# INTERVIEW

## Open All Hours

*The OpenAntiVirus Project was started two years ago to address what was seen by its founders as a serious lack of open-source solutions in the anti-virus field. The intention was to build and nurture a network of AV developers within the open source community by providing the relevant resources for communication and project management.* VB *spoke to co-founder Rainer Link and developer Kurt Huwig about the project.*

***How did the project come about?***

The OpenAntiVirus Project was officially started in August 2000, when we registered the project at sourceforge.net and we reserved the openantivirus.org domain.

It was started by Howard Fuhs and Rainer Link – the idea itself was conceived in January 2000 during a telephone call between the two of us. We both have a very strong belief in open-source software and we feel that, especially in the field of security, open protocols and open/free software are essential.

OpenAntiVirus is a platform for those who are seriously interested in anti-virus research and network/computer security. Its aim is to facilitate communication amongst researchers and consequently the development of solutions for various security problems and development of new security technologies. Researchers are encouraged to work together, share their ideas and re-use existing code. Although a healthy amount of competition is welcomed, all-out 'war' between projects is discouraged!

Mailing lists are provided as the main source of communication for participants. Currently there are three lists (each provided by a sourceforge.net version of GNU Mailman): openantivirus-announce is a mailing list dedicated to announcements from the OpenAntiVirus team; openantivirus-discuss is a general discussion mailing list; and openantivirus-developer is for developers.

The project is open to anyone who has a genuine and serious interest in white hat anti-virus research and computer security.

***What are the ongoing projects?***

There are a number of official OpenAntiVirus.org (OAV) projects. ScannerDaemon, VirusHammer and PatternFinder are the first implementations of a GPL'ed virus scanning engine (VirusHammer is a standalone virus scanner that can be run by end users); squid-vscan is a third-party application which allows traffic passing through Squid HTTP-proxy to be scanned for known viruses; samba-vscan is a proof-of-concept module for Samba, using the virtual file system features of Samba 2.2.x/3.0 alphaX (this also supports a wide range of commercial anti-virus scanners); finally, a Mini-FAQ text file is maintained, which lists anti-virus products available for Unix/*Linux*.

Alongside the official OAV projects, the OpenAntiVirus.org members have developed a number of applications and tools. Email virus scanner AMaVis was initially set up by Christian Bricart and is maintained by Lars Hecking and co-developed by Rainer Link; httpf is a WWW security proxy co-developed by Gregor Goldbach; and Inflex and XaMime are email content-filtering and virus scanning tools developed by Paul L. Daniels, whose SignatureDB provides signatures/fingerprints of common non-viral but undesirable emails or files.

Many of the subscribers to our mailing lists are also working on their own projects.

***How many developers work on the project? Is there a central core of developers?***

The core OpenAntiVirus team consists of co-founders Rainer Link (project admin) and Howard Fuhs, webmaster Frank Ziemann and developers Christian Bricart and Kurt Huwig. Currently, most of the development work is carried out by Kurt Huwig and Rainer Link. Kurt's work is focused on the core virus scanning engine (ScannerDaemon/VirusHammer) and the third-party application squid-vscan. Rainer's work is focused mainly on developing third-party applications such as AMaViS and samba-vscan.

***Your primary scanning engine is written in Java – what influenced this choice? Do you think the speed of your scanning engine suffers because of it?***

(*Kurt*) I knew this would be one of the top FAQs even before I released the first version. Because everyone uses the poor Java implementations in browsers, they think Java is inherently slow. The fact is that the current engine scans about 12 Megabytes per second on a Duron 800, which is more than a 100 MBit NIC can transfer, so I do not think that it presents a problem for anyone's Internet connection besides the real big carriers.

I carried out some testing before I started to develop the scanner and these tests showed that an optimized version can scan 125(+) Megabytes per second on an Athlon 600 (I switched machines in between). This is about the memory transfer rate of my current machine, so I do not think that speed will be an issue for me in the future.

Another developer has implemented a scanner based on the signature file of the OAV project. He uses an inferior scanning engine, which means that his is about eight times

*slower* than the current Java implementation. Another team is working on porting the OAV algorithm to C (Clam Antivirus).

The following is a comparison of scanning speeds between the OAV Java implementation (ScannerDaemon) and ClamAV, written in C:

| | |
|---|---|
| **100 Mb random file** | |
| ScannerDaemon 0.5.1 | 8.95 s |
| ClamAV 0.20 | 9.012 s |
| **5 Mb random file** | |
| ScannerDaemon 0.5.1 | 0.22 s |
| ClamAV 0.20 | 0.468 s |

The differences are minimal – clamscan builds the tree each time. (This was tested on a 1.2 GHz Athlon desktop, with JRE 1.4.0 and the same virus database and algorithm settings.)

***Do you find you get a large number of patches/suggestions from users?***

We do receive some suggestions from users and also some patches. The core has yet to settle and I guess once it is stable, people will write extensions to it.

***How much interest has the project generated? Do you have a rough estimate of the number of users?***

(*Kurt*) The openantivirus-discuss mailing list has roughly 300 subscribers. Recently the OAV ScannerDaemon was added to Debian and I was asked not to change the interfaces for the virus updates. According to the peak of downloads after a new release of the signature file, I would estimate that we have between 400 and 1000 active users.

***Primarily, who do you find your users are?***

(*Rainer*) I'd say mostly sysadmins of smaller companies, but it's difficult to give exact figures here. SuSE has shipped AMaViS since SuSE Linux 7.2 (and offers it for users of the SuSE email Server); samba-vscan is shipped on the update release CD of the SuSE Linux Enterprise Server 7 and it will be shipped on the next SuSE Linux release, too.

(*Kurt*) The majority of feedback I get is from sysadmins trying to get OAV into their system.

***What are the benefits of open-source anti-virus software? Do you feel there are downsides?***

We are not tied to any business plans or political restrictions. We can detect dialers and governmental tapping software, which some of the commercial vendors choose not to do. You can use our products in other open-source products without the need to buy a licence either for yourself or for your customer. Recently, we have been contacted by a group that writes an IRC client and who would like to add virus scanning to their product for the file transfer.

Open source prohibits the use of NDA documentation, but we can use a number of GPL-licensed algorithms so, altogether, it is easier to do the open-source thing.

***Do you think the availability of commercial scanning libraries on* Linux *and* FreeBSD *inhibits the adoption of open-source anti-virus software?***

Currently, there is not much competition between commercial products and our product. The commercial products detect many more viruses, so anyone who relies on virus detection for their protection really has to choose the commercial scanners.

On the other hand, our product is free of charge, which makes it ideal for use in universities, schools, NGO, the health care sector, projects in the developing world and so on – organizations and projects that may not have sufficient funds to pay for the commercial product licences. Using our product they get at least some protection against some 95 per cent (plus) of all viruses.

***A significant barrier to entry into the anti-virus field is getting hold of real virus specimens – how do you go about attaining them?***

(*Kurt*) The anti-virus community is quite friendly to me. Most of the time when I ask for a virus sample, someone sends it to me. Currently, I have more samples than I can analyse, so I am experiencing something of a bottleneck. I do not have access to the big 'In the Wild' collections. However, at the current time my primary concern is to stabilize the engine and once that has been achieved I will head towards the integration of more viruses.

***Have you encountered any hostility from the anti-virus industry?***

(*Rainer*) Not via personal mail, but there has been some negative feedback on some newsgroups/mailing lists. I have a very good relationship with a lot of anti-virus vendors, especially as some of the companies benefit from projects like AMaViS or samba-vscan – I know that some AV companies who do not have their own email gateway solution suggest AMaViS to their customers.

***Does OAV plan to undertake any specific projects in the future?***

There are a number of projects in the pipeline for the OpenAntiVirus team, including a rescue disk/CD, general on-access scanning and a remote management system.

*For more information on the OpenAntiVirus project, including information on how you can join the mailing lists and contribute, visit http://www.openantivirus.org/.*