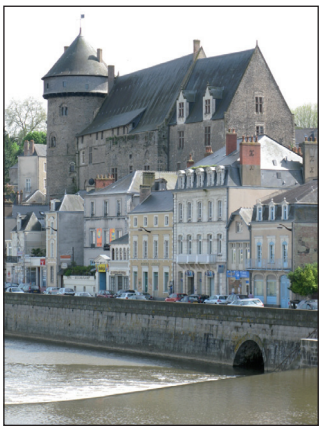
CONFERENCE REPORT

EICAR 2008, C'ÉTAIT MERVEILLEUX!

Eddy Willems
Kaspersky Lab and EICAR, Belgium



This year EICAR held its 17th annual conference at the conference centre Les Ondines in Laval, France. After financial problems forced the organizers to cancel the conference in 2007, it was a brave decision to go ahead and plan for an event in 2008. Laval may seem an unusual choice for the location of an international conference in its come-back year, but the excellent conference facilities on offer at Les Ondines were enough to offset any disadvantage of the venue being off the beaten track.

This year's conference theme was 'IT security is facing a paradigm shift – new threats and more subtle methods of attack require different approaches and solutions'. The theme draws attention to the issues arising from the reality of an 'anytime, anywhere' web and an increasingly invisible enemy.

The conference was opened by Professor Dr Nikolaus Forgo from the University of Hannover and Vienna, who gave a keynote speech about prosecution and law enforcement in the context of IT security solutions development. Professor Forgo will lead a new legal advisory board that EICAR is setting up in response to the increasing role of legal issues in the context of IT.

Professor Forgo's presentation made it clear that even gathering information from a network is not as easy, from a legal point of view, as most of us believe. I think that many of us in the audience would think twice even about using some of our sniffer tools again.

Next, two of Professor Forgo's students presented a deep look at the criminalization of hacker tools in the new German law and compared it with other European legal systems.

After the best conference lunch I've had in my 17 years of attending conferences, the real agenda kicked off with presentations split between an industry papers track and an academic paper track.

François Paget from *McAfee* presented an interesting view of the malware problems related to virtual worlds such as *WoW* and *Second Life*. Meanwhile, in the other track Vanja Svajcer and Boris Lau of *Sophos* looked into virtual machine detection in malware using a dynamic-static tracing system. Richard Ford outlined a danger theory-based artificial immune system for the MANET (mobile ad hoc networks) environment. He showed how a simple reputation system can be improved in this environment by considering the experiences of similar systems.

Next up, 'Simulating malware with MAlSim', presented by Rafal Leszczyna, Igor Nai Fovino and Marcelo Masera from the European Commission, was quite a controversial talk about a mobile agent framework used to address security assessments based on simulation of attacks against the systems – something like a combination of penetration and malware testing on real systems. In my opinion these researchers should exercise caution as their work treads a precarious line and could easily be misinterpreted or misused. Fraser Howard of *Sophos* rounded off the first day's sessions with a nice, deep overview of Web 2.0-based attacks.

The gala dinner that evening will be remembered by most of the attendees as being tastier even than the aforementioned lunch – you simply can't beat the real France for good food and wine! The dinner was held at the old Laval castle, a magnificent mediaeval palace in the centre of the picturesque town.

The second day of the conference opened with a realistic and deep view of Win32.Ntldrbot (Rustock.C) given by Boris Sharov of *Doctor Web*. Afterwards, Mario Vuksan from *Bit9* described the use of a whitelisting approach to improve the quality of security software and effect a radical transformation of anti-malware and HIPS products. He also demonstrated the power of this system in tracking down new types of malicious software. Finally, a talk by Andrei Gherman of *Avira* about the latest botnets trends gave a very good view of the real problem and described several different monitoring solutions.

With more than 26 papers and talks it is not possible to provide a summary of them all, so I urge readers to look them up on the EICAR website: http://www.eicar.org/conference/.

This year's EICAR conference was a fresh start and I firmly believe that EICAR is running once again in the right direction with some interesting new projects on the horizon. The quality of the conference papers was excellent – just ask any of the people who attended. Let's hope for some even more interesting presentations next year, when the conference moves to Germany, taking place either in Dresden or in Berlin.