

Kiberbiztonság - VI. szekció – Kibervédelem II.

RENDSZERMEMÓRIA ELLENI TERHELÉSES TÁMADÁS HATÉKONY DETEKTÁLÁSA

HORCSIN Bálint

Sok x86-64 utasításkészletű processzor memória elérése sérülékeny terheléses támadásokkal szemben. Jelen dolgozatomban tárgyalt módszer már korábban is ismert volt, és úgy csökkentették a processzor számítási teljesítményét, hogy több cache line-t érintő atomi utasításokat hajtottak végre egymás után, amelyekkel bus lock-okat váltottak ki, amely drasztikusan csökkentette a processzor számítási teljesítményét. Ez a támadás olyan esetben is sikeres volt, hogyha a támadó kód hardveresen gyorsított virtuális gépen futott. Egyes újabb processzorokon beállítható, hogy védett legyen ilyen típusú támadás ellen. Ugyanakkor sok processzor továbbra is üzemben van, amelyek esetén nincs ismert megoldás a sérülékenységek elhárítására. Annak érdekében, hogy egy támadásra lehessen reagálni, képesnek kell lenni detektálni, amikor ezt a sérülékenységet kihasználják. Több kutatás is foglalkozott azzal, hogy miképpen detektálható egy folyamatban lévő támadás. Ezek 1-30 mp alatt adtak eredményt, amely az esetek 5-30%-ban téves volt. Korábbiaktól eltérő mérési és statisztikai módszerrel átlagosan 80 µs alatt tudtam elvetni a támadás tényét, ha nem volt támadás alatt a számítógép; és átlagosan 1-3 ms alatt tudtam érzékelni egy aktív támadást, lényegében hiba nélkül. A támadás detektálásában elért új eredmények demonstrálása céljából rejtett kommunikációs csatornát alakítottam ki két virtuális gép között, amelyen 832 bit/mp sebességgel voltam képes adatot továbbítani.

Kulcsszavak:

processzor, virtualizáció, rejtett kommunikáció, memória

Cybersecurity - session VI. – Cyber defence II.

EFFICIENTLY DETECTING DENIAL OF SERVICE ATTACKS AGAINST SYSTEM MEMORY

Bálint HORCSIN

Many x86-64 processors are susceptible to denial-of-service attacks due to the way they access system memory. The method discussed in this paper was already known, which executes unaligned atomic instructions on the processor. These instructions trigger bus locks, and they drastically degrade the compute performance of the given processor. The attack is also successful when it is performed on a virtual machine thanks to hardware-accelerated virtualization. Some newer processors can be set to be resilient against this kind of denial-of-service attack. But many processors that are still in operation cannot be protected against such attacks using any known methods. In these cases, the only way of mitigating this threat is by detecting an ongoing attack and react accordingly.

Multiple papers were published on how an ongoing attack can be detected. These solutions have typically been able to detect such an attack in 1-30 seconds with an error rate of 5-30%. By using other measurement and statistical methods, I was able to reject that the computer was being attacked in 80 μ s on average, and I was able to detect an ongoing attack in 1-3 ms with almost perfect accuracy. To demonstrate my results in attack detection, I established a covert communication channel between two virtual machines with a data rate of 832 bits/sec.

Keywords:

processor, virtualization, memory, covert communication, bus lock