Project:Rosenbrdige – ‘Hardware Backdoors in x86 CPUs’

Originalartikel

Backup

<html> In this 50-minute presentation (video below) from black hat USA 2018, Christopher Domas discusses hardware backdoors in “some” x86 processors 😮 with special attention given to VIA C3 CPUs. Thankfully he’s open-sourced all his research, including his presentation slides, white paper discussing the topic, and crucially a GitHub repo of the tools used to test his theories. From the white paper, <blockquote> Abstract—As the complexity of x86 processors grows unbounded, the realities of the hidden and unexpected behaviors of these chips become apparent. While micro-architectural vulnerabilities such as speculative execution side channels are unsettling, more powerful, unknown capabilities remain buried deeper still. Here, we finally demonstrate what everyone has long feared but never proven: there are hardware backdoors in some x86 processors, and they’re buried deeper than we ever imagined possible. </blockquote>   Watch: <iframe width=„500“ height=„281“ src=„https://www.youtube.com/embed/_eSAF_qT_FY?feature=oembed“ frameborder=„0“ allow=„autoplay; encrypted-media“ allowfullscreen=„allowfullscreen“>[embedded content]</iframe> <div class=„ctx-subscribe-container ctx-personalization-container ctx_default_placement ctx-clearfix“/> <div class=„ctx-social-container ctx_default_placement ctx-clearfix“/> <div class=„ctx-module-container ctx_default_placement ctx-clearfix“/> </html>