SpectrEM: Exploiting Electromagnetic Emanations During Transient Execution

Jesse De Meulemeester Antoon Purnal Lennert Wouters
Arthur Beckers Ingrid Verbauwhede

COSIC, KU Leuven

Can transient instructions create physical covert channels?

Transient Execution Attacks

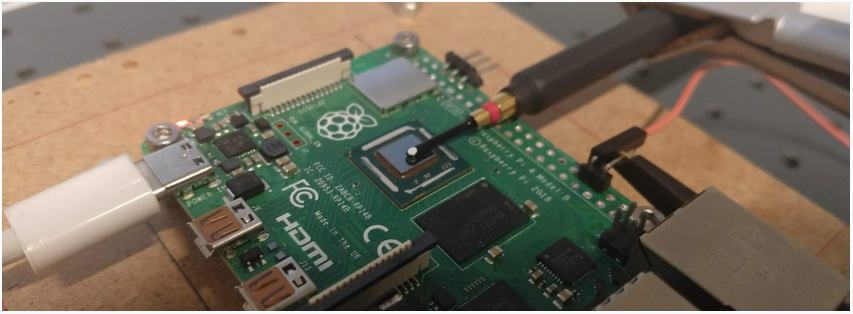
```
if (index < array_size) {
  value = array[index];

  leak(value);
}
```

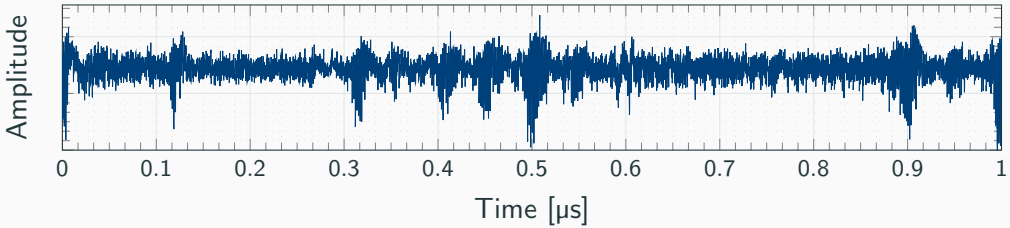
index in bounds
index in bounds
index in bounds
index out of bounds

```
value = access_secret();

leak(value);
```

Generate fault

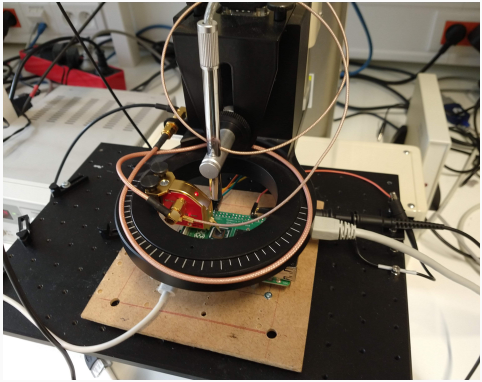
Physical Covert Channels





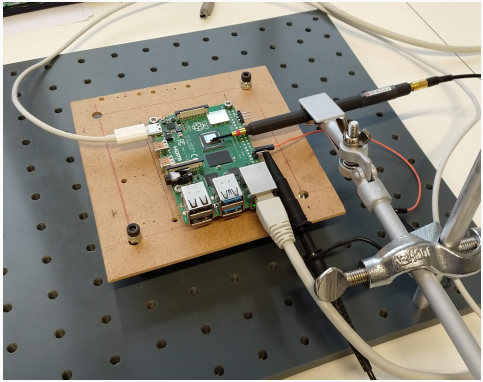
Physical Covert Channels

Setup A



$25 000

Setup B



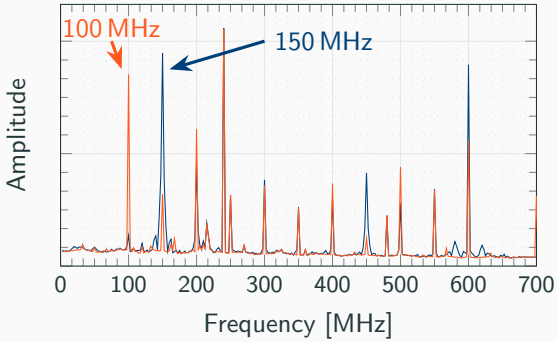
$1000

Target: Arm Cortex-A72

EM Covert Channels

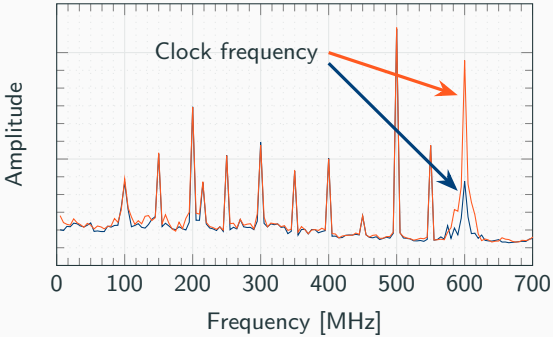
Operand-dependent timings

- Example: `udiv`
  - Divide by 0 (4 clock cycles)
  - Divide by -1 (6 clock cycles)



Control flow dependencies

- Nested branch prediction
  - Correct prediction
  - Misprediction



SpectrEM: A Physical Spectre Attack

Instruction gadget

```
if (index < len) {
  bit = array[index] & bitmask;

  res = dividend / (bit-1);
}
```

Control flow gadget

```
if (index < len) {
  bit = array[index] & bitmask;

  if (bit) {
    ...
  }
}
```

MeltEMdown: A Physical Meltdown Attack

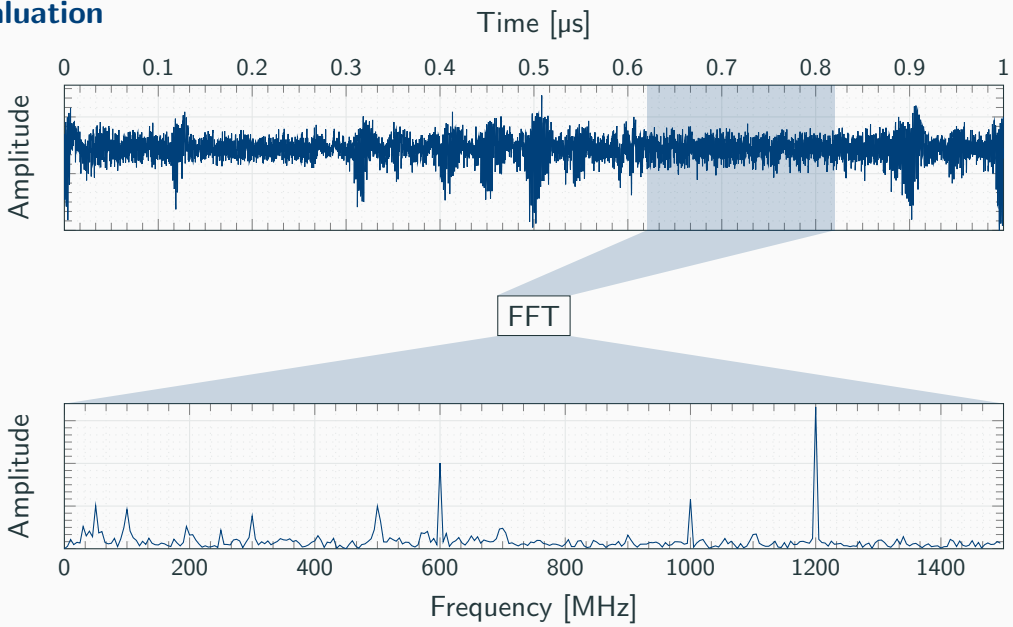
Instruction gadget

```
bit = access_secret();

res = dividend / (bit-1);
```

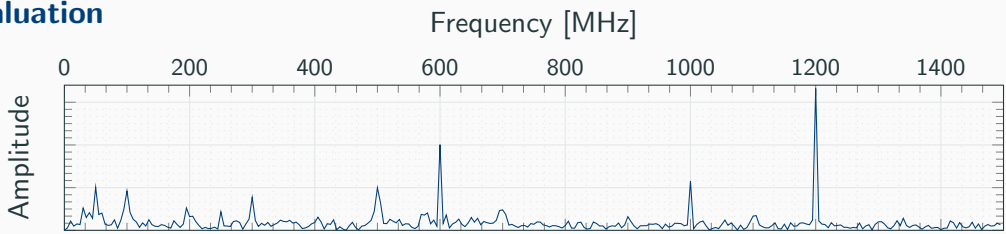
Control flow gadget

```
bit = access_secret();

if (bit) {
  ...
}
```

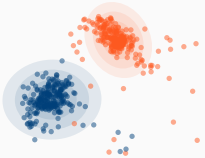
Evaluation


Time [µs]
0
0.1
0.2
0.3
0.4
0.5
0.6
0.7
0.8
0.9
1
Amplitude
FFT
Amplitude
0
200
400
600
800
1000
1200
1400
Frequency [MHz]

Evaluation

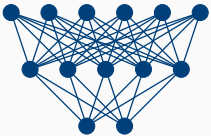


Clustering



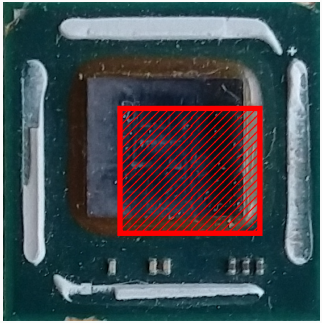
\+ No training data
– Lower accuracy

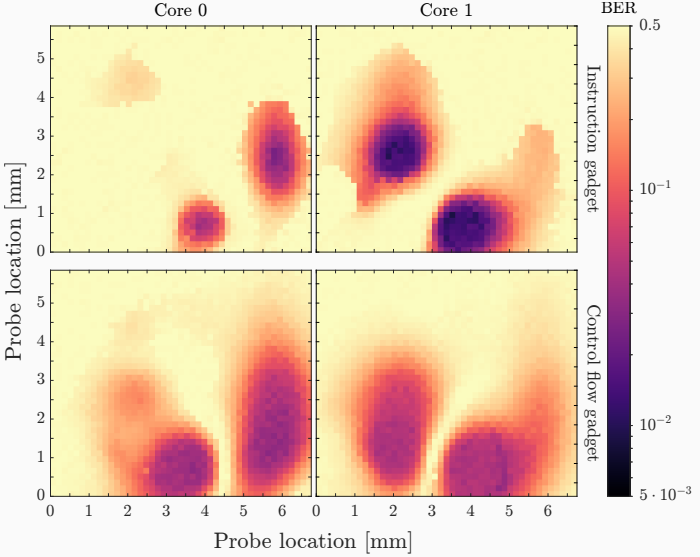
Neural Network



– Requires training data
\+ Higher accuracy

Evaluation




Core 0
Core 1
BER
0.5
10^{-1}
10^{-2}
$5 \cdot 10^{-3}$
Instruction gadget
Control flow gadget
Probe location [mm]
Probe location [mm]
0
1
2
3
4
5
6

Evaluation

	Covert channel	Code Execution	Physical Access	Bitrate [bit/s]	BER [%]
Spectre	Cache	Yes	No	80 000	<0.01
NetSpectre	Cache	No	No	0.004	–
NetSpectre	AVX	No	No	0.017	–
SpectrEM – Instruction	EM	No	Yes	366	<0.01
SpectrEM – Control flow	EM	No	Yes	350	0.769

Case Study: OpenSSH

```
Channel *channel_by_id(struct ssh *ssh, int id) {
  if (id < 0 || (u_int)id >= ssh->chanctxt->channels_alloc) {
    logit_f("%d: bad id", id);
    return NULL;
  }

  Channel *c = ssh->chanctxt->channels[id];

  if (c == NULL) {
    logit_f("%d: bad id: channel free", id);
    return NULL;
  }
  return c;
}
```

SpectrEM: Exploiting Electromagnetic Emanations During Transient Execution

Jesse De Meulemeester Antoon Purnal
Lennert Wouters Arthur Beckers
Ingrid Verbauwhede

COSIC, KU Leuven

KU LEUVEN

COSIC

Artifact

KULeuven-COSIC/SpectrEM