The Monkey Debugging System

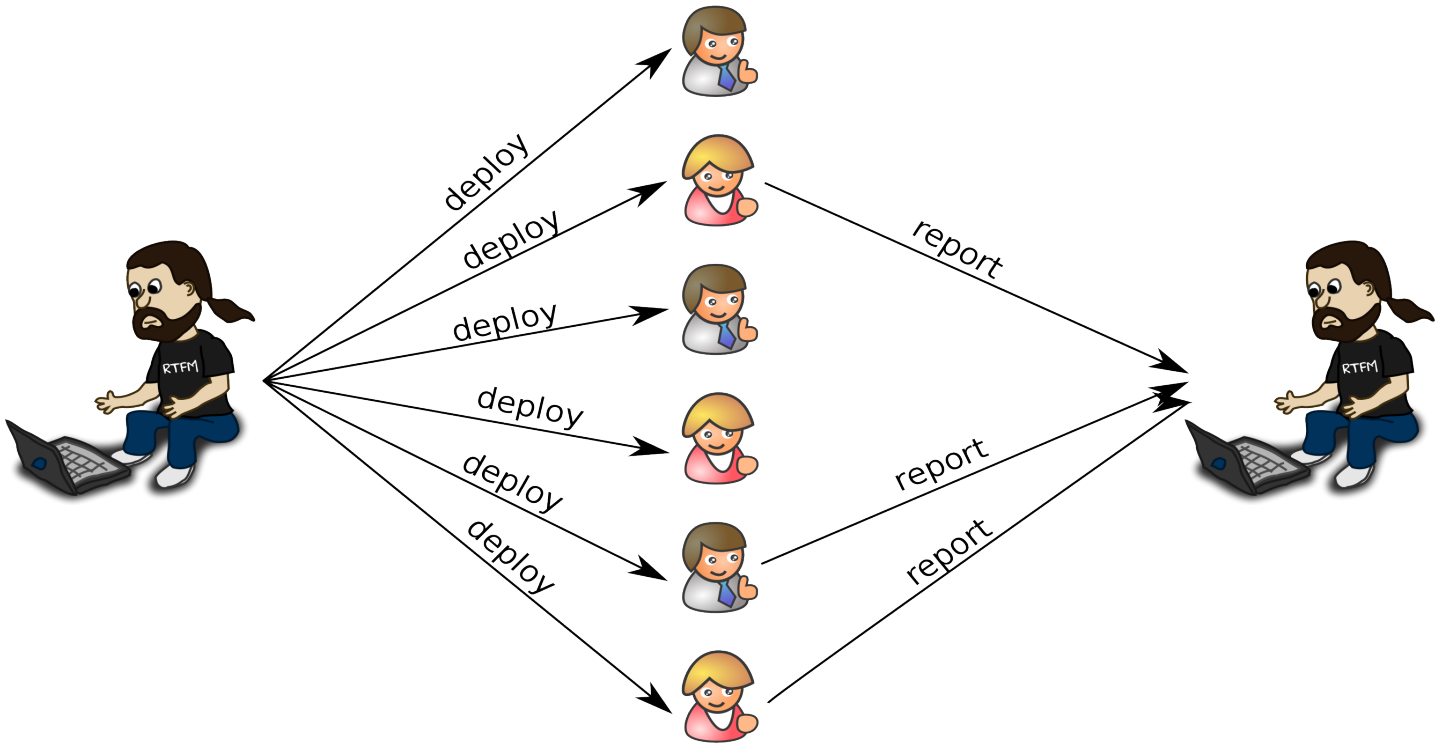
Generating Useful Bug Reports Automatically

Markus Teich

Related Work and Problems

- Access to users machine
  - → Automatic crash report generation
- Apport, Windows Error Reporting, Google Breakpad, …
- Report content
  - Too verbose (Private Data)
  - Too superficial (Not useful)
- Amount of reports

System Overview



Cparser
Seaspider

Pathologist

Entomologist
Scrutinizer

Cparser/Seaspider

- Static code analysis
- Find all expressions in syntax tree
- Filter out critical expressions
- Outputs expression database in sqlite format

Table: Expression

	expr_ID	file_name	expr_syntax	start_lineno	end_lineno
86391	114801	tor_main.c	tor_git_revision	10	32767
86392	114802	tor_main.c	argc	29	31
86393	114803	tor_main.c	argv	29	31

Pathologist

- Run client application within gdb
- Catch SIGSEGV, SIGABRT, SIGFPE, SIGBUS
- Evaluate relevant expressions post mortem
- Output result in json format
- Run custom script to submit report

Entomologist

- Distance heuristic
- Modified K-Clustering
  - No mean report → use representative system
  - Initial centroids choice
- Output representatives for each cluster / bug
- min inter-cluster and max in-cluster distance

Scrutinizer

```
839       memcpy(extended_desc_cookie, client->descriptor_cookie,
840              REND_DESC_COOKIE_LEN);
841       extended_desc_cookie[REND_DESC_COOKIE_LEN] =
842         ((int)s->auth_type - 1) << 4;
843       if (base64_encode(desc_cook_out, 3*REND_DESC_COOKIE_LEN_BASE64+1,
844                         extended_desc_cookie,
845                         REND_DESC_COOKIE_LEN+1) < 0) {
846         log_warn(LD_BUG, "Could not base64-encode descriptor cookie.");
847         goto err;
848       }
849       desc_cook_out[strlen(desc_cook_out)-3] = '\0'; /* Remove A= and
850                                                         newline. */
851       tor_snprintf(buf, sizeof(buf),"%s.onion %s # client: %s\n",
852                    service_id, desc_cook_out, client->client_name);
853     }
854
855     if (fputs(buf, hfile)<0) {
856       log_warn(LD_FS, "Could not append host entry to file: %s",
857                strerror(errno));
858       goto err;
859     }
860   } SMARTLIST_FOREACH_END(client);
861
862   finish_writing_to_file(open_cfile);
863   finish_writing_to_file(open_hfile);
864
865   goto done;
866 err:
867   r = -1;
868   if (open_cfile)
869     abort_writing_to_file(open_cfile);
870   if (open_hfile)
871     abort_writing_to_file(open_hfile);
872 done:
873   tor_strclear(client_keys_str);
874   tor_free(client_keys_str);
875   strmap_free(parsed_clients, rend_authorized_client_strmap_item_free);
876
877   memset(cfname, 0, sizeof(cfname));
878
879   /* Clear stack buffers that held key-derived material. */
880   memset(buf, 0, sizeof(buf));
881   memset(desc_cook_out, 0, sizeof(desc_cook_out));
882   memset(service_id, 0, sizeof(service_id));
883   memset(extended_desc_cookie, 0, sizeof(extended_desc_cookie));
884
885   return r;
886 }
```

Symbolic stack trace

function	file:line
tor_strclear	util.c:663
rend_service_load_auth_keys	rendservice.c:873
rend_service_load_keys	rendservice.c:687
rend_service_load_all_keys	rendservice.c:628
options_act	config.c:1551
set_options	config.c:754
options_init_from_string	config.c:4786
options_init_from_torrc	config.c:4643
tor_init	main.c:2333
tor_main	main.c:2646
__libc_start_main	libc-start.c:226
No source code available	

Bug detected: null pointer access

Expression syntax	value
s	<optimized out>
hfname	0x7fffffffcb40 "/tmp/hs /hostname"
strmap_new	{strmap_t *(void)} 0x55555563f5d0 <strmap_new>
tor_snprintf	{int (char *, size_t, const char *, ...)} 0x555555639320 <tor_snprintf>
cfname	[512]
sizeof(cfname)	512
s->directory	
client_keys_str	0x0

Demo

Survey results

Correct answers	tor-04	tor-03	st-01
Backtrace	6 / 8	3 / 8	0 / 5
Core dump	0 / 5	3 / 5	1 / 11
Monkey	5 / 8	5 / 8	0 / 5

Median time to find correct answer	tor-04	tor-03	st-01
Backtrace	312 s	238 s	
Core dump		271 s	364 s
Monkey	106 s	359 s	

- Monkey can help to find the correct bug
- Monkey can be faster
- Core dump is too verbose?

Future Work

- Deploy on GNUnet, … your Application?
- Collect reports to tweak Entomologist
- Integrate Entomologist into Scrutinizer
- Valgrind / reverse execution