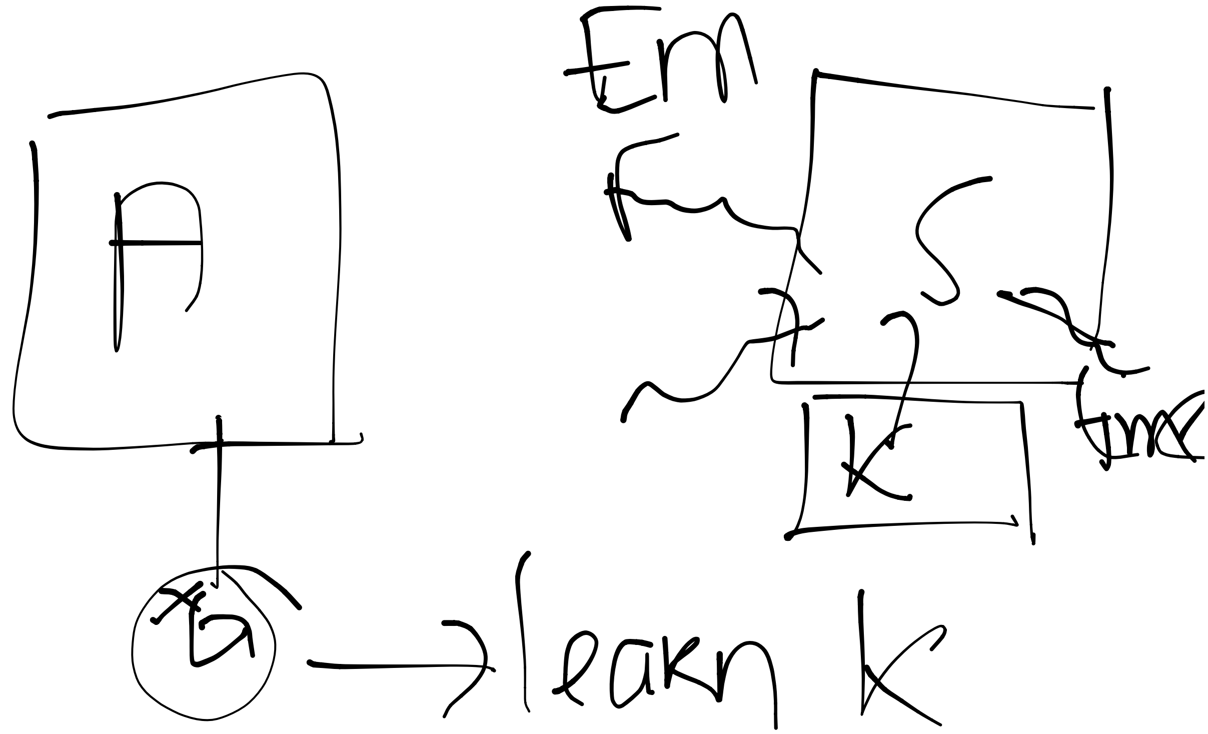
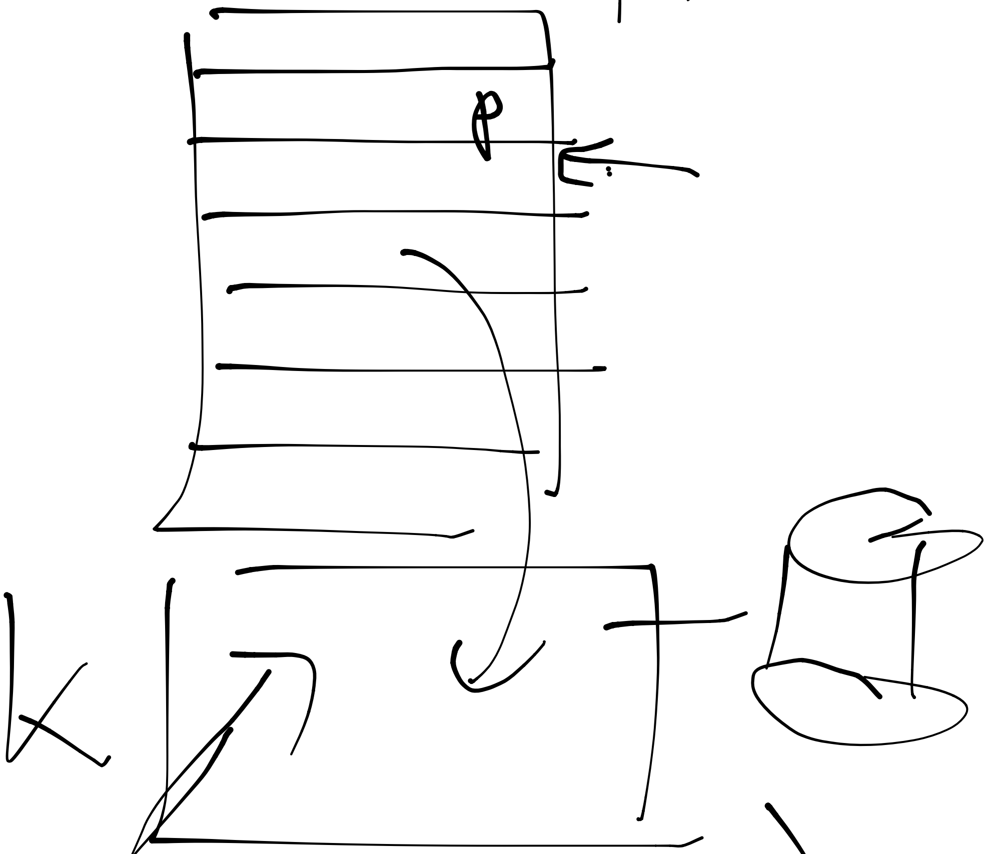
Side channels



Tempest W.II

75% plaintext
crypto

Tenex (1970)



pwcheck(pw)

@ 256 X N

Side channels (2018)

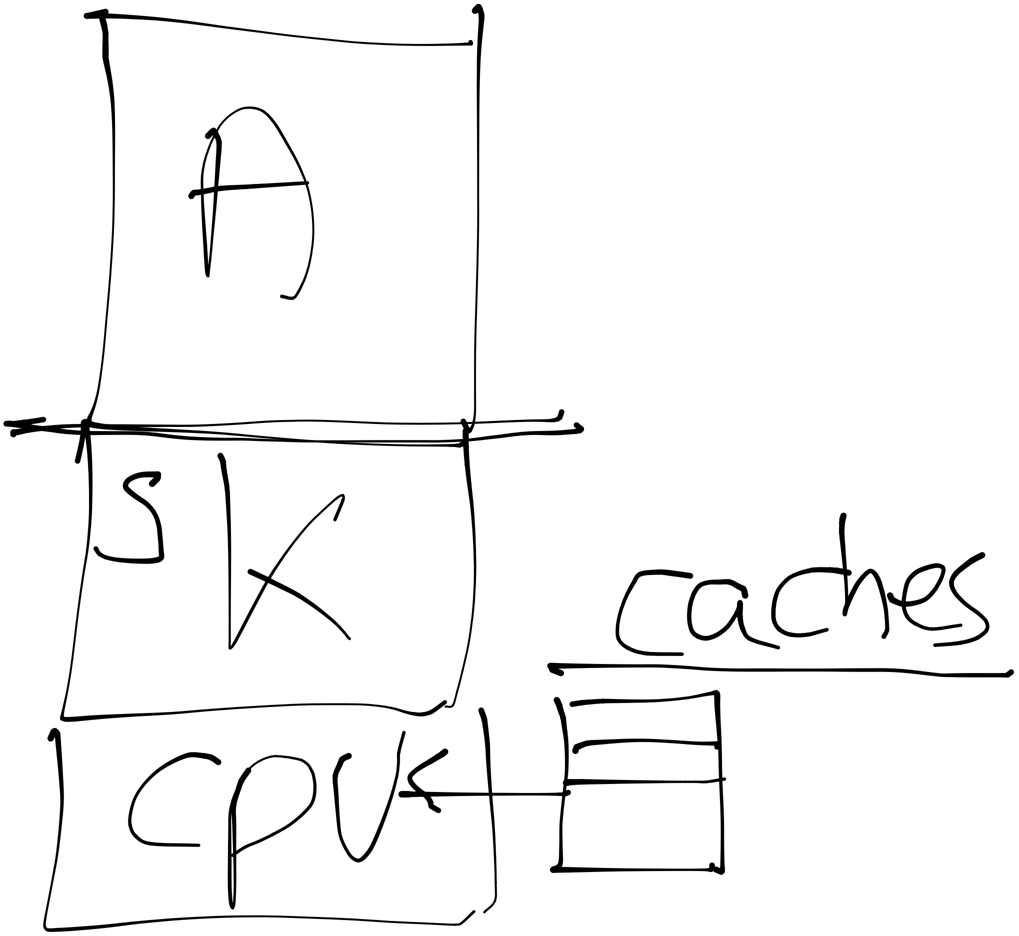
& threat model

Crypto impl

Spectre

Spectre:

breaks isolation



Speculative execution

if (a<5) {

miss

}

→ 100s cycles

misprediction

cpu state

caches

Spectre v1

```
char secret[10]
if (off < sz) {      → Not spe
    v = array1[off]
    v' = array2[v]
}
    array2[0]
    array2[1]
→   array2[2]
```

Challenges

Caches

Train branch predictor

Evict sz

Evict array2

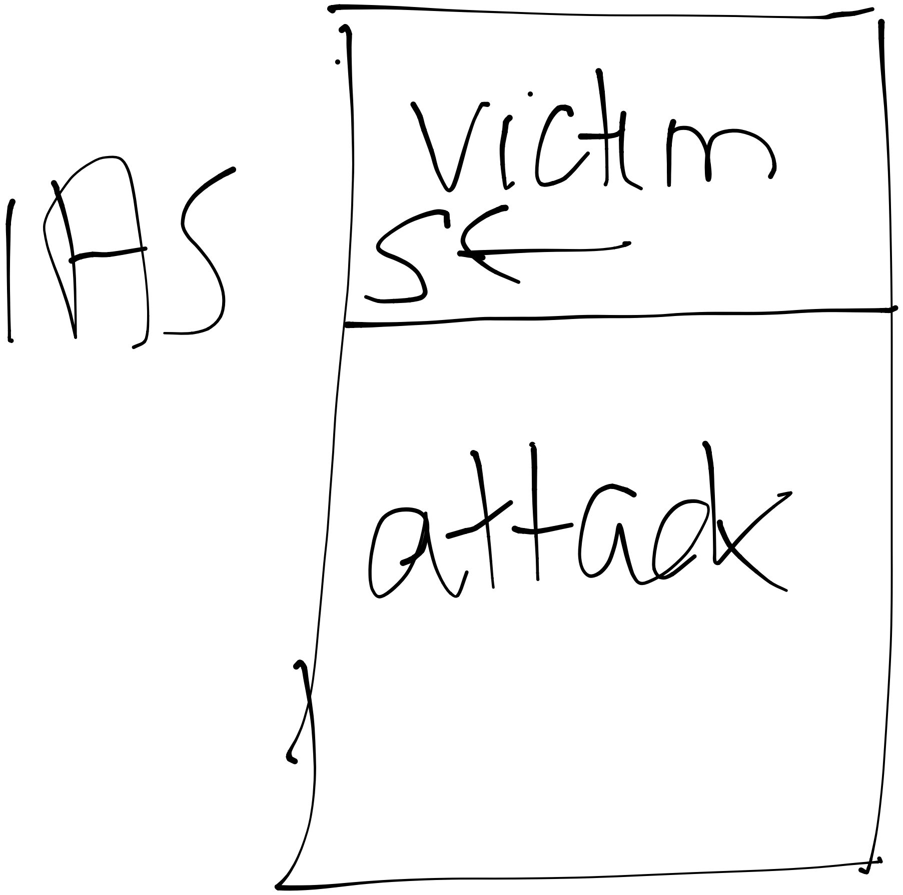
Read array2

Find gadget

Noise

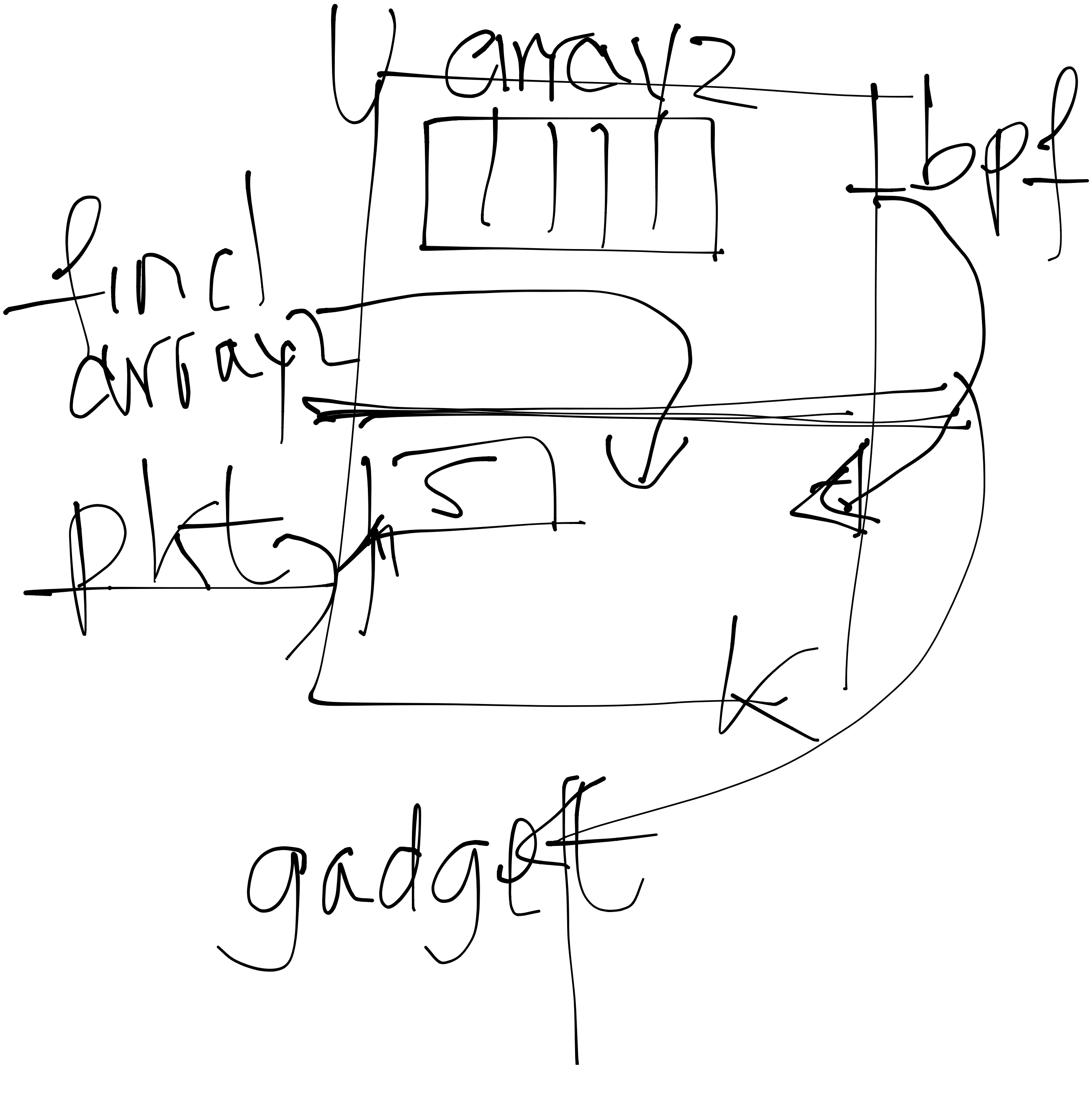
Appendix A

Not real attack.



Project Zero

Proof-of-concept



Mediations

- modify src code: disable speculation
- modify micro code
- kernel page table
- Harden browser

Spectre v2

```
if (off < sz) {
    v = array[off];
    (*f)() <-
}
```

poisson branch predictor

Deep learning

High perf

+

Confidentiality

Stop side channel

Any shared state

No shared state

Measure side channel → low

Spectre

Side channel

Shared caches

timing