J Ambient Intell Human Comput (2014) 5:169–171
DOI 10.1007/s12652-013-0208-5

EDITORIAL

Prosperity of IT security technologies in homeland defense

Kangbin Yim · Aniello Castiglione · Ilsun You

Published online: 5 October 2013

Homeland is defined as the physical region that includes the nations possessions, territories, and surrounding territorial waters and airspace (Moseley 2006). Homeland Security is defined as a concerted national effort to prevent terrorist attacks within a nation, reduce its vulnerability to terrorism and minimize the damage and recover in case an attack occurred. Homeland Defense represents the protection of territory, sovereignty, domestic population, and critical infrastructure of a nation against external threats and aggression, or other threats such as the environmental pollution or natural disasters (Sharp 2007). Meanwhile, the Information and Communication Technologies (ICT) is one of the most considerable points in the Homeland Security and Defense because it requires the secure ICT integration into various traditional industries, whose foundations are all components of the homeland and those components have been computerized into the ICT infrastructure.

Although the fundamentals of the ICT were originated for military purposes and they were confidentially developed to be used in militaristic field, no more than 20 years ago, the situation was changed in many ways by penetration of these technologies into public domain in the form of wired or radio signals and protocols for the PSTN, cellular networks and the wireless Internet. As a result, ICT became more prevail in general industries and societies than that in military.

Currently, the ICT is becoming hugely focused again in Homeland Security and Defense in light of development and deployment of successful and perspective security solutions in general industries. Now, such solutions additionally require specific design considerations and techniques for new security architectures and reasonable security procedures or algorithms that will be implemented on many different security planes spanning from advanced platform systems to new communication protocols to work along with heterogeneous organizations and strategies required to protect Homeland facilities.

In regards to protecting the homeland infrastructures, several essential keywords are also required to be thoroughly considered, which include environmental surveillance, location assurance, disaster management, risk analysis and reasoning, and so forth. A large scaled intelligent video surveillance network has substituted the CCTV system, and the intelligent secure wall has been fielded with sensors on the border fence between countries. The power plants are now also controlled by a remote interface over a public network. Many projects are still involved with deploying unmanned surveillance and defensive systems for military, public, and private infrastructures nation-wide. Along with this ICT convergence into significant infrastructures, related security problems and consequent defense strategies against homeland threats are becoming a big topic of discussion.

The main objective of this special issue is to invite researchers and practitioners from academia and industry

K. Yim
Department of Information Security Engineering, Soonchunhyang University, 646 Eupnae, Shinchang, Asan 336-745, South Korea
e-mail: yim@sch.ac.kr

A. Castiglione (✉)
Department of Computer Science, University of Salerno, Via Giovanni Paolo II, 132, 84084 Fisciano, SA, Italy
e-mail: castiglione@ieee.org; castiglione@acm.org

I. You
School of Information Science, Korean Bible University, 16 Danghyun 2-gil, Nowon-gu, Seoul 139-791, South Korea
e-mail: isyou@bible.ac.kr

to share problems and solutions regarding the various aspects of Homeland Security and Defense technologies, particularly aiming to promote more state-of-the-art research activities in this field. To meet the goal, we deeply reviewed the papers presented in the 2nd IFIP International Workshop on Security and Cognitive Informatics for Homeland Defense (SeCIHD'12) held at University of Economics in Prague, Czech Republic on August 20–24, 2012 in conjunction with the ARES 2012 International Conference. Though we found many high quality research results with outstanding practical contributions to the technological advancements on the Homeland Security and Defense in aspects to the topics listed above, only five papers were distilled from them.

Disaster management is one of the most critical missions of the responsible authorities for Homeland Security. In the paper "Security Issues on IT Systems During Disasters", Kiyomoto et al. (2013) provide a survey on current research trends and security or privacy issues on IT systems that may be used during disasters. The survey outlines security and privacy risks in three main fields: system continuity management, network access and information gathering. It presents an interesting and quite complete perspective of the involved security scenario and proposes the possible solutions for these security issues. The work can be helpful to people outside the field as well as to researchers who are going to address some of these issues.

Precise risk management for homeland infrastructures is another important issue, which includes proper understanding the security needs and maintaining appropriate incident preparedness. Usually this task is challenging because the overall risk figure may be strongly affected by changes in a few of the systems in the infrastructure. In order to continuously manage risks for an adequate level of protection, there is a need to continuously maintain the validity of risk models while systems change and evolve. The paper "Model-Driven Risk Analysis of Evolving Critical Infrastructures" by Solhaug and Seehusen (2013) describes a model-driven approach for adapting the existing risk models to the evolving systems in order to maintain the continued adequacy of risk-management models. Its objective is to support the update of risk models as changes occur in new systems without the need of re-analyzing the entire system from scratch.

Intelligent video surveillance is one of the most popular services for Homeland Security and Defense. Understanding and verifying the context and the location of the monitored videos is an essential requirement for the intelligent video surveillance. In the paper "Secure and Distributed Video Surveillance via Portable Devices" Albano et al. (2013) present a framework for distributed video surveillance system providing reliable, high speed, secure and real-time communication. Since mobile devices usually exist as connected devices, supporting portable devices as a client in the Server/Client model of the framework is considered necessary and useful for many real-world scenarios that need to receive real-time data from selected cameras at a moving position. The security of the transactions among the participating components is guaranteed by using the SSL/TLS protocol. An invisible digital watermarking algorithm is also applied on each image for integrity. After being watermarked, an image is sent from the server to a portable device where it extracts the watermark from the image in order to verify the identity of the node.

Performing a risk assessment is an essential step to be undertaken in order to evaluate the effectiveness of the security measures especially to protect privacy of information in a networked system, for example. In the paper "Tableau Systems for Reasoning about Risk" Cristani et al. (2013) introduce a logical framework that allows to reason about risks by means of operators that formalize causes, effects, preconditions, prevention and mitigation of events that may occur in a system. In this process, authors give tableau rules and discuss a number of interesting variants that could be considered. They also prove soundness and completeness of the resulting tableau systems and give an algorithm for satisfiability.

In case of a disaster, managing the response operations is a crucial responsibility of the concerned authorities. Assuring the accurate locations of the first responders is a critical problem to solve for effective management of emergency situations. As a common approach, the radio-based positioning solutions are used to search responders' locations, which require a heavy process of site survey. In the survey, radio signatures have to be collected and stored in a radio map for further comparison and matching, which involves intensive manual effort and time. In the paper "Calibration-less indoor location systems based on wireless sensors" Ficco (2013) proposes a solution for rapid site survey. The author also developed a specific tool to draw the site topography and to define the radio map generated by the wireless sensors located in the considered area, by using an accurate signal attenuation model.

We would like to thank the authors for the above papers published in this special issue, and regret that more papers could not be included. We appreciate all reviewers for their time and effort in reviewing the assigned papers on time and providing invaluable comments and suggestions to authors for improving their papers. We also want to thank Professor Vincenzo Loia, Editor-in-Chief of the Journal of Ambient Intelligence and Humanized Computing. His warm-hearted help and support have made this special issue a reality. Hopefully, this special issue will bring forth advancements in science and technology and improve practices and applications as well, in the field of Homeland Security and Defense.

References

Albano P, Bruno A, Carpentieri B, Castiglione A, Castiglione A, Palmieri F, Pizzolante R, Yim K, You I (2013) Secure and distributed video surveillance via portable devices. J Amb Intell Human Comp, pp 1–9. http://dx.doi.org/10.1007/s12652-013-0181-z

Cristani M, Karafili E, Vigano L (2013) Tableau systems for reasoning about risk. J Amb Intell Human Comp, pp 1–33. http://dx.doi.org/10.1007/s12652-013-0186-7

Ficco M (2013) Calibration-less indoor location systems based on wireless sensors. J Amb Intell Human Comp, pp 1–13. http://dx.doi.org/10.1007/s12652-013-0192-9

Kiyomoto S, Fukushima K, Miyake Y (2013) Security issues on it systems during disasters: a survey. J Amb Intell Human Comp, pp 1–13. http://dx.doi.org/10.1007/s12652-013-0177-8

Moseley M (2006) Homeland operations, US Air Force, Doctrine document 2–10. http://www.fas.org/irp/doddir/usaf/afdd2-10.pdf

Sharp W (2007) US Department of Defense, Homeland Security. http://www.fas.org/irp/doddir/dod/jp3_27.pdf

Solhaug B, Seehusen F (2013) Model-driven risk analysis of evolving critical infrastructures. J Amb Intell Human Comp, pp 1–18. http://dx.doi.org/10.1007/s12652-013-0179-6