Targets

This page summarizes some of the work that students have done during the course.

Software fuzzed

For the most part fuzzing targets were recent software, with a few deliberately old ones (not all of which actually crashed despite this). Coverage included 6 operating systems, mostly image viewers, some PDF viewers and image metadata viewers, office software, self-written software, browsers and curl (fuzzed URLs), ffmpeg, audio players, file compression and some command-line tools. Two students fuzzed software of their own and didn't crash those - but the image viewer crashed the X session instead, which strikes me as doubly cool.

This is a quickly compiled list of stuff that got fuzzed and best results where available (pardon me if the names or assumption of Linux, which is the default for everything below Mac OS X stuff, are wrong, I've learned these last few days that the world is full of image viewers I have never heard of).

- Android Gallery (crash, sudden restart), QuickPic, Photos
- Sailfish's default image viewer
- Windows Photo Viewer, XP's Windows Explorer (crash via thumbnails), Picasa ('fatal error'), ACDSee on XP, SumatraPDF (crash), Fast Stone Image Viewer (crash and hang), vlc (crashes)
- FreeBSD: Eye of Gnome and xv
- Mac OS X Finder and preview, Gwenview (hang)
- Eye of MATE, GThumb, GIMP, Pinta, feh, Comicseer, ristretto, GLiv (momentary hang), gpicview, GQview, thunar/tumblerd (potential for local DoS), GPicView (stack overflow, strange library call error), asciiview (4 unique crashes), sxiv, F-Spot (unreproduceable crash, one image looking different every time it's opened), Imagemagick, KDE desktop background randomizer, mate-image-viewer, Gwenview
- exiftags (floating point exceptions), rdjpgcom, imageinfo, ImageMagick 'convert', file
- Konqueror (unreproduceable crashes), Firefox, Google Chrome
- Nautilus (unreproduceable crash on fuzzed image dir viewing)
- Okular (crashes, prolonged hangs), Adobe Reader (full GUI freeze), Evince (several crashes)
- Misc: Ffmpeg, vlc, Banshee, OpenOffice, LibreOffice, gtar, bc, Dia (crash), curl (segfaults)
- own HTTP server software
- own image viewer software (crashed X)

Looks like image viewers did pretty well, PDF viewers not so great.

Tools reviewed

The tool reviews consisted of mostly static analysers, I've tried to munge the others into some parenthesed category to give some idea:

- Black Duck (keeping track of OSS components) x 3
- Checkmarx x 3
- Chucky (research tool, anomaly-detection based missing check finder)
- Clang
- Coverity x 4
- Codenomicon Defensics x 2 (fuzzer)
- Findbugs x 3
- Metasploit x 3 (exploit toolkit and vulnerability scanner)
- Nessus x 4 (network analysis)
- Purify
- RATS
- Microsoft's SDL threat modelling tool x 2
- Splint
- Veracode SAST
- Webinspect (web scanner)
- XSSer (finding cross-site scripting vulnerabilities)

(The reviews plus two general overviews and a summary overview from avs have been packaged for distribution via Moodle to course participants.)