Descoperind Vulnerabilități Hardware cu Fuzzing: Cazul Zenbleed

Fuzzingul este o tehnică de testare prin furnizarea de intrări invalide, incorecte sau aleatoare în cadrul sistemului testat, cu scopul de a identifica erori de funcționare sau vulnerabilități de securitate. Ideea principală este să se testeze cum reacționează sistemul în fața unor situații neașteptate și să se identifice modurile în care acesta poate eșua sau poate fi exploatat.

În contextul software-ului, o strategie eficientă în cadrul procesului de fuzzing implică ghidarea programelor de testare prin diverse metrici, cea mai utilizată fiind "code coverage-ul". Totuși, în domeniul hardware-ului, implementarea unei astfel de strategii este mai dificilă, deoarece nu există o metrică de "coverage" la nivel de CPU, iar identificarea erorilor sau bug-urilor generate exclusiv de instrucțiunile assembly este complexă, fără a avea la dispoziție excepții precum cele din Java sau segfaults din limbajul C.

Astfel, cercetatorul Tavis Ormandy și echipa sa au explorat o nouă abordare, utilizând performance counters de la nivelul procesorului pentru a detecta schimbări drastice și neobișnuite în comportamentul sistemului, indicând posibile probleme sau vulnerabilități. De asemenea, au considerat ca evenimente semnificative identificarea diferențelor între variantele de cod serializate și versiunile lor paralelizate.

Prin aceste tehnici Tavis a descoperit vulnerabilitatea pe care a denumit-o Zenbleed. Zenbleed abuzează de execuția speculativă prin crearea unei ramuri speculative care induce procesorul să execute instrucțiuni care accesează memoria kernelului. Chiar dacă instrucțiunile speculative sunt ulterior anulate, accesul la memoria kernelului are loc totuși, permițând atacatorului să citească date sensibile.

Această abordare reprezintă o contribuție semnificativă în domeniul testării de securitate, furnizând o metodă inovatoare de detectare a problemelor și vulnerabilităților în sistemele hardware, și poate servi drept fundament pentru dezvoltarea ulterioară a unor tehnici mai precise și eficiente în acest sens.

Referințe:

1. "Zenbleed: Exploiting Data Forwarding in Intel Processors" - https://lock.cmpxchg8b.com/zenbleed.html
2. "Intel Skylake Server Performance Monitoring Events" - https://perfmon-events.intel.com/skylake_server.html
3. "Fuzzing Hardware with Performance Counters" - https://www.youtube.com/watch?v=neWc0H1k2Lc