J Ambient Intell Human Comput (2016) 7:149–151
DOI 10.1007/s12652-016-0348-5

EDITORIAL

Editorial: security and reliability of critical systems

Massimo Ficco[1]

Published online: 17 February 2016

Command and control applications are a vital part of modern distributed critical systems in various application areas, such as generation and distribution of electric power, storage and distribution of gas and oil, water supplies, banking and finance, government services, traffic control, and critical infrastructures. Centralized control is being replaced by distributed and more open control systems that possess increasing levels of autonomy. Communication networks, software architectures and intelligent systems are at the core of these developments. Such systems must be able to recover from the failures and intrusion in order to maintain their functions. Therefore, achieving resilience and security in such complex, interconnected, and inter-dependent systems, requires an integrated approach in engineering to address of resilience considerations across all constituent systems, cyber and physical.

The main purpose of this special issue is to invite researchers from academia and industry to contribute with ideas, show up problems and describe solutions regarding security and reliability of critical systems and infrastructures, particularly aiming to promote more state-of-the-art research in this area.

In particular, critical infrastructures protection is a complex and delicate activity, which can impact human lives and material goods, threatened by both natural phenomena, as well as the consequences of human errors. In this direction, Choras et al. (2015) present key results of the research activity conducted in the framework of FP7 CIPRNet project. Authors show an extended analysis of services composing the decision support system for critical infrastructures protection. Specific decision makers are presented to support 'decision-making process', both in the preparedness "*cold*" phase, as well as in the crisis "*hot*" phase. Moreover, dependability evaluation is an important, mandatory step in designing and analyzing critical systems. Accurate models are required to deal with dynamic, dependent behaviors, especially in complex systems. Therefore, Distefano (2015) identifies the main dynamic-dependent aspects that can affect the dependability of a critical system. Starting from the concept of dependence, author proposes an analytic formal framework for representing critical system dependability, as well as presents specific common dynamic aspects of dynamic-dependent systems.

As regards security aspects, in Li et al. (2015), authors propose a novel image authentication algorithm based on trisecting the original image to generate the authentication blocks as small as possible. In this algorithm, an image is split adaptively into some authentication blocks, which are composed of a number of fine-grained basic blocks. A recursive trisection method and adjacent strategies are adopted to connect basic blocks in sequence into a link. When the watermark payload cannot be embedded into an authentication block, the algorithm tries to merge only one basic block from the blocks linked to current authentication block. Theoretical analysis shows that the algorithm can adaptively adjust the size of each authentication block according to the image features to optimize the scale and adjacency of the authentication block. Experimental results show that, the authentication blocks division in the algorithm is finer, and the algorithm significantly improves the tamper localization accuracy. Han et al. (2015) focus on the design and analysis of a new biometrics-based

✉ Massimo Ficco
massimo.ficco@unina2.it

[1] Department of Industrial and Information Engineering, Second University of Naples, Via Roma 29, I-81031 Aversa, CE, Italy

authentication scheme for multi-server environment. In this work, authors firstly review Yoon and Yoo's authentication scheme (Yoon and Yoo 2013), and find that their scheme cannot resist the privileged insider attack, the user impersonation attack and the stolen smart card attack. Therefore, the authors proposed an improved scheme to overcome these weaknesses, as well as compared the performance and security properties to Yoon and Yoo's scheme. Moreover, public key infrastructure (PKI) authentication is the most important part for the security of business critical system, where each entity in the system need to confirm and validate the server certificate before a secure connection can be established. However, most current studies assume that different users have different security requirements, and even, the same users has different security requirements in different scenarios. Therefore, Zhiwei (2015) propose a new and flexible PKI authentication scheme based on certificate path trust index. Analysis and experimental results show that users can give a trade-off between security and efficiency, and the scheme has a higher efficiency and no bottleneck when authenticating with the higher level certification authority. In Jing et al. (2015), authors propose a novel attribute-based signature (ABS) scheme for general circuits based on correlation-relaxed two-to-one recoding system in multilinear maps setting. The paper proves selective enforceability of the proposed ABS under the $(n + d + l + 1)$-Multilinear Computational Die-Hellman assumption. As regards privacy aspects, in Yu et al. (2015), authors address an interesting question in cloud computing, that is, how to securely outsource scientific computation to cloud servers. In particular, malicious intrusions can falsify the computation and influence the result of a computation. Such issues are critical in cloud computing because of the untrust of the third party service. The approach that authors consider to cope with this issue is mathematical camouflage methods. In that context, authors first present several scientific computation problems, then, they survey the most relevant methods to keep the secret unknown to the host cloud servers, and then, propose a set of improvements to each of them, considering disguise methods, abstract equations, linear and non-linear equations. The detailed security analysis also give solid security guarantee for the privacy. Moreover, large-scale critical infrastructures are characterized by several distributed subsystems closely interdependent, which depend on underlying computer-communication information infrastructures. If the security of such infrastructure is weak, many problems and even disaster results could be risen. Therefore, using strong cryptography is essential to protect the security of such systems. In particular, the concept of proxy re-encryption is a promising techniques to deal with the key management. Therefore, a Cramer–Shoup based encryption scheme is proposed by Wang et al. (2015a). In order to support secure interactions among the subsystems of distributed critical systems, a multi-agent-based approach is proposed in Wang et al. (2015b). In particular, authors present a survey on rational secure multi-party computing systems, concerning the interaction among several utility-based agents (rational parties), which guarantee security of the computation in the presence of external attacks, as well as compare many adopted protocols. They present an IND-CCA2 secure proxy re-encryption scheme in standard model without pairings. Moreover, in Sicuranza et al. (2015) authors present a sophisticated and quick approach in retrieving sensitive clinical information about patients. The proposed strategy consists of an access control system, whose goal is to guarantee data integrity and privacy basing on RBAC (role-based access control) mechanisms and applying the principle of least privilege to the clinical information about the patient, which is the access limitation to the minimal level that allows normal operations. Finally, advanced cyber-threats are growing in frequency and sophistication. Therefore, sophisticated solutions are needed, which are able to reliably and timely detect frauds across multiple channels that process millions of transactions per day. These security solutions are required to process logs produced by different systems and correlate massive amounts of information in real-time. In this direction, Coppolino et al. (2015) propose a new approach to detect fraud in mobile money transfer (MMT). In particular, they adopt Dempster–Shafer theory to provide evidence combination from multiple and heterogeneous data sources. Moreover, a framework and the related workflow to detect frauds by using data fusion in the MMT system is presented. Simulation is also adopted to reproduce the set of transaction activities. In Tan et al. (2015), authors propose an artificial intelligence based approach to protect big data, which can be implemented in the command and control applications of critical systems. The presented solution can be used to analyze a very huge amount of data to detect unsafe schema. In order to support the image matching and stitching in the field of digital image security, Xie et al. (2015) propose an improved image mosaic algorithm, which is based on both wavelet transform and compressed sensing. The proposed algorithm has been validated through testing. In particular, testing results show that the proposed method achieves fast image matching, thus overcoming the shortcomings of heavy computation and low efficiency during the extraction of image features. Again, the proposed method ensures matching accuracy and stitching efficiency, so it meets the real-time requirements in machine vision system.

In Pascarella et al. (2015), deal with the generation of optimal flight trajectories for unmanned aerial vehicles (UAVs). In particular, they propose the parallelization of

the Core Paths Graph algorithm, which converts the trajectory optimization problem into a minimum cost path search, by a weighted and oriented graph. After presenting the mathematical formulation of the problem and the algorithm, the paper presents some test results, showing the obtained improvement of the proposed parallel algorithm. Moreover, for secure consideration, tracking the interesting targets within the coverage region is important in the radar surveillance systems. However, conventional mono-static radars suffer several threats, such as stealth targets, electronic jamming, anti-radiation missiles and the ultra-low altitude penetration. In order to reduce such threats, multistatic geometry and specified operational frequency based solutions could be adopted. In this direction, in Wen et al. (2014) authors propose a weighted least square method, which is applied by using a time of arrival (TOA) and angle of arrival (AOA) location estimation scheme. To evaluate the performance of the proposed scheme, the root mean square error distribution is employed.

Finally, in Toporkov et al. (2015) authors propose and analyze an interesting hybrid scheduling approach, based on a combination of cycling, back-filling and heuristic schemes, for efficient resources utilization in virtual organizations of utility grids. Different algorithms and approaches are compared, and results are provided to prove the correctness of the proposed one and justify its use in different situations. In particular, the simulations show that each of studied approaches can provide the best results under specific conditions, while the proposed hybrid scheme is able to balance such results, thus providing better efficiency under different conditions.

Acknowledgments I would like to thank the authors for the above papers published in this special issue. I 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 security and reliability of critical systems.

References

CIPRNet–Critical Infrastructure Preparedness and Resilience Research Network project. https://www.ciprnet.eu/summary.html

Coppolino L, D'Antonio S, Formicola V, Massei C, Romano L (2015) Use of the Dempster–Shafer theory to detect account takeovers in mobile money transfer services. J Ambient Intell Humaniz Comput 6(6):753–762

Distefano S (2015) Dependability assessment of critical systems. J Ambient Intell Humaniz Comput 6(6):713–720

Han S, Chongzhi G, Debiao H, Libing W (2015) New biometrics-based authentication scheme for multi-server environment in critical systems. J Ambient Intell Humaniz Comput 6(6):825–834

Jing Z, Jiang G, Gu C, Yu Z, Xu L (2015) Anonymous authentication for circuits from correlation relaxed two-to-one recoding. J Ambient Intell Humaniz Comput. doi:10.1007/s12652-015-0306-7

Kozik R, Choras M, Flizikowski A, Theocharidou M, Rosato V, Rome E (2015) Advanced services for critical infrastructures protection. J Ambient Intell Humaniz Comput 6(6):783–795

Li X, Li R, Huang Q, Luo J (2015) Minimized-expansion based lossless image authentication algorithm. J Ambient Intell Humaniz Comput 6(6):845–854

Pascarella D, Venticinque S, Aversa R, Mattei M, Blasi L (2015) Parallel and distributed computing for UAVs trajectory planning. J Ambient Intell Humaniz Comput 6(6):773–782

Sicuranza M, Esposito A, Ciampi M (2015) An access control model to minimize the data exchange in the information retrieval. J Ambient Intell Humaniz Comput 6(6):741–752

Tan X, Zhang X, Li J (2015) Big data quantum private comparison with the intelligent third party. J Ambient Intell Humaniz Comput 6(6):797–806

Toporkov V, Toporkova A, Tselishchev A, Yemelyanov D, Potekhin P (2015) Heuristic strategies for preference-based scheduling in virtual organizations of utility grids. J Ambient Intell Humaniz Comput 6(6):733–740

Wang Y, Li T, Qin H, Li J, Gao W, Liu Z, Xu Q (2015a) A brief survey on secure multi-party computing in the presence of rational parties. J Ambient Intell Humaniz Comput 6(6):807–824

Wang XA, Ma J, Yang X (2015b) A new proxy re-encryption scheme for protecting critical information systems. J Ambient Intell Humaniz Comput 6(6):699–711

Wen J-H, Li J-S, Chen H-C, Chen C-H, Yang C-Y, Mao C-H (2014) Localization scheme based on multistatic radar systems. J Ambient Intell Humaniz Comput. doi:10.1007/s12652-016-0347-6

Xie X, Xu Y, Liu Q, Hu F, Cai T, Jiang N, Xiong H (2015) A study on fast SIFT image mosaic algorithm based on compressed sensing and wavelet transform. J Ambient Intell Humaniz Comput 6(6):835–843

Yoon E-J, Yoo K-Y (2013) Robust biometrics-based multi-server authentication with key agreement scheme for smart cards on elliptic curve cryptosystem. J Supercomput 63(1):235–255

Yu J, Wang X, Gao W (2015) Improvement and applications of secure outsourcing of scientific computations. J Ambient Intell Humaniz Comput 6(6):763–772

Zhiwei G (2015) CPTIAS: a new fast PKI authentication scheme based on certificate path trust index. J Ambient Intell Humaniz Comput 6(6):721–731