Portland State UNIVERSITY

Maseeh College of Engineering and Computer Science

Clang Randstruct Project

Meeting Name: **Requirements Elicitation**	Date: **11/02/2018**

Attendees: (Black=present, Red=absent, Blue=scribe, Green=not required)

Kees Cook (m)	**Bart Massey (m)**	**Tim Pugh (m)**
Connor Kuehl (m)	**Cole Nixon (m)**	**Nikk Forbus (m)**
Jordan Cantrell (m)	**James Foster (m)**	**Jeff Takahashi (m)**

Meeting Agenda & Summary

1) Full Randomization
    a) All structures marked with "__randomize_layout" have their field positions randomized, including bit fields.
        i) Reproducible random number (same seed needs to be saved as part of the build)
        ii) Programs report field location manually (structure layout in gcc happens before plugin invocation)

2) Performance-sensitive randomization (**possible stretch**)
    a) Best-effort limit randomization to cache-line (64 byte) size regions, keep adjacent bit-fields together.
3) Automatic structure selection (**possible stretch**)
    a) Find structures that should be automatically selected (for example, structures of entirely function pointers), disabled with "__no_randomize_layout".
4) Regression tests
    a) Since the randomization must be stable from source-to-source, the randomization seed needs to be externally recorded (i.e. it is a build artifact).
    b) Regression tests to check all the corner cases should be built and included in the implementation (i.e. hooked to the standard LLVM/Clang regression tests)

5) **Publish this, regardless of upstream acceptance**

6) **Goal: upstream in LLVM/Clang (stretch)**
    a) Submit work upstream for review
    b) Implement changes based on feedback
    c) Repeat until accepted into LLVM/Clang upstream

7) Kees -- possibly assist in finding right person to ask a question to in the event of us getting blocked

Full Random → Regression testing → upstream

Automatic structure selection → performance randomization

Sign off:

Sponsor: Kees Cook

Team lead: Tim Pugh

Member: Connor Kuehl

Member: Jeff Takahashi