NSC Cloud Computing and Information Security Program

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

2012/11

Content

- Taiwan Delegation
- TWISC(TaiWan Information Security Center)
- iCAST(The International Collaboration for Advancing Security Technology)
- NSC Cloud Computing Program
- NSC Information Security Technology Program
- NSC Botnet Program
- Information Security Research in iSLAB(intelligent Systems Laboratory, NTUST)

Taiwan Delegation(NSC)

- NSC (National Science Council)
  - Director General, Department of the Engineering and Applied Sciences, Dr. Ching-Ting Lee (Chair Professor of NCKU)
  - Program Director, Department of International Cooperation, Dr. Hui-Chuan Cheng
  - Assistant Researcher, Department of the Engineering and Applied Sciences, Shih-Yu Hwang

Taiwan Delegation(Team members)

- Dr. Cheng-Chung Chu, Professor/Director, Tunghai University
- Dr. Wei-Cheng Huang, Researcher, National Center for High-performance Computing(NCHC)
- Dr. Yau-Hwang Kuo, Distinguished Professor/Dean, National Cheng Chi University(NCCU)
- Dr. Chin-Laung Lei, Professor, National Taiwan University(NTU)
- Dr. Hahn-Ming Lee, Distinguished Professor, National Taiwan University of Science & Technology(NTUST)

Taiwan Delegation(Team members)(cont.)

- Dr. Yau-Jr Liu, Deputy Director, Taiwan Institute of Economic Research(TIER)
- Dr. Wei-Chung Teng, Assistant Professor, National Taiwan University of Science & Technology(NTUST)(Ph.D., University of Tokyo)
- Dr. Wen-Guey Tzeng, Professor/Chairman, National Chiao Tung University(NCTU)
- Dr. Yih-Kuen Tsay, Professor, National Taiwan University(NTU)
- Dr. Chu-Sing Yang, Professor/Director, National Cheng Kung University(NCKU)

TWISC(Taiwan Information Security Center)

- 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

TWISC(Taiwan Information Security Center)

- Research Activities
  - **Data Security** Cryptology, algebraic cryptanalysis, cloud computing security, post-quantum cryptosystems, database security and access control
  - **Network Security** Security protocol analysis, intrusion detection and prevention, social networking, and wireless network security
  - **Software/Hardware Security** Formal verification and model checking, S/H security assessment, smart card/RFID/FPGA security testing

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

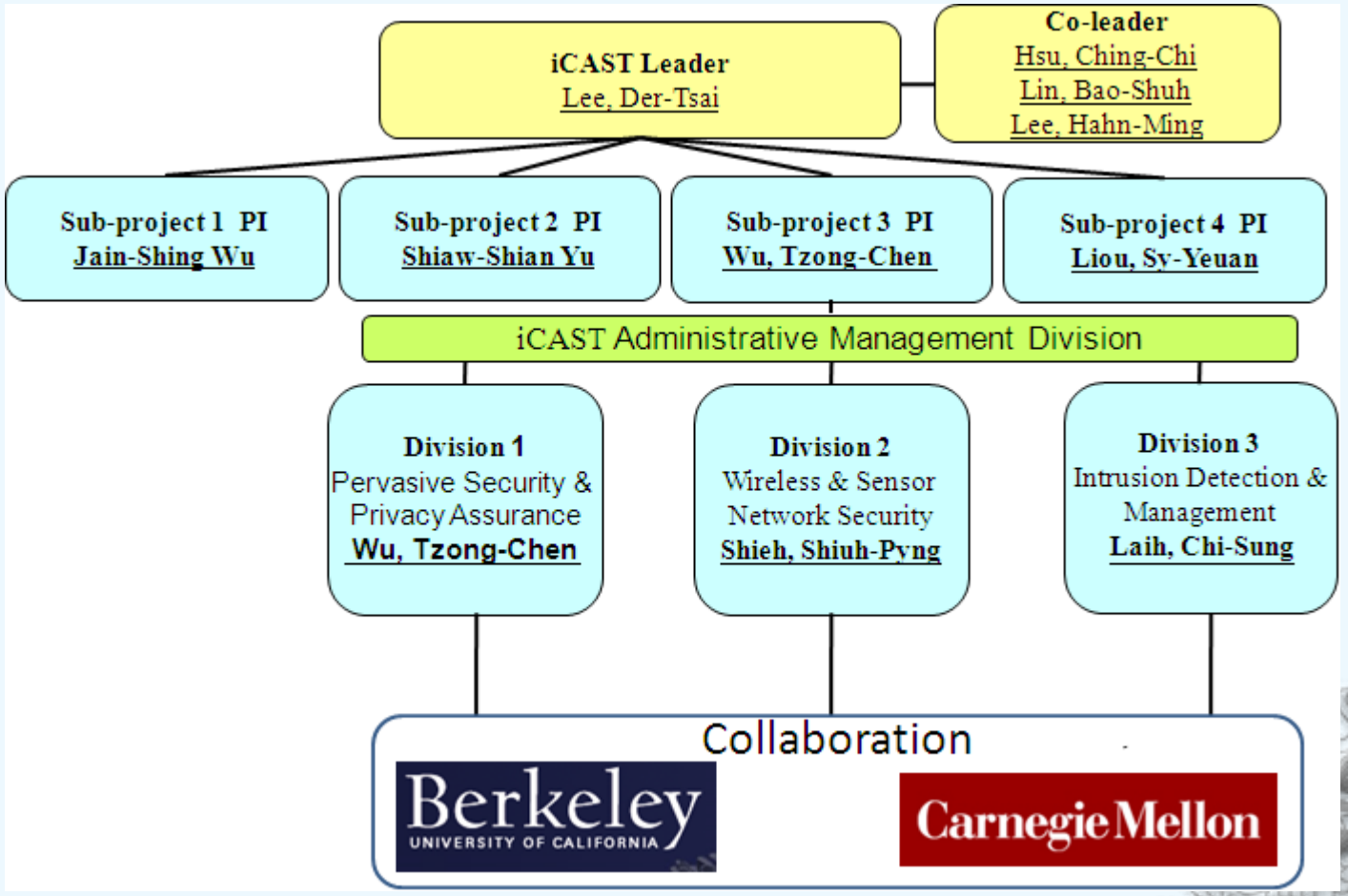
Accomplishments

- **iCAST (2006/6-2009/7)** TWISC/III/ITRI/NDU and CMU/UCB
  - **http://www.icast.org.tw/info/achievements-and-contributions/**
- Development of basic security testing tools for code review and establishment of a web application vulnerability scan platform for vulnerabilities detection, including SQL injection, XSS, etc.
- Development of Smart Card/RFID/FPGA hardware testing techniques, including timing analysis, power analysis and electromagnetic analysis.
- Establishment of **Emulab-based testbed,** Testbed@TWISC that provides a large-scale, user-configurable and controlled environment for network security testing.
- Establishment of an experimental **observation network for wireless network security**, SWOON@TWISC, and a **wireless penetration platform**, WiSec@TWISC, that provides penetration testing of heterogeneous multiple networks, malware discovery and penetration testing in mobile devices.

Accomplishments (cont.)

- **Authenticated Trust Establishment** Development of a prototype for scalable authenticated key exchange using local presence (ACM MobiCom 2008, ACM+Unsenix MobiSys 2009)
- **ECM on Graphics Cards** Efficient implementations of cryptographic and cryptanalysis algorithms on multi-core/many-core computers, achieving a record-setting performance for the elliptic-curve method of integer factorization on graphics cards (*EUROCRYPT* 2009)
- **Phishing detection** Developed a phishing detection scheme based on web page similarity (*IEEE Internet Computing*, 2009)
  - A Firefox plug-in has been implemented and made publicly available
- **Botnet detection** Developed the first real-time detection scheme for fast-flux web sites based on intrinsic properties of fast-flux botnets, including web page fetching delay and processing delay

iCAST(The International Collaboration for Advancing Security Technology) Project Structure



RoadMap

- Security Theory -- cryptology, post-quantum cryptosystem attack analysis, key exchange protocol
- Mobile (and Cloud) Security -- public/private cloud security, mobile privacy protection, anti-infiltration/ anti-phishing mechanism, P2Pcommunication security

- **Communication (and Web) Security -- heterogeneous wireless environment penetration analysis, network protocol security,**
- **Platform Security Testing -- software security assessment, hardware (networking gears, smart card) security testing, embedded system testing**

- Develop algorithms and cutting-edge technologies to sustain secure computing and counter rampant cyber-crime in this interconnected world
- Make the omni-present, always-on networking environment more secure and be best equipped for fast-changing challenges
- Design more secure protocols for networking and communication
- Improve network equipment's reliability and help detect weakest link that hinders infiltration-proofing

2010 | 2011 | 2012 | 2013 | 2014 | 2015 | 2015-2018

NSC Cloud Computing Program Objective

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

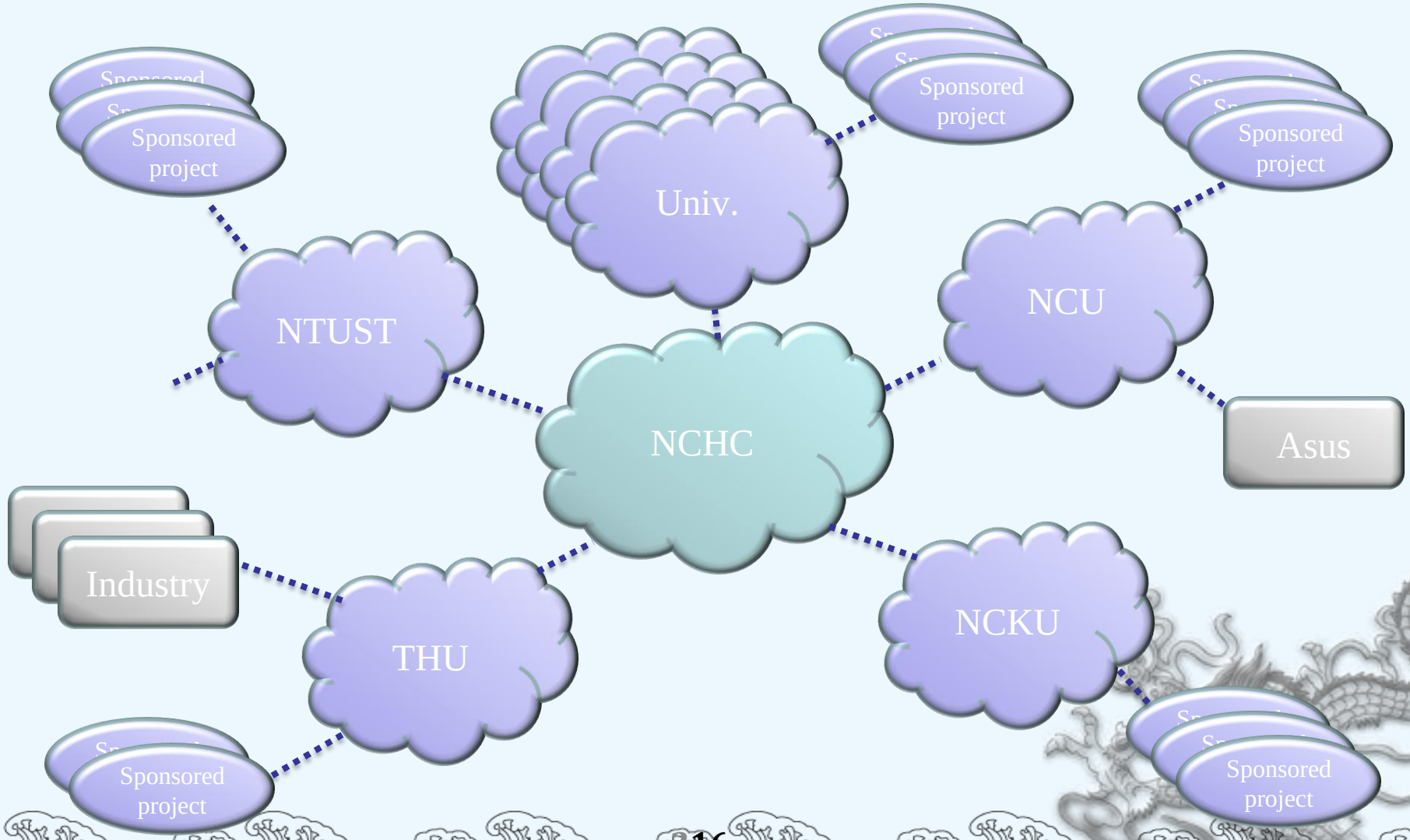
Cloud Computing Research Topics

- **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 Research Topics (cont.)

- **Cloud computing innovative applications**
  - Highlight merit different to classic IaaS, PaaS or SaaS models
  - Capable of verifying whether the cloud computing key technology or innovative operation model can scale up user population with verification plan
  - Application technology or services with a connotation of scientific R & D

Academic and Research Cloud



NSC Information Security Technology Program Objective

- Improve the research power of security and innovative application key technologies
- Promote enterprise, academic and research organizations to collaborate developing information security software and innovative applications
- Train engineering and creative talents required by security software industry
- Encourage cooperation of Taiwan academic and international top research organization for developing information security technology
- Promote information security community

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 data 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

NSC Botnet Program Objective

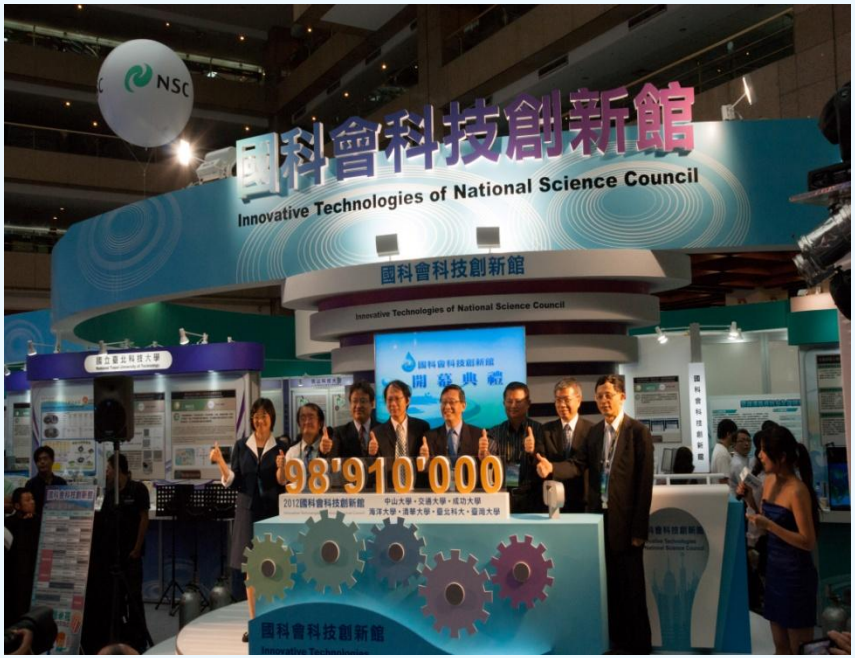
- Develop cloud security middleware and build demonstrative investigation and prevention facilities
- Construct security event and signature database, developing environment and detection and protection tool
- Encourage cooperation of Taiwan academic and international top research organization for constructing security database, joint investigation and prevention environment
- Offer accumulated security event data

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

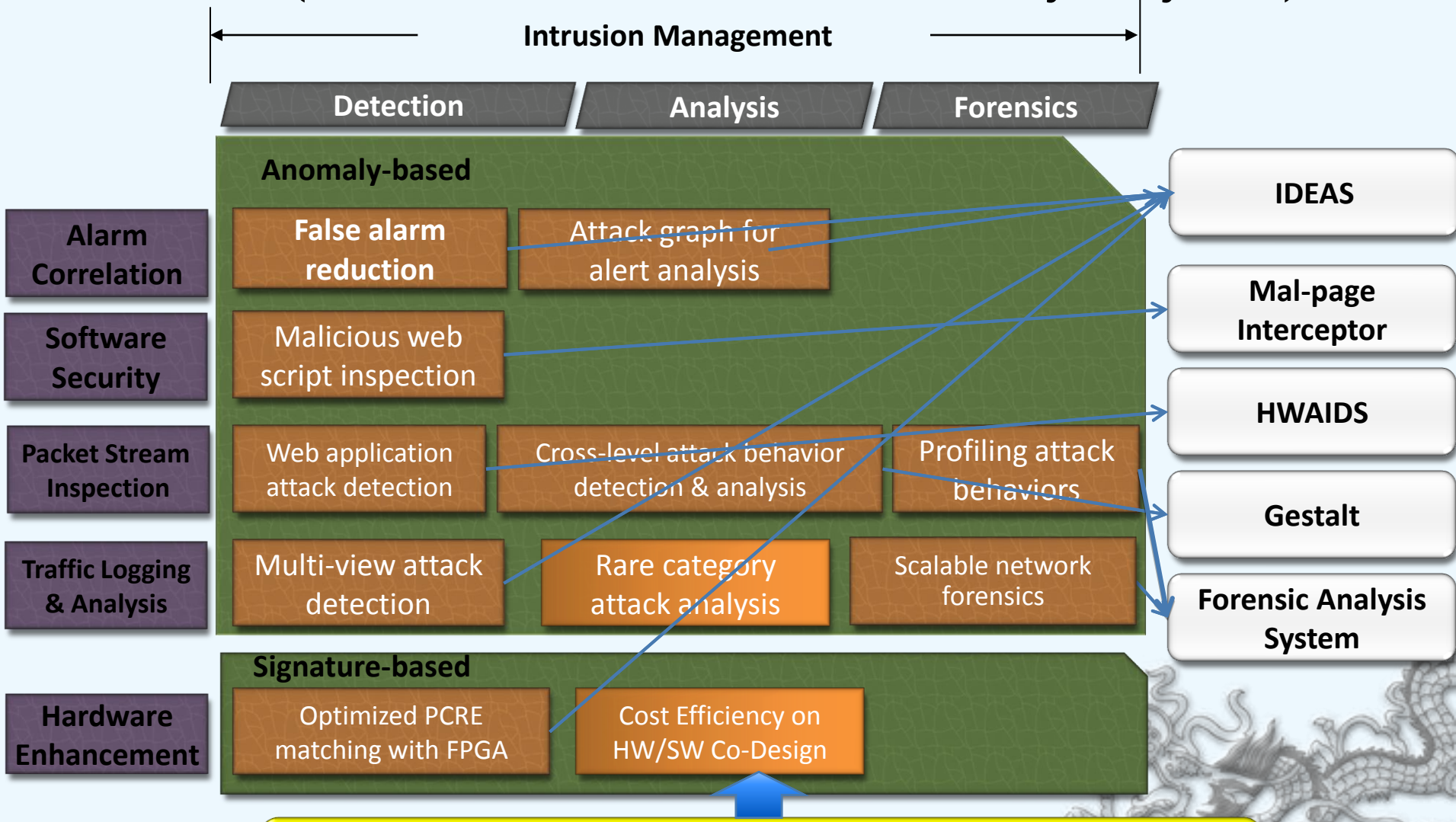
Program Performance

- Outstanding project teams are recommended to show at **2011/2012 Taipei International Invention Show & Technomart-NSC technology innovation section**
- Exhibit time: 2011/9/29~10/2; 2012/9/20~9/23
- Exhibit place: Taipei World Trade Exhibition Hall

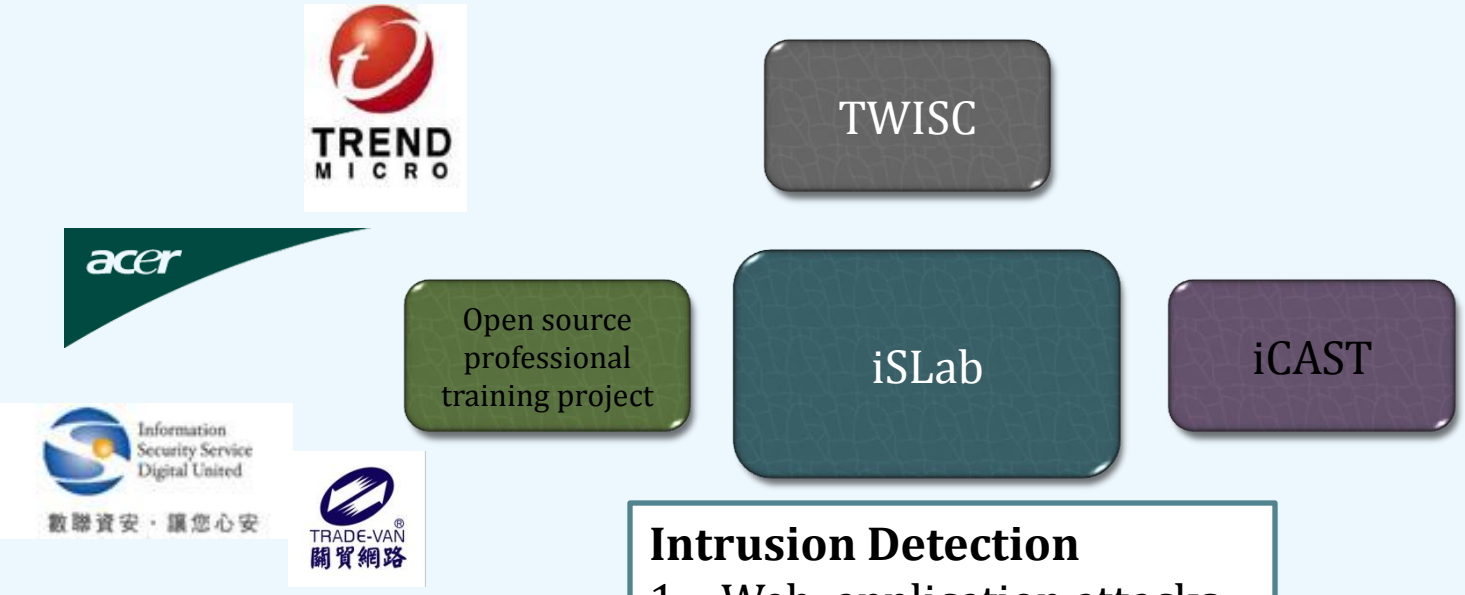


Information Security Research in iSLAB(intelligent Systems Laboratory, NTUST)

IDEAs(Intrusion Detection and Event Analysis System)



The Bridge in Information Security-iSLAB



Academia Sinica

Carnegie Mellon University

Cornell University

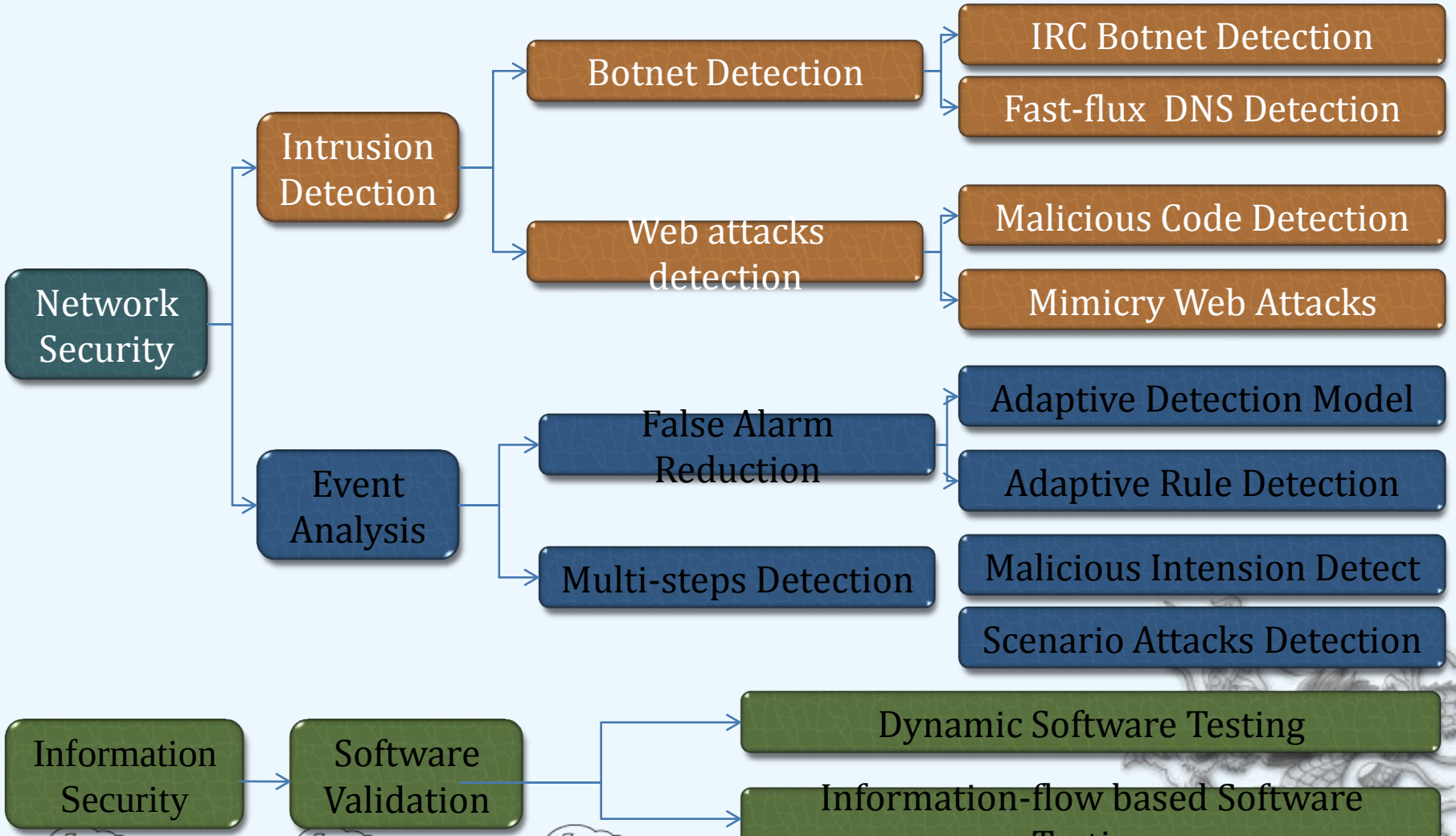
Intrusion Detection
1. Web application attacks
2. Botnet Detection
3. Anti-spam

Event Analysis
1. False alarm reduction
2. Multi-steps detection

Software Validation
1. Dynamic testing

Business application ← → Core tech. R&D

Roadmaps of Information Security Research in iSLAB



INTRUSION DETECTION IN NETWORK

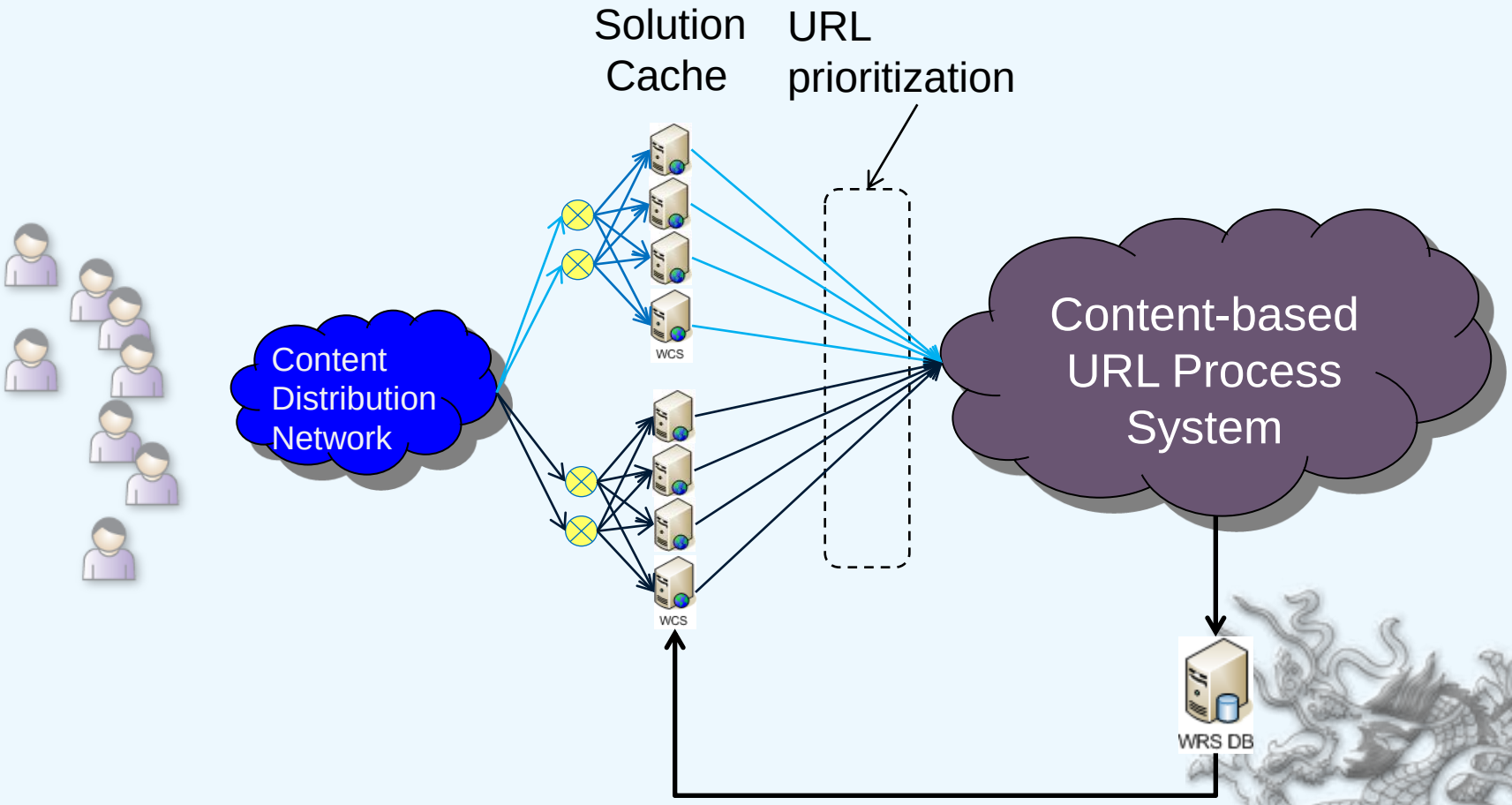
IRC Botnet C&C Detection

Fast-flux DNS Service Detection

Web-Application Attacks Detection

Suspicious URL Filter

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.

Obfuscated Malicious JavaScript Detection by Causal Relations Finding

DroidMat:
Android Malware Detection through Manifest and API Calls Tracing

THANK YOU!