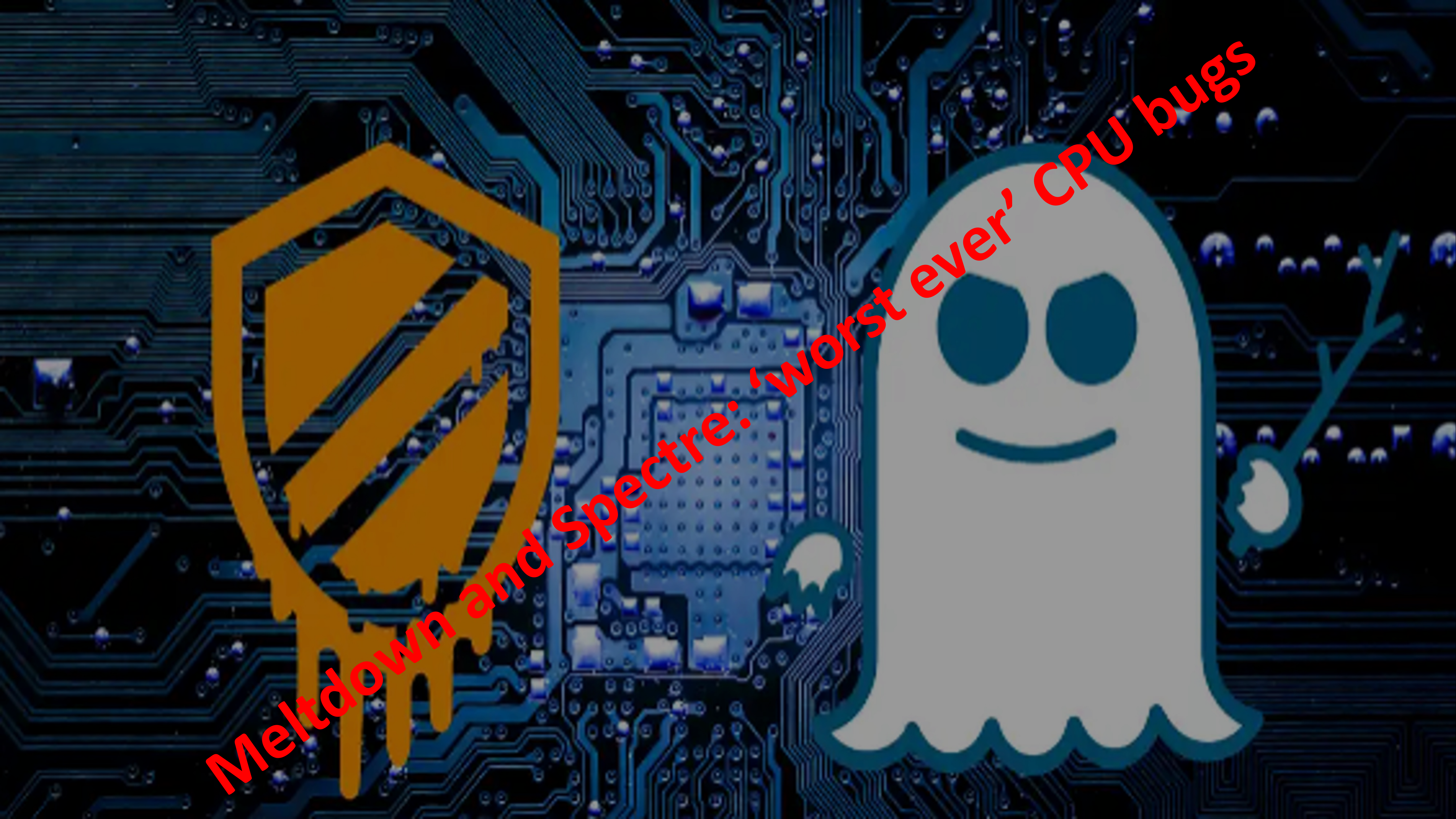
NUS
National University of Singapore

CONSTSPEC: Mitigating Cache-based Spectre Attacks via Fine-Grained Constant-Time Accesses

Arash Pashrashid

26 March 2023



Meltdown and Spectre: ‘worst ever’ CPU bugs

- **Always-on mitigations adds huge performance overhead**

- **Many of them are unnecessary**

- **Using side-channel attack detectors to detect malicious activities**

- Enabling appropriate mitigation only when system is at risk; and avoid unnecessary slowdowns

- We design an attack to evade Cyclone detection mechanism
- Patching their detection would cause high false positive rate

- We design an attack to evade Cyclone detection mechanism
- Patching their detection would cause high false positive rate

- We design another attack to show the vulnerability of Avenger, a mitigation based on Cyclone, even if using ideal cyclic detection

- We design an attack to evade Cyclone detection mechanism
- Patching their detection would cause high false positive rate

- We design another attack to show the vulnerability of Avenger, a mitigation based on Cyclone, even if using ideal cyclic detection

Our solution: ConstSpec

Resolving the limitations of existing detection-based mitigations by addressing potential leaks through a constant-time mitigation

Main benefits over State-of-the-art

- ***Robust***: Resistant against evasive attacks
- ***Fast***: mitigating before the key extraction from the attacker
- ***Efficient***: Negligible performance and efficiency overheads
- ***Accurate***: 0% false negative for known Spectre and evasive attacks; Low false positive rate for benign programs