fuzzyDuck.sh

iOS Fuzzin Wrapper Script

Who am i?

- isa56k
- Hobbiest hacker, bit more than a skiddie but long way from l33t... (Workin on it)!
- Do a little bit of Obj C development and have been doing MDM stuff for a few years.
- t:@isa56k ~ e:me@isa56k.com ~ w:www.isa56k.com

What is fuzzyDuck?

- fuzzyDuck.sh is a bash script wrapper for zzuf
- Based on the examples in the iOS Hackers Handbook & stuff I learnt in #OpenJailbreak IRC
- Designed to automate the fuzzing process and help find crashes and save for later inspection

Where can you get it?

- Download it from github:
- https://github.com/isa56k/fuzzyDuck
- Designed to be run on a jailbroken iOS device

How do you use it?

- Jailbreak Device, install OpenSSH, APT 0.7 Strict from cydia.
- Download // Copy to device // run
  - **./fuzzyDuck.sh <filename> <url> <port> <sleep>**
  - **./fuzzyDuck.sh fuzzThis.mov http://localhost 3000 15**
- Use screen to keep terminal session going. Can reconnect if ssh connection drops.

What is it doing? (1/2)

- Checks for required software, downloads and installs (apt-get, wget, sbopenurl, lighttpd, zzuf)
- Creates a test cases directory and a crashes directory
- Starts a small http server to serve up test case

What is it doing? (2/2)

- Loops creating new test cases with zzuff:
  - zzuf -s $seed -r 0.0001:0.001 < $testfile > $testcasedir/$testcase
- Then tests using sbopenurl to open testcase.
- If it finds crash copies test case and crash dump to crashes directory for later inspection.
- Keeps going till it falls over (kernel panic) or is killed off (ctrl+c).

Issues :(

- At the moment doesn't capture kernel panics / all crashes.
- Only looks for crash in:
  - /private/var/mobile/Library/Logs/CrashReporter/LatestCrash.plist
- Should also capture kernel panics from:
  - /private/var/mobile/Library/Logs/CrashReporter/Panics

What next?

- Fix the issues!
- Automate recovery from a kernel panic / reboot so that allows testing to continue uninteruppted
- Copy crash dumps to a central server that can then be reviewed with “crash wrangler” or similar?

Suggestions / Quetions?

- HELP! Always room for improvement!
- Happy to incorporate others ideas.
- Let me know how it works for you?