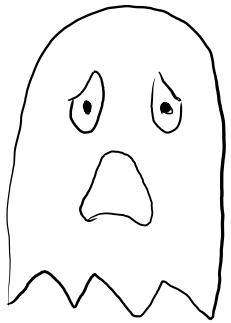
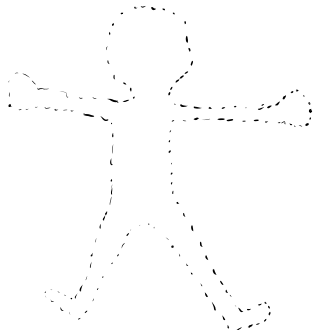
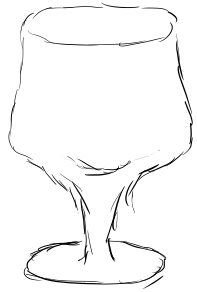
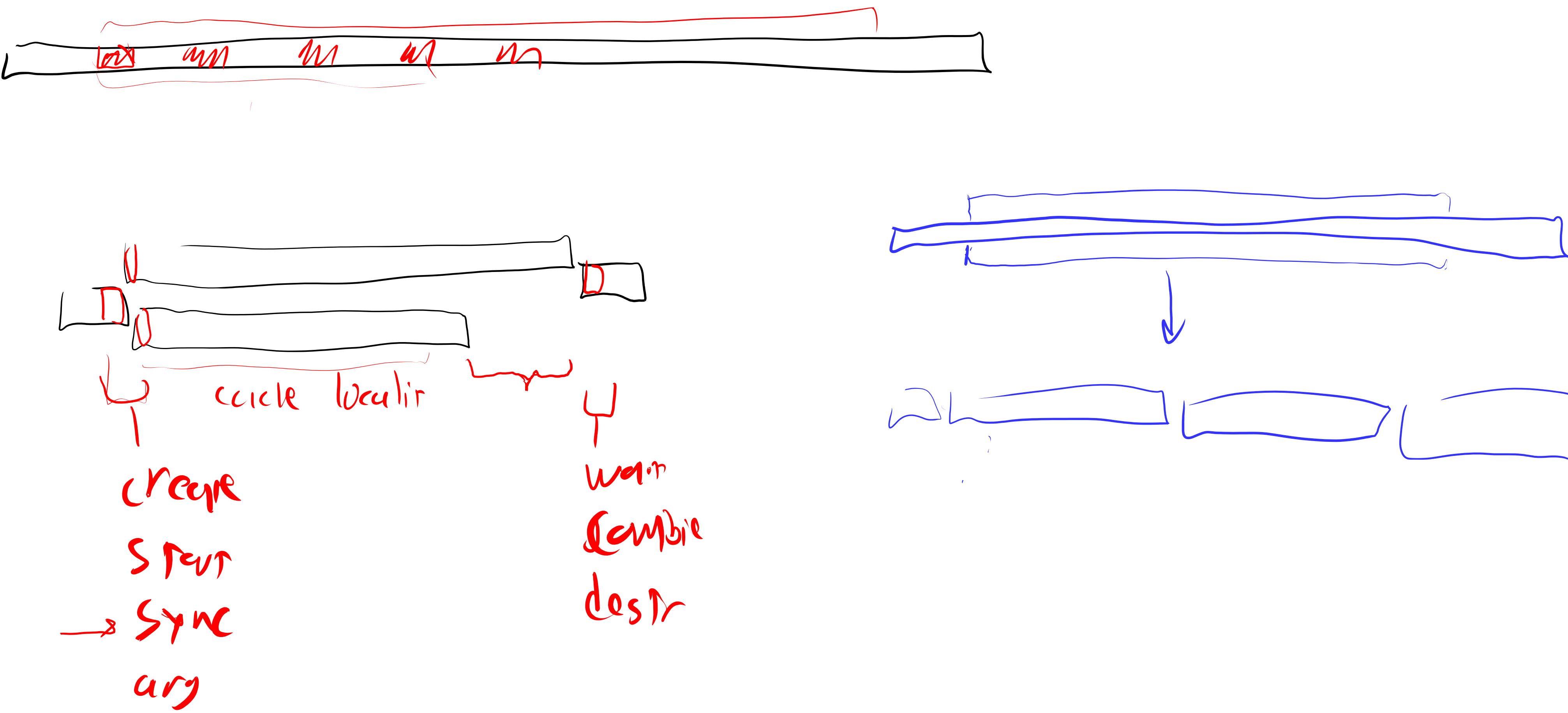







creare
start
sync
arg
wait
destr

Meltdown

goal: read kernel mem in user mode

Speculative read

but discarded, impact cache

check cache locality

x = arr[(*km) * 4096]

Specter

goal: bypass sw protection

arr[x]

C | -1 | Java

C → memory contents

*(arr + x)

-1 → ArrayIndexOutOfBoundsException

y = arr[x] →

if x<0 or x ≥ length
    throw AIOOBE
y = arr[x]

not cached

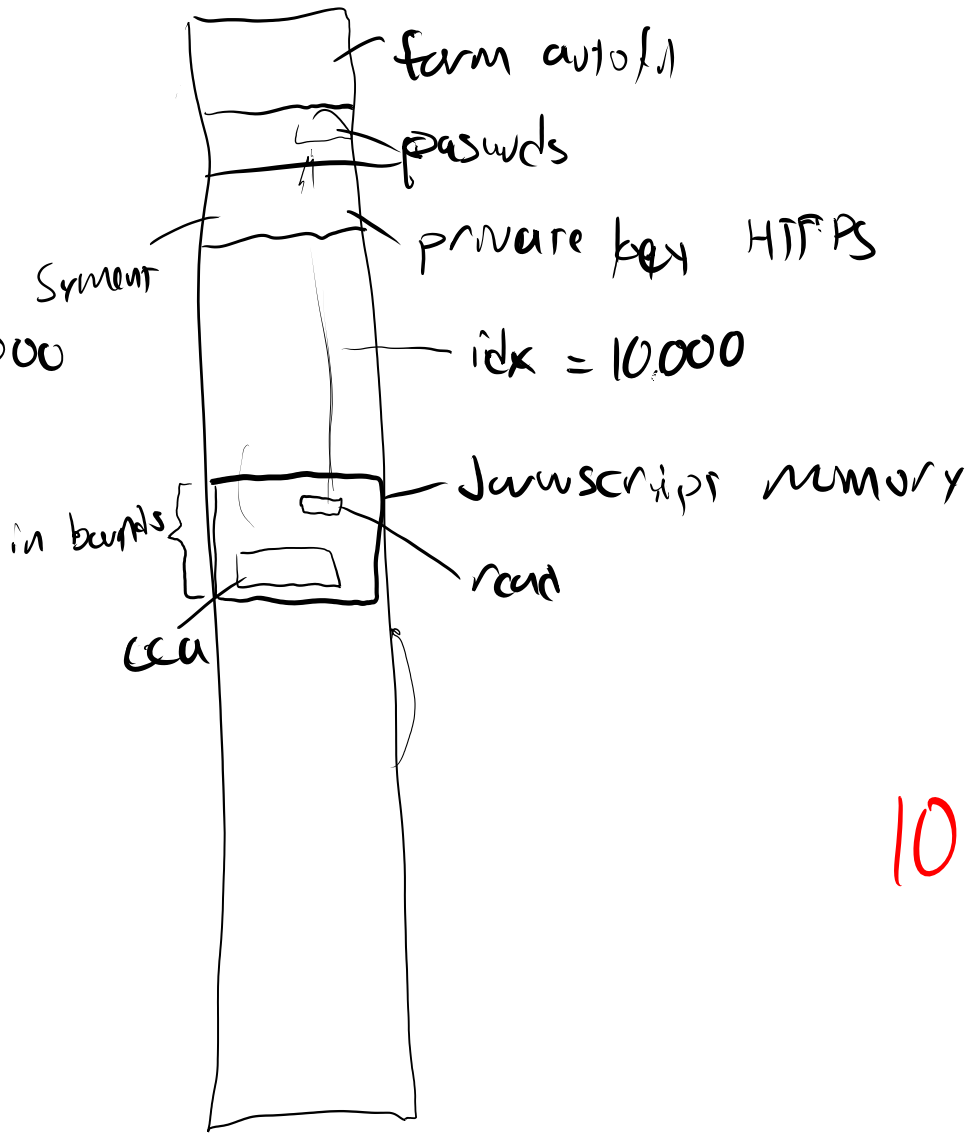
cmp x, len
Ja bad
Mov arr(x), y

branch prediction

cached arr x

arr[ok]
arr[ok]
.
.
.
arr[ok]
y = arr[bad]
x = arr2[y * 4096]

Web browser



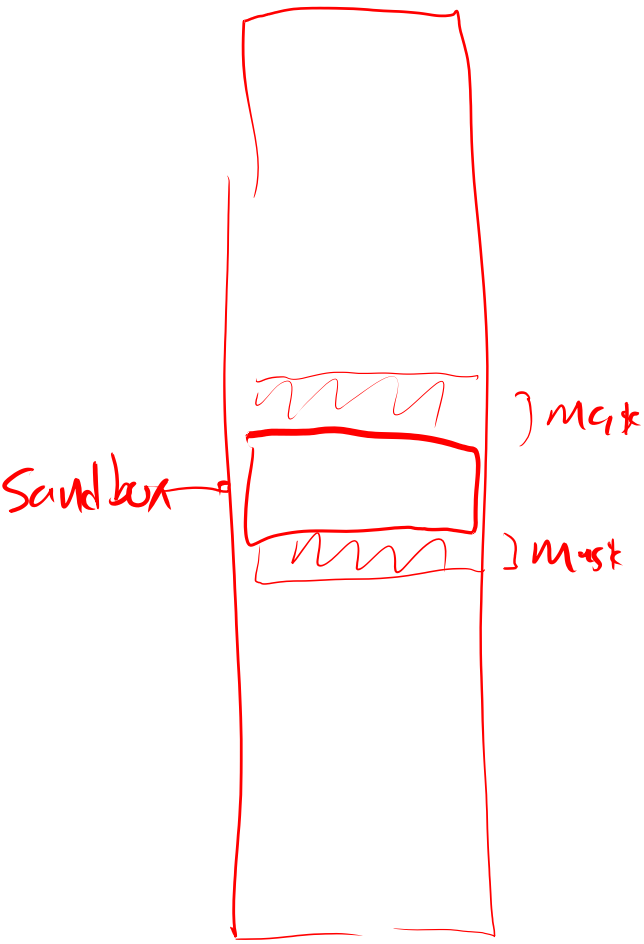
loop:
  x = read [i] ~~x~~ cached length
  if i>0 : y = cca [x * 4096]

i = 0, 0, 0, 0, 0 ... , 0, 10000

foo:
  x = read [i]
  return x

10 KB/s

loop:
  foo(0)
  conflict w/ length ← legal pw check
y = cca [foo (10000) * 4096]



10

```
if ( i ≥ length) throw
 arr [i & mask]
```

00...01111

F

0
1
10
11
100
101
110
111
1000
1001
1010
1100
1101
1110
1111