Rust + Unsafe code

Diane Hosfelt | @avadacatavra

July 8, 2017

Rust safety guarantees– type safety! memory safety!

Prevents by default:

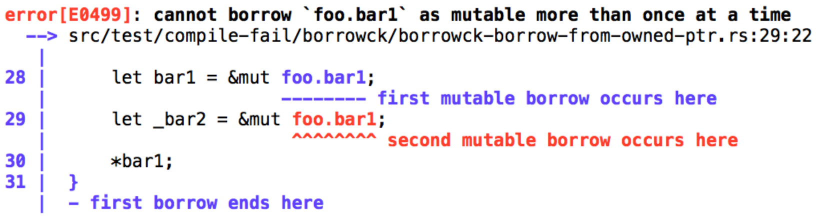
- Dangling pointers
- Data races
- Integer overflow (default in debug builds)
- Buffer overflow
- Iterator invalidation

Integer overflow and buffer overflow prevention require runtime checks.

Buffer overflow checks minimized idiomatically by iterators

wtf does 'unsafe' mean

Rust has a *borrow checker*:



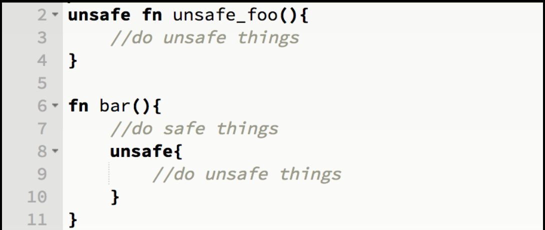
```
error[E0499]: cannot borrow `foo.bar1` as mutable more than once at a time
  --> src/test/compile-fail/borrowck/borrowck-borrow-from-owned-ptr.rs:29:22
   |
28 |      let bar1 = &mut foo.bar1;
   |                      -------- first mutable borrow occurs here
29 |      let _bar2 = &mut foo.bar1;
   |                       ^^^^^^^^ second mutable borrow occurs here
30 |      *bar1;
31 |  }
   |  - first borrow ends here
```

- each value is uniquely owned by a single variable *x*
- if that value is assigned to a different variable *y*, the value has moved to *y*
- now *y* owns the value, and compiler aborts if *x* tries to access the value
- values can be immutable borrowed any number of times, but only one mutable reference is allowed

you still haven’t explained what ’unsafe’ is

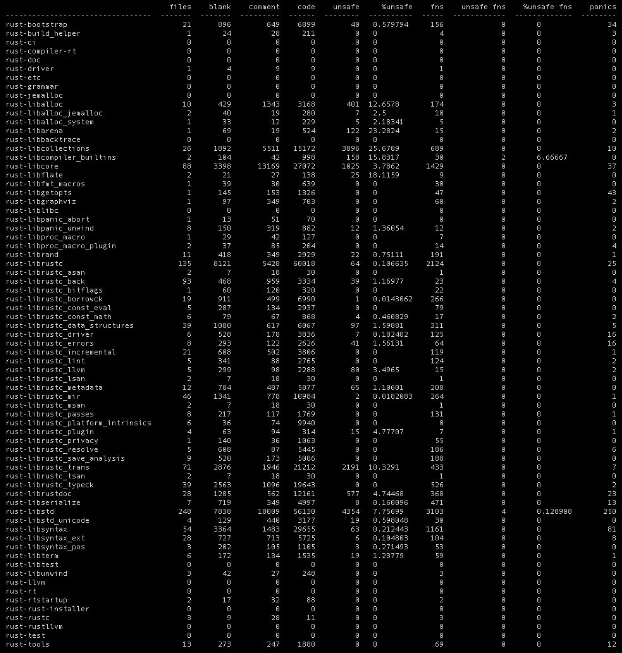
You can’t do everything in ’safe’ blocks. Sometimes you need to violate these rules.

- dereference raw pointers
- call unsafe functions (including C functions)
- implement unsafe traits
- mutate statics



```rust
unsafe fn unsafe_foo(){
    //do unsafe things
}

fn bar(){
    //do safe things
    unsafe{
        //do unsafe things
    }
}
```



```
                                     files    blank    comment    code    unsafe     %unsafe    fns    unsafe fns    %unsafe fns    panics
---------------------------------  -------  -------  ---------  ------  --------  ----------  -----  ------------  -------------  --------
rust-bootstrap                          21      896        649    6899        40   0.579794     156             0  0                    34
rust-build_helper                        1       24         28     211         0   0              4             0  0                     3
rust-ci                                  0        0          0       0         0   0              0             0  0                     0
rust-compiler-rt                         0        0          0       0         0   0              0             0  0                     0
rust-doc                                 0        0          0       0         0   0              0             0  0                     0
rust-driver                              1        4          9       9         0   0              1             0  0                     0
rust-etc                                 0        0          0       0         0   0              0             0  0                     0
rust-grammar                             0        0          0       0         0   0              0             0  0                     0
rust-jemalloc                            0        0          0       0         0   0              0             0  0                     0
rust-liballoc                           10      429       1343    3168       401  12.6578       174             0  0                     3
rust-liballoc_jemalloc                   2       40         19     280         7   2.5           10             0  0                     1
rust-liballoc_system                     1       33         12     229         5   2.18341        5             0  0                     0
rust-libarena                            1       69         19     524       122  23.2824        15             0  0                     2
rust-libbacktrace                        0        0          0       0         0   0              0             0  0                     0
rust-libcollections                     26     1892       5511   15172      3896  25.6789       689             0  0                    10
rust-libcompiler_builtins                2      104         42     998       158  15.8317        30             2  6.66667               0
rust-libcore                            88     3398      13169   27072      1025   3.7862      1429             0  0                    37
rust-libflate                            2       21         27     138        25  18.1159         9             0  0                     0
rust-libfmt_macros                       1       39         30     639         0   0             30             0  0                     0
rust-libgetopts                          1      145        153    1326         0   0             47             0  0                    43
rust-libgraphviz                         1       97        349     703         0   0             60             0  0                     2
rust-liblibc                             0        0          0       0         0   0              0             0  0                     0
rust-libpanic_abort                      1       13         51      70         0   0              0             0  0                     0
rust-libpanic_unwind                     8      150        319     882        12   1.36054       12             0  0                     2
rust-libproc_macro                       1       29         42     127         0   0              7             0  0                     0
rust-libproc_macro_plugin                2       37         85     204         0   0             14             0  0                     4
rust-librand                            11      418        349    2929        22   0.75111      191             0  0                     1
rust-librustc                          135     8121       5428   60018        64   0.106635    2124             0  0                    25
rust-librustc_asan                       2        7         18      30         0   0              1             0  0                     0
rust-librustc_back                      93      468        959    3334        39   1.16977       23             0  0                     4
rust-librustc_bitflags                   1       60        120     320         0   0             22             0  0                     0
rust-librustc_borrowck                  19      911        499    6990         1   0.0143062    266             0  0                     0
rust-librustc_const_eval                 5      287        134    2937         0   0             79             0  0                     0
rust-librustc_const_math                 6       79         67     868         4   0.460829      17             0  0                     2
rust-librustc_data_structures           39     1080        617    6067        97   1.59881      311             0  0                     5
rust-librustc_driver                     6      528        178    3836         7   0.182482     125             0  0                    16
rust-librustc_errors                     8      293        122    2626        41   1.56131       64             0  0                    16
rust-librustc_incremental               21      608        502    3806         0   0            119             0  0                     1
rust-librustc_lint                       5      341         88    2765         0   0            124             0  0                     2
rust-librustc_llvm                       5      299         98    2288        80   3.4965        15             0  0                     2
rust-librustc_lsan                       2        7         18      30         0   0              1             0  0                     0
rust-librustc_metadata                  12      784        487    5877        65   1.10601      208             0  0                     0
rust-librustc_mir                       46     1341        778   10984         2   0.0182083    264             0  0                     1
rust-librustc_msan                       2        7         18      30         0   0              1             0  0                     0
rust-librustc_passes                     8      217        117    1769         0   0            131             0  0                     1
rust-librustc_platform_intrinsics        6       36         74    9940         0   0              0             0  0                     0
rust-librustc_plugin                     4       63         94     314        15   4.77707        7             0  0                     1
rust-librustc_privacy                    1      140         36    1063         0   0             55             0  0                     0
rust-librustc_resolve                    5      608         87    5445         0   0            186             0  0                     6
rust-librustc_save_analysis              9      520        173    5086         0   0            188             0  0                     0
rust-librustc_trans                     71     2876       1946   21212      2191  10.3291       433             0  0                     7
rust-librustc_tsan                       2        7         18      30         0   0              1             0  0                     0
rust-librustc_typeck                    39     2563       1096   19643         0   0            526             0  0                     2
rust-librustdoc                         28     1285        562   12161       577   4.74468      368             0  0                    23
rust-libserialize                        7      719        349    4997         8   0.160096     471             0  0                    13
rust-libstd                            248     7838      18009   56130      4354   7.75699     3103             4  0.128908            250
rust-libstd_unicode                      4      129        440    3177        19   0.598048      30             0  0                     0
rust-libsyntax                          54     3364       1483   29655        63   0.212443    1161             0  0                    81
rust-libsyntax_ext                      28      727        713    5725         6   0.104803     104             0  0                     8
rust-libsyntax_pos                       3      202        105    1105         3   0.271493      53             0  0                     0
rust-libterm                             6      172        134    1535        19   1.23779       59             0  0                     1
rust-libtest                             0        0          0       0         0   0              0             0  0                     0
rust-libunwind                           3       42         27     248         0   0              3             0  0                     0
rust-llvm                                0        0          0       0         0   0              0             0  0                     0
rust-rt                                  0        0          0       0         0   0              0             0  0                     0
rust-rtstartup                           2       17         32      88         0   0              2             0  0                     0
rust-rust-installer                      0        0          0       0         0   0              0             0  0                     0
rust-rustc                               3        9         28      11         0   0              3             0  0                     0
rust-rustllvm                            0        0          0       0         0   0              0             0  0                     0
rust-test                                0        0          0       0         0   0              0             0  0                     0
rust-tools                              13      273        247    1880         0   0             69             0  0                    12
```

...why did i include the image with the tiny text

Rust's compiler is written in Rust!

This shows the amount of 'unsafe code' in each compiler module

- Lots of them are 0%!
- The worst is rust-libcollections at 25%

How this should actually be done

- simplified AST
- test predicates
- categorize unsafe as FFI or not

Questions?

- avadacatavra 🐦
- avadacatavra
- avadacatavra@mozilla.com
- avadacatavra.github.io/