

Workshop Description:

The proliferation of Internet services and applications is bringing systems and network security issues to the fore. The past few years have seen significant increase in cyber attacks on the Internet, resulting in degraded confidence and trust in the use of Internet and computer systems. There is an increasing demand for measures to guarantee the privacy, integrity, and availability of resources in distributed systems, such as Grid and P2P systems. The attacks, including DDoS, email virus, and worms, are getting more sophisticated, spreading faster, and causing more damages. The attacks originally exploited the weakness of the individual protocols and operating systems, but now also have started to attack the basic infrastructure of the Internet. There is a consensus that a key contributing factor leading to cyber threats is the lack of integrated and cohesive strategies that extend beyond the network level, to protect the applications and devices at system level as well. Many techniques, algorithms, protocols and tools have been developed in the different aspects of cybersecurity, namely, authentication, access control, availability, integrity, privacy, confidentiality and non-repudiation as they apply to both networks and systems. This workshop aims to bring together the technologies and researchers who share interest in the area of network and distributed system security. The main purpose is to promote discussions of research and relevant activities in security-related subjects. It also aims at increasing the synergy between academic and industry professionals working in this area.

Topics of interest include but are not limited to:

- Ad hoc and sensor network security

- Cryptographic algorithms and distributed digital signatures
- Distributed denial of service attacks
- Distributed intrusion detection and protection systems
- Firewall and distributed access control
- Grid computing security
- Key management
- Network security issues and protocols
- Mobile codes security and Internet Worms
- Security in e-commerce
- Security in peer-to-peer and overlay networks
- Security in mobile and pervasive computing
- Security architectures in distributed and parallel systems
- Security theory and tools in distributed and parallel systems
- Video surveillance and monitoring systems
- Information hiding and multimedia watermarking in distributed systems
- Web content secrecy and integrity

General Co-Chairs:

Cheng-Zhong Xu, Wayne State University, USA

Xiaobo Zhou, University of Colorado at Colorado Springs, USA

Program Chair:

Li Xiao, Michigan State University, USA

Program Committee:

Kevin Butler, Pennsylvania State University, USA

David Chadwick, University of Salford, UK

Songqing Chen, George Mason University, USA

Wenliang Du, Syracuse University, USA

Yong Guan, Iowa State University, USA

Minaxi Gupta, Indiana University, USA

Anca Ivan, IBM T. J. Watson Research Center, USA

James B. D. Joshi, University of Pittsburgh, USA

Alex X. Liu, Michigan State University, USA

Donggang Liu, University of Texas at Arlington, USA

Geyong Min, University of Bradford, UK

Vassilis Prevelakis, Drexel University, USA

Jian Ren, Michigan State University, USA

Chik How Tan, Gjøvik University College, Norway

Wietse Venema, IBM T.J. Watson Research Center, USA

Haining Wang, College of William and Mary, USA

Jianbin Wei, South Dakota School of Mines, USA

Greg B. White, The University of Texas at San Antonio, USA

S. Felix Wu, University of California at Davis, USA

Ye Xia, University of Florida, USA

Bin Xiao, Hong Kong Polytechnic University

Dongyan Xu, Purdue University, USA

Dong Xuan, The Ohio State University, USA

Ossama Younis, University of Arizona, USA

Sheng Zhong, State University of New York at Buffalo, USA

Sencun Zhu, Pennsylvania State University, USA

Advisory Committee:

Kai Hwang, University of Southern California, USA

George Cybenko, Dartmouth College, USA

Xiaodong Zhang, Ohio State University, USA

C. Edward Chow, University of Colorado at Colorado Springs, USA