INTERNATIONAL JOURNAL OF INTELLIGENT CONTROL AND SYSTEMS
VOL. 12, NO. 4, DECEMBER 2007, 282

Editorial of Special Issue on Information Assurance

Wanyu ZANG, and Qijun GU

Information assurance is one of the most pressing challenges to various systems of business today, ranging from traditional distributed systems and networks to newly proliferated applications like P2P systems, sensor networks and ubiquitous computing systems. Attackers can access, tamper and delete valuable information by exploiting vulnerabilities of operating systems, protocols, database systems, or web servers. Research on defensive techniques, which manage to be effective in keeping information safe and preventing or tolerating intrusions, becomes an active area.

To achieve a high quality of information assurance, traditional security aspects such as data confidentiality, integrity, access control, and availability should be fully attained. Techniques in other research areas such as data mining, and high performance computing should also be considered.

The special issue concentrates on the information assurance of the distributed, and the intelligent system. We believe all the papers in this issue could provide the readers with new and broader views of the system security.

The first paper by Li et al. proposes an in-broker access control scheme for geographically distributed database systems. The scheme deploys access control in the information brokerage system, instead of using a traditional approach that access control is deployed in each database system. Hence, the access control can be integrated with query brokerage to provide security and query simultaneously. The paper shows that the scheme can significantly improve the performance of memory consumption, end-to-end query directing time and network occupancy without hurting the system-wide security.

Tang et al. develops a scalable architecture of Wireless Mesh Sensor Network which is a combination of that of sensor network and mesh network. It puts forward two routing protocols to minimize the number of hops and to maximize the lifetime of sensor networks. The paper also takes security into account and designs a secure routing protocol.

The paper by Zang et al. presents a game theoretic analysis on unclear signatures DDoS attacks when signature-based rate limiting defense is deployed. They model the countering DDoS attacks as a Bayesian game. A high volume of simulations for computing Nash equilibrium and the upper bound of the defense system's resilience under DDoS attacks are given in the paper.

Cao and Chen provide a resource oriented security solution (ROSS) to protect the network connectivity of HCSNs and this protocol is embedded into network layer operations. The proposed protocol ROSS is a robust security solution which encompasses prevention, detection, and reaction mechanisms to defense against both external attackers and compromised nodes. They demonstrate the effectiveness of ROSS through both analysis and simulation results.

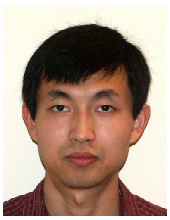
Garrett et al. extends the work of Hernandez, et al, in which genetic algorithms are used to solve the problem of determining whether a given cipher produces random output. They show that carefully tailored genetic algorithms are capable of finding efficient distinguishers for ciphers much faster than has previously been reported.

The paper by Galice et al. proposes a framework to handle trust in ambient networks. The main contribution of the paper is the idea of allowing two stranger devices to establish trust by exchanging histories of their common trusted devices.

Gu and Drissi propose two protocols for localized broadcast authentication in large sensor networks. L-TESLA identifies the subsets according to the deployment of the trusted nodes at the expense of increasing broadcast overhead due to updating localization information. LD-TESLA incorporates the technique of dominating nodes in broadcast authentication. Both protocols significantly reduce the average verification delay.

In the last paper, Han and Ng propose a secure protocol to compute the Pseudo-Scalar Product for multiple parties holding arbitrarily partitions of data. Their paper showed that determining the PSP yields the scalar product of binary vectors. The proposed protocol is as efficient as the best existing protocols for performing the same task, and as secure against colluding parties as the most secured protocols for performing the same task so far.

Wanyu Zang received the M.S. degrees in Computer Science from the Northeastern University, China, in 1998 and Ph.D. degree in Computer Science from Nanjing University, China in 2001. She is currently a visiting assistant professor at Computer Science department of Western Illinois University. Her research interests include computer security and wireless networks.



Qijun Gu is an assistant professor at the Department of Computer Science, Texas State University - San Marcos. He received the Ph.D. degree in Information Sciences and Technology from Pennsylvania State University in 2005, the Master degree and the Bachelor degree from Peking University, China, in 2001 and 1998. His research interests includes vulnerability in sensor applications, authentication in ad hoc and sensor networks, and security in peer to peer systems.

Wanyu Zang is with Western Illinois University, IL 61455, USA. Email: w-zang@wiu.edu

Qijun Gu is with Texas State University, San Marcos, TX 78666, USA. Email:qijun@txstate.edu