NETSAP 2015: The 5th IEEE International Workshop on Network Technologies for Security, Administration and Protection

Program
Saturday July 4
17:15 - 18:45
Location: H106
Session Chair: Chu-Hsing Lin, Tunghai University, Taiwan

- Security Design for Configuration Management of Android Devices
  Cheng-Liang Kuo, Chung-Huang Yang
- Malware Detection System based on API Log Data Mining
  Chun-I Fan, Han-Wei Hsiao, Chun-Han Chou, Yi-Fan Tseng
- Web Server Protection against Application Layer DDoS Attacks Using Machine Learning and Traffic Authentication
  Jema David Ndibwile, A. Govardhan, Kazuya Okada, Youki Kadobayashi
- A Simulation Approach to Quantify Network Survivability on MANETs
  Zhipeng Yi, Tadashi Dohi

This workshop aims to discuss and advance research and development of practical systems to fight against cyber attacks. The workshop focuses on development of practical systems and methodologies including measurement and analysis of real traffic and also privacy issues about network monitoring. The workshop addresses researchers from different disciplines in academia and industry, as well as industry.

Announcements
Signichat conference mobile app is now available!

The COMPSAC 2015 Survey has been posted!

Hotel information has been posted to the Travel and Venue page.

The link for registration has been posted to the Registration page.

Important Dates

PC Meeting: March 13-14, 2015 - Shanghai,
COMPSAC 2015 Deadlines
April 6, 2015: Extended: April 15, 2015 - Camera-ready copy & registration due
Workshop & Tutorial Deadlines
April 10, 2015 - Extended: April 15, 2015 - Update Workshop paper notifications
April 14, 2015 - Updated: April 24, 2015: May 8 - Camera-ready registration due
Fast Abstracts, Posters Deadlines
April 24, 2015: Poster/paper notification Updated: May 8
Updated: May 22 - Camera-ready registration due
Student Research Symposium/Competition
April 15, 2015: Updated: April 28, 2015: Notifi
April 28, 2015 Updated: April 30 - Camera-ready registration due
practitioners, who share interests in countermeasures against cyber attacks.

Because of recent expansion of cyber attacks, many organizations and persons have been affected through their activities on the internet. DDoS attacks to government sites, online trading/shopping sites are typical examples where many people cannot access their desired information. Furthermore, there are many online services that offer DDoS attacks, so that attackers easily intimidate organizations to perform DDoS attacks.

Increase of targeted attacks and variant explosion of malwares make security systems difficult to detect such malicious activities. As a result, incidents of information leakages have silently and frequently occurred in many organizations.

In order to take countermeasures against the attacks, various types of systems have been proposed in literature. Although benchmark results and simulation experiments could show good performance, most methods cannot be practically applicable to the real environment. Basically, this gap between theory and practice is caused by too much benchmark-optimization on algorithms or by unrealistic assumptions on simulation settings.

In this workshop, we focus on practical systems to fight against cyber attacks. Mechanisms, algorithms and strategies that are used in the real field will be discussed. Measurement and analysis of real traffic is also welcomed for aiming at new directions of future research. In addition to practical systems, we would like to discuss privacy issues about network monitoring.

Any submission whose content is relevant to the area of network technologies for security, administration and protection will be considered, but any submission whose subject matter is related to one of the following topics will be particularly welcome:

- Intrusion detection and protection
- DoS attack detection and protection
- Malware analysis
- IP Traceback
- Computer Forensics
- Countermeasures against advanced persistent threats
- Privacy in network monitoring
- Trusted computing
- Cloud security
- IoT security
- Big data security
- Mobile security

Authors are invited to submit original, unpublished research papers as well as industrial practice papers. Simultaneous submissions to other publications and conferences are not permitted.

The length of a camera ready paper will be limited to 6 pages (IEEE Proceedings style) with up to 2 additional pages (with charges for each additional page) printed on 10-12 point fonts.

Authors must follow IEEE CS Press Proceedings Author Guidelines (http://www.computer.org/web/cs-cps/authors) to prepare papers. At least one of the authors of each accepted paper is required to pay full registration fee and present the paper at the workshop in person.