Dazuko: An Open Solution to Facilitate 'On Access' Scanning

DAZUKO

An Open Solution to Facilitate 'On Access' Scanning

John Ogness
Software Engineer

H+BEDV Datentechnik GmbH
Tettnang, Germany

www.antivir.de

Forms of Virus Protection

- on-demand file scanning
- on-access file scanning
- scanning as specialized plug-in
- proxy scanning
- stream scanning

Forms of Virus Protection

- on-demand file scanning
- **on-access file scanning**
- scanning as specialized plug-in
- proxy scanning
- stream scanning

Problem

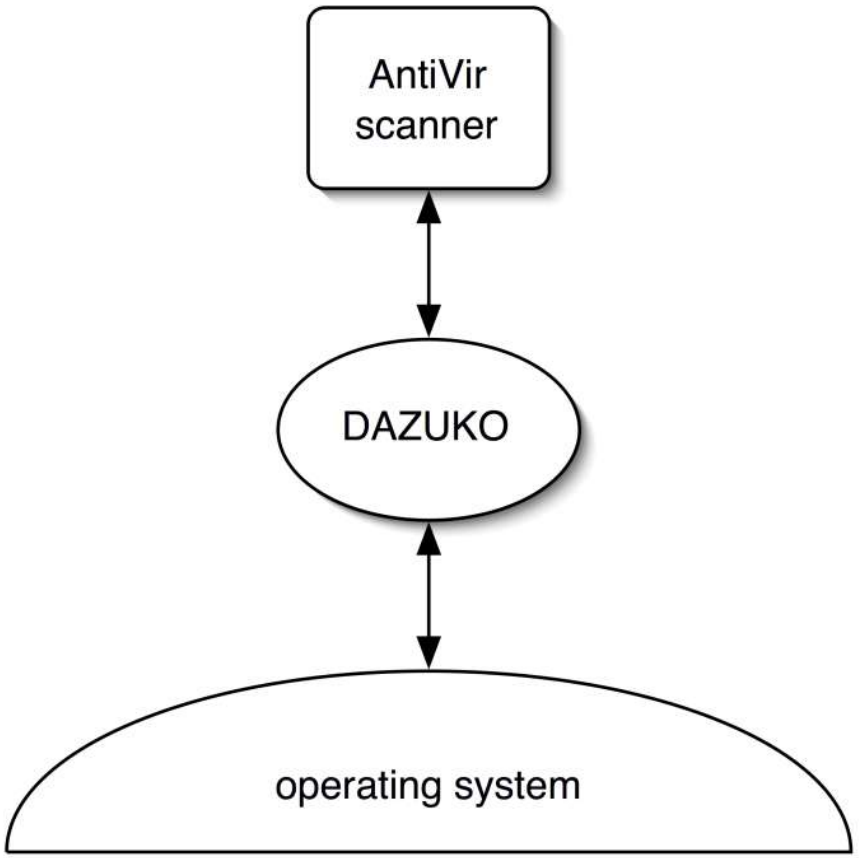
- requires an intimate relationship
  - → many operating systems
  - → many architectures
  - → many licenses
- everyone does it independently
- incompatible solutions

Solution

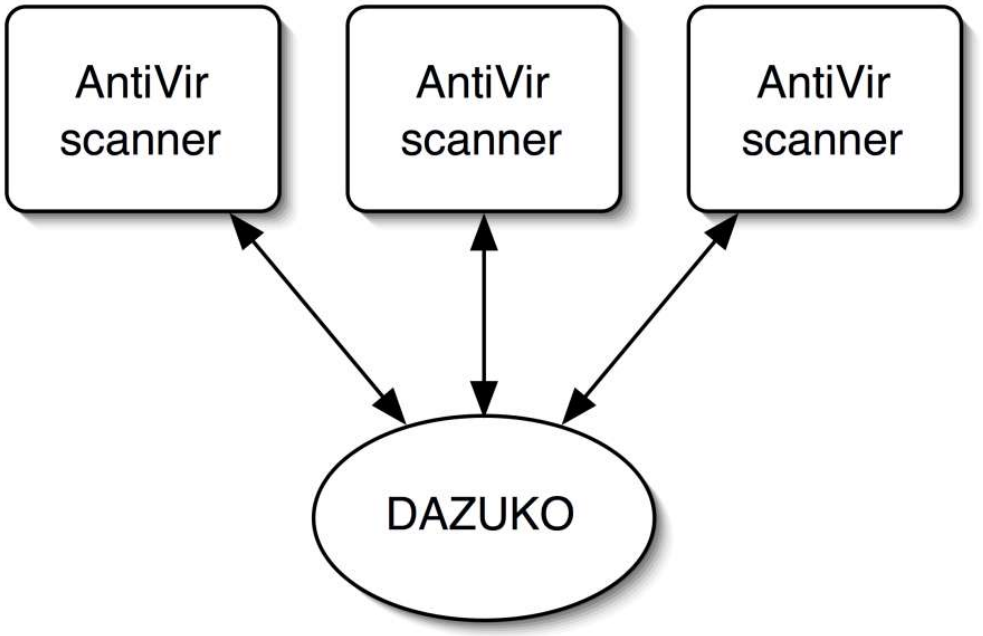
- anti-virus interface available from the operating system
- common for all systems
- flexible license

Dazuko

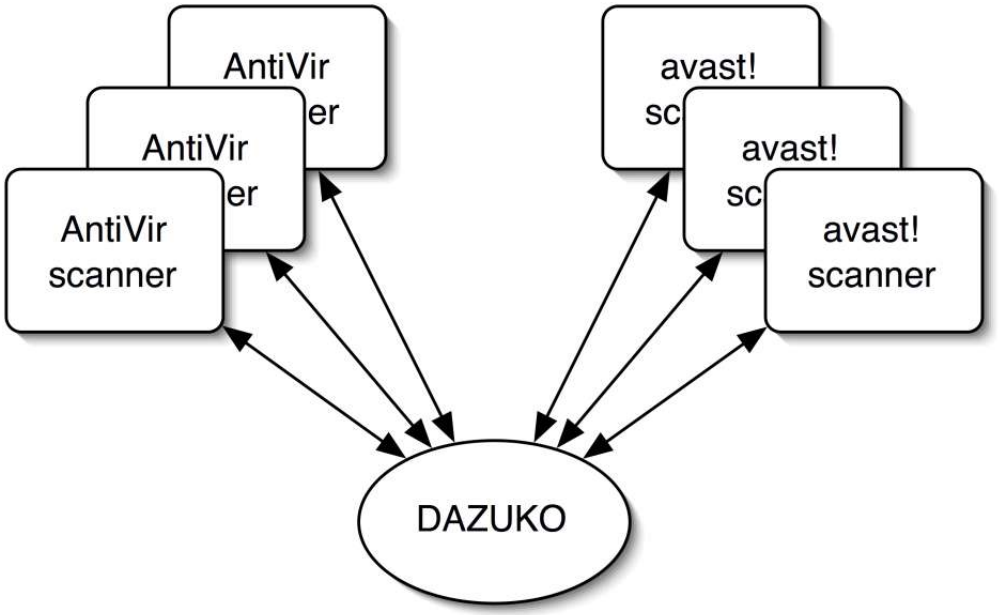
Concept



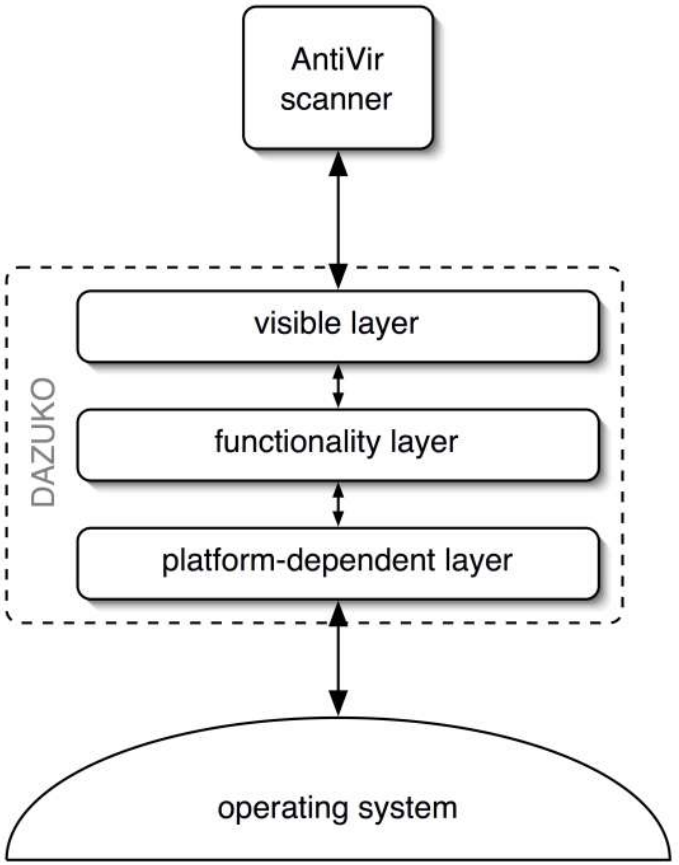
Sharing



Cascading



Abstraction (Layers)



Abstraction (Protocol)

key = value

unknown keys ignored

Interface

- implemented in C and Java
- 7 functions
  - register
  - configure (3)
  - get access
  - return access
  - unregister
- supports multiple threads

Demo

Current Status

- BSD license*
- Linux and FreeBSD support
- recognized
- community development
- building a common foundation
- making on-access easy

Future

- expand to more platforms
- improve documentation
- establish relationships
- support existing standards
- improved security model

Conclusion

- handles the "dirty work"
- strong basis for expansion
- active in the community
- interested in open standards
- the word is getting out

Questions