J Comput Virol (2007) 3:1–2
DOI 10.1007/s11416-007-0038-0

FOREWORD

Foreword

This special issue is devoted to the first international workshop on theory of computer viruses (TCV), which held on May 4th and 5th 2006 in Nancy at Loria. This workshop springs from meetings with E. Filiol and both of us. It became then clear that computer virology has strong theoretical computer science roots.

From an epistemological point of view, it is rightful to wonder why there are only a few theoretical studies while it is one of the important flaws in software engineering. However, this reason is not enough to justify a theoretical study. A stronger motivation comes from the necessity to have a better understanding of the viral mechanisms at a fundamental level in order to bring new answers to computer diseases. For this, we do think that theoretical computer science has a key role to play by developing an abstract computer virology that underpins these products and practices in virology.

Indeed, the common opinions is that computer virus defences is a matter of good engineering and of updated commercial anti-virus softwares. However, viruses have been plaguing our computers for 30 years. The workshop TCV is an attempt to build a bridge between engineering and theoretical computer science in the domain of computer virology.

What is behind the scene? Viruses are an inherent disease of computations because their existence is closely related to fascinating S. Kleene's (second) recursion Theorem and so computer viruses are unavoidable in a general and common programming environments. The seminal studies of F. Cohen and of L. Adleman lie both on S. Kleene's recursion Theorem. They thus represent classes of evolving viruses, consider their duplications, and how to protect a system against them. The main result is the undecidability of the detection of viruses.

A distinctive feature of viruses is self-replicating, and in fact a virus or a worm is a self-replicating entity. Here again, S. Kleene's recursion Theorem, but also works of von Neumann on self-reproduction, shed some new lights on nature of those computer infections. It also recalls us that the word "virus" is not only there to frighten people, but also to point out some analogies with biology which is well worth to explore. That is why, there was an invited talk on biological viruses by C. Finance of Nancy-University.

There are four papers, which were selected. P. Beaucamps and E. Filiol paper concerns program obfuscation. They begin by an insight discussion on Barak & al result, then they present several practical obfuscation methods. E. Filiol, G. Jacob and M. le Liard present a methodology to evaluate virus detection procedures, which are based on behavioural analysis. This work follows a previous work of E. Filiol on the evaluation of virus detection procedures based on signature recognition. Both papers can be seen as an evaluation framework of anti-virus softwares from a rigorous mathematical analysis.

The paper of B. Morin and L. Mé analyze the difference and the similarities of Intrusion Detection Systems and Virus Detection Systems. They establish that both domains suffers from a large gap between the practical approach and their theoretical counterpart. As was already mentioned by F. Cohen, self-replicating programs can have positive effects. R. State and O. Festor concentrate on the strengths of viral techniques and their limits in Network Management.

The workshop TCV would not have been possible without the support of Loria, of the university of Nancy, of the Région Lorraine, and of two French scientific projects, which are the project Virus (ARA SSIA) and the project QSL.

To conclude, we would like to insist on the fact that theoretical computer virology is a foundational challenge with

an exciting future, and we hope that conceptual concepts will migrate to security engineering. For these reasons, the second edition of the workshop TCV will hold at Loria in May 2007.

Guillaume Bonfante and Jean-Yves Marion

Nancy-Université, Loria

INPL-ENSMN