Information Security and Risk Management: Trustworthiness and Human Interaction

Stephen C. Phillips[1], Nicholas Fair[1(✉)], Gencer Erdogan[2], and Simeon Tverdal[2]

[1] IT Innovation Centre, University of Southampton, Southampton, UK
{S.C.Phillips,N.S.Fair}@soton.ac.uk
[2] Sustainable Communication Technologies, SINTEF Digital, Oslo, Norway
{gencer.erdogan,simeon.tverdal}@sintef.no

1 Tutorial Abstract

As digital information has come to underpin the majority of modern systems in almost all domains (e.g. business, finance, government, education, health, third sector), increasingly sophisticated cybersecurity attacks have become an unavoidable reality of modern life. In the face of this, regulation and best practice are increasing moving from simplistic security control tick-lists towards risk management frameworks (such as recommended in the EU's GDPR and NIS directive and described in standards such as ISO 27005). Consequently, it is highly relevant for students, practitioners, and researchers alike to understand risk management, systems modelling, attack paths, and human interactions and risks in order to understand the central value and importance of cybersecurity risk management in supporting trustworthiness in information systems.

As part of the H2020 CyberKit4SME project, this interactive, hands-on tutorial will explore state-of-the-art approaches to trustworthy cybersecurity risk management that is able to effectively and sufficiently account for the risks that humans introduce into any information system [1]. After establishing the basic concepts around cybersecurity, trustworthiness, system modelling, risk management and socio-technical theory, an exploration of the importance and role of visualised attack paths in providing easily understood risks, thereby ensuring intelligent risk management tools do not become 'black boxes' to their users, will be undertaken. Alongside this, how attack paths help support human decision-making by pinpointing the most effective risk mitigation strategies will be investigated. In addition, the tutorial will explore human interaction flows and how they can combine with attack paths to empower comprehensive cybersecurity risk assessments and help guide holistic mitigations. In the final part of the tutorial, there will be an opportunity to get practical experience of modelling an information system and identifying and mitigating the cybersecurity risks to it using two tools: the System Security Modeller [2, 3] (University of Southampton) and the Human and Organisational Risk Modelling framework (SINTEF) which is derived from the Customer Journey Modelling Language [4, 5] (CJML).

Acknowledgements. This work has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No. 883188.

R. Guizzardi et al. (Eds.): RCIS 2022, LNBIP 446, pp. 821–822, 2022.
https://doi.org/10.1007/978-3-031-05760-1

Learning Goals

By the end of the tutorial attendees will have a general understanding of risk management; of what is meant by trustworthiness in cybersecurity system modelling and of the risk impact of humans in information systems. A specific understanding of the role of visualised attack paths in promoting trustworthiness and human choice in cybersecurity system modelling; of how to conceptualise and model human interaction flows and of how attack paths and human interaction flows interact when assessing cybersecurity risk and risk mitigation strategies will be imparted along with experience using a system modeller and interaction flow charts to identify cybersecurity risk and risk mitigation strategies.

Presenters

Dr. Stephen C. Phillips, Principal Research Engineer, technical coordinator of the H2020 CyberKit4SME project, System Security Modeller product manager.
Dr. Gencer Erdogan, Research Scientist, technical lead H2020 CyberKit4SME, developer of the Human and Organisational Risk Modelling framework.
Dr. Nic Fair, Research Engineer, digital education and learning expert, contributor to the System Security Modeller.
Simeon Andersen Tverdal, Researcher, developer of Human and Organisational Risk Modelling framework.

References

1. Boletsis, C., Halvorsrud, R., Pickering, J.B., Phillips, S.C., Surridge, M.: Cybersecurity for SMEs: introducing the human element into socio-technical cybersecurity risk assessment. In: Proceedings of the 16th International Joint Conference on Computer Vision, Imaging and Computer Graphics Theory and Applications (VISIGRAPP 2021), vol. 3, pp. 266–274
2. Surridge, M., et al.: Modelling compliance threats and security analysis of cross border health data exchange. In: Attiogbé, C., Ferrarotti, F., Maabout, S. (eds.) MEDI 2019. CCIS, vol. 1085, pp 180–189 (2019). Springer, Cham. https://doi.org/10.1007/978-3-030-32213-7_14
3. Mohammadi, N., Goeke, L., Heisel, M., Surridge, M.: Systematic risk assessment of cloud computing systems using a combined model-based approach. In: Proceedings of the 22nd International Conference on Enterprise Information Systems, vol. 2, pp. 53-66
4. Halvorsrud, R., Kvale, K., Følstad, A.: Improving service quality through customer journey analysis. J. Serv. Theory Pract. **26**, 840-867 (2016)
5. Halvorsrud, R., Boletsis, C., Garcia-Ceja, E.: Designing a modeling language for customer journeys: lessons learned from user involvement. In: Proceedings of the 24th ACM/IEEE International Conference on Model Driven Engineering Languages and Systems (MODELS), pp. 239–249 (2021)