IEEE Systems Journal

Special Issue on "Traffic Forensics: Systems, Tools, and Experimentations"

CALL FOR PAPERS

GUEST EDITORS

Ying-Dar Lin, National Chiao Tung University, Taiwan, ydlin@cs.nctu.edu.tw
Yuan-Cheng Lai, National Taiwan University of Science and Technology, Taiwan, laiyc@cs.ntust.edu.tw
George Kesidis, The Pennsylvania State University, USA, kesidis@cse.psu.edu
Athanasios V. Vasilakos, Kuwait University, Kuwait, vasilako@sci.kuniv.edu.kw

SCOPE

As social networking, business activities, entertainment applications, and multimedia services on the Internet are becoming more popular, many cyber criminals are using a greater variety of IT techniques to generate more serious threats to network security. The consequences, including private information leakage, service outages, and damage to software and hardware, generate significant economic losses. Guarding the network against these threats is obviously necessary and requires advances in network forensics to capture, record, and analyze events, occurring in the end-hosts and the networks, in order to, e.g., discover the source of security breaches or other problematic incidents (i.e., attribution). Though network forensics has been actively researched for over a decade, many challenging issues remain pending without satisfactory solutions. The techniques of network forensics can be applied to processing events on end-hosts and networks.

This special issue focuses on "traffic forensics" pertaining to processing events on networks in complex systems and systems of systems, to advance and disseminate system research that deals with the acquisition, preservation, examination, analysis, and presentation of network-traffic evidences for deeper or broader traffic forensics, tools realizing these techniques, and experimental studies based on these consolidated systems and tools. Topics of interest in complex systems and systems-of-systems at the system level include, but are not limited to:

- Traffic forensics
- Traffic forensic frameworks and analysis tools
- Cooperative and distributed forensics systems
- Anti-forensics techniques, methods, and systems
- Data visualization systems in traffic forensic analysis
- Tools for traffic capture, replay, classification, and extraction
- Methodologies, systems, and tools in handling real traffic
- Experimental studies based on traffic forensic systems and tools
- Repositories of malicious traffic including intrusions, malware and spam
- Mobile application security systems for mobile malware
- Modeling, evaluation, and analysis tools for traffic forensics
- Traffic forensic systems and tools in peer-to-peer networks
- Traffic forensic systems and tools in mobile networks
- Traffic forensic systems and tools in social networks
- Traffic forensic systems and tools in cloud computing

SUBMISSION GUIDELINES

Authors are invited to submit original research contributions by following the detailed instructions given in the "Information for Authors" at http://ieeesystemsjournal.org. In the cover letter, authors should explicitly state that the paper is submitted to the "Special Issue on Traffic Forensics: Systems, Tools, and Experimentations". Questions about the special issue should be directed to the Guest Editors.

SCHEDULE

Paper submission deadline:	Jan 31, 2014
Notification of the first review:	May 15, 2014
Revised paper submission:	June 30, 2014
Notification of acceptance:	August 31, 2014
Final manuscript:	October 15, 2014
Expected publication:	early 2015