Graded lab assignment: Memory safety

1 Overview

In this exercise, you will analyze part of `psutils`.

Description: PSUtils is a collection of useful utilities for manipulating PostScript documents. Programs included are `psnup`, for placing out several logical pages on a single sheet of paper, `psselect`, for selecting pages from a document, `pstops`, for general imposition, `psbook`, for signature generation for booklet printing, and `psresize`, for adjusting page sizes.

Homepage: `http://www.knackered.org/angus/psutils/`

In the version you are given, a bug that has been introduced into the source code of `psselect`. Your job is to diagnose the defect and to fix it. If you try `psselect` on some examples, you will find out that the buggy version does not produce the correct output.

1.1 Installation, running tests

1. Unpack the sources:
   ```
   tar -xzf psutils.tar.gz
   cd psutils/
   ```
2. Compile the sources with `-g` (debug information):[1]
   ```
   make -f Makefile.unix
   ```
   Compilation will generate some compiler warnings, which you can ignore.
3. Run the tool, for example:
   ```
   ./psselect -h
   ```

1.2 Valgrind usage

If you run the tests, everything looks fine. Let's try valgrind:

```
valgrind ./psselect [arguments that produce a problem]
```

If you use valgrind to run psselect with the right options on an example, you will see an error trace like this:

```
==2863== Memcheck, a memory error detector
==2863== Copyright (C) 2002-2017, and GNU GPL'd, by Julian Seward et al.
==2863== Using Valgrind-3.14.0.GIT and LibVEX; rerun with -h for copyright info
==2863== Command: ./psselect -p1 /tmp/valgrind.ps /tmp/out.ps
==2863==
==2863== Conditional jump or move depends on uninitialised value(s)
==2863==    at 0x100002504: main (psselect.c:182)
==2863==
  ...
==2863==
==2863== HEAP SUMMARY:
==2863==     in use at exit: 27,204 bytes in 166 blocks
==2863==   total heap usage: 182 allocs, 16 frees, 33,348 bytes allocated
==2863==
```

[1] The original Makefile.unix has been modified in two ways: (1) `CFLAGS` now includes `-g` so valgrind can display line numbers. (2) The path to Perl is now `/usr/bin/perl` (instead of `/usr/local/bin/perl`).