ROOTS: Out-Of-Order Execution As A Cross-VM Side Channel And Other Applications – Sophia d'Antoine

Posted on **November 15,2017** by **sanna**

Given the rise in popularity of cloud computing and platform-as-a-service, vulnerabilities, inherent to systems which share hardware resources, will become increasingly attractive targets to malicious software authors. In this talk, Sophia will introduce a novel side channel across virtual machines through the detection of out-of-order execution. She and her colleagues created a simple duplex channel as well as a broadcast channel. She'll discuss possible adversaries for this channel and proposes further work to make this channel more secure, efficient and applicable in realistic scenarios. In addition, she considers seven possible malicious applications of this channel: theft of encryption keys, program identification, environmental keying, malicious triggers, denial of service attacks, determining VM co-location, malicious data injection, and side channels.

We asked Sophia a few questions about her talk.
Please tell us the top 5 facts about your talk.

- We introduce a novel side channel across the Pipeline using Out-of-Order execution to alter and leak co-located process state.
- We abstract out hardware side channels and apply a model to all shared hardware elements both in virtualized environments (the cloud) and on a standard computer.
- This talk also explains some fundamental dynamic resource allocations used in the cloud that cause resource contentions.
- From here, we theorize that optimizations are the root cause of many side channels both in the hardware and software layers.
- We discuse several new optimizations in the x86 and ARMv8-A spec which could possibly lead to useful side channels.

How did you come up with it? Was there something like an initial spark that set your mind on creating this talk?

Messing around with threads in university, I started to see a recordable pattern of erroneous results depending on other applications running in the background. Digging deeper into it I started learning about Out-of-Order execution, how by using it I could force a thread to receive incorrect results and how to deterministically leak system information.

Why do you think this is an important topic?

- Shared resources in untrusted environments are becoming increasingly common. This leads to virtual allocations of physical resources and dynamic changes to resource distribution. These dynamic changes are the result of one process and may affect another process outside of its security boundary.
- New hardware optimizations are also being introduced.

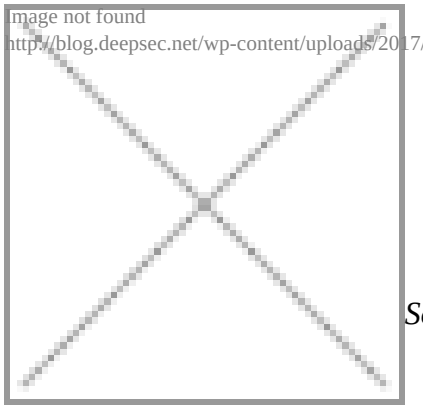
Is there something you want everybody to know - some good advice for our readers maybe?

Nope!

A prediction for the future - what do you think will be the next innovations or future downfalls when it comes to your field of expertise / the topic of your talk in particular?

In the future we'll see more hardware solutions to software side channels. Case in point, recently ARM released extensions to the architecture for the purpose of mitigating cryptographic side channels in the multiply function. It is called Data Independent Timing and forces the upper bound execution time for all instructions (example: multiplications) when a specific flag is set. This means that 1x1 will take the same time as 2546483x245303. I think we will see more solutions like this to other security problems - not just side channels.

The implementation of these solutions may not be perfect however, and either may not completely solve the problem or introduce new vulnerabilities. For instance, this ARM constant time instruction flag does not enforce constant time loads and stores, depending on the memory being accessed. This could possibly be abused to bypass the solution.



Sophia d’Antoine is a senior security researcher at Trail of Bits in NYC and a graduate of Rensselaer Polytechnic Institute. She is a regular speaker at security conferences around the world, including RECon, HITB, and CanSecWest. Her present work includes techniques for automated software exploitation and software obfuscation using program analysis. She spends too much time playing CTF and going to noise concerts.

Posted in:Conference,Security | Tagged:Cross-VM Side Channel,Malicious Applications,Out-of-Order Execution,ROOTs,Talk | With 0 comments