Tutorial 4

Secure Event Dissemination in Publish-Subscribe Networks

Ling Liu
College of Computing
Georgia Institute of Technology
lingliu@cc.gatech.edu

With the increasing popularity of publish-subscribe networks and event-driven computing architecture, event dissemination in publish-subscribe networks is a target of adversaries. There are many security threats to event-dissemination networks. Adversary can prevent users from getting correct data from pub-sub nodes by modifying the contents of the messages, or spoofing the identity of the publishers, subscribers, or pub-sub routing nodes. An adversary can block communication between a publisher and subscribers by creating false routing information, or simply generating jamming signals. An adversary can gain control of an entire pub-sub tree by spoofing the identity of a publisher. An adversary can compromise a routing node, get all information from that node, and can even re-program it to behave like a malicious node. The design and implementation of a secure and dependable publish-subscribe network must simultaneously address three research challenges: (1) Vulnerability of event dissemination in pub-sub networks to eavesdropping, unauthorized access, spoofing, replay, and denial of service attacks; (2) Challenges of providing secure content-based event dissemination while providing complex publication-subscription matching in the pub-sub networks, and supporting anonymity of publishers and subscribers; and (3) Added security risk of individual nodes being compromised to behave like a malicious node.

This tutorial will discuss some of the latest techniques that have been proposed to address these research challenges. The tutorial is designed to be self-contained, and gives the essential background for anyone interested in learning about the concept, the alternative models and techniques for secure event dissemination, and the general principles and techniques for design and development of a secure and efficient publish-subscribe architecture for scalable and dependable event dissemination. The main objective of this tutorial is to provide an in-depth coverage of the design and implementation issues in building a dependable and secure publish-subscribe systems and applications, the key trade-offs in secure event dissemination, as well as the limitations of current approaches.

About the speaker

Dr. Ling Liu is an Associate Professor in the College of Computing at Georgia Institute of Technology. There she directs the research programs in Distributed Data Intensive Systems Lab (DiSL), examining performance, security, privacy, and data management issues in building large scale distributed computing systems. Dr. Liu and the DiSL research group have been working on various aspects of distributed data intensive systems, ranging from event driven architecture, secure and scalable processing of complex events. Decentralized overlay networks, including publish-subscribe networks, to mobile computing and location based services, sensor network and event stream processing. She has published over 200 international journal and conference articles in the areas of Internet Computing systems, Internet data management, distributed systems, and information security. Dr. Liu is currently on the editorial board of several international journals, including IEEE Transactions on Knowledge and Data Engineering, IEEE Transactions on Service Computing, International Journal of Peer-to-Peer Networking and Applications (Springer), International Journal of Web Services Research, Wireless Network Journal (WINET). Dr. Liu is the recipient of the best paper award of ICDCS 2003, the best paper award of WWW 2004, a recipient of 2005 Pat Goldberg Memorial Best Paper Award. Dr. Liu's research is primarily sponsored by NSF, DARPA, DoE, and IBM. For more information see http://www.cc.gatech.edu/~lingliu.