'Hot pixels' attack steals data through CPU readings

May 31 2023, by Peter Grad

Credit: Pixabay/CC0 Public Domain

A team of security researchers at Georgia Tech, the University of Michigan and Ruhr University Bochum in Germany has reported a new form of side-channel attack that capitalizes on power and speed management methods used by graphics processing units and systems on a chip (SoCs).

The researchers demonstrated how they could steal personal information by targeting data released by the Dynamic Voltage and Frequency Scaling (DVFS) mechanisms found on most modern chips.

As manufacturers race to develop thinner and more energy-efficient devices, they must train their sights on constructing SoCs that balance power consumption, heat generation and processing speed.

As Georgia Tech Professor Hritvik Taneja explained in a paper published on the pre-print server *arXiv* last week, SoCs "exhibit instruction- and data-dependent behaviors as they struggle to balance the three-way tradeoff between frequency, power, and temperature."

Using Arm-based SoC units, Intel CPUs, and AMD and Nvidia GPUs, researchers were able to detect behavior patterns that emerge as processors continuously balance power demands and heat restrictions. Such patterns were revealed through data leaked by sensors embedded in the processors.

The researchers' "hot pixel" attack forces one of the variables tracked by DVFS to remain constant. By monitoring the two other variables, they were able to determine which instructions were being executed.

Arm chips used in smartphones, which contain passively-cooled processors, can leak data containing power and frequency readings, while actively-cooled processors used in desktop devices can leak data through temperature and power readings.

The researchers deployed several types of attacks, such as history sniffing and website fingerprinting operations, based on such data readings.

A hacker could sniff browsing history by detecting the different color of

a user's previously visited links. Once a sensitive site, such as a bank, is confirmed, the hacker could then deliver a link to a phony site that resembles the real site.

Researchers tested the Apple MacBook Air (M1 and M2), Google Pixel 6 Pro, OnePlus 10 Pro, Nvidia GeForce RTX 3060, AMD Radeon RX 6600 and Intel Iris Xe (i7-1280P).

All devices leaked data, with the AMD Radeon RX 6600 faring most poorly, with a 94% accuracy rate in unauthorized data extraction. The Apple devices had the best ratings with a data retrieval accuracy rate of between only 60% and 67%.

The authors recommended manufacturers enforce hardware-based thermal limitations, curb unprivileged access to sensor readings and limit thermal-controlled devices.

All affected manufacturers were notified of the vulnerabilities by the researchers. No new preventive actions have yet been announced, but proposals to restrict OS-level access to sensors measuring thermal, power and frequency levels have previously been discussed.

More information: Hritvik Taneja et al, Hot Pixels: Frequency, Power, and Temperature Attacks on GPUs and ARM SoCs, *arXiv* (2023). DOI: 10.48550/arxiv.2305.12784