Title: The house is built on sand: exploiting hardware glitches and side channels in perfect software
Speaker: Herbert Bos

Abstract: For years, we have tried to address security problems by fixing software bugs and misconfigurations. For critical systems we may even choose to formally verify software to guarantee the absence of bugs. However, the question is whether getting rid of bugs in the software is sufficient. In this talk, I will discuss vulnerabilities in hardware that allow attackers to compromise systems even in the absence of software bugs. In particular, these vulnerabilities offer attackers the read and write primitives needed to leak and modify sensitive information. For the write primitive, we will look at the evolution of the Rowhammer vulnerability in DRAM chips that has matured from a mere curiosity to a serious attack vector across all sorts of systems in just a few years. For read primitives, we will discuss several advanced side channel vulnerabilities, such as found in memory deduplication and Translation Lookaside Buffers.

Bio: Herbert Bos is full professor at Vrije Universiteit Amsterdam in the Netherlands where he heads the VUSec research group. He obtained his Ph.D. from Cambridge University Computer Laboratory (UK). Coming from a systems background, he drifted into security a few years ago and never left. He is very proud of his (former) students, four of whom have won the Roger Needham Ph.D. Award for best Ph.D. thesis in systems in Europe. In addition, VUSec has won three of the four Pwnie Awards awarded to researchers in the Netherlands. He claims that his life would be happier if he found a very good systems postdoc to hire (so if this is you, do apply!).