Journal of Network and Computer Applications ∎ (∎∎∎∎) ∎∎∎–∎∎∎

Contents lists available at ScienceDirect

Journal of Network and Computer Applications

journal homepage: www.elsevier.com/locate/jnca

Editorial

Advanced technologies for homeland defense and security

In recent years significant work has been undertaken by both national and local government agencies to protect critical data and infrastructures from cyber attacks. As a result, many Homeland Security solutions have been newly developed and deployed, requiring the design of new computer systems technologies, as well as techniques allowing security procedures to be executed on many different areas, from system, communication and organization security to the security of the state to ensure its defense capabilities. Advanced security technologies based on the intelligent algorithms can analyze group behavior and interpret complex patterns or situations, and they are increasingly becoming the building blocks of the aforementioned Homeland Security solutions. In this context, we believe that it is worth noting research that combines security and defense aspects with achievements in designing advanced systems for the acquisition and sophisticated semantic analysis of complex image patterns and group behaviors. Such systems use modern cognitive models of semantic interpretation, and can be applied to develop algorithms and protocols used for the security of computer systems themselves, but also to ensure the confidentiality and security of communication networks. They can also be employed to develop globally understood safe solutions connected with activities to strengthen national defense capability.

Threats to critical infrastructures, e.g. from organized crime and terrorism, endanger human life directly and indirectly. Resilience of critical infrastructures has gained importance as a core concept to cope with such threats. In general, this means strengthening those infrastructures to prevent or mitigate such threats and to consistently deliver the intended services in a trustworthy way even in changing and challenging situations. The information and communication infrastructure is the one of the primary critical infrastructures. Hence, it has been the central target from cyber attacks. As a consequence, effective response capabilities must be properly organized and closely coordinated to protect the infrastructure because, at the time of a cyber-attack, it is not possible to immediately determine whether the attacker is a script kiddie, an insider, a rogue actor (organized crime, terrorist organization, or radical), or a nation state.

Considering the broad yet interesting problems from the homeland defense and security areas, we have decided to publish a Special Issue on "*Advanced Technologies for Homeland Defense and Security*", which presents selected subjects concerning practical and methodological solutions from such fields as: homeland security and information processing, personal security and biometric, target recognition, sensor and data analysis in secure environment, embedded systems in internal or external security, knowledge-based Internet security, privacy and trust for Internet services, and biologically inspired security systems.

This SI is a collection of 10 papers carefully selected as the best from total 35 publications submitted on these subjects. Each accepted article has been subject to a rigorous peer review procedure and has been assessed by several independent reviewers.

In the paper entitled "*A Simulation Study of* Ad Hoc *Networking of UAVs with Opportunistic Resource Utilization Networks*" (Lilien et al., 2014) a specialized ad hoc network for unmanned aerial vehicles (UAVs) has been proposed. Particularly the application of Opportunistic Resource Utilization Networks (Oppnets), a novel type of MANETs, for UAV ad hoc networking was discussed. The Oppnets provide middleware to facilitate building flexible and adaptive distributed systems that provide all kinds of resources or services to the requesting application via a helper mechanism. The authors performed simulation of a homeland defense using case for Oppnets that involves detecting a suspicious watercraft. The simulation results show that Oppnets are a promising framework for high-performance ad hoc UAV networking, and provide excellent performance even under imperfect conditions.

In the paper "*Text Analysis for Detecting Terrorism-Related Articles on the Web*" (Choi et al., 2014) the classification procedures for text messages were presented to reveal the terrorism-related web documents. The proposed method uses the word similarity, and is based on WordNet hierarchy with N-gram data frequency. Their experimental results show this technique is effective for extracting context words from the text and identifying terrorism-related documents.

The paper entitled "*A Botnet-based Command and Control Approach Relying on Swarm Intelligence*" (Castiglione et al., 2014) was focused on a new more robust and scalable botnet-based command and control architecture, aiming at wiping off any rigid master–slave relationship and autonomizing the bot operating roles, with significant agility gains in the communication infrastructure. It relies on swarm intelligence and in particular on stigmergic communication, ensuring spontaneous, implicit coordination and collaboration among the independent bot agents. Described techniques may constitute the basis for an evolutionary malware-based control and management scheme, which can be used in several homeland security scenarios in strategic military or intelligence operations.

In the paper "*Cognitive Systems and Bio-inspired Computing in Homeland Security*" (Ogiela and Ogiela 2014) some biological models for data protection and securing confidential information were presented. Very unique personal information and individual biometrics lead to extracting information classes necessary for personal data protection processes. Such processes can be used to secure various types of data. Adding semantic data analysis processes to computer systems, which are used to conceal processes of personal data management offers opportunities for semantically analyzing and interpreting strategic data while it is being decrypted.

The paper entitled "*Detecting Mobile Malware Threats to Homeland Security Through Static Analysis*" (Seo et al., 2014) discussed

1084-8045/$ - see front matter © 2013 Published by Elsevier Ltd.
http://dx.doi.org/10.1016/j.jnca.2013.12.001

UNCORRECTED PROOF

ARTICLE IN PRESS

the characteristics inherent in mobile malware and show mobile attack scenarios which are feasible against Homeland Security. The authors proposed the static analysis tool, called DroidAnalyzer, which identifies potential vulnerabilities of Android apps and the presence of root exploits. There are some examples of analysis for various mobile malware samples, and targeting apps such as banking, flight tracking and booking, and home and office monitoring applications.

The paper "*Low-Cost Prioritization of Image Blocks in Wireless Sensor Networks for Border Surveillance*" (Irgan et al., 2014) described a cost-effective method for dynamic prioritization of image macro-blocks in border monitoring and surveillance applications using Wireless Sensor Networks. Authors employed a simple encoding scheme at the source node by labeling data blocks based on the information they contain. The network allows to transmit only important data blocks over reliable paths. The obtained results indicated the usefulness of the proposed prioritization scheme in terms of transferred image quality, delay and energy.

The paper "*A Trusted Versioning File System for Passive Mobile Storage Devices*" (Catuogno et al., 2014) presented a new Trusted Versioning File System (TVFS) which stores data in secure manner on untrusted storage devices. The new file system TVFS ensures the integrity and confidentiality of stored data, as well as allow for trustworthy data retention and retrievability. It also allows access to verifiable history of changes, and corruption detection. The authors highlighted that TVFS could fit some scenarios where different stakeholders concurrently access and update shared data, such as financial and e-health multiparty services, as well as civil protection application systems such as hazardous waste tracement systems, where the ability to reliably keep track of documents history is a legally enforced requirement.

In the paper "*A Semantic Authorization Model for Pervasive Healthcare*" (Li et al., 2014) the authors investigated how to secure sharing of complex data objects among pervasive information systems. They proposed an advanced authorization model that supports specifying and enforcing authorizations in flexible and efficient ways. The model employs ontology and semantic web technologies to conceptualize data and explicitly express the relationships among concepts and instances involved in information sharing. Additionally a novel decision propagation model is proposed to enable fast evaluation and updating of concept-level access decisions.

The paper "*A Multi-Issued Tag Key Agreement with Time Constraint for Homeland Defense Sub-department in NFC Environment*" (Chen 2014) presented a multi-issued tag key agreement procedure with time constraint, accompanying a new type of secure tag, called as a secure multi-issued tag. This solution facilitates the management of multiple secure accesses to large duplicated storage space. To achieve the requirement of near field spatial communications (NFC) in mobile devices, each secure multi-issued tag can be authorized by distinct missions belonging to group served among homeland defense sub-departments.

In the paper "*An Improved Side Channel Attack Using Event Information of Subtraction*" (Park et al., 2014) was proposed the new cryptanalysis subtraction algorithm analysis on equidistant data (SAED), which extracts sensitive information using the event information of the subtraction operation in a reduction algorithm. SAED is an attack approach which uses algorithm-dependent power signal changes. An adversary can extract a key using differential power analysis (DPA) of the subtraction operation.

We strongly believe that the presented papers in this SI make a significant contribution to the field of Homeland Security and critical infrastructure protection, and will interest academic researchers and industry professionals who want to extend their knowledge from the areas of modern and advanced technologies for homeland defense, security systems, cryptography, advanced and secure cognitive information processing, as well as secure distributed computing and communication.

We would like to express our sincere appreciation to all of the authors for their valuable contributions. Our special thanks go to the editorial board for this SI and Prof. Mohammed Atiquzzaman, Editor in Chief of Journal of Network and Computer Applications, for his invitation to organize this SI and his great support throughout the entire publication process.

References

Castiglione Aniello, De Prisco Roberto, De Santis Alfredo, Fiore Ugo, Palmieri Francesco. A Botnet-based command and control approach relying on Swarm Intelligence. J Network Comput Appl 2014;37:600–15.

Catuogno Luigi, Lohr Hans, Winandy Marcel, Sadeghi Ahmad-Reza. A trusted versioning file system for passive mobile storage devicesm. J Network Comput Appl 2014;37:600–15.

Chen Hsing-Chung. A multi-issued tag key agreement with time constraint for homeland defense sub-department in NFC environment. J Network Comput Appl 2014;37:600–15.

Choi Dongjin, Ko Byeongkyu, Kim Pankoo. Text analysis for detecting terrorism-related articles on the web. J Network Comput Appl 2014;37:600–15.

Irgan Kerem, Unsalan Cem, Baydere Sebnem. Low-cost prioritization of image blocks in wireless sensor networks for border surveillance. J Network Comput Appl 2014;37:600–15.

Li Zang, Chu Chao-Hsien, Yao Wen. A semantic authorization model for pervasive healthcare. J Network Comput Appl 2014;37:600–15.

Lilien Leszek T, Ben Othmane Lotfi, Angin Pelin, DeCarlo Andrew, Salih Raed M, Bhargava Bharat. A Simulation Study of Ad Hoc Networking of UAVs with Opportunistic Resource Utilization Networks. J Network Comput Appl 2014;37:600–15.

Ogiela Lidia, Ogiela Marek R. Cognitive systems and bio-inspired computing in Homeland Security. J Network Comput Appl 2014;37:600–15.

Park Jong-Yeon, Han Dong-Guk, Yi Okyeon, Kim JeongNyeo. An improved side channel attack using event information of subtraction. J Network Comput Appl 2014;37:600–15.

Seo Seung-Hyun, Gupta Aditi, Mohamed Sallam Asmaa, Bertino Elisa, Yim Kangbin. Detecting mobile malware threats to Homeland Security through static analysis. Journal of Network and Computer Applications 2014;37:600–15.

Ilsun You
Korean Bible University, South Korea
E-mail address: ilsunu@gmail.com

Marek R. Ogiela
AGH University of Science and Technology, Poland
E-mail address: mogiela@agh.edu.pl

A. Min Tjoa
Vienna University of Technology, Austria
E-mail address: amin@ifs.tuwien.ac.at

Dongwan Shin Q1
New Mexico Tech, USA
E-mail address: doshin@nmt.edu

UNCORRECTED PROOF