Bindle: Automatic Harness Generation

Bill Bierman, GrammaTech
https://grammatech.github.io/

Harnesses are an important part of fuzz testing: connecting fuzzing software to the target in a meaningful way. Manual creation of a harness can take hours, if not days, and is an obstacle for many analysts.

Bindle removes this obstacle by generating harnesses automatically in minutes!

Record → **Create** → **Run**

Observe execution

Configure and refine harness

Mutable blob for fuzzer

Goals:

- Fuzzer agnostic
- Automatic creation of harnesses and seeds
- Unlock fuzzing of multiple inputs
- Portability: Remove equipment bottleneck
- *Dramatically* increase analyst efficiency

Use Cases:

- Cyber-physical systems
- Network applications
- Foreign materiel exploitation
- Applications with multiple inputs
- Convert unit tests to seed inputs

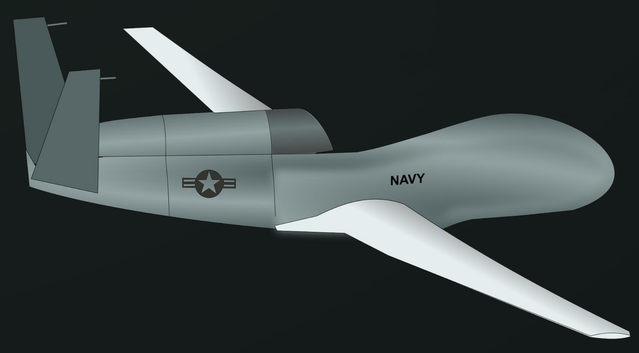
Example: UAV

Harness generated with test flight sensor data, recorded at test range, brought to home base

Fuzzing reveals system-of-systems weakness:

- Ground radio jamming
- Satellite radio jamming
- GPS spoofing

Result: *Hijack!*



GRAMMATECH

THE TWENTY-THIRD ANNUAL
HIGH CONFIDENCE SOFTWARE AND SYSTEMS CONFERENCE
MAY 8 -10, 2023 | http://cps-hcss.org