TechWeb.com, 2004.10.19:

“Fingerprint system for border security is criticized

“US-VISIT, the federal government’s multibillion dollar effort to create a ‘virtual border’ monitored by computer networks, was criticized Tuesday by Congressman Jim Turner, D-Texas, who released a 130-page report on the U.S. Department of Homeland Security’s (DHS) management of the nation’s southern border.

“And, in a letter to DHS Secretary Tom Ridge, Turner said terrorists could slip through the US-VISIT's two-fingerprint system. Turner cited a study by Stanford University researchers who said only three of four persons can be identified by the system. The congressman favors a 10-fingerprint system.

"Turner, who is the ranking member of the House Select Committee on Homeland Security, introduced the report, which called for the transformation of the U.S. Southern Border.

" 'DHS has failed to deploy adequate technology to help screen the millions of people, thousands of vehicles, and tons of cargo that cross the Southern Border,' the report stated. 'Little planning and inadequate funding have gone into technological advancements to modernize the border. Much of the technology found on the Southern Border is over 25 years old.'

"Republican congressmen responded to Turner's report by saying it was an example of partisan politics."

Assignment due 2004.10.15: read textbook Chapter 6 pages 233–244.

Assignment due 2004.10.18: read textbook Chapter 6 pages 244–253.

Assignment due today: read textbook Chapter 6 pages 254–263.

Assignment due 2004.10.22: read textbook Chapter 6 pages 263–276.

Details of the man attack

Joe creates a fake manual page:

```
    mkdir -p /home/joe/man/man1
    vi /home/joe/man/man1/pwd.1
```

Joe runs the `man` program:

```
    env MANPATH=/home/joe/man \
    man pwd
```

`man` looks in `$MANPATH`
(i.e., in `/home/joe/man`),
finds Joe's `pwd.1`,
converts it to screen format,
and displays the converted result.

The `man` program also
saves the converted page in
`/var/cache/man/man1/pwd.1`.
It can do this because it's setuid.

Bill then reads the manual:

```
    man pwd
```

The `man` program finds
`/var/cache/man/man1/pwd.1`
and displays it for Bill.

Oops! That's Joe's page.
Joe controls what Bill sees.

Fix: When `man` uses `$MANPATH`,
it no longer caches converted pages
in `/var/cache/man`.

Simpler fix: System administrator
converts all manual pages
upon installation, whether or not
they'll actually be read.
No need for `man` to be setuid.

Another setuid security hole

Sendmail bug fixed 1996.11.17:

```
    execv(argv[0],argv);
```

What is this? Why is it a bug?

When Sendmail starts,
it reads several configuration files.
Sendmail can run for days
handling thousands of messages.
What if configuration changes?

User can tell Sendmail
to re-read configuration.
How does Sendmail do this?
By restarting itself.