



# OpenAntiVirus

Kurt Huwig  
CEO iKu Systemhaus AG  
kurt@openantivirus.org

Rainer Link  
rainer@openantivirus.org

# The Projekt (I/III)

- Founded August 2000
- Core Team Members
  - ◆ Rainer Link (Founder)
  - ◆ Howard Fuhs (Co-Founder + Evangelist)
  - ◆ Frank Zieman
  - ◆ Christian Bricart
  - ◆ Kurt Huwig (Developer Core Technologies)

# The Project (II/III)

- official OpenAntiVirus projects
  - ◆ **ScannerDaemon / VirusHammer / PatternFinder**
  - ◆ **Squid-vscan**
  - ◆ **Samba-vscan**
  - ◆ **lkml-vscan**
  - ◆ **Mini-FAQ**
  - ◆ **Bootdisk**

# The Project (III/III)

- Related projects

- ◆ **AMaViS (A Mail Virus Scanner)**
- ◆ Inflex / Xamime
- ◆ httpf
- ◆ mod\_vscan

# The solution: OAV

- **PatternFinder (Java)**
  - ◆ Creates the virus sigs
- **ScannerDaemon (Java)**
  - ◆ Virens scanning service
- **VirusHammer (Java)**
  - ◆ Stand-alone GUI virus scanner

# The solution: OAV

- Samba-vscan (C)
  - ◆ On-Access virus protection for Samba
- Squid-vscan (C)
  - ◆ Access-Scan for Squid
- Linux-Kernel Modul (C)
  - ◆ On-Access scan

# Samba-vscan (I/IV)

- Uses Samba Virtual File System (VFS)
- Scans files on open
  - ◆ Denies access when file is infected
- Scans files on close
  - ◆ Only logging possible

# Samba-vscan (II/IV)

- Other features

- ◆ Run-time config file
- ◆ Moving infected files into quarantine
- ◆ LRU mechanism to improve performance
- ◆ Notification via win-popup

# Samba-vscan (III/IV)

- Supports various scanners via API/socket comm
  - ◆ OAV ScannerDaemon, ClamAV (socket)
  - ◆ F-Prot Daemon (socket)
  - ◆ Mks32 (API)
  - ◆ Sophos Sweep, via Sophie (socket)
  - ◆ Trend Micro, via Trophie (socket)
  - ◆ Kaspersky AntiVirus (API)
  - ◆ Symantec AntiVirus Engine via ICAP

# Samba-vscan (IV/IV)

- planned features

- Skip scan based on file type (WIP)
- Support more virus scanners
- More code-reorg
- Comparison
  - Kernel module
  - Ld preload method
- Status

# ICAP

- Internet Content Adaption Protocol (RFC3507)
  - ◆ Lightweight protocol for executing 'remote procedure call' in HTML messages
  - ◆ Four types of operation (only two mentioned in RFC)
- Can be used as a generic virus scanning protocol
- Successor: OPES (Open Pluggable Edge Services)

# Scan Engine

## General Overview

- virtual filesystem
  - offers access to compressed files
  - ZIP, UPX etc.
- sensors
  - check the file contents
  - string search
  - heuristics

# String Search

- fast string search is essential for virus scanning
- algorithm used is from Aho/Corasick
- **n** strings within **m** bytes
  - runtime  $O(m)$
  - independent of number of patterns
  - optimized Java version: 120 MB/second on Athlon 600

# String Search

- BUT: high memory consumption
- memory is about 100.000 times the size of the patterns
- modified algorithm: only 4 byte patterns
- linear search within all patterns starting with the same 4 bytes
- trading speed for memory
- 14 MB/second -> enough for practical uses

# Digital Signatures

- virus patterns are digitally signed
- two step scheme using certificates and a certification authority (CA)
  - the core developer is the CA
    - but: everyone can be his own CA
  - keys are signed by the CA
  - patterns are signed by signed keys
  - pattern signature and key signature are validated

# Digital Signatures

- several levels of trust
- level 1: no identity check has been made
- level 2: untrusted GPG identity
- level 3: trusted GPG identity
- level 4: personal identity check completed
- default setting: level 3 or better needed
- up to now: 51 level 1 keys, one level 3 key

# Pattern Finder

- research tool: what do other scanners detect?
- you need:
  - a virus
  - a virus scanner detecting the virus
- file is overwritten systematically
- each time, scanner is asked if the file is infected
  - if it is not infected any more: revert the change

# Pattern Finder

- a „skeleton“ of the virus remains
- easier analysation
- some patterns can be used for string search
- shows how to cloak a virus from current search engines
  - Valve Software: keyboard input logged by a trojan that was not detected by virus scanning software

# ICAP Server

- Internet Content Adaption Protocol
- „content filtering over TCP/IP“
- Samba-vscan supports it
- Squid patch available

# Problem: how to prevent „user timeout“?

- ▶ file needs to be complete to check it
- ▶ headers have to be sent early
- filter uses a buffer
  - ▶ user gets the file minus several kB
- if the file is infected, download is canceled
  - ▶ current browsers delete the file

# Problem: how to inform the user?

- notification via email or popup is possible
- easiest solution: cache the result
  - what does the user do if the download has been canceled?
  - click on the file a second time!
  - display an error message now

# Why Java?

- fast enough: 14 MB / second on Athlon 600
- ClamAV
  - C implementation of the same algorithm
  - no speed improvement
- platform independent
- no buffer overflows
  - we are not part of the problem

# Future

- virus and pattern upload server
- more containers for virtual filesystem
- better heuristical search
- better support for Microsoft Office files

# Questions? & Answers!

- <http://www.openantivirus.org/>
- <http://www.iku-ag.de/>