

Preface

Computers and IT infrastructure play ever-increasing roles in our daily lives. The technological trend toward higher computational power and ubiquitous connectivity can also give rise to new risks and threats. To ensure economic growth and prosperity, nations, corporations, and individuals constantly need to reason about how to protect their sensitive assets.

Security is hard: it is a multifaceted problem that requires a careful appreciation of many complexities regarding the underlying computation and communication technologies and their interaction and interdependencies with other infrastructure and services. Besides these technical aspects, security provision also intrinsically depends on human behavior, economic concerns, and social factors. Indeed, the systems whose security is concerned are typically heterogeneous, large-scale, complex, dynamic, interactive, and decentralized in nature.

Game and decision theory has emerged as a valuable systematic framework with powerful analytical tools in dealing with the intricacies involved in making sound and sensible security decisions. For instance, game theory provides methodical approaches to account for interdependencies of security decisions, the role of hidden and asymmetric information, the perception of risks and costs in human behavior, the incentives/limitations of the attackers, and much more. Combined with our classic approach to computer and network security, and drawing from various fields such as economic, social, and behavioral sciences, game and decision theory is playing a fundamental role in the development of the pillars of the “science of security.”

Since its inception in 2010, GameSec has annually attracted original research in both theoretical and practical aspects of decision making for security and privacy. The past editions of the conference took place in Berlin (2010), College Park (2011), Budapest (2012), FortWorth (2013), and Los Angeles (2014). This year (2015), it was hosted for the first time in the UK, in the heart of London.

We received 37 submissions this year from which, 16 full-length and five short papers we selected after a thorough review process by an international panel of scholars and researchers in this field. Each paper typically received three reviews assessing the relevance, novelty, original contribution, and technical soundness of the paper. The topics of accepted papers include applications of game theory in network security, economics of cybersecurity investment and risk management, learning and behavioral models for security and privacy, algorithm design for efficient computation, and investigation of trust and uncertainty, among others.

We would like to thank Springer for its continued support of the GameSec conference and for publishing the proceedings as part of their *Lecture Notes in Computer*

Series (LNCS) with special thanks to Anna Kramer. We anticipate that researchers in the area of decision making for cybersecurity and the larger community of computer and network security will benefit from this edition.

November 2015

MHR Khouzani
Emmanouil Panaousis
George Theodorakopoulos

<http://www.springer.com/978-3-319-25593-4>

Decision and Game Theory for Security

6th International Conference, GameSec 2015, London,

UK, November 4-5, 2015, Proceedings

Khouzani, M.; Panaousis, E.; Theodorakopoulos, G.

(Eds.)

2015, X, 371 p. 90 illus. in color., Softcover

ISBN: 978-3-319-25593-4