Puzzle of the Day

October 17, 2016

The program *sendmail* is a message transport agent; that is, it moves mail from one host to another. It also logs each use in the syslog file. One day, I observed the following entries:

```
Oct 12 06:14:08 nob sendmail[18680]: setsender: /dev/null: invalid or unparseable,
    received from unknown.example.edu [10.2.3.4]
Oct 12 06:14:15 nob sendmail[18680]: GAA18680: /bin/sed... Cannot mail directly to files
Oct 12 06:14:51 nob sendmail[18680]: GAA18680: from=MAILER-DAEMON, size=18, class=0, pri=30018,
    nrcpts=1, msgid=<199610280614.GAA18680@nob>, proto=SMTP, relay=unknown.example.edu [10.2.3.4]
Oct 12 06:14:52 nob sendmail[18682]: GAA18680: to=nobody, delay=00:00:44, mailer=local, stat=Sent
```

The next entry was:

```
Oct 12 06:14:539 nob sendmail[18682]: GAA18681: to=<decode>, from=</dev/null>, delay=00:00:44,
    mailer=prog, stat=Sent
```

1. What is suspicious about the first set of syslog entries? What do you think the author of the first mail message was trying to do? Did it work?
2. Given that the decode address passes a message to the *uudecode*(1) program, which turns a text file into a binary, sets permission modes as indicated in the mail header, and installs it where the mail header says, does this entry indicate a problem? Why or why not?
3. What fundamental problem do these illustrate?