Dazuko

John Ogness
UNIX Team Leader
H+BEDV Datentechnik GmbH
Tettnang, Germany
http://www.antivir.de

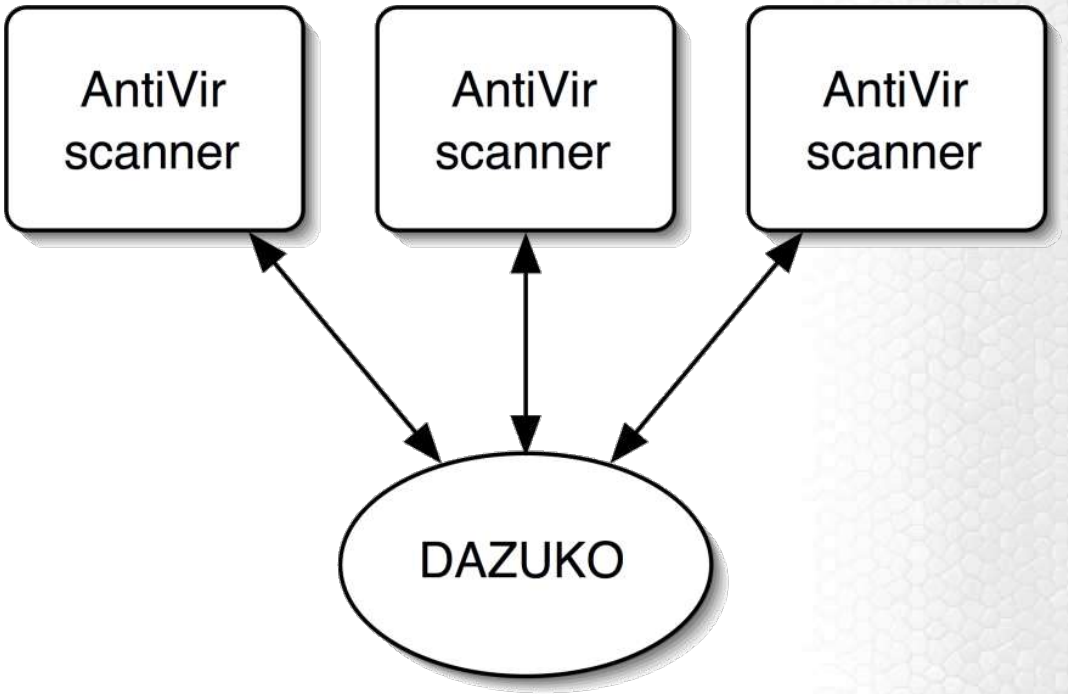
Copyright © 2005 H+BEDV Datentechnik GmbH

What is Dazuko?

- kernel module (GPL) + userspace library (BSD)
- provides mechanism for file access control from userspace
- common interface on all systems
  (GNU/Linux, FreeBSD, Solaris*)
- interface available in various languages
  (C, Java, Perl, Python, PHP*, Ruby*, LUA*)
- supports load sharing and cascading
- 100% backward compatible with version 1.0
- no recompiling of kernel required*

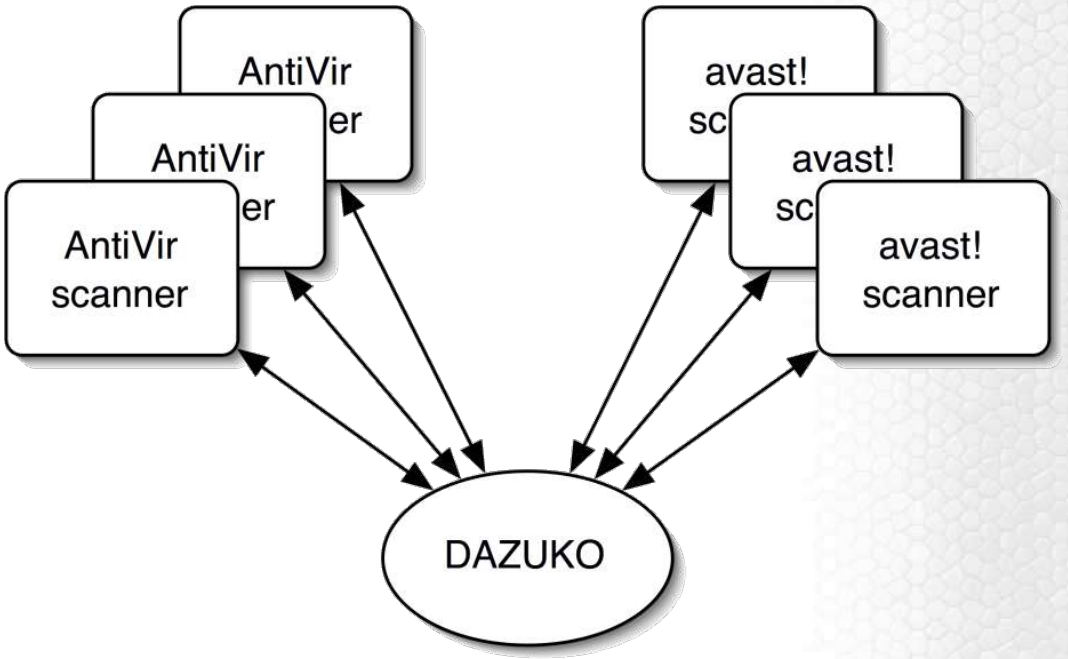
Copyright © 2005 H+BEDV Datentechnik GmbH

Sharing



Copyright © 2005 H+BEDV Datentechnik GmbH

Cascading



Copyright © 2005 H+BEDV Datentechnik GmbH

Concept

- access control application procedure
  - register to begin file access control
  - define events of interest
  - events received (through blocked polling)
  - responses to events returned (allow/deny)
  - unregister to stop excercising file access control
- registered applications allowed to open files “unnoticed”
- one application from each group receives event
- an event is always received by all groups
- if any one group returns “deny”, access is denied

Copyright © 2005 H+BEDV Datentechnik GmbH

Current Problems

- system call table not enough
- event information varies between events and situations
- “close” events unreliable
- “close” events may occur before filesystem flush
- no “close” events under Linux 2.6
- only registered applications allowed “unnoticed” file access
- only classical filesystem access events supported
- global configuration for events of interest
- no handling of registered application state (dead/hung/stopped)
- no access to `__d_path()` within Linux 2.6

Copyright © 2005 H+BEDV Datentechnik GmbH

Proposed Solutions

- system call table not enough
- event information varies between events and situations
- “close” events unreliable
- “close” events may occur before filesystem flush
- no “close” events under Linux 2.6
- only registered applications allowed “unnoticed” file access
- only classical file access events supported
- global configuration of events of interest
- no handling of stopped applications
- no access to Linux 2.6

DazukoFS

Trusted Applications

Event Injector

Kernel Monitor

Separate Configurations

Kernel Patch + Political Pressure

Copyright © 2005 H+BEDV Datentechnik GmbH

DazukoFS

- stackable filesystem
- deeper in kernel
- events more abstract
- based on FiST?

Copyright © 2005 H+BEDV Datentechnik GmbH

Trusted Applications

- trusted application procedure
  - request for trusted access from a group (using token)
  - “request token” given to access control application as event
  - access control application allows/denies trusted application
  - trusted application receives result
  - if allowed, trusted application may now access files “unnoticed” by group
  - trusted application relinquishes trusted status
- trusted application verified with each file access
- being able to allow trusted applications is specified in the access mask

Copyright © 2005 H+BEDV Datentechnik GmbH

Event Injector

- application registers as event injector also giving “protocol” (for example “ftpfs”)
- event injector application sends events and receives responses
- events are sent to all registered, interested access control applications
- event filenames are in the form *`protocol`*`:`*`filename`* (for example “ftpfs:user:pwd@ftp.antivir.de/pub/antivir.tgz”)

Copyright © 2005 H+BEDV Datentechnik GmbH

Proposed Solutions

- system call table not enough
- event information varies between events and situations
- “close” events unreliable
- “close” events may occur before filesystem flush
- no “close” events under Linux 2.6
- only registered applications allowed “unnoticed” file access
- only classical file access events supported
- global configuration of events of interest
- no handling of stopped applications
- no access to Linux 2.6

DazukoFS

Trusted Applications

Event Injector

Kernel Monitor

Separate Configurations

Kernel Patch + Political Pressure

Copyright © 2005 H+BEDV Datentechnik GmbH

Questions

Copyright © 2005 H+BEDV Datentechnik GmbH

DAZUKO

Malware on Linux Detection Meeting 2005

Copyright © 2005 H+BEDV Datentechnik GmbH