J Comput Virol (2006) 2:1–2
DOI 10.1007/s11416-006-0019-8

FOREWORD

Foreword

Vlasti Broucek · Eric Filiol · Paul Turner

Published online: 30 June 2006
© Springer-Verlag France 2006

Addressing technical, organisational and socio-legal issues arising in the era of the 'wireless web' presents significant challenges. This is particularly the case, as awareness of the interrelatedness of these issues highlights the critical need for approaches that effectively balance requirements for network security, individual privacy and legally admissible digital evidence.

In this special issue, it is a pleasure to be able to present selected papers from the 15 th Annual EICAR Conference 2006 (www.eicar.org) held in Hamburg, Germany (April 29 – May 2, 2006). EICAR continues to build its international reputation as a high quality institute that successfully bridges industry, government and academia. As the selected papers below illustrate, this year's conference entitled 'Security in the Mobile and Networked World' was no exception to this tradition. Experts from industry, government, military, law enforcement, academia, research and end-users came together to share information, insights and knowledge on new research, development and commercialisation in the areas of malware and computer viruses, intrusion detection and prevention and socio-legal issues related to network security, e-forensics and computer crime. The continuing success of EICAR bears witness to the recognition amongst participants of the importance and benefit of encouraging interaction and collaboration between industry and academic experts from within the public and private sectors. Indeed, as digital technologies become evermore pervasive in society and reliance on digital information grows, the need for better integrated socio-technical solutions has become even more urgent and important.

The papers presented in this special issue neatly illustrate the diversity of perspectives and approaches being explored at both theoretical and practical levels. Taken as a whole, the papers also clearly reveal the on-going challenges arising from convergence and clash amongst these different streams of research and development. More promisingly, however, they also illustrate that the benefits of bringing research from these different domains together enable the commencement of the difficult task of moving towards the generation of more coherent integrated responses to the challenges faced.

Broucek and Turner's paper opens this special issue by revisiting research conducted over the last decade in forensic computing domain. Whilst calling for greater multi-disciplinary collaboration the authors acknowledge the factors that continue to impede progress in this regard. As a consequence, they outline a methodological approach to generate data that they anticipate will improve the possibility of calibrated responses that more effectively and coherently balance the interests for security, privacy and legal admissibility. Ford and Gordon also adopt a high-level conceptual approach in their analysis of on-going discussions and definitions of computer crime that they view as creating confusion amongst academics, industry experts and governments. Following a re-definition of terms, the authors' present two case studies to illustrate the role of crime-ware and offer some observations on the role of cognition in the process of cyber-crime. These first two papers provide

V. Broucek · P. Turner
University of Tasmania, School of Informations Systems,
Tasmania, Australia
e-mail: Vlasti.Broucek@utas.edu.au
e-mail: Paul.Turner@utas.edu.au

E. Filiol (✉)
Laboratoire de Virologie et de Cryptologie,
Ecole Supérieure et d'Application des Transmissions, France
e-mail: efiliol@esat.terre.defense.gouv.fr

an interesting conceptual background for the remaining papers presented in this special issue that variously explore different aspects of some of the challenges faced in network intrusion detection, malware, anti-virus research and end-to-end security.

Tripp's paper explores a novel approach for string matching for high speed Intrusion Detection Systems (IDS) drawing on a finite state machine approach. This approach advocates the use of a set of finite state machines each working on a single byte of the data input. The paper illustrates Tripp's hardware design for a parallel string matching engine built for implementation in a Xilinx Field Programmable Gate Array and tested by simulation. Following an exploration of problems with commercial malware scanners black-box analysis, Filiol's paper presents a new model of malware detection pattern based on Boolean functions. This paper also describes a combinatorial, probabilistic malware pattern scanning scheme that limits black-box analysis and can only be bypassed where there is collusion between a number of malware copycats.

Josse's paper makes a useful contribution in relation to the criteria that can be used to assess the effectiveness of anti-virus products. A protection profile for assisting software manufacturers to design anti-virus products in accordance with a common criteria standard is advocated and a number of tests that can be carried out to validate the security requirements presented. Josse suggests that use of a protection profile and the specification of tests is a valuable basis for measuring the effectiveness of anti-virus products. Bayer, Kirda and Kruegel's paper presents TTAnalyze, a tool for dynamically analysing the behaviour of Windows executables. This tool runs binaries in an unmodified Windows environment and the authors argue that this leads to excellent emulation accuracy and makes the TTAnalyze tool ideal for quickly understanding the behaviour of an unknown malware.

Aycock, DeGraaf and Jacobson's paper presents a new method of anti-disassembly based on cryptographic hash functions which is portable, hard to analyse and can be used to target particular computers or users. They suggest that the obscured code is not available in any analysable form, even an encrypted form, until it successfully runs and that they have been able to empirically validate their results. The authors then proceed to examine possible countermeasures for this basic anti-disassembly scheme, as well as variants scaled to use massive computational power.

Kayayurt and Tuglular's paper explores the end-to-end security protocol Transport Layer Security Protocol (TLS) with mobile devices for ensuring maintainability and extensibility. The authors then examine cryptographic operations via the use of the Bouncy Castle Cryptography Package. Their implementation has been tested with a variety of cases and they argue that the object oriented architecture of this proposed end-to-end security protocol implementation makes the replacement of this library with another cryptography package easier.

The papers presented in this special issue illustrate the on-going challenges arising from the convergence and clash of different streams of research, development and commercialisation and support the argument for open forums and discussion amongst representatives from industry, government, military, law enforcement, academia, research and end-users.

Finally, we would like to thank all the authors who spent significant time preparing their manuscripts for the conference as well as for this special issue. Please enjoy the papers. We look forward to many more submissions to the journal as well as to the EICAR2007 conference.