J Comput Virol (2007) 2:241–242
DOI 10.1007/s11416-006-0034-9

FOREWORD

Foreword

Published online: 1 February 2007

The current challenges in computer security are closely intertwined. Various manifestations of security incidents—whether classical viruses, pernicious flash-worms,"script-kiddie" 's dabbling in hacking or stealthy "trojan horse" malware—involve closely interrelated sorts of "intrusion technology". In order to effectively counter these heterogeneous threats, security mechanisms should combine state-of-the-art protection techniques against various kinds of malicious activity. Moreover, significant synergies can be gained by comparative analysis and cross-application of different security mechanisms. In this special issue, it is a pleasure for us to present selected papers from the 3rd International Conference on Detection of Intrusions and Malware & Vulnerability Accessment (DIMVA), held in July 2006 in Berlin, Germany, which exemplify the potential benefits of a scientific dialogue between major branches of computer security.

Since its inception in 2004, DIMVA provides an academic forum for presentation and discussion of novel, mature research in three crucial areas of computer security: intrusion detection, malware detection, and vulnerability assessment. The main focus of DIMVA is thus on reactive methods of computer security, in contrast to proactive mechanisms such as firewalls and secure communication. Due to the fundamental lag between the time when a new vulnerability is discovered and a preventive mechanism gets in place, these three fields are a significant part of a good security concept. Despite much prior work, both in academia and industry, new attacks are developed at a brisk pace and constantly challenge existing technology.

The main objectives of DIMVA are to foster scientific exchange in the international security community and to facilitate the dialogue between academics and practitioners. DIMVA has been conceived and is supported by the German Informatics Society (GI). It is organized by GI's special interest group Security Intrusion Detection and Response (SIDAR). Each year the conference features a dynamic 2-day scientific program; exciting invited talks; active participation of academic, commercial, and governmental institutions, and, last but not the least, an informal, productive atmosphere.

The papers published in this special issue underwent a stringent review process. The initial submissions to DIMVA were reviewed by an internationally recognized program committee, the acceptance rate being less than 30%. Authors of accepted contributions to DIMVA were invited to submit extended versions of their papers to the this special issue. These submissions were further reviewed by at least one reviewer from the DIMVA program committee and at least one reviewer chosen by the editorial board. The three papers selected as a result of this process constitute novel and significant contributions to computer security literature.

We would like to thank all the authors who spent significant amount of time preparing their manuscripts

E. Filiol (✉)
Ecole Sypérieure et d'Application des Transmissions,
DEASR/Laboratoire de Virologie et de Cryptologie,
Rennes, France

R. Büschkes
TWG AG, Essen, Germany

P. Laskov
Fraunhofer Institut FIRST IDA,
Berlin, Germany

for the conference and for this special issue, as well as the reviewers whose diligent work was instrumental in securing the high scientific level of the contributions. We hope that the papers included in this issue will provide valuable insights to scientists as well as practitioners, and will contribute to further progress in such a vital field as computer security.

Roland Büschkes and Pavel Laskov, Guest Editors;
Eric Filiol, Editor-in-Chief.