NAME

smrsh − restricted shell for sendmail

SYNOPSIS

smrsh −c command

DESCRIPTION

The *smrsh* program is intended as a replacement for *sh* for use in the ‘‘prog’’ mailer in *sendmail*(8) configuration files. It sharply limits the commands that can be run using the ‘‘|program’’ syntax of *sendmail* in order to improve the over all security of your system. Briefly, even if a ‘‘bad guy’’ can get sendmail to run a program without going through an alias or forward file, *smrsh* limits the set of programs that he or she can execute.

Briefly, *smrsh* limits programs to be in the directory /usr/adm/sm.bin, allowing the system administrator to choose the set of acceptable commands, and to the shell builtin commands ‘‘exec’’, ‘‘exit’’, and ‘‘echo’’. It also rejects any commands with the characters ‘`’, ‘<’, ‘>’, ‘;’, ‘$’, ‘(’, ‘)’, ‘\r’ (carriage return), or ‘\n’ (newline) on the command line to prevent ‘‘end run’’ attacks. It allows ‘‘||’’ and ‘‘&&’’ to enable commands like: ‘‘"|exec /usr/local/bin/procmail -f- /etc/procmailrcs/user || exit 75"’’

Initial pathnames on programs are stripped, so forwarding to ‘‘/usr/ucb/vacation’’, ‘‘/usr/bin/vacation’’, ‘‘/home/server/mydir/bin/vacation’’, and ‘‘vacation’’ all actually forward to ‘‘/usr/adm/sm.bin/vacation’’.

System administrators should be conservative about populating /usr/adm/sm.bin. Reasonable additions are *vacation*(1), *procmail*(1), and the like. No matter how brow-beaten you may be, never include any shell or shell-like program (such as *perl*(1)) in the sm.bin directory. Note that this does not restrict the use of shell or perl scripts in the sm.bin directory (using the ‘‘#!’’ syntax); it simply disallows execution of arbitrary programs.

COMPILATION

Compilation should be trivial on most systems. You may need to use −DPATH=\"*path*\" to adjust the default search path (defaults to ‘‘/bin:/usr/bin:/usr/ucb’’) and/or −DCMDBIN=\"*dir*\" to change the default program directory (defaults to ‘‘/usr/adm/sm.bin’’).

FILES

/usr/adm/sm.bin − directory for restricted programs

SEE ALSO

sendmail(8)