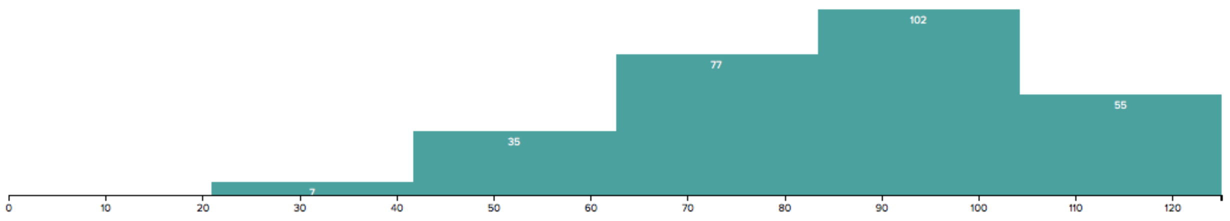
CS107
M Chang & J Zelenski

June 16, 2018

Final Solution



MINIMUM	MEDIAN	MAXIMUM	MEAN	STD DEV
31.0	88.0	124.0	85.78	20.17

The exam was a great testament to all the hard work, growth, and learning that went in this quarter! Bravo! Review your graded final exam on Gradescope and enjoy seeing how far you have come.

Problem 1: Floats

```
NAN -> false
INFINITY -> true
```

`y` has to be sufficiently small relative to x such that when added to x will not register but also large enough that 2*y is enough to get over threshold. For float, ratio of y/x is in range $\mathbf{2^{24}}$ to $\mathbf{2^{23}}$

Epsilon of `FLT_MAX` is 2^{103}, largest int `INT_MAX` is 2^{31}-1 and even 2x washed out in the addition.

Problem 2: Assembly

```
int pinky(long param1, long *param2)
{
    *param2 = param1;
    if (!param1)
       return 107*param1;
    else if (param1 < 0)
       param1 = -param1;
    return pinky(param2[param1] + param1, param2);
 }
```

The tail-recursive call was rewritten into a loop. It will `jne` to the start of the function when `param1` is non-zero.

The original sequence

```
test   %rdi,%rdi
jns    .L2
neg    %rdi
```

became the optimized sequence

```
 mov    %rdi,%rax
 sar    $0x3f,%rax
 xor    %rax,%rdi
 sub    %rax,%rdi
```
The optimized version is a branchless absolute value.

The original instruction
```
imul   $0x6b,%edi,%eax
```
was replaced by
```
 xor    %eax,%eax
```
The original multiply was known to be a multiply against 0, xor used to zero the register instead.

Problem 3: Stack

The call to `getenv` has the rights to all callee-owner registers. `authorize` must use a caller-owned register to preserve state across the call (in this case, base address of username on account)

Shift left by 5 is effectively a multiply by 32 and 32 = `sizeof(struct customer)`
Offset of customer array in struct database is 24 bytes (20 bytes bankname + 4 byte count)

`authorize(-1)` doesn't touch `%rax`, so whether call will succeed or fail is determined by the current value leftover in the register.

`authorize(LONG_MAX)` will exit the function with the count of customers in `%rax`, so as long as there is at least one customer, call succeeds.

The overly-long name corrupted the resume address on stack, crashes when exiting function.

```
confirm_passcode("BANKVAULT7777", '7')
```

This version writes two bytes into cust_code, the digit character '7' and the terminating null. The passcode is the ascii value of digit character '7' could instead by written as 0x37 or 55.

Problem 4: Heap

```
#define INUSE    ~(-1UL >> 1)
#define SIZE     (INUSE - 1)

b->status ^= INUSE;

(long)b->status >= (long)requested
```

It is illegal to do pointer arithmetic (subtraction) on a void *, thus the need to treat as char *.

```
char *one = *(char **)a;

return bsearch(&payload, blocks, nblocks, sizeof(*blocks), cmp);

b->payload == blocks[nblocks - 1].payload
b == &blocks[nblocks - 1]
```

```
b + 1

void coalesce(blockinfo_t *left, blockinfo_t *right)
{
    left->status += right->status;
    memmove(right, right+1, (char *)(blocks+nblocks) - (char *)(right+1));
    nblocks--;
}
```