CONFERENCE REPORT

EICAR 2006 IN A NUTSHELL

Eddy Willems
NOXS and EICAR, Belgium

The 15th annual EICAR conference took place last month in the German town of Hamburg. Set on Hamburg's harbour front with stunning views, the Hotel Hafen Hamburg provided an ideal setting for the conference.

The event started with two professional clinics, during which Vlasti Broucek demonstrated some 'Art of data visualisation' and Elizabeth Bates and Bill Haffner explained the 'Security and privacy risks in biometric deployments'.

The clinics took place in the morning, and after lunch the conference was opened officially with a welcome address from Rainer Fahs and a keynote address given by Sarah Gordon. Sarah's address reminded me of the reason I have been coming to this conference for 15 years: security knowledge lies in the details. A panel discussion came next in the schedule. Hosted by David Perry and Sarah Gordon, the discussion, entitled 'Birds of a feather flock together', gave a nice overview of the various anti-malware groups in the industry – like CARO, AVIEN, WildList, etc.

After this, the conference split into a well-planned two-stream programme, featuring some highly accomplished presenters.

I have always found it hard to decide which session to attend in these multiple-stream conferences, and this year it was even harder than before. If you know how to split yourself in two, please share it with me! The following are some of the highlights of the sessions I attended.

Two spam papers grabbed my attention. The first, by Christopher Lueg, Jeff Huang and Michael Twidale of the Universities of Tasmania and Illinois, explained nicely where spam comes from. The second spam paper – and probably the most controversial – was written by John Aycock and Nathan Friess of the University of Calgary. During their presentation they described some new spamming techniques that have not (yet) been seen in the wild. Let's hope spammers do not start to use these techniques.

The second day started with some definitions of crimeware given by Richard Ford (*Florida Inst. Technology*) and Sarah Gordon (*Symantec*) and spyware given by Jason Bruce (*Sophos*) and Martin Overton (*IBM*). Larry Bridwell (*iCSA Labs*) and Josh Harriman (*Symantec*) showed us some problems relating to spyware testing. Tony Lee and Jigar Mody of *Microsoft* proposed a behaviour-based automated classification method based on distance measure and machine learning.

A controversial paper by Eric Filiol (Army Signal Academy), entitled 'Malware pattern scanning schemes against black box analysis', was rather too theoretical for me, but it proved interesting for the more mathematically-minded delegates.

More practical and accessible to all delegates were the papers 'Enlisting the end-user', given by Jeannette Jarvis (*Boeing*); 'Pharming: a real threat?', given by David Sancho and François Maillard (*Trend Micro*); 'Unpacking – a hybrid approach', given by Vanja Svajcer and Samir Mody (*Sophos*) and 'Evolution from a Honeypot to a distributed honey net', given by Oliver Auerbach (*Avira*).

This year's gala dinner was unusual in that, for the first time in four years, there wasn't a new virus outbreak to talk about. There seemed to be a trend emerging, with the release of Sober.P on the first day of last year's EICAR conference, the appearance of Sasser during the 2004 conference and Bugbear.B during the 2003 conference – but thankfully this year's event was virus-free.

The third day of the conference is dedicated to non-academic papers – which tend to be more commercially oriented. Nevertheless, the final day started with one of the most interesting keynote speeches I have heard for a long time: Professor Klaus Brunnstein (University of Hamburg) with 'Inherent technical risks will lead information and knowledge societies into a risk society'.

Most people assume that everything ends after the three official conference days – but not so. In what we call a post-conference programme two task forces (Awareness and Content Security) meet to discuss and agree on real practical goals and objectives. Our RFID task force has already provided a guideline for implementing RFID technology.

The EICAR 2006 agenda was interesting and varied, and the papers were the best I have seen at an EICAR conference so far. Planning has already begun for the 2007 conference and details will be announced shortly at http://www.eicar.org/. The organizers are looking at Budapest and Barcelona as possible locations – but of course other suggestions are always welcome.

As one of the founding members of EICAR, I remember the first constitutional EICAR conference in Brussels in 1991. A lot has happened, changed and improved during those 15 years. And I fully expect this to continue over the next 15 years.