J Comput Virol (2007) 3:63–64
DOI 10.1007/s11416-007-0053-1

Foreword

Vlasti Broucek · Paul Turner

Published online: 25 April 2007

In recent years EICAR has emerged as one of the few internationally recognised institutes that successfully bring together experts from industry, government and academia to examine technical, organisational and socio-legal issues surrounding network security, malware, ICT security management, digital privacy and electronic evidence.

This special issue presents academic papers originally submitted and accepted for presentation at the EICAR 2007 conference. These papers cover a broad range of issues from on-going technical issues in detecting and identifying malware including new types of code, worms and rootkits; through analysis and response to bot-like activities; to hacker profiling, support for improved information assurance processes and consideration of privacy issues in mobile service environments. This interesting mix of topics illustrates the utility and importance of the forum EICAR provides. Ensuring that the latest information and knowledge on these diverse issues are presented together provokes new and innovative thinking on how to respond to their points of connection and inter-relatedness. By stimulating thinking across discourses on malware and computer viruses, intrusion detection and prevention and socio-legal issues related to network security, information assurance and computer crime, recognition of the need for more integrated solutions is highlighted.

Filiol and Josse's paper opens this special issue with a statistical model of malware detection revealing how this points to the possibility for the development of undetectable malware. Building on research by Chess and White (2000) they demonstrate how existing detection techniques can be statistically modelled and precise definition of false-positive and non-detection is presented. They conclude their paper by presenting a statistical variant of Cohen's (1986) undecidability results of virus detection. Developing some of these ideas Filiol's paper illustrates a new class of codes (potentially malicious) called k-ary codes. Instead of containing the whole instructions composing the program's action, these type of codes are composed of *k* distinct parts (each containing a subset of the instructions) which constitute a partition of the entire code. As a result, each part cannot be detected by anti-malware programs from conventional program code. Filiol proceeds to present a formalisation of these codes using Boolean functions and presents detailed taxonomy. The paper concludes that besides a huge number of beneficial applications using k-ary codes (e.g. protection against software piracy), these codes represent a potentially huge risk in terms of the generation of new malware. According to Filiol's experiments, existing antivirus technologies are totally inefficient at detecting those codes since the detection has to face combinatorial problems that cannot be solved in an amount of time that is compatible with most commercially available antivirus software.

This research on the dangers of undetectable malware provide an interesting context for the next four papers in this special issue looking at problems associated with worm propagation and evaluation, bots and rootkit detection. Avlonitis et al. present a new spatial stochastic model of worm propagation by incorporating non-uniformities within interacting subnets. The authors argue that efficient monitoring strategies can be deployed based on the results of random scan strategies and local preference scan worms. Ondi and Ford in their paper on metrics for worm and anti-worm measures argue that there exist no meaningful metrics by which one can quantitatively compare the effectiveness of different protection paradigms. They present several possible metrics for measuring worm spread and countermeasure effectiveness and highlight that the 'correct' metric for comparative

V. Broucek (✉) · P. Turner
School of Information Systems, University of Tasmania,
Hobart, Australia
e-mail: Vlasti.Broucek@utas.edu.au

purposes will vary depending on the goal of the defender. They conclude by discussing what changes induced by worm design or countermeasures are actually meaningful in the real world.

In Vinoo and Nitin's paper the focus is also on practical measures but here in relation to counter-measures against bots on organisational internal networks. The authors argue that organisations should not rely only on their security vendor's protection against this type of malware but rather should develop their own intelligence gathering methods to improve protection. More specifically, the authors propose setting up an IRC honeypot on internal networks to function as an early warning system against bot-like activities. They argue that such a system can be set up with minimal effort and investment but can provide significant assistance in the fight against these types of malware. Related to this concern with internal organisational security problems is Josse's paper on rootkit detection which presents a secure engine specifically designed for the security analyst to analyse rootkits and related programs that interact deeply with operating systems, including AV, FW and HIPS. This paper presents 'state-of-the-art' algorithms for rootkit detection and reviews forensic techniques and advanced heuristics. Interestingly the paper uses a human analysis framework to conduct comparative analysis of security aspects of security products like AV, FW, HIPS and deals with the robustness of their driver stack and the quality of their implementation. The paper also proposes a reliable system for automatically gaining information about a rootkit and its interaction with the OS executive (stealth native API hooking and kernel objects integrity checking). Tripp's paper also examines the problem of detection but here in relation to a hardware design for use within network intrusion detection systems. The paper describes an optimised finite state automata based hardware design for implementing high speed regular expression matching. The approach presented addresses the conventional memory problem faced by standard Field Programmable Gate Arrays (FPGA). Tripp explains how using an existing 'packed array' style of table based automata implementation can be enhanced by adding a form of input compression to group together characters. The paper then outlines the hardware design and the results of simulation testing.

The final five papers of this special issue explore different dimensions of the human side of security, information assurance and privacy. Preuss, Furnell and Papadaki explore the potential of criminal profiling for combating hacking based on the results of German case studies. The paper presents the commonalities and differences in motive and modus operandi (MO) identified in the twelve case studies provided by the Bundeskriminalamt (German Federal Criminal Police Office). The authors conclude that a basic principle that can be identified is that despite differing motivations hackers tend to take the path of least resistance in making their attacks. Overill and Coles-Kemp argue for the need for a specialised facilitation role in information security risk assessment. The authors suggest that without this role the possibility of generating outputs that are meaningful for businesses to act upon are much reduced. Their point of view is supported by reference to field observations of certification audits of a number of organisations combined with the standard models of BSI/ISO/IEC and FRAAP. Gattiker examines the issues of information assurance and education in the light of the Bologna Declaration.[1] The paper focuses on European undergraduate and graduate education efforts in the area of computer security. Following an analysis of the issues the paper summarizes key findings and practical implications for European information assurance processes into the future. Educational issues are also a concern in Linfeng and Helenius's paper on the use of anti-phishing toolbars. Based on a usability evaluation the authors highlight issues and propose mechanisms for improvement particularly in relation to the client side of the available tools. The final paper of this special issue examines the privacy risks arising from the development of new context aware mobile services. Jorns, Jung and Quirchmayr argue that without the implementation of proper privacy protection contextual information processed by third party application providers may present privacy risks to end users. To address this problem the authors present a novel service architecture which fosters the development of innovative applications but contains an underlying privacy enhancing mechanism that is based on the notion of pseudonyms. This service architecture is demonstrated through a transportation ticket application that supports location-tracking functionality.

The papers presented in this special issue highlight both the challenges and emerging solutions arising in response to the increasingly pervasive nature of the digital environment into every aspect of our lives. This special issue presents a strong argument in favour of more forums and discussions amongst experts from different disciplines and domains—a pathway that EICAR will continue to forge into the future. Finally, we would like to thank all the authors for the time and effort spent on preparing their manuscripts and we encourage and look forward to many more submissions to the journal and to EICAR 2008.

Vlasti Broucek & Paul Turner
Guest Editors

[1] See http://ec.europa.eu/education/policies/educ/bologna/bologna.pdf.