A number of side-channel attacks on Intel and ARM processors have been released this week byPaul Kocher and collaborators. These attacks exploit processor features such as speculative execution to let un-privileged processes read kernel memory, essentially breaking the entire security model of the operating system.

https://spectreattack.com/spectre.pdf

As a proof-of-concept, JavaScript code was written that, when run in the Google Chrome browser, allows JavaScript to read private memory from the process in which it runs.

Interesting to understand how will this apply to Ethereum wallets, specically Browser-base wallets … A question is whether Metamask and Mist are vulnerable to attackers stealing private keys … Note that the poc code reads the private memory of the browser process, but from reading the rest of the paper it seems that the entire memory space is vulnerable …