INSIGHT

Research and Other Hobbies

Many people have become 'names' in the anti-virus world, for research and for programming: the former category has Professor Klaus Brunnstein as a member. Head of Hamburg University's Virus Test Centre (VTC), his career has seen controversy and success. Brunnstein is one of the 'old guard' of computing: his first exposure to the technology was during his university studies (Hamburg 1957-1962), where he used IBM 7047s and Telefunken TR-4/TR-440s in his dissertation.

'Programs were written in Algol and, for the IBM 7047, translated into Fortran,' he said. 'We had to operate the computer ourselves, from booting (working in single process mode) to diagnosing and curing errors. Despite these limitations, they were great times, where users did not interrupt my work with hardware, software, and systems!'

A Career in Computing

Brunnstein's professional life began in 1964, when he took up a post at the German Electron Accelerator computer centre, working with minicomputers and mainframes. In 1967, he gave his first lectures on the operating systems of mainframes and minicomputers. That year, he also developed a Library Information System with one of the first SDI (Selected Dissemination of Information) devices.

1969/70 saw his secondment to a group founded for the purpose of preparing the ground for Hamburg University's Informatik-Fakultät (IT Faculty): Brunnstein's responsibility was to develop the library and computer centre. In 1973, he became the first European professor for the application of Information Technology, concentrating on education.

In the 1970s, Brunnstein changed the direction of his research to business applications for Data Protection and Security. Since 1983, he has been chairman of the Advisory Committee for Europe's first Backup Computer Centre.

A Virus Outbreak

It was not until 1987, when Jerusalem appeared in the wild, that Brunnstein became aware of the threats posed by viruses. The following year, his minicomputer laboratory was transformed into the Virus Test Centre (VTC).

At the VTC, reverse engineering at every level is studied: viruses, explained Brunnstein, are an ideal medium for this purpose, being complex but not impossible. Researcher Vesselin Bontchev spent several years studying at the VTC, as did Morton Swimmer. Brunnstein has also been teaching a two-year course on Computer and Communication Security, which was inaugurated in 1989: the course currently running has eighty students.

The Faculty for Information Technology includes the VTC and the Net Test Centre, where network safeguards are tested under various operating systems (*Novell*, *Windows NT*, *OS/2*, etc). Although the VTC has well-established relationships with many anti-virus software developers, it is not funded by any of them, as it is part of Hamburg University: 'We don't get *any* funding for our anti-virus work,' explained Brunnstein. 'Our funds come from the university,' and, in a rueful aside: 'And are consequently rather meagre.'

CARO as Colleagues

Klaus Brunnstein is one of the founder members of the *Computer Anti-Virus Research Organisation* (*CARO*). This group was initially 'a little community aware of the threats and aiming at public information more than at business'.

'Most *CAROts* had research and academic interests,' he said, 'even when Alan (Solomon) and Fridrik (Skulason) began to develop their products. When Vesselin joined the VTC in 1990, he and Fridrik became active via email (Virus-L was indeed sometimes Vesselin-L!), attracting many new friends.

'CARO's international membership means new threats can be immediately analysed,' he added. 'Moreover, virus detection methodology has improved through discussion, including awareness of user needs and demands of testers. Vesselin in particular has contributed significantly to testing methodology during his studies.'

The Virus Threat

Brunnstein sees viruses as a threat essentially only on PCs and on the Amiga: less than 50 Macintosh viruses are known, and only a few UNIX viruses (none of which are in the wild).

'Virus authors write (for the most part, they merely modify) viruses as an experiment in program and system behaviour on related platforms,' commented Brunnstein. 'Very few viruses are written with the intent to damage.'

Fledgling authors, he feels, do not realise how damaging their creations might be. Only when they mature do they understand the ethical (and in some countries legal) implications of viruses and their potential for havoc.

'As long as schools and universities do not educate students on the malicious impact of what they are doing,' asserted Brunnstein, 'the wave of viruses will continue. The race between virus authors and anti-virus producers will continue. New methods will be more difficult to understand and detect. Macro viruses, which work on a higher software platform, are a new threat. Such viruses have been predicted and demonstrated by Professor Harold Highland as early as 1989/1990, but even today their malicious potential has not been realised.'

There are also dangerous developments outside the virus field, in Brunnstein's view. He feels in particular that Trojan horses and worms will be a more serious problem, especially to enterprise LANS and WANS.

'This threat will grow,' he continued, 'when software to install and autonomously distribute intelligent agents is more broadly available. Even when such languages (e.g. Java) have inherent security features, misuse will not be prevented as new threats exploit safety rather than security.'

Brunnstein forecasts that viruses will become less important, despite their increasing numbers, and that network threats will grow significantly, eventually dominating in enterprise and public networks. The only anti-virus producers he envisages surviving this change are those which enhance their products to become anti-malware packages.

'The advent of complex self-hiding methods,' Brunnstein said, 'is part of the game virus authors play with anti-virus developers. Creating a polymorphic engine does not need a genius – reverse-engineering is more difficult. Few producers seem to analyse code: developing and testing algorithmic detection is more time-intense and costly than extracting scan strings. Heuristics can help detect new viruses and variants with similarities, but is inherently less reliable than traditional methods.'

On the Legal Front

Brunnstein does not believe that present legislation can cope with the problems posed by viruses: 'Laws often require prerequisites which cannot be proven,' he explained. 'In German computer sabotage and espionage laws, for example, deliberate intent is required, which is not easily provable when virus authors argue that their intent was purely educational.

'Second,' he continued, 'Lawyers and judges rarely understand technical terms or have a basic understanding of computers. Third, PCs and most networks have no inherent auditing which stores traces of malware; prosecutors (even if capable) always have difficulties proving damage.

Man in the Mirror

A controversial article, Rächer im Datennetz (Network Avengers) appeared in the German magazine *Der Spiegel* (German for 'mirror') some time ago, accusing Brunnstein of being little more than a virus profiteer. The article quoted him, amongst other things, as having said that the Michelangelo virus would destroy hundreds of thousands of PCs.

Brunnstein's official response was that the article was so full of misconceptions and false allegations that he was not willing to comment. He recalled numerous confrontations with the journalist in question: in fact, not only was Brunnstein never asked if the quotes were correct, but there was no contact between the two when the article was written: 'I decided,' he said simply, 'that non-reaction was best.'

Klaus Brunnstein, academic and researcher, is constantly seeking new challenges.

Outside the VTC

Although Brunnstein plans to remain at the Virus Test Centre and to carry on with his work in education, he does have other areas of interest, both personally and professionally. His main area of work at the moment is analysing incidents on computer and net-based systems, from hacking and malicious software to real-time systems such as electronic flight control and medical systems.

He is at present writing two books; one on the methodologies of incident analysis and response, another based on his university courses. Together with colleagues, his work on the ethical and legal aspects of information technology is ongoing, and he is also currently analysing potential net threats from intelligent agents.

Although currently not active politically, Brunnstein has also been a Member of the German Parliament, and leader of a German coalition party. His political activities include a campaign to stop the Census Law of 1983: the term 'informational self-determination' was taken by the courts from the action of 'Brunnstein et al against the Federal Republic of Germany'. Brunnstein in fact feels that some of the controversies may relate to different political positions on the social implications of IT.

Sailing is another of his passions: he and his wife Gunda ('A garden architect responsible for some English-style parks in Hamburg,' said Brunnstein. 'She is interested in computing, though garden architects don't use computers much presently!') are often to be found on their 48-foot Newfoundland schooner. 'Based on the Bluenose's lines, but rigged as a staysail schooner,' he explained.

Brunnstein professes to enjoy life with his family, of all of whom he is manifestly proud: 'My daughter Anke is just now working on her doctorate in ornithology, specialising in rare birds, and my son Jochen is studying Economics, including computer methods and applications, here at Hamburg University.'

Music and literature take up much of the rest of his leisure time, and what remains is spent with the family's animals; two dogs and a horse.

Klaus Brunnstein has strong views on many subjects: whether controversial or conservative, these views will doubtless continue to be aired, and to provide, as before, ever more topics for discussion.