Security and Privacy for Emerging IoT and CPS Domains

Elisa Bertino
bertino@purdue.edu
Purdue University

Ravi Sandhu
ravi.sandhu@utsa.edu
The University of Texas at San Antonio

Bhavani Thuraisingham
bxt043000@utdallas.edu
The University of Texas at Dallas

Indrakshi Ray
Indrakshi.Ray@colostate.edu
Colorado State University

Wenjia Li
wli20@nyit.edu
New York Institute of Technology

Maanak Gupta
(Moderator)
mgupta@tntech.edu
Tennessee Tech University

Sudip Mittal
(Moderator)
mittal@cse.msstate.edu
Mississippi State University

ABSTRACT

The proliferation of IoT and CPS technologies demand novel conceptual, foundational and applied cybersecurity solutions. The dynamic behaviour of these distributed systems augmented with physical and computational constraints of smart devices, require cybersecurity approaches for timely prevention and detection of attacks. This panel aims to discuss open challenges and highlight future research directions for cybersecurity in IoT and CPS.

ACM Reference Format:
Elisa Bertino, Ravi Sandhu, Bhavani Thuraisingham, Indrakshi Ray, Wenjia Li, Maanak Gupta, and Sudip Mittal. 2022. Security and Privacy for Emerging IoT and CPS Domains. In *Proceedings of the Twelveth ACM Conference on Data and Application Security and Privacy (CODASPY '22), April 24–27, 2022, Baltimore, MD, USA*. ACM, New York, NY, USA, 2 pages. https://doi.org/10.1145/3508398.3519314

Statement of Elisa Bertino Protecting IoT systems is a major challenge as these systems are large-scale in many environments, such as smart homes, smart manufacturing plants, and smart communities. In addition, such systems are often highly dynamic and heterogeneous, and may include devices with actuation capabilities, thus be able to execute "physical actions". It is important to notice that in the future those systems will likely be managed by AI techniques, such as reinforcement learning (RL) techniques, as manually managing those systems will not be feasible. The characteristics of IoT systems have implications on the security approaches but also on the AI techniques used for their management. As an example, consider the well-known fuzzing techniques used to test software security. An issue with the application of those techniques is when IoT devices have actuation capabilities. In this case, testing the effect of input parameter values may require the execution of actual actions in some physical space, which may not be always feasible. An initial approach to address this problem has been proposed by Han at al. [1] for the application of fuzzing to detect unsafe combinations of control parameters for drones. The key idea of this approach is to use a machine learning predictor to predict the effect of the fuzzed control parameters values. However, much work needs to be done including how to systematically and formally analyze these systems to detect security vulnerabilities when the number of parties in the systems is very large as current formal methods may not scale up. Concerning the AI-based management of IoT systems, it is critical that the used AI techniques be safety and security aware. An initial example toward addressing such a requirement is by Mudgerikar and Bertino [2] for the case of a RL-based framework to manage IoT systems in smart home environments. The key idea of the approach is to constrain the explorations by the RL agent by specifying actions that should not be considered because of safety and/or security risks. Such an approach is just an initial step and research is needed to develop metrics to quantify security and safety risks for use in quality functions of RL-based models, to learn security and safe actions for specific environments, and to design security/safety aware RL techniques for other application domains. Last but not least, techniques are required to secure AI based management systems from attacks aiming to make these systems learn unsafe/unsecure policies and actions.

Elisa Bertino is professor of Computer Science at Purdue University. Prior to joining Purdue, she was a professor and head at the Department of Computer Science and Communication of the University of Milan. She is a Fellow member of IEEE, ACM, and AAAS. She received the 2002 IEEE Computer Society Technical Achievement Award for "For outstanding contributions to database systems and database security and advanced data management systems", the 2005 IEEE Computer Society Tsutomu Kanai Award for "Pioneering and innovative research contributions to secure distributed systems", and the 2019-2020 ACM Athena Lecturer Award.

Statement of Ravi Sandhu Security challenges can seem overwhelming. (Incidentally, I use security as an overarching term that definitely includes privacy.) We have done such a lousy job in the traditional enterprise domain, so how can we hope to do anything at all in such complex domains even as they are rapidly evolving as we contemplate them. We have to think differently. The four fundamental cyber security technologies (protection, detection, policy and attacks) are intrinsically intertwined and interdependent. Yet our pedagogy, research and practice are hopelessly siloed. The community must make a conscious effort to move towards convergence and synergy. This can only be done by transdisciplinary teams at a scale that the cyber security community is simply not familiar with. How do we get there? I would like to see some discussion on this issue, not just at the panel but even more so in the community.

CODASPY '22, April 24–27, 2022, Baltimore, MD, USA

ACM ISBN 978-1-4503-9220-4/22/04.
https://doi.org/10.1145/3508398.3519314

Ravi Sandhu is Professor of Computer Science, Executive Director of the Institute for Cyber Security and Lead PI of the NSF Center for Security and Privacy Enhanced Cloud Computing at the University of Texas at San Antonio, where he holds the Lutcher Brown Endowed Chair in Cyber Security. Previously he served on the faculty at George Mason University (1989-2007) and Ohio State University (1982-1989). He holds BTech and MTech degrees from IIT Bombay and Delhi, and MS and PhD degrees from Rutgers University. He is a Fellow of IEEE, ACM, AAAS and the National Academy of Inventors. He has received numerous awards from IEEE, ACM, NSA, NIST and IFIP, including the 2018 IEEE Innovation in Societal Infrastructure award for seminal work on role-based access control (RBAC). He was Chairman of ACM SIGSAC, and founded the ACM CCS, the ACM SACMAT and the ACM CODASPY. He is an inventor on 31 security technology patents and has accumulated over 45,000 Google Scholar citations for his papers. At UTSA his team research in both the scientific foundations of cyber security and their applications in diverse cyber technology domains, including cloud computing, IoT, autonomous vehicles, big data and blockchain. Particular focus is on foundations and technology of attribute-based access control (ABAC) as a successor to RBAC in these contexts, and on converegnce of access control concepts to solve real-world challenges. His web site is at www.profsandhu.com.

Statement of Indrakshi Ray With the advancement of technology, we are seeing the emergence of cyber physical systems and cyber physical social systems. We are gradually entering an era of a smart and connected world in which we envision seamless functionality across various ecosystems. Users can access services anytime and anywhere. Such improved functionalities come at a cost: systems are now more complex, harder to understand and analyze and are more vulnerable to attacks. Widespread connectivity may cause an attack to have far reaching consequences. Traditional security mechanisms are unsuitable for protecting such systems because of the unique constraints imposed by physical laws compounded with the fact that such systems are used by humans with very diverse technological background and capabilities. Analyzing such large-scale complex system to provide assurance about their secure and correct behavior using formal methods alone is infeasible. The analysis must be augmented with data analytics to ensure that the system is behaving as expected. We use a smart home as an example IoT environment. Smart homes have IoT devices with sensors and actuators which are connected to the network and are operated by humans, so they fall under the category of cyber physical social systems. Most IoT devices are designed without considering security, and applications controlling these devices often have poor security postures. IoT devices in a smart home gather large volumes of data about the home environment. This data contains sensitive and private information pertaining to the residents. We demonstrate how one can use this data to prevent and detect attacks in the IoT network. Such data can also be used by external agencies to provide services to the residents. We discuss the challenges to the use of such data. Finally, we demonstrate how system analytics can be used to provide assurance of secure and correct behavior in a smart home.

Indrakshi Ray is a Professor in the Computer Science Department at Colorado State University. She is the Director of Colorado Center for Cyber Security at Colorado State University. She is also the Site Director of NSF IUCRC Center for Cyber Security Analytics and Automation. She has been a visiting faculty at Air Force Research Laboratory, Naval Research Laboratory, and at INRIA, Rocquencourt, France. She obtained her Ph.D. in Information Technology from George Mason University. Dr. Ray's research interests include software assurance, data analytics and security. Dr. Ray is on the editorial board of IEEE Transactions on Services Computing, International Journal of Information Security, Computer Standards and Interfaces, and Associate Editor of IEEE Security Privacy. Dr. Ray is served the program committees of various conferences including ACM CODASPY, ACM SACMAT, DBSec, ESORICS, ICDE. She is a senior member of the IEEE and the ACM. She was awarded Professor Laureate from the College of Natural Sciences at CSU.

Statement of Wenjia Li In recent years, the concept of connected vehicles has attracted extensive attentions from both academia and industry. Vehicular network is a key enabling technology to support connected vehicles, in which traffic-related messages are generated and exchanged to improve safety and efficiency. However, these traffic-related messages could be erroneous, which can be caused by various reasons, ranging from an onboard device (OBD) sensor malfunctioning and reporting incorrect reading to the message being tampered by a malicious vehicle. To address these rapidly increasing security challenges, we propose to apply both deep learning and the blockchain technology to the trust management system, which could enhance its effectiveness and also make the trust managament system resistant to various malicious attacks. In the proposed AIT system, each vehicle first senses, generates, and exchanges messages with other vehicles. These messages then get validated by the neighboring vehicles. As vehicles receive and validate messages from other nearby vehicles, they will establish and manage the trust of those nearby vehicles, which is enabled by utilizing the deep learning algorithm. Once a vehicle identifies untrustworthy vehicles, it reports them to the nearby roadside unit (RSU), and the RSU will validate the authenticity of the report as well as the identity of the vehicle by using the emerging blockchain technique. The security credentials of untrustworthy vehicles will then be revoked by the RSU. We consider three types of attacks against the trust management system, namely Simple Attack (SA), Bad Mouth Attack (BMA), and Zigzag Attack (ZA).

Dr. Wenjia Li is an Associate Professor of Computer Science at New Yrok Institute of Technology (NYIT). His research interest include cyber security, mobile computing, and wireless networking, particularly security, trust, and policy issues for wireless networks, CPS, IoT, and ITS. His research has been supported by the NIH and the U.S. DOT Region 2 University Transportation Research Center (UTRC). He was the recipient of the 2019 IEEE Region 1 Technological Innovation (Academic) Award. He was also the recipient of 2020 NYIT Presidential Excellence Award for Student Engagement in Research, Scholarship, or Creative Activities.

REFERENCES

[1] Ruidong Han, Chao Yang, Siqi Ma, JiangFeng Ma, Cong Sun, Juanru Li, and Elisa Bertino. Control parameters considered harmful: Detecting range specification bugs in drone configuration modules via learning-guided search. *arXiv preprint arXiv:2112.03511*, 2021.

[2] Anand Mudgerikar and Elisa Bertino. Jarvis: Moving towards a smarter internet of things. In *2020 IEEE 40th International Conference on Distributed Computing Systems (ICDCS)*, pages 122–134. IEEE, 2020.