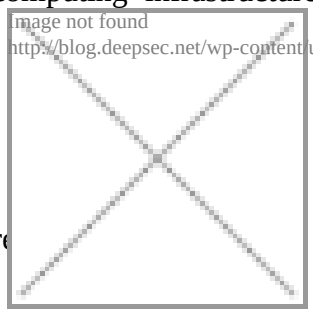
# Meltdown & Spectre – Processors are Critical Infrastructure too

Posted on **January 06,2018** by **lynx**

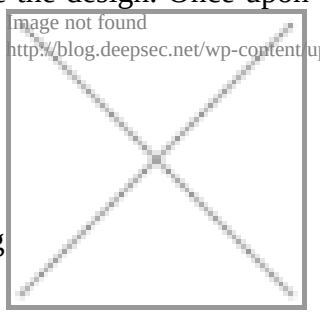
Information security researchers like to talk about and to analyse critical infrastructure. The power grid belongs to this kind of infrastructure, so does the Internet (or networks in general). Basically everything we use has components. Software developers rely on libraries. Usually you don't want to solve a problem multiple times. Computer systems are built with many components. Even a System on a Chip (SoC) has components, albeit smaller and close to each other. 2018 begins with critical bugs in critical infrastructure of processors. Meltdown and Spectre haunt the majority of our computing infrastructure, be it the Cloud, local systems, servers, telephones, laptops, tablets, and many mor




Information security relies on the weakest link. Once your core components have flaws, then the whole platform may be in jeopardy. In 2017 malicious hypervisors in terms of bugs/backdoors in the Intel® Management Engine (for example, AMD™ has a similar technology) came to light. Coreboot is one way to replace the attack surface of your BIOS/UEFI firmware. These approaches can't do much once the processor is affected.

Hindsight doesn't help, but bugs in the processor core or its microcode have been happened before. There is the famous FDIV bug, F00F, and other CPU bugs have been around for decades. The reason is sometimes the security-performance trade-off, it may be due to an architectural design error, or just simple oversight. Debugging is hard, hence hardware. If you are lucky, you run a platform that is not vulnerable. The Raspberry Pi ARM core is not affected by Meltdown or Spectre. So if you run on Raspberrys, then you are fine. Building a cloud platform is tricky (we tried to install OpenStack on a number of Raspberry Pis, it almost worked, but 1 GB memory is barely enough for the controller node).

We haven't even mentioned embedded devices and the notorious Internet of Things (IoT). The history of bugs is huge. Back in 2014 there was an article on how hard/impossible it is to fix this ecosystem. The recent DeepSec conference featured a talk about the Mirai botnet and possible successors. There is not much you can do about it unless you can change the design. Once upon a time there were approaches to have reduced instruction sets on processors. Inspecting




all the feature sets of modern CPUs looks like a higher level language. Of course we want our code to run as fast as possible. Who wants to wait? However there are designs that take security into account, and when it comes to critical infrastructure we will have the patience. Otherwise we will have to say goodbye to the idea of a secure platform.

Let's see how many bugs in hardware 2018 brings. If you find some, please let us know and submit a presentation. Submissions for trainings are welcome as well. The Call for Papers for DeepSec 2018 and DeepINTEL 2018 open soon.

Posted in:Discussion,High Entropy | Tagged:Cloud,Hardware,Infrastructure | With 0 comments