Trolling with Math

$f(yourMom) = 2d + 1m$

where d = dicks, m = mouth

Trolling with Math

wat

- frank^2
- DC{949,310}
- oCTF

it's pronounced "two," by the way. not "squared."

Trolling with Math

wat

```
 <> We demand guid0h we demand cock!
21:14 <@frank^2> >_r(_tsin(_w('JUST WAGGIN MY DICK'),4,20,50))
21:14 <+omgomglol>                        J U S T  W A G G I N  M Y  D I C K
21:15 <+omgomglol>                           J U S T  W A G G I N  M Y  D I C K
21:15 <+omgomglol>                              J U S T  W A G G I N  M Y  D I C K
21:15 <+omgomglol>                                 J U S T  W A G G I N  M Y  D I C K
21:15 <+omgomglol>                                   J U S T  W A G G I N  M Y  D I C K
21:15 <+omgomglol>                                    J U S T  W A G G I N  M Y  D I C K
21:15 <+omgomglol>                                    J U S T  W A G G I N  M Y  D I C K
21:15 <+omgomglol>                                    J U S T  W A G G I N  M Y  D I C K
21:15 <+omgomglol>                                 J U S T  W A G G I N  M Y  D I C K
21:15 <+omgomglol>                              J U S T  W A G G I N  M Y  D I C K
21:15 <+omgomglol>                           J U S T  W A G G I N  M Y  D I C K
21:15 <+omgomglol>                        J U S T  W A G G I N  M Y  D I C K
21:15 <+omgomglol>                     J U S T  W A G G I N  M Y  D I C K
21:15 <+omgomglol>                  J U S T  W A G G I N  M Y  D I C K
21:15 <+omgomglol>               J U S T  W A G G I N  M Y  D I C K
21:15 <+omgomglol>            J U S T  W A G G I N  M Y  D I C K
21:15 <+omgomglol>         J U S T  W A G G I N  M Y  D I C K
21:15 <+omgomglol>      J U S T  W A G G I N  M Y  D I C K
21:15 <+omgomglol>   J U S T  W A G G I N  M Y  D I C K
21:15 <+omgomglol> J U S T  W A G G I N  M Y  D I C K
21:15 <+omgomglol> J U S T  W A G G I N  M Y  D I C K
21:15 <+omgomglol> J U S T  W A G G I N  M Y  D I C K
21:15 <+omgomglol>   J U S T  W A G G I N  M Y  D I C K
21:15 <+omgomglol>      J U S T  W A G G I N  M Y  D I C K
21:15 <+omgomglol>         J U S T  W A G G I N  M Y  D I C K
21:15 <+omgomglol>            J U S T  W A G G I N  M Y  D I C K
```

some asshole spammer on Twitter has "frank2."

Trolling with Math

wat

- Let's get this out of the way.
- Do you know:
  - ... the basics of organization of assembly?
  - ... function pointers?
  - ... math?

also at about this point in time in making this talk I think I've had, like...

Trolling with Math

oh

YOU'RE FUCKED!

four or five hits or something.

Trolling with Math

How does this shit work?

- Take a block of assembly.
- Allocate some memory somewhere.
- Make a big-ass number relative to the amount of instructions. *Huge*.
- For every assembly instruction:
  - `y = f(x)`
  - mem[y][x] = instruction
- Mark memory as executable.
- Start execution!

Trolling with Math

How does this shit work?

```
MOV   EAX,5355434B
MOV   EBX,20412044
XOR   EAX,EBX
CALL  49434B20
MOV   EDX,EAX
SUB   AX,46
XOR   EAX,41545459
```

```
MOV   EAX,5355434B
  JMP
    MOV   EBX,20412044
     JMP
       XOR   EAX,EBX
      JMP
       CALL  49434B20
       JMP
       MOV   EDX,EAX
       JMP
       SUB   AX,46
     JMP
   XOR   EAX,41545459
```

Trolling with Math

But you're still fucked

- This assumes that there aren't any caveats.
- There are lots of caveats.

seriously though, that episode of South Park was spot-on.

Trolling with Math

But you're still fucked

- Remember why I said you should know about the little stupid intricacies of assembly?
- Here's what's fucked:
  - Your conditional jumps
  - Your register jumps
  - Your jumps
  - You

I apparently have this thing called "racing thoughts."

Trolling with Math

But you're still fucked

- Your jumps are fucked because they're relative.
- JMP BEEFBABE is more like JMP A-FEW-BYTES-BACK-I-DONT-KNOW-MAYBE-ABOUT-30-BYTES-I-GUESS?-GIVE-OR-TAKE?

you think "insomnia" is a bullshit diagnosis?

Trolling with Math

But you're still fucked

- JMP EAX? Good luck figuring out where the fuck that's going accurately.
- Might as well just quit while you're ahead there.

tell me "racing thoughts" doesn't sound completely made up.

Trolling with Math

But you're still fucked

- You're going to have to convert all your JMP SHORTs to JMP PANTs.
- The actual distance from a given jump inside the buffer to another jump is typically bigger than 255.
- So fix that shit.

the doctor's form is like "how do you prefer smoking? blunts? bongs?"

Trolling with Math

Un-fucking yourself

- While you're performing your f(x) loop, keep track of JMP instructions. Store them and their targets off in an array somewhere.
- Once you've finished solving for Y, replace the old offsets with the new ones.
- Congrats! That dick unjammed by a few inches!

personally, I prefer pipes, but being blunted works too.

Trolling with Math

Are you un-fucked yet?

HELL YEAH

see what I did there? it's called alliteration. nnnnailed it.

Trolling with Math

The cool shit

- Now that we have a method for arbitrarily placing the stray assembly instructions, let's have some fun:

```
f(x) = sin(x/freq) * amp
```

I'm trying really, really hard not to say "weed." it's obvious, I know.

Trolling with Math

The cool shit

- This is the formula for a sinewave. Given index X, we get an arbitrary Y value, giving us an X and Y value to place on our plot that ultimately looks like a sinewave.

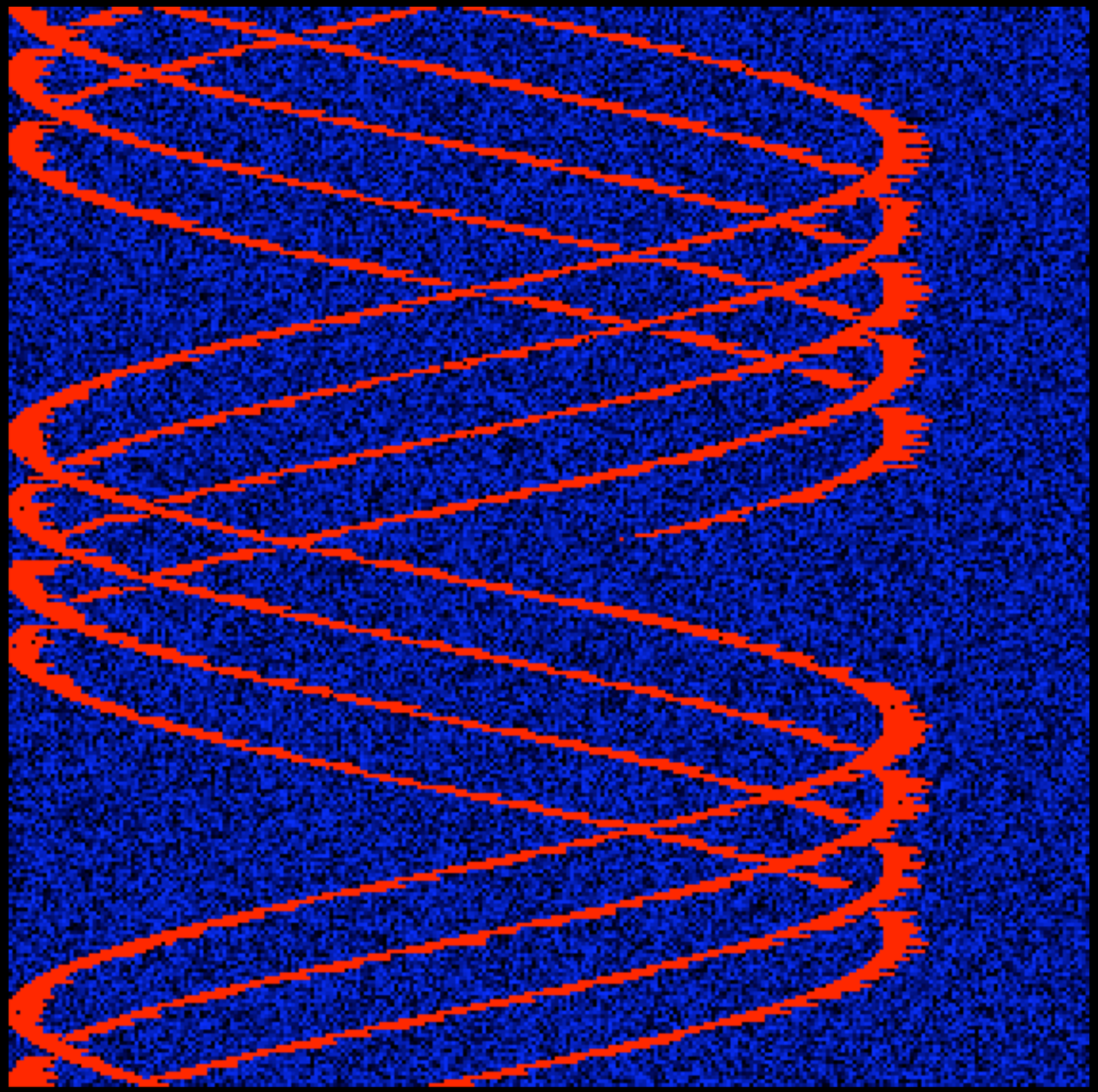
but it totally changed my life. write your congressman!

Trolling with Math

The cool shit

Trolling with Math

BAM



Trolling with Math

Kinda trivial, though

- Tracing from the entry point and following JMP instructions easily breaks this.
- Since you have to arbitrarily link everything together by jumps anyway, you can essentially format your chunks like so:
  - preamble data
  - assembly data
  - post data

I bet that totally fucked with your eyes.

Trolling with Math

Like A Boss

- Considering this, we can add anti-debug instructions to the pre-amble and make the post-amble JMP a more obfuscated one.

that's right. I can troll your vision, too.

Trolling with Math

Type Cookie You Idiot

- Take every assembly instruction that corresponds with a numerical constant and make that the randomized bed of your new code buffer.
- Recursive-traversal disassemblers don't know what the fuck.
- Like OllyDBG, for example.

this also makes scrolling really really annoying.

Trolling with Math

It's Evolution, Baby

- If you can iteratively determine f(x), you can randomly determine it as well.
- While this most certainly changes your entry point, it most definitely irritates the living hell out of someone trying to analyze your code.

holy fuck I HATE it when malware does that, seriously.

Trolling with Math

It's Evolution, Baby

- You can arbitrarily combine the functions as well. Remember, the only important input here is X.
- f(g(x)) works
- g(f(x)) works
- f(a(g(x))) works

so I guess they win, because they're slowing me down and pissing me off.

Trolling with Math

Conclusions

- x86 is a beautiful clusterfuck