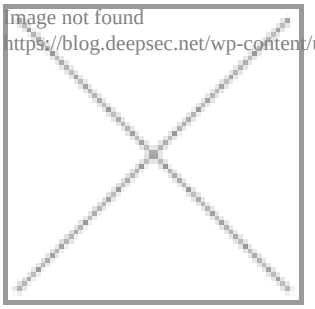
Manufacturers integrate Blockchain into Processors to counter Spectre and Meltdown

Posted on **April 01,2018** by **lynx**

The Spectre and Meltdown security vulnerabilities gathered a lot of attention in January. Processor manufacturers have rushed to fix the design of the chips and to patch products already in production. The vulnerabilities show that secure design is critical to our modern infrastructure. Computing has become ubiquitous, so has networking. The current fixes change 

microcode on the chips. Altering the flow of assembler instructions is bound to have a detrimental impact on performance. There is not much you can do about this - but there is hope. Future generations of processors will have a defence against unknown security vulnerabilities – the blockchain!

The past decade in information security has taught us that a pro-active holistic approach to IT defence is not enough. To counter unknown threats you have to go below 0(day). The blockchain offers a perfect solution to the problem of weaknesses at the processor level. The key is consensus. Since all modern processors have multiple cores, the components act as peers that don't trust each other. Instructions are regarded as transactions. Every core verifies every transaction by its own ledger containing a history of known good instructions. The consensus protocol between all cores guarantees that instructions are verified and can be trusted. Storage for the ledger is provided by the firmware, ensuring that the ledger cannot leave the system. Hidden storage without a published documentation has been an important key ingredient for secure systems for many decades. It adds another protective layer. Storage can be extended by Cloud services (with military-grade encryption) in case the systems runs longer or is subject to high processor load. You cannot work without being connected to the Internet anyway. Thus any performance impact can be regarded as negligible.

The first blockchain-based processors are expected for November 2018. Since you will have to use the new chipsets as well, the manufacturers have conveniently changed the socket again (one socket specification per manufacturer, so multiply your choices by the number of competitors).

If you have read this far, then you should already have some doubts on „modern technology“. The big problem with 1 April and satire in general is that reality has caught up. Given the density of buzzwords and hypes in information technology, it's next to impossible to separate the hard facts from the (marketing) agenda. Information security is no exception. Most events centre around products. They create needs you do not have, and they provide solutions to problems that aren't yours. Taking a step back and re-evaluating your current and future situation is the key. We have seen a lot of technological cul-de-sac designs when it comes to information security. We still pursue quite some questionable approaches to solving problems we do not have. Blockchain speaks for itself once you analyse what it is about. Your information security defence strategy should not get distracted by fashion trends.

DeepSec and DeepINTEL were created to help you seeing through all the distractions you are exposed to throughout the year. Let's keep in touch.

Posted in:Discussion,High Entropy | Tagged:Hardware,Mindset,Observation | With 0 comments