Sefcom/BSS meeting

Source-to-source code transformations

Biodesign Institute
Arizona State University

Problem and Hypothesis

- There are many un-repaired bugs that current APR tools can not patch.
- There is a discrepancy between the granularity of the mutation operation and the required granularity of the repair.

Transformations

- Decouple assignment and declaration.
- Extract the content of function calls.
- Extract function calls from conditional statements.
- Add in repair ingredients (Pemma fix this wording)

Example

```
/* Original buggy code */
if (cgc_receive_delim(0, string, 128, '\n') != 0)
    return -1;
------------------------------------------------
/* After transformations and successful APR */
  int tlv1 ;
...
  tlv3 = 0;
  tlv4 = string;
  tlv5 = sizeof(string);
  tlv6 = (char )'\n';
  tlv1 = cgc_receive_delim(tlv3, tlv4, (cgc_size_t const   )tlv5, tlv6);
  if (tlv1 != 0) {
    return (-1);
  }
```

Biodesign Institute
Arizona State University

Progress

- Case study: Found a “high quality repair” for the CGC challenge binary ***Palindrome***.
- Preparing to run on the entire CGC challenge binary set.
  - We have identified 6 more CGC tests that transformations will aid.
  - Want to find more “quality” repairs.