QMVC
Qmail Mail and Virus Control

Dr. Erwin Hoffmann

feh@fehcom.de
http://www.fehcom.de

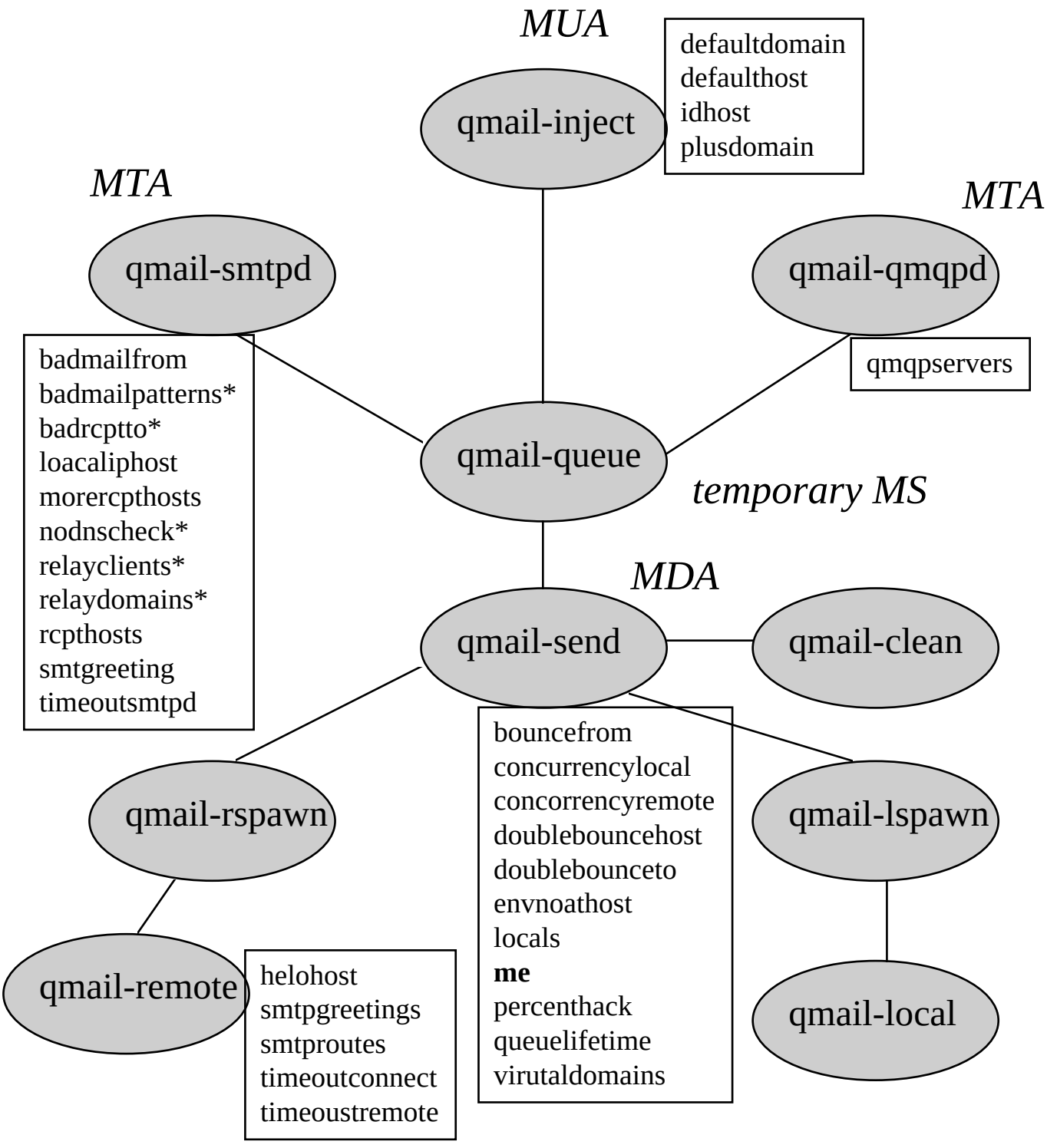
FFG - Frühjahrsfachgespräch
Bochum, 2002-2-28

QMVC what ?


Google
Web
Bilder
Groups
Verzeichnis
QMVC
Google-Suche
Auf gut Glück!
Erweiterte Suche
Einstellungen
Sprach-Tools
Suche: Das Web Seiten auf Deutsch Seiten aus Deutschland
Probieren Sie unser neues do-it-yourself Marketingsystem aus.
Suchtipps - Alles über Google - Google.com [English]


Google
Erweiterte Suche
Einstellungen
Sprach-Tools
Suchtipps
QMVC
Google-Suche
Suche: Das Web Seiten auf Deutsch Seiten aus Deutschland
Web
Bilder
Groups
Verzeichnis
Das Web wurde nach QMVC durchsucht. Resultate 1 - 10 von ungefähr 245. Suchdauer: 0.11 Sekunden
QMVC - Qmail Mail and Virus Control - [Diese Seite übersetzen]
QMVC - QMAIL Mail and Virus Control. QMVC. is an unidirectional
Mail Filter and Virus Scanner ...
www.fehcom.de/qmvc.html - 9k - Im Archiv - Ähnliche Seiten
Clubs-Q-Verzeichnis
Quedlinburger Motor-Veteranen-Club eV (QMVC). Quedlinburger
Motor-Veteranen-Club eV (QMVC) Herr ...
www.auto.de/Oldtimer/Clubs/clubs-q-verzeichnis.htm - 1k - Im Archiv - Ähnliche Seiten

QMAIL - The MTA



E-Mail Situation Today and in Future

- Currently, 10 % of all E-Mails have an attachment (mostly MIME)
- 1% of E-Mails are virus infected; this rate is probably increasing
- Virus-Bombs becoming a thread for ISPs:
  - Web sites are scanned for E-Mail addresses (mailto:) and serve as targets for infected mails send with high frequency
  - The same happens to well known E-Mail addresses (info@domain.com or postmaster@domain.com).
- For Qmail, some anti-virus tools are available:
  - Qmail-Scanner
  - AMaVis
  - Kaspersky Lab AVP
  - OdeiaVir
- It is necessary, not only to protect for virus mails but additionally to understand their "sources" and "sinks"

QMVC Design Principles

- ***qmvc*** works uni-directional; only E-Mails to be locally delivered will be checked
- ***qmvc*** runs with stock Qmail, no patches have to be applied
- ***qmvc*** does not interfere with Qmail's standard delivery process and queueing
- ***qmvc*** depends solely on the ***qmail-local*** mechanism
- No PERL interpreter needed, just C-binaries and the Korn-Shell
- ***qmvc*** runs with minimal permissions
- QMVC scales well up 100 000 E-Mails / day (assumptions: i386/1GHz CPU, 512 MB mem, 10% attachments, 1% viruses, 3 AV scanners mutually used)

QMVC Features

- ***qmvc*** supports Qmail's (and vpopmail) *virtualdomains* with different security profiles
- ***qmvc*** comes with standard E-Mail filter:
  - Subject: Line
  - Body-Text
  - Attached file names
  - Attached file types (mime)
  - Null-Sender Mails (without SMTP Sender)

  ☞ E-Mails identified by at least one criterion are called ***Badmails***
- (Mutually) Supported Anti-Virus Scanners:
  - F-Secure, Sophos, NAI/McAfee, Trend-Micro,
  - CA/InoculateIT
- Incident Messages to administrators, recipient, and (multilingual) to sender (on demand)
- Detected Badmails or infected Mails may be kept or forwarded
- Easy Administration:
  - On-the-fly configuration
  - Minimal logging, easily parseable
  - On-time reporting functionality (incident messages)
  - Excellent analysis tools (Virulator)
  - Automated updates of virus patterns
- QMVC protects (automatically) from Virus-Bombers

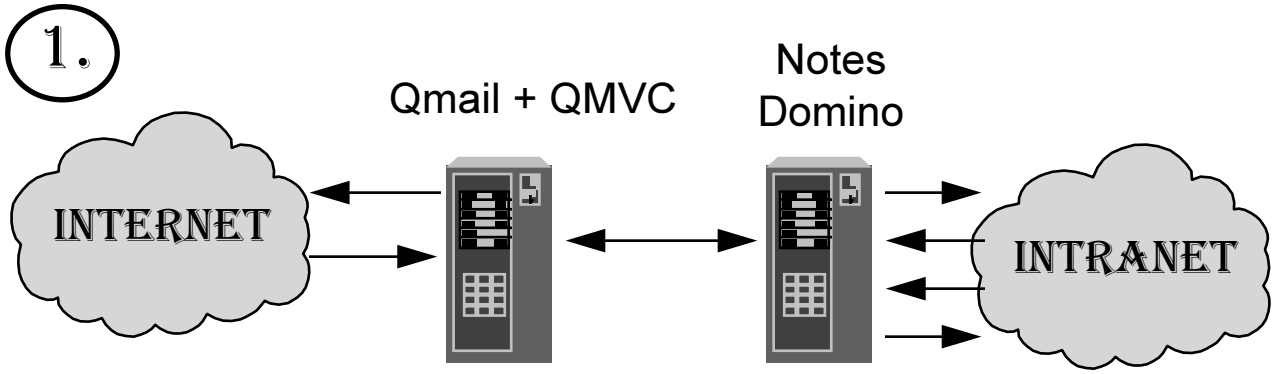
QMVC No-Features

- ***qmvc*** does not apply an
  - "X-Virus-Checked:" Header field to the processed E-Mail; it's simply stupid
- ***qmvc*** does not try to un'tar, un'pack, or un'zip the identified MIME attachements
  - it's the task of the AV scanners to look into the archives
- ***qmvc*** does not block tar-ed, pack-ed, or zip-ed E-Mails even if the archive contains a file to be filtered
  - it's not forseen to completely block E-Mail traffic, rather to control it
- ***qmvc*** will never kill Qmail or stop Qmail from receiving
  - the maximum is a (deferred) delivery, until the situation is cleaned (eg. file system full)

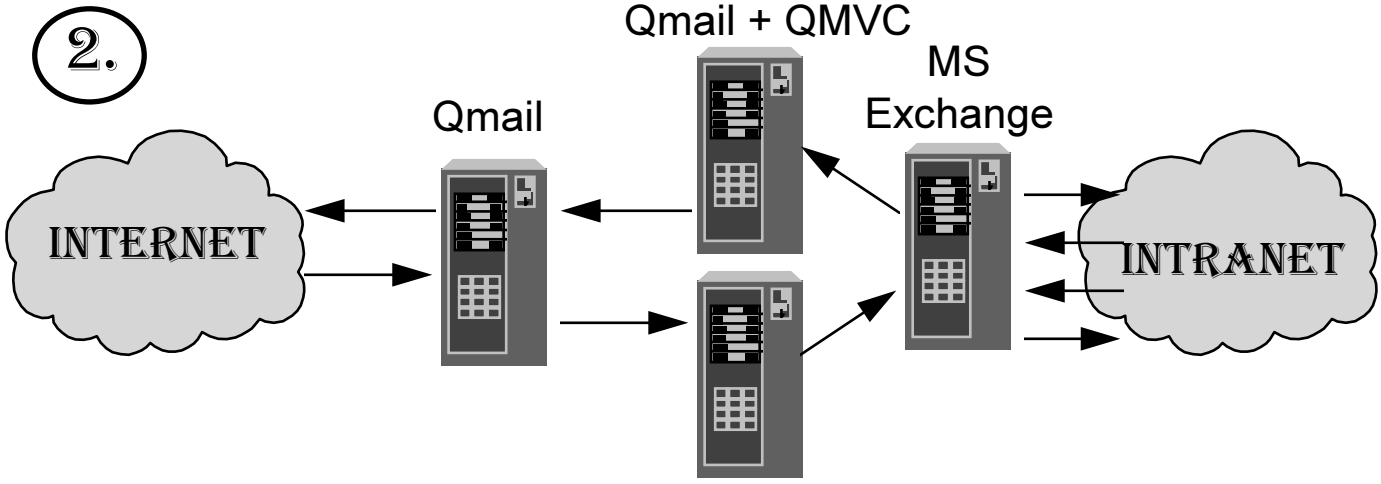
QMVC Dependencies

- QMAIL (1.03)
- William Bextor qtools (0.55) - E-Mail parser
- Sam Varshavchik's Maildrop (1.3.7) - MIME parser ***reformime***
- File (3.3.7) utility - identifying MIME files
- Korn-Shell
- PERL for analysis routines (Virulator, qmvlog2html)
- (SPAMCONTROL patch)
- AV Scan-Engines
  - F-Secure ***fsav***
  - Sophos ***sweep***
  - NA/McAfee ***uvscan***
  - Trend-Micro ***vscan***
  - CA InoculateIT (***inocumd***)

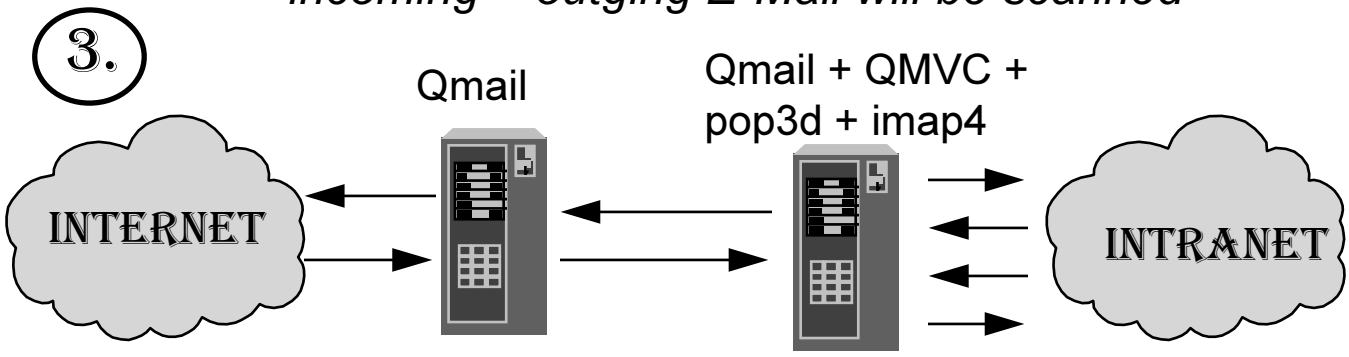
Application Studies



incoming E-Mail will be scanned



incoming + outging E-Mail will be scanned



incoming E-Mail will be scanned individually

Virus Scanning

Product	Version	Path	Library	Size (byte)	Pattern file	Size
Sophos Sweep	3.51	/usr/local/bin/sweep		105.256	ver__dat + *.ide	1.981.687 + X
McAfee UVSCAN	4.12	/usr/local/uvscan/uvscan		120.831	scan.dat	1.687.421
Trend Micro VSCAN	3.1	/etc/iscan/vscan	VSAPI 5.5	23.632 + 981.180	lpt$vpn*	5.264.044
CA InoculateIT	6.0	/usr/local/inoculate/ inocucmd		901.484	virsig.dat	1.185.484

- Virus Scanning is ressource consumptive in particular if serveral AV Scan Engines are used mutually
  - the executable,
  - the necessary libraries, and
  - the pattern files

  have to be loaded into memory for each file.
- ***qmvc*** allows by-passing of AV Scan Engines if a Badmail conditions is met or one Engine has already identified a virus in the mail

Incident Reporting

- QMVC creates (on demand) Incident Reports in case of badmail and/or infected mail to:
  - Anti-Virus Guards
  - Badmail Guards
  - (the targeted) Recipient
  - Sender
- Incident Reports to the Sender may be multi-lingual (depending on the domain-suffix).
- All messages can be customized by means of templates

Date: 9 Jan 2002 16:37:48 -0000
From: qmvc@orion.fehnet.de
Subject: Infected E-Mail
To: erwin@orion.fehnet.de

>>>>>>>>>>> In der an Sie gerichteten E-Mail
<<<<<<<<<<<
Absender / Subject

Erwin Hoffmann <feh@fehcom.de> / TESTMAIL

wurde im Anhang ein Virus entdeckt.
Die E-Mail wird daher nicht an
Sie zugestellt.

Virus-Information:
McAfee: Found the W32/Goner@MM virus !!!
Found the W32/SirCam@MM virus !!!
Found the W32/SirCam@MM virus !!!
Trend Micro: *** Found virus JOKE_GESCHENK in file /var/tmp/qmvc.3021/content/geschenk.exe
*** Found virus WORM_SIRCAM.A in file /var/tmp/qmvc.3021/content/GF112.doc.com
*** Found virus WORM_SIRCAM.A in file /var/tmp/qmvc.3021/content/FOLHA2001.xls.com

Falls Sie Fragen hierzu haben,
konsultieren Sie unseren
Anti-Virus-Beauftragten:

<mailto: feh@fehcom.de>

QMVC Logging

- ***qmvc*** writes two different log files:
  - qmvc.log - well structured, easy parsable one-line action log file
  - qmvc.rep - report file, in case of badmails and/or virus mails
- ***qmvclog2html*** transforms qmvc.log into HTML format
- The "Virulator" correlates boths logs and gives a accurate description of the corrent badmail and virus mail situation

```
qmvc Pid:94761|20011106 09:22:47|cgi-mailer-bounces@kundenserver.de|gisela.wohlrabe@wdr.de|+E:0+S:0+O:0+R:0+A:0|RC:0|09:22:47
qmvc Pid:94935|20011106 09:22:51||Verkehr@wdr.de|+E:0+S:0+O:0+R:0+A:1+F:0+C:0|+M:1+T:1|RC:99|09:22:52
qmvc Pid:95171|20011106 09:22:52|qmvc@smtp01.wdr.de|Verkehr@wdr.de|+E:0+S:0+O:0+R:0+A:0|RC:0|09:22:53
qmvc Pid:95357|20011106 09:22:57|Andrea.Roeltgen@taskarena.net|karin.schueller@wdr.de|+E:0+S:0+O:0+R:0+A:0|RC:0|09:22:58
```

QMVC Development

- Currently QMVC 1.3.7 is available
- With Version 1.4.x an enhanced log-format will be introduced
- With Version 2.x the ***qmvc*** executable has to be rewritten in C (djb-c) and the auxiliar routines shall be embedded