

Preface

Contemporary information and communication technology evolves fast not only in terms of sophistication, but also in diversity. The increasing complexity, pervasiveness, and connectivity of today's information systems raises new challenges to security, and cyberspace has become a playground for people with all levels of skills and all kinds of intention (positive and negative). With 24/7 connectivity having become an integral part of people's daily life, protecting information, identities, and assets has gained more importance than ever. While oil and coal have been the most important commodities in past centuries, information is the commodity of the twenty-first century, and cyberwarfare is widely about gaining the most of the resource "information," as much as past decades have seen wars for land or wealth.

Traditional security has successfully accomplished a long way toward protecting well-defined goals like confidentiality, integrity, availability, and authenticity (CIA+). However, the term "security" has evolved into meaning much more than CIA+ these days. The Internet is surely an indispensable supporting infrastructure, but also an equally rich source of threats. Around the beginning of the new millennium, a paradigm extension in the field can be observed, with the first scientific considerations on how game theory can be used for security. Although the situation between an attacker and a defender being the most natural incarnation of non-cooperative competition, it comes somewhat as a surprise that it took until the new millennium for the first scientific work on game theory applied to security. Ever since then, interest in the field has grown rapidly, and game theory and decision theory have become a systematic and well-proven powerful fundament of today's security research. Indeed, while conventional security aims at preventing an anticipated set of forbidden actions that make up the respective security model, game theory and decision theory take a different and more economic viewpoint: Security is not the absence of threats, but the point where attacking a system has become more expensive than not attacking. Starting from a game and decision theoretic root thus achieves the most elegant form of security, by analyzing and creating incentives to actively encourage honest behavior rather than preventing maliciousness. At the same time, the economic approach to security is essential as it parallels the evolution of today's attackers. Cybercrime has grown into a full-featured economy, maintaining black markets, supply chains, and widely resembling an illegal counterpart of the official software market. Traditional security remains an important fundament for tackling the issue from below, but game- and decision theory offer the top-down view by adopting the economic and strategic view of the attackers too, and as such complements purely technological security means.

The optimum is, of course, achieved when both routes are taken toward meeting in the middle, and this is what the GameSec conference series initiated in 2010 in Berlin, Germany. It brings together internationally recognized researchers from the security field, optimization, economics, and statistics, to discuss challenges and advance solutions to contemporary security issues. Following the success of this first scientific event

of its kind, subsequent conferences were organized in College Park Maryland (USA, 2011), Budapest (Hungary, 2012), Fort Worth Texas (USA, 2013), Los Angeles (USA, 2014), London (UK, 2015), New York (USA, 2016), and this year in Vienna, Austria, during October 23–25.

In all these years, GameSec has showcased a continuously increasing number of novel, high-quality theoretical and practical contributions to address issues like privacy, trust, infrastructure security, green security, and many more, and densely connected a scientific community of experts all over the globe and from various fields of computer science, economics, and mathematics, under the common goal of security. This year continued this tradition, and we are proud to present a new set of high-quality scientific contributions to advance security. The program of GameSec 2017 featured 28 full papers, selected from a total of 71 submissions, based on three reviews per paper. Submissions were received from all over the world, which underpins the global relevance of security and the methods pursued by the community. In addition, a special track on “Data-Centric Models and Approaches” was introduced in recognition of the problem of gathering and analyzing data about security incidents. Companies and security agencies may be reluctant in releasing such information to protect their reputation or the targets of attack. The special track’s focus was thus on gathering data and building models from it, and as such contributed to closing this gap between theory and practice.

We would like to thank the Austrian Institute of Technology for hosting this year’s event, and we also thank Springer for its continuous support of the conference series, by publishing this book as part of the *Lecture Notes in Computer Science* (LNCS) series. We hope that you enjoy reading as much as we enjoyed compiling this volume. Let us together take this step toward the next level of security!

October 2017

Stefan Rass
Bo An
Christopher Kiekintveld
Stefan Schauer
Fei Fang

Decision and Game Theory for Security

8th International Conference, GameSec 2017, Vienna,
Austria, October 23-25, 2017, Proceedings

Rass, S.; An, B.; Kiekintveld, C.; Fang, F.; Schauer, S.
(Eds.)

2017, XI, 534 p. 137 illus., Softcover

ISBN: 978-3-319-68710-0