

# 指令型遠控軟體輕鬆談

簡報者

**Kelp**

**kelp@phate.tw**

HIT Conference 2008

# 簡介

u 了解指令型遠端操控軟體的基本架構

HIT Conference 2008

# 訓練大綱

u 單元 1：何謂遠控軟體

u 單元 2：遠控軟體分析

u 單元 3：總結

HIT Conference 2008

# 單元 1：何謂遠控軟體

- u 能夠控制遠端電腦的軟體都能稱為遠端操控軟體。
- u 遠控軟體大部分透過網路進行遠端電腦控制。

HIT Conference 2008

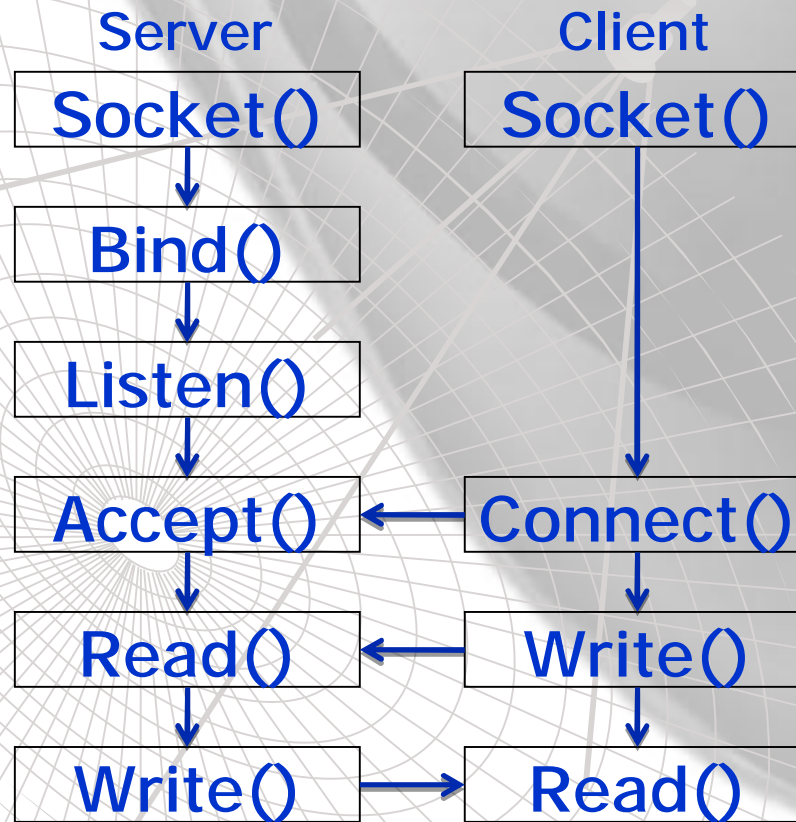
# 單元 1：何謂遠控軟體

木馬  
後門  
VNC  
.....

HIT Conference 2008

# 單元 2：遠控軟體分析

如何連線?



HIT Conference 2008

# 單元 2：遠控軟體分析

如何連線？

反向連結

一般木馬都使用這種連線方式。

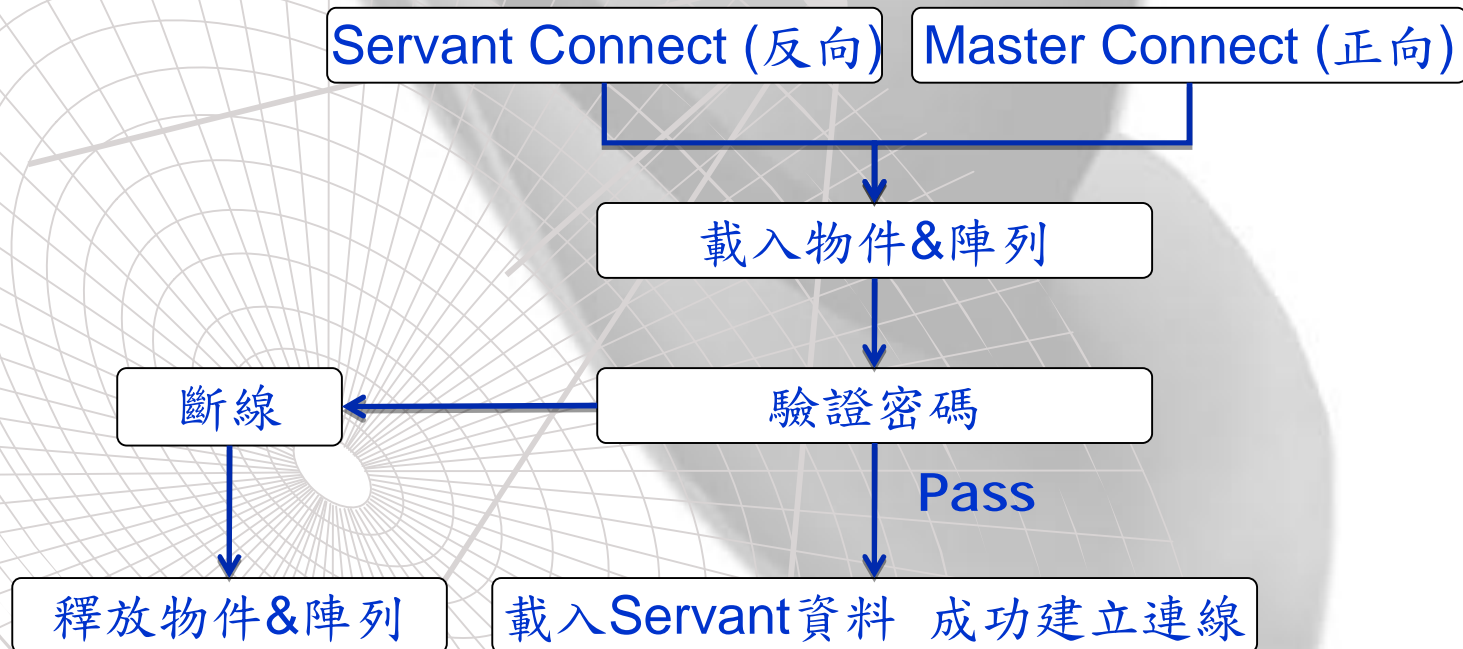
正向連結

遠端桌面就是用此方式連結。

HIT Conference 2008

# 單元 2：遠控軟體分析

## 如何連線?



HIT Conference 2008



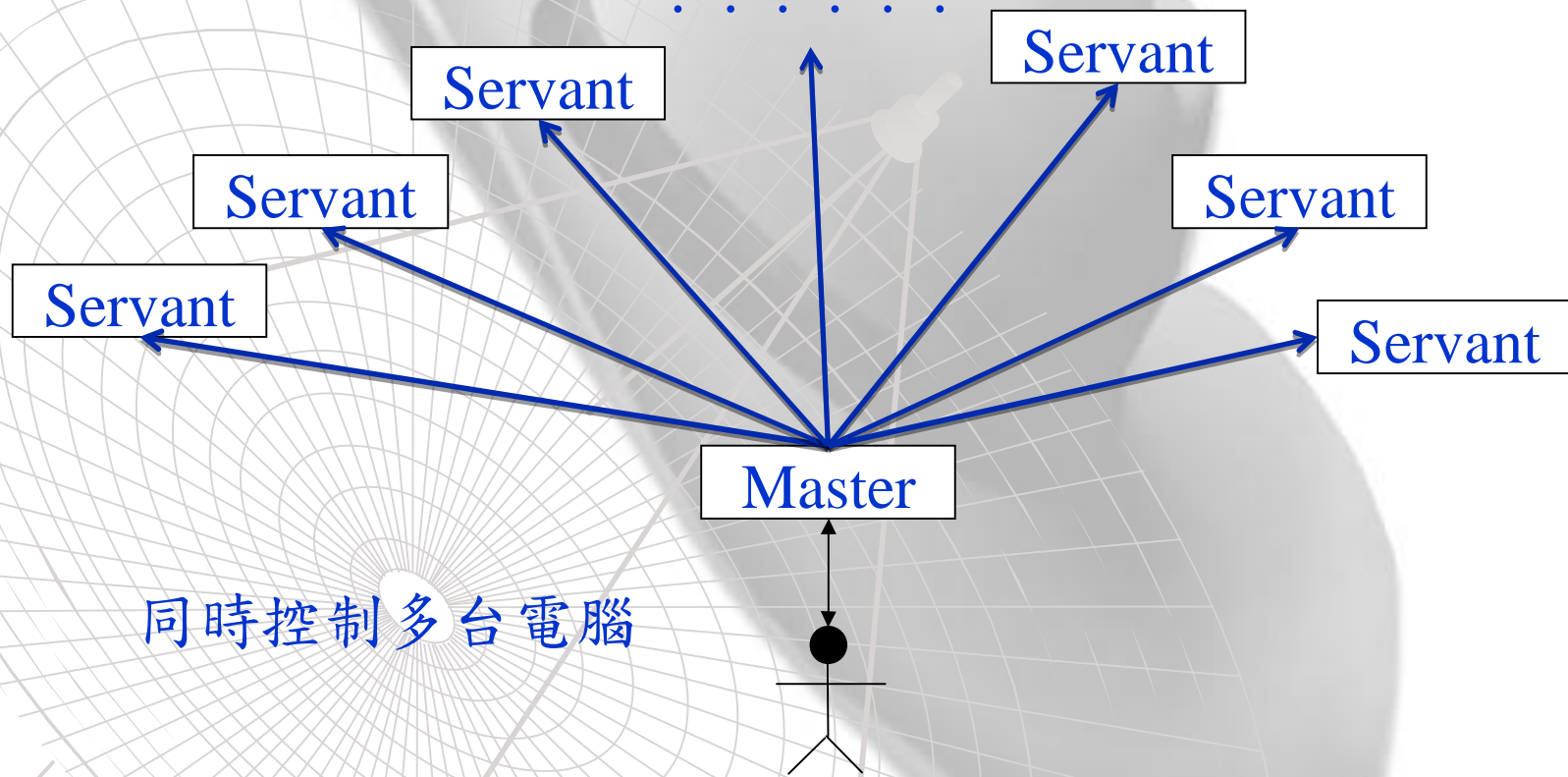
# 單元 2：遠控軟體分析



一對一進行操控

HIT Conference 2008

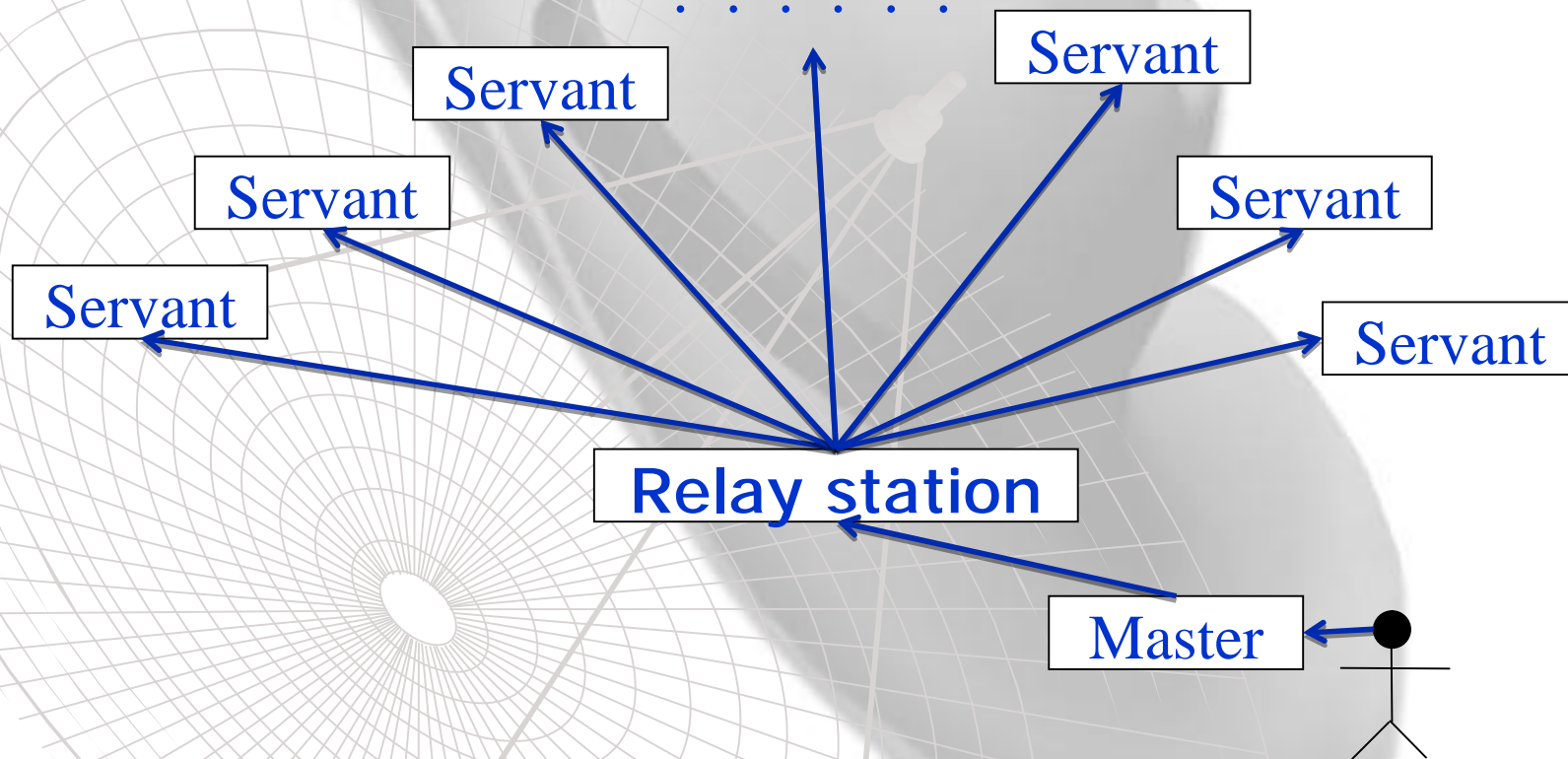
# 單元 2：遠控軟體分析



同時控制多台電腦

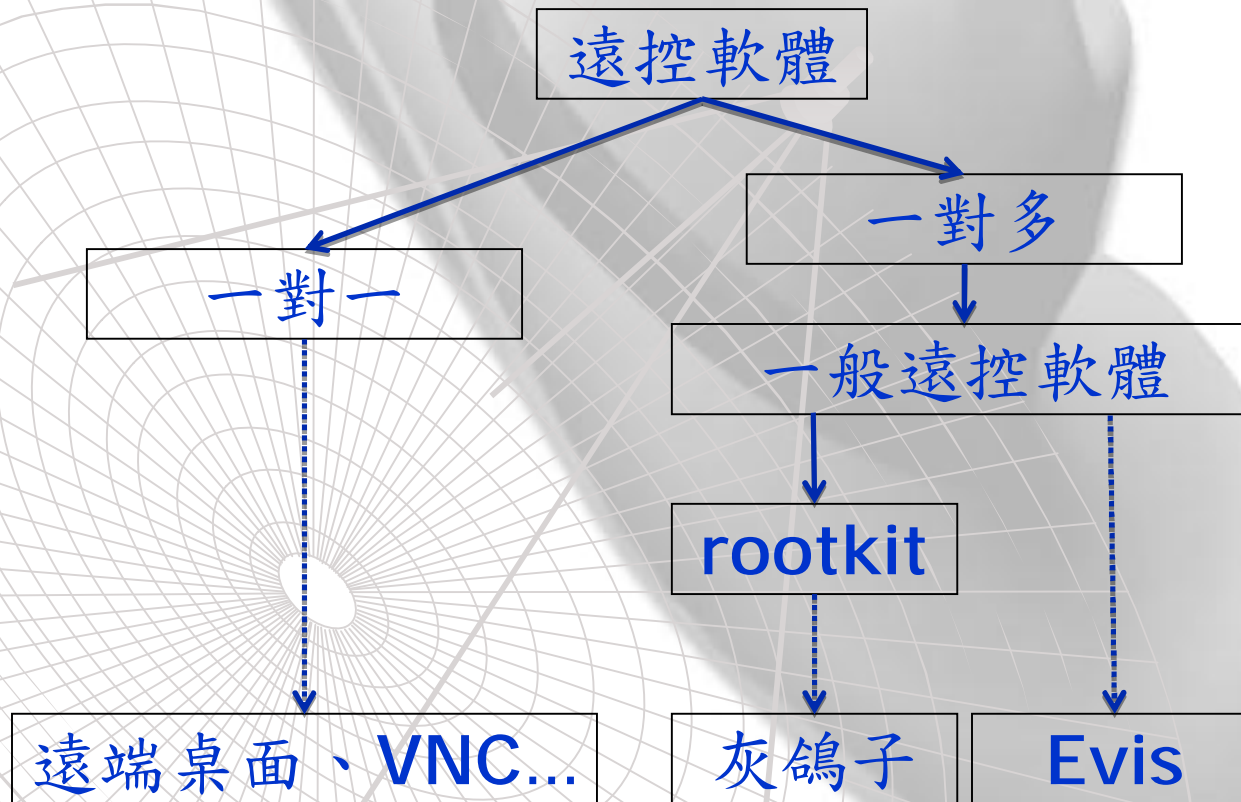
HIT Conference 2008

# 單元 2：遠控軟體分析



HIT Conference 2008

# 單元 2：遠控軟體分析



HIT Conference 2008

# 單元 2：遠控軟體分析



HIT Conference 2008



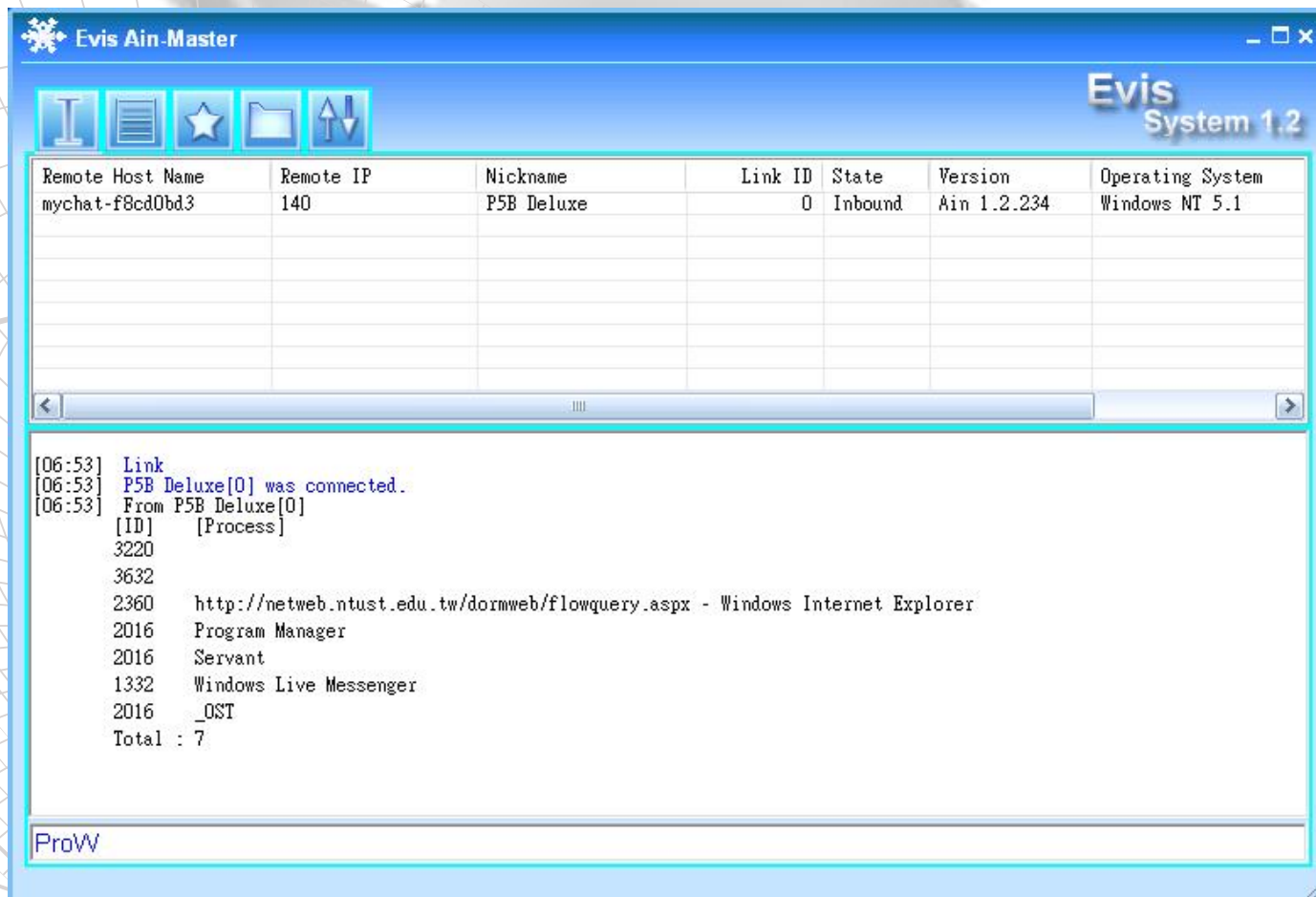
# 單元 2：遠控軟體分析

## 功能不夠?!

- 功能越多檔案越大
- 功能越多按鈕越多
- 設計者沒有想到的功能

HIT Conference 2008

# 單元 2：遠控軟體分析



The screenshot displays the Evis Ain-Master software interface. The title bar reads "Evis Ain-Master" and the version is "Evis System 1.2". The main window contains a table with the following data:

| Remote Host Name | Remote IP | Nickname   | Link ID | State   | Version     | Operating System |
|------------------|-----------|------------|---------|---------|-------------|------------------|
| mychat-f8cd0bd3  | 140       | P5B Deluxe | 0       | Inbound | Ain 1.2.234 | Windows NT 5.1   |

Below the table, a log window shows the following output:

```
[06:53] Link
[06:53] P5B Deluxe[0] was connected.
[06:53] From P5B Deluxe[0]
[ID] [Process]
3220
3632
2360 http://netweb.ntust.edu.tw/dormweb/flowquery.aspx - Windows Internet Explorer
2016 Program Manager
2016 Servant
1332 Windows Live Messenger
2016 _OST
Total : 7
```

The status bar at the bottom of the window displays "ProW".

HIT Conference 2008



# 單元 2：遠控軟體分析

指令介面的優點

巨集

讓使用者自行組合指令。

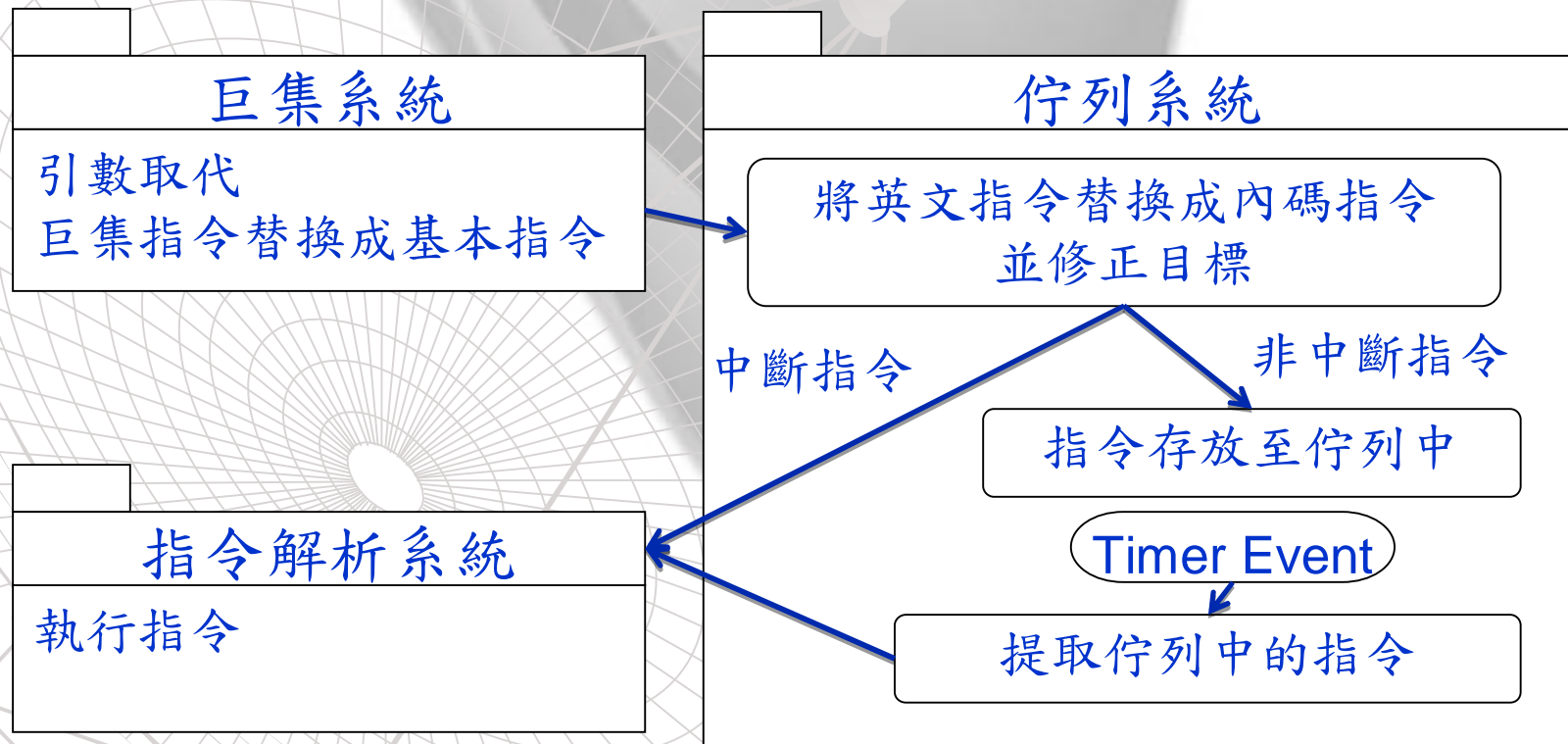
畫面簡潔

省掉一堆按鈕。

HIT Conference 2008

# 單元 2：遠控軟體分析

## 如何執行指令？



HIT Conference 2008

# 單元 2：遠控軟體分析

## 巨集系統

```
ExitOS = ExitWindowsEx 5           /*關機
ReloadOS = ExitWindowsEx 6        /*重開機
RNetUser = CmdExA net user
RNetStat = CmdExA netstat

Dload url = Download url|C:\test.rar|1

UIP = UIP1 ftp://upload.myweb.hinet.net/IP.htm + UIP2 ftp://upload.myweb.hinet.net/IP.htm
```

**Dload** http://test.tw/1.rar

**Download** http://test.tw/1.rar|C:\test.rar|1

HIT Conference 2008

# 單元 2：遠控軟體分析

## 指令送給正確的接收端？

### u 本地執行指令

- 如清除螢幕
- 設定控制端功能

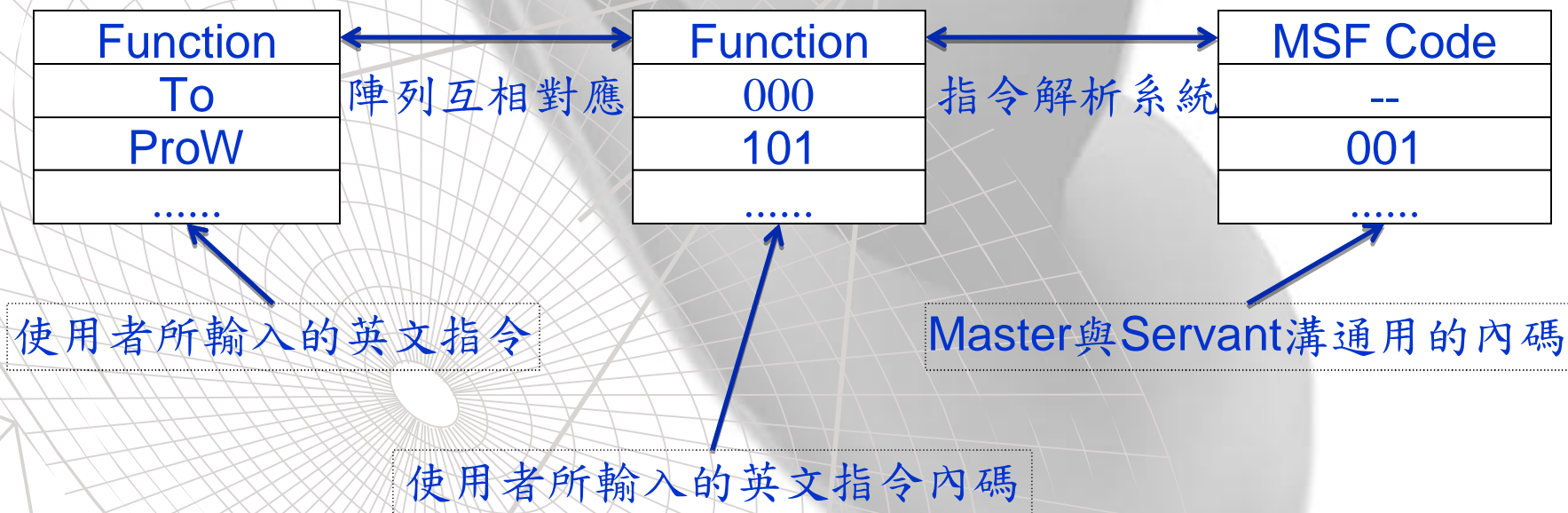
### u 遠端執行指令

- 查看遠端所有程序
- 要求遠端下載檔案

HIT Conference 2008

# 單元 2：遠控軟體分析

## 指令編碼



HIT Conference 2008

# 單元 2：遠控軟體分析

## demo

使用者輸入

```
Urun C:\a.exe
```

巨集內容

```
Urun ads = Send ads|C:\a.exe + RunS a.exe
```

引數取代

```
FSend C:\a.exe|C:\a.exe + RunS a.exe
```

替換指令

```
FSend C:\a.exe|C:\a.exe
```

```
RunS a.exe
```

HIT Conference 2008

# 單元 2：遠控軟體分析

## demo

轉換內碼 修正目標 放入佇列中

```
101 C:\a.exe|C:\a.exe
```

```
120 a.exe
```

執行指令 並傳送檔案傳輸信號

```
Write (001C:\a.exe|10240|1)
```

開始傳輸

```
建立另一組連線後傳輸binary資料
```

傳輸完成後 執行佇列中下個指令

```
Write (020C:\a.exe)
```

# 單元 2：遠控軟體分析

**Demo**

**Google 搜尋 Evis Ain**

**HIT Conference 2008**



# 單元 3：總結

- u 透過巨集能夠讓使用者創造新的功能
  - 傳輸/下載執行檔加以執行
  - 傳輸/下載dll檔進行呼叫

HIT Conference 2008