

MoLD - samba-vscan

Rainer Link
rainer@openantivirus.org

Agenda

- personal background
- introduction
- current status
- future

personal background

- interested in computer-viruses and anti-virus technology since 1991
- Mini-FAQ anti-virus software for Linux established in 1998/99
- joined the AMaViS development team in 1999
- founded OpenAntiVirus.org in 2000
- samba-vscan started in 2001

Introduction

- samba-vscaan uses the (POSIX) Virtual File System (VFS) in Samba 2.2 / 3.0
- requires 3rd party anti-virus product
- originally developed for Sophie and Trophie
- currently more than ten anti-virus products are supported
- current version (still **sigh**) 0.3.5

Samba VFS (I)

- Originally developed by Tim Potter
- First introduced in Samba 2.2.0
- allows to “hook” various disk/file/ACL operations (e.g. open, close, read, write)
- Samba 2.2: only one VFS module per share possible, e.g.
[test]
 vfs object = /path/to/vfs-object.so

Samba VFS (II)

- VFS modules are no stackable (i.e. more than one module per share)

[test]

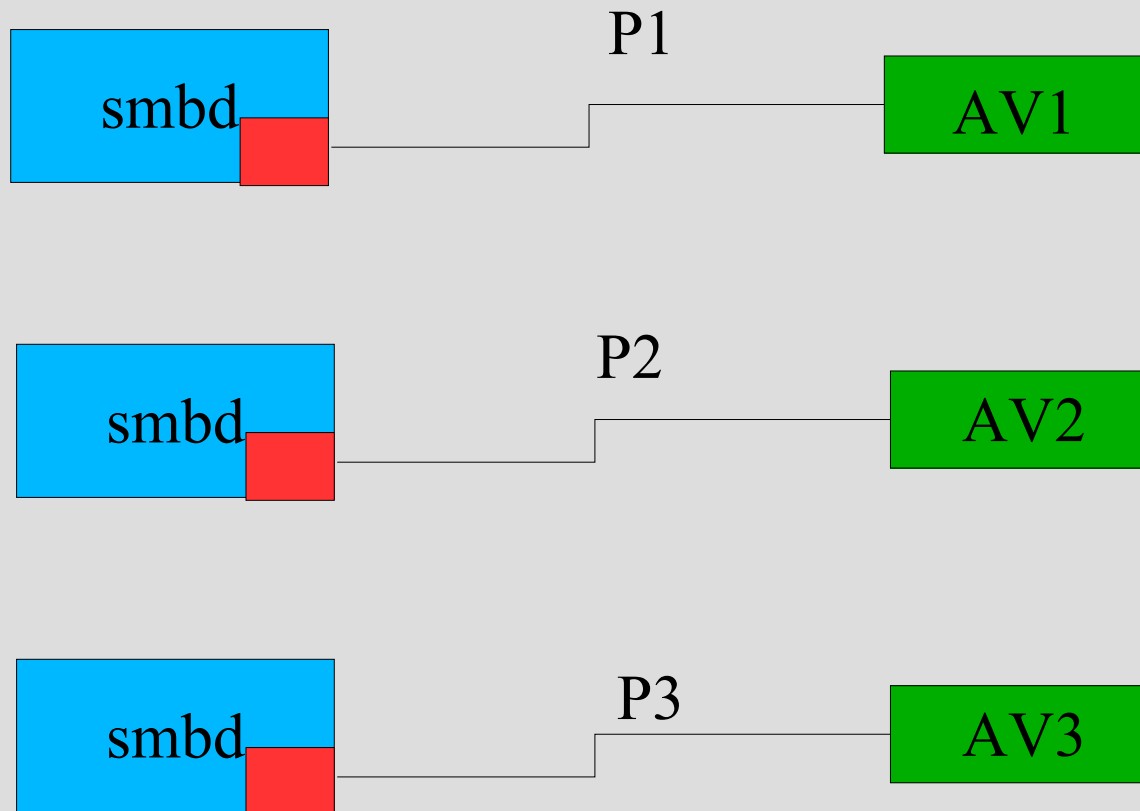
vfs objects = vfs1 vfs2 vfs3

- several operation layers are possible (e.g. noop, opaque, transparent)

samba-vscan (I)

- Hooks open / close (blocking)
- no on-the-fly scanning by hooking read / write
- deny access / quarantine / logging
- scanning results caching to improve performance
- current design: one VFS module for each supported virus scanner
- a “framework” provides commonly used functions for all modules

samba-vscaan (II)

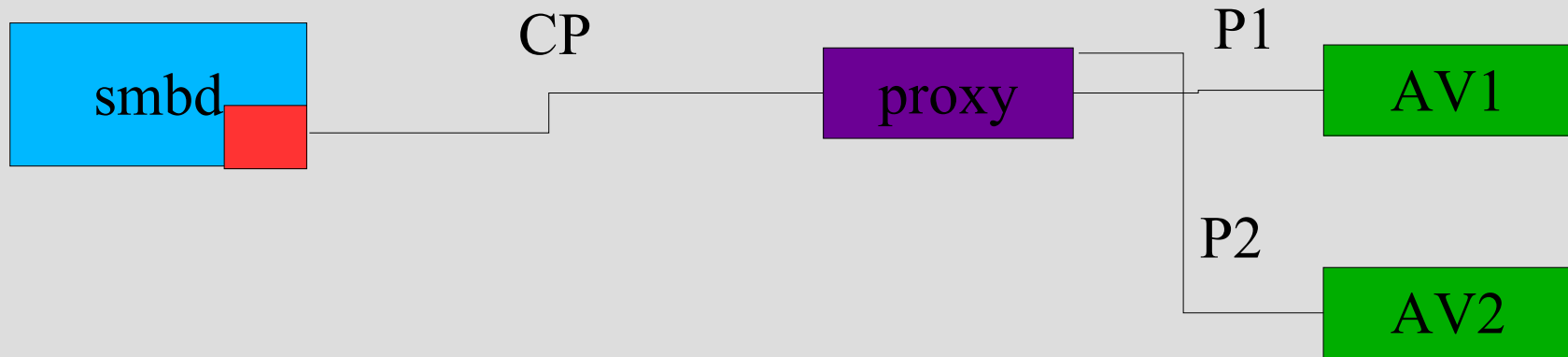


Each AV daemon speaks his own protocol; one module for each means multiple work!

commercial VFS plugins

- Dr Web (source code available for download)
- Kaspersky (source available on request)
- F-Secure (dunno)
- Bitdefender (dunno)
- probably others?!

samba-vscaan (III)



A sole module communicating with the proxy via common protocol, proxy then communicates with corresponding AV daemon. This could be extended to commercial AV VFS modules, too. So, similar to dazuko, one commonly used AV VFS module. The proxy could be avoided if one common protocol is used.

License stuff

- VFS module must be licensed GPL
- therefore, VFS module must not be linked to a virus scanning lib
- therefore, VFS module must communicate via socket to AV

Outlook

- more code re-write (extend the “framework”)
- Samba4 support
- drop Samba 2.2.x support (2.2.x is dead)
- more actions on virus event
- add CRC support (unsure)
- fix some FIXMEs :)

Samba 4

- Samba has asynchronous design (non-blocking)
- NTVFS should act asynchronous, but can be synchronous as well (as in Samba 3)
- an NTVFS module must implement all NTVFS calls (most cases simply call a macro which calls default behaviour)
- NTVFS is more “low-level” than VFS
- For details RTFS of samba4 :-)

URLs

- ICAP: www.i-cap.org
- OPES/OCP: www.ietf-opes.org
- My diploma thesis (can ICAP be used as AV-protocol for multiple purposes):
<http://www.openantivirus.org/diploma-thesis.pdf>

Questions / Thanks

- Comments?
- Feedback?
- Suggestions?