1400 - Breaking the x86 Instruction Set

Friday at 14:00 in Track 3

45 minutes | Demo, Tool

Christopher Domas*Security Researcher, Battelle Memorial Institute*

A processor is not a trusted black box for running code; on the contrary, modern x86 chips are packed full of secret instructions and hardware bugs. In this talk, we'll demonstrate how page fault analysis and some creative processor fuzzing can be used to exhaustively search the x86 instruction set and uncover the secrets buried in your chipset. We'll disclose new x86 hardware glitches, previously unknown machine instructions, ubiquitous software bugs, and flaws in enterprise hypervisors. Best of all, we'll release our sandsifter toolset, so that you can audit - and break - your own processor.

Christopher Domas

Christopher Domas is a cyber security researcher and embedded systems engineer, currently investigating low level processor exploitation. He is best known for releasing impractical solutions to non-existent problems, including the world's first single instruction C compiler (M/o/Vfuscator), toolchains for generating images in program control flow graphs (REpsych), and Turing-machines in the vi text editor. His more relevant work includes the binary visualization tool ..cantor.dust.. and the memory sinkhole x86 privilege escalation exploit.

@xoreaxeaxeax

#defcon25/by_track/track3/friday #defcon25/By_Day/_Friday