Finding and Exploiting CPU Features using MSR Templating

IEEE Symposium on Security and Privacy 2022

Andreas Kogler
Graz University of Technology

Daniel Weber
CISPA Helmholtz Center for Information Security

Martin Haubenwallner
Graz University of Technology

Moritz Lipp
Amazon Web Services

Daniel Gruss
Graz University of Technology

Michael Schwarz
CISPA Helmholtz Center for Information Security

Agenda

- **Motivation**
- **Framework**
  - Detection
  - Classification
  - Extensions
- **Case Studies**

Andreas Kogler @0xhilbert andreas.kogler@iaik.tugraz.at

Motivation

- **Model Specific Registers** (MSRs)
  - 2^{32} 64-bit Registers
  - Documented
  - Undocumented

Andreas Kogler @0xhilbert andreas.kogler@iaik.tugraz.at

Motivation

- **Model Specific Registers** (MSRs)
  - 2^{32} 64-bit Registers
  - Documented
  - Undocumented
- **Influences** on instructions

Andreas Kogler @0xhilbert andreas.kogler@iaik.tugraz.at

Motivation

- **Model Specific Registers** (MSRs)
  - 2^{32} 64-bit Registers
  - Documented
  - Undocumented
- **Influences** on instructions
- **Security** patches

Andreas Kogler @0xhilbert andreas.kogler@iaik.tugraz.at

Motivation

- **Model Specific Registers** (MSRs)
  - 2^{32} 64-bit Registers
  - Documented
  - Undocumented
- **Influences** on instructions
- **Security** patches
- **Hidden** features (e.g., Domas [1])

Andreas Kogler @0xhilbert andreas.kogler@iaik.tugraz.at

The Framework: MSR Scanning

$\underbrace{\qquad\qquad\qquad}_{\textbf{MSR Detection}}$ $\underbrace{\qquad\qquad\qquad\qquad\qquad\qquad}_{\textbf{MSR Classification}}$

Andreas Kogler @0xhilbert andreas.kogler@iaik.tugraz.at

The Framework: MSR Scanning

- **Scan** all MSR addresses
  - `rdmsr` → GP-Fault?
  - `wrmsr` → GP-Fault?

Andreas Kogler @0xhilbert andreas.kogler@iaik.tugraz.at

The Framework: MSR Scanning

- **Scan** all MSR addresses
  - `rdmsr` → GP-Fault?
  - `wrmsr` → GP-Fault?

✓ Complete MSR list

Andreas Kogler @0xhilbert andreas.kogler@iaik.tugraz.at

The Framework: MSR Scanning

- **Scan** all MSR addresses
  - `rdmsr` → GP-Fault?
  - `wrmsr` → GP-Fault?

✓ Complete MSR list

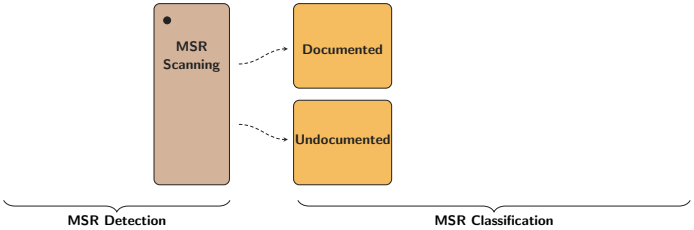
✓ *R*, *W*, *RW* or *not*-present

Andreas Kogler @0xhilbert andreas.kogler@iaik.tugraz.at

The Framework: Documented vs Undocumented

Andreas Kogler @0xhilbert andreas.kogler@iaik.tugraz.at

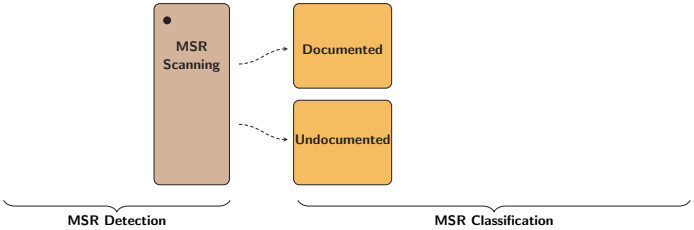
The Framework: Documented vs Undocumented



- **Parse** official PDFs
  - AMD's Reference
  - Intel's SDM

Andreas Kogler @0xhilbert andreas.kogler@iaik.tugraz.at

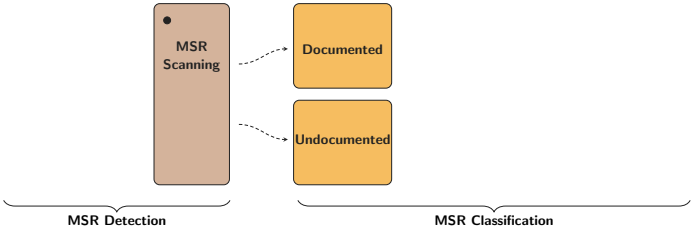
The Framework: Documented vs Undocumented



- **Parse** official PDFs
  - AMD's Reference
  - Intel's SDM
- **Extract** table structures
  - Python script

Andreas Kogler @0xhilbert andreas.kogler@iaik.tugraz.at

The Framework: Documented vs Undocumented



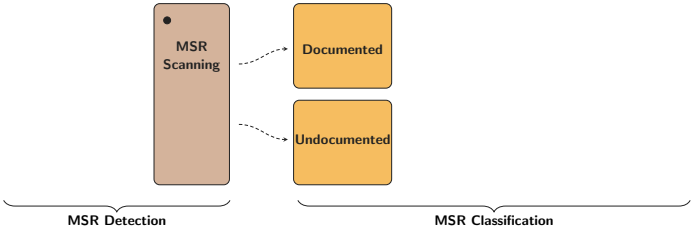
- **Parse** official PDFs
  - AMD's Reference
  - Intel's SDM
- **Extract** table structures
  - Python script

✓ Documented MSRs

✓ Undocumented MSRs

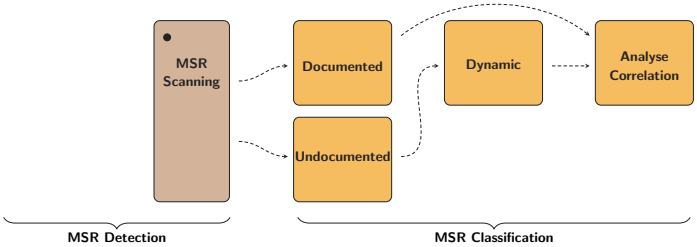
Andreas Kogler @0xhilbert andreas.kogler@iaik.tugraz.at

The Framework: Dynamic Analysis



Andreas Kogler @0xhilbert andreas.kogler@iaik.tugraz.at

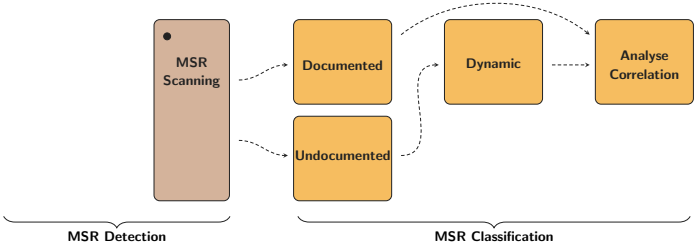
The Framework: Dynamic Analysis



- **Dynamic** MSR:
  - Changing signals

Andreas Kogler @0xhilbert andreas.kogler@iaik.tugraz.at

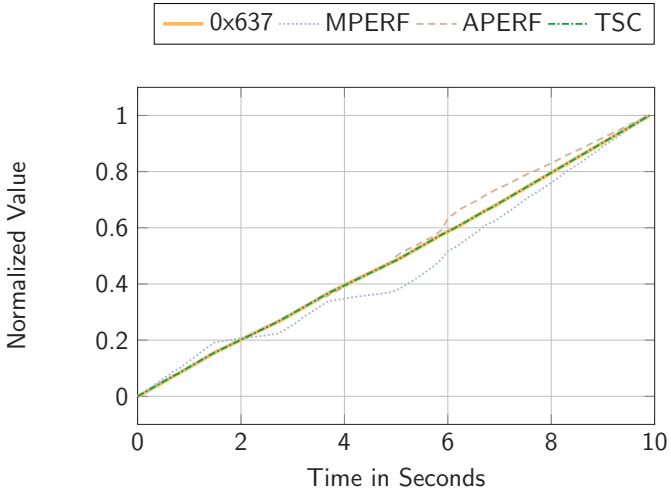
The Framework: Dynamic Analysis



- **Dynamic** MSR:
  - Changing signals
- **Correlation** analysis
  - Similarity
  - Source

Andreas Kogler @0xhilbert andreas.kogler@iaik.tugraz.at

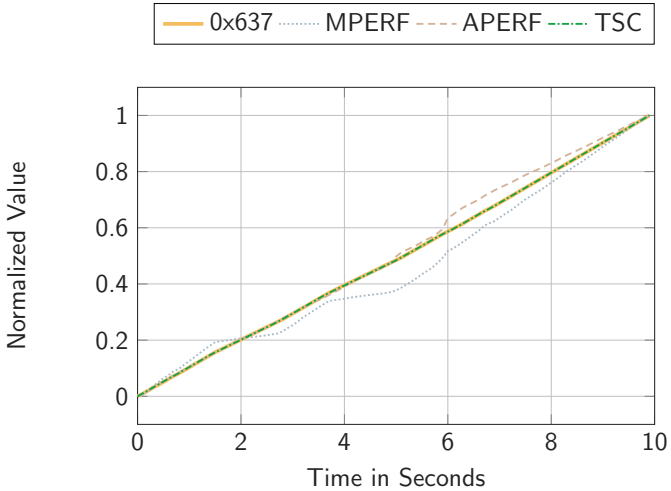
The Framework: Dynamic Analysis



- **Dynamic** MSR:
  - Changing signals
- **Correlation** analysis
  - Similarity
  - Source
- **Example:** MSR 0x637

Andreas Kogler @0xhilbert andreas.kogler@iaik.tugraz.at

The Framework: Dynamic Analysis



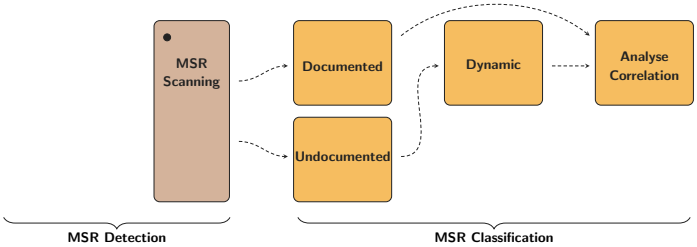
- **Dynamic** MSR:
  - Changing signals
- **Correlation** analysis
  - Similarity
  - Source
- **Example:** MSR 0x637

✓ Similar MSRs

✓ Source hints

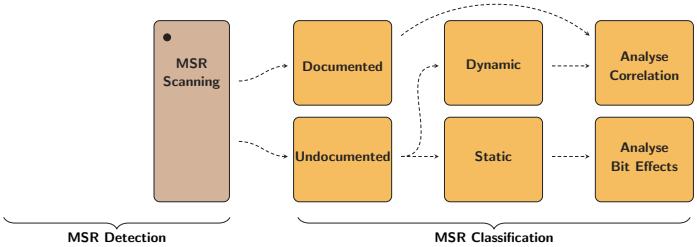
Andreas Kogler @0xhilbert andreas.kogler@iaik.tugraz.at

The Framework: Static Analysis



Andreas Kogler @0xhilbert andreas.kogler@iaik.tugraz.at

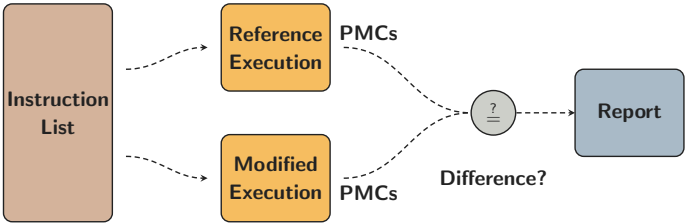
The Framework: Static Analysis



- **Static** MSR:
  - Configuration bits

Andreas Kogler @0xhilbert andreas.kogler@iaik.tugraz.at

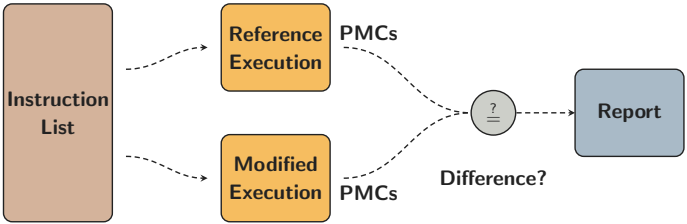
The Framework: Static Analysis



- **Static** MSR:
  - Configuration bits
- **Execute** instruction twice
  - Reference
  - Modified

Andreas Kogler @0xhilbert andreas.kogler@iaik.tugraz.at

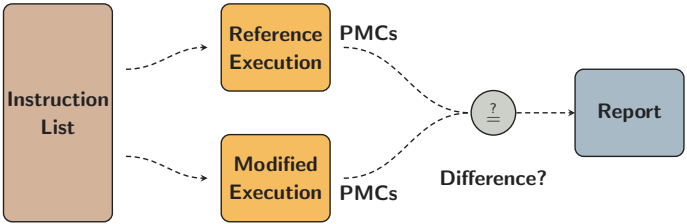
The Framework: Static Analysis



- **Static** MSR:
  - Configuration bits
- **Execute** instruction twice
  - Reference
  - Modified
- **Analyze** PMC differences

Andreas Kogler @0xhilbert andreas.kogler@iaik.tugraz.at

The Framework: Static Analysis

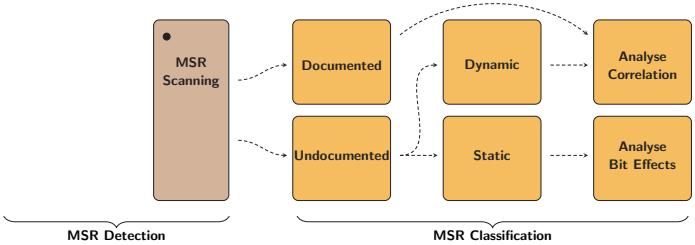


- **Static** MSR:
  - Configuration bits
- **Execute** instruction twice
  - Reference
  - Modified
- **Analyze** PMC differences

✓ Influenced instructions

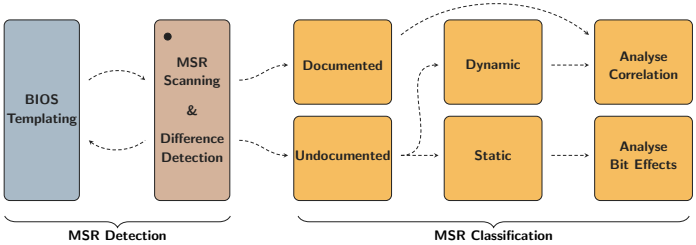
Andreas Kogler @0xhilbert andreas.kogler@iaik.tugraz.at

The Framework: BIOS Templating



Andreas Kogler @0xhilbert andreas.kogler@iaik.tugraz.at

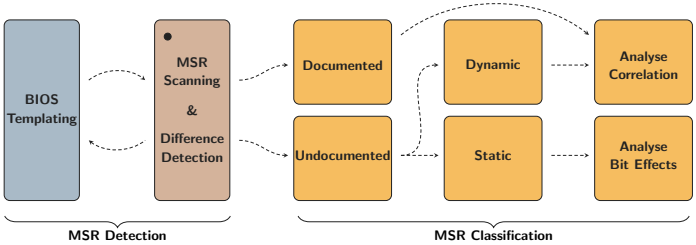
The Framework: BIOS Templating



- **Extend** search space

Andreas Kogler @0xhilbert andreas.kogler@iaik.tugraz.at

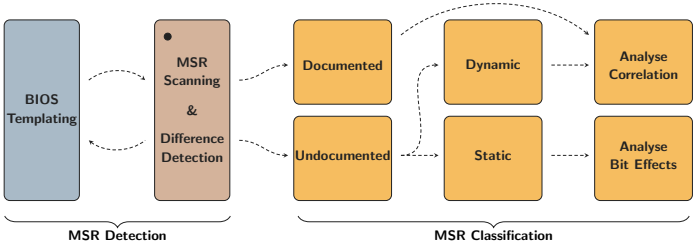
The Framework: BIOS Templating



- **Extend** search space
- **Change** BIOS feature

Andreas Kogler @0xhilbert andreas.kogler@iaik.tugraz.at

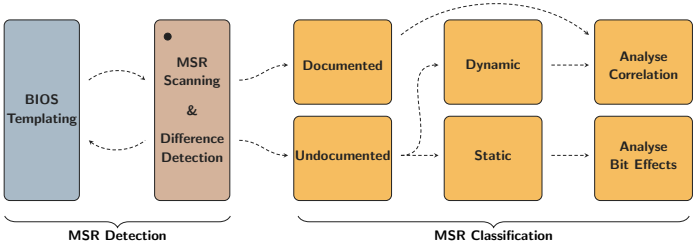
The Framework: BIOS Templating



- **Extend** search space
- **Change** BIOS feature
- **Trace** differences

Andreas Kogler @0xhilbert andreas.kogler@iaik.tugraz.at

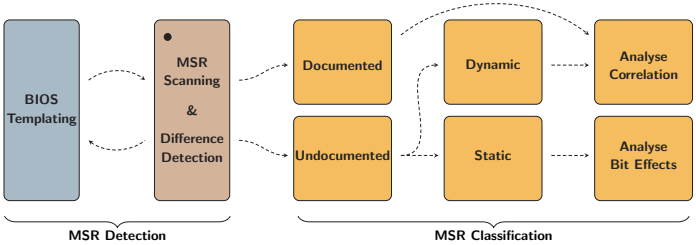
The Framework: BIOS Templating



- **Extend** search space
- **Change** BIOS feature
- **Trace** differences
- ✓ Changed MSRs

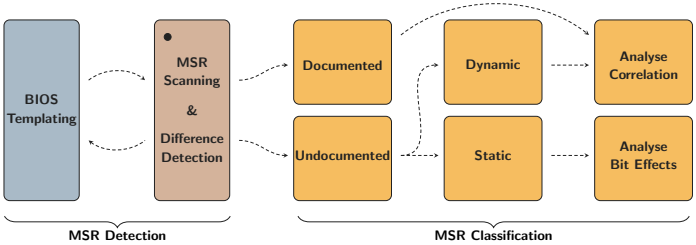
Andreas Kogler @0xhilbert andreas.kogler@iaik.tugraz.at

The Framework: Summary



Andreas Kogler @0xhilbert andreas.kogler@iaik.tugraz.at

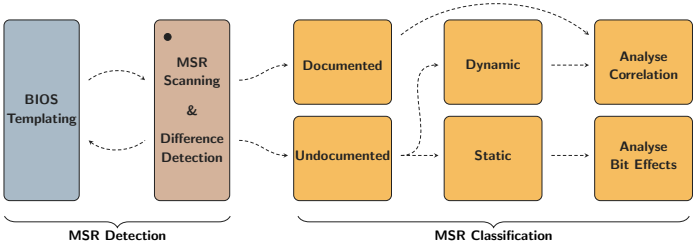
The Framework: Summary



✓ List (R, W, RW, or NP)

Andreas Kogler @0xhilbert andreas.kogler@iaik.tugraz.at

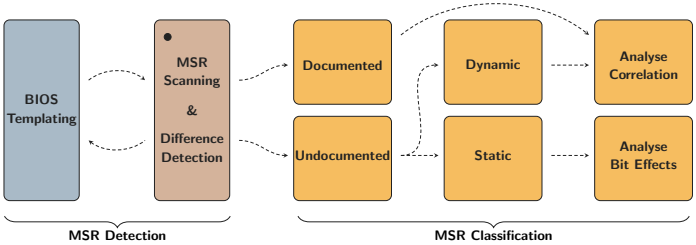
The Framework: Summary



- ✓ List (*R*, *W*, *RW*, or *NP*)
- ✓ Dynamic: similar MSRs

Andreas Kogler @0xhilbert andreas.kogler@iaik.tugraz.at

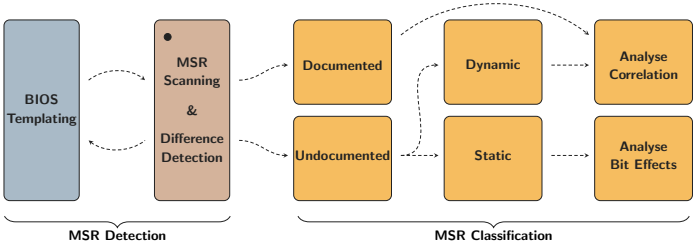
The Framework: Summary



- ✓ List (*R*, *W*, *RW*, or *NP*)
- ✓ Dynamic: similar MSRs
- ✓ Static: influenced instruction

Andreas Kogler @0xhilbert andreas.kogler@iaik.tugraz.at

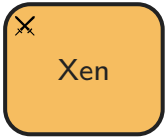
The Framework: Summary



- ✓ List (*R*, *W*, *RW*, or *NP*)
- ✓ Dynamic: similar MSRs
- ✓ Static: influenced instruction
- ✓ BIOS: changed MSRs

Andreas Kogler @0xhilbert andreas.kogler@iaik.tugraz.at

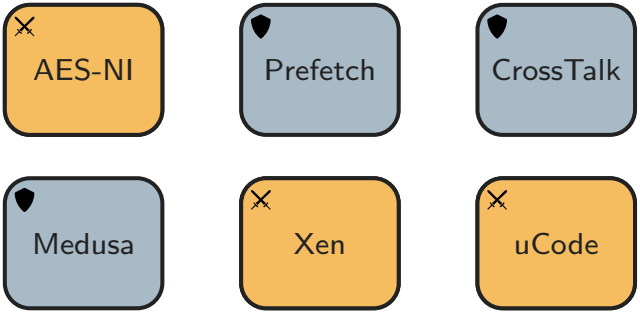
Case Studies



- **Attack** case studies

Andreas Kogler @0xhilbert andreas.kogler@iaik.tugraz.at

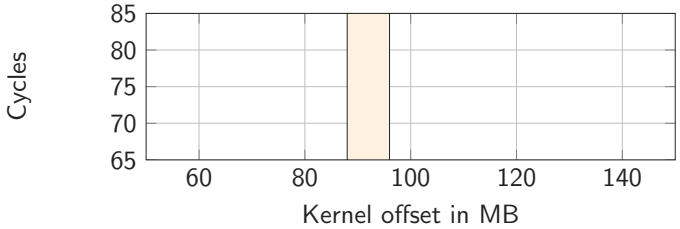
Case Studies



- **Attack** case studies
- **Defense** case studies

Andreas Kogler @0xhilbert andreas.kogler@iaik.tugraz.at

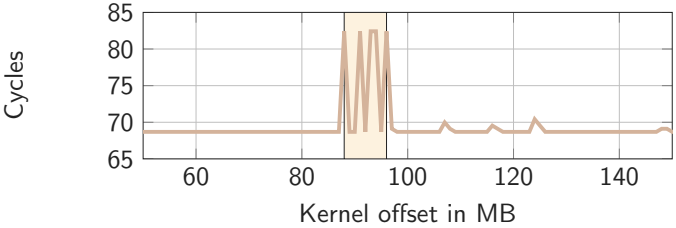
Case Study: Prefetch



- **Prefetch-based** attacks [2]

Andreas Kogler @0xhilbert andreas.kogler@iaik.tugraz.at

Case Study: Prefetch



- **Prefetch-based** attacks [2]

Andreas Kogler @0xhilbert andreas.kogler@iaik.tugraz.at

Case Study: Prefetch

Instruction	MSR	PMC Effect
`PREFETCHNTA`	Bit 2	-1 LdDispatch
`PREFETCHT0`	Bit 3	-1 LdDispatch
`PREFETCHT1`	Bit 4	-1 LdDispatch
`PREFETCHT2`	Bit 5	-1 LdDispatch
`PREFETCHW`	Bit 6	-1 LdDispatch
`PREFETCH`	Bit 7	-1 LdDispatch

- **Prefetch-based** attacks [2]
- **Search** configuration bits

Andreas Kogler @0xhilbert andreas.kogler@iaik.tugraz.at

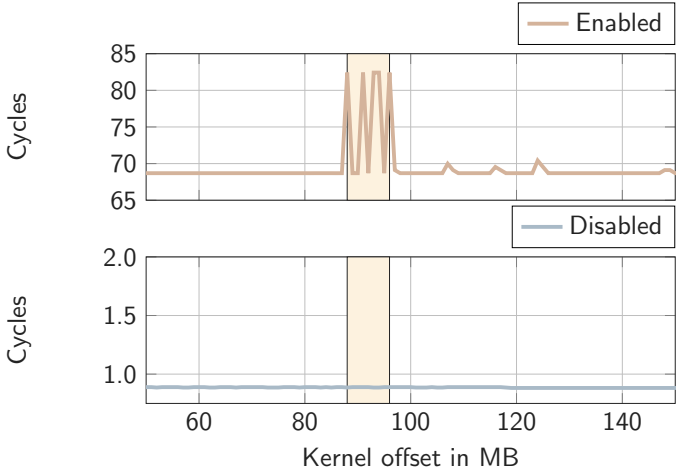
Case Study: Prefetch

Instruction	MSR	PMC Effect
`PREFETCHNTA`	Bit 2	-1 LdDispatch
`PREFETCHT0`	Bit 3	-1 LdDispatch
`PREFETCHT1`	Bit 4	-1 LdDispatch
`PREFETCHT2`	Bit 5	-1 LdDispatch
`PREFETCHW`	Bit 6	-1 LdDispatch
`PREFETCH`	Bit 7	-1 LdDispatch

- **Prefetch-based** attacks [2]
- **Search** configuration bits
- **Disable** `prefetch*`

Andreas Kogler @0xhilbert andreas.kogler@iaik.tugraz.at

Case Study: Prefetch

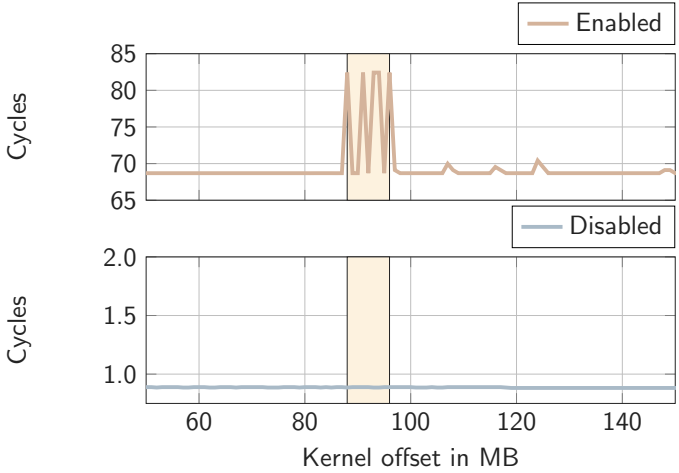


- **Prefetch-based** attacks [2]
- **Search** configuration bits
- **Disable** `prefetch*`

✓ **No** prefetch-based attacks

Andreas Kogler @0xhilbert andreas.kogler@iaik.tugraz.at

Case Study: Prefetch



- **Prefetch-based** attacks [2]
- **Search** configuration bits
- **Disable** `prefetch*`

✓ **No** prefetch-based attacks

✓ 1% Binaries → 0.04% SPEC

Andreas Kogler @0xhilbert andreas.kogler@iaik.tugraz.at

Case Study: AES-NI

- **Lock** bit

Andreas Kogler @0xhilbert andreas.kogler@iaik.tugraz.at

Case Study: AES-NI

- **Lock** bit
- **Disable** at runtime

Andreas Kogler @0xhilbert andreas.kogler@iaik.tugraz.at

Case Study: AES-NI

```
/* ... */
if( mbedtls_aesni_has_support( MBEDTLS_AESNI_AES ) )
        return( mbedtls_aesni_setkey_enc( ctx->rk, key, keybits ) );
/* ... */
switch( ctx->nr ) {
    case 10:
        for( i = 0; i < 10; i++, RK += 4 ) {
            RK[4]  = RK[0] ^ RCON[i] ^
            ( FSb[ ( RK[3] >>  8 ) & 0xFF ]       ) ^
            ( FSb[ ( RK[3] >> 16 ) & 0xFF ] <<  8 ) ^
            ( FSb[ ( RK[3] >> 24 ) & 0xFF ] << 16 ) ^
            ( FSb[ ( RK[3]       ) & 0xFF ] << 24 );

            RK[5]  = RK[1] ^ RK[4];
            RK[6]  = RK[2] ^ RK[5];
            RK[7]  = RK[3] ^ RK[6];
        }
        break;
    /* additional cases for different key lengths */
}
/* ... */
```

- **Lock** bit
- **Disable** at runtime
- **MbedTLS** in SGX

Andreas Kogler @0xhilbert andreas.kogler@iaik.tugraz.at

Case Study: AES-NI

```
/* ... */
if( mbedtls_aesni_has_support( MBEDTLS_AESNI_AES ) )
        return( mbedtls_aesni_setkey_enc( ctx->rk, key, keybits ) );
/* ... */
switch( ctx->nr ) {
    case 10:
        for( i = 0; i < 10; i++, RK += 4 ) {
            RK[4]  = RK[0] ^ RCON[i] ^
            ( FSb[ ( RK[3] >>  8 ) & 0xFF ]       ) ^
            ( FSb[ ( RK[3] >> 16 ) & 0xFF ] <<  8 ) ^
            ( FSb[ ( RK[3] >> 24 ) & 0xFF ] << 16 ) ^
            ( FSb[ ( RK[3]       ) & 0xFF ] << 24 );

            RK[5]  = RK[1] ^ RK[4];
            RK[6]  = RK[2] ^ RK[5];
            RK[7]  = RK[3] ^ RK[6];
        }
        break;
    /* additional cases for different key lengths */
}
/* ... */
```

- **Lock** bit
- **Disable** at runtime
- **MbedTLS** in SGX
  - Check AES-NI

Andreas Kogler @0xhilbert andreas.kogler@iaik.tugraz.at

Case Study: AES-NI

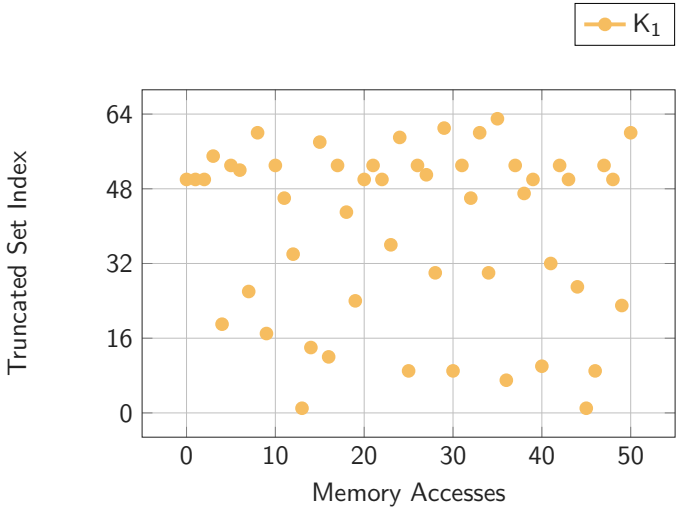
```
/* ... */
if( mbedtls_aesni_has_support( MBEDTLS_AESNI_AES ) )
        return( mbedtls_aesni_setkey_enc( ctx->rk, key, keybits ) );
/* ... */
switch( ctx->nr ) {
    case 10:
        for( i = 0; i < 10; i++, RK += 4 ) {
            RK[4]  = RK[0] ^ RCON[i] ^
            ( FSb[ ( RK[3] >>  8 ) & 0xFF ]       ) ^
            ( FSb[ ( RK[3] >> 16 ) & 0xFF ] <<  8 ) ^
            ( FSb[ ( RK[3] >> 24 ) & 0xFF ] << 16 ) ^
            ( FSb[ ( RK[3]       ) & 0xFF ] << 24 );

            RK[5]  = RK[1] ^ RK[4];
            RK[6]  = RK[2] ^ RK[5];
            RK[7]  = RK[3] ^ RK[6];
        }
        break;
    /* additional cases for different key lengths */
}
/* ... */
```

- **Lock** bit
- **Disable** at runtime
- **MbedTLS** in SGX
  - Check AES-NI
  - Fallback T-Tables

Andreas Kogler @0xhilbert andreas.kogler@iaik.tugraz.at

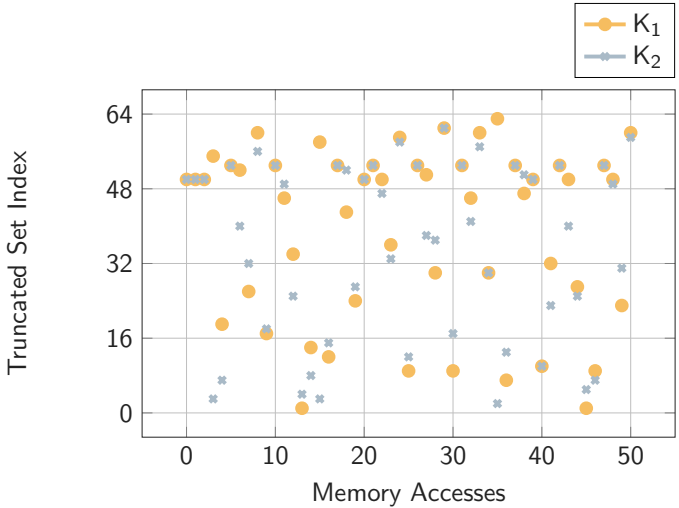
Case Study: AES-NI



- **Lock** bit
- **Disable** at runtime
- **MbedTLS** in SGX
  - Check AES-NI
  - Fallback T-Tables
  - LLC P+P

Andreas Kogler @0xhilbert andreas.kogler@iaik.tugraz.at

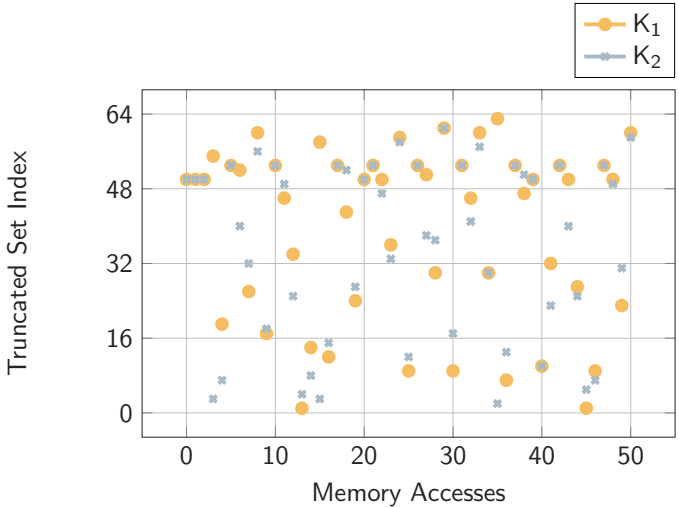
Case Study: AES-NI



- **Lock** bit
- **Disable** at runtime
- **MbedTLS** in SGX
  - Check AES-NI
  - Fallback T-Tables
  - LLC P+P

Andreas Kogler @0xhilbert andreas.kogler@iaik.tugraz.at

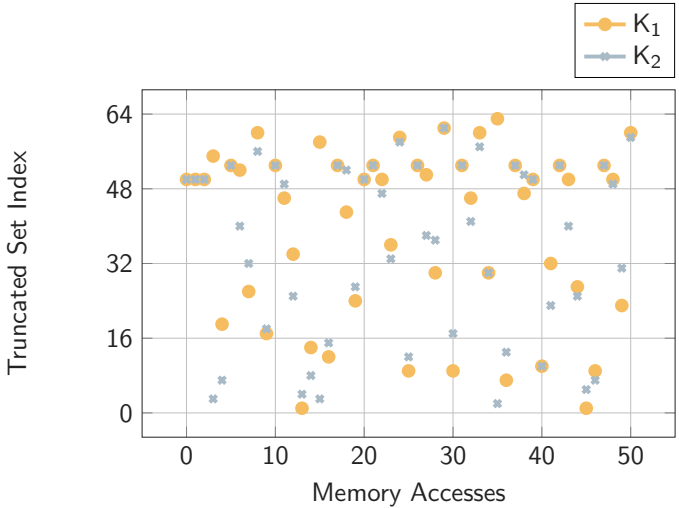
Case Study: AES-NI



- **Lock** bit
- **Disable** at runtime
- **MbedTLS** in SGX
  - Check AES-NI
  - Fallback T-Tables
  - LLC P+P
  - Z3 Solver

Andreas Kogler @0xhilbert andreas.kogler@iaik.tugraz.at

Case Study: AES-NI



- **Lock** bit
- **Disable** at runtime
- **MbedTLS** in SGX
  - Check AES-NI
  - Fallback T-Tables
  - LLC P+P
  - Z3 Solver

✓ Full key

Andreas Kogler @0xhilbert andreas.kogler@iaik.tugraz.at

Case Study: CrossTalk

- **CrossTalk** attack [3]

Andreas Kogler @0xhilbert andreas.kogler@iaik.tugraz.at

Case Study: CrossTalk

- **CrossTalk** attack [3]
- **Unpriviledged** leakage
  - `cpuid` → 88.9%
  - `rdseed` → 0.4%

Andreas Kogler @0xhilbert andreas.kogler@iaik.tugraz.at

Case Study: CrossTalk

- **CrossTalk** attack [3]
- **Unpriviledged** leakage
  - `cpuid` → 88.9%
  - `rdseed` → 0.4%
- **Search** configuration bits

Andreas Kogler @0xhilbert andreas.kogler@iaik.tugraz.at

Case Study: CrossTalk

- **CrossTalk** attack [3]
- **Unpriviledged** leakage
  - `cpuid` → 88.9%
  - `rdseed` → 0.4%
- **Search** configuration bits
- **CPUID** trap

Andreas Kogler @0xhilbert andreas.kogler@iaik.tugraz.at

Case Study: CrossTalk

- **CrossTalk** attack [3]
- **Unpriviledged** leakage
  - ~~`cpuid` → 88.9%~~
  - `rdseed` → 0.4%
- **Search** configuration bits
- **CPUID** trap

✓ Reduced by **211.4** times

Andreas Kogler @0xhilbert andreas.kogler@iaik.tugraz.at

Case Study: Xen Foreshadow

Hardware:

Xen HV:

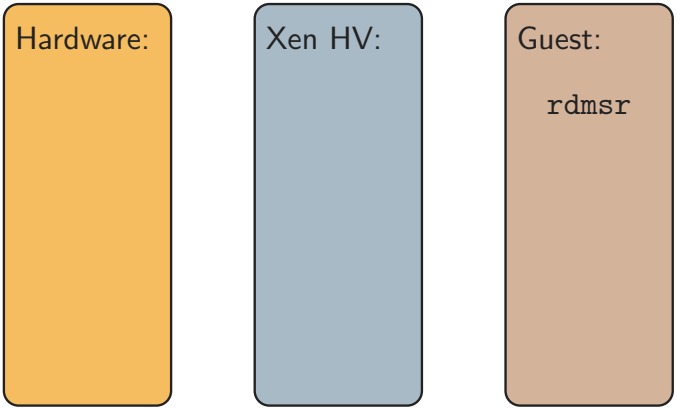
Guest:

```
rdmsr
```

- **Hypervisor** handles MSRs

Andreas Kogler @0xhilbert andreas.kogler@iaik.tugraz.at

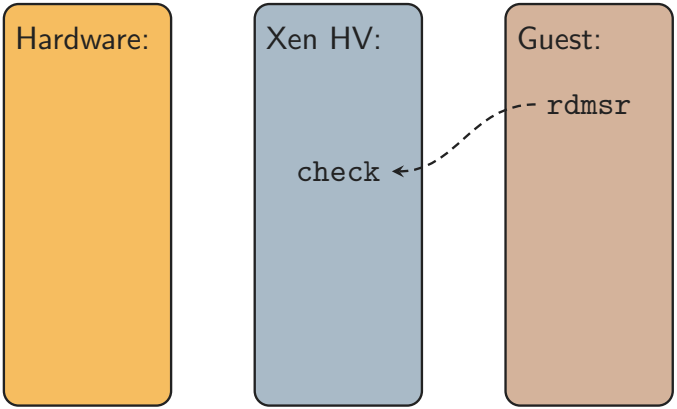
Case Study: Xen Foreshadow



- **Hypervisor** handles MSRs
- **XEN** deny list

Andreas Kogler @0xhilbert andreas.kogler@iaik.tugraz.at

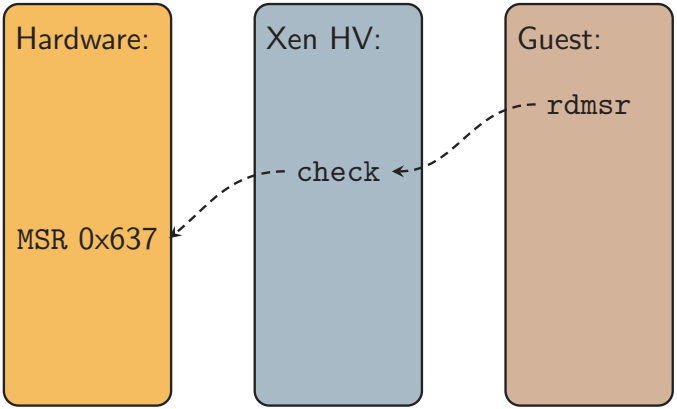
Case Study: Xen Foreshadow



- **Hypervisor** handles MSRs
- **XEN** deny list

Andreas Kogler @0xhilbert andreas.kogler@iaik.tugraz.at

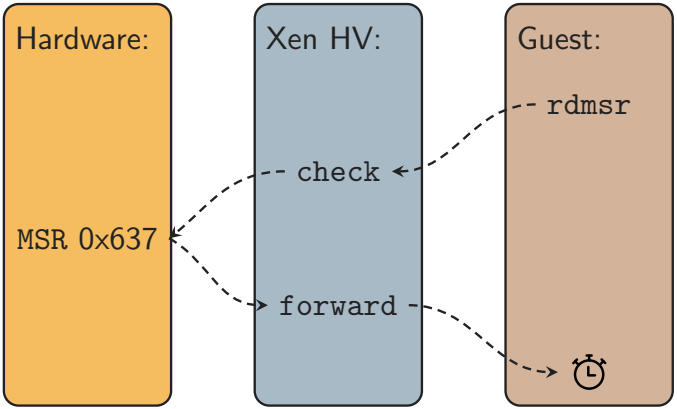
Case Study: Xen Foreshadow



- **Hypervisor** handles MSRs
- **XEN** deny list
- **Unrestricted** read access

Andreas Kogler @0xhilbert andreas.kogler@iaik.tugraz.at

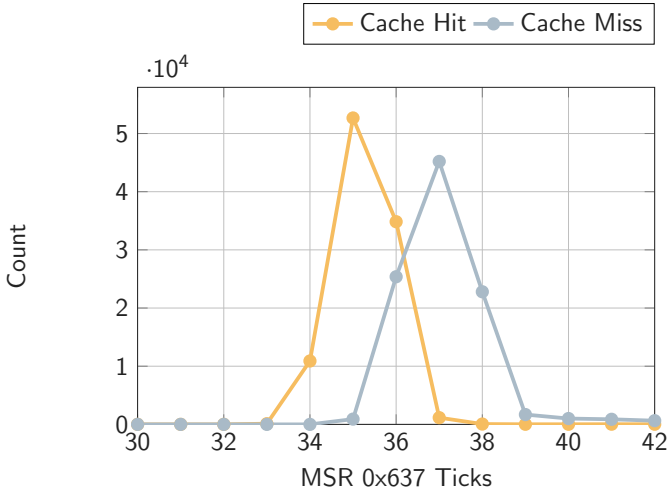
Case Study: Xen Foreshadow



- **Hypervisor** handles MSRs
- **XEN** deny list
- **Unrestricted** read access
- **Timer** MSR

Andreas Kogler @0xhilbert andreas.kogler@iaik.tugraz.at

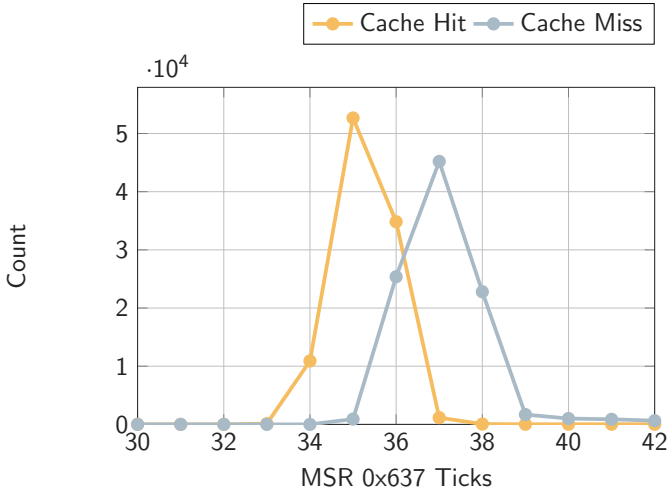
Case Study: Xen Foreshadow



- **Hypervisor** handles MSRs
- **XEN** deny list
- **Unrestricted** read access
- **Timer** MSR
  - Cache hit vs miss

Andreas Kogler @0xhilbert andreas.kogler@iaik.tugraz.at

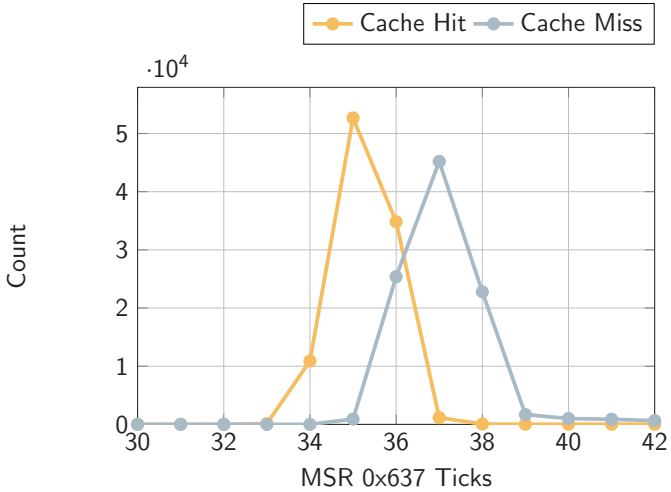
Case Study: Xen Foreshadow



- **Hypervisor** handles MSRs
- **XEN** deny list
- **Unrestricted** read access
- **Timer** MSR
  - Cache hit vs miss
  - Foreshadow attack [4]

Andreas Kogler @0xhilbert andreas.kogler@iaik.tugraz.at

Case Study: Xen Foreshadow

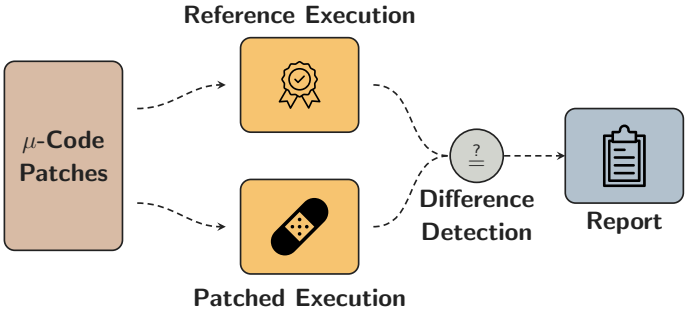


- **Hypervisor** handles MSRs
- **XEN** deny list
- **Unrestricted** read access
- **Timer** MSR
  - Cache hit vs miss
  - Foreshadow attack [4]

✓ Leak **214** Byte/s

Andreas Kogler @0xhilbert andreas.kogler@iaik.tugraz.at

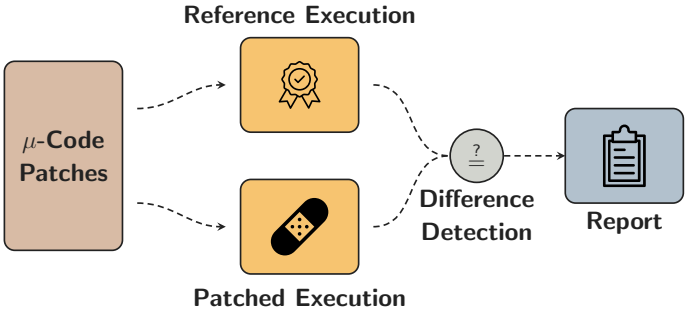
Case Study: uCode Diffing



- **Analyze** μ-Code Patches

Andreas Kogler @0xhilbert andreas.kogler@iaik.tugraz.at

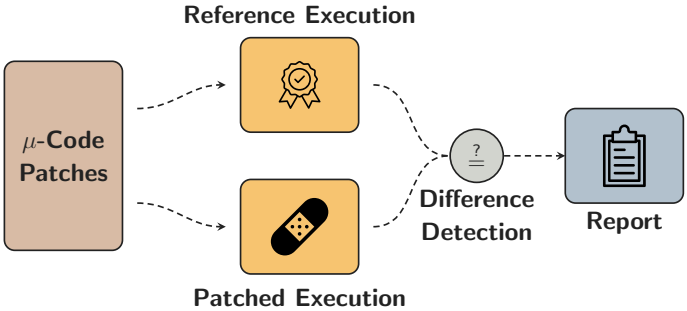
Case Study: uCode Diffing



- **Analyze** μ-Code Patches
- **Detect** new

Andreas Kogler @0xhilbert andreas.kogler@iaik.tugraz.at

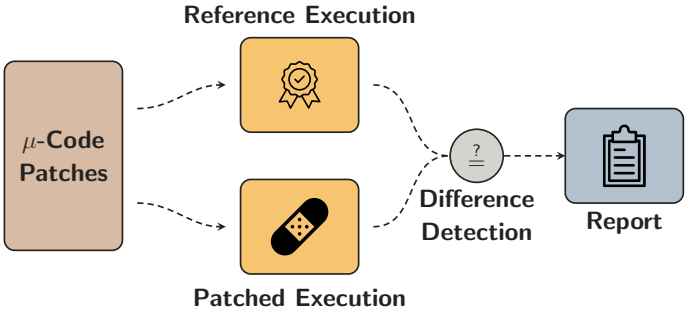
Case Study: uCode Diffing



- **Analyze** μ-Code Patches
- **Detect** new
- **Detect** affected instructions

Andreas Kogler @0xhilbert andreas.kogler@iaik.tugraz.at

Case Study: uCode Diffing



- **Analyze** μ-Code Patches
- **Detect** new
- **Detect** affected instructions

✓ Before public disclosure

Andreas Kogler @0xhilbert andreas.kogler@iaik.tugraz.at

Conclusion

- **Framework** https://github.com/IAIK/msrevelio

Andreas Kogler @0xhilbert andreas.kogler@iaik.tugraz.at

Conclusion

- **Framework** `https://github.com/IAIK/msrevelio`
- **Case Studies**

Andreas Kogler @0xhilbert andreas.kogler@iaik.tugraz.at

Conclusion

- **Framework** https://github.com/IAIK/msrevelio
- **Case Studies**
- **MSRs** enable defenses

Andreas Kogler @0xhilbert andreas.kogler@iaik.tugraz.at

Conclusion

- **Framework** https://github.com/IAIK/msrevelio
- **Case Studies**
- **MSRs** enable defenses
- **MSRs** open new attack vectors

Andreas Kogler @0xhilbert andreas.kogler@iaik.tugraz.at

Conclusion

- **Framework** https://github.com/IAIK/msrevelio
- **Case Studies**
- **MSRs** enable defenses
- **MSRs** open new attack vectors
- For more details ...

Andreas Kogler @0xhilbert andreas.kogler@iaik.tugraz.at

Conclusion

- **Framework** https://github.com/IAIK/msrevelio
- **Case Studies**
- **MSRs** enable defenses
- **MSRs** open new attack
- For more details

Read the Paper

Andreas Kogler @0xhilbert andreas.kogler@iaik.tugraz.at

Finding and Exploiting CPU Features using MSR Templating

IEEE Symposium on Security and Privacy 2022

Andreas Kogler **@0xhilbert** **andreas.kogler@iaik.tugraz.at**

References i

- Christopher Domas. Hardware Backdoors in x86 CPUs. In: Black Hat US (2018).
- Daniel Gruss, Clémentine Maurice, Anders Fogh, Moritz Lipp, and Stefan Mangard. Prefetch Side-Channel Attacks: Bypassing SMAP and Kernel ASLR. In: CCS. 2016.
- Hany Ragab, Alyssa Milburn, Kaveh Razavi, Herbert Bos, and Cristiano Giuffrida. CrossTalk: Speculative Data Leaks Across Cores Are Real. In: S&P. 2021.
- Ofir Weisse, Jo Van Bulck, Marina Minkin, Daniel Genkin, Baris Kasikci, Frank Piessens, Mark Silberstein, Raoul Strackx, Thomas F Wenisch, and Yuval Yarom. Foreshadow-NG: Breaking the virtual memory abstraction with transient out-of-order execution. In: (2018).

Andreas Kogler @0xhilbert andreas.kogler@iaik.tugraz.at

Overall Results

CPU	AMD	Intel			
	Threadripper 1920X	i7-6700k	i7-8700k	i9-9900k	Xeon Silver 4208
μ-**Arch**	Zen	Skylake	Coffee Lake	Coffee Lake	Cascade Lake
μ-**Code**	0x8001137	0x9e	0xb4	0xde	0x5003102
# Found[1]	5244 (5223, 17, 4)	477 (363, 108, 5)	517 (388, 122, 7)	537 (413, 117, 7)	1109 (957, 142, 10)
# Undoc[1]	4876 (4873, 2, 1)	105 (68, 35, 2)	126 (89, 35, 2)	136 (99, 35, 2)	647 (591, 52, 4)
# Static[2]	4873 (4871, 2)	99 (68, 31)	121 (89, 32)	132 (99, 33)	601 (553, 48)
# Dynamic[2]	2 (2, 0)	4 (0, 4)	3 (0, 3)	2 (0, 2)	42 (38, 4)
# Similar	0	2	3	2	42

[1] $\sum$ (RW, RO, WO) [2] $\sum$ (RW, RO)

Andreas Kogler @0xhilbert andreas.kogler@iaik.tugraz.at