CONFERENCE REPORT

The Second International Virus Bulletin Conference

It hardly seems a batting of the proverbial eye-lid since the inaugural *Virus Bulletin* conference, and now the second *VB* event is over! This year's conference was larger than the first, with 207 delegates from twenty countries converging on the beautiful (and wet!) city of Edinburgh. This made *VB '92* the biggest ever 'virus gathering' to date.

The first event of the conference was the speakers' dinner which began, as all good things should, in the bar. This gave the speakers the chance to sample the *Balmoral Hotel's* fine range of whisky, and to meet a spectral apparition who proved a source of speculation throughout the evening. Many voiced their opinions as to who *exactly* this ghostly companion was, but in order to protect the guilty and the innocent, none of their suggestions will be repeated here.

Conference Themes

As last year, there were continuing complaints from the delegates that researchers are too obsessed with collecting and classifying new viruses. Many picture these researchers collecting viruses like stamps and trading them like school-boys in the playground. Given that there are now well over 1500 known viruses, with fewer than a hundred normally seen 'in the wild', this does seem a reasonable criticism. Jim Bates summed it up neatly: 'What are we doing to help the *user*?' - a question which everyone involved in the anti-virus community should continually ask themselves.

Users care about *detection* and *recovery*, not about esoteric debates as to the relative virtues of various strains of the Jerusalem virus. Outside the carefully controlled world of virus research labs the information that users need about a virus includes:

➤ What has it done to my computer?

➤ Has it done any damage?

➤ How do I get *rid* of it?

Speakers Corner. (Clockwise from back left) Joe Norman (*Inmos Ltd*, UK), Jonathon Lettvin (*Lotus Development Corporation*, USA), Dr Jan Hruska (*Sophos*, UK), Dominic Storey (*Novell*, UK), Steve White (*IBM T J Watson Research Centre*, USA), Fridrik Skulason (*University of Iceland*, Iceland), Christoph Fischer (*University of Karlsruhe*, Germany), Roger Riordan (*Cybec Pty Ltd*, Australia), Paul Faulkner (*Barclays Bank plc*, UK), Edward Wilding (*Virus Bulletin*, UK), Jim Bates (*Bates Associates*, UK), Vesselin Bontchev (*Virus Test Centre*, Germany), Dennis Steinauer (*NIST*, USA), David Ferbrache (*Defence Research Agency*, UK), Chris Johnson (*University of Texas*, USA), Mick Wigfield (*Centre-file Ltd*., UK), Barbara Cookson (*Titmus, Sainer & Webb*, UK), Noel Bonczoszek (*Computer Crime Unit*, UK), Rod Parkin (*Midland Bank plc*, UK), Ferenc Leitold (*Hunix Ltd.*, Hungary), Jeff Kephart (*IBM T J Watson Research Centre*, USA).

This divergence of emphasis between the parties concerned was already apparent a year ago (see *VB*, December 91 pp. 2 - 5). Reasonable and realistic demands must be dealt with for the good of the industry, which must not forget that it exists to serve the end-user.

The onslaught of new viruses has led many people to develop automatic methods of analysis. This year saw the presentation of several new ideas aimed at accelerating the task of classifying and disassembling new specimens, either by cross-correlation with other viruses, or by a variety of virus analysis languages. Most virus researchers are insomniacs, and are happiest burrowing away into the early hours, their veins awash with caffeine, their eyes scrutinising a vintage copy of DEBUG. These researchers are unworldly, eccentric creatures, and are all individual in their approach; whether automating virus analysis will be universally acclaimed is open to debate.

The long arm of the law is now beginning to feel the collars of the perpetrators of 'high tech' crimes such as virus writing. With the introduction of the *Computer Misuse Act 1990*, computer users within the UK are no longer defenceless against the questionable activities of 'Cracker Jack' and his ilk, though as yet the implications of this new act are not well known. Barbara Cookson, a solicitor from *Titmus Sainer & Webb*, guided the delegates on a useful tour through the complexities of the Act. The SysOps of virus exchange bulletin boards would do well to acquaint themselves with Section 3 of the Act: they are committing an offence which could lead to a five-year jail sentence.

Cookson stressed the need for reliable reporting of virus incidents in order to assist the police with their enquiries. Most people would report a break-in to the police even if nothing were stolen - the same ethical rule should apply to incidents of computer hacking and virus outbreaks.

It is hardly surprising that many people are still unaware of the laws concerning computers and computer crimes, as there has been little publicity given to the *Computer Misuse Act*. In a survey conducted by *Computer Weekly* dozens of respondents did not know of the Act's existence, including two party parliamentary candidates who had worked in the IT industry for most of their lives. Given the serious nature of these issues it is important that the legal position is clear to all - in order for the law to have a deterrent effect upon potential virus writers they must be aware that they can face imprisonment and hefty fines.

VB '92 was not all work, work, work. Here, Mike Lunt of the Home Office receives a round of applause from delegates on his 28th wedding anniversary

Sadly, even though virus exchange bulletin boards are now illegal in the UK, this legislation cannot hope to be effective until there is some international cooperation to prevent the exchange of virus code. Until then, any such board may remain open in areas not covered by this or similar laws.

A Problem Shared...

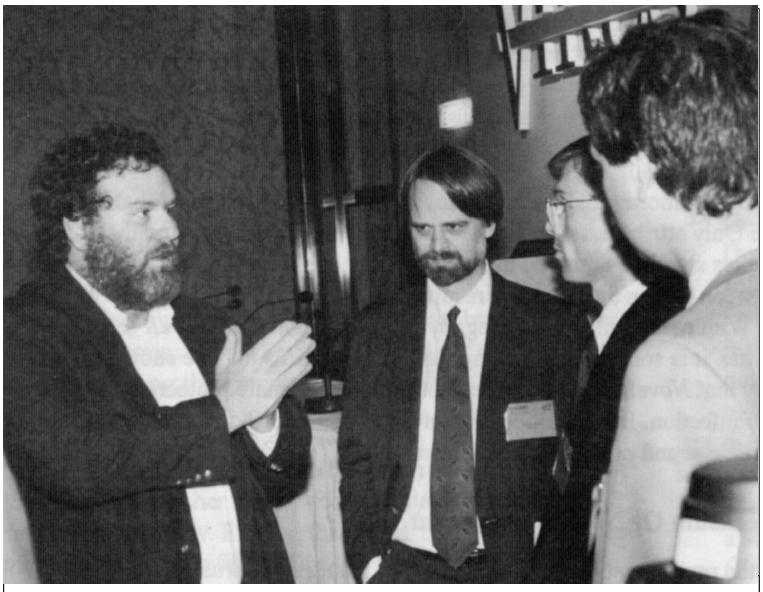
In an effort to stop the cut-throat competitiveness which is seen throughout the MS-DOS anti-virus community Steve White of *IBM* suggested pooling resources and sharing virus disassemblies. Such a suggestion is enough to cause apoplexy for the chieftains of the warring tribes, as they dance around their respective totem poles. In order to stop the exchange system being dominated by any single group there need to be rules. As White put it: 'You're worried about the rules, right? Well let's make the rules simple: the rules are that there are no rules'.

This apolitical approach has been used by the Macintosh community for some time with astonishing success, and White sees no reason why it could not be even more successful for the MS-DOS virus community. Apart from the animosity within the research community itself, the fundamental problem is persuading people to forget their short term financial concerns and see things from a more long-term perspective - sharing code means less research time for all. In order to benefit the community as a whole, *Virus*

Bulletin has always published its search strings for viruses and will do so for the foreseeable future. In the long term, cooperation is the only way forward. In the meantime, however, there seems little hope of an end to the internecine warfare being waged in the PC anti-virus community - only time will tell.

...Is A Problem Doubled

One of the most controversial aspects of the conference this year was the publication by *IBM* of statistics and calculations concerning the rate of spread of computer viruses. Until the publication of this paper, the seminal work in this field was by Dr Peter Tippett, who claimed that the prevalence of computer viruses would grow exponentially, until approximately 20% of all computers were infected. On first inspection this seems unrealistic, as it does not take into account any interaction by the user. In the last year we have seen a measurable decrease in the susceptibility of many computers to infection, due to increased awareness on the part of the user, widespread dissemination of anti-virus software, and centralised reporting and response. *IBM*'s statistics show that the growth in the number of incidents is linear rather than exponential, and that this increase is approximately 0.5 incidents per 1000 PCs per year. The wildly inaccurate estimates of the prevalence of the Michelangelo virus have underlined the need for caution in extrapolating infection statistics from a complex data sample. In 1991 *Dataquest* conducted a survey of computer virus prevalence, by putting a number of questions to those responsible for computer virus protection in large organisations. It was the results from that survey which seemed to indicate that the computer virus problem was very large indeed. Kephart claims that the original data samples used by *Dataquest* did not represent the true picture due to an unclear wording on their survey forms. When considering statistics of this kind it is important to remember the prejudices and vested interests that may be concealed within the results. Both *Dataquest* and Dr Tippett are sponsored by firms who produce anti-virus software and *IBM*, which manufactures PCs, may have an interest in belittling the seriousness of the virus problem.



Can man speak without moving his arms? Fred Cohen, hands firmly glued together, attempts to communicate to Steve White and Jeff Kephart the error of their ways.

In the wake of the Michelangelo 'frenzy', a scientific approach is urgently needed. The question of how these figures should be estimated led to a heated debate after the talk between Fred Cohen and Kephart and White of *IBM*, which spilled over into the lunch break - it seems that the formulation of such an epidemiology will prove a time-consuming and highly contentious process (see photo!).

Another welcome set of statistics came from Noel Bonczoszek who presented prevalence data collected by Scotland Yard's *Computer Crime Unit*. This is the first time that the *CCU* has chosen to present this information publicly. The data shows that while there have not been a large number of reports to the *CCU*, the sites which *have* been hit have been hit hard - for example, many of the machines reported as being infected with the Spanish Telecom virus (more than 750) were all involved in the same incident.

Once within an organisation, a virus can often spread like wildfire, contained only by the barriers which go to make up departments or companies. The situation is rather like the threat of being hit by a car; it is unlikely to happen to you, but unpleasant if it does. It is therefore vital that adequate precautions are taken - this means a frequently updated, well written scanner, and preferably some kind of integrity checker. The statistics show that nearly all incidents are caused by a handful of viruses. Therefore the 'scanner A detects 200 more viruses than scanner B' argument should be summarily dismissed when considering the relative merits of anti-virus software.

Home grown can be best

It is often educational to see how a corporate anti-virus policy is put together. The conference was lucky to have two extremely good talks on this subject; one by Paul Faulkner of *Barclays Bank PLC*, and one by Mick Wigfield of *Centre-file Ltd*, a computer

services company. At long last, it seems, large companies are becoming less reluctant to discuss the issue of virus protection publicly.

Barclays has taken a novel approach by developing its own proprietary virus scanner and disk error detection system, known as *DEDS+*. When *Barclays* first became aware of the computer virus problem it decided that no contemporary software package provided either the reliability or the support that they required, and that nobody was prepared to offer a global licence which was affordable. It was a relatively simple step to decide to develop its own diagnostic software. As the number of viruses spirals, however, the difficulty in maintaining *DEDS+* will increase. It is an open question whether *Barclays* would take the same decision today. This move towards scanning for viruses at the same time as checking the disk's integrity seems to be a logical one, as both tackle different aspects of the same problem: data loss.

Centre-file Ltd first became painfully aware of the virus threat when it was hit hard by the Cascade virus. However, rather than using a purely 'home-brewed' solution, a combination of commercial products and 'in-house' software is deployed in order to provide the desired level of cover. Two commercial scanners are used within the company - one to scan every new disk which enters a PC, the other by the engineers and technicians when they are called upon to investigate suspected virus situations. This is analogous to a professional bodyguard and his selection of weapons - a man-stopping revolver supported by a rapid fire automatic. In addition to scanning disks, a fast home-grown checksummer is used to look for any alterations to files on the disk. This is used once a day, and once a week a more thorough check is done. This regime has led to extremely effective results - since these anti-virus defences were set up in 1989 *Centre-file* has stopped all viruses 'at the door'.

Some day all viruses will be built this way!
Vesselin Bontchev outlines his chilling vision of the future.

Execute Only?

At the conference this year, much of the discussion centred around the security of *Novell* networks, and as is common in this industry, there was further lively debate as to the propagation of computer viruses on networked systems. The first speaker of the conference, Fred Cohen, discussed how the access rights of a file inhibited or enabled virus propagation under *Novell NetWare*. This had been done experimentally, by setting up a server running *NetWare* and allowing various viruses to attempt to infect it under controlled conditions. Cohen states that the complexity of the *Novell* file Rights system mean that it is possible for a seemingly insignificant change to lead to counter-intuitive results. He has identified by trial and error the Rights and Attributes necessary to secure *NetWare*. Supervisor, Modify, Access Control, and Create must be disabled. Additionally, Write must be disabled *or* Read Only must be enabled! By far the most surprising result Cohen presented was that setting the attributes of a file to Execute Only does not stop the spread of companion viruses, even though the supervisor himself cannot scan the contents of files labelled as Execute Only.

The following morning Dominic Storey from *Novell UK* claimed that the Execute Only attribute *does* provide protection against viruses and that all executables should be marked as Execute Only and Read Only. The contradiction between Cohen and Storey's results means that, quite simply, one of them is wrong. With many millions of Megabytes of data stored on *Novell* servers worldwide, it is somewhat alarming that Cohen claims to have shown experimentally that *Novell's* solution does not provide adequate protection from the threat of infection. It is incumbent upon *Novell* to resolve this conflict quickly and provide sound protection guidelines.

To Checksum Or Not To Checksum?

One of the preoccupations of companies producing anti-virus software is the growing number of polymorphic viruses which are relatively difficult to detect using virus-specific software. Traditional wisdom dictates that some form of integrity checking method be used. However, since many viruses now aim to avoid detection by memory-resident monitors and scanners, it is inevitable that

viruses specifically designed to avoid detection by integrity checkers will also be seen. Vesselin Bontchev's paper dealt with the issue of subversion; more specifically, he outlined techniques by which integrity checkers can be undermined. He concluded that there are many ways in which a virus can avoid detection by a badly-written integrity checker. The important thing to note is that it is impossible, if using a well-written integrity checker, for a file to become infected without the change being registered. The vital things to remember are:

- The integrity checking software and its checksums should always be stored on a floppy disk.
- The PC should always be booted from a write-protected system disk.

In an interesting *Gedanke* Bontchev proposed a model for a virus and considered how it would replicate, slipping past the watchful eye of an integrity checking program. Against a 'slow' infector such as this virus, an integrity checking program does not provide any protection. As the operating system *itself* modifies or creates a file, a slow infector strikes, infecting the target file. While an integrity checking program will alert the user that this file has changed this will be of no surprise, as the host file is either new to the disk or has been altered for some perfectly legitimate purpose. While Bontchev is correct in his assertion that a 'perfect' virus of this type would be extremely difficult to detect, its description bears little resemblance to the bug-ridden scraps of code which make up the vast majority of viruses encountered to date. The apocalypse is nigh, says Bontchev, but the rest of the world waits to be convinced.

False Positives

The greatest mirth was caused by accident. One of the acts booked to entertain the delegates during the Gala Dinner was a troupe of jugglers; flaming torches comprised its grand finale. Unfortunately, the hotel management had neglected to deactivate the smoke detectors in the ballroom...

Within minutes, the hotel foyer was filled with partially clad guests, rudely awakened from their slumber by the clamour of the fire alarms. This is a perfect example of a false positive. [Among their number was one Nigel Kennedy - he of the violin and 'right on' accent. What a shame! Ed.].

Acknowledgements, as ever, to the organisational acumen of Petra Duffield and her team, who kept the conference running so smoothly. Finally, thanks are due to the delegates who took the time to fill in the assessment forms at the conference - their comments have been noted. The venue for the *Third International Virus Bulletin Conference* in 1993 has yet to be announced. The programme will contain some radical departures - watch this space.

NEWS

Magazine Mayhem - That *PCW* Review!

The October edition of the UK magazine *Personal Computer World* carried a review of anti-virus software by computer journalist Ken Mann. The results of the review caused momentary astonishment to many seasoned observers, as it called into doubt the effectiveness of some of the best known packages in the industry!

Fifteen different packages were run on supposedly infected files in an attempt to ascertain their detection efficiency. The results showed that four of the products (*Norton Anti-Virus, Dr Solomon's Anti-virus Toolkit, IDS Virus-Pro* and *Certus NOVI*) did not detect *any* of the test 'viruses' at all. *PCW* is (or was!) a well-respected publication in the UK and these 'revelations' have sparked a minor controversy amongst the virologists and their customers.

The virus test set consisted of four viruses (Friday 13th, Alabama, Kennedy and MIX 1A). The selection of viruses is bizarre - the test set is far too small to conduct an accuracy test and it is unrepresentative. While it is not strictly necessary to test a scanner against many hundreds of different viruses, any sensible review should try to select samples which are either particularly hard to detect (such as those which are self-modifying) or particularly prevalent in the real world. The *PCW* review did neither and this was its most obvious error.

The reason that four of the packages did not identify any of the viruses is more subtle. The viruses were described by the reviewer as 'dead', that is, they were not capable of replicating. Exactly how they were disabled is not known, but the wording of the article and the results of the test indicate that the initial JMP or CALL instruction of the virus had been modified so that it no longer executed the remainder of itself. Due to the ever-increasing number of viruses, anti-virus software producers are continually looking for ways to speed up their scanners. One way to do this is to examine the first instruction of a file, and then selectively search areas pointed to by the initial jump for different viruses. This means that if the start of a program has been modified (and the virus completely disabled) a scanner which searches for viruses in this manner will obviously fail to detect *any* viral remnants. Since the virus cannot execute, the correct result a scanner should return is that all the files were clean. Clearly, the *PCW* test was fundamentally flawed.

The danger of product reviews in the popular press is that there is a dearth of specialist knowledge to spot mistakes such as these in the review procedure.