

INSIGHT

Hyppönen, that Data Fellow

Megan Palfrey

Like most people in the computer world, Mikko Hyppönen has been around computers almost as long as he can remember. PCs and the Hyppönen family are inextricably intertwined: even before his birth, Hyppönen's mother was working at the *Finland State Computing Centre*. She brought her two sons up in the world of IT, ensuring a computer was always among their toys.

This led to careers in computing for both: the two brothers work for the same company, *Data Fellows*, international publishers and distributors of the renowned and respected *F-Prot Professional*. Mikko is Technical Support Manager, active on the anti-virus side, and his brother is involved with the company's next big project, *'Vineyard'*, a *Windows*-based groupware product.

Catching the Bug

Hyppönen went from school to the *Institute of Information Technology* in Helsinki, although he still worked part-time at *Data Fellows*. The company's only contact with the anti-virus scene at that time was in a training capacity. 'Anti-virus products were around, but most companies hadn't started developing them. This was circa 1990; use of this software hadn't become widespread,' said Hyppönen. 'I wasn't interested in viruses at all at that stage.'

Data Fellows' CEO, Risto Siilasmaa, however, was thinking about viruses and anti-virus software. Many users were asking the company which product they should buy to protect their system, but no-one had an answer. Products which were available lacked good Finnish technical support, or indeed any Finnish technical support at all. The first step towards solving this was to contact Fridrik Skulason, author of *F-Prot*, and technical editor of *Virus Bulletin*.

'So, the company went anti-virus, but I still wasn't interested. In fact, I couldn't have cared less!' Hyppönen viewed viruses as 'fashionable'; something with which everyone was busying himself. He had no desire to jump on the bandwagon. This attitude was not to last much longer: in late 1990, a virus called Omega appeared in Finland. Hyppönen was hooked.

'I decided to study it,' said Hyppönen. 'It interested me. At that time I knew practically nothing about PC assembly language, which you need to understand to analyse viruses.' So he started to learn, and was soon analysing and disassembling viruses, teaching himself how to extract searchstrings, garnering as much information about viruses and anti-virus software as he could, even dedicating time to research into international marketing of anti-virus products.

Despite this, he sees himself more as a technician than a salesman: 'Most technical people are not marketers. It's the same for me: I don't like marketing hype. I don't like to sell, but it's something I have to do every now and then. Although I don't do much of the actual coding, a lot is done at *Data Fellows*; we create the *Windows* and *OS/2* versions, while Fridrik [Skulason] takes care of the DOS side. I do analyses and co-ordinate the international support. If someone calls with a problem, I try to analyse what's going on. This sort of role reflects what I like to do; check out what's happening, keep up to date in the virus field.'

The World Outside

Viruses are not an all-consuming passion for Hyppönen, however; electronic communication and the *Internet* are other areas of active interest. *Data Fellows* has been developing a *World Wide Web* site relating to virus information which aims to make available to users all the most recent data about viruses held in their laboratories.

He sees advances in technological understanding also in the user community: 'The *Internet* has been around for over ten years now, but until recently there was a wealth of information which nobody who wasn't a computer expert could use. Now, I could take anyone off the street, and if he knows how to use a mouse, he could probably get around the information and forget himself at the terminal for four or five hours, going from one side of the world to another.'

Research and Anti-Research

The issue of contact with virus authors is a complex one for Hyppönen, and problematic for any anti-virus researcher: it is all too easy to destroy one's reputation by being in contact with virus authors while investigating their actions. He views this sort of research as valid nonetheless, albeit a dilemma of the same proportion as whether to buy the now-infamous CD-ROM of viruses released by Mark Ludwig.

There is, affirms Hyppönen, no reason to write a virus, and he believes most people concur with this viewpoint. 'I've created a virus with NuKE's Virus Creation Laboratory (VCL); I believe all researchers have - but why write a real virus? The only reason for an anti-virus researcher to do that would be testing - but it's easy to do that with a program that doesn't self-replicate. Personally, I don't find the idea of writing viruses at all interesting; I've never had the urge, or even thought about doing that.'

The Art of Writing

The topic of virus writers is one with which Hyppönen is familiar, having researched in-depth who is writing viruses and exactly what they are doing. He has been contacted via

the IRC (*Internet Relay Chat*) by several well-known virus-writers; however, his conclusion was that such contact is not helpful in the long run: 'It is quite surprising that some virus-writers seem to be very nice persons when you talk to them, but you are always aware that they are doing something wrong, writing viruses. They were probably just bluffing...'

Many people involved in anti-virus research believe the only way to prevent virus authors writing viruses is through re-education, but Hyppönen takes a slightly harder line: 'Yes, education is important, but they have to take responsibility for what they do. They should be punished - I'm pretty sure that it's not enough just to tell them that they did the wrong thing and to start to re-educate them. They are breaking the law, or at least acting irresponsibly, and every single one of them knows that.'

He finds it almost incomprehensible that someone could write a virus just for fun, without being fully aware of the implications: 'I think everybody knows it's bad.'

There is some small comfort in this story, however: 'I think that most virus writers just come onto the scene, write a couple of viruses and get out: it's fairly random. There are very few long-term virus authors - those who make a career of it. Sooner or later, most of them get bored, and leave.'

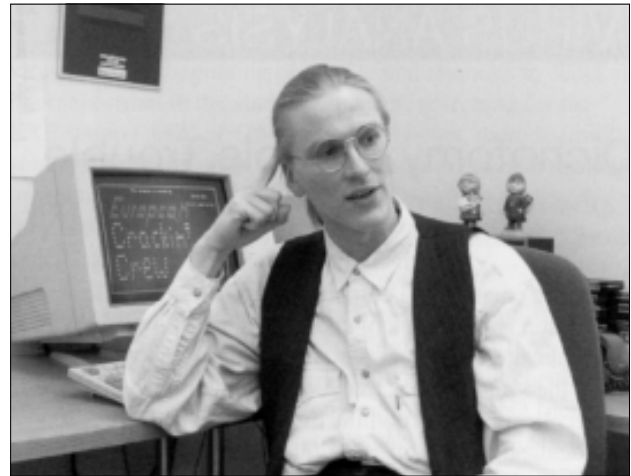
The Shape of Things to Come

It surprises Hyppönen that new products are still appearing on the market: 'I think most scanners will be overcome by the number of viruses, and I'm not just talking about not being able to keep up with new viruses. I'm talking about practical things, like the fact that products need more disk and memory space; some of them can't be run from low-density floppies anymore. Products are getting much too big, much too slow. The corporate side will start to look for alternatives, and I believe this will be integrity checking.'

He is convinced that all anti-virus products will eventually incorporate integrity checking; that people will be able to eradicate a virus without knowing what they had. 'This will become a problem, however, because often, you would still want to know what the virus was; for example, if you had a data diddler on your system, you would definitely need to know that. You can't be satisfied with generic detection.'

'We will see integrity checkers integrated with scanners that would find only the most important viruses. Virus-specific scanners and integrity checkers will work together, but the scanner will do a much smaller job.' He sees the industry going towards localization, relying more on local technical support as opposed to a centralized department which may not be able to help regional crises.

'When a new virus is found in Finland, a competent local support team will be able to find a remedy right away; companies which do not have local representatives will have problems - 24 hours is a long time when your network is



Hyppönen takes a tough line on virus writers: 'education is important, but they [virus writers] have to take responsibility for what they do. They should be punished...'

down. A week is too long; you start to format your hard drives and go from zero instead of waiting. What companies need now and will need more in the future is local technical support to respond to viruses, and local tools to create a solution to a problem.'

As a corollary, Hyppönen sees the number of anti-virus researchers increasing, as the need grows for localized and specialized support. Nevertheless, he does not see viruses themselves as the main threat - the biggest direct risk to a computer is the user himself doing something incorrectly.

'The problem with viruses will in fact diminish: the more complicated a system, the more different problems it has; for example, reliability. The worst problem with a computer system is that people are so dependent on them that when something does go wrong, they have what you might call a "denial of service" attack.'

Hyppönen's opinion is that as long as there are programmable computers, there will be viruses; and that viruses are just one more problem with computing in general, to be accepted as a business risk and dealt with accordingly.

The Flip Side

Hyppönen's life has always been linked with computers: even now, his wife runs her own computer business, specialising in teaching and consultancy - 'That's why I married her!' he joked. 'We were both workaholics; at the office around the clock, completely computer-minded - in fact, we arranged our first date over a modem. Now we try to separate our work from our private life, though.'

The future is certain: 'I will stay with viruses; I believe there is a job for anti-virus researchers. If everybody stopped writing viruses now, there would be work for the next ten to fifteen years, anyway. But I don't see them stopping. And while they're still writing, I'll still be disassembling. Where they are, we'll be right behind them!'