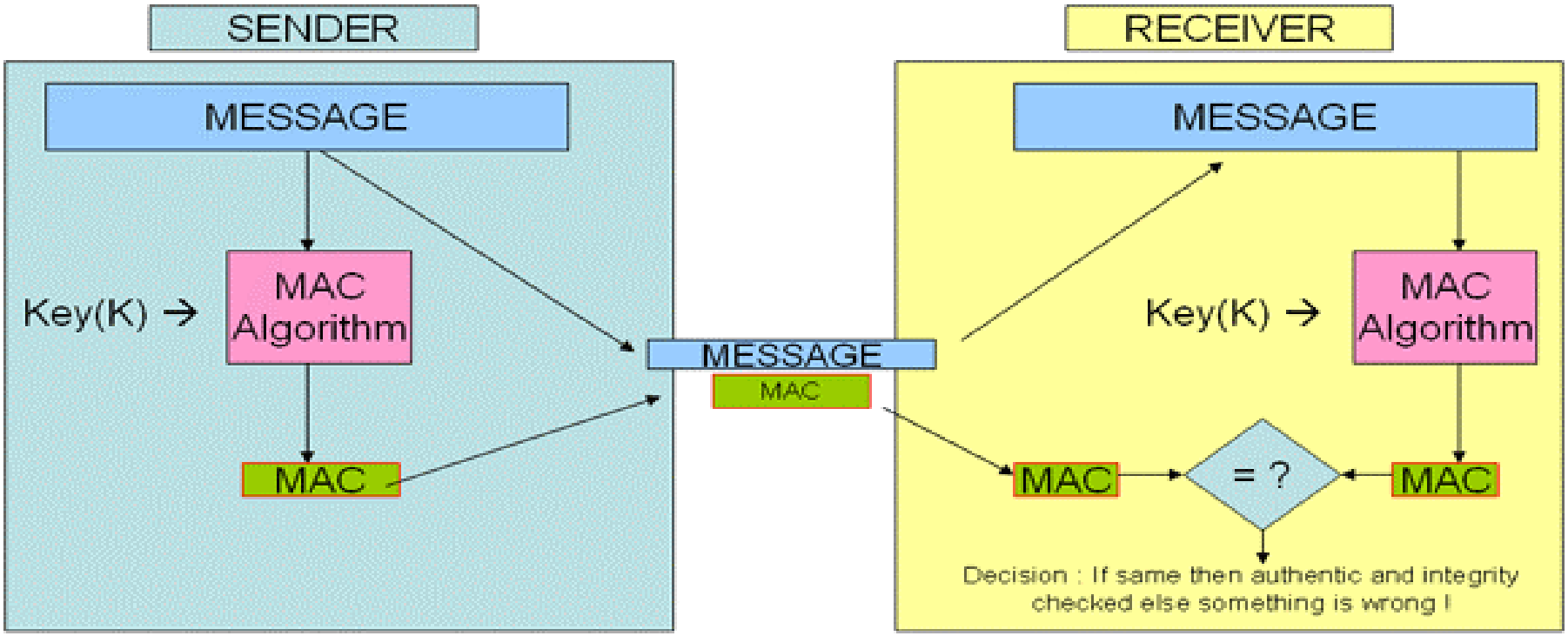
以多重密秘金鑰來辨識MMORPG機器人程式



以動態認證模組反制MMORPG機器人程式

- 天下武功，無堅不摧，唯快不破
- 再高的招術終究會被破解
  - 加殼保護
  - Signature Base Detection
  - 數位簽章
- 迅速反應才是正途
  - 出招一定會被破解
  - 多久之後能出下一招?

訊息鑑識碼技術

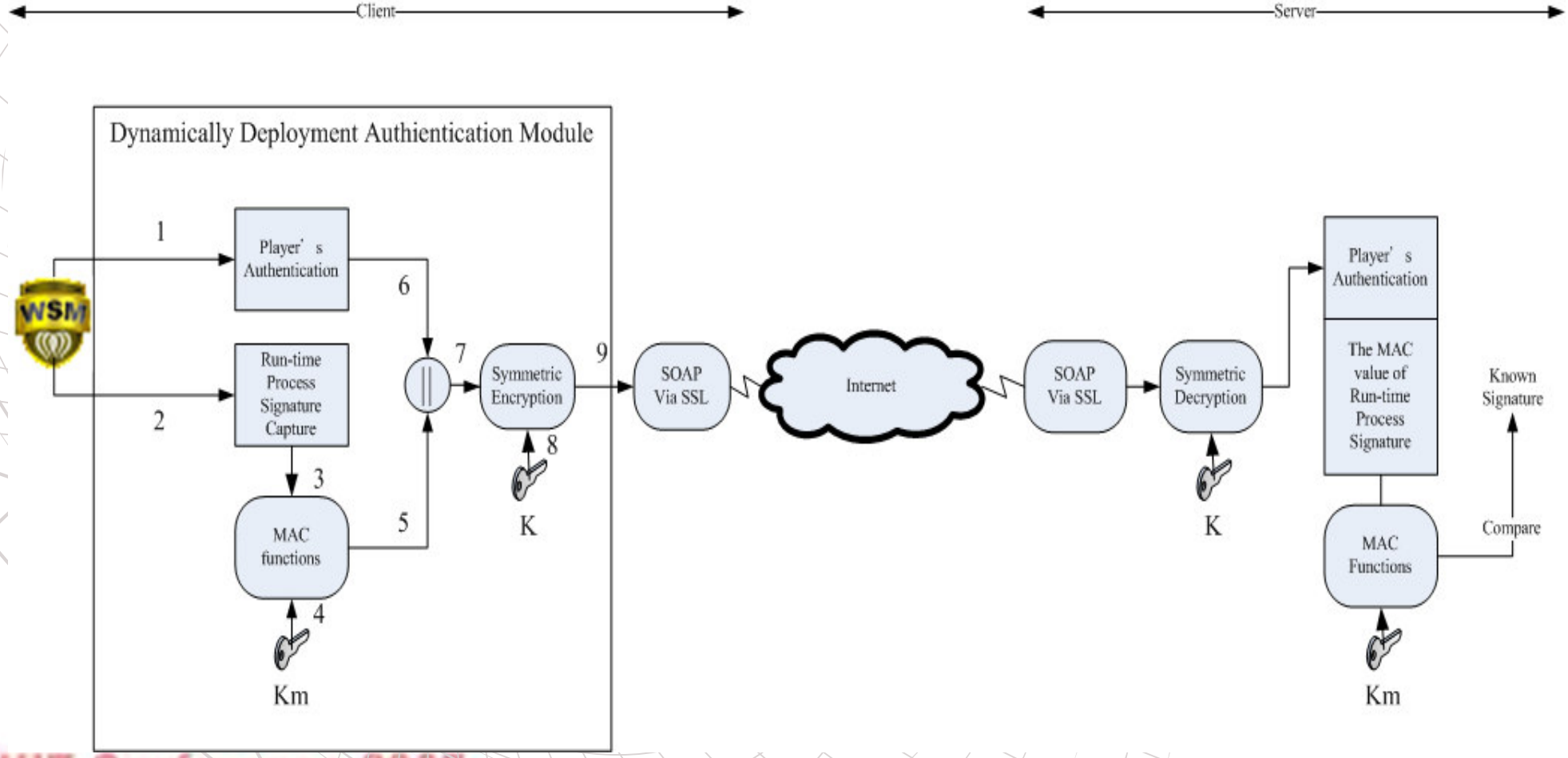


MAC – Message Authentication Code

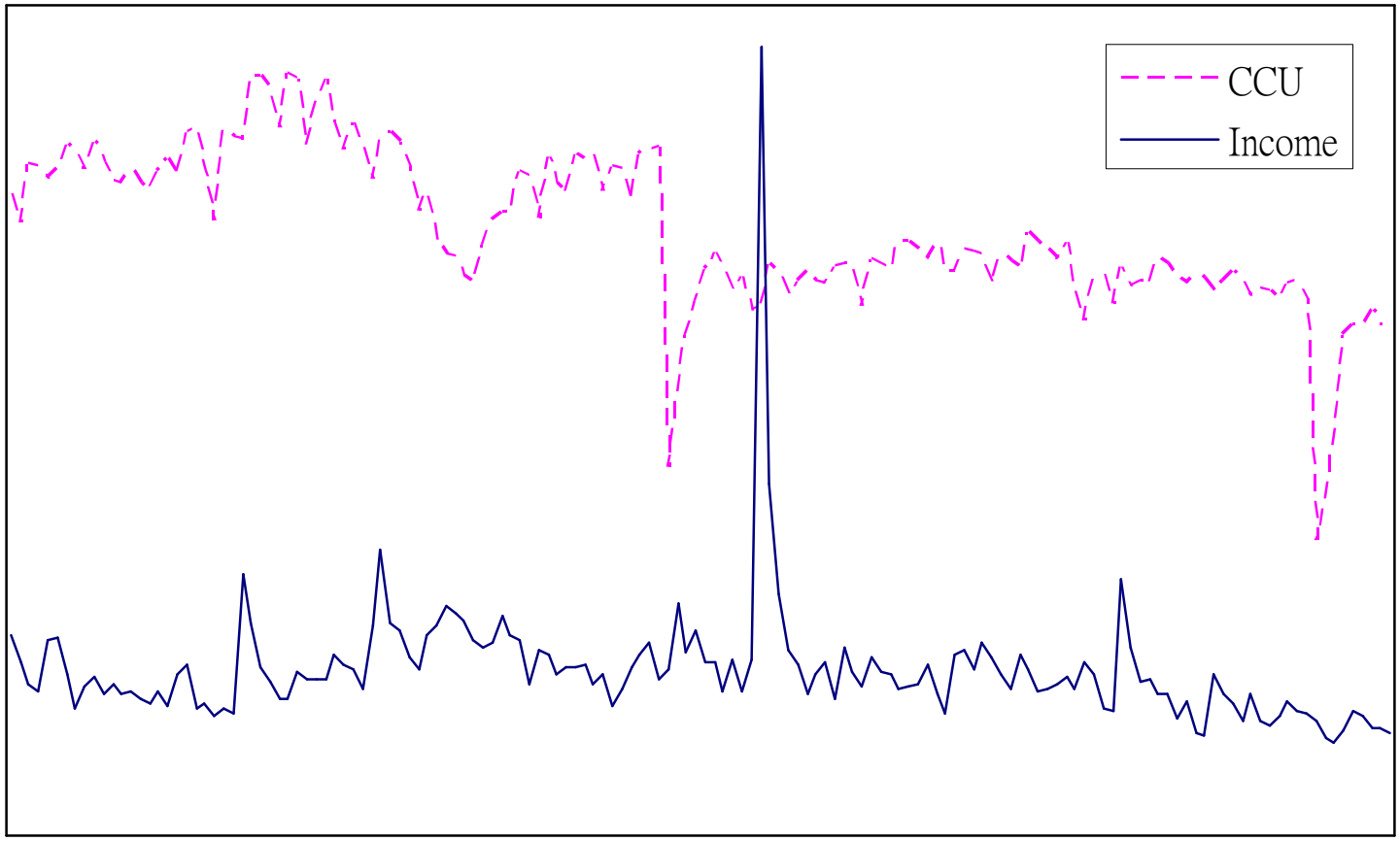
動態認證模組

- MAC系統的變型
  - 不同的程式執行時期的程式區段必然不同
  - MAC系統用來辨識Run-time Process Signature
  - 抓取的特徵區段由我們指定
- 結合身份認證
  - 沒有認證無法進行遊戲，Bots一但使用模組，特徵就會被我們所辨識
- 模組隨時動態發佈
  - 對抗專業Bots研發者的逆向工程技術

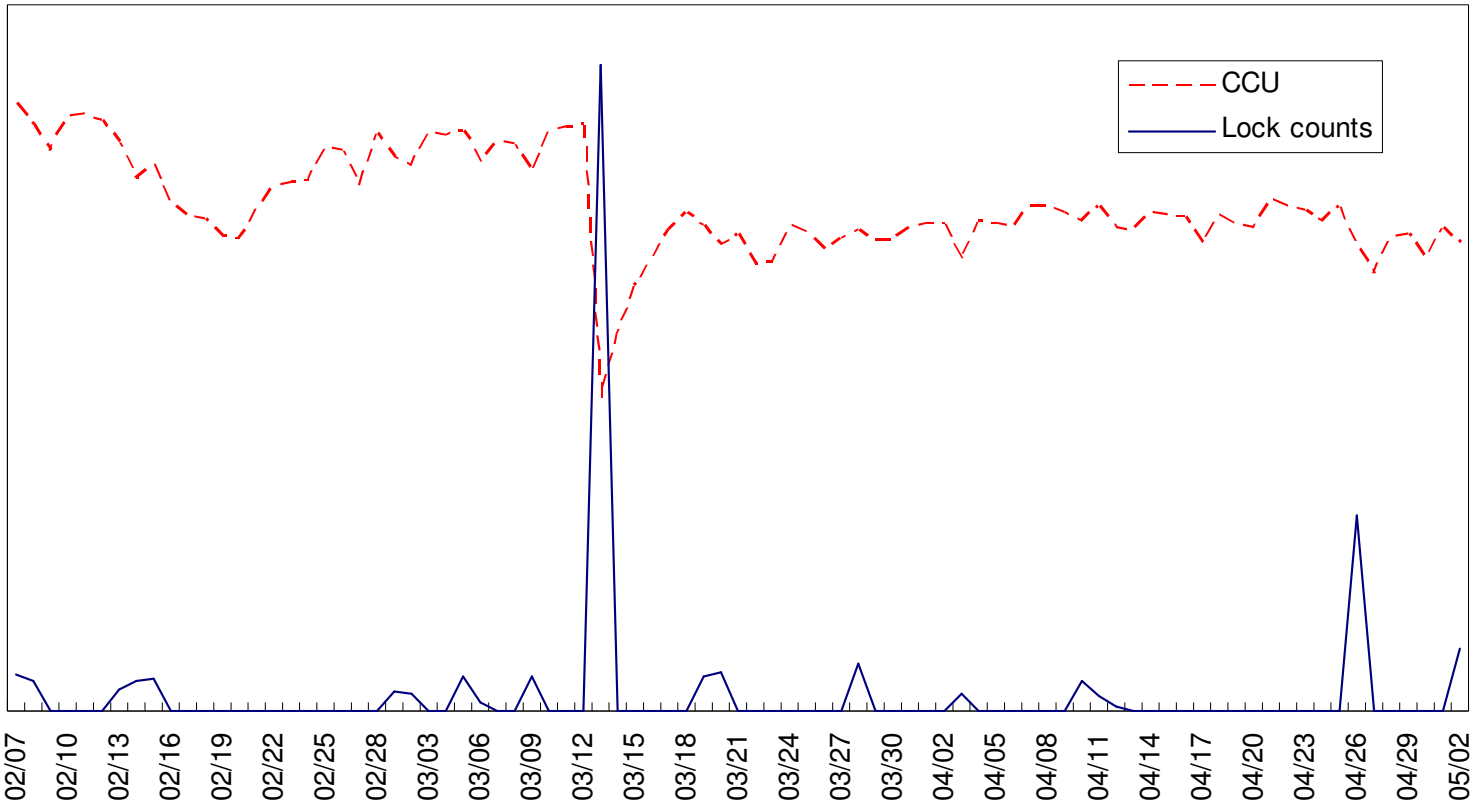
結合玩家身份認證與客戶端程式辨識的動態認證模組技術



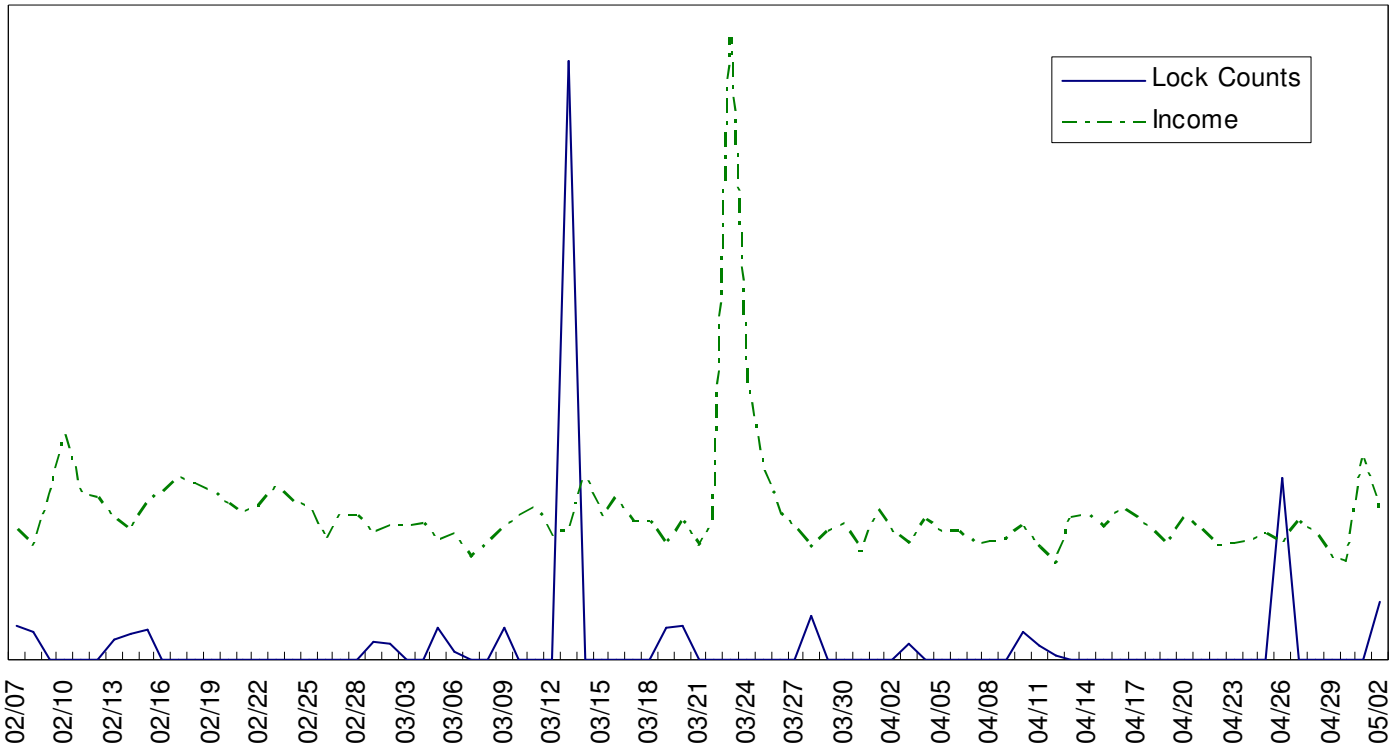
2007年上半統計數據



採取反制措施的統計數據



採取反制措施的統計數據



成效

- 2007年上半年同時上線人數曲線與消費數據相關系數是0.0477
- 2007年2月-5月停權人數與同時上線人數，相關系數是-0.3951
- 2007年2月-5月停權人數與消費數據,相關系數是-0.0643
- 2007年以1月份與5月份來比較，熱血江湖同時上線人數下降了22.37%，消費數據大概只下降了16.89%

實作的議題

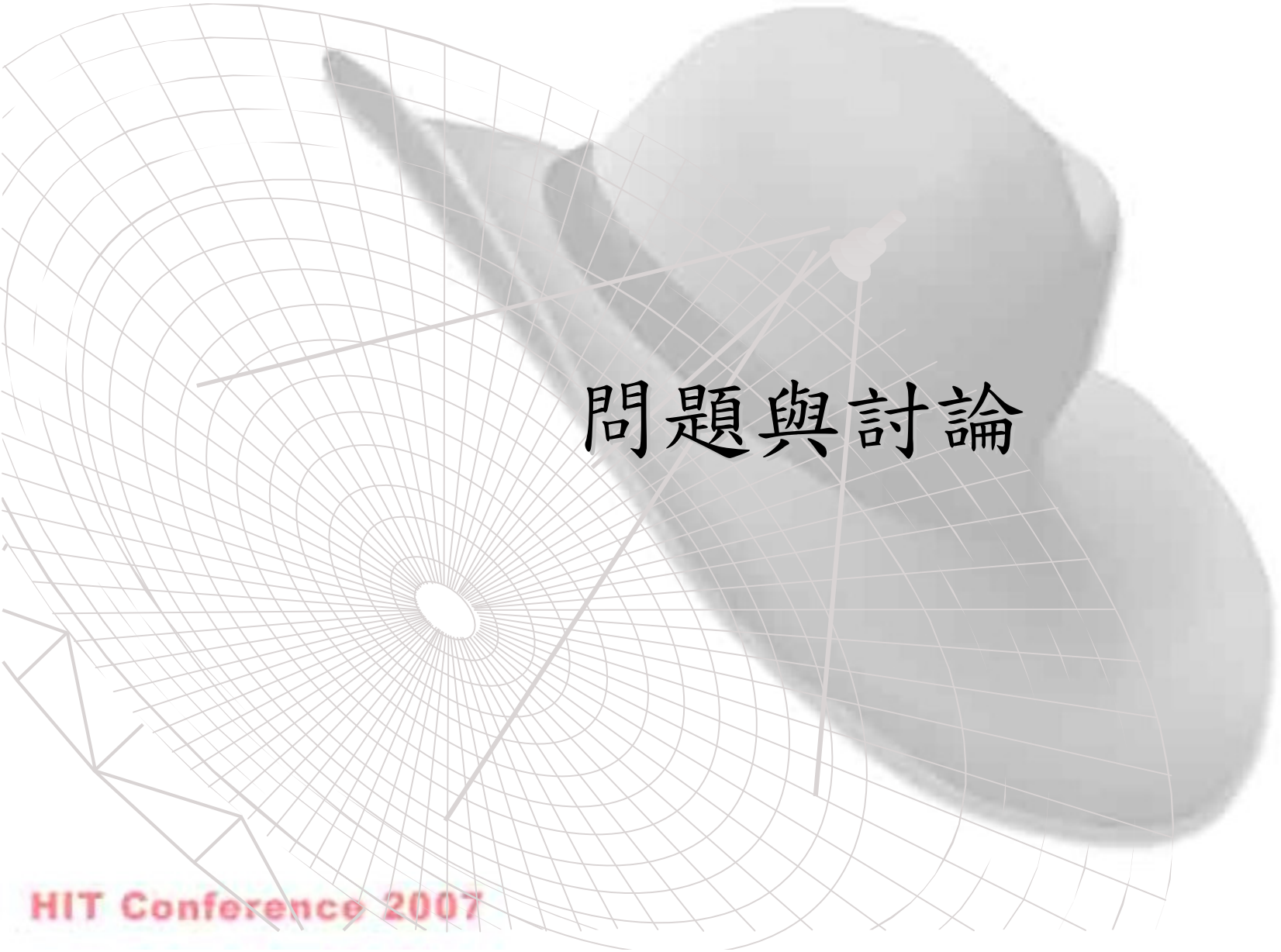
- Run-time Process Signature必需是能夠精確辨識而不會隨著執行環境改變的特徵
- One-Way Hash Collisions(MD5,SHA1)
- 金鑰被以逆向工程的方式解讀出來
- 加密演算法被重製

結論

- Traffic Analysis
  - 使用統計的方法
  - 舉證不容易
- CAPATCHA
  - 人工智慧的難題
  - 干擾正常使用者
- Signature Based Detection
  - 使用Anti-virus同樣的方式
  - 無法對付脫機版

以動態認證模組反制MMORPG機器人程式

- 密碼學理論: 使用MAC鑑識是否為官方發行的客戶端, 幾乎不會誤判.
- 動態發佈模組: 反制逆向工程
- 與身份認證結合: 迫使Bots必需使用模組



問題與討論