week 2

Extremely critical crypto flaw in iOS may also affect fully patched Macs

Coding blunder that exposed sensitive data may still be putting users at risk.

by **Dan Goodin** - Feb 22 2014, 2:45pm EST

http://arstechnica.com/security/2014/02/extremely-critical-crypto-flaw-in-ios-may-also-affect-fully-patched-macs/

Apple promises to fix OS X encryption flaw 'very soon'

The iPhone and iPad maker on Friday issued a fix for its mobile devices, but left its Mac lineup unpatched. But not for long, Apple says.

by **Zack Whittaker** @zackwhittaker / February 22, 2014 7:33 PM PST

http://www.cnet.com/news/apple-promises-to-fix-os-x-encryption-flaw-very-soon/

Apple finally fixes 'gotofail' OS X security hole

After a multiday delay that irked users, Apple has released a system software update for OS X Mavericks that fixes what's become known as the "gotofail" security vulnerability.

by Declan McCullagh @declanm / February 25, 2014 11:00 AM PST

http://www.cnet.com/news/apple-finally-fixes-gotofail-os-x-security-hole/

Description: Secure Transport failed to validate the authenticity of the connection. This issue was addressed by restoring missing validation steps.

```
static OSStatus
SSLVerifySignedServerKeyExchange(SSLContext *ctx, bool isRsa, SSLBuffer signedParams,
                                 uint8_t *signature, UInt16 signatureLen)
{
    OSStatus        err;
    ...
    if ((err = ReadyHash(&SSLHashSHA1, &hashCtx)) != 0)
        goto fail;
    if ((err = SSLHashSHA1.update(&hashCtx, &clientRandom)) != 0)
        goto fail;
    if ((err = SSLHashSHA1.update(&hashCtx, &serverRandom)) != 0)
        goto fail;
    if ((err = SSLHashSHA1.update(&hashCtx, &signedParams)) != 0)
        goto fail;
        goto fail;
    if ((err = SSLHashSHA1.final(&hashCtx, &hashOut)) != 0)
        goto fail;
    ...
fail:
    SSLFreeBuffer(&signedHashes);
    SSLFreeBuffer(&hashCtx);
    return err;

}
```

```
if ((err = ReadyHash(&SSLHashSHA1, &hashCtx)) != 0)
    goto fail;
if ((err = SSLHashSHA1.update(&hashCtx, &clientRandom)) != 0)
    goto fail;
if ((err = SSLHashSHA1.update(&hashCtx, &serverRandom)) != 0)
    goto fail;
if ((err = SSLHashSHA1.update(&hashCtx, &signedParams)) != 0)
    goto fail;
    goto fail;
if ((err = SSLHashSHA1.final(&hashCtx, &hashOut)) != 0)
    goto fail;
```

```
if ((err = ReadyHash(&SSLHashSHA1, &hashCtx)) != 0)
    goto fail;
if ((err = SSLHashSHA1.update(&hashCtx, &clientRandom)) != 0)
    goto fail;
if ((err = SSLHashSHA1.update(&hashCtx, &serverRandom)) != 0)
    goto fail;
if ((err = SSLHashSHA1.update(&hashCtx, &signedParams)) != 0)
    goto fail;
    goto fail;
if ((err = SSLHashSHA1.final(&hashCtx, &hashOut)) != 0)
    goto fail;
```

```
if ((err = SSLHashSHA1.update(&hashCtx, &signedParams)) != 0)
    goto fail;
    goto fail;
```

```
if ((err = ReadyHash(&SSLHashSHA1, &hashCtx)) != 0)
    goto fail;
if ((err = SSLHashSHA1.update(&hashCtx, &clientRandom)) != 0)
    goto fail;
if ((err = SSLHashSHA1.update(&hashCtx, &serverRandom)) != 0)
    goto fail;
if ((err = SSLHashSHA1.update(&hashCtx, &signedParams)) != 0)
    goto fail;
goto fail;
if ((err = SSLHashSHA1.final(&hashCtx, &hashOut)) != 0)
    goto fail;
```

```
if ((err = ReadyHash(&SSLHashSHA1, &hashCtx)) != 0)
    goto fail;
if ((err = SSLHashSHA1.update(&hashCtx, &clientRandom)) != 0)
    goto fail;
if ((err = SSLHashSHA1.update(&hashCtx, &serverRandom)) != 0)
    goto fail;
if ((err = SSLHashSHA1.update(&hashCtx, &signedParams)) != 0)
    goto fail;
goto fail;
if ((err = SSLHashSHA1.final(&hashCtx, &hashOut)) != 0)
    goto fail;
```

gotofail.com

sections start Sun 9/21

to be announced via email by this weekend

office hours

cs50.harvard.edu/hours

assessment

Scope

To what extent does your code implement the features required by our specification?

Correctness

To what extent is your code consistent with our specifications and free of bugs?

Design

To what extent is your code written well (i.e., clearly, efficiently, elegantly, and/or logically)?

Style

To what extent is your code readable (i.e., commented and indented with variables aptly named)?

1 2 3 4 5

1	2	3	4	5
poor	fair	good	better	best

$$\text{scope} \times (\text{correctness} \times 3 + \text{design} \times 2 + \text{style} \times 1)$$

academic honesty

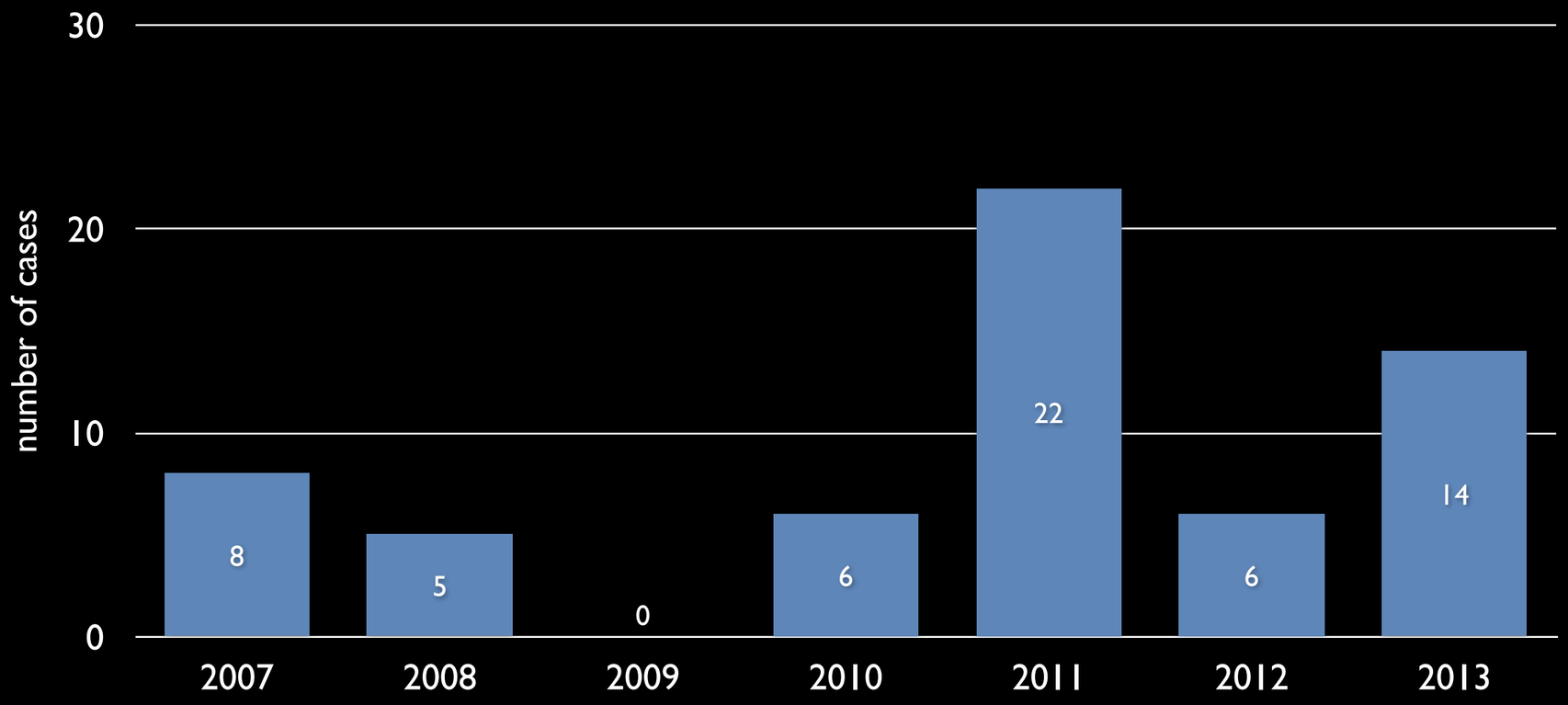
cs50.harvard.edu/syllabus

"Be reasonable."

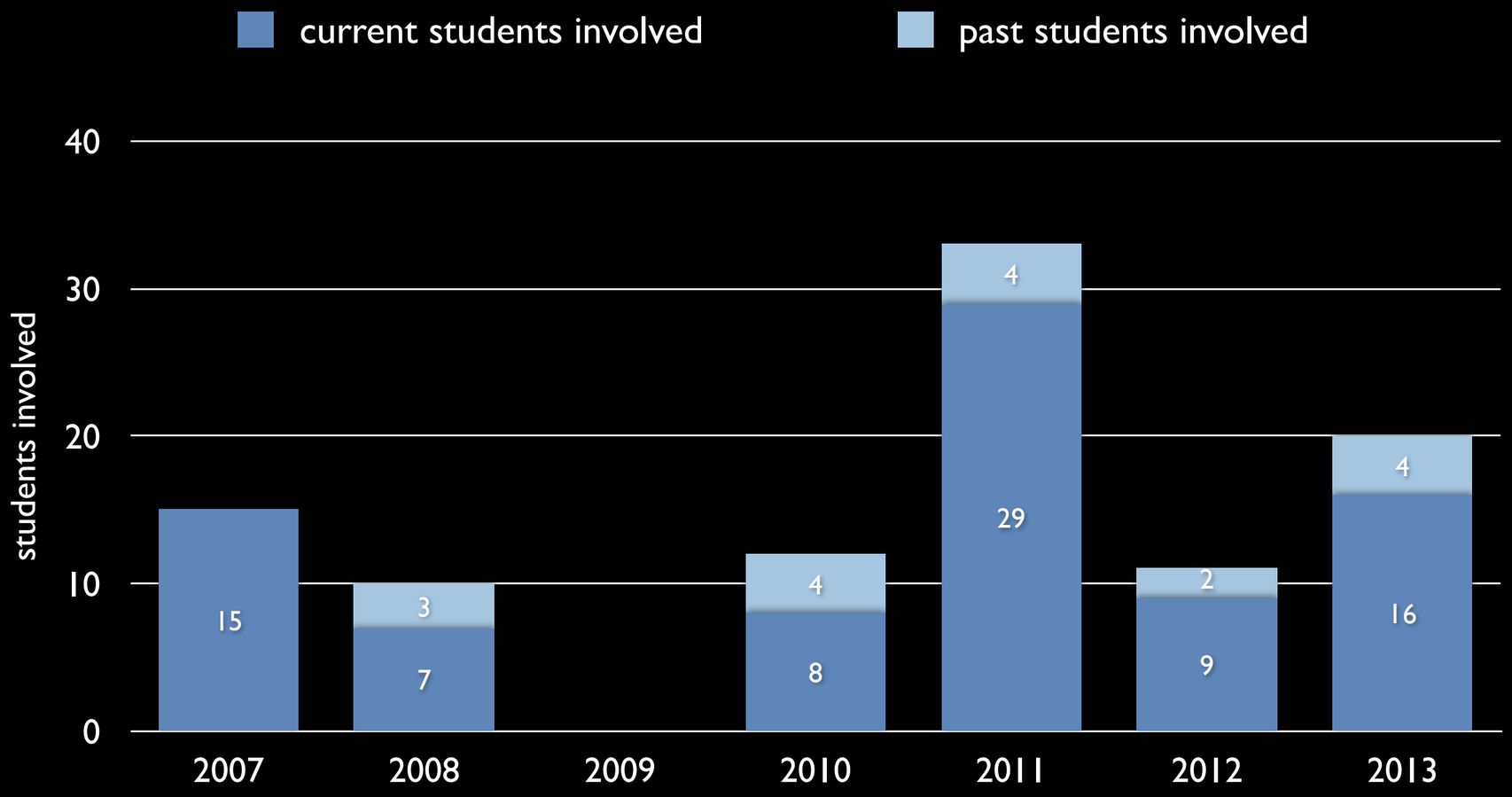
"The essence of all work that you submit to this course must be your own."

"… you may show your code to others, but you may not view theirs, so long as you and they respect this policy's other constraints."

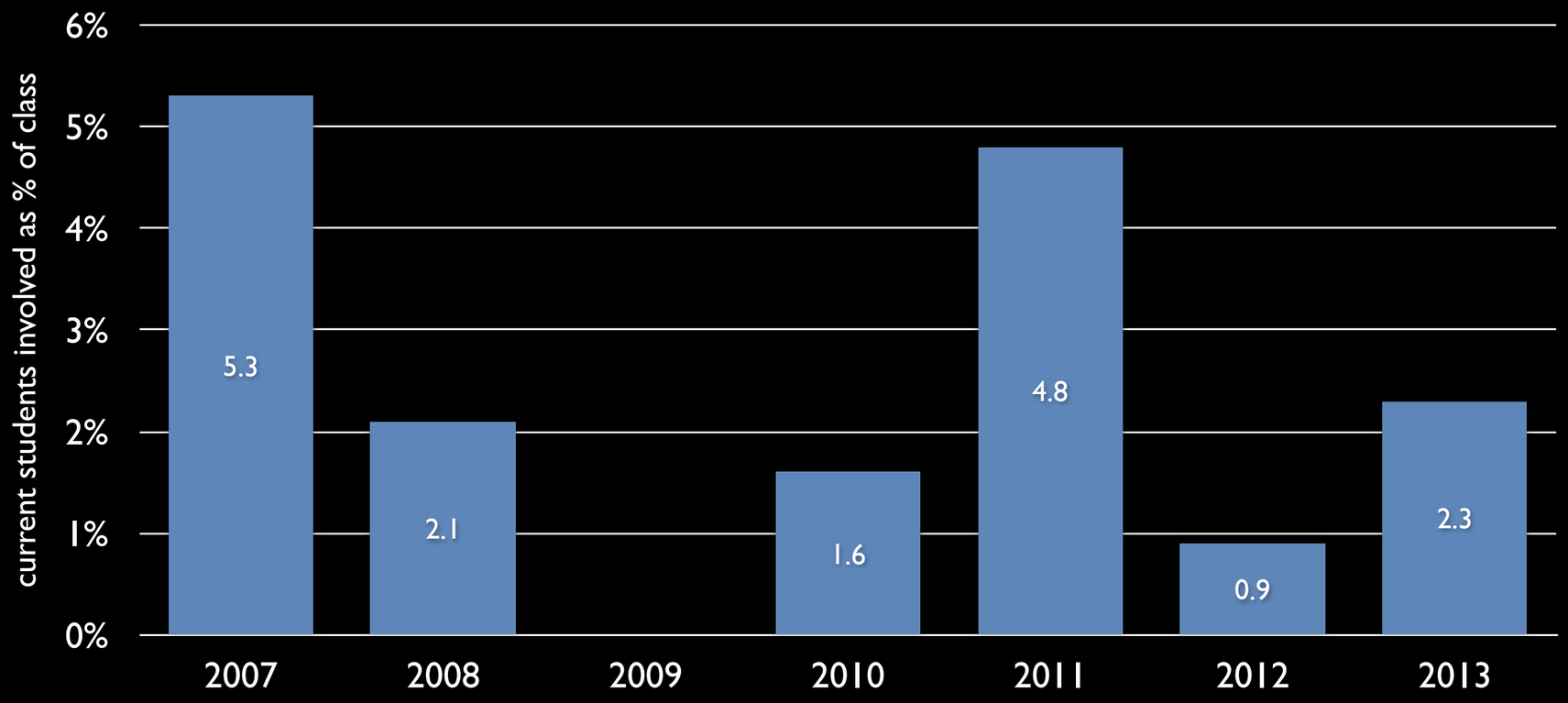
cases


30
20
10
0
number of cases
8
5
0
6
22
6
14
2007
2008
2009
2010
2011
2012
2013

students involved



students involved (%)



all current submissions
all past submissions
code repos
discussion forums
job sites
...

regret clause

"If you commit some act that is not reasonable but bring it to the attention of the course's heads within 72 hours, the course may impose local sanctions that may include an unsatisfactory or failing grade for work submitted, but the course will not refer the matter to the Administrative Board."

abstraction

functions

side effects, return values

scope

local versus global

representation of information

types

```
char

int

float

double

long long

...
```

types

```
1  char

   int

   float

   double

   long long

   ...
```

types

```
1   char
4   int
    float
    double
    long long
    ...
```

types

```
1   char
4   int
4   float
    double
    long long
    ...
```

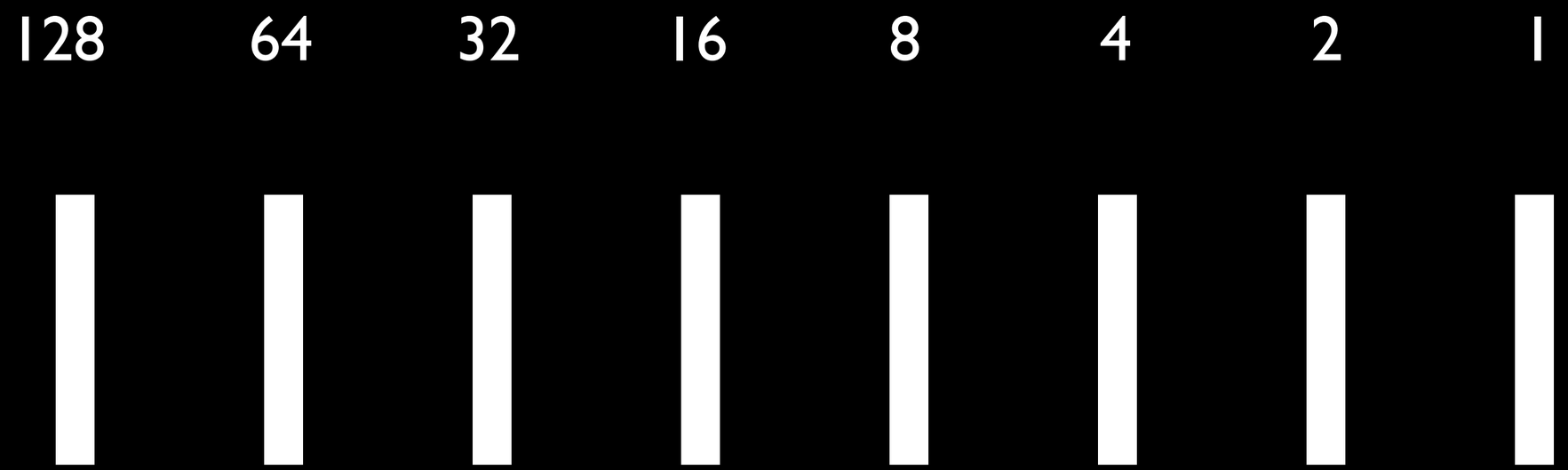
types

```
1   char
4   int
4   float
8   double
    long long
    ...
```

types

```
1  char

4  int

4  float

8  double

8  long long

   ...
```

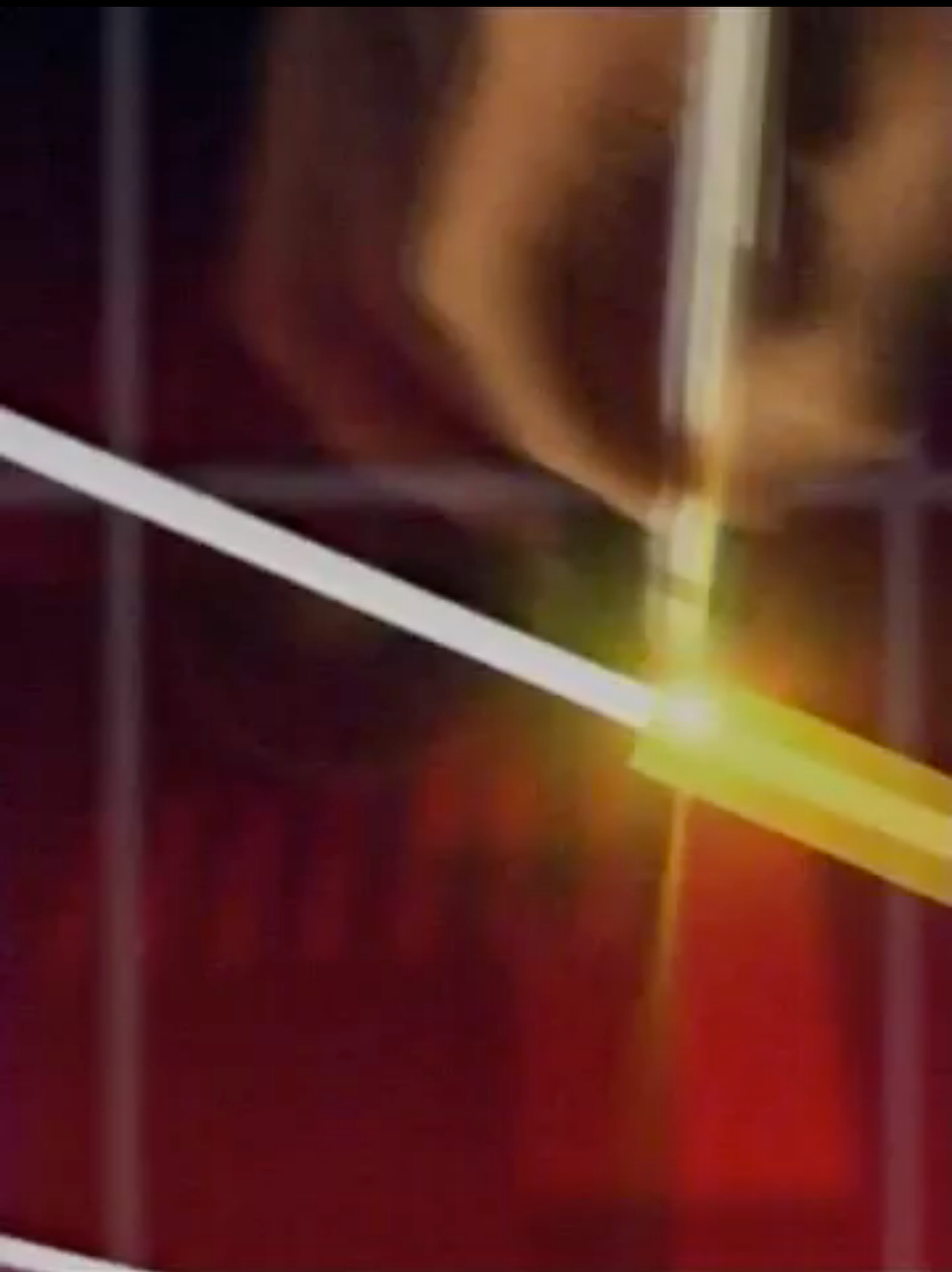
integer overflow


128
64
32
16
8
4
2
1

128 64 32 16 8 4 2 1

00000000

floating-point imprecision



to be continued...