

19th EICAR Annual Conference

"ICT Security: Quo Vadis?"

Call for Papers

Submission deadlines: Peer reviewed papers due Other papers (non reviewed)	December 20th, 2009 December 13th, 2009
Acceptance notification to authors: Peer reviewed papers Other papers (non reviewed) – Initial selection Other papers (non reviewed) – Final selection	February 21st, 2010 December 22nd, 2009 January 31st, 2010
Final papers due	March 21st, 2010

The 19th Annual EICAR Conference to be held on **May 10th and May 11th 2010, with a pre-conference program on May 8th and 9th at the ESIEA Engineer School/Institute of Computer Science** in Paris, France.

The conference brings together experts from industry, government, military, law enforcement, academia, research and end-users to examine and discuss new research and development in anti-virus, malware, e-security, e-forensics, Information and Communications Technology (ICT) Management and legal aspects of the information technology.

While the EICAR conference traditionally covers all aspects of malicious code and the development of "anti" measures, the conference 2010 intends to go deeper also concentrate into the usability and issues related to independent testing of Anti-Virus (Malware) products and initiate reflexions on the worrying trends and evolution of ICT security and especially with respect to anti-malware world.

The AV world -- and more widely the computer security world-- is facing since a few years big challenges. BUT contrary to partially wrong feelings those challenges are not only coming from the bad guys: usually all those ugly actors who think to be intelligent or having some sort of power by distributing malware everywhere. While all the instances (the defenders, e.g. AV vendors, governments, researchers, IT experts...) involved in fighting those stupid and malevolent guys (the attackers), the motivations has begun to diverge substantially since a few months, in such a way that it not only becomes more difficult to make the difference between defenders and attackers but also finally the result is that finally the activity of the attackers is made easier: here precisely lie the new challenges that the EICAR 2010 conference has decided to address. Hence the main theme of the event: "**ICT Security – Quo Vadis?**" I would be tempting to use an equivalent formula: is the AV

world and the ICT world going mad? Two illustrative but worrying recent issues are militating in favour of considering this general conference theme.

The first one refers to AV evaluation – which will be addressed at EICAR 2010 as a one of the major topics. The situation is somehow worsening making that evaluation, from an independent, technical perspective more and more difficult not only from a technical point of view but also from a legal point of view. To realise how things are evolving, anyone can read AV software licence document (the one which nobody reads in fact): you will discover very strange and worrying things. Aside the classical academic and industry papers which will be presented, the two-day preconference program will propose tutorials, student/industry sessions around the topic of AV software and AV policy evaluation. Especially, we intend to offer and promote new tools and tutorials with respect to them that everyone could use to evaluate his own AV security and policy himself. It will be the occasion to recall that the only independent way to test an AV without using any malware – a critical issue in itself – was, and still is, the EICAR test file. We will propose, especially for the industry, a tutorial on that file and on new open forthcoming tools that will be disclosed and presented during EICAR 2010. Those tools are directly inspired by the EICAR test file but go far ahead to address the new challenges and needs. So it should be a good reason to attend the conference.

The second case is the very worrying evolution of the use of malware for so-called “investigation” and “copyright protection” purposes. A number of western countries have officially announced that malware-like technologies (e.g. Trojan horses for the most part) are now authorized to enforce the law. More worrying is the use for commercial purposes (e.g. to fight piracy). The question is: is the remedy not worse than the disease? Such issues should be addressed at the EICAR 2010 conference. BUT the main consequence of that evolution lies in the way the AV community will react and what it will decide: if AV vendors accept not to detect those malware-like technologies they are going to lose their credibility and legitimacy very quickly, making precisely the game of the bad guys. Why? Because they implicitly would accept the fact that there are such things as good and bad Trojan Horses. What is quite impossible to manage from a technical point of view, would be a nightmare from a legal/society/privacy point of view. In fact, they are just about to open the Pandora box? That is the reason why we have decided at EICAR 2010 to also address these kinds of topics. The ICT world has now invaded our society and personal lives and we cannot remain blind to its evolution.

To summarize, the rapid evolution of technologies requires the adaptation of human behaviour and in consequence leads to new needs for laws and regulations of direct relevance to the users. The EICAR conference 2010 will therefore concentrate on legal aspects and user liability.

This call for scientific/technical/ industry papers invites therefore the submission of full papers and abstracts on one or more topics devoted to malware and anti-malware technologies, which may include but are not restricted to:

- Malicious code and its side effects
- Viruses and worms
- Spyware and phishing
- Vulnerabilities
- Vulnerability reporting
- e-Crime and e-Forensics
- Cyber Terrorism
- Legal aspects of ICT and in particular :
 - Legal liability for security flaws in Europe.
 - Enforcement of IT-Security.
 - Differences of legal regimes and their impact on IT-security.
 - Technical versus legal governance of IT-security.
 - The human factor in IT-security and its control by law.
 - International security threats and national legal regimes.
 - Legal, Privacy and Social Issues of ICT Security
 - National-, European- and international law
 - Ethical, moral and political issues on writing/developing and using malicious code
 - Ethical, moral and political issues on malware detection limitations
 - Legal aspects of security product evaluation and testing
- Identity Management
- ICT Security and Policy Management
- Intrusion Detection and Prevention
- Emerging technologies (WiFi, RFID, biometrics...) with respect to malware.
- User awareness and education
- Malicious cryptography and steganography
- AV evaluation and testing
 - New methods/new tools
 - Secure evaluation/testing methodologies (e.g. not requiring to use malware)
 - Theoretical foundations of antivirus and evaluation.

The conference committee is seeking submissions of papers for oral presentation at the conference in two major categories:

- **Peer reviewed papers** – these papers will be selected on basis of blind peer review by members of the program committee and other independent reviewers (where necessary). Case studies, research in progress and full research papers including theoretical papers will be considered for the inclusion in the conference program. There is no definitive word limit for the submissions; however, it is anticipated that submissions will be between 3500 and 5500 words. The program committee will not accept research proposals for submission to the conference.
- **Other papers** – these papers will not be peer reviewed. However, due to the considerable interest in the conference in the previous years, these papers will also be reviewed and selected for acceptance by the program committee. This category covers corporate papers, best practices, new technologies, policy issues etc and the conference

committee are eager to obtain submissions from industry, government and other sectors for this category. **However, marketing papers will not be accepted for the conference.**

The conference committee can accept only a limited number of papers in each category and the acceptance ratio in the past few years was about 30-40% of submitted papers only. All accepted papers will be published in electronic form on the Conference CD-ROM and will be published in the printed version of the EICAR Conference Proceedings (book with ISBN). The best papers will be published in a special issue of the *Journal in Computer Virology*, a research journal published by Springer Verlag.

The best "Student" Paper will be awarded by the conference committee.

Deadlines and forms of submission:

Authors wishing to submit papers for peer review category and acceptance for the conference should submit full papers by no later than **December 20th, 2009**. These papers will be blind peer reviewed by at least two reviewers. Authors of accepted papers will be notified by **February 21st, 2010**.

Authors wishing to submit other papers should submit at least 300-word abstract by no later than **December 13th, 2009** for selection by the program committee. A first selection process will be performed to check whether the proposed papers fit to the EICAR conference policy and topics. A pre-notification will occur no later than **December 22nd, 2009**. Authors of selected papers will be notified by **January 31st, 2010**.

All submissions will be handled electronically and the review/acceptance process will be conducted anonymously by the conference committee:

- Academic papers should be submitted via on-line submission and review system available at <http://conference.eicar.org/> in portable document format (PDF), rich text format (RTF) or Microsoft Word 97 or newer format (DOC). All information enabling the identification of authors must be removed from the submissions. Papers in LaTeX format are particularly welcome.
- Non-academic abstracts should be submitted as plain text via the web-based form that will be available on <http://conference.eicar.org/>

Final camera ready papers (**accepted in RTF, DOC or preferably LaTeX format**) in both paper categories must be submitted by **March 21st, 2010**. The EICAR conference uses simplified APA5 format for papers published in the proceedings (description, MS-Word (.DOT), RTF and LaTeX templates are available at <http://conference.eicar.org/>).

Conference Fee Waiver

The conference fee will be waived for one presenter for each accepted paper.

EICAR Students Fund

Limited conference attendance incentives (e.g. subsidised rate for accommodation at the conference venue) may be offered from the newly founded EICAR Students Fund for student papers. Eligibility for funds is subject to EICAR Board resolution upon recommendation from the Program Chair based on individual written request.

Student and Industry pre-conference program

On May 8th- 9th, 2010, tutorials with technical and/or practical contents devoted to the main topic of the conference (Anti-malware evaluation, new Eicar testing tools) will be organized. They are primarily open to students but depending on the number of registrations, anyone can attend.

Tentative Invited Talks

Doctor Jurgen Kraus (the "European father" of modern computer virology, who defended his PhD thesis in 1980. Unfortunately, this thesis was never published for obscure reasons and has been translated and published in 2009 only, in the Journal in Computer Virology. It is a major contribution to computer science which addresses all the modern issues of computer virology both on a theoretical and practical level) will give the opening keynote talk.

Conference Program Committee

The following, provisional list of distinguished researchers and/or practitioners (listed alphabetically) have confirmed their membership of the conference program committee to date:

- Fred Arbogast (CSRRT-LU, Luxembourg)
- Dr John Aycok (University of Calgary, Canada)
- David Bénichou (Investigation judge, Department of Justice, France)
- Vlasti Broucek (University of Tasmania, Australia)
- Andreas Clementi (AV-Comparatives e.V., Germany)
- Professor Hervé Debar (Telecom Sud Paris, France)
- Dr. Werner Degenhardt (LMU Universität München, Germany)
- Professor Eric Filiol (**Program Chair**) (ESAT/ESIEA, France)
- Professor Richard Ford (Florida Institute of Technology, USA)
- Professor Nikolaus Forgo (Leibniz University Hannover, Germany)
- Professor Steven Furnell (University of Plymouth, UK)
- Professor William (Bill) Hafner (Nova Southeastern University, USA)
- Dr Sylvia Kierkegaard (President of International Association of IT Lawyers, Denmark)
- Dr Cédric Lauradoux (Inria Grenoble, France)
- Dr Ferenc Leitold (Veszprog Ltd, Hungary)
- Professor Grant Malcolm (University of Liverpool, UK)
- Professor Yves Pouillet (University Notre-Dame, Namur, Belgium)
- Professor Gerald Quirchmayr (University of Vienna, Austria)
- Dr Frédéric Raynal (Sogeti/Security Labs, France)
- Sebastian Rohr (Accessec gmbh, Germany)
- Professor Paul Turner (University of Tasmania, Australia)
- Professor Andrew Walenstein (University of Louisiana, USA)
- Dr Stefano Zanero (Politecnico di Milano, Italy)