J Comput Virol (2005) 1: 2–3
DOI 10.1007/s11416-005-0001-x

EDITORIAL

Foreword

Published online: 7 October 2005

Launching a new research journal is not an easy project. Launching a journal devoted to computer virology is a big and stimulating challenge. The risk of misperception is always present and must be permanently kept in mind. The big question is: "Is it useful and safe to work on and publish information on such "hot topics", as malevolent people may use the knowledge to attack and harm networks and computers?" Well, answering this question is not easy, and there is no right or wrong answer. By way of comparison, the same question could be applied to research journals devoted to sensitive fields as organic chemistry, nuclear technology, genetics etc.... However, such scientific journals do exist.

But what is the bigger danger? Is to publish scientific results that might be used for harmful purposes, or to keep security professionals and "good people" ignorant of how the risk from viruses might evolve in the future ? Taking the first approach, the more common attitude, shows a lack of humility and insight. Defence by restricting knowledge has never worked in whatever field. Moreover, this attitude pre-supposes that only one person or research organisation will arrive at a particular scientific solution or result. The history of science has proved this hypothesis to be false, and recent computer security experience has done so on an almost daily basis. Some "bad guys" will inevitably manage to arrive at the same results and use the knowledge to attack others. The medicine is always worst than the disease. On the contrary, adopting the second approach gives a better chance to the defenders. By publishing research knowledge, the "bad guys" and "good boys" will be competing on the same level. Keeping such knowledge concentrated and available only to small groups of people has always proved to be a very dangerous practice. Published research may help users to keep a little bit ahead the risk itself.

The aim of the journal on computer virology is clearly and definitively to work for defence, not only in a reactive way – waiting for the next attack and learning from it to strengthen the protection – but also in the proactive way – imagining what the threat could be the future in order to beat attackers to it. However, this project is motivated by the following important rules and attitudes.

- Ethics. This is the most important one. The ultimate goal is to help people, computer security professionals, simple users, researchers etc., and not to help, in any way, the evil to spread and strengthen. All accepted papers will be evaluated according to this very important principle. This implies that any potential critical result, that may endanger computer security, will first be disclosed to computer security professionals before being made public. Otherwise, it would be a total negation of our motivation.
- Awareness and truth. There is no "forbidden knowledge". If a risk exists, it must be scientifically analysed and analysis made available to all, so that everyone has a clear and unbiased idea of the risk. Once again, ignorance is not a defence. Everyone must be involved in the protection and the defence.
- Independence and respect. The aim of the journal is to work for the general good and interest, not for only a few people. That means that no political consideration, in the broadest sense, or particular interest, except the purely scientific one, will be taken into consideration. Authors' opinions and perceptions will be respected, provided that they comply with the previous aspects. In particular, we will pay special attention to the requirement the each article's content must not violate any of the national laws in force in reviewers' countries.
- Quality. Submitted papers will be reviewed mainly on their inherent quality rather than only on their academic form. In other words, the spirit will be more important than the letter. New results, didactical approach, innovating approach etc. will be particularly appreciated. Once again, the deep motivation of the journal is to make protection progress in the quickest way.

We wish a great success to this journal and hope that many researchers and computer security professionals will be interested in submitting scientific or technical papers.

I would like to thank all the board members who have agreed to take part in this stimulating adventure and to be involved with the reviewing work, which is not an easy job. As the editor-in-chief, I am proud to have them as members

of what can be considered a “dream team”. Their help and involvement is invaluable.

Finally, I would like to thank the Springer-Verlag France team which made this project possible. All of its members have been very enthusiastic from the outset and have been totally involved since. Their help has no price. I would like also to thanks Vlasti Broucek and Paul Turner, from the University of Tasmania, Australia. It was a very good idea to propose to the journal that it should publish the best student paper(s) accepted for presentation at the EICAR Conference. It is precisely the sort of way to promote active research in the field of computer virology.

Eric Filiol
Ecole Supérieure et d’Application des Transmissions
Laboratoire de virologie et de cryptologie
B. P. 18
35998 Rennes – France
E-mail: Eric.Filiol@inria.fr