社會網路與網路安全

李漢銘
臺灣科技大學資訊工程系 教授
中央研究院資訊科學研究所 研究員
Email: hmlee@mail.ntust.edu.tw
Website: http://neuron.csie.ntust.edu.tw

台灣科大智慧型系統實驗室

Outline

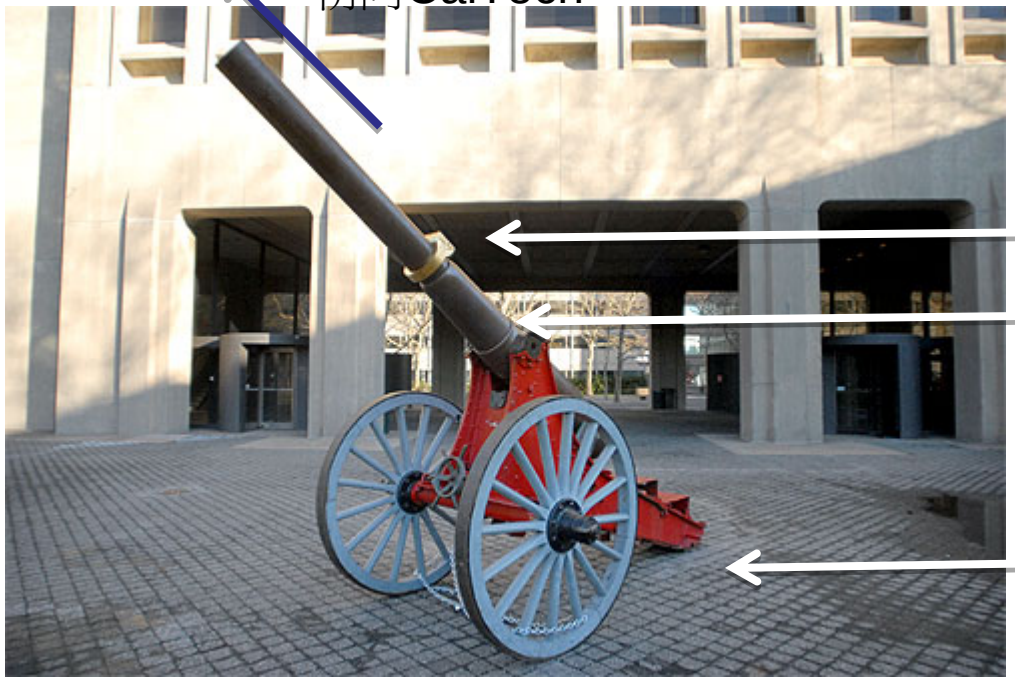
- 真實案例與背景
- 社會網路
- 社會網路於網路安全的研究
- **Intrusion Detection and Event Analysis (IDEAs)**
- 結論

資安事件不斷推陳出新

真實案例與背景

社交工程的幽默案例-Fleming Cannon

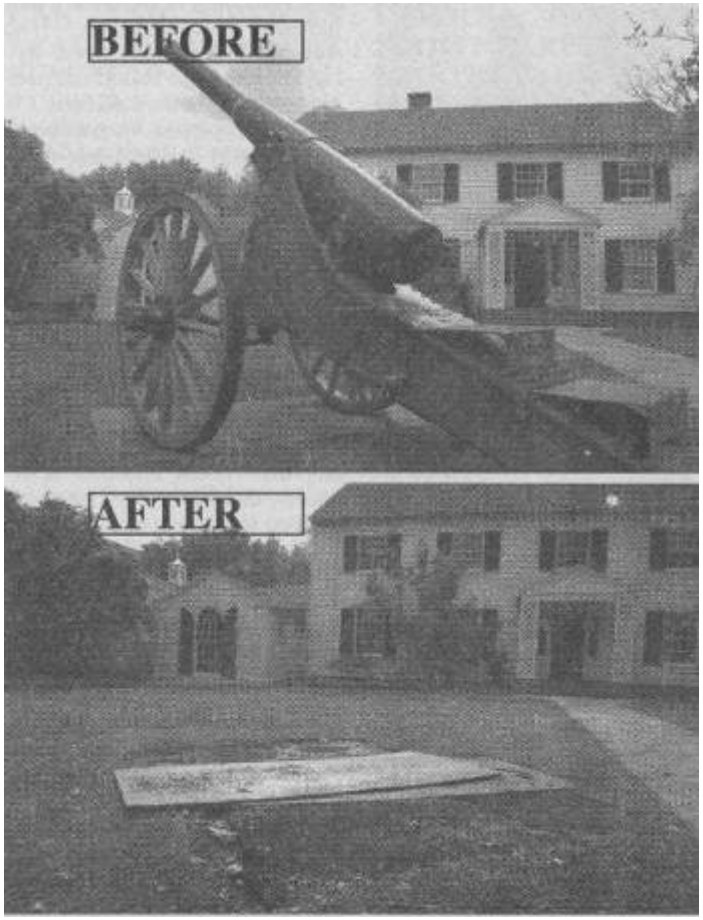
美國麻省理工學院(MIT)的惡作劇學生在把加州理工學院(CalTech)的一尊有130年歷史的加農砲偷到了MIT，並把砲口朝向CalTech所在的Pasadena，同時砲管上套了一個大尺寸的MIT金戒指。



MIT學生怎麼辦到的?

這些MIT的學生假造了一個叫做Howe & Ser Moving Company 的公司，之後再由真正的搬運公司把這個兩噸重的加農砲橫越美國境內運送到東岸。

這其實是一個非常典型的社交工程手法，也就是以細膩的誘騙手法，利用人性弱點，而非以技術或系統漏洞來入侵保護周延的環境，受害者往往還不知所以就上鉤了。



案例1:偽造電子郵件傳遞木馬程式

中央某機關同仁辦公室電腦於**96年4月24日**接獲**happy@mail.gio.gov.tw**寄送「本日新聞重點分析」內含惡意木馬程式之電子郵件

電子郵件

?

電信業者

電子郵件位址被偽造
happy@mail.gio.gov.tw
(此郵件位置原本應位於行政院新聞局)

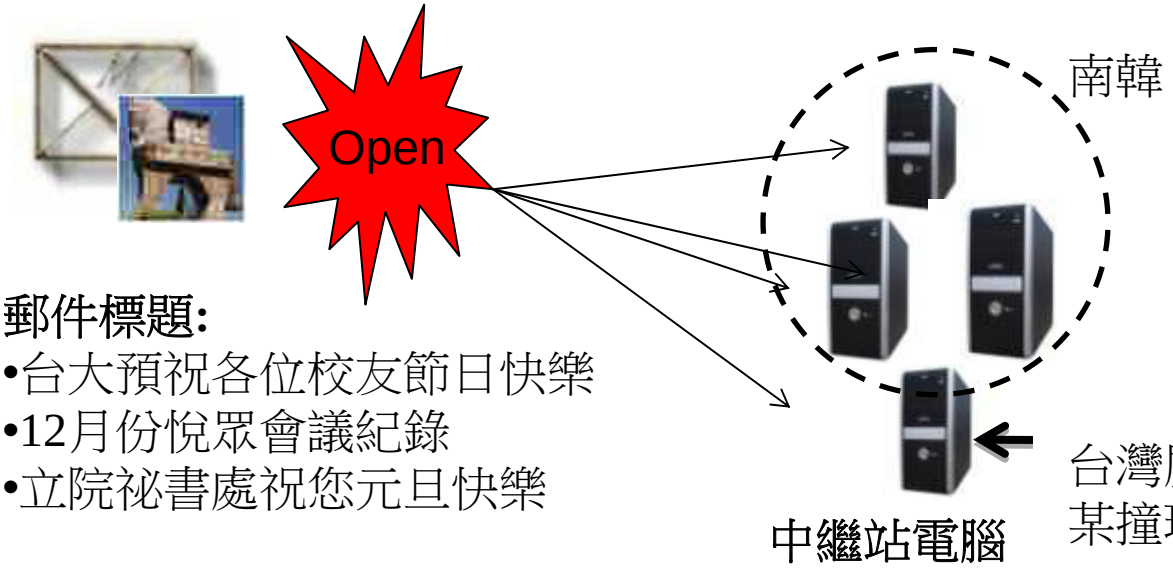
1. 檢視該郵件原始碼並向電信公司查詢得知該IP位址係由高雄市某旅行社使用

2. 經解析網路側錄資料顯示，含括**23個政府機關、16個大學院校、3個國營機構及30個團體與公司行號**等總計488個郵件使用者係該中繼站寄送惡意郵件對象。

查局乃於**96年7月4日**派員至該公司進行鑑識分析及相關作業

案例2:木馬電子郵件並建立秘密通道

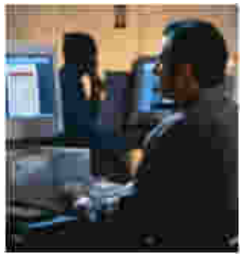
中央某機關電腦，自95年9月起陸續接獲內含惡意木馬程式之電子郵件



郵件標題:

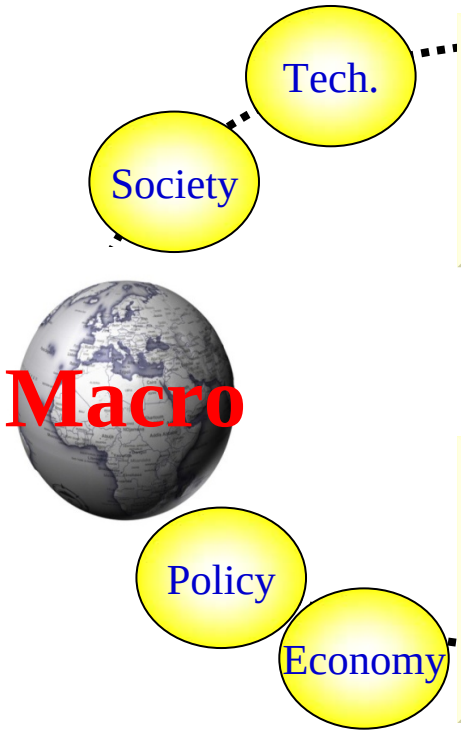
- 台大預祝各位校友節日快樂
- 12月份悅眾會議紀錄
- 立院祕書處祝您元旦快樂

調查局於96年3月16日派員至該休閒館進行鑑識分析及相關作業



經解析網路側錄資料顯示，計有6個政府機關、7個學校、34個公司行號電腦及210台個人電腦曾與該駭客中繼站伺服器主機進行連線。

資安攸關各層面 損害範圍逐年擴大



金融交易面

商業交易與相關活動日漸依賴資通訊技術，企業電子商務逐漸普及，民眾進行網路交易的頻率與金額日漸升高，也因此更遭受有心人事的覬覦。

科技與國防面

面對[illegible]安全與政府機密的威脅，建構強力且完整的資安防護能力，方能確保國家安全，並且強化國家安全形象，並能配合科技發展。

商業經營面

不管是[illegible]資料、資訊或物品傳遞，政府與企業單位無不利用資通科技進行各類商業或機密和個人隱私管理，藉大量應用IT技術提升生產力與降低成本。

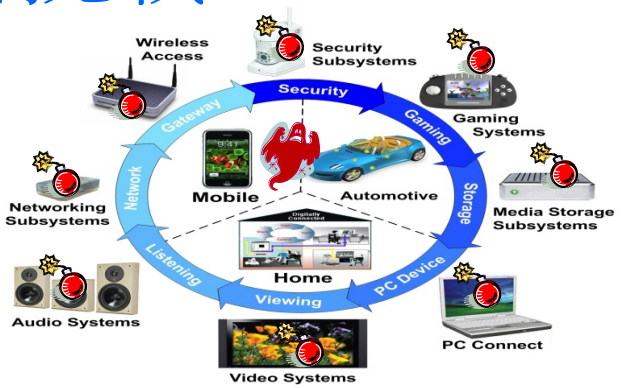
民眾防護面

目前資[illegible]都為金錢或報復，攻擊型式已轉為複合型態。現成的攻擊軟體與操作方法已俯拾皆是，加上家用市場對資通安全概念不足，更顯資通訊安全防護能力不足。

- **McAfee 研究指出2008年全球企業因資料外洩所造成的損失，達1兆美元以上。**
- **美國消費者統計報導，2006-2008年全國因電腦病毒/間諜軟體造成一般消費者共達85億美元之損失。**
- **Gartner報告指出2007年全美因網路釣魚攻擊共造成32億美元損失。**
- **2007年5月愛沙尼亞爆發史上首場網路戰，全國電腦網路遭受可能來自俄**

數位應用趨勢衍生新興資安挑戰

趨勢一、數位匯流架構複雜化 潛藏更多的資安疑慮



- 網路匯流－ 惡意攻擊更易擴散
- 服務匯流－ 易於駭客潛藏隱匿

趨勢二、智慧行動應用崛起、引爆新興資安議題

- 終端平台多元整合－ 資安脆弱性易於被利用
- 行動商務應用漸增－ 成為駭客新一波目標

趨勢三、數位生活興起、資安威脅成隱憂

- 在家連網工作－居家網路安全需求升高
- 貼心生活應用－個資保護級隱私受重視

資安威脅與法規要求 驅動全球市場快速成長

全球資安產值 US$M

2009 Nokia 手機弱洞
影響簡訊功能

2008 花旗網路銀行個資遭竊,
DNS主要安全弱點揭露

2005 邏輯炸彈造成
Medco醫療產品斷貨

2003 SQL Slammer
造成核能電廠事故

2001 Code Red 蠕蟲，
攻擊全球各大網站, 金融系統停擺

2000 DDoS攻擊癱瘓Yahoo,
CNN, Amazon, e-Bay 網站

在法規與威脅的驅動下
全球資安產業蓬勃發展
預計2012年達到818億美金

資安威脅不斷翻新變化，
防禦需求緊追其後持續成長...

CAGR=14%

120000
80000
40000
0

2000 2001 2002 2003 2004 2005 2006 2007 2008 2009 2010 2011 2012

1995
95/46/EC

1996
HIPPA法案

2002
SOX法案

2003
FISMA法案

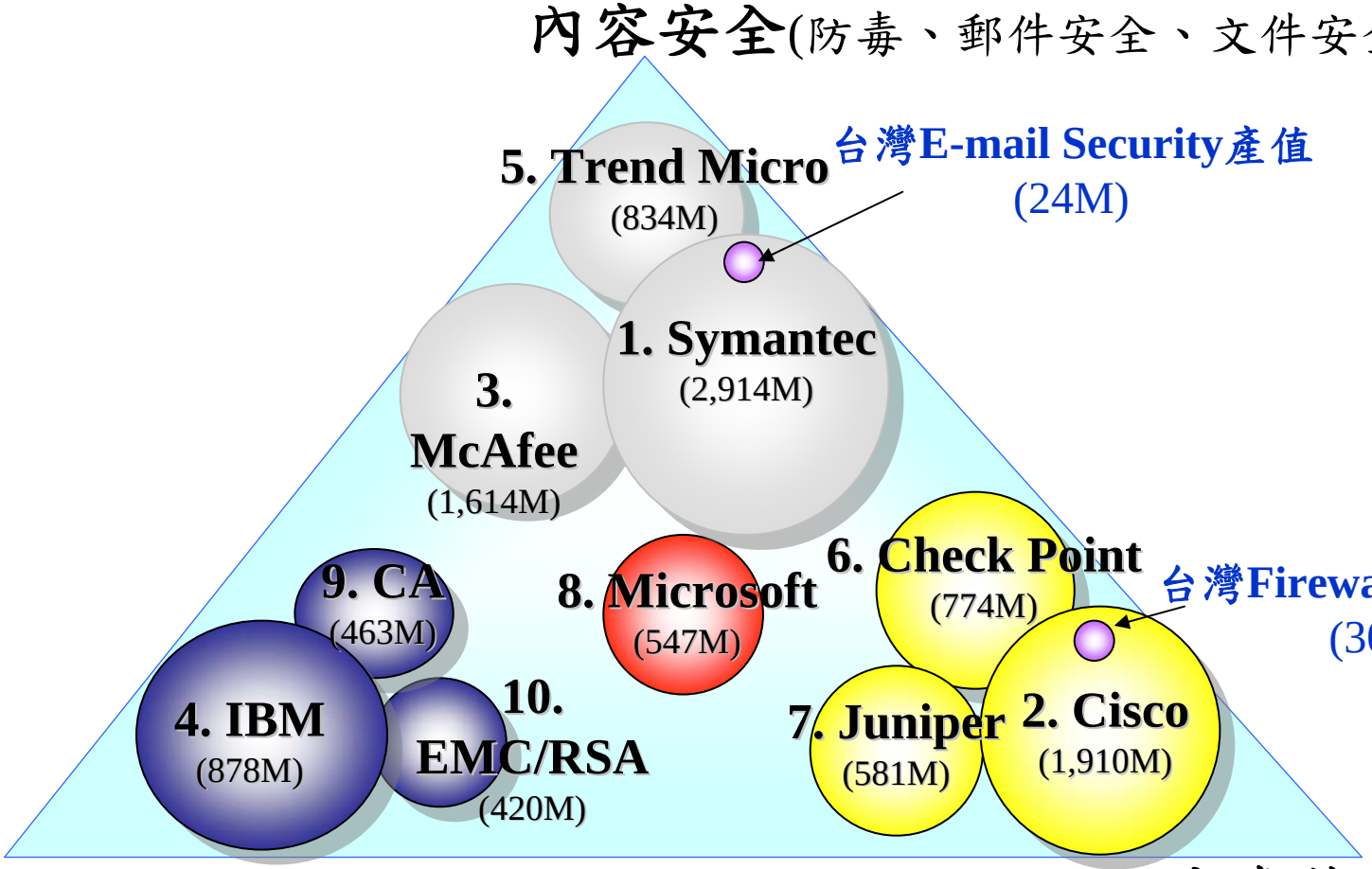
2005
ISO 27001

2008
PCI DSS

TREND MICRO
IBM
VeriSign
symantec.

資料來源：IDC 資策會整理

全球前10大資安廠商其主要產品類別



備註：圓圈大小表該廠商資安營收規模(百萬美元)相對大小，廠商前序號表該廠商於全球資安產值市佔率排名

資料來源：資策會MIC，2009年6月

資安應用需求趨勢

資訊應用

Cloud & Ubiquitous Service

Internet 應用已進入 Web Service 時代，並朝雲端與行動運算服務邁進，伴隨著更為嚴峻之資安挑戰...

Cloud & Ubiquitous Service Security

Virtual Resources
Cloud Client Mash-up

Cloud App (XML/RIA) Guard (威脅管理)
Proactive Malware Detection (內容安全)
Mobile Security/Privacy (威脅管理/內容安全)

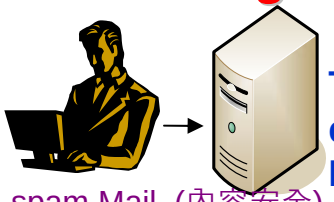
Web Service Security

Web Service

SOA, Blog,
Web-based Office..

Web App Firewall (威脅管理)
Web DB Security Monitor (威脅管理)
SIEM/Taint Analyzer (內容安全/ 弱點管理)

Inter-networking Security



Telnet/FTP/
e-Mail/
Browsing..

Anti-spam Mail, (內容安全)
VA, F/W, IDS, IPS (威脅管理)
PKI, VPN (身分辨識)

Internet service

2005 2010 2015

隱藏的邏輯

社會網路

Six degree and small world

What is "Six Degrees"?

- "Six Degrees of Separation" -- John Guare,1990
  - "Six degrees of separation between us and everyone else on this planet"
  - 「我從某處得知，在地球上，人與人之間只被六個人隔絕．六度的分隔，正是這個星球的人際距離」
- An urban myth? ("5 handshakes to the President")

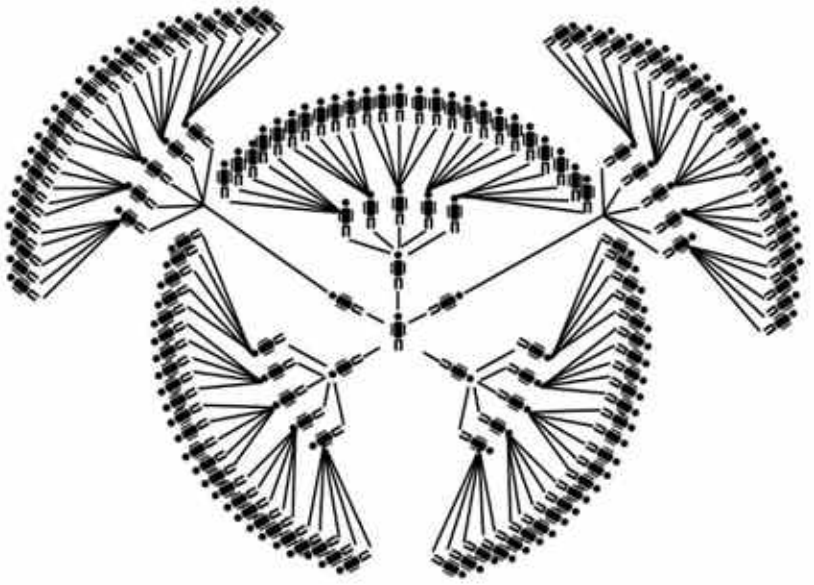
- "What is the probability that two strangers will have a mutual friend?" ----------1950's, Pool and Kochen asked
  - i.e. the "small world" of cocktail parties

http://www.nd.edu/~networks/linked/newfile7.htm

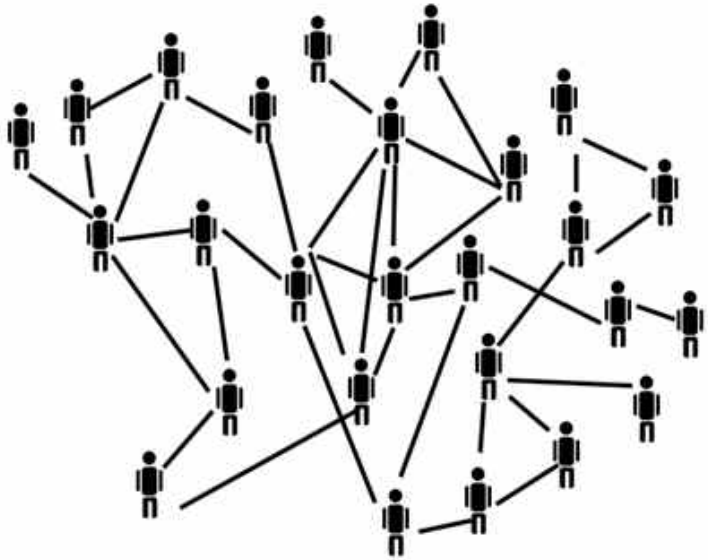
Six degree and small world

數學性與社會性思考的落差

- 數學性的思考 vs. 社會性思考



數學性的思考
每個人有5個朋友, 連通數量迅速膨脹



社會性的思考
朋友之間往往互相認識, 造成群聚的現象

Six degree and small world
數學性與社會性思考的落差 (cont.)

- 數學式思考 vs. 社會性思考
- 群聚性(clustering)
  - 朋友之間往往也是朋友
  - 社群：分享共同的經驗,地理位置, 興趣
  - 結果:冗餘(redundancy)
- 試驗結果的弔詭:
  - 群聚性很高
  - 連結任何一個人的步驟甚少(人際距離很近)
  - 小世界現象!!
  - Small world networks are everywhere!

Six degree and small world

Examples of six degree in entertainments


張菲

【報告典獄長】


廖峻

【大小老千】


洪金寶

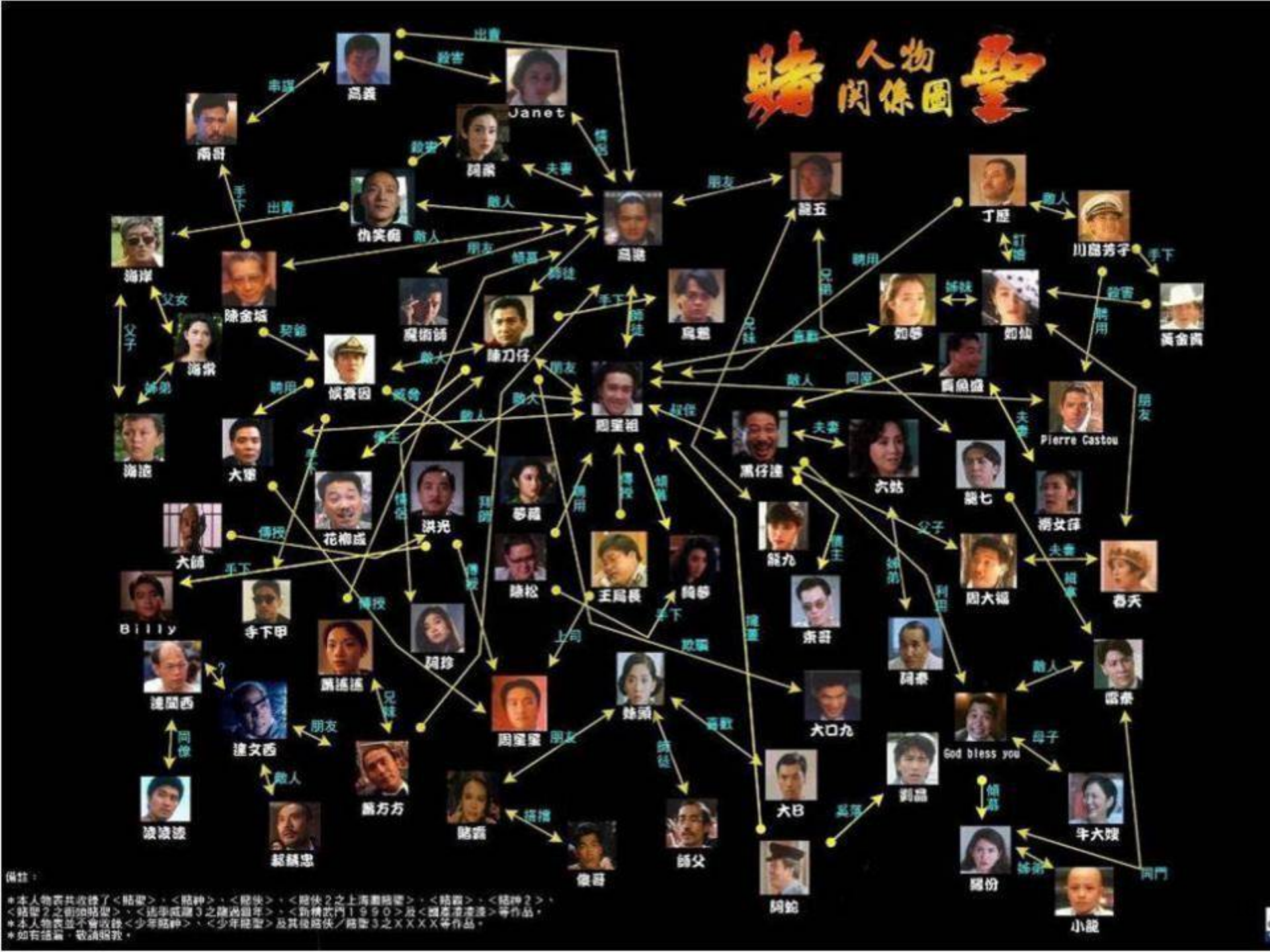
【猛龍】


Maggie Q

【不可能的任務】


湯姆克魯斯

周星馳呢?



備註：

＊本人物表共收錄了＜賭聖＞、＜賭神＞、＜賭俠＞、＜賭俠２之上海灘賭聖＞、＜賭霸＞、＜賭神２＞、＜賭聖２之街頭賭聖＞、＜逃學威龍３之龍過年＞、＜新精武門１９９０＞及＜國產凌凌漆＞等作品。
＊本人物表並不會收錄＜少年賭神＞、＜少年賭聖＞及其後賭俠／賭聖３之ＸＸＸＸ等作品。
＊如有錯漏，敬請賜教。

Six degree and small world

The small world experiment

- Stanley Milgram 的小世界實驗 (1967)
  - A single “target” in Boston (證券業務員 Sharon)
  - 300 initial “senders” in Boston and Omaha
  - Each sender：寄給他認為最接近Sharon的一位朋友
  - The friends got the same instructions
- 結果
  - 64/300到達
  - 6個步驟!!!

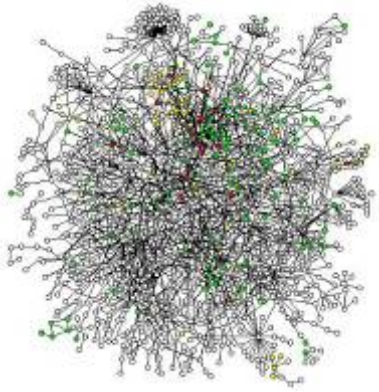
Milgram實驗所發現的問題

為何在兩個陌生人之間總會存在一條最短的人際關係鏈結
(short chains of acquaintances linking)?

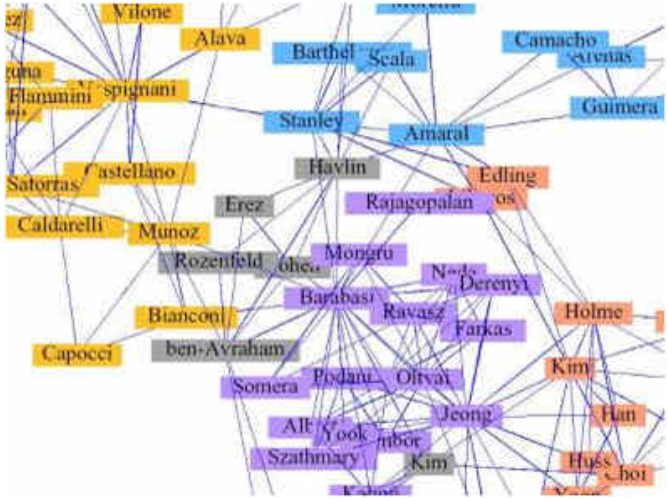
Social networks

What is a social network?

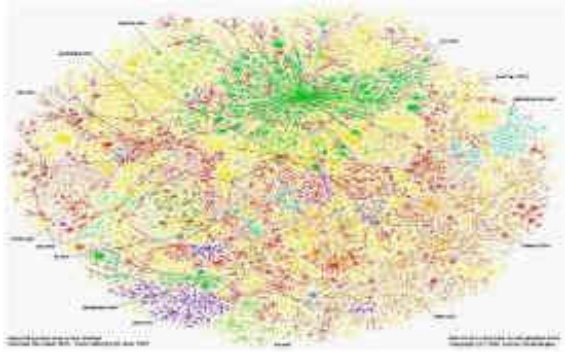
- A set of dyadic ties, all of the same type, among a set of actors
  - Actors can be persons, organizations, groups
  - A tie is an instance of a ***specific*** social relationship



Protein Interaction Network



Scientific Collaboration Network



Internet

Social networks

History of social networks

- 1967: **Small World Phenomenon** (Stanley Milgram)
- 1974: **The Strength of Weak Ties** (Mark Granovetter)
- 1998: **Collective Dynamics of Small-World** (Duncan J. Watts and Steven H. Strogatz)
- 2003: **Wikipedia** (An online community that connects people through networks of friends for dating or making new friends), 無名小站
- Now: **There are thousands of applications applied to social networks**

Stanley Milgram

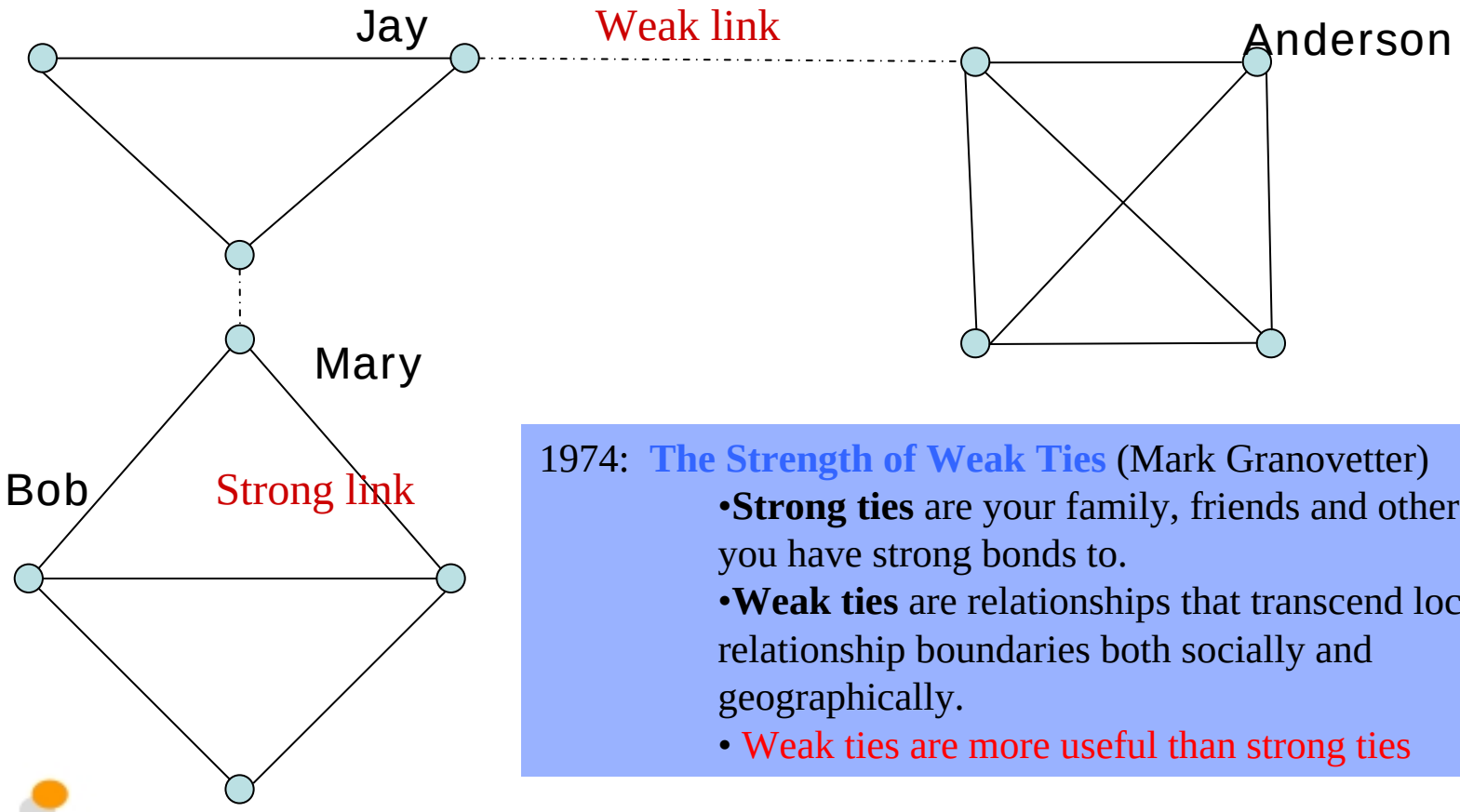
Social networks

What can social networks help ?

- How does a kind of fashion become an vogue?
- How does a virus spread and infect people?
- How does a research topic become a hot topic

Social networks analysis

Strong link V.S. Weak link



1974: **The Strength of Weak Ties** (Mark Granovetter)

- **Strong ties** are your family, friends and other people you have strong bonds to.
- **Weak ties** are relationships that transcend local relationship boundaries both socially and geographically.
- Weak ties are more useful than strong ties

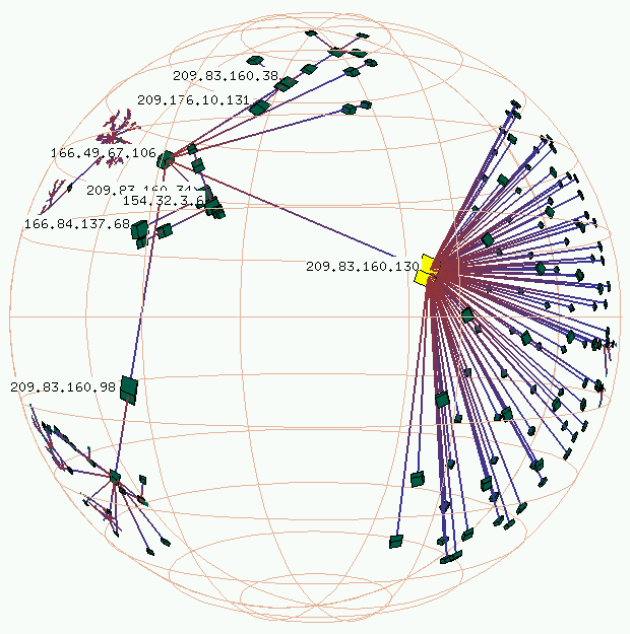
社會網路更容易透過網路的環境而建立

社會網路於網路安全的研究

Internet social networks

Internet Structure

- Internet structure is also a small world
- It possess a scale-free topology
- A data transferred from a computer to another computer only needs four step (Four Degrees of Separation)

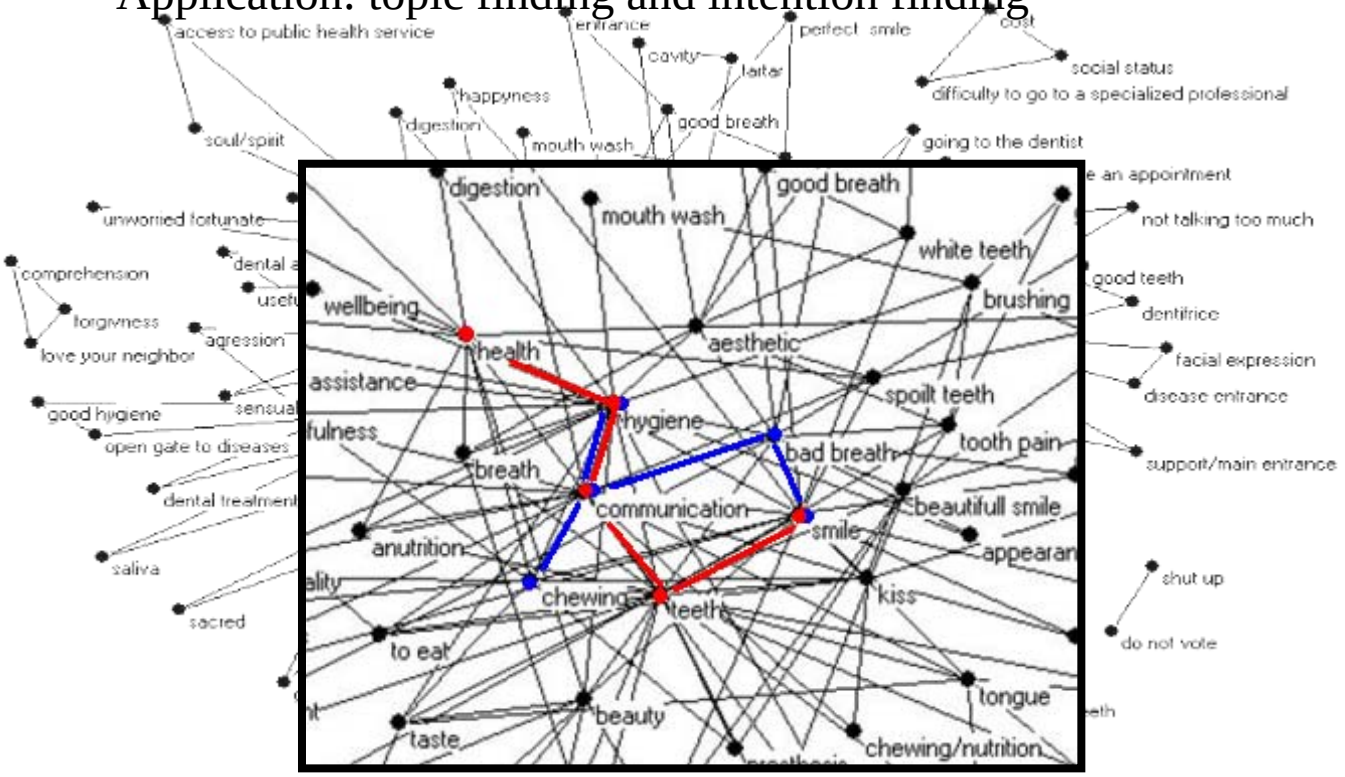


•Internet Connections (http://caida.org/)

Words social networks

A sketch of the WSN for the word theme of mouth

- Properties related to connectivity and distances in words-graphs
  - Application: topic finding and intention finding

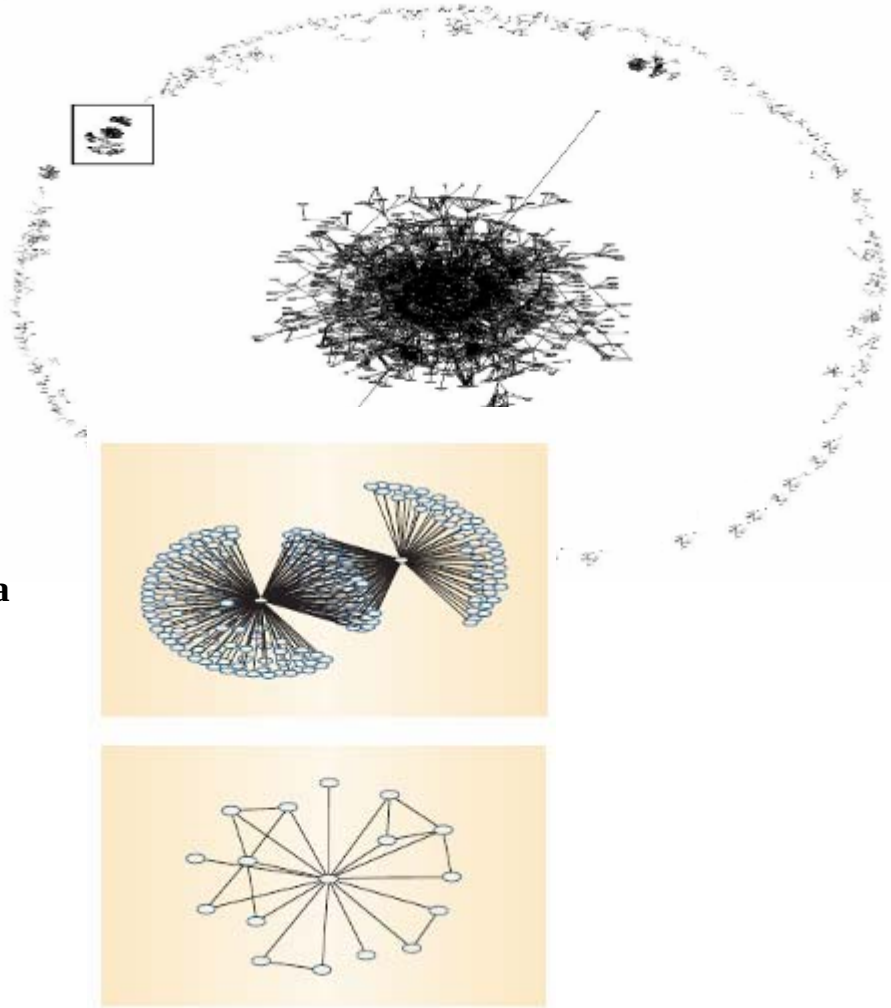


反垃圾郵件

Anti-spam research based-on social networks

Personal e-mail social networks

In the largest component , none of nodes share neighbors



Subgraph of a spam component. Two spammers share many corecipients (middlenodes). In this subgraph, no node shares a neighbor with any of its neighbors.

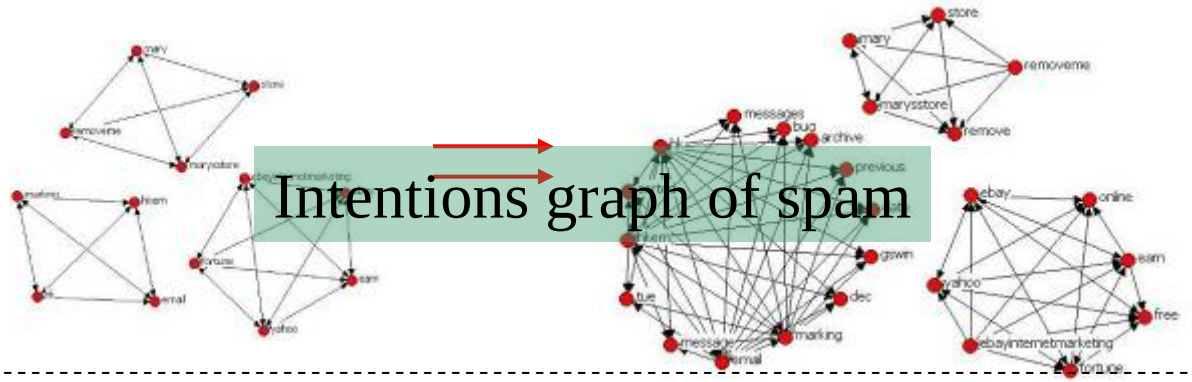
Subgraph of a nonspam component. The shows a higher incidence of triangle Structures (neighbors Sharing neighbors) than the spam subgraph.

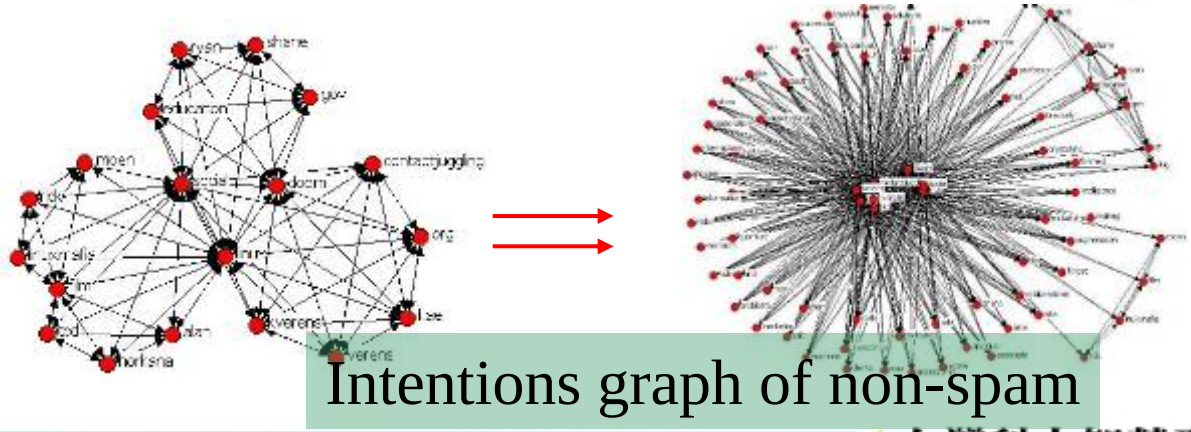
P. O. Soykin and V. P. Roychowdhury, "Leveraging social networks to fight spam," IEEE Computer, 38(4):61-68, April 2005

Anti-spam research based-on social networks

Intentions graph for detecting spam

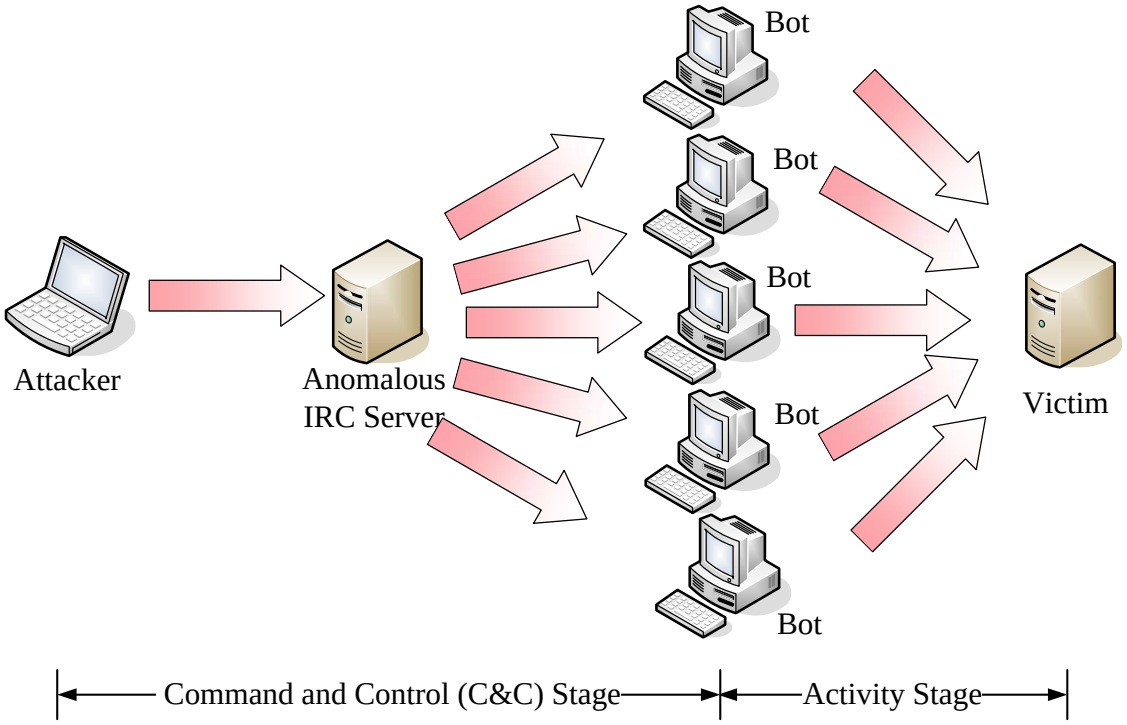
- Intentions of spammer are almost the same (even expands their social relationship to Internet)





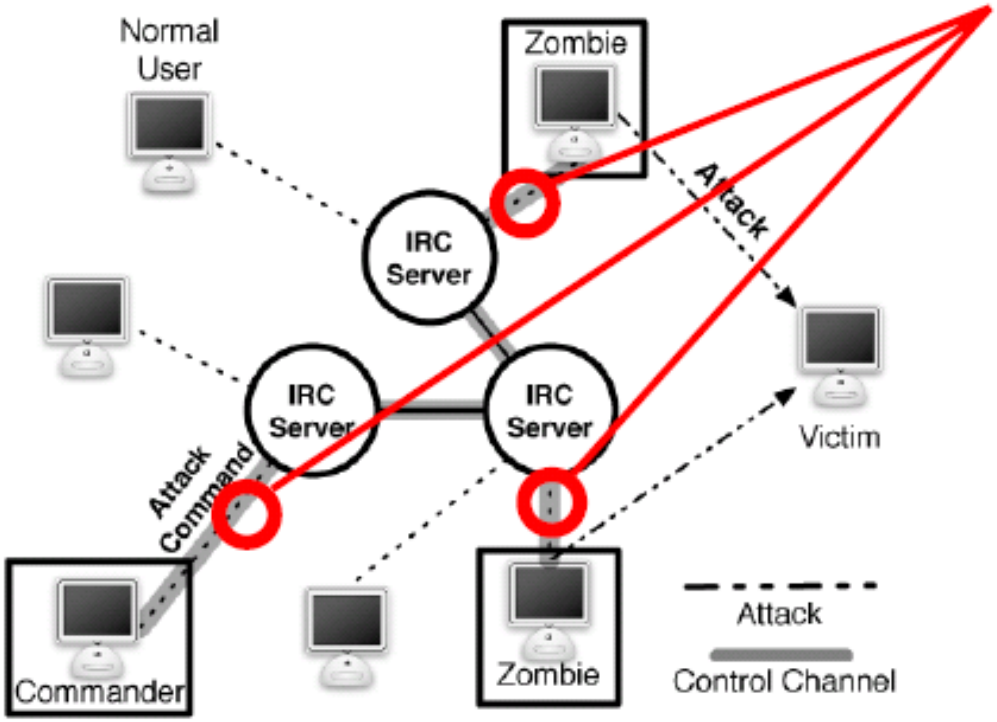
Botnet detection 殭屍網路的偵測

- A **Botnet** is a compromised hosts (**bots**) remotely controlled by an attacker and the owners are not aware
  - E.g. Invoke a DDoS (Distributed Deny of Service) attack



Detecting Bot Communication

Many bots use IRC for Command and Control



- Detect IRC Bot Commands
- IRC Behavior Modeling
- Inspect Payloads (*advscan*…)
- Traffic Behavior Analysis

Intrusion Detection and Event Analysis (IDEAs)

The Bridge in Information Security-iSLAB

TWISC
資通安全研究與
教學中心

Academia Sinica

資安開放源碼軟
體專業人才培訓
暨知識平台建立

iSLab
台灣科大智慧型
系統實驗室

iCAST
跨國資安先進技
術合作計畫

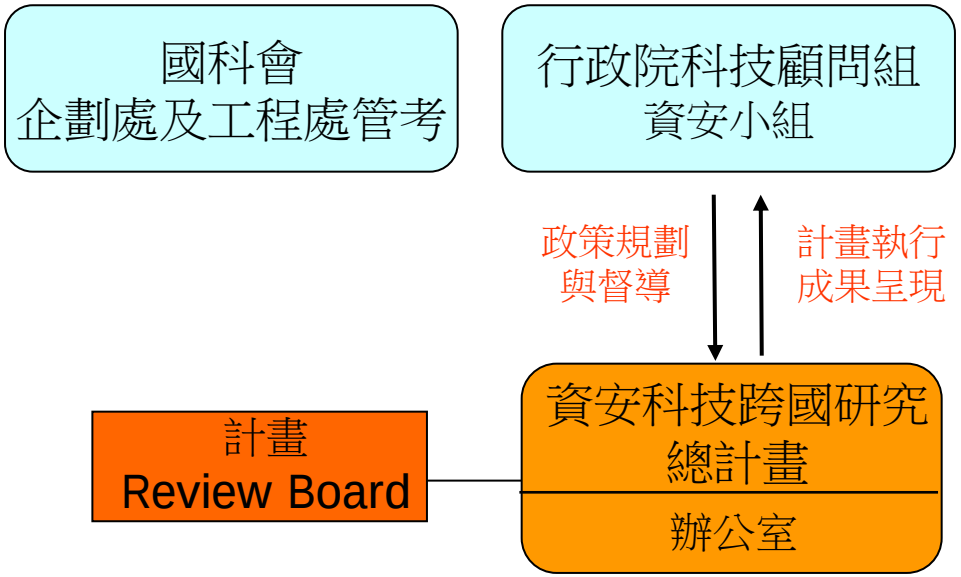
Carnegie Mellon University

Cornell University

Intrusion Detection
1.Web application attacks
2.Botnet Detection
3.Anti-spam
Event Analysis
1.False alarm reduction
2.Multi-steps detection
Software Validation
1. Dynamic testing

產業應用 ← → 核心技術研發

計畫架構

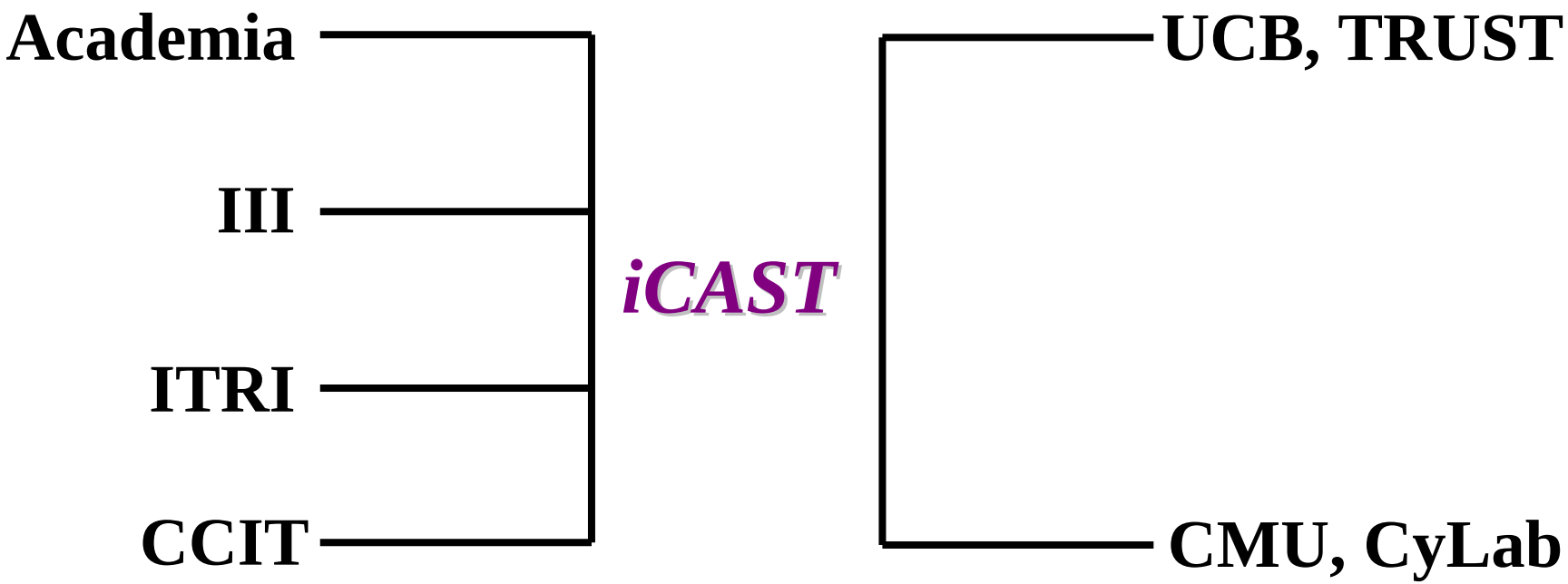


主持人 李德財	中央研究院 資訊科學研究所	所長
許清琦 （共同）	資訊工業策進會	副執行長
林寶樹 （共同）	工業技術研究院資通所	所長
李漢銘 （共同）	台灣科技大學	教授

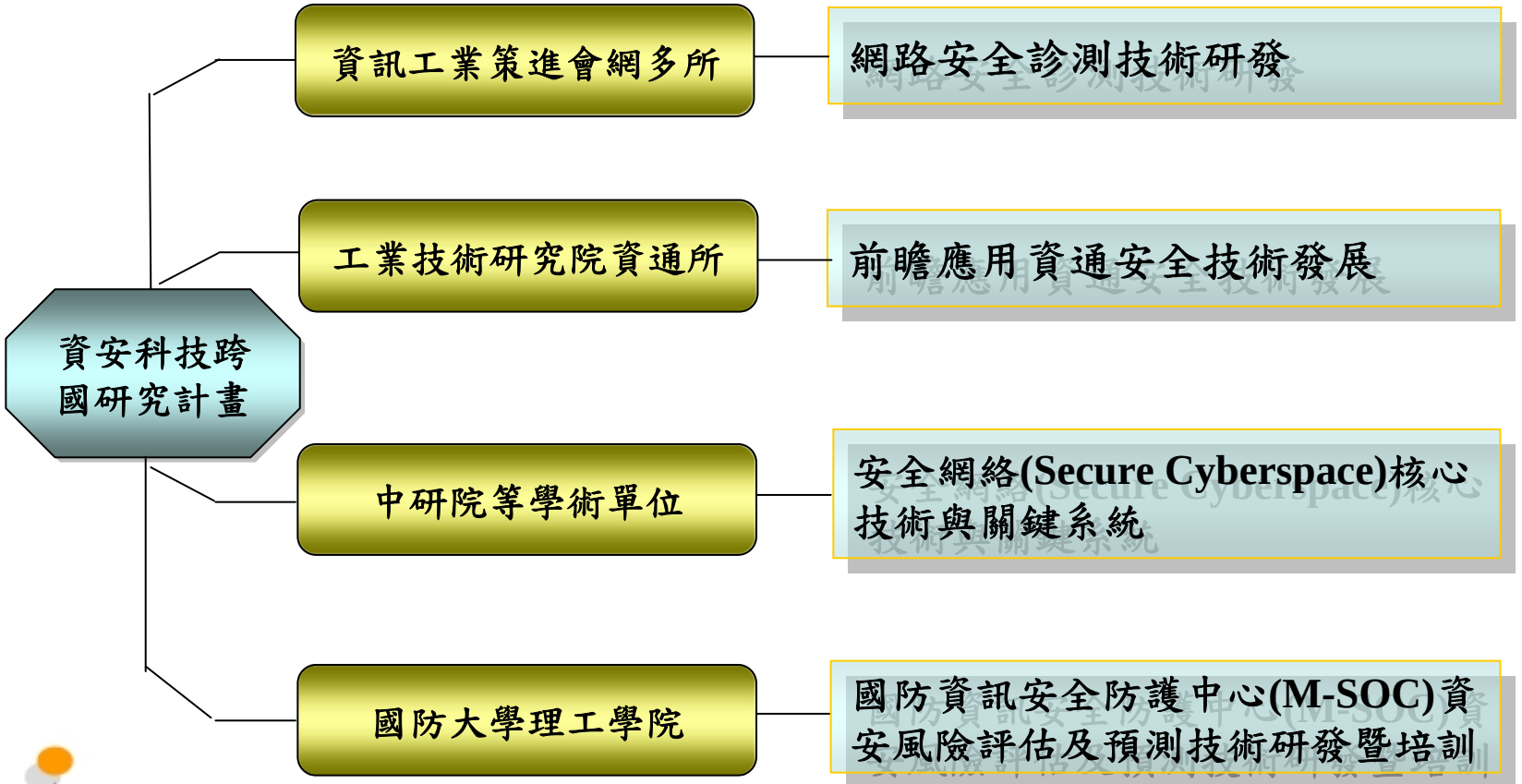
分項計畫一	吳建興	資訊工業策進會網多所	顧問	網路安全診測技術研發
分項計畫二	余孝先	工業技術研究院資通所	副所長	前瞻應用資通安全技術發展
分項計畫三	雷欽隆	中研院等學術單位	教授	安全網絡(Secure Cyberspace)核心技術與關鍵系統
分項計畫四	劉思遠	國防大學理工學院	少將院長	國防資訊安全防護中心(M-SOC)資安風險評估及預測技術研發暨培訓

*以上分項計畫內容係第3年度（2008年）現況

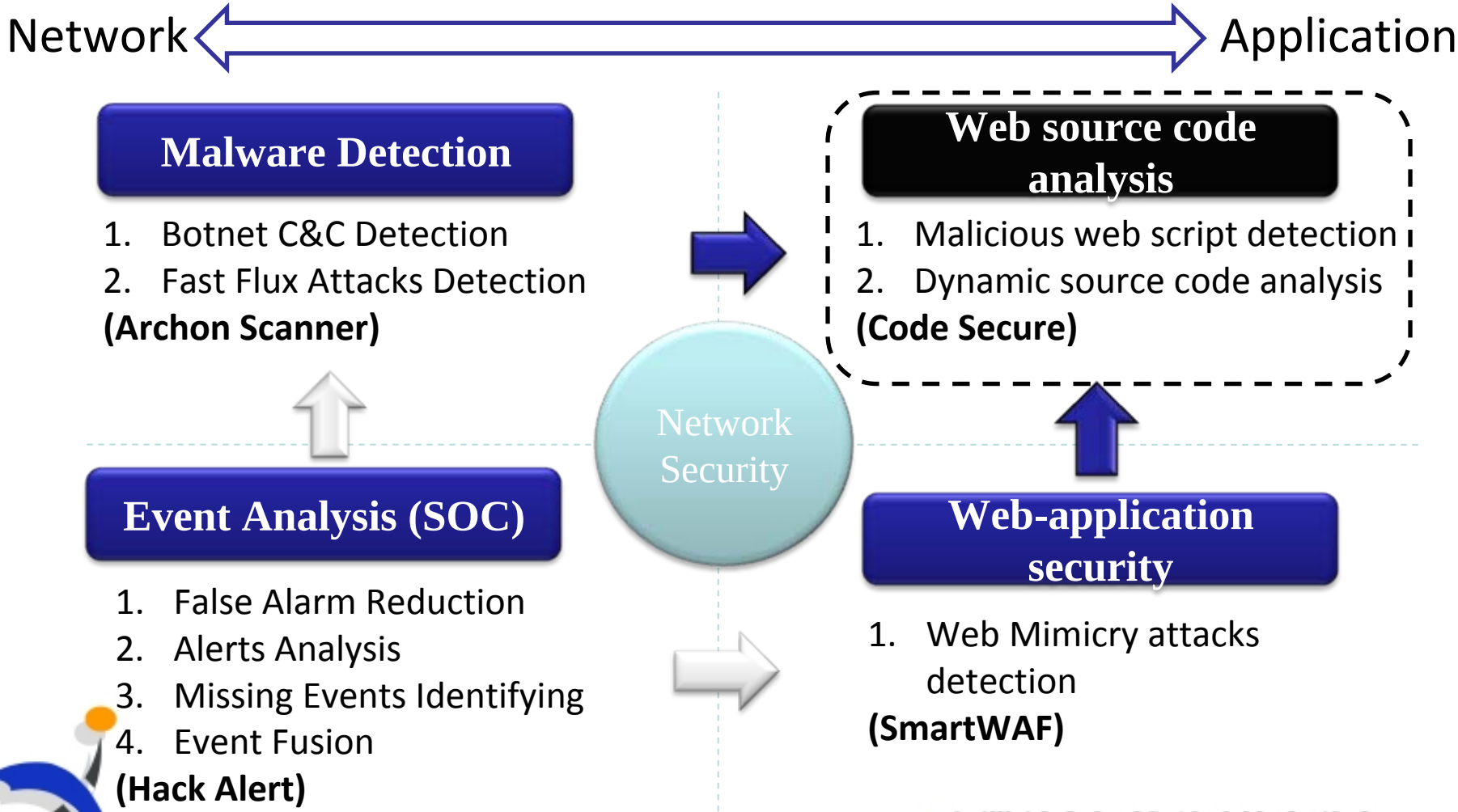
計畫架構（續）



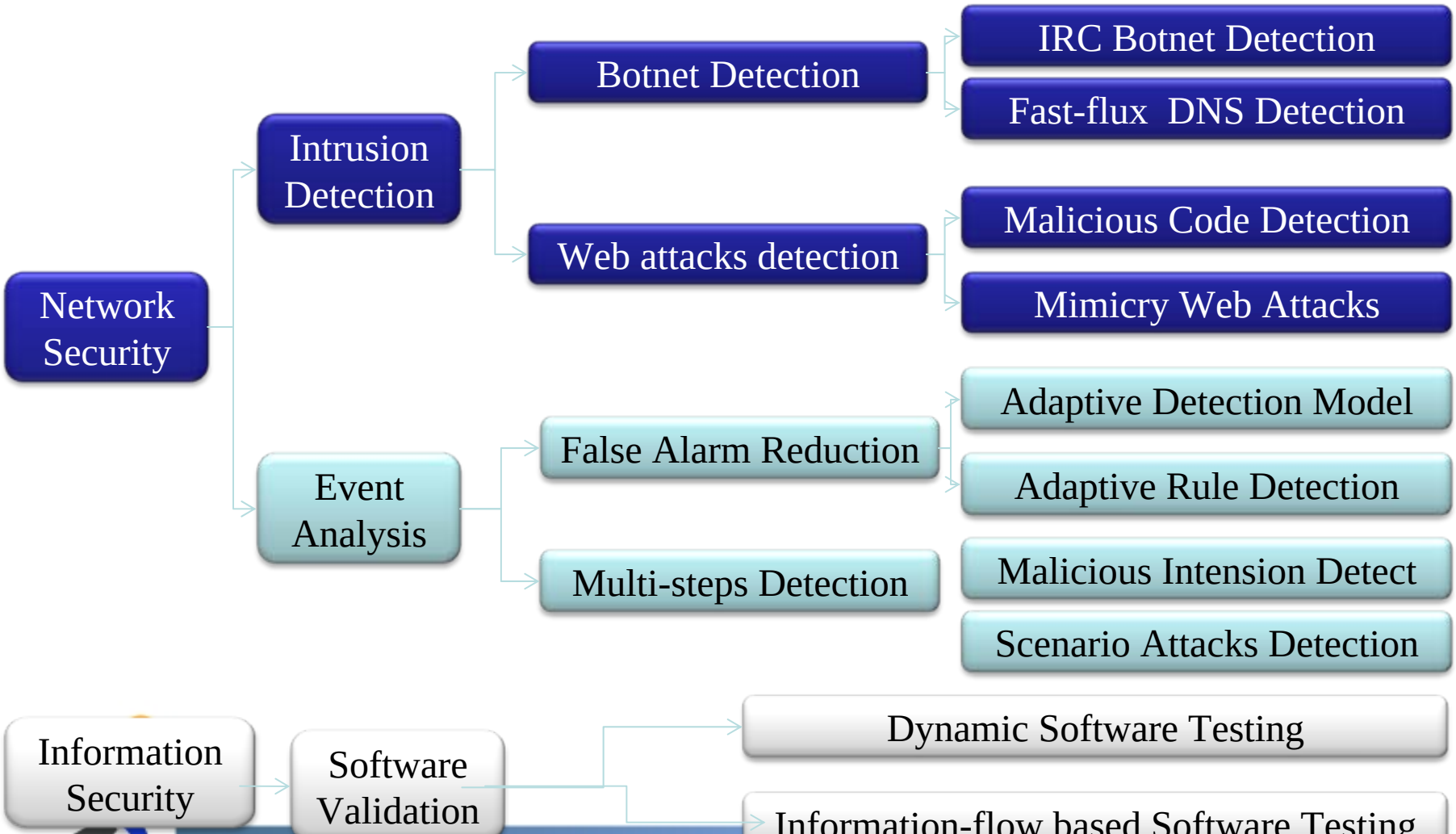
計畫架構（續）


資安科技跨國研究計畫
資訊工業策進會網多所
網路安全診測技術研發
工業技術研究院資通所
前瞻應用資通安全技術發展
中研院等學術單位
安全網絡(Secure Cyberspace)核心技術與關鍵系統
國防大學理工學院
國防資訊安全防護中心(M-SOC)資安風險評估及預測技術研發暨培訓

Information Security Research Roadmap



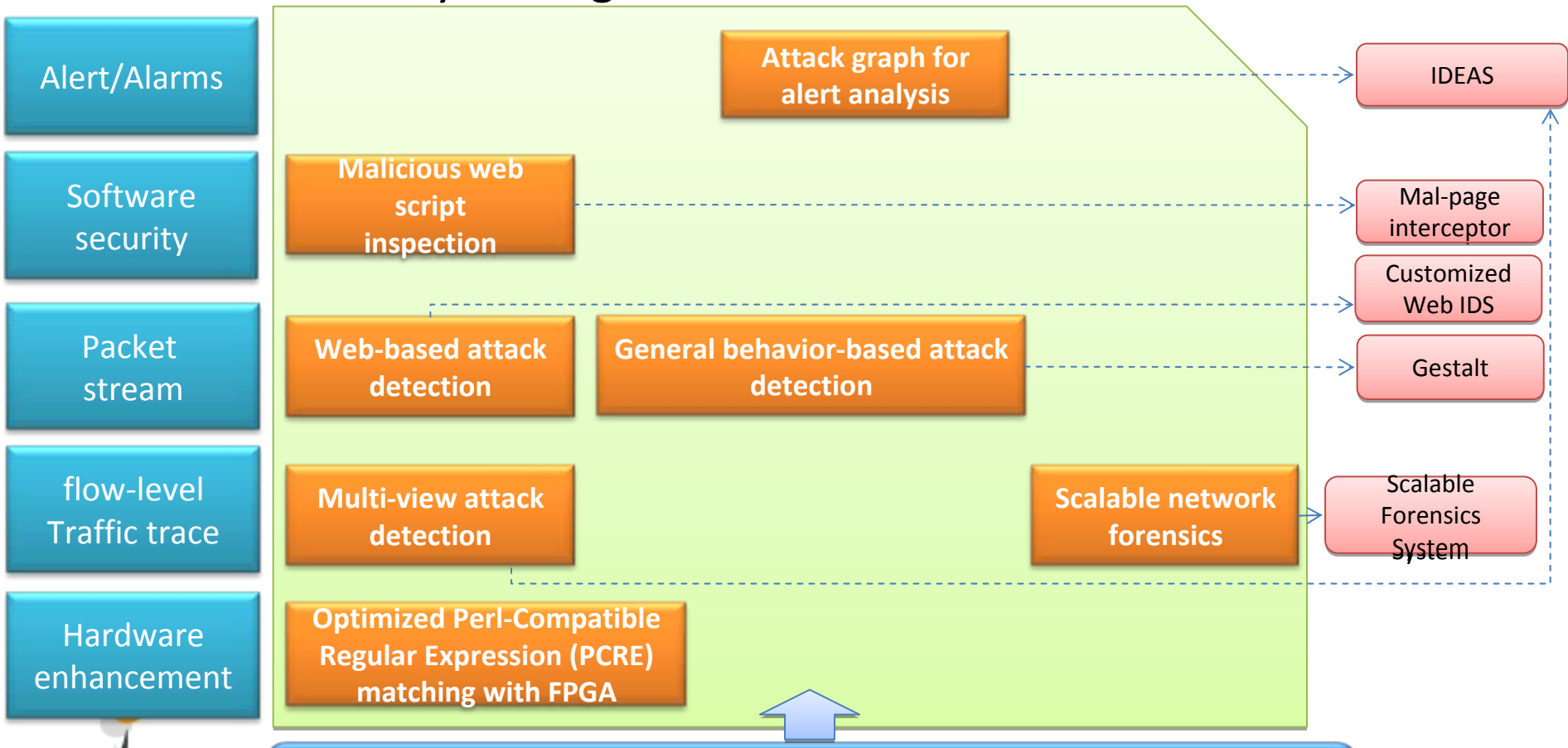
Roadmaps of Information Security Research in iSLAB



Attack Analysis Life Cycle

Detection | Analysis | Forensics

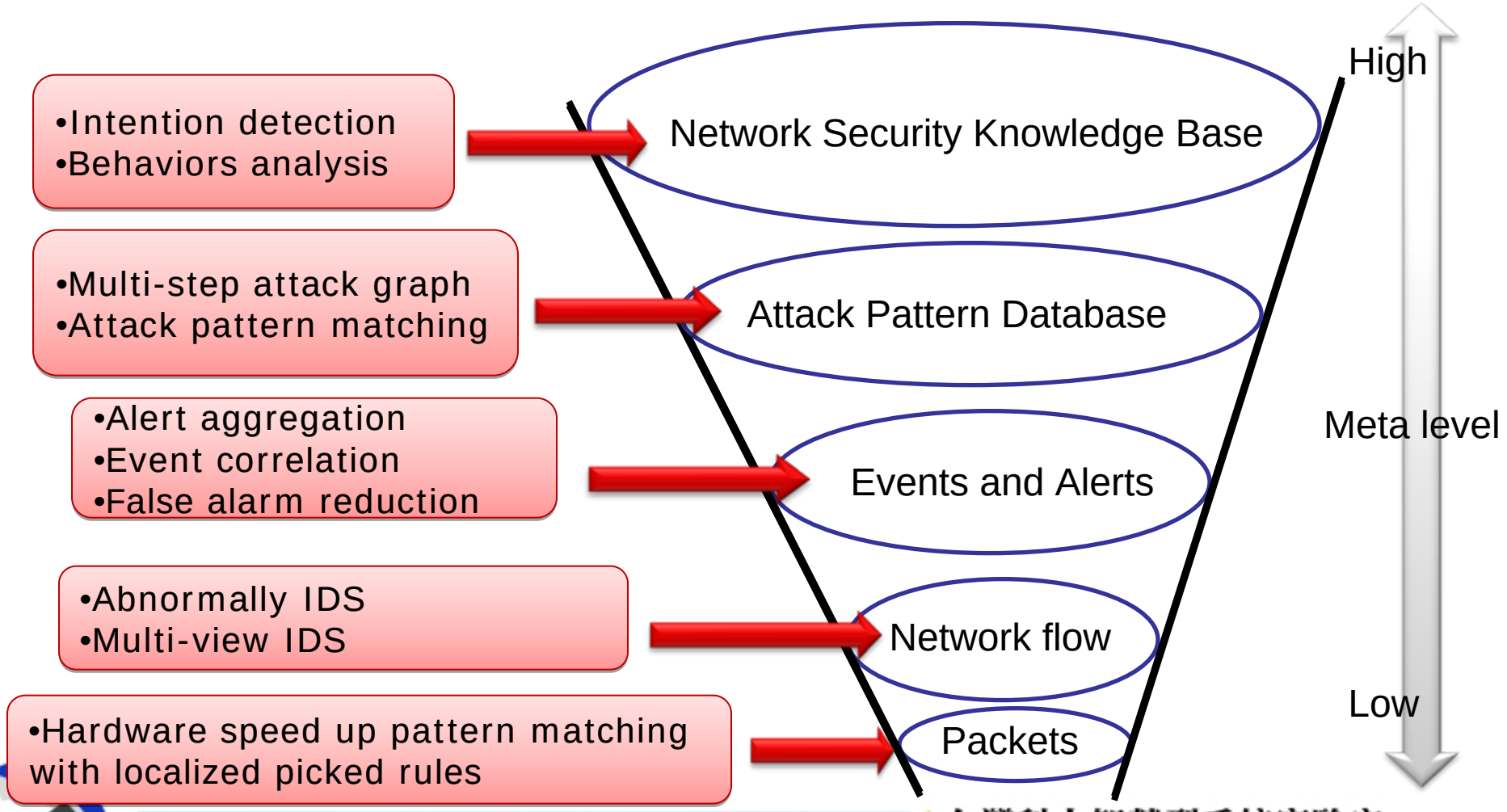
Anomaly management



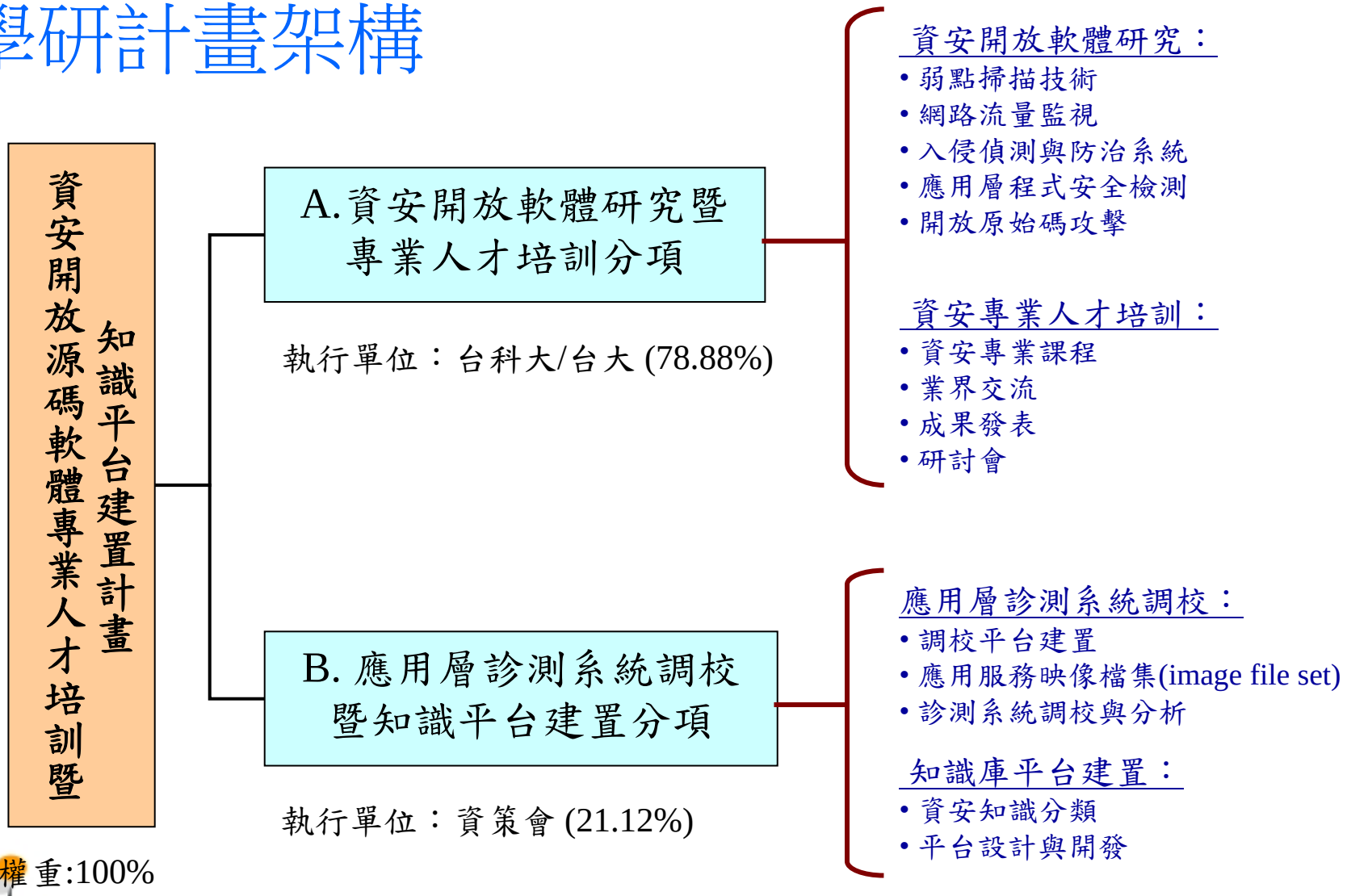
Machine Learning Core Technology
(LLASA: A Library of Learning Algorithm for Information Security)

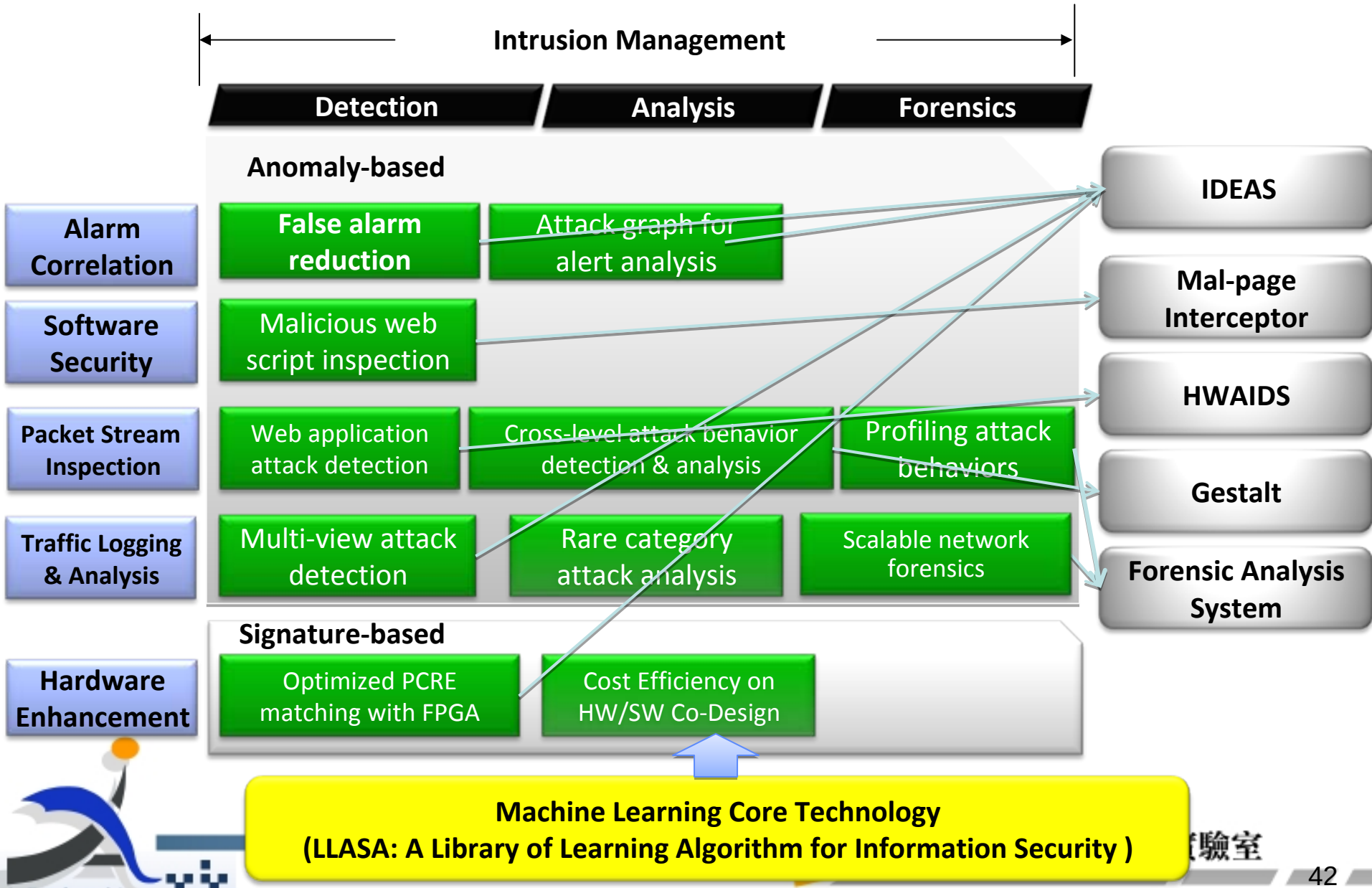
Intrusion Detection and Event Analysis System

IDEAs Scope



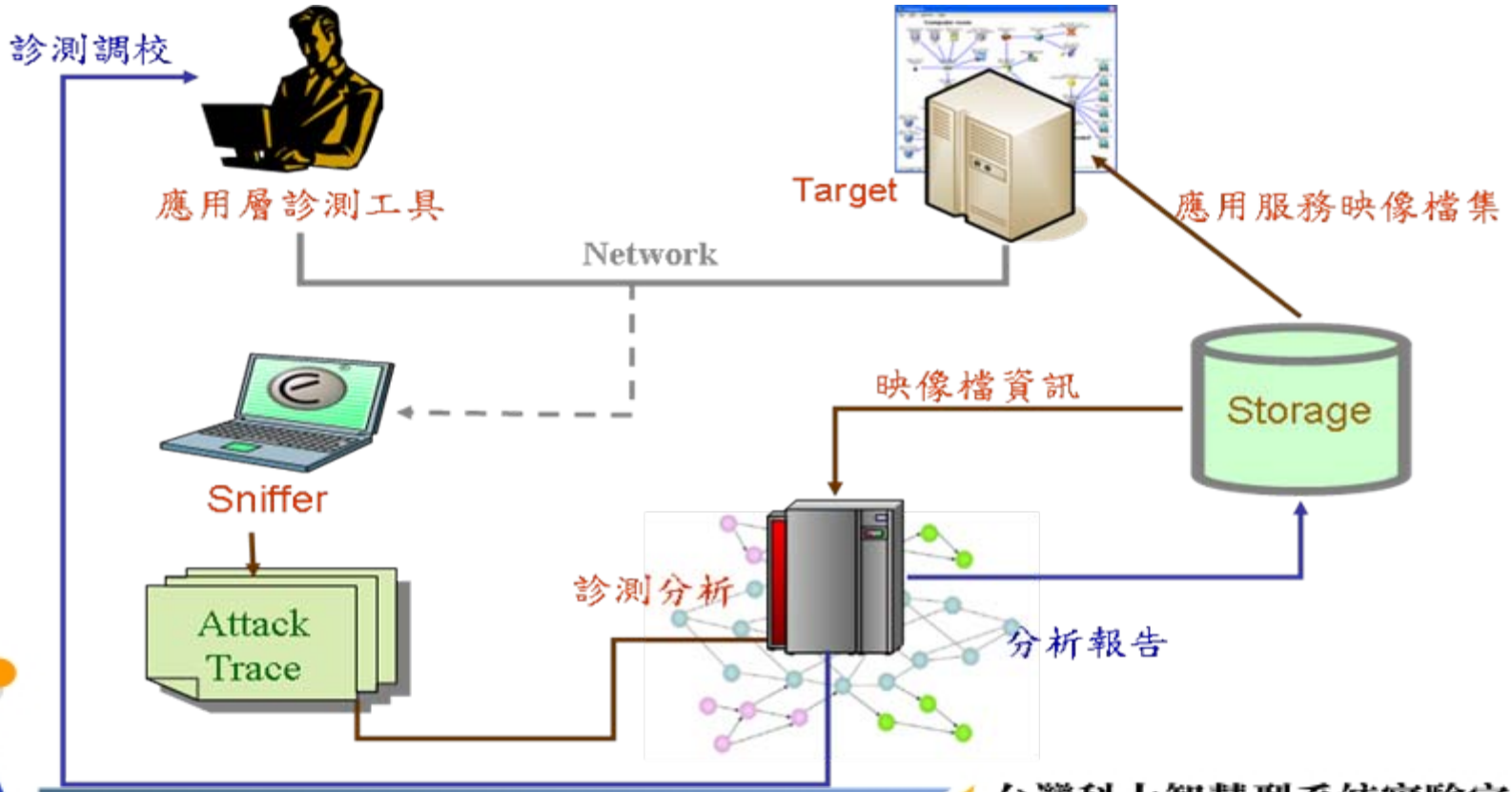
學研計畫架構


資安開放源碼軟體專業人才培訓暨知識平台建置計畫
權重:100%
A.資安開放軟體研究暨專業人才培訓分項
執行單位：台科大/台大 (78.88%)
B. 應用層診測系統調校暨知識平台建置分項
執行單位：資策會 (21.12%)
資安開放軟體研究：
• 弱點掃描技術
• 網路流量監視
• 入侵偵測與防治系統
• 應用層程式安全檢測
• 開放原始碼攻擊
資安專業人才培訓：
• 資安專業課程
• 業界交流
• 成果發表
• 研討會
應用層診測系統調校：
• 調校平台建置
• 應用服務映像檔集(image file set)
• 診測系統調校與分析
知識庫平台建置：
• 資安知識分類
• 平台設計與開發


Intrusion Management
Detection
Analysis
Forensics
Anomaly-based
Alarm Correlation
False alarm reduction
Attack graph for alert analysis
Software Security
Malicious web script inspection
Packet Stream Inspection
Web application attack detection
Cross-level attack behavior detection & analysis
Profiling attack behaviors
Traffic Logging & Analysis
Multi-view attack detection
Rare category attack analysis
Scalable network forensics
Signature-based
Hardware Enhancement
Optimized PCRE matching with FPGA
Cost Efficiency on HW/SW Co-Design
IDEAS
Mal-page Interceptor
HWAIDS
Gestalt
Forensic Analysis System
Machine Learning Core Technology
(LLASA: A Library of Learning Algorithm for Information Security)

應用層診測系統調校示意圖

依診測需求，建立不同弱點的應用服務的映像檔，搭配對應的滲透測試手法，並分析驗測過程封包，以調校並強化應用層診測系統。



Machine Learning in IDEAs

- Learning
  - Automatically learning from expert feedback
- Adaptation
  - Reduce labor work on configuration to a specific environment
- Detection
  - Detecting novel attacks
- Evaluation
  - Ex. Detection rate vs. cost, Accuracy rate …

Criminal Investigation Center

Security Operation Center

Intrusion Detection and **Event Analysis** system

Internet Backbone

High speed links

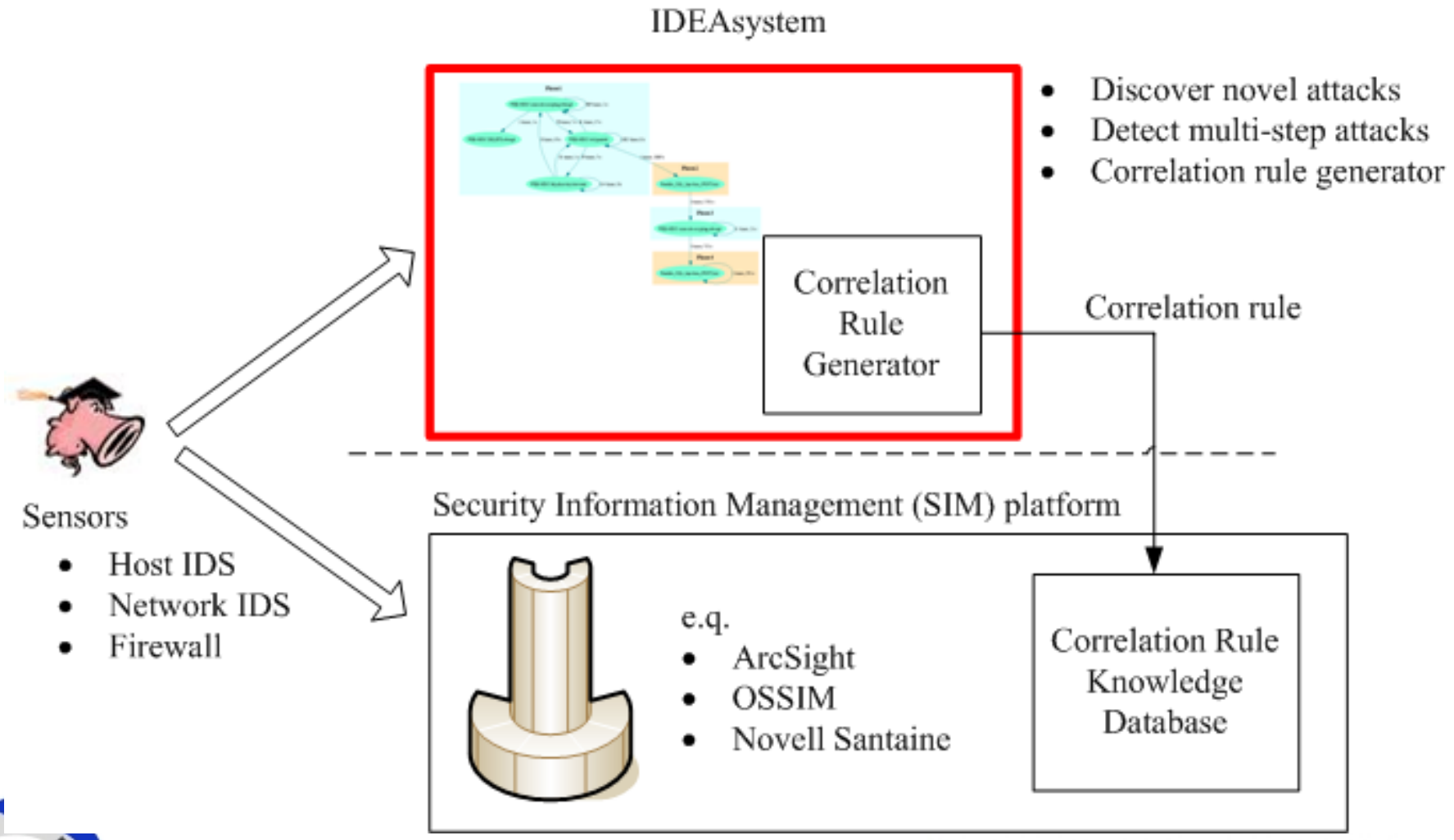
Internet Service Provider

Gateway

Enterprise Servers

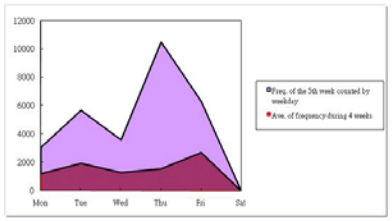
Enterprise Networks

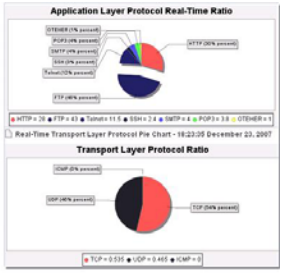
What can IDEAs do for SOC?

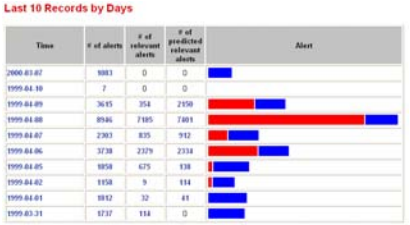


Information Security Station

- Conquer Zero-day attacks with security news collection
- Real-time network traffic abnormally chart
- Daily survey for easily and quickly controlling network statement
- Risk & Threat estimation

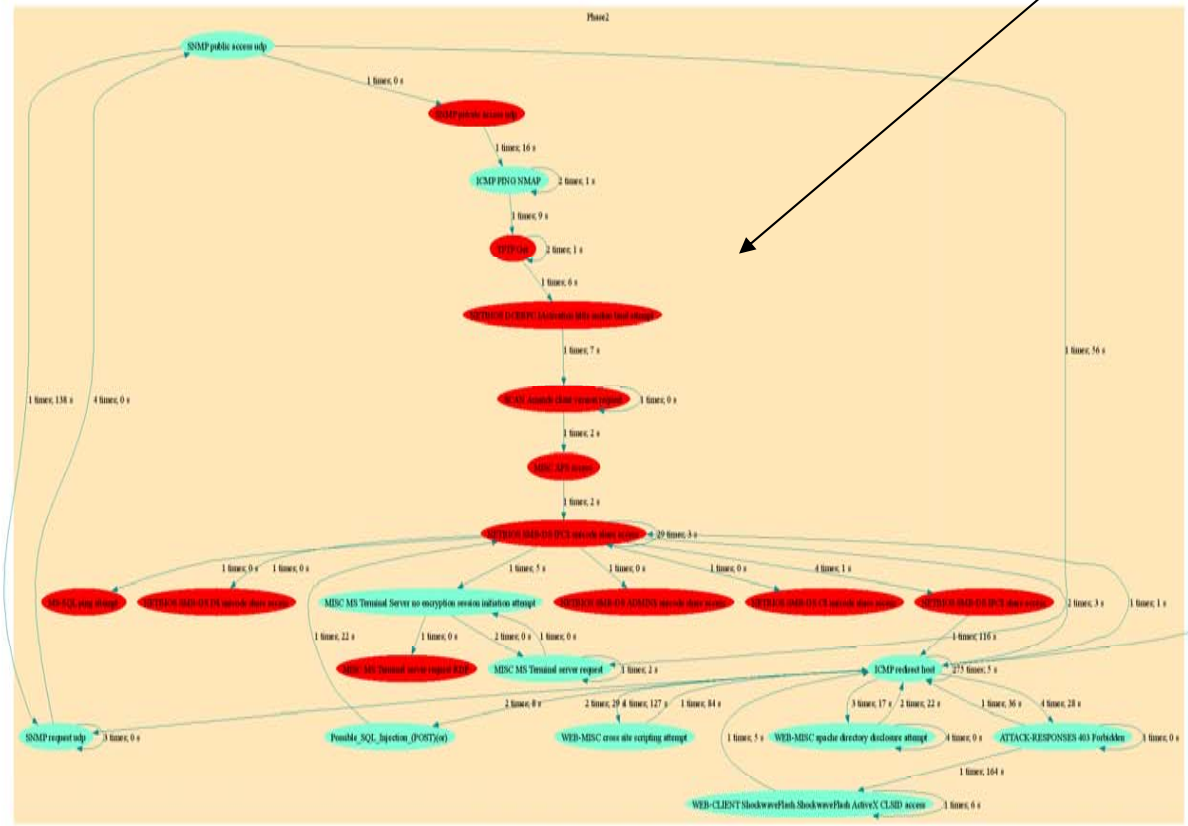




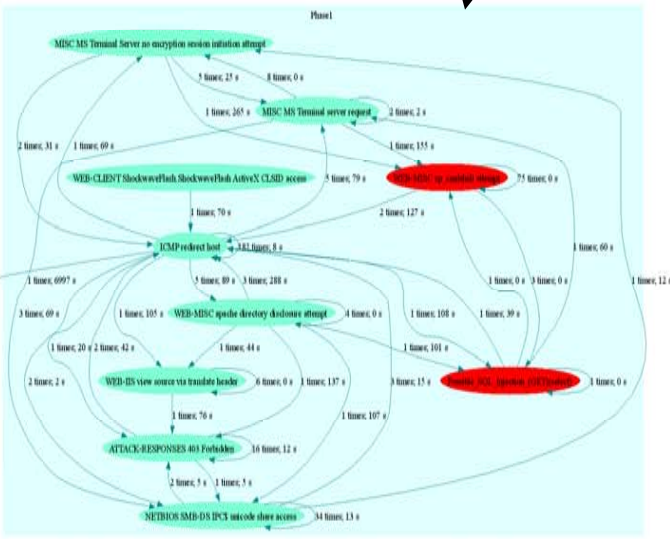


Real Case 1: Trojan Behavior (Data stealth & Self-duplicate)

Phase 2. Scan service and self-duplicate attempt



Phase 1. Data stealth thru web vulnerability



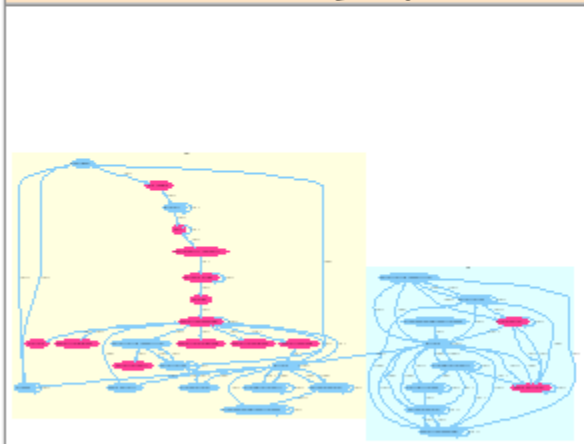
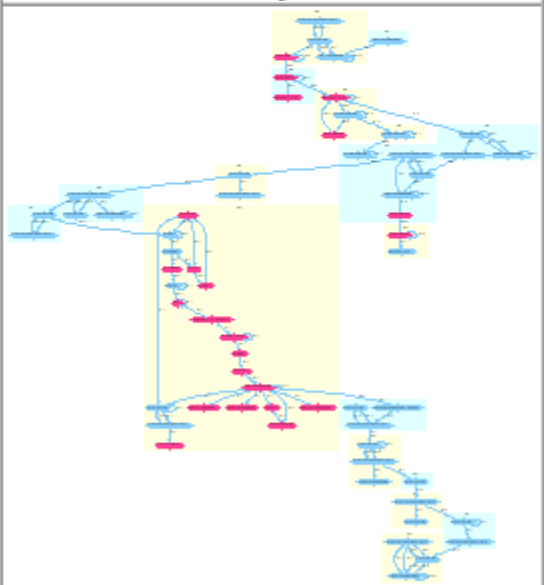
Similar Behavior and Intention Search

Search Similar Graphs

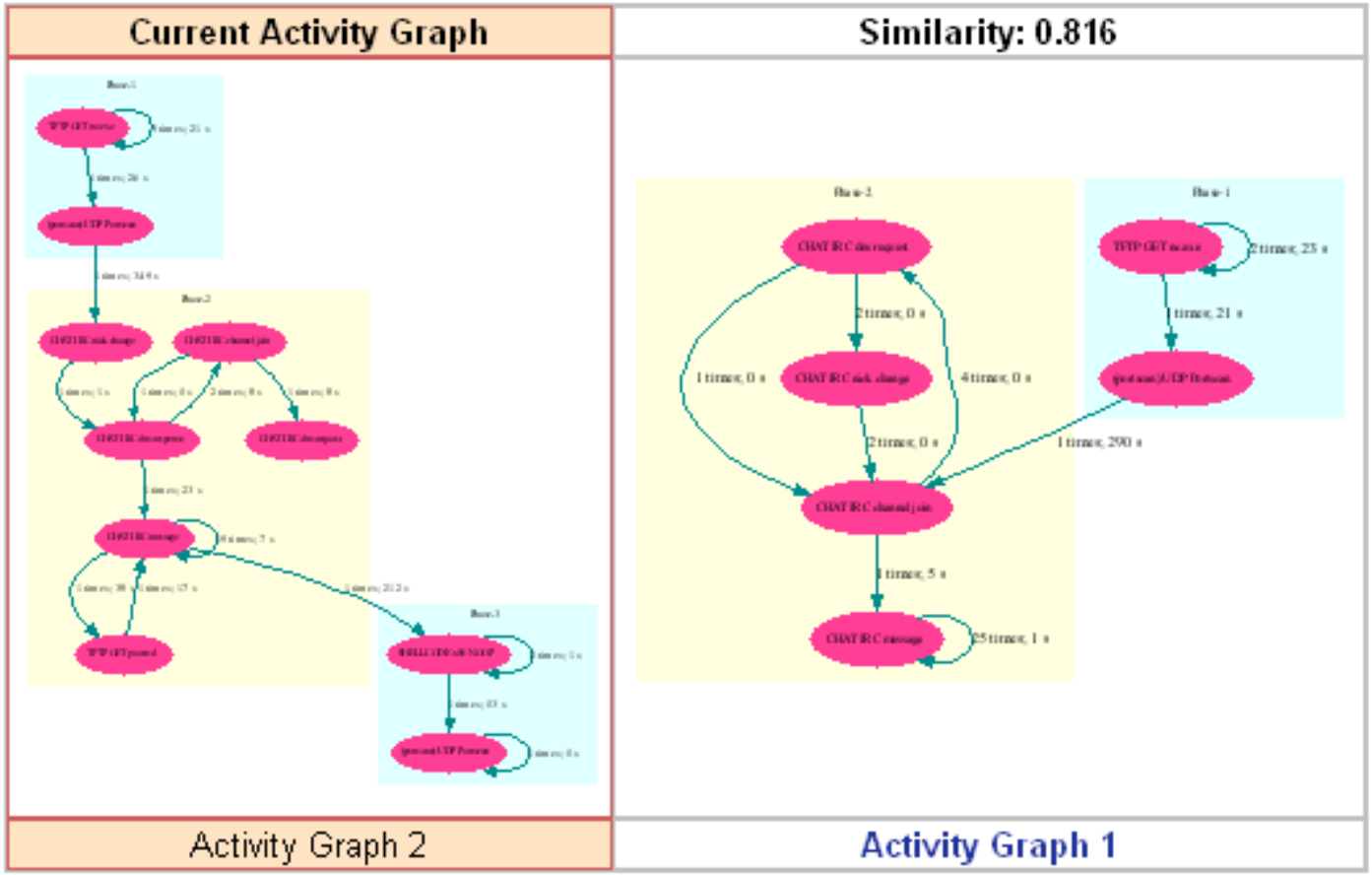
Time Criteria

Similar Graphs : on September 7 2007 -- { month } { year } Order By: predict

Filter Similar Graphs

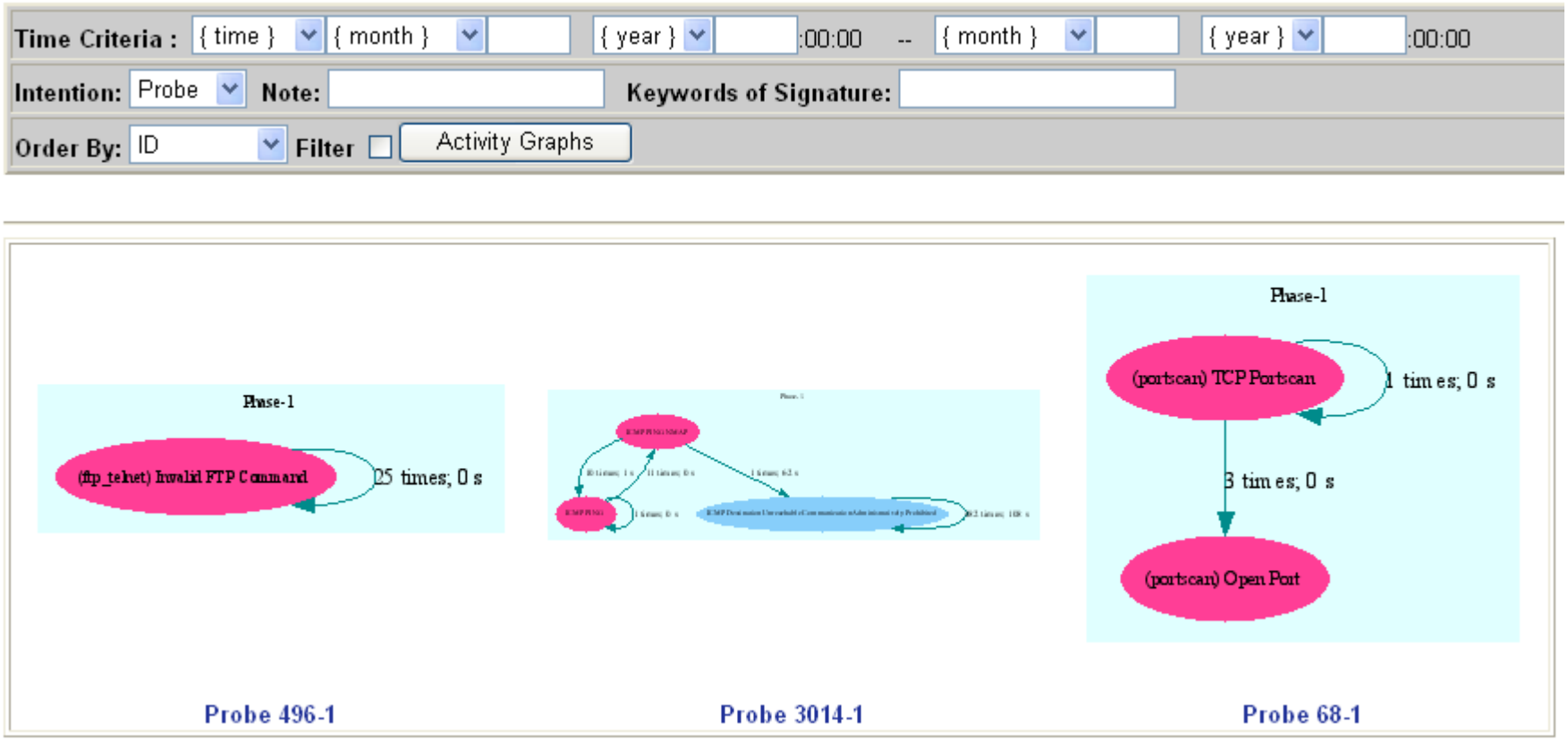
Current Activity Graph	Similarity: 0.846	Similarity: 0.577
		
Activity Graph 286	Activity Graph 113	Activity Graph 434

Case 2: Detect Mutated Bot (Partial Match)



Intention Knowledge Database

- Ex. Intention - Probe pattern



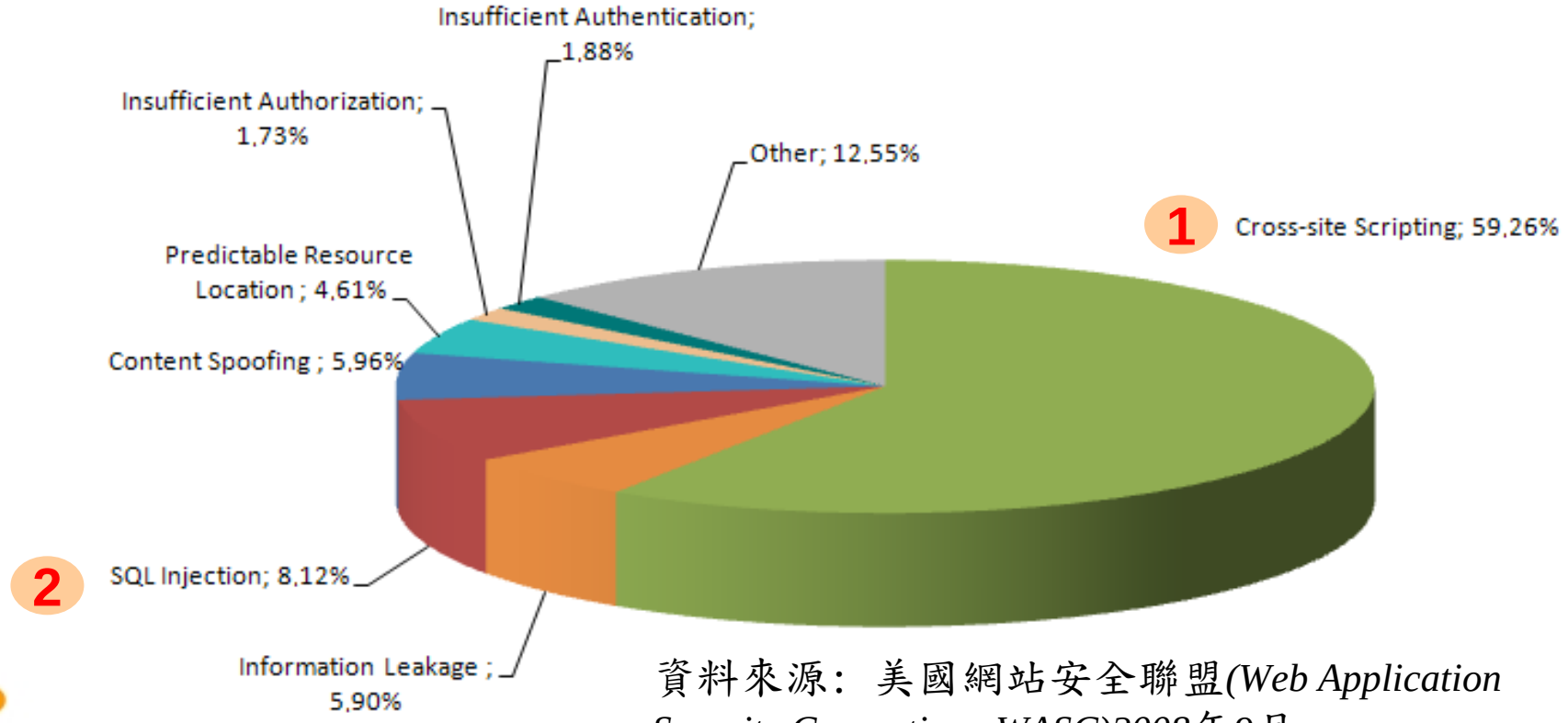
Further Research

- Correlation rule generator
  - Auditing suspicious packets or events for making correlation rule
- Mutated alarm detection
  - Intention knowledge database
- Hard to give all labels on Massive Network data
  - Active learning
- Network Environment is changeable
  - Adaptive Profile
- Alarms vs. Asset vs. Host
  - Relation Data Mining

Conclusion

2008年9月Web AP弱點類型分布

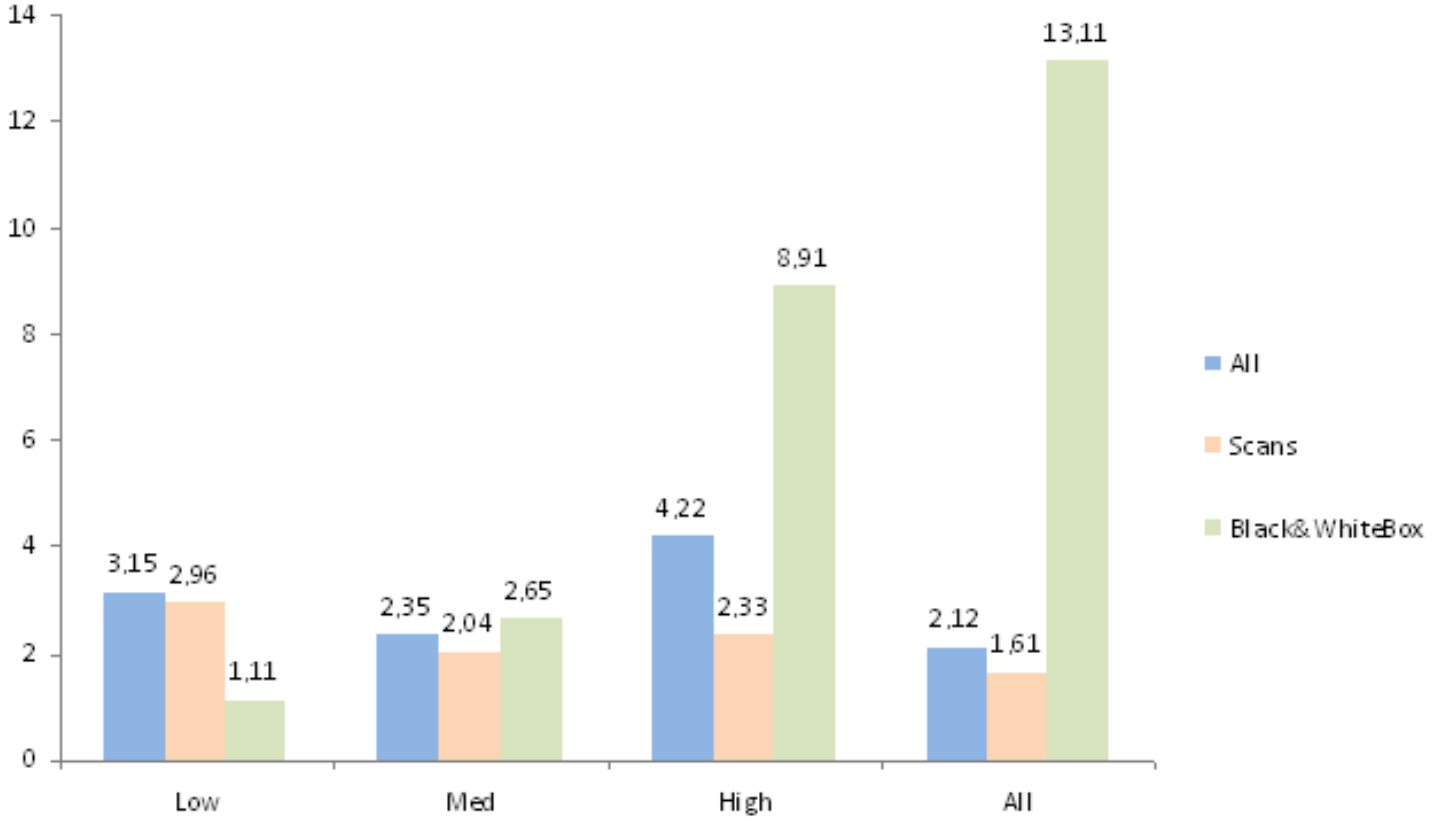
- **超過半數的弱點是跨網站入侵字串(XSS)，其次是SQL嵌入攻擊(SQL Injection)**



資料來源：美國網站安全聯盟(*Web Application Security Consortium, WASC*)2008年9月

網站平均有8.91個嚴重漏洞

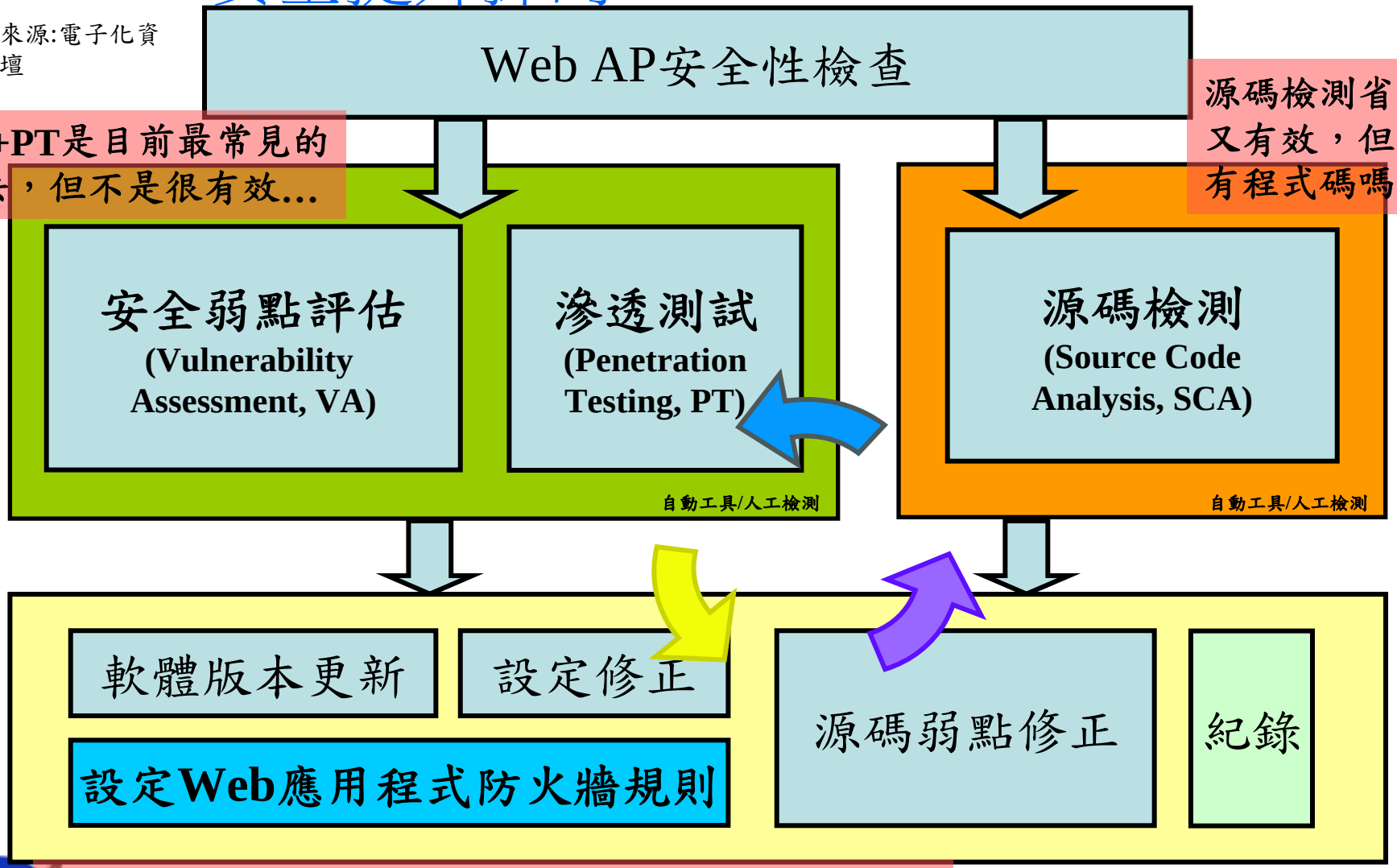
- 程式碼檢測與滲透測試等技術檢測3萬個網站
- 每個網站平均有13.11個漏洞(包括8.91個嚴重漏洞)



資料來源：美國網站安全聯盟(*Web Application Security Consortium, WASC*) *2008*年*9*月

Web AP安全提升探討

資料來源:電子化資安論壇



討論議題

- 政策面
  - *Web AP* 安全仍為重要資安威脅之一，推動策略為何？
  - 承商如何提升*Web AP* 安全能力？
- 標準規範面
  - 如何發展*Web AP* 安全相關標準、規範或檢測工具？
  - *Web AP* 委外採強制或自願性遵循相關標準、規範？或依據系統安全等級規定？
- 稽核管理面
  - 如何建立*Web AP* 安全稽核與驗證機制？
  - 哪些單位適合擔任第三方檢測/驗證單位？

Related resources

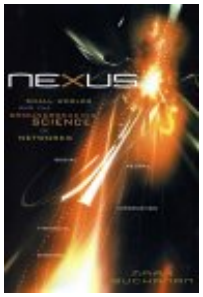
[Information]

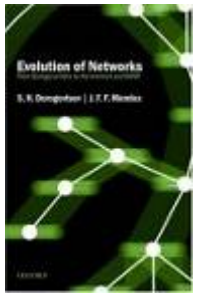
- Social networks - Wikipedia, the free encyclopedia
  http://en.wikipedia.org/wiki/Social_networking
- How to do social network analysis
  http://www.orgnet.com/sna.html
- International Network for Social Network Analysis (INSNA)
  http://www.sfu.ca/~insna/
- NetLab (provides up-to-date information
  on social networks in the broadest sense)
  http://www.chass.utoronto.ca/~wellman/netlab

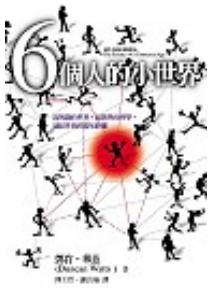
[Tools]

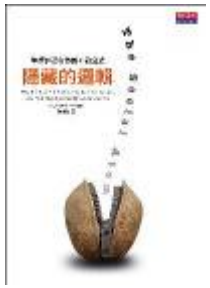
- InFlow (Social Network Mapping Software) http://www.orgnet.com/index.html
- NetMiner (SNA Software)
  http://www.netminer.com/NetMiner/home_01.jsp
- UCINET (SNA Software)
  http://www.analytictech.com/ucinet_5_description.htm
- International Network for Social Network Analysis http://www.insna.org/INSNA/soft_inf.html

References for complex network theory









- Watts, D.J.; Strogatz, S.H. (1998). "Collective dynamics of 'small-world' networks.". Nature 393 (6684): 409–10.
- R. Albert and A.-L. Barabási, Rev. Mod. Phys. **74**, 47 (2002) with 215 references
- S. N. Dorogovtsev and J. F. F. Mendes, Adv. Phys. **51**, 1079 (2002) with 252 references
- M. E. J. Newman, SIAM Rev. **45**, 167 (2003) with 429 references
- S. Boccaletti, V. Latora, Y. Moreno, M. Chavez, and D.-U. Hwang, Phys. Rep. **424**, 175 (2006) with 888 references
- [book] Mark Buchanan,NEXUS:small worlds and the groundbreaking science of networks. 中文譯本:連結
- [book] Duncan J. Watts, SIX DEGREES: The Science of a Connected Age. 中文譯本:6個人的小世界
- [book] Mark Buchanan, The Social Atom：Why the Rich Get Richer, Cheaters Get Caught, and Your Neighbor Usually Looks Like You 中文譯本:隱藏的邏輯：掌握群眾行為的不敗公式

Related resources

- 1) Zone-H (網頁毀容 Defacement為主) http://www.zone-h.org/ ; http://www.zone-h.org/archive/special=1
- 2) 大砲開講 (知名blog) http://rogerspeaking.com/
- 3) 資安之眼 (TW 網站淪陷資料庫) http://www.itis.tw/compromised
- 4) Malware Domain List (寫的蠻詳細的惡意連結清單, 連病毒類型或攻擊方式都列出來) http://www.malwaredomainlist.com/mdl.php?inactive=&sort=Domain&search=&colsearch=All&ascordesc=ASC&quantity=100&page=0
- 5) 中國被黑站點統計系統(仿Zone-H)"：http://www.zone-h.com.cn
- 6) cross-site scripting attached information http://www.xssed.com/archive

IDC Worldwide Security 2008 Top 10 Predictions:

1. 3SN will merge security, systems, storage, and network management.
   三S一N將結合：資安，系統，儲存，與網路安全

2. Web 2.0 and Business 2.0 applications and communities will become a major source of identity fraud, privacy violations, and corporate data loss.
   Web 2.0 與 Business 2.0 的應用將是造成身份偽造，隱私破壞，與企業資料損失的主要原因

3. Crime ecosystems will sell, support, and service crimeware as products or services.
   犯罪經濟體系將把犯罪軟體當作產品與服務來販售，支援與提供服務

4. Datacenter security will be resurrected by a crisis in access and skilled support.
   大型系統的資安因為前代熟大型系統操作人員的退休而有危機

5. Security virtualization will develop in three areas.
   資安將與虛擬環境結合

*: IDC, Christiansen et al., “Worldwide Security 2008 Top 10 Predictions: Security's Troublesome Twins , Crime and Compliance, Ride the Web to Drive 2008 Trends,” Jan 2008, IDC #210400

IDC Worldwide Security 2008 Top 10 Predictions(續):

6. IP protection and data leakage will become major security drivers outside the United States
   美國境外的個人隱私洩漏會非常嚴重

7. Managed and hosted security services will boom.
   線上資安服務將急速成長

8. Mergers and acquisitions will continue, but new companies will continue to enter the market.
   合併與併購將加速，但是新公司將繼續不斷出現

9. Applications testing will be used by large corporations to test software they buy and renegotiate contracts based on service-level agreements (SLAs)
   大型企業將借助測試軟體來定義外包中的SLA與執行驗收驗收

10. Consumer security products and services will migrate away from point products.
    單一產品線已經沒有生存空間，客戶要整合的解決方案

*: IDC, Christiansen et al., "Worldwide Security 2008 Top 10 Predictions: Security's Troublesome Twins , Crime and Compliance, Ride the Web to Drive 2008 Trends," Jan 2008, IDC ##10400

Thank you for your attention !!