Side channels

\( \text{Em} \)

\( \text{learn k} \)

\( \text{Tempest w. II} \)

\( \text{G75 \% plaintext crypto} \)
Tenex (1970)

\[ \text{pwcheck(pw)} \rightarrow 256 \times N \]
Side channel (2018)

... threat model

Crypto impl

Spectre
Spectre breaks isolation

Speculative execution

A

S K

CPU

Caches
cycles
miss

3

1000 cycles
misprediction
unmapped caches
constant
Spectre v1

char secret[]

if (off < 52)
    v = array1[off]
    vl = array2[v]

? array2[0]
    array2[1]
    array2[2]
Challenges
Caches
Train branch predictor
Evict st
Evict array 2
Read array 2
Find gadget Noise
Appendix A

Not real attack

IAS

\[
\begin{array}{c}
\text{victim} \\
\leftarrow \\
\text{attack}
\end{array}
\]
Project Zero
Proof-of-concept

find array
array

pkt

k

gadget
Mediations

- modify src code: disable speculation
- modify micro code
- kernel page table
- Harden browser
Spectre v2

if (off < st) {
    v = arr[jtop];
    } else {
    possson branch predictor.


Deep tension
High perf
+ Confidentiality
Stop side channel

Any shared state
No shared state

Measure side channel → low
Spectre
Shared Caches
Side Channel
Timing