J Comput Virol (2008) 4:1–3
DOI 10.1007/s11416-007-0073-x

FOREWORD

Foreword

Philippe Biondi · Eric Filiol

In the last 5 years, the *Symposium sur la Sécurité des Systèmes d'Information et de Communication*[1] (SSTIC) has emerged as the first French international conference devoted to all aspects of ICT security: network and system security, malware, cryptography …. Every year the SSTIC attract more than 400 attendees from all the French speaking language countries. More significantly the SSTIC successfully bring together experts from industry (50%), government (20%) and academia (30%).

While the technical level has been very high from the first edition in 2003, the 2007 edition has reached the level that only a few renowned international conferences succeed to achieve. From outstanding surveys to high-level, new technical and/or technical contributions, most of the aspects of computer security have been covered with respect to substance and form. Unfortunately, all those papers were presented in French and scientific existence is only possible in the English language. That is the reason why we decided to select the best technical papers for publication in the Journal in Computer Virology. The present issue as well as the next issue presents the most outstanding contributions to the SSTIC 2007 edition.

These papers cover a broad range of issues which all relates to computer virology in a way or another. This interesting mix of topics illustrates the utility and importance of the forum SSTIC 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 interrelatedness.

The research on the dangers of security vulnerabilities provides an interesting context for the first four papers in this special issue looking at problems associated with vulnerability formalisation, automated identification and exploitation by attackers. Allamigeon and Hymans' paper is an outstanding paper dealing with a very critical issue for IT security and which is of high concern as far as the protection against malware is concerned. Many malwares operates by exploiting software flaws or vulnerabilities. Consequently, detecting such weaknesses is of the highest importance in order to prevent the spread of malicious codes. Allamigeon and Hymans' paper presents an efficient formalisation of overflow detection as well as an efficient and sound technique for practical detection up to the underlying complexity bounds, using abstract interpretation. This paper has won the SSTIC 2007 Best Technical Paper Prize. In the second paper, Butti and Tinnès consider the hot issue of efficiently detecting critical 802.11 driver security vulnerabilities. They exposed in a very interesting and illustrative way how to detect such flaws through the technique of fuzzing. They focus on the design and implementation of a fully-featured 802.11 fuzzer that enabled them to detect several critical implementation bugs that could be potentially exploitable by attackers. In order to give a deeper knowledge on the critical risk attached to 802.11 driver security, the authors detail the successful exploitation of the first 802.11 remote kernel stack overflow under Linux (madwifi driver). Then Duverger's paper exhaustively studies the problem of kernel exploits under Linux. The impact of such exploits become dramatic at the

P. Biondi
EADS Innovation Works, Suresnes, France
e-mail: phil@secdev.org

E. Filiol (✉)
Army Signals Academy,
Virology and Cryptology Lab, Rennes, France
e-mail: efiliol@esat.terre.defense.gouv.fr

[1] Literally translated by Symposium on the Security of Technologies of Information and Communications.

kernel level since they offer a complete control to the successful attacker over the whole system. The author first present the essential difference between user and kernel level regarding exploits used by attackers. Then, the author suggests a global point of view around major kernel data structures that help handling processes under Linux 2.6 on IA-32 architecture. Finally, considering the application level vulnerabilities, Feil and Nyffenegger's paper proposes an exhaustive survey of existing *Cross-Site Request Forgery* attacks and presents new techniques which can be used by potential intruders to make them more effective. This paper in particular describes a new technique that preserves the malicious code on the target system even after the browser window is closed. More interestingly, Feil and Nyffenegger are exposing the best solutions to prevent these attacks and to enable everyone (users, browser or Web applications developers, professionals in charge of IT security in an organization or a company) to prevent or manage this threat. The next paper could be also related to vulnerabilities issue since in many cases, the lack of password strength is generally far too neglected and underestimated. In this respect, Marechal's paper addresses the very interesting security issue of actual password security and strength. For most people, this issue seems to have little connection with malware. First, the evergrowing computing power of the target machines gives to malware huge computing capabilities that could be used to crack or perform exhaustive search of passwords and thus gain total control over the system. At last, malware can also collect protected password and send them to the remote attacker who can then brute-force them to connect to the compromised machine with a more privileges access. This paper surveys various techniques that have been used in public or privates tools in order to enhance the password cracking process. One of the main interest of this paper lies in the experimental results which are shown, comparing several implementations.

In the next issue, the next two papers will explore complementary aspects regarding the security at the memory level. Ruff's paper will present a comprehensive survey of all known "live" memory collection techniques on a Windows system, and freely available memory analysis tools. Ruff also will review the limitations and known anti-collection techniques that could be used to prevent memory from being analysed. The great interest of this paper is the detailed technical illustration of every techniques exposed, in particular drawn from past forensics challenges. While this paper is indeed mostly forensics-oriented, it nonetheless provides valuable information to malware analysts that are fighting against stealth rootkits. Live Memory collection can also be used directly by malware in order to collect sensitive data that could be used to enhance the attack. Duc and Keryell's paper will consider the opposite side of the memory security problem and will present a powerful computing hardware architecture, called CryptoPage, which implements memory encryption, memory integrity protection checking and information leakage protection. This architecture relies on strong cryptographic tools and represents an interesting solution to strongly limit many existing malware to operate at the memory level. Their paper shows that powerful solution can definitively prevent the spread of large classes of malware directly at the hardware level, provided that the computer industry makes the good technological choices.

The final three papers in the next issue will explore different aspects of ICT security which all have strong links with the malware issue. Malware document (whose the most known subset are the infamous macro viruses) are probably representing again a critical issue in a very near future, especially with the emergence of new document formats. In this respect, Lagadec's paper will present the security issues of both OpenDocument and Open XML file formats for office documents. Both of these formats suffer from many security issues, similar to previous Office formats but they also both of them introduce new viral risks including XML and ZIP obfuscation techniques that may be used to bypass anti-viruses. This paper significantly extends previous study on OpenOffice document security published in a previous issue of this Journal (de Drézigué et al., 2006). But the main interest of this paper lies on the fact that the author gives technical details to design efficient filters to greatly limit the spread of malicous Office documents. Analysing the attacker's behaviour is of the highest importance for the future defense capabilities and for developing a quick response ability. Alata et al.'s paper will address the issue of monitoring and better understanding the behavior of attackers evolving inside a compromised machine by means of high-interaction honeypots. However, whereas in classical honeypots observations are generally limited to the operations performed by the attackers on the honeypot itself, in the present paper the authors consider a dynamic, on-the-fly redirection mechanism of connections initiated from the honeypot towards remote machines, in order to monitor the attacker behaviour on his way across the different machines he has compromised. This mechanism gives the attacker the illusion that he is actually connected to a remote machine whereas he is redirected to another local honeypot.

In the last (but not least) paper, the problem of stealth and rootkit technology will be addressed. While rootkits are sometimes considered by some people as a promising technology for commercial applications, it represents before all tremendous risks that are likely to defeat existing detection capabilities. Lacombe et al.'s paper will deal with rootkit conception which is nowadays a very critical issue. The authors will show how these particular malicious codes are innovative comparing to usual malware. From that, they introduce a functional architecture for rootkits as well as some criteria to characterize a rootkit and thus, to qualify and assess

the different kinds of rootkits. In particular, they consider the communication between the attacker and his tool, and the induced interactions with the system. In order to provide a general view regarding the issue of rootkits, the authors present a rootkit paradigm that runs in kernel-mode under Linux and some new techniques that could be used by attackers to improve the stealth features of rootkits.

The papers presented in the present issue and in the next 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. Both these issues present a strong argument in favour of more forums and discussions amongst experts from different disciplines and domains—a pathway that SSTIC 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 SSTIC 2008.

We would also like to thank all the experts and researchers who have been involved in the review process. Their work and efficiency as well as their professionalism have greatly contributed to the high scientific quality of these two first 2008 issues. Finally, we would like to express our special thanks to Dr Daniel Bilar, from the Department of the Computer Science at the Wellesley College, Wellesley, USA for his help in correcting the English language of most of the present papers and having suggested valuable comments to some authors thus greatly helping them in finalizing their paper. He thus has contributed to the overall quality of those issues.