Erol Gelenbe · Marija Jankovic ·
Dionysios Kehagias · Anna Marton ·
Andras Vilmos (Eds.)

Communications in Computer and Information Science 1596

Security in Computer and Information Sciences

Second International Symposium, EuroCybersec 2021
Nice, France, October 25–26, 2021
Revised Selected Papers

Springer

OPEN ACCESS

Communications in Computer and Information Science 1596

Editorial Board Members

Joaquim Filipe
Polytechnic Institute of Setúbal, Setúbal, Portugal

Ashish Ghosh
Indian Statistical Institute, Kolkata, India

Raquel Oliveira Prates
Federal University of Minas Gerais (UFMG), Belo Horizonte, Brazil

Lizhu Zhou
Tsinghua University, Beijing, China

More information about this series at https://link.springer.com/bookseries/7899

Erol Gelenbe · Marija Jankovic ·
Dionysios Kehagias · Anna Marton ·
Andras Vilmos (Eds.)

Security in Computer and Information Sciences

Second International Symposium, EuroCybersec 2021
Nice, France, October 25–26, 2021
Revised Selected Papers

Springer

Editors
Erol Gelenbe
IITIS-PAN
Gliwice, Poland

Marija Jankovic
ITI-CERTH
Thessaloniki, Greece

Dionysios Kehagias
ITI-CERTH
Thessaloniki, Greece

Anna Marton
Safepay Systems
Budapest, Hungary

Andras Vilmos
Safepay Systems
Budapest, Hungary

ISSN 1865-0929 ISSN 1865-0937 (electronic)
Communications in Computer and Information Science
ISBN 978-3-031-09356-2 ISBN 978-3-031-09357-9 (eBook)
https://doi.org/10.1007/978-3-031-09357-9

© The Editor(s) (if applicable) and The Author(s) 2022. This book is an open access publication.
Open Access This book is licensed under the terms of the Creative Commons Attribution 4.0 International License (http://creativecommons.org/licenses/by/4.0/), which permits use, sharing, adaptation, distribution and reproduction in any medium or format, as long as you give appropriate credit to the original author(s) and the source, provide a link to the Creative Commons license and indicate if changes were made.
The images or other third party material in this book are included in the book's Creative Commons license, unless indicated otherwise in a credit line to the material. If material is not included in the book's Creative Commons license and your intended use is not permitted by statutory regulation or exceeds the permitted use, you will need to obtain permission directly from the copyright holder.
The use of general descriptive names, registered names, trademarks, service marks, etc. in this publication does not imply, even in the absence of a specific statement, that such names are exempt from the relevant protective laws and regulations and therefore free for general use.
The publisher, the authors, and the editors are safe to assume that the advice and information in this book are believed to be true and accurate at the date of publication. Neither the publisher nor the authors or the editors give a warranty, expressed or implied, with respect to the material contained herein or for any errors or omissions that may have been made. The publisher remains neutral with regard to jurisdictional claims in published maps and institutional affiliations.

This Springer imprint is published by the registered company Springer Nature Switzerland AG
The registered company address is: Gewerbestrasse 11, 6330 Cham, Switzerland

Preface

The Second International ISCIS Symposium on Security in Computer and Information Sciences (EuroCybersec 2021) was held in Nice, France, during October 25–26, 2021. It was supported by the European Commission H2020 Program through the IoTAC Research and Innovation Action, under Grant Agreement No. 952684.

The symposium was organized by the European Union's IoTAC project and the Institute of Theoretical and Applied Informatiocs of the Polish Academy of Sciences (IITIS-PAN), based on an open call for papers and presentations selected by the Program Committee.

After the oral presentations, the Program Committee then reviewed the papers that were presented to evaluate once again their originality, scientific quality, and technical maturity, and made a further selection resulting in the nine papers included in these proceedings. All papers coauthored by committee members were handled in an appropriate review process.

The key areas covered by these proceedings include the Internet of Things (IoT), cybersecurity, IoT gateways, IoT attack detection and mitigation, the IoT massive access problem, adaptive routing for security, quality of service (QoS), and energy optimization in Fog and Edge systems that support the IoT.

EuroCybersec 2021 follows up on a previous workshop held in 2018 at Imperial College London, UK [15], as part of the sequence of International Symposia on Computer and Information Sciences (ISCIS) that started in 1986 and have been held over the years in Turkey, France, the USA, the UK, and Poland [2, 7–9, 14, 18–20, 37].

The ease of access to the Internet with a very high traffic yet inexpensive business model has raised major concerns with regard to cybersecurity, since the Internet offers low cost high volume access not only to legitimate users but also to various malicious users. The advent of IoT has thus created even more opportunities to attack not just virtual facilities but also cyber-physical systems [24].

Of course, various organizations, including the European Union, have published recommendations for Internet security and privacy [12], but this has by no means reduced the number of cyberattacks over the years. This growing insecurity in systems and networks also results in increased energy consumption by ICT [16, 34] due to increased traffic as well as more software that is meant to insure secure operation. These concerns also raise major issues that combine performance and QoS, security, and energy consumption [27].

As a consequence, the European Commission has increasingly supported research projects in these fields [1], with projects such as NEMESYS on the cybersecurity of mobile telephone systems [3, 33], SDK4ED on energy savings in dependable and secure systems [35, 36], KONFIDO [10, 11, 31, 32] on the security of health informatics systems, GHOST [5, 6, 26] regarding the security of IoT home gateways, and SerIoT on the cybersecurity of IoT systems[4, 13].

The current project IoTAC [25] pursues this work and aims at securing IoT networks by protecting IoT gateways using techniques such as Botnet detection and system wide

vulnerability assessement [28, 29], disruptive checkpoints, and assuring efficient massive IoT device access to gateways [21, 23]. The topics covered by the EuroCyberSec 2021 symposium reflected the aims of the IoTAC project.

Over 20 paper presentations were submitted of which 15 were retained for the symposium, and nine full papers were selected for these proceedings by the Program Committee based on technical quality. One additional review paper was invited. Over 40 participants attended, with some 15 physically present and the remainder online.

The papers in these proceedings discuss aspects specifically relevant to the IoTAC project, and also of broad interest to cybersecurity and related European Union projects, including other research projects and some of their outcomes, such as the combined societal and technical implications of IoT cybersecurity.

Since software is the ultimate target of cyberattacks, software vulnerability detection methods were examined by examining the influence of the "vocabulary" used inside programs, relating to the security by design for software systems considered in IoTAC. Signal processing techniques applied to digital data on the internal computer data transfer "bus" can help detect anomalies or attacks on servers, while incremental attack detection can also be performed, with ongoing learning and detection occurring as the packet traffic flows into a gateway [30].

The important issue of energy consumption for battery powered drone surveillance missions, in order to optimize actions within a mission and maximize mission duration, is of great importance in both civilian and military applications, and is also relevant to one of the IoTAC use cases involving Airbus industries.

The authentication of IoT devices by hardware and software means with a hybrid approach connects us to the SETIT project, also funded by the European Commission. Secure authentication schemes are also discussed, as well as fast adaptive routing-based methods aimed at reducing energy consumption while improving both performance and system security at the Edge [22].

IoT also has a massive access problem when a large number of IoT devices access a gateway frequently or periodically, which can be addresed by novel traffic shaping techniques [17].

We hope that you find these papers interesting and fruitful for your own research.

Erol Gelenbe
Marija Jankovic
Dionysios Kehagias
Anna Marton
Andras Vilmos

References

1. https://www.grantsoffice.com/Portals/0/funded/issues/FUNDEDOct2021.pdf
2. Abdelrahman, O.H., Gelenbe, E., Görbil, G., Lent, R. (eds.): Information Sciences and Systems 2015 - 30th International Symposium on Computer and Information Sciences, ISCIS 2015, London, UK, 21–24 September 2015, Lecture Notes in Electrical Engineering, vol. 363. Springer (2016)
3. Abdelrahman, O.H., Gelenbe, E., Görbil, G., Oklander, B.: Mobile network anomaly detection and mitigation: The NEMESYS approach. In: Information Sciences and Systems 2013, pp. 429–438. Springer (2013)
4. Baldini, G., et al.: Iot network risk assessment and mitigation: the seriot approach. In: Soldatos, J. (ed.) Security Risk Management for the Internet of Things: Technologies and Techniques for IoT Security, Privacy and Data Protection. pp. 87–104. NOW Publishers (2020). https://doi.org/10.1561/9781680836837, https://www.nowpublishers.com/article/Chapter/9781680836820?cId=978-1-68083-683-7.ch5
5. Brun, O., Yin, Y., Gelenbe, E.: Deep learning with dense random neural network for detecting attacks against IoT-connected home environments. Procedia Computer Science **134**, pp. 458–463 (2018)
6. Collen, A., et al.: GHOST - safe-guarding home IoT environments with personalised real-time risk control. In: Gelenbe, E., Campegiani, P., Czachorski, T., Katsikas, S., Komnios, I., Romano, L., Tzovaras, D. (eds.) Recent Cybersecurity Research in Europe: Proceedings of the 2018 ISCIS Security Workshop, Imperial College London. Communications in Computer and Information Science, vol. 821, pp. 68–78. Springer (2018)
7. Czachórski, T., Gelenbe, E., Grochla, K., Lent, R. (eds.): Computer and Information Sciences - 31st International Symposium, ISCIS 2016, Kraków, Poland, October 27–28, 2016, Proceedings, Communications in Computer and Information Science, vol. 659. Springer (2016)
8. Czachórski, T., Gelenbe, E., Grochla, K., Lent, R.: Computer and Information Sciences - 32nd International Symposium, ISCIS 2018, held at the 24th IFIP World Computer Congress, WCC 2018, Poznan, Poland, September 20–21, 2018, Proceedings (2018)
9. Czachórski, T., Gelenbe, E., Lent, R. (eds.): Information Sciences and Systems 2014 - Proceedings of the 29th International Symposium on Computer and Information Sciences, ISCIS 2014, Krakow, Poland, October 27–28, 2014. Springer (2014)
10. Diamantopoulos, S., et al.: Secure cross-border exchange of health related data: The KONFIDO approach. In: International Conference on Internet and Distributed Computing Systems, pp. 318–327. Springer (2019)
11. Diamantopoulos, S., et al.: Secure cross-border exchange of health related data: The KONFIDO approach. In: EDCC, pp. 73–74. IEEE (2019)
12. European Commission Cybersecurity Policies: https://digital-strategy.ec.europa.eu/en/policies/cybersecurity-policies
13. Frötscher, A., Monschiebl, B., Drosou, A., Gelenbe, E., Reed, M.J., Al-Naday, M.: Improve cybersecurity of C-ITS road side infrastructure installations: the SerIoT - secure and safe IoT approach. In: 2019 IEEE International Conference on Connected Vehicles and Expo (ICCVE), pp. 1–5. IEEE (2019)
14. Gelenbe, E.: The 24th International Symposium on Computer and Information Sciences, ISCIS 2009, 14–16 September 2009, North Cyprus. IEEE (2009)
15. Gelenbe, E., et al.: Security in computer and information sciences: First International ISCIS Security Workshop, Euro-Cybersec 2018, London, UK, February 26–27, 2018, revised selected papers (2018)

16. Gelenbe, E., Caseau, Y.: The impact of information technology on energy consumption and carbon emissions. Ubiquity 2015 (June), pp. 1–15. ACM (2015)
17. Gelenbe, E., Czachorski, T., Marek, D., Nakıp, M.: Mitigating the massive access problem in the internet of things. In: EuroCybersec 2021. Springer (2022)
18. Gelenbe, E., Lent, R. (eds.): Computer and Information Sciences III - 27th International Symposium on Computer and Information Sciences, Paris, France, October 3–4, 2012. Springer (2013)
19. Gelenbe, E., Lent, R. (eds.): Information Sciences and Systems 2013 - Proceedings of the 28th International Symposium on Computer and Information Sciences, ISCIS 2013, Paris, France, October 28–29, 2013, Lecture Notes in Electrical Engineering, vol. 264. Springer (2013)
20. Gelenbe, E., Lent, R., Sakellari, G., Sacan, A., Toroslu, I.H., Yazici, A.: Computer and Information Sciences - Proceedings of the 25th International Symposium on Computer and Information Sciences, London, UK, September 22–24, 2010, Lecture Notes in Electrical Engineering, vol. 62. Springer (2010).
21. Gelenbe, E., Nakip, M., Marek, D., Czachorski, T.: Diffusion analysis improves scalability of IoT networks to mitigate the massive access problem. In: IEEE MASCOTS 2021: 29th International Symposium on Modelling, Analysis and Simulation of Computer and Telecommunication Systems, pp. 1–6. IEEE (2021)
22. Gelenbe, E., Nowak, M.P., Frohlich, P., Fiołka, J., Chęciński, J.: Energy, QoS and security aware services at the edge. In: EuroCybersec 2021. Springer (2022)
23. Gelenbe, E., Sigman, K.: IoT traffic shaping and the massive access problem. In: ICC 2022, IEEE International Conference on Communications, 16–20 May 2022, Seoul, South Korea. pp. 2290–2295 (2022)
24. Gelenbe, E., Wu, F.J.: Future research on cyber-physical emergency management systems. Future Internet **5**(3), pp. 336–354 (2013)
25. Siavvas M., et al.: The IoTAC software security-by-design platform: Concept, challenges, and preliminary overview. In: DRCNN 2022: 1st International Workshop on Key challenges in Global Cybersecurity: Efforts and Trends in EU (KCYEU), pp. 1–6. IEEE (2022)
26. Kadioglu, Y.M., Gelenbe, E.: Product-form solution for cascade networks with intermittent energy. IEEE Syst. J. **13**(1), pp. 918–927. IEEE (2019)
27. Kehagias, D.D., Jankovic, M., Siavvas, M.G., Gelenbe, E.: Investigating the interaction between energy consumption, quality of service, reliability, security, and maintainability of computer systems and networks. SN Comput. Sci. **2**(1), 23 (2021)
28. Nakip, M., Gelenbe, E.: Mirai botnet attack detection with auto-associative dense random neural networks. In: 2021 IEEE Global Communications Conference. vol. 2021, pp. 1–6. IEEE (2021)
29. Nakip, M., Gelenbe, E.: Randomization of data generation times improves performance of predictive IoT networks. In: IEEE World Forum on Internet of Things (WF IoT), July 14–21, 2021. p. 5161. IEEE (2021)
30. Nakip, M., Gelenbe, E.: Botnet attack detection with incremental online learning. In: EuroCybersec 2021. Springer (2022)

31. Nalin, M., et al.: The European cross-border health data exchange roadmap: Case study in the Italian setting. Journal of Biomedical Informatics **94**, 103183 (2019)
32. Natsiavas, P., et al.: Developing an infrastructure for secure patient summary exchange in the eu context: Lessons learned from the KONFIDO project. Health Informatics Journal **27**(2), 14604582211021459 (2021)
33. Pavloski, M., Gelenbe, E.: Mitigating for signalling attacks in UMTS networks. In: Information Sciences and Systems 2014, pp. 159–165. Springer (2014)
34. Pernici, B., Aiello, M., Vom Brocke, J., Donnellan, B., Gelenbe, E., Kretsis, M.: What IS can do for environmental sustainability: a report from CAiSE'11 panel on green and sustainable IS. Communications of the Association for Information Systems **30**(1), 18 (2012)
35. Siavvas, M., et al.: An empirical evaluation of the relationship between technical debt and software security. In: ICIST 2019 Proceedings. vol. 1, pp. 199–203 (2019)
36. Siavvas, M.G., Gelenbe, E.: Optimum interval for application-level checkpoints. In: CSCloud/EdgeCom. pp. 145–150. IEEE (2019)
37. Tugcu, T., Caglayan, M.U., Alagoz, F., Gelenbe, E. (eds.): New Trends in Computer Networks: 20th International Symposium on Computer and Information Sciences (2005)

Organization

Organizing Committee

Erol Gelenbe	IITIS, Polish Academy of Sciences, Poland
Marija Jankovic	ITI-CERTH, Greece
Dionysios Kehagias	ITI-CERTH, Greece
Anna Marton	SafePay, Hungary
Andras Vilmos	ATOS, Hungary

Program Committee

Erol Gelenbe (Chair)	IITIS, Polish Academy of Sciences
Levente Buttyan	Budapest University of Technology and Economics, Hungary
Ufuk Caglayan	Yasar University, Turkey
Maria Carla Calzarossa	University of Pavia, Italy
Tadeusz Czachorski	IITIS, Polish Academy of Sciences, Poland
Cuneyt Guzelis	Yasar University, Turkey
Peter Hoffman	T-Sec, Germany
Marija Jankovic	ITI-CERTH, Greece
Dionysios Kehagias	ITI-CERTH, Thessaloniki, Greece
Ioannis Mavridis	University of Macedonia, Greece
Miltiadis Siavvas	ITI-CERTH, Greece

Contents