The Evolution of Transient-Execution Attacks

Claudio Canella[1], **Khaled N. Khasawneh**[2], **Daniel Gruss**[1]

September 7-9, 2020

[1] Graz University of Technology [2] George Mason University

Motivation

- Many different transient-execution attacks

Claudio Canella[1], Khaled N. Khasawneh[2], Daniel Gruss[1]

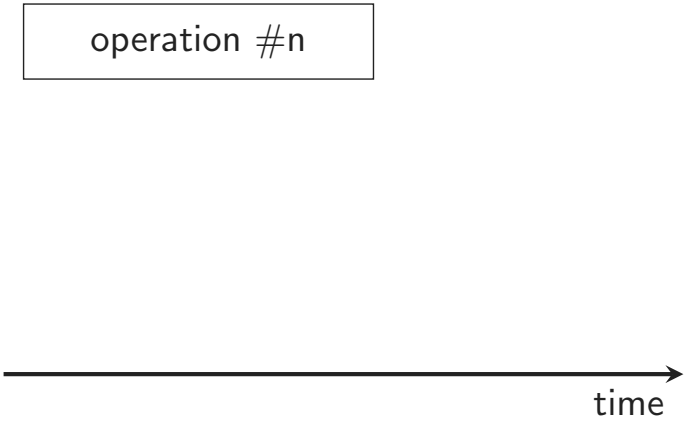
Motivation

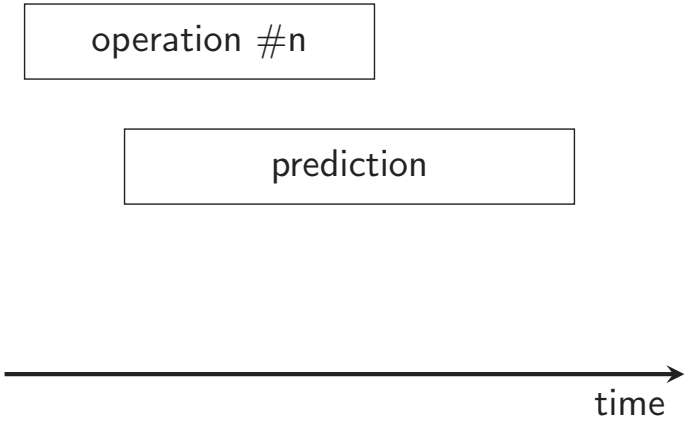
- Many different transient-execution attacks
- Previous work looked at differences of attacks

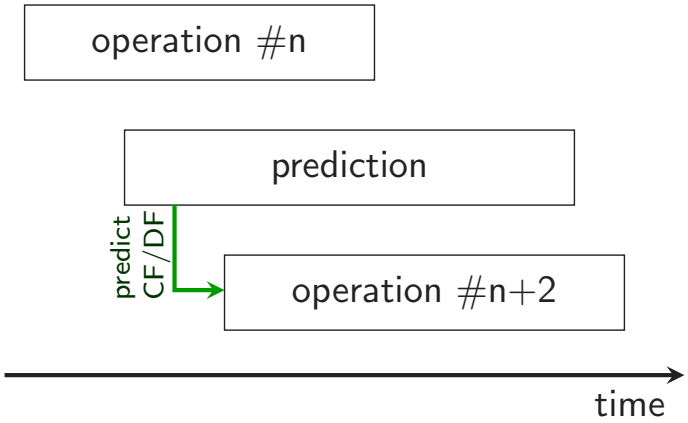
Claudio Canella[1], Khaled N. Khasawneh[2], Daniel Gruss[1]

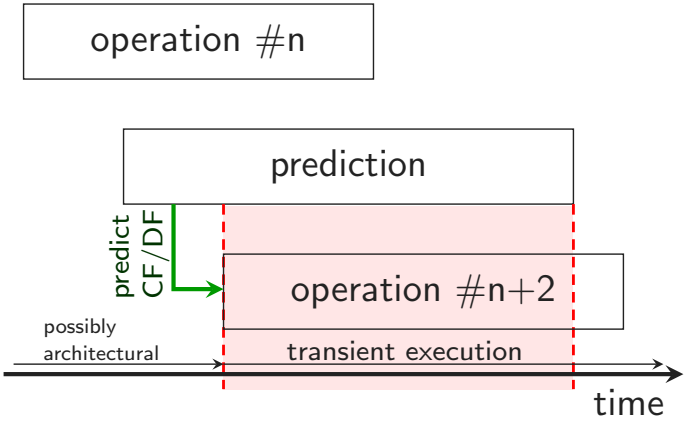
- Many different transient-execution attacks
- Previous work looked at differences of attacks
- What are the similarities?

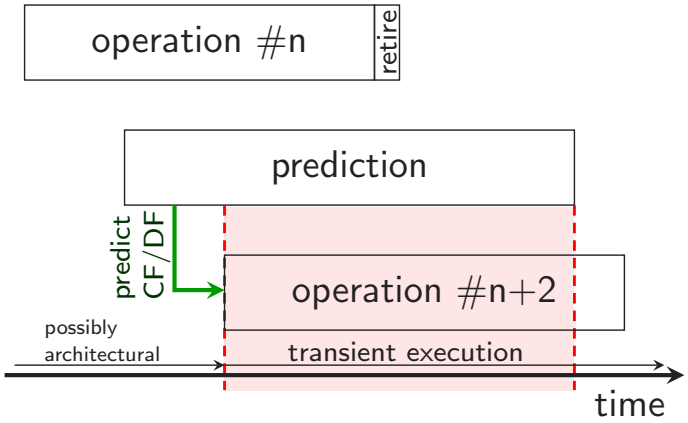
Claudio Canella[1], Khaled N. Khasawneh[2], Daniel Gruss[1]

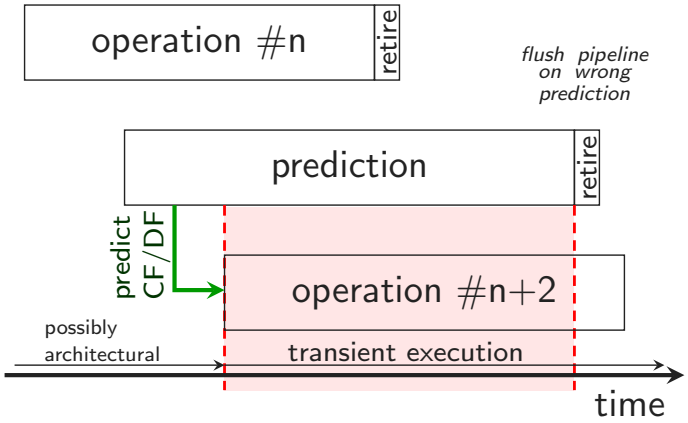

operation #n
time

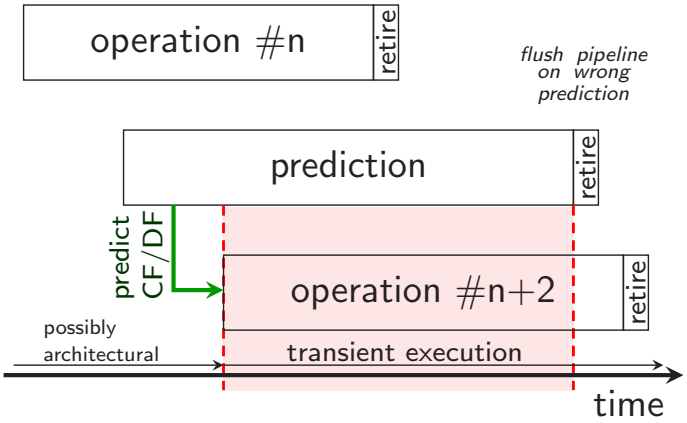

operation #n
prediction
time

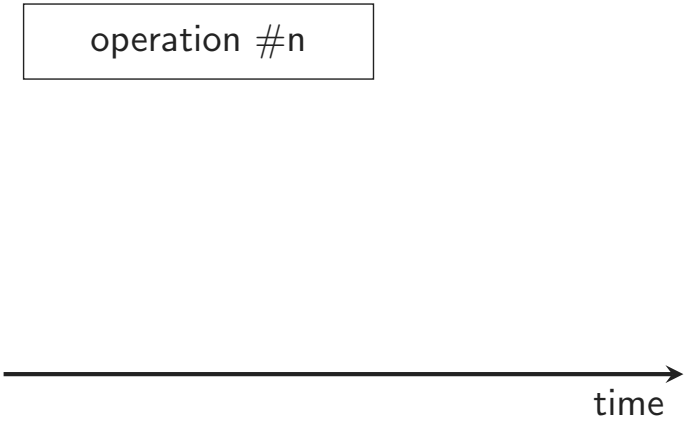

operation #n
prediction
predict
CF/DF
operation #n+2
time

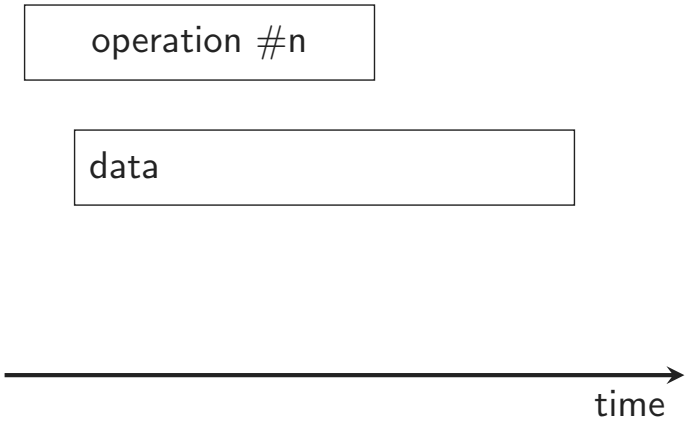

operation #n
prediction
predict CF/DF
operation #n+2
possibly architectural
transient execution
time

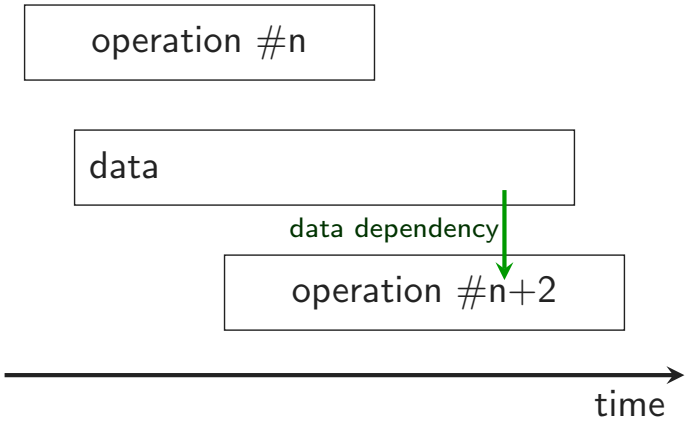

operation #n
retire
prediction
predict CF/DF
operation #n+2
possibly architectural
transient execution
time

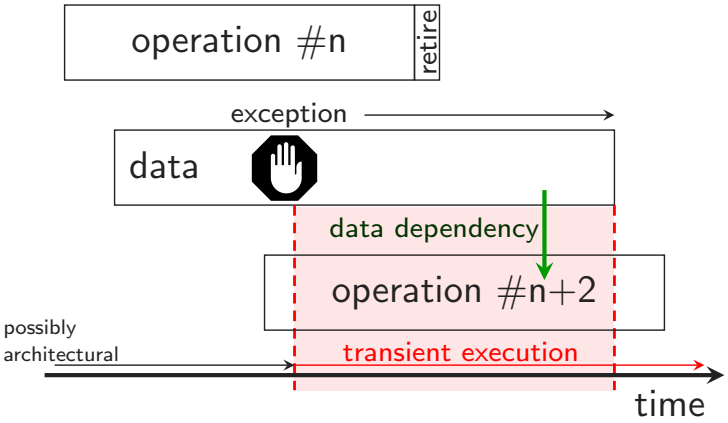

operation #n
retire
flush pipeline on wrong prediction
prediction
retire
predict CF/DF
operation #n+2
possibly architectural
transient execution
time

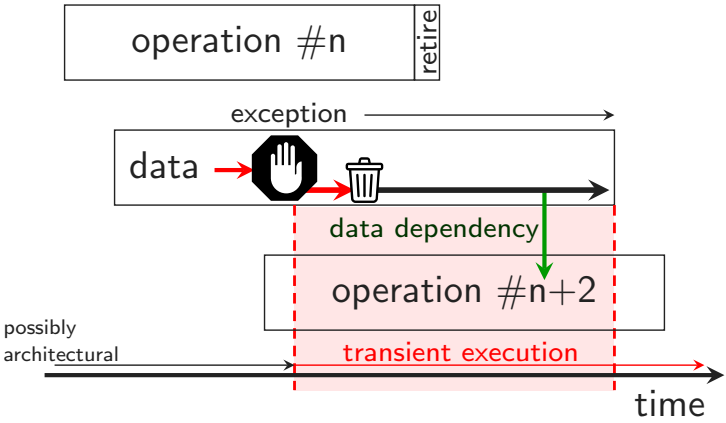

operation #n
retire
flush pipeline on wrong prediction
prediction
retire
predict CF/DF
operation #n+2
retire
possibly architectural
transient execution
time

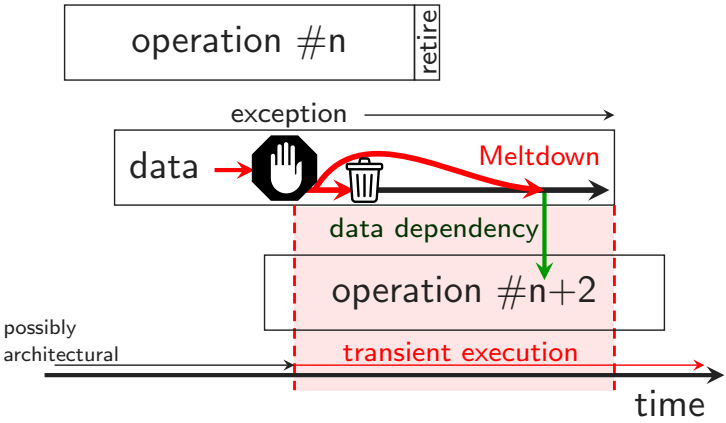

operation #n
time

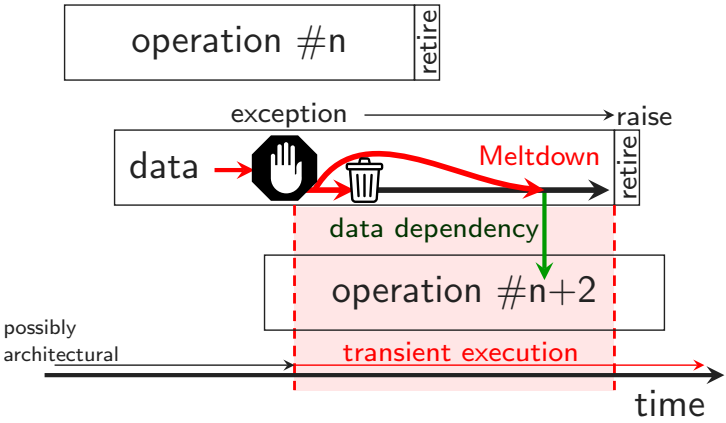

operation #n
data
time


operation #n
data
data dependency
operation #n+2
time

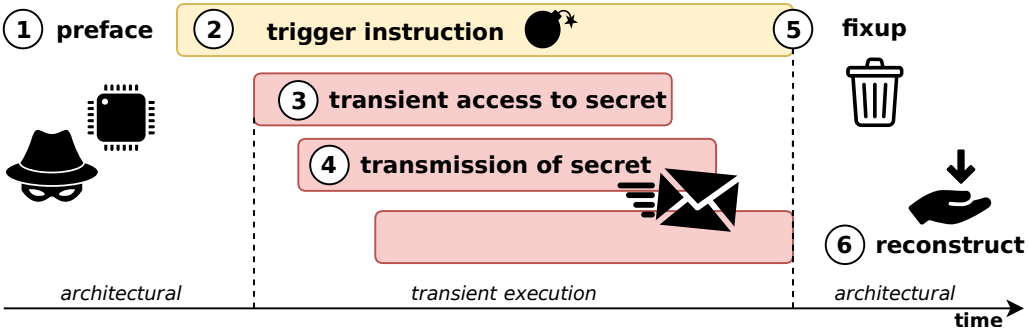

operation #n
retire
exception
data
data dependency
operation #n+2
possibly
architectural
transient execution
time


operation #n
retire
exception
data
data dependency
operation #n+2
possibly
architectural
transient execution
time

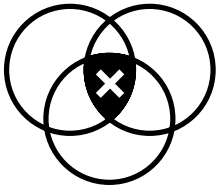

operation #n
retire
exception
data
Meltdown
data dependency
operation #n+2
possibly
architectural
transient execution
time


operation #n
retire
exception
raise
data
Meltdown
retire
data dependency
operation #n+2
possibly
architectural
transient execution
time

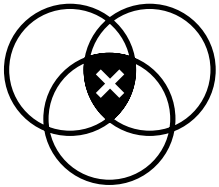
Transient-Execution Attack Phases



Claudio Canella[1], Khaled N. Khasawneh[2], Daniel Gruss[1]

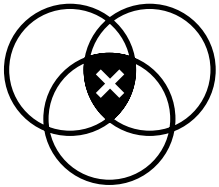


Similarities allows to group into 3 categories:



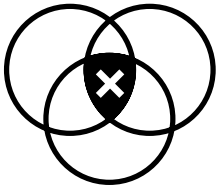
Similarities allows to group into 3 categories:

- Deferred permission check



Similarities allows to group into 3 categories:

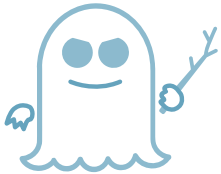
- Deferred permission check
- Incorrect use of intermediate values

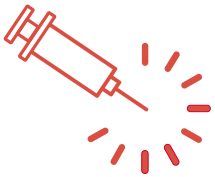


Similarities allows to group into 3 categories:

- Deferred permission check
- Incorrect use of intermediate values
- Use-after-free

Load Value Injection





Claudio Canella[1], Khaled N. Khasawneh[2], Daniel Gruss[1]

More details in the paper

- More details on the individual attacks
- Information on store-to-load forwarding
- ...

GLSVLSI'20

Claudio Canella, Khaled N. Khasawneh, Daniel Gruss.
The Evolution of Transient-Execution Attacks.

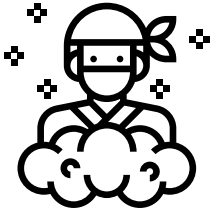
Recap

- Extended previous phases with an explicit transient access phase

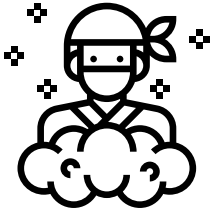
Recap

- Extended previous phases with an explicit transient access phase
- Highlighted the similarities between Meltdown-type attacks

- Extended previous phases with an explicit transient access phase
- Highlighted the similarities between Meltdown-type attacks
- Discussed the evolution of transient-execution attacks

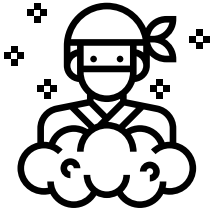


- Transient Execution Attacks are...



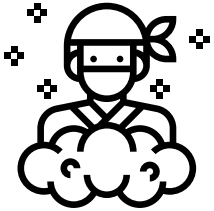
- Transient Execution Attacks are...
  - ...a novel class of attacks

Conclusion

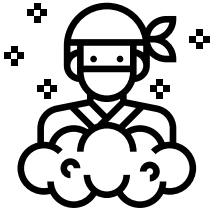


- Transient Execution Attacks are...
  - ...a novel class of attacks
  - ...extremely powerful

Claudio Canella[1], Khaled N. Khasawneh[2], Daniel Gruss[1]



- Transient Execution Attacks are...
  - ...a novel class of attacks
  - ...extremely powerful
  - ...only at the beginning



- Transient Execution Attacks are...
  - ...a novel class of attacks
  - ...extremely powerful
  - ...only at the beginning
- Many optimizations introduce side channels $\rightarrow$ now exploitable

The Evolution of Transient-Execution Attacks

Claudio Canella[1], **Khaled N. Khasawneh**[2], **Daniel Gruss**[1]

September 7-9, 2020

[1] Graz University of Technology [2] George Mason University

Acknowledgments

This project has received funding from the European Research Council (ERC) under the European Union's Horizon 2020 research and innovation program (grant agreement No 681402). This work has been supported by the Austrian Research Promotion Agency (FFG) via the project ESPRESSO, which is funded by the province of Styria and the Business Promotion Agencies of Styria and Carinthia. Additional funding was provided by generous gifts from ARM. Any opinions, findings, and conclusions or recommendations expressed in this paper are those of the authors and do not necessarily reflect the views of the funding parties.