Editorial

Fredrick Japhet Mtenzi*

School of Computing,
Dublin Institute of Technology,
Kevin Street, Dublin 8, Ireland
E-mail: Fredrick.Mtenzi@dit.ie
*Corresponding author

Al-Dahoud Ali

Computer Science Department,
Faculty of Science and Information Technology,
Al-Zaytoonah University,
Airport Street, Amman, Jordan
E-mail: aldahoud@alzaytoonah.edu.jo

Galyna Akmayeva

University of Wales,
King Edward VII Ave.,
Cardiff CF10 3NS, UK
E-mail: g.akmayeva@infonomics-society.org

Biographical notes: Fredrick Japhet Mtenzi is a Lecturer at the School of Computing, Dublin Institute of Technology (DIT), Ireland. Prior to joining DIT, he worked as a Lecturer at the University of Dar es salaam in Tanzania. His research interest includes design of algorithms for solving combinatorial optimisation problems, energy aware routing in mobile ad hoc networks and its related security issues, cybercrime, ubiquitous computing and e-healthcare information systems security. He has organised and chaired number of international conferences. He has been a Guest Editor in a number of journal special issues. He is a member of the IEEE, ACM, and ISSA.

Al-Dahoud is an Associated Professor at Al-Zaytoonah University, Jordan. He is working at Al-Zaytoonah University since 1996, and established the ICIT as a Program Chair since 2003. He has directed and led many projects sponsored by NUFFIC/Netherlands. He participates in the following conferences as general chair, program chair, and session's organiser or in the publicity committee of: ICITs, ICITST, ICITNS, DepCos, ICTA, ACITs, IMCL, WSEAS, and AICCSA. He worked as an Editor in Chief or Guest Editor or in the editorial board of the following journals: *JDIM*, *IAJIT*, *JCS*, *IJITST*, and *UBICC*. He published many books and journal papers.

Galyna Akmayeva is a Consultant in E-Learning Security Enhancement. Her research interests are in the fields of e-learning security. She has authored and co-authored many papers in e-learning security and trust related field. She has organised and chaired a number of international conferences and workshops and a Guest Editor to *IJITST*.

Summary of all the paper in the special issue

This special issue 'Security enhancement' of *IJITST* includes nine research papers that present the best selected papers of ICITST 2008 which was held at the Dublin Institute of Technology – Ireland in 2008. The papers have been extended and updated to fulfil *IJITST* standards. The summary of the papers in this special issue are as follows:

The 'LH*$_{RS}^{P2P}$: a fast and high churn resistant scalable distributed data structure for P2P systems' by Hanafi Yakouben and Sahri Soror proposes a new scalable distributed data structure (SDDS) for P2P applications called LH*$_{RS}^{P2P}$. This new data structure deals with two major issues in P2P systems. One is efficient location of the peers with searched data records. The other is the protection against data unavailability due to churn of peers. LH*$_{RS}^{P2P}$ applies the LH*$_{RS}$ SDDS principles to peer nodes. Unlike the LH*$_{RS}$, LH*$_{RS}^{P2P}$ node acts as a client and at least potentially, as a server. In the latter role, it stores LH*$_{RS}^{P2P}$ application data or parity data for high-availability protecting against churn. This dual role reduces key search messaging to at most one forwarding message (hop). This is an improvement over two messages at most per search of LH*$_{RS}$. It is also the least number of worst case hops for any SDDS known at present and likely the least possible. The scheme provides the fastest key search for any known SDDS or, more generally, any P2P addressing scheme, with unicast messaging. In addition, using this structure, a scan of the file requires at most two rounds. This is also the fastest known result. For example, in order to deal efficiently with churn, LH*$_{RS}^{P2P}$ expands LH*$_{RS}$ parity management principles. As the result, the file transparently supports unavailability or withdrawal of up to any $k \geq 1$ peers, where k is a parameter that may scale dynamically with the file.

Yi-Tung Chan, Galyna Akmayeva and Charles Shoniregun's paper titled 'A novel approach against the system buffer overflow' presents the system buffer overflow (SBO) universal problem in information security. The SBO attack utilises the system programme which writes data into the buffer zone without doing the bound checking. In this loophole, attackers can modify the data structure of the control programme procedure such as the return address or the function pointer and then the system programme procedure will be turned to the code-injection attacks (CIA) or the return-into-libc attacks. In the traditional defence mechanisms, the SBO prevents shell code execution and neglect unsuccessful attack that makes system procedures terminated abnormally. When the SBO attack is launched by attackers, unsuccessful attack may destroy the attacked process of the memory content and then the attacked procedure will be terminated abnormally.

In 'Forty years of movie hacking: considering the potential implications of the popular media representation of computer hackers from 1968 to 2008' by Damian Gordon examines the movies that feature hackers (and hacking) to identify common themes that emerge from these movies. Increasingly movies are being produced which feature plots that incorporate elements of computer security and hacking, and cumulatively these movies are creating a public perception as to the nature of computer security. To achieve this, first he created a corpus of hacking movies, and then using a qualitative data analysis technique, he developed guidelines which distinguish those movies that actually have the potential to create a perception with the general public. The resultant dataset is analysed and the salient details are compared to the reality of hacking. His research has implications in a range of fields, including: the education of computer

students, organisation computer security, and in the behaviour of the general public when using computers.

One of the most challenging issues facing sensor networks is how to detect node capture attacks, compromised or malicious nodes. The paper by Maryam Fanaeepour and Mohammad Reza Kangavari titled 'Malicious node detection system in wireless sensor networks: a decentralised approach' reviews different techniques for detecting malicious nodes in wireless sensor networks and they introduce a new system called HyPIDS. The main idea of their system is in using additional sensor nodes, called 'monitor nodes', inserted and distributed into the network in order to detect malicious nodes so that they can monitor the propagated messages of common sensors through the network. Their solution exploits a distributed detection method to identify intrusions into the network aiming to minimise the workload of common nodes. They further propose a distributed scheme using aggregator nodes to monitor nodes in a decentralised approach. They model the distributed and decentralised solution using Petri nets and their evaluation results show that the utilisation of common nodes increased. The decentralised approach of the proposed scheme and detection of malicious nodes are simulated using a new Java-based tool called SIDnet which supports heterogeneous sensor networks and has a suitable layering of these networks.

Ion Tutănescu, Emil Sofron and Maaruf Ali's paper titled the 'Security of internet-connected computer networks' presents some of the passive and active attacks against the computer networks. The security of computer networks connected to the internet is an important, vital and hotly contested real-world issue. Once the computer networks get connected to the internet, the number of attacks, their strength and intensity grow exponentially. All the attacks then exploit breaches in the network security. The anatomy of the attack is presented showing the phases and the techniques for penetrating into the computer networks – with the purpose to stress and highlight the several dangers faced by the network manager and the utmost necessity of setting a proper corporate network security policy in place. They demonstrate that detection of an attack is a difficult task because the detection technology is still in its infancy and has yet to mature; also, once the attack is detected, the attacker in most cases still remains unknown.

In 'A lightweight secure architecture for wireless sensor networks' paper by Michael Collins, Simon Dobson and Paddy Nixon, a secure lightweight architecture that takes account of the constraints of sensor networks was proposed. The adoption and widespread deployment of wireless sensor networks means that security issues are of critical concern. To date, much research has focused on the usability of these networks in a variety of environments where conventional wired networks may not be feasible. However, less emphasis was placed on the security issues of employing a sensor network and its exposure to potential threats. Due to the severe physical constraints in sensor nodes, traditional cryptographic mechanisms are not suitable to deal with such potential security threats. They use a base station to form a hierarchical network topology that enables end-to-end communication between sensor nodes with the aid of intermediary nodes where necessary. The architecture also supports the detection and isolation of aberrant nodes.

The 'Improving TCP performance over mobile ad hoc networks' by Ahmad Dalal'ah, Samir Bataineh and Awos O. Kan'an discusses the challenges of deploying standard TCP in wireless mobile ad hoc networks (MANETs) that can lead to poor performance of TCP. They argue that the main problem that faces TCP in ad hoc networks is its inability

to distinguish between packet losses due to congestion and those due to route failures. In order to adapt TCP to MANET environment, they propose several TCP improvements that differentiate between different types of packet losses using explicit notification messages from lower layers. Specifically, they propose a new end-to-end technique that does not require any participation from intermediate nodes within the network. Their proposed scheme relies on expanding the retransmission timeout (RTO) interval in order to reduce the number of timeouts that do not result from congestion. Simulation results show that their scheme can improve TCP throughput, delay and outperforms the standard TCP in simulation experiments.

In 'Providing location privacy in pervasive computing through a hybrid mechanism' by Mohsen Sharifi and Leila Naghavian, the hybrid mechanism for location privacy in pervasive computing was proposed. Advances in pervasive computing technology on the one hand, and the widespread use of mobile computing devices combined with improvements in embedded positioning capabilities on the other hand, testify the need for new mechanisms and applications to realise these innovative technologies with particular concern for users' privacy and consent. Although several researches on these new technologies and their privacy are undergoing, there is still a long way to realise all their benefits.

The 'Trust algorithms in p2p file sharing networks' paper by Sem Daskapan is based on a taxonomy of 17 trust algorithms as found in literature. The evaluation is done by means of both a literature study and a series of simulation tests. To be able to choose the right peers, a trust valuation algorithm is needed. Such an algorithm calculates the trust that the trustee puts in the peer who possesses the file in demand, on the basis of certain characteristics. The outcome of the computation process is often expressed as a number and labelled as a trust value describing the peer's trustworthiness. Several trust algorithms have been proposed already. However, given the fact that the current peer to peer (p2p) networks do not use any of the current trust algorithms, we throw doubt on their reliability. From this observation we derived the objective of this paper, namely, to single out the advantageous parts of the existing trust algorithms, so that future researchers can compose a new and better trust algorithm for file sharing in p2p networks.

Acknowledgements

The guest editors of the special issue on 'Security enhancement' of the Volume 1, Number 4, of the *International Journal of Internet Technology and Secured Transactions* (*IJITST*), would like to thank the Editor-in-Chief of *IJITST*, Prof. Charles A. Shoniregun, reviewers and all authors that submitted to this special issue. However, we would like to show appreciation to all the authors of the selected papers published in this issue, for their enthusiasm and commitment.