Title:

Abnormal Traffic Analysis in Cloud Computing

Abstract:

The rapid development of Internet techniques especially the widely used cloud computing makes the development and deployment of services more and more easily. However, the emerging malicious software such as trojans, ransomware, and espionage also use the cloud platform to deploy their command and control, repository or guiding server. Meanwhile, to hide the attack trace, the attackers also will use the cloud platform as the step-stone to achieve the anonymity. Abnormal traffic analysis aims to find those dangerous or suspicious network communications, detect and locate the abusively used cloud host. The aim of this workshop is to bring together the researchers from academia and the industry to share the latest research accomplishments and discuss their novel thoughts and viewpoints.

Scope and Topics:

This workshop covers various aspects of abnormal traffic analysis in cloud environments. We encourage prospective authors to submit their research papers on the subject of both: theoretical approaches and practical case reviews. The topics include but are not limited to:

- ✧ Abnormal DNS traffic detection
- ✧ Abnormality detection based on flow content
- ✧ Abnormal interactive C&C traffic detection
- ✧ Abnormal encryption traffic detection
- ✧ Abnormal encryption traffic analysis
- ✧ Obfuscated traffic detection
- ✧ Network covert channel detection
- ✧ Stepstone virtual host detection.
- ✧ Communication behaviors modeling
- ✧ Machine learning of network traffic
- ✧ Large-scale traffic processing architecture
- ✧ Large-scale monitoring log storage
- ✧ Security visualization for traffic monitoring

Program Committee Chairs:

Guangjie Liu, Nanjing University of Science and Technology, China
Guangjie Liu is associate professor of Nanjing University of Science and Technology. He received his BE degree in Information Engineering in 2002, and his PhD degree in Control Science and Engineering in 2006, both from Nanjing University of Science and Technology (NJUST). During 2007 to 2009, he was a postdoctoral research fellow with Pattern Recognition Key Lab. of NJUST and Lecturer with Department of Information Engineering. Since 2010, he has been an Associate

Professor with NJUST. Since 2015, he has been Director of NUST Cyber Security Institute, leading the research of Network Traffic Analysis. He has published around 90 scientific papers, and his research interests are mainly on covert communication (underwater acoustics communication, covert wireless communication), cyber security (including digital forensics, information hiding and digital watermarking, network covert channel, network traffic analyzing, systems security, trust management), multimedia computing (including image/video processing, analyzing and comprehending), applications of artificial intelligence (NOT theory) in cyber security and multimedia computing, and applications of nonlinear science (chaos) in cryptography. He is a Member of the IEEE and ACM, technical program committee of several international conferences.

Victor Govindaswamy, Concordia University, USA
Dr. Victor Govindaswamy is with Concordia University Chicago. He is associate professor of computer science and director of computer science programs. his research involved real time distributed systems and software engineering when he was actively involved in the United States' Department of Defense (DoD)'s Defense Advanced Research Projects Agency (DARPA) and Naval Surface Warfare Center (NSWC) sponsored DeSiDeRaTa middleware project. He had also researched in security, telemedicine, telehealth and green technology. He had developed novel schemes such as the RECHOKe (REpeatedly CHOose and Keep for responsive flows, REpeatedly CHOose and Kill for unresponsive flows), RCUBE (Receiver-Window Modified Random Early Detection queues with RECHOKe), RWM (Receiver-Window Modified) and Clumpsort, and had also developed a software process that guarantees to provide survivability, timeliness, scalability and profiling services, even under heavy tactical loads, to applications without the need for writing massive programs to provide such services. He has contributed more than 100 paper and was involved in more 500 international conferences and more than a dozen journals as an editor, also has chaired about 5 international conferences.

Jinwei Wang, Nanjing University of Information Science & Technology, China
Jinwei Wang was born in Inner Mongolia, China, in 1978. He received the B.A.Sc. in automatic control from Inner Mongolia Electric Power College in 2000. He was a teaching assistant at Inner Mongolia University of Technology from July 2000 to September 2002. He received the Ph.D. student in information security at Nanjing University of Science & Technology in 2007 and was a visiting scholar in Service Anticipation Multimedia Innovation (SAMI) Lab of France Telecom R&D Center (Beijing) in 2006. He worked as a senior engineer at the 28th research institute, CETC from 2007 to 2010. He worked as a visiting scholar at New Jersey Institute of Technology, NJ, USA from 2014 to 2015. Now he works as a professor at Nanjing University of Information Science and Technology. His research interests include multimedia forensics, multimedia encryption and multimedia watermarking. He has published more than 60 papers, hosted and participated in more than 10 projects.

Krzysztof Szczypiorski, Warsaw University of Technology, Poland
Krzysztof Szczypiorski is Professor of Telecommunications at Warsaw University of Technology (WUT), Poland. He is the head and founder of Cybersecurity Division, Institute of Telecommunications (IT), faculty of Electronics and Information Technology (FEIT), WUT. And coordinator of B.Sc. Program in Cybersecurity at FEIT, WUT. Krzysztof holds a D.Sc.

(habilitation/higher doctorate, 2012), a Ph.D. (doctorate, 2007), and a M.Sc. (master's degree, 1997) all in Telecommunications with specialization in Information Security from WUT. He also finished his postgraduate studies in Psychology of Motivation (2013) at SWPS University of Social Sciences and Humanities, Warsaw, Poland. In 2013 Krzysztof graduated from Hass School of Business, University of California, Berkeley, USA. For 20+ years Krzysztof serves as the independent consultant in fields of cybersecurity, telecommunications and computer science for many entities including: Cisco Systems, Hewlett-Packard, Ministry of Finance (Poland), National Security Bureau (Poland), Oracle, Orange, Parliament of Republic of Poland, Polish Energy Group, PwC, T-Mobile Poland. Krzysztof is an author (or a co-author) of 180+ papers and 70+ invited talks as well as an inventor of 3 patent applications (one of them is granted). A guest editor of 10+ special issues of top ICT journals.

Program Committee:

pending