PLATYPUS

Software-based Power Side-Channel Attacks on x86

Moritz Lipp, Andreas Kogler, David Oswald, Michael Schwarz, Catherine Easdon, Claudio Canella, Daniel Gruss

May 23, 2021

IEEE Symposium on Security and Privacy 2021

CPU Power Management

In order to save power, you can …

CPU Power Management

In order to save power, you can …

Shut down resources

CPU Power Management

In order to save power, you can …

Shut down resources

Reduce voltage

CPU Power Management

In order to save power, you can ...

Shut down resources

Reduce voltage

Reduce frequency

Intel RAPL

- Need for Platform Thermal Management, Platform Power Limiting, Power/Performance Budgeting

Intel RAPL

- Need for Platform Thermal Management, Platform Power Limiting, Power/Performance Budgeting
- **Intel Running Average Power Limit** (RAPL) provides ...

Intel RAPL

- Need for Platform Thermal Management, Platform Power Limiting, Power/Performance Budgeting
- **Intel Running Average Power Limit** (RAPL) provides . . .

power limiting

Intel RAPL

- Need for Platform Thermal Management, Platform Power Limiting, Power/Performance Budgeting
- **Intel Running Average Power Limit** (RAPL) provides ...

power limiting

accurate energy reading

Intel RAPL

- On **Linux**, counters can be accessed using the `powercap` framework

  `/sys/devices/virtual/powercap/intel-rapl`

Intel RAPL

- On **Linux**, counters can be accessed using the `powercap` framework

  `/sys/devices/virtual/powercap/intel-rapl`

- On **macOS** and **Windows**, a driver from Intel needs to be installed

Intel RAPL: Properties

Unprivileged power meter

Intel RAPL: Properties

Unprivileged power meter

No physical access

Intel RAPL: Properties

Unprivileged power meter

No physical access

Low refresh rate

What can we do with this?

Distinguishing Instructions

- Measure the energy consumption of **different instructions**

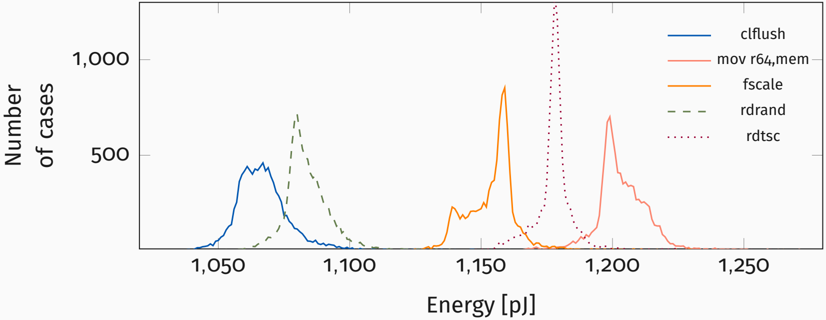


Figure 1: A histogram of the power consumption of various instructions on the i7-6700K (desktop) system.

Distinguishing Operands

- Measure the energy consumption of **different operands**

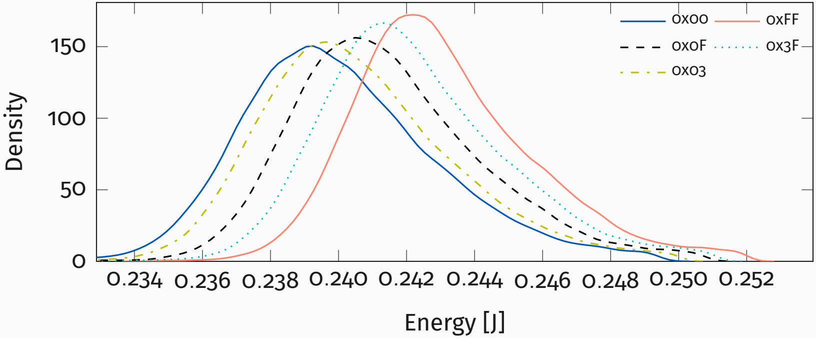


Figure 2: Measured energy consumption of the `imul` instruction with one operand fixed to 8 and the other varying in its Hamming weight.

Distinguishing Data

- Measure the energy consumption of **different load values**

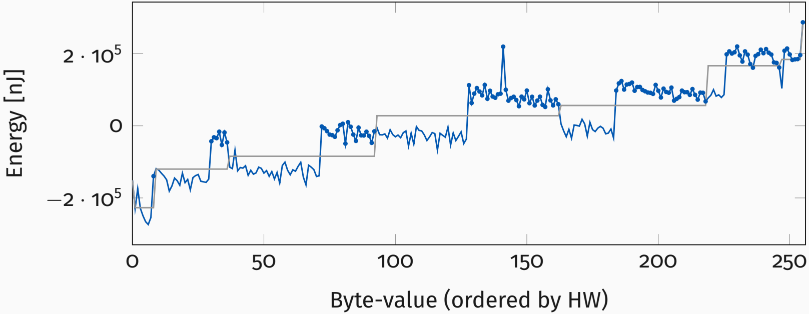


Figure 3: Energy consumption of the `movb` instruction for all byte values, ordered by Hamming Weight (HW) and value. The circle marks values where the most-significant bit is set.

Distinguishing Load Targets

- Measure the energy consumption of **different load targets**

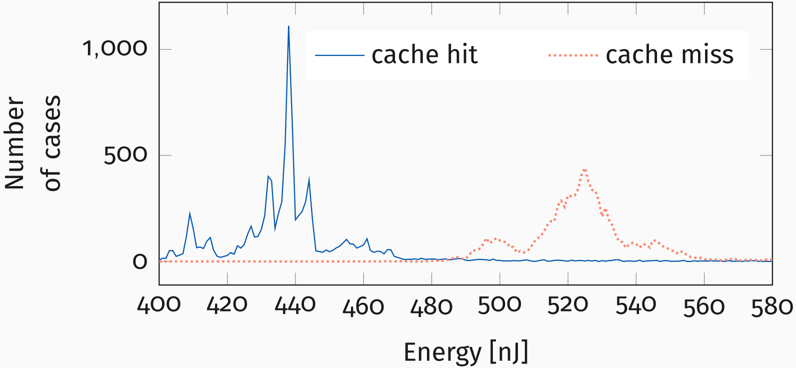
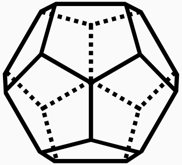


Figure 4: Using RAPL to distinguish whether the target of a memory load is cached (cache hit) or not (DRAM access).

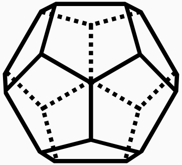
Let’s exploit this!

Breaking KASLR



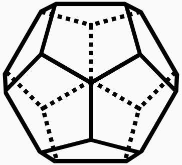
- Kernel Address Space Layout Randomization (KASLR) randomizes kernel location

Breaking KASLR



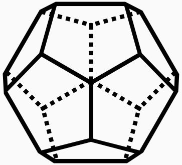
- Kernel Address Space Layout Randomization (KASLR) randomizes kernel location
- Exploit **energy consumption differences** between

Breaking KASLR



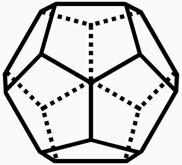
- Kernel Address Space Layout Randomization (KASLR) randomizes kernel location
- Exploit **energy consumption differences** between
  - Mapped addresses

Breaking KASLR



- Kernel Address Space Layout Randomization (KASLR) randomizes kernel location
- Exploit **energy consumption differences** between
  - Mapped addresses
  - Unmapped addresses

Breaking KASLR



- Kernel Address Space Layout Randomization (KASLR) randomizes kernel location
- Exploit **energy consumption differences** between
  - Mapped addresses
  - Unmapped addresses
- **Valid address translations** are cached in the **TLB**

Breaking KASLR

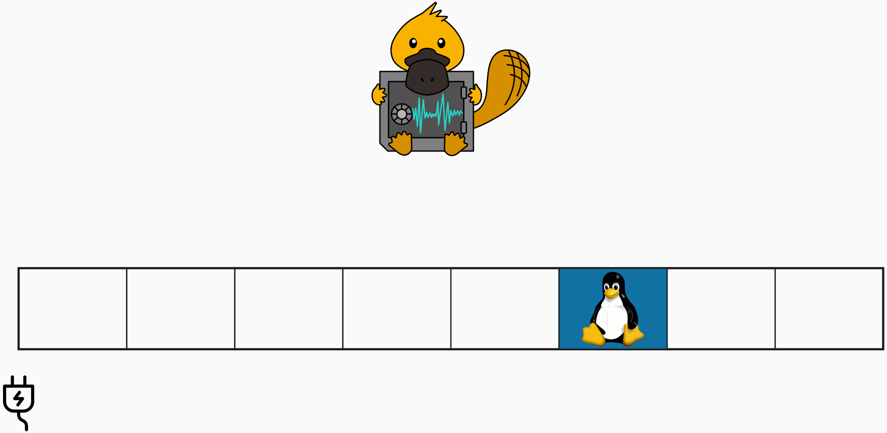


Figure 5: Page-table walks for unmapped pages require more power

Breaking KASLR

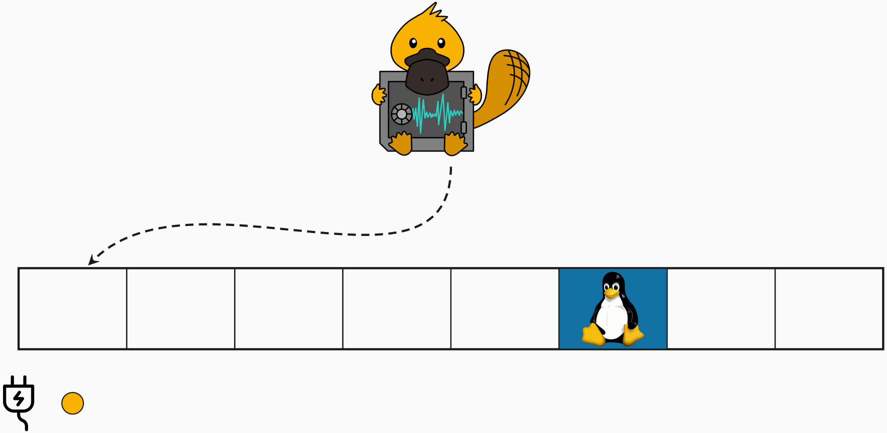


Figure 5: Page-table walks for unmapped pages require more power

Breaking KASLR

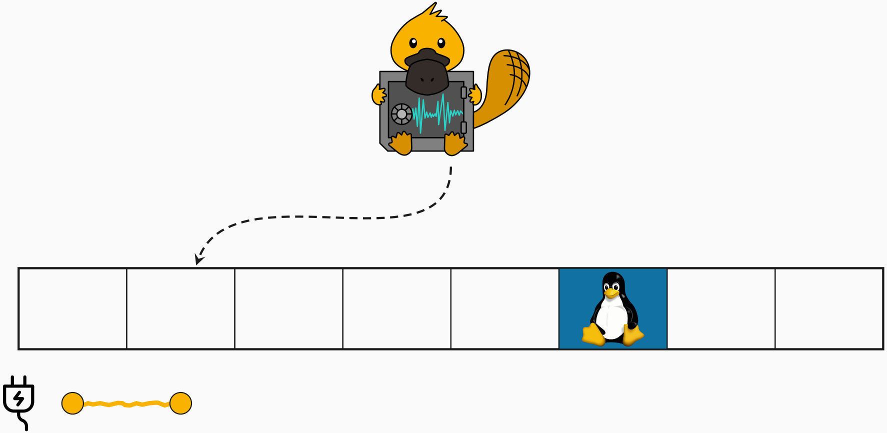


Figure 5: Page-table walks for unmapped pages require more power

Breaking KASLR

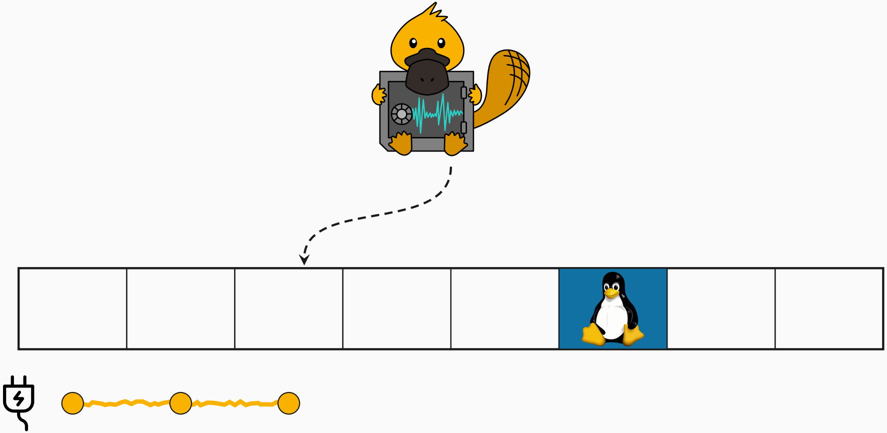


Figure 5: Page-table walks for unmapped pages require more power

Breaking KASLR

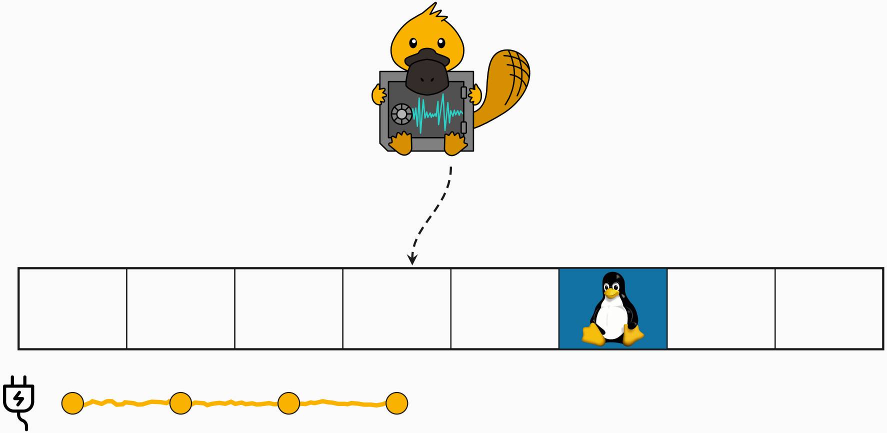


Figure 5: Page-table walks for unmapped pages require more power

Breaking KASLR

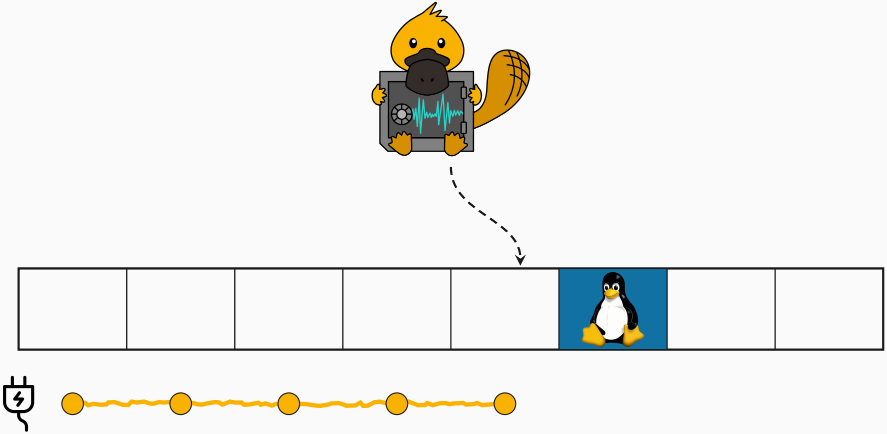


Figure 5: Page-table walks for unmapped pages require more power

Breaking KASLR

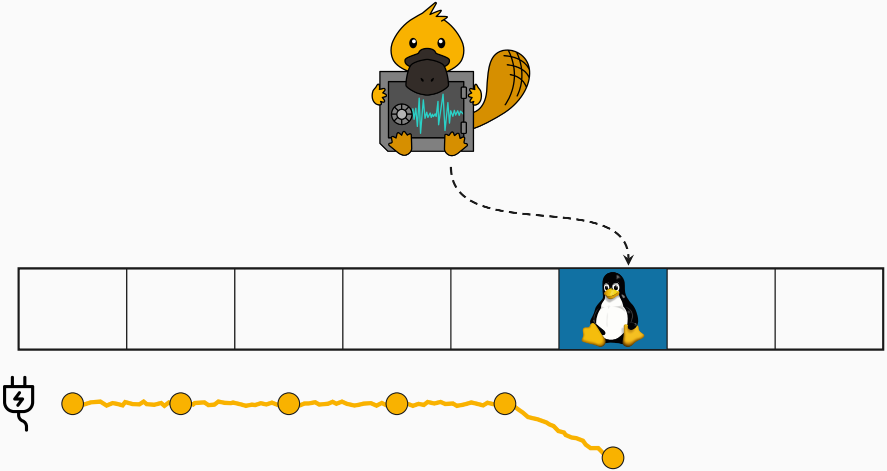


Figure 5: Page-table walks for unmapped pages require more power

Breaking KASLR

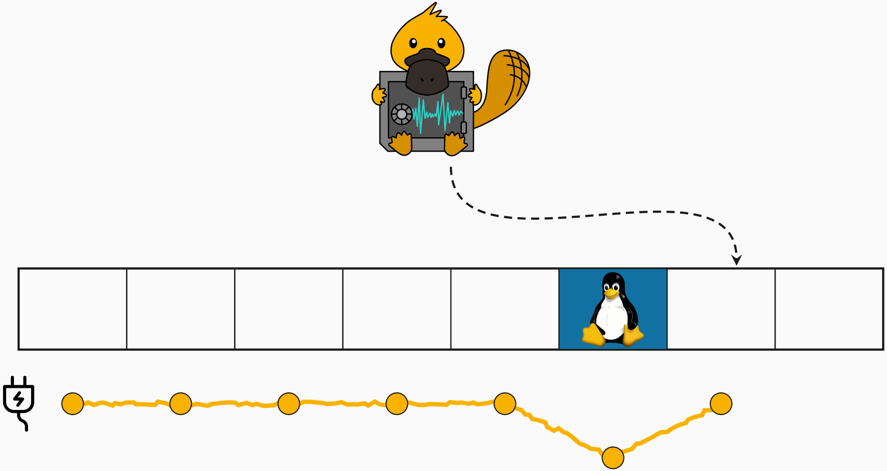


Figure 5: Page-table walks for unmapped pages require more power

Breaking KASLR

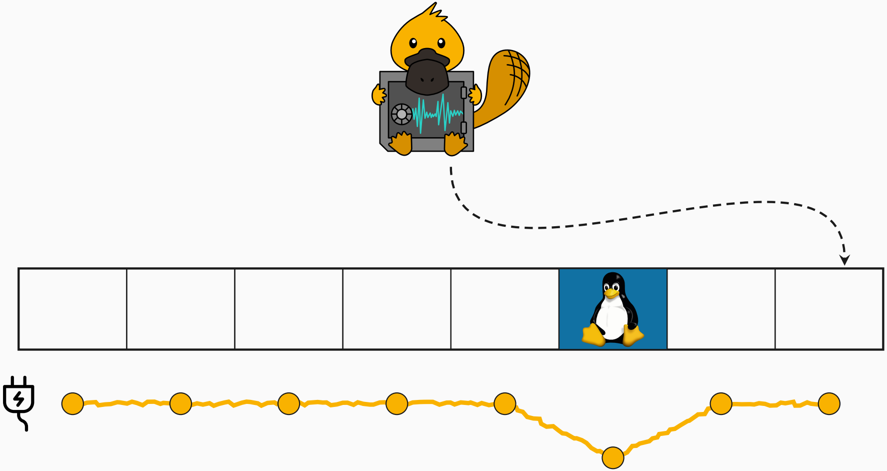
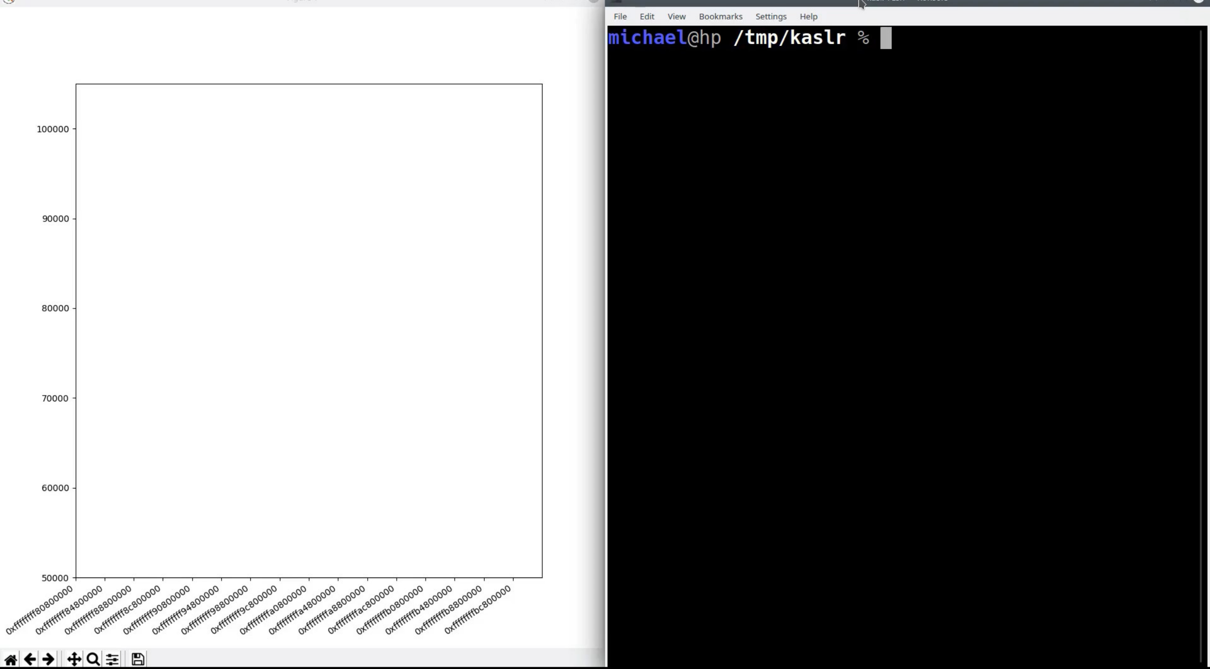
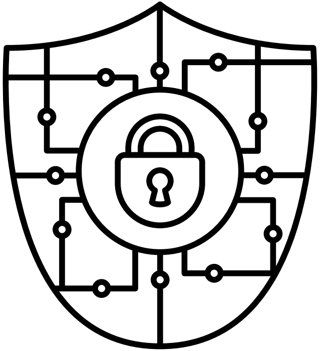


Figure 5: Page-table walks for unmapped pages require more power

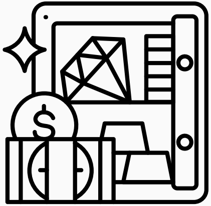


```
michael@hp /tmp/kaslr %
```



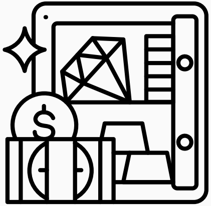
Attacking Crypto: RSA Key Recovery

Attacking Intel SGX



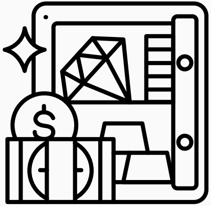
- Instruction-set extension

Attacking Intel SGX



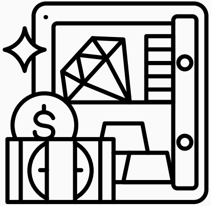
- Instruction-set extension
- Integrity and confidentiality of code and data in **untrusted environments**

Attacking Intel SGX



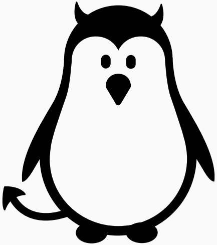
- Instruction-set extension
- Integrity and confidentiality of code and data in **untrusted environments**
- Run programs in **enclaves** using protected areas of memory

Attacking Intel SGX



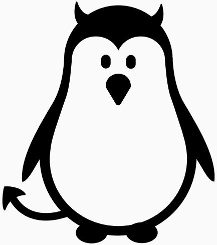
- Instruction-set extension
- Integrity and confidentiality of code and data in **untrusted environments**
- Run programs in **enclaves** using protected areas of memory
- Operating system can be **compromised**

Attacking Intel SGX



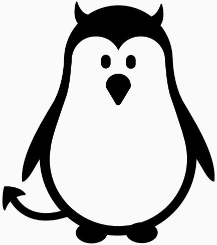
- More power as an evil operating system

Attacking Intel SGX



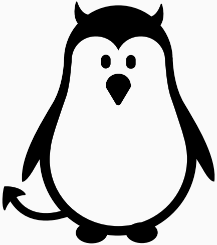
- More power as an evil operating system
- Hook the SGX Enclave exit point

Attacking Intel SGX



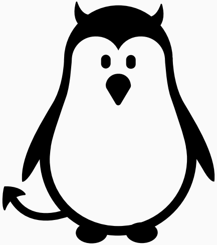
- More power as an evil operating system
- Hook the SGX Enclave exit point
- Directly read out the **RAPL values** from the MSRs

Attacking Intel SGX



- More power as an evil operating system
- Hook the SGX Enclave exit point
- Directly read out the **RAPL values** from the MSRs
- No operating system overhead!

Attacking Intel SGX



- More power as an evil operating system
- Hook the SGX Enclave exit point
- Directly read out the **RAPL values** from the MSRs
- No operating system overhead!
- Interrupt victim often to increase resolution

SGX Step

- **SGX-step** is an open-source Linux kernel framework

SGX Step

- **SGX-step** is an open-source Linux kernel framework
- Configure APIC timer interrupts

SGX Step

- **SGX-step** is an open-source Linux kernel framework
- Configure APIC timer interrupts
- Single and zero-step enclave execution

SGX Step

- **Combine** Intel RAPL with SGX-step

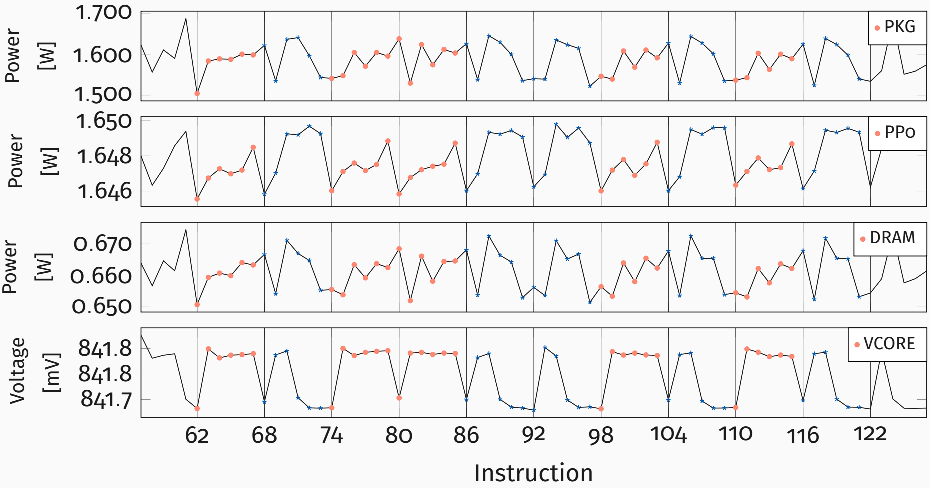
SGX Step

- **Combine** Intel RAPL with SGX-step
- Measure the energy consumption of **single instructions**

Attacking RSA

- Implemented using a Square-and-multiply algorithm
  - **Keybit 0**: Compute square operation
  - **Keybit 1**: Compute square operation and multiplication
- Consumes different amount of energy depending on the key bit

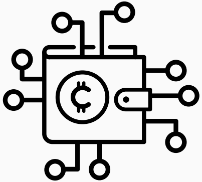
RSA Toy Cipher



Attacking mbed TLS

- **Extract RSA** key from mbed TLS 2.13.0

Attacking mbed TLS



- **Extract RSA** key from mbed TLS 2.13.0
- Square-and-multiply algorithm

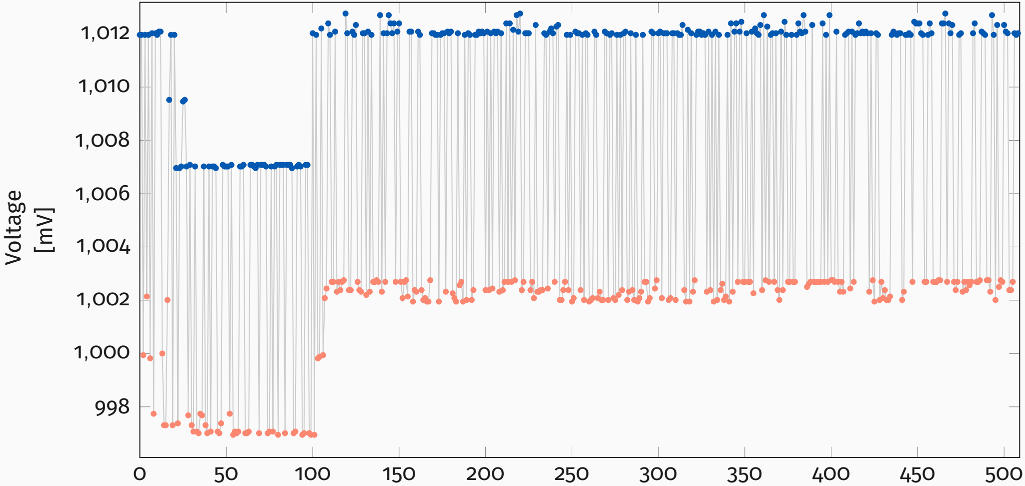
Attacking mbed TLS

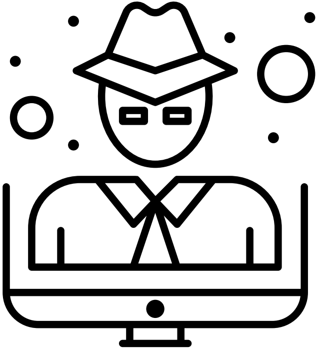
- **Extract RSA** key from mbed TLS 2.13.0
- Square-and-multiply algorithm
- Multiplication function uses AVX memset

Attacking mbed TLS

- **Extract RSA** key from mbed TLS 2.13.0
- Square-and-multiply algorithm
- Multiplication function uses AVX memset
- Number of instructions executed depends on the key

RSA Toy Cipher





Crypto Attacks from User Space

Repeat Repeat Repeat

- **Difficult** to measure parts without SGX-step

Repeat Repeat Repeat

- **Difficult** to measure parts without SGX-step
- **Can** measure over the **overall execution**

Correlation Power Analysis

- Building a power consumption **model** of the device:

Correlation Power Analysis

- Building a power consumption **model** of the device:

Hamming Weight

Number of bits set

Correlation Power Analysis

- Building a power consumption **model** of the device:

Hamming Weight

Number of bits set

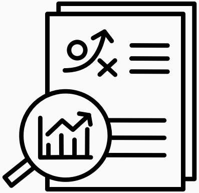
Hamming Distance

Bits flipping between operations

Correlation Power Analysis

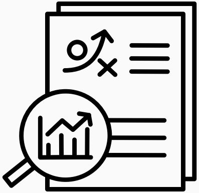
- **AES-NI**: Side-channel resilient instruction-set extension
- Target **AES-NI** in a scenario where we can trigger encryption/decryption of many blocks
  - Disk encryption/decryption
  - TLS
  - (Un)sealing SGX enclave state

Correlation Power Analysis



- We control the plain text

Correlation Power Analysis

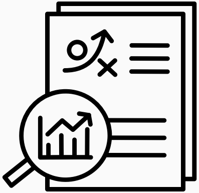


- We control the plain text
- We observe the cipher text

Correlation Power Analysis

- We control the plain text
- We observe the cipher text
- We measure the energy consumption over many operations

Correlation Power Analysis

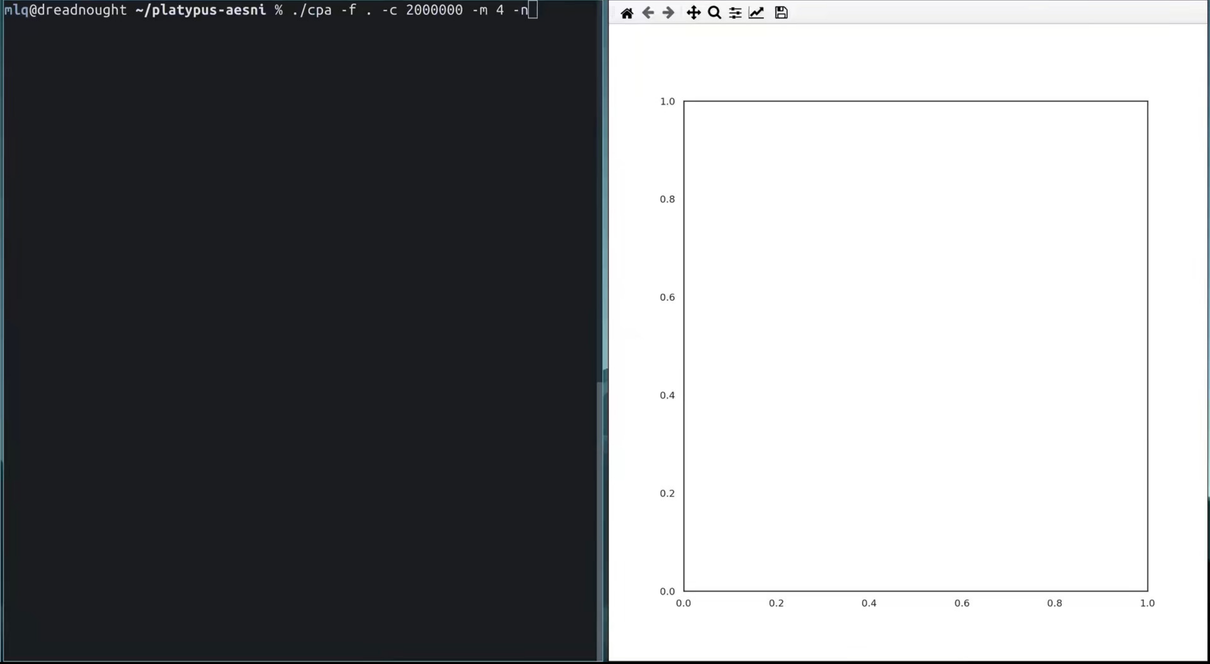


- We control the plain text
- We observe the cipher text
- We measure the energy consumption over many operations
- We guess the key

Correlation Power Analysis

- We control the plain text
- We observe the cipher text
- We measure the energy consumption over many operations
- We guess the key

- With our model and all possible values, **where** is the **correlation** the highest?



```
mlq@dreadnought ~/platypus-aesni % ./cpa -f . -c 2000000 -m 4 -n
```

Countermeasures

Countermeasures

- Remove the unprivileged access to the RAPL MSRs

Countermeasures

- Remove the unprivileged access to the RAPL MSRs
- **1 Line Patch** for the Linux Kernel

Countermeasures

- Threat model of SGX allows a **compromised operating system**

Countermeasures

- Threat model of SGX allows a **compromised operating system**
  - Operating system patch does not help

Countermeasures

- Threat model of SGX allows a **compromised operating system**
  - Operating system patch does not help
- **Microcode updates** are necessary

Countermeasures

- Threat model of SGX allows a **compromised operating system**
  - Operating system patch does not help
- **Microcode updates** are necessary
  - Fallback to a model of the energy consumption

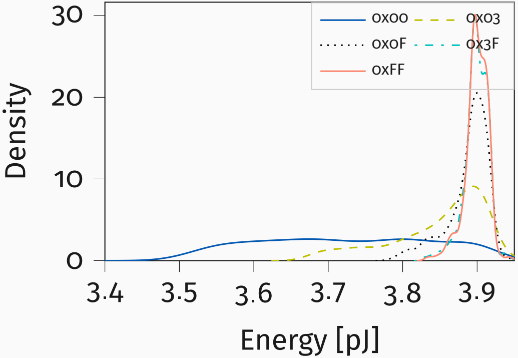
Countermeasures

- Threat model of SGX allows a **compromised operating system**
  - Operating system patch does not help
- **Microcode updates** are necessary
  - Fallback to a model of the energy consumption
  - Does **not allow** to distinguish data/operands any more

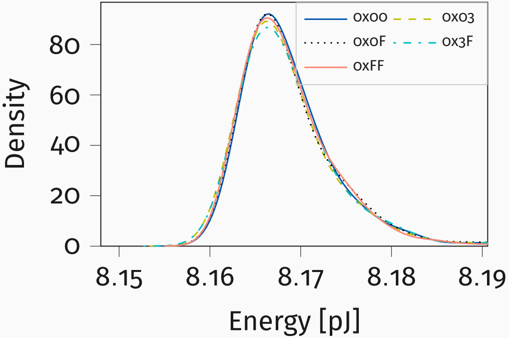
Countermeasures

- Threat model of SGX allows a **compromised operating system**
  - Operating system patch does not help
- **Microcode updates** are necessary
  - Fallback to a model of the energy consumption
  - Does **not allow** to distinguish data/operands any more
  - **Constant-time implementations** are necessary

Mitigation



Without Mitigation



With Mitigation

Takeaways

- Power side-channel attacks can be exploited **from software** on modern CPUs

Takeaways

- Power side-channel attacks can be exploited **from software** on modern CPUs
- Threat model of Intel SGX requires more complex mitigations
- Other CPU manufacturers provide similar interfaces

PLATYPUS

Software-based Power Side-Channel Attacks on x86

Moritz Lipp, Andreas Kogler, David Oswald, Michael Schwarz, Catherine Easdon, Claudio Canella, Daniel Gruss

May 23, 2021

IEEE Symposium on Security and Privacy 2021