FlippyR.AM

Large-Scale Rowhammer Study

Andreas Schmidt (ndrscodes, ndrscodes)

March 23, 2025

Hof University, University of Applied Sciences

TU Graz

Hochschule Hof
University of Applied Sciences

FWF
NeRAM
Der Wissenschaftsfonds.
DFG Deutsche Forschungsgemeinschaft

Rowhammer

- Physical side-channel in DRAM: Frequently accessing (read or write) DRAM addresses leads to bit flips in spatially near DRAM cells
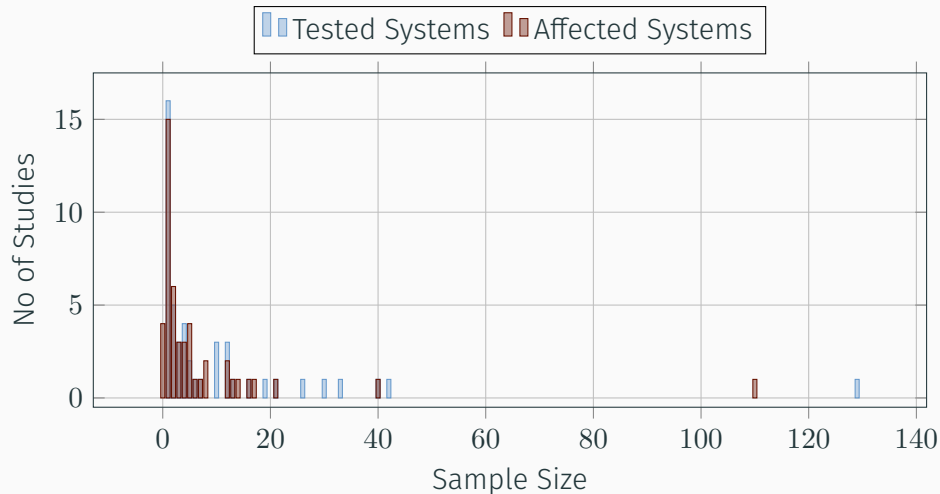
Rowhammer

- Physical side-channel in DRAM: Frequently accessing (read or write) DRAM addresses leads to bit flips in spatially near DRAM cells
- "Flipping Bits in Memory without accessing them"

Bank

Row 0
Row 1
Row 2
Row 3
Row 4
Row 5
Row 6
Row 7

Rowbuffer
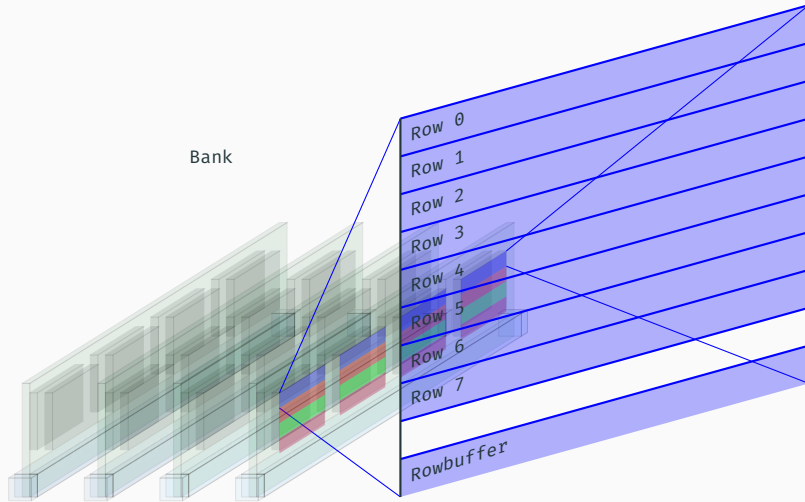
- Many exploits were published in recent years
    - NaCl Sandbox Escape
    - Local Privilege Escalation on Linux
    - Local Privilege Escalation on Android Devices
    - Bit Flips from JavaScript
    - Bit Flips over the Network
    - Bit Flips on DDR5
    - …

- Reliability? Yes, but...

Is Rowhammer relevant?

- Reliability? Yes, but...
- Exploits? Yes, but..

- Reliability? Yes, but...
- Exploits? Yes, but..
- Prevalence? Are even that many system affected?

Is Rowhammer relevant?

- Reliability? Yes, but...
- Exploits? Yes, but..
- Prevalence? Are even that many system affected?
- $\rightarrow$ We don't know!

Goal of our Study

- Real-world conditions on real systems
- Large-scale prevalence observations
- Reproducibility of bit flips
    - $\rightarrow$ are Rowhammer PUFs even practical?

How can I participate?

- Get a free bootable USB stick from us

- G

How can I participate?

- Get a free bootable USB stick from us
- or download bootable ISO from `https://FlippyR.am`
- → Run our tests while you don't need the system
  (e.g., while sleeping/at work)
- → Upload your results → then they contribute to our study

- Everything is open source: `https://FlippyR.am`
- Build the ISO and flash it yourself
- Docker-Image is available as well
- ISO-Image booted via USB is best
    - your own or ours, doesn't matter for us

Why should I participate?

- How relevant is Rowhammer on real systems?
- Academics cannot answer this alone
  - we need real users to know
- Other perks, if you want to:
  - Keep your flippyr.am USB stick
  - Get a flippyr.am t-shirt if you test at least 10 systems (2 left)
  - You can win a gift card (see website)
  - Get your name in the acknowledgements of our study
  - Learn if your own hardware is affected

- More information about FlippyR.AM on our talk Ten Years of Rowhammer: A Retrospect (and Path to the Future)
- Rowhammer: reliability issue + exploitable
- Real-world prevalence still unclear
- Join us: Contribute to the large-scale flippyr.am study!

FlippyR.AM

Large-Scale Rowhammer Study

Andreas Schmidt (ndrscodes, ndrscodes)

March 23, 2025

Hof University, University of Applied Sciences