Wietse’s mailer project

Wietse Venema

wietse@watson.ibm.com
wietse@porcupine.org
wietse@wzv.win.tue.nl

Overview of presentation

- Intro, obligatory jokes, etc.
- Why write yet another mailer?
- Why is sendmail vulnerable?
- Architecture and implementation
- Early experiences and plans

Sendmail’s horror story of advisories

CA-88:01 ftpd and sendmail vulnerability
CA-90:01 SUN sendmail vulnerability
CA-93:15 SUN sendmail vulnerability
CA-93:16 sendmail vulnerability
CA-94:12 sendmail vulnerability
CA-95:05 sendmail vulnerability
CA-95:08 sendmail vulnerability
CA-95:11 sendmail vulnerability
CA-95:13 sendmail vulnerability
CA-96:04 sendmail vulnerability
CA-96:20 sendmail vulnerability
CA-96:24 sendmail vulnerability
CA-96:25 sendmail vulnerability

Will qmail be the answer?

```
void err_qqt() { out("451 qqt failure (#4.3.0)\r\n"); }
void smtp_helo(arg) char *arg; {
 smtp_greet("250-"); out("\r\n250-PIPELINING\r\n250 8BITMIME\r\n
 seenmail = 0;
 dohelo(arg ? arg : ""); }
void smtp_rset() {
 seenmail = 0;
 out("250 flushed\r\n"); }
void smtp_mail(arg) char *arg; {
 if (seenmail) { err_seenmail(); return; }
 if (!arg) { err_syntax(); return; }
 if (!addrparse(arg)) { err_syntax(); return; }
 bmfcheck();
 seenmail = 1; out("250 ok\r\n");
 if (!stralloc_copys(&rcptto,"")) outofmem();
 if (!stralloc_copys(&mailfrom,addr.s)) outofmem();
 if (!stralloc_0(&mailfrom)) outofmem(); }
void smtp_rcpt(arg) char *arg; {
 if (!seenmail) { err_wantmail(); return; }
 if (!arg) { err_syntax(); return; }
 if (!addrparse(arg)) { err_syntax(); return; }
```

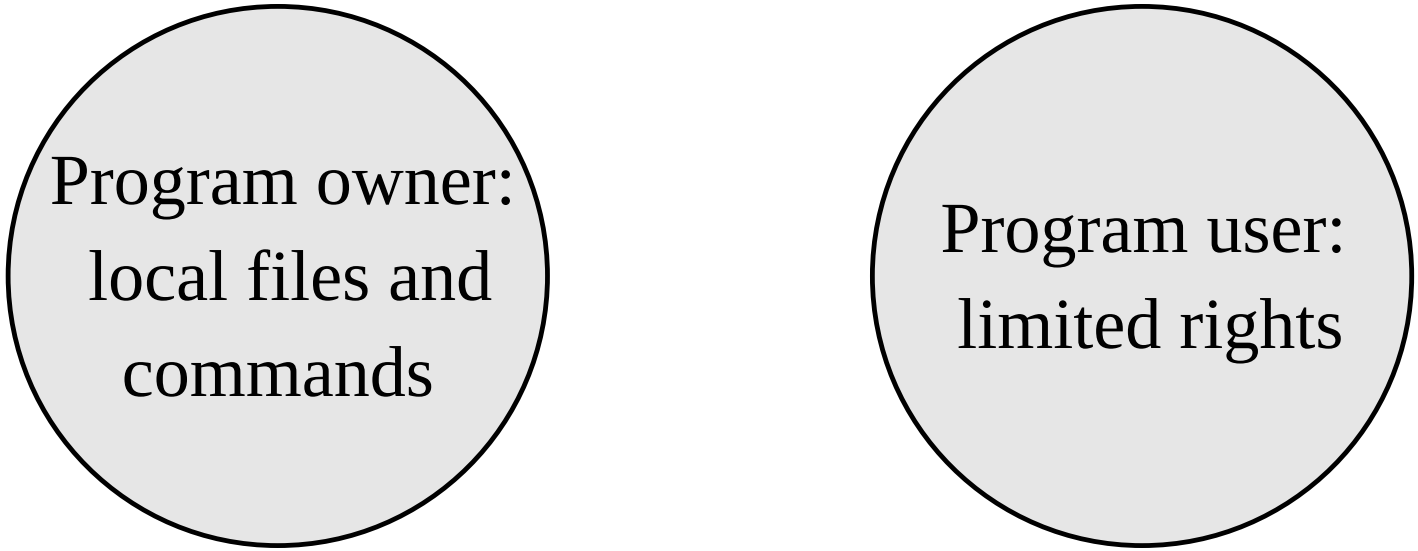
qmail.fig

Choice of non-proprietary mailer software

- sendmail: monolithic, privileged
- smail: essentially, sendmail in disguise
- exim: essentially, smail++
- zmailer: modular, relatively clean, but slow
- qmail: modular, agressive
- wietse’s mailer: modular, compatible

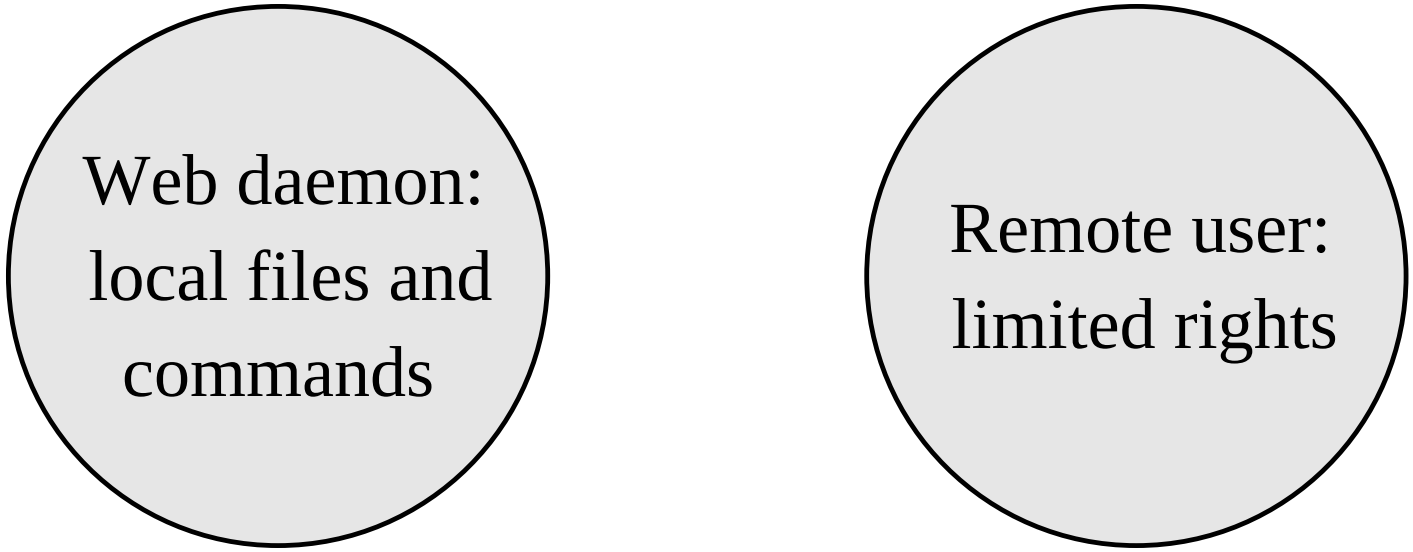
mailers.fig

Set-userid program: two rights domains



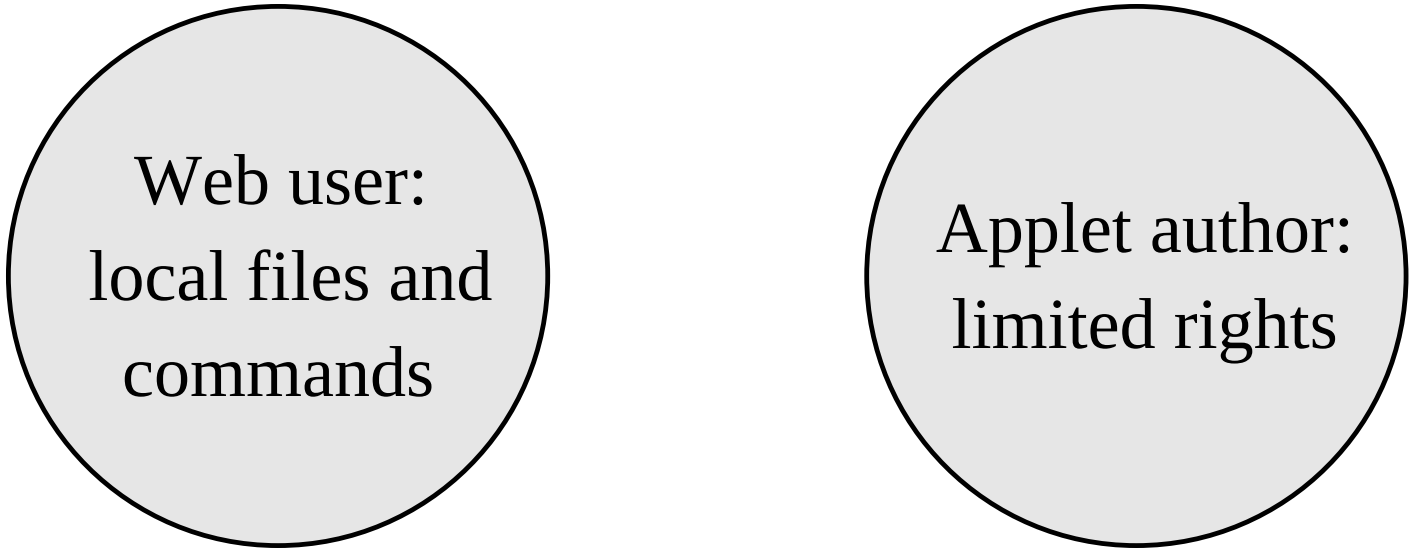
setuid.fig

WWW server: two rights domains



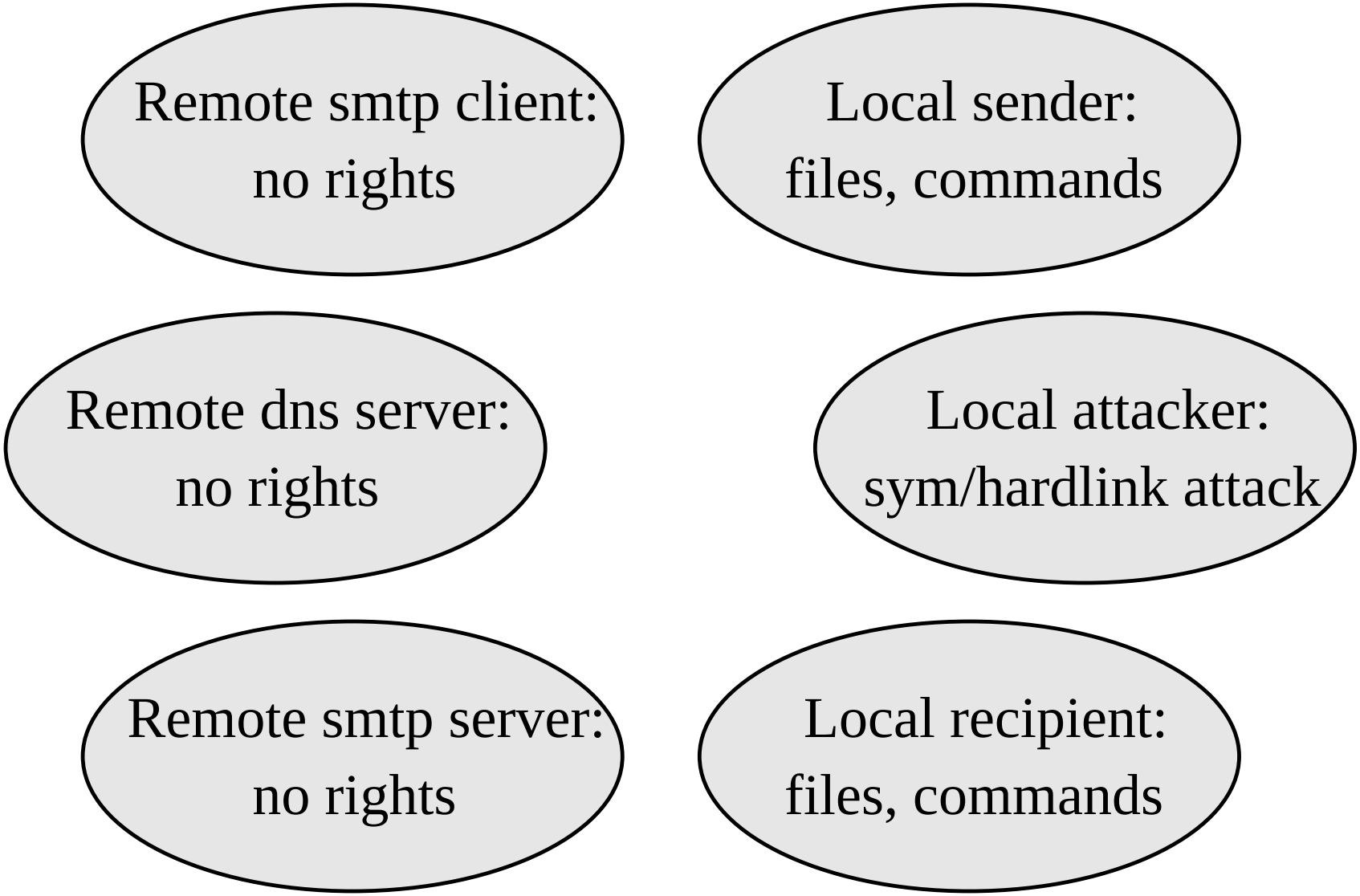
www-server.fig

WWW browser: two rights domains



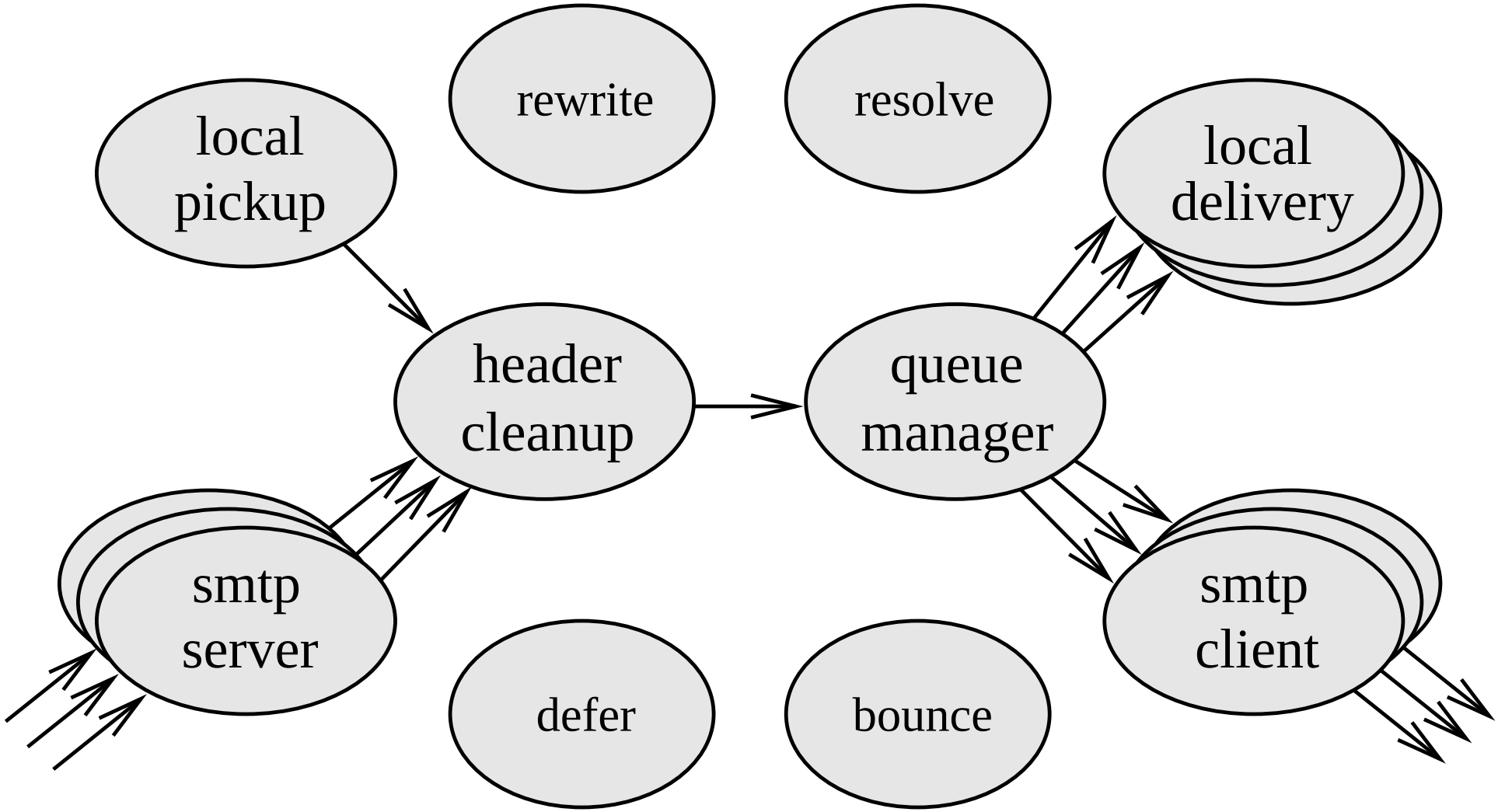
www-client.fig

Mail software: many rights domains



mail-boundaries.fig

Wietse’s mailer architecture



architecture.fig

Wietse’s mailer primary goals

- Wide deployment by giving it away
- Compatibility
- Performance
- Security
- Flexibility
- Reliability
- Example for book with Dan

goals.fig

Compatibility

All the good things from sendmail, none of the pain

- /etc/aliases, NIS aliases (TODO)
- /var/spool/mail/user, /var/mail/user, .lock files
- $HOME/.forward
- Delivery to /file/name
- Delivery to "| command"
- No sendmail.cf file

Performance

Three times faster than qmail (common case)

- From network to single local recipient
- From network to single remote recipient

At least as fast as qmail (special case)

- From network to many remote recipients

performance.fig

Security

Multiple layers of defense against intrusion

- Almost every program runs in chroot/low privilege jail
- No set-uid programs
- No /tmp race conditions
- No trust in queue file contents
- No trust in messages from other mail processes
- No remote data in shell variables

Reliability

Designed to behave rationally under stress

- Limited number of smtp/smtpd/etc. processes
- Limited nr. of connections from/to the same site (TODO)
- Controlled use of memory resources
- Back off when the host runs out of resources
- Back off in case of local mailer configuration problems
- Back off in case of local mailer software bugs

reliability.fig

SPAM mail controls

Basic spam controls:

- Mail relay control (default: from/to own network/domain)
- SMTP client blacklisting (name/domain/address/network)
- Sender domain blacklisting

TODO: support for local policies:

- Little programming language for customizable policies
- Pattern-based filtering (envelope/header/body)

spam-control.fig

What’s in a name

- vmail (charles palmer)
- blackmail (dan farmer)
- mx (wietse)
- vapormail (dan bernstein)
- vm (wietse)
- venemail, wail, venomail...

Wietse’s mailer status and future plans

- Alpha release done early January
- First general release 2Q1998
- Support several releases
- Won’t run on Windows, but might grow a GUI interface for configuration/administration
- More info on: http://wzv.win.tue.nl/vmailer/