Published in IET Information Security
doi: 10.1049/iet-ifs.2010.9128

Special Issue on Multi-Agent & Distributed Information Security

ISSN 1751-8709

Editorial
Multi-Agent & Distributed Information Security

Information Security (IFS) addresses a sensitive part of information technology where the success of virtually all new technological developments depends on efficient use of automation for human resource management, computer technologies for trustworthy internet, many new communication services and distributed sensor systems for human quality of life and global stability which all heavily depend on our systems and devices working securely and reliably. The level of research activities and rate of publications in this field, however, has been too slow for many decades and never shown any significant development to measure up its importance.

Many experts have realised this need but due to restricted issues and controlled activities, very little funding at national and international levels has been allocated to promote any meaningful research activities in this area.

Due to a limited level of submissions, the IFS papers were published as a small part of the Communications Journal (IEE/IET-COM). Some years into the new millennium we at the IEE recognised the need for promoting IFS papers, as the number of submissions from various parts of the world started to grow, particularly in the far-east countries.

We then realised that a further surge of Communications papers would suppress Information Security even further. Thus, in 2005, we at the IET Journals Office decided to promote Information Security into a new Journal IET-IFS to serve both global academic and industrial communities with a wider scope, more effectively. Progress has been considerable since its divergence from IET-COM but still far from the amount needed to help the IFS technologies to grow sufficiently to support rapidly growing competitive fields such as wireless communications, computer systems, sensors and internet technologies.

To this effect we, therefore, initiated this Special Issue with the following goals in mind:

1 – Expanding/widening the scope of IFS (too narrow to attract required research papers). Selection of MADS injects some significant dynamics into the process:

A. Agent approach to the distributed intelligence,

B. Multi-Agent problem solving as new approach to distributed systems,

C. Introduction of security layer as part of traditional network management

D. Introduction/reassurance of new/enhanced measures for the new systems and services such as trust, reliability and dependability

2 – Revitalising the problem solving approaches in information security from direct application of traditional cryptography into more effective distributed security.

3 – Injection of new dynamics into solving the ever growing information security issues causing severe performance degradation in services and declining trust of the internet as a reliable/dependable infrastructure for building a better global life for everyone.

4 – Stimulating/triggering new market and new interests in the most wanted areas of info tech research activities by motivating new researchers.

The process has been rather lengthy but very fruitful, with a compilation/amalgamation of 18 interesting research papers addressing various parts of the expected scope for this Special Issue and to make it both unique and special.

The first paper from Rashvand *et al.* is a review paper exploring various dimensions of MADS. This review paper should be interesting for researchers who are new to 'agent and distributed security'. The remaining 17 papers can be classified into three categories.

The first 6 papers explore various critical aspects of 'cooperative and multi-agent security' where content and trust play significant roles. Nojoumian *et al.* under 'Unconditionally Secure Social Secret Sharing Scheme' introduce the notion of a Social Secret Sharing Scheme, where the shares are allocated based on players' reputation and the way they interact with other participants. During the social tuning phase, weights of players are adjusted such that more cooperative participants end up with more shares. Then, 'Trust-based On-demand Multipath Routing in Mobile Ad Hoc Networks' from Li *et al.* introduces an Ad hoc On-demand Trusted-path Distance Vector which is a reactive multi-path secure routing protocol for mobile ad hoc networking. This protocol uses some multiple trust path route discovery candidates to meet the required dependability. As an intelligent agent, a source node evaluates these paths from two aspects: hop counts and trust values, it selects the shortest trusted path to forward the packets to reduce any hazardous actions from malicious nodes. The third paper entitled 'Covert-Channel Resistant Information Leakage Protection using a Multi-Agent Architecture' is from Bishop *et al.* which uses a special multi-agent system for processing data watermarking and subsequently analyses to prevent possibility of information leakage caused by covert-channel attacks. Here, applying context-based watermarks to a set of files, laundering of such files between security domains detected disabling attackers to remove a file's watermark without destroying the file's contents. The paper 'Digital Publication Transaction Mechanism for Electronic Auction Environment' of Yen *et al.* proposes a digital product transaction mechanism for electronic auction in the multi-agents system environment. It introduces a convenient platform to protect the privacy of both buyers and sellers, and track digital product further in an electronic auction environment using a simple cryptography technique, ensuring the security of transactions as well as providing a safe and fair mechanism for electronic auction. Then Sakarindr and Ansari in their paper 'Security Services on Group Communications' warn that in spite of rapid growth and maturity in group communications facilitating emerging group-oriented applications there are several security concerns and requirements that have still not been fully addressed. Following provision of some properties for evaluating group communications security services, they present a survey on recent advances of secure group communications systems to layout for remaining issues and design challenges including a better understanding of possible attacks in group communications, security requirements and existing security services. The last paper of this category is from Jensen who under 'Supporting Multi-Agent Reputation Calculation in the Wikipedia Recommender System' addresses the quality issues of massive contributions in information systems where multiple autonomous agents contribute to the same resource (e.g., crowd sourcing). To this effect the author describes the design and implementation of the Wikipedia Recommender System providing an assessment method for measuring the quality of Wikipedia articles based on collaborative filtering techniques, underlying structure and the general problem of establishing trust in a collaboratively generated resource in a distributed multi-agent system.

The 5 follow-up papers can be categorised as 'Architectural Frameworks for Distributed Security'. 'Integrated Security Analysis Framework for an Enterprise Network – A Formal Approach' by Bera *et al.* proposes an integrated framework for analysing distributed security implementations of enterprise networks. Having their framework formally verified with distributed security deployment of the organisational security policy, the authors claim this framework should help extracting correct distributed security implementation procedures for enterprise networking. The next paper from Amini *et al.* titled 'Multi-Level Authorisation Model and Framework for Distributed Semantic-Aware Environments' uses semantic technology for distributed computational environment to increase interoperability and machine readability of information through passing the semantics to underlying information resources. This new authorisation system for semantic-aware environment satisfies the requirements of an authorisation framework model controlling all aspects of security including inference channels in the abstract semantic layer. The authors' proposed authorisation model uses a formulated logic to enable policy specification and inference for both conceptual and ground levels. The third paper from Chandrasekhar *et al.*, 'Efficient Proxy Signatures Based on Trapdoor Hash Functions', discusses use of proxy signature for authenticating agents in various new distributed systems. They present a technique to construct provable secure and efficient proxy signature schemes using trapdoor hash functions that can be used to authenticate and authorise agents acting on behalf of users in agent-based computing systems. Baig and Salah under 'Multi-Agent Pattern Recognition Mechanism for Detecting DDoS Attacks', propose a new distributed solution for detecting the Distributed Denial of Service attacks in typical production networks. Using a multi-agent pattern recognition mechanism, the solution deploys detection agents in a distributed fashion. The authors show that their solution is optimised for its effectiveness so that it can achieve high accuracy detecting such attacks with low false alarms. The last paper in this category is 'Recovery of Data Integrity under Multi-Tier Architectures' from Yu and Zang who elaborate on how software components of a distributed system at different layers collaborate to restore data integrity after some information security attacks. After a brief discussion on context issues of multi-layer service architecture they use a Multi-layer dependency graph to

IET Inf. Secur., 2010, Vol. 4, Iss. 4, pp. 185–187

doi: 10.1049/iet-ifs.2010.9128

track down the damage, analyse and device a recovery plan. They also discuss conditions that a compromised system can be recovered.

The remaining 6 papers are categorised under 'secure network applications and mobility'. 'Cluster-based Secure Communication Mechanism in Wireless Ad Hoc Networks' from Guo *et al.*, proposes a secure communication mechanism for MAS environment which uses Diffie-Hellman key exchange protocol to generate the session key. The proposed method reduces the communication overload in the cluster and avoids the time synchronisation problems in node authentication whilst preserving required total secrecy. Then, under 'Outlier Detection and Countermeasure for Hierarchical Wireless Sensor Networks', Zhang *et al.* look into security aspects of the most promising technology, the distributed sensors where outliers in wireless sensor networks are sensor nodes that issue attacks due to abnormal behaviour or fake message dissemination. The authors argue that existing security techniques are both too complex and mainly practically unable to detect such inside attacks causing outlying recognition to be both critical and challenging for secure dissemination of data. Authors present a novel Outlier Detection and Countermeasure Scheme that can be deployed under various mechanisms suitable for detecting the outliers. The proposed interoperable mechanisms provide required countermeasures to defend various outliers including illegal messages rejection and re-key approach. The third paper in this category is from Misra *et al.* Under the title of 'Adaptive Link-State Routing and Intrusion Detection in Wireless Mesh Networks' this paper opens up security issues of potential but vulnerable wireless networks where intrusion is an immense source of problems. One of the common bottlenecks in such a network is the use of insecure classic routing mechanisms. This paper presents an enhanced routing protocol capable of detecting intrusions whilst implementing the network-based classic routing tasks. Further discussion on performance evaluation and effectiveness of the detection provides new insights. Then, in order to achieve better scalability and less communication overhead 'Physical Layer Assisted Authentication for Distributed Ad-Hoc Wireless Sensor Networks' by Wen *et al.*, explores the possibility of integrating the conventional message authentication schemes and the physical layer authentication mechanisms. Further discussions on this title are on the usefulness of such secure mechanisms for ad hoc and wireless sensor networks under the resource limitation constraints. The fourth paper of this category is 'Anonymity and Security for Autonomous Mobile Agents' from Raji and Ladani who propose a new secure protocol which provides anonymity to the agent owners as well as the agent itinerary. This protocol claimed that none of the hosts in the network can learn the true identity of the agent owner and also the path in which it has traversed through so far can be kept covert enabling anonymous agents to roam autonomously from one platform to another. The last paper, 'Towards an Authorisation Model for Distributed Systems based on the Semantic Web', from Calero *et al.*, provides a formal access control model, addressing security aspects of semantic web technologies which can enable the description of the semantics of protected objects whilst avoiding any mismatch problems between semantics of the authorisation model and semantic of protected objects. Further discussions on advanced authorisation features such as hierarchical role-based access control, an authorisation system suitable for distributed systems, object hierarchies and information privacy and trust management provide new insights into secure web applications.

Special Issue Editors of 'Multi-Agent & Distributed Information Security':

Professor HABIB F. RASHVAND
Professor LEIN HARN
Dr JONG H. PARK
Dr KHADED SALAH