TU Graz
SCIENCE
PASSION
TECHNOLOGY

When Good Kernel Defenses Go Bad:

Reliable and Stable Kernel Exploits via Defense-Amplified TLB Side-Channel Leaks

Lukas Maar Lukas Giner Daniel Gruss Stefan Mangard

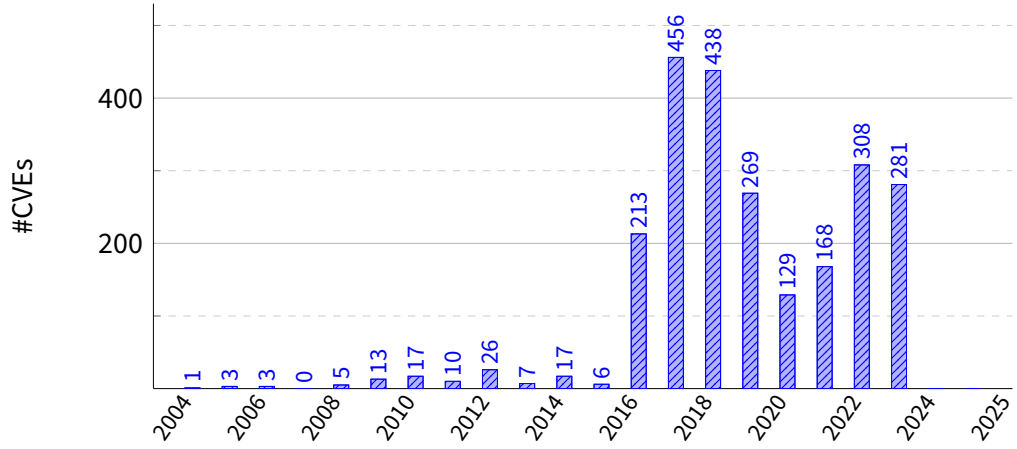
August 13-15, 2025

USENIX Security

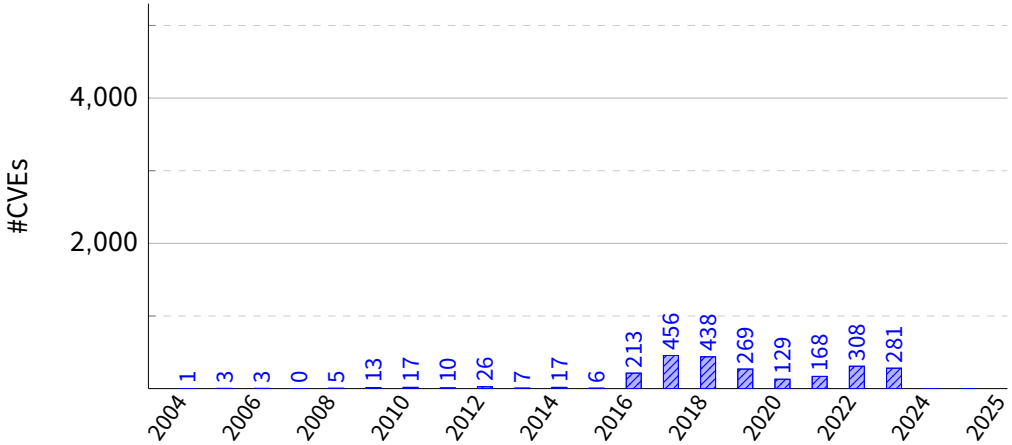
› isec.tugraz.at

Motivation

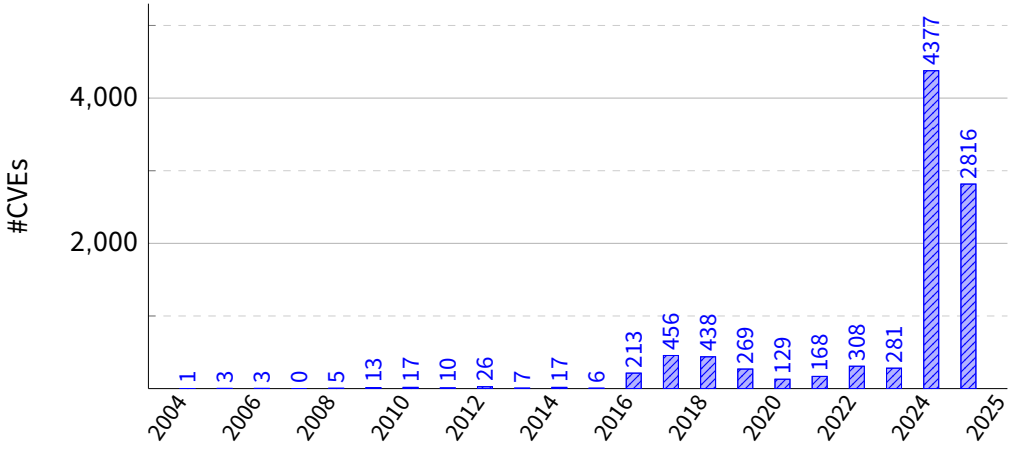
Motivation


#CVEs
400
200
1
3
3
0
5
13
17
10
26
7
17
6
213
456
438
269
129
168
308
281
2004
2006
2008
2010
2012
2014
2016
2018
2020
2022
2024
2025

Motivation

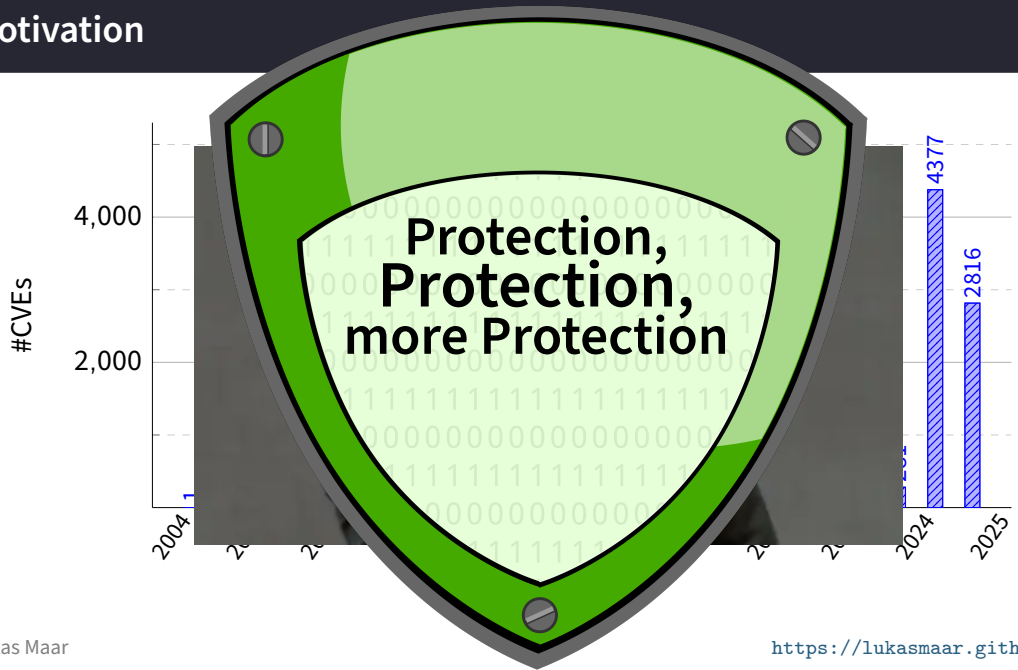

#CVEs
4,000
2,000
1
3
3
0
5
13
17
10
26
7
17
6
213
456
438
269
129
168
308
281
2004
2006
2008
2010
2012
2014
2016
2018
2020
2022
2024
2025

Motivation


#CVEs
4,000
2,000
1
3
3
0
5
13
17
10
26
7
17
6
213
456
438
269
129
168
308
281
4377
2816
2004
2006
2008
2010
2012
2014
2016
2018
2020
2022
2024
2025

Motivation

Motivation

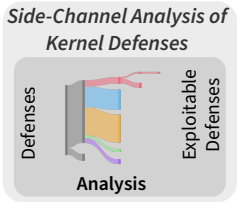

#CVEs
4,000
2,000
4377
2816
2024
2025
Protection,
Protection,
more Protection

Our Contributions

Reliable and stable side-channel-assisted kernel exploitation

Our Contributions

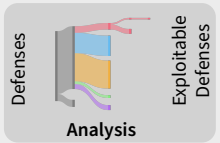
Reliable and stable side-channel-assisted kernel exploitation



Our Contributions

Reliable and stable side-channel-assisted kernel exploitation

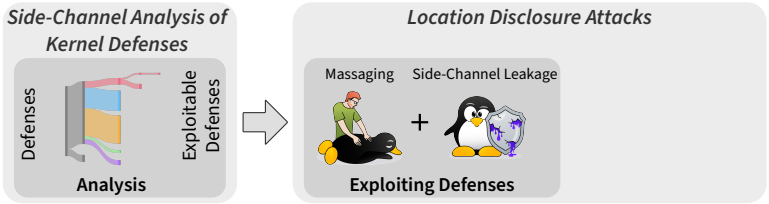
Side-Channel Analysis of Kernel Defenses



Location Disclosure Attacks

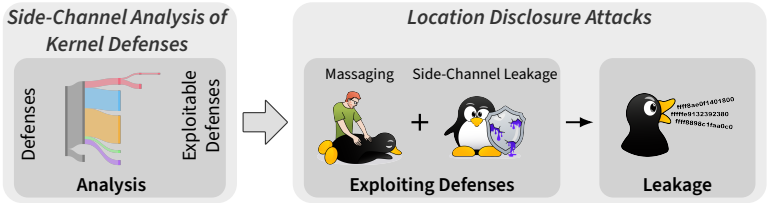
Our Contributions

Reliable and stable side-channel-assisted kernel exploitation



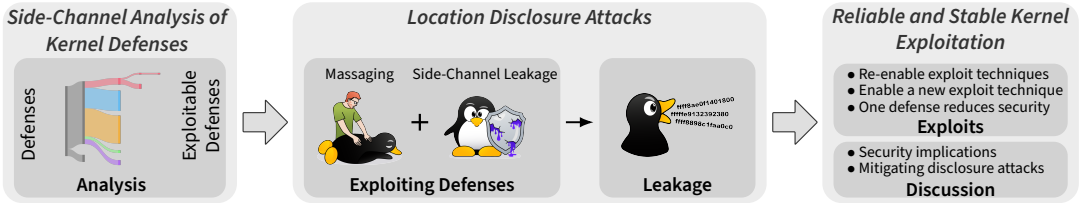
Our Contributions

Reliable and stable side-channel-assisted kernel exploitation



Our Contributions

Reliable and stable side-channel-assisted kernel exploitation



Our Contributions contd

Our Contributions contd

- **Analysis:**
  - Virtualization of the kstack
  - Virtualization of the kheap
  - Strict memory permission enforcement

Our Contributions contd

- **Analysis:**
  - Virtualization of the kstack
  - Virtualization of the kheap
  - Strict memory permission enforcement
  - Additional allocator design decisions

Our Contributions contd

- **Analysis:**
  - Virtualization of the kstack
  - Virtualization of the kheap
  - Strict memory permission enforcement
  - Additional allocator design decisions
- **Evaluation:**
  - Intel CPUs from 8th to 14th gen
  - Generic Ubuntu kernels from v5.15 to 6.8

Our Contributions contd

- **Analysis:**
  - Virtualization of the kstack
  - Virtualization of the kheap
  - Strict memory permission enforcement
  - Additional allocator design decisions
- **Evaluation:**
  - Intel CPUs from 8th to 14th gen
  - Generic Ubuntu kernels from v5.15 to 6.8
- **Results:**
  - Three side-channel-assisted exploit techniques
  - Near 100 % reliability
  - No system crashes

TU Graz
SCIENCE
PASSION
TECHNOLOGY

When Good Kernel Defenses Go Bad:

Reliable and Stable Kernel Exploits via Defense-Amplified TLB Side-Channel Leaks

Lukas Maar Lukas Giner Daniel Gruss Stefan Mangard

August 13-15, 2025

USENIX Security

› isec.tugraz.at