

Virtualizáció, mint energia hatékony informatikai eszköz

Önálló laboratórium feladat összefoglalója (II. félév)

Laposa László (EJWQMM)

Konzulens: Pásztor Péter László

**BME Méréstechnika és Információs Rendszerek Tanszék
Informatikai infrastruktúra tervezése szakirány, 2007/2008. II. félév**

Második féléves önálló laboratóriumi feladatom kezdeteként megpróbáltam utánajárni, hogy milyen lehetőséget rejt magába a technológia, mik azok az előnyök és lehetőségek, amelyeket az informatika számos területén haszonnal lehet kamatoztatni és mik azok a nehézségek, buktatók és esetleges biztonsági kockázatok, amelyekre érdemes nagy figyelmet fordítani. Így jutottam el első lépésként a TCG (Trusted Computing Group) kezdeményezés ma elérhető, eszközeihez. Mivel a fő kutatási irányom a virtualizáció és előző félévben főleg a processzor által hardveresen támogatott virtualizációval foglalkoztam, ezért most is az egyes architektúrák által nyújtott szolgáltatásokra koncentráltam, mit például az AMD K8 /10 generációjú CPU-iban implementált SKINIT utasítás és az a köré csoportosuló egyéb utasítások, amely feladata egy megbízható számítási környezet kialakítása. Mindehhez különböző működési rendszabályokat alkalmazva és kiaknázva a biztonsági szoftverlenyomatokban rejtőző módosítás jelző lehetőségeket. Szintén a biztonság témakörébe tartozik a mind Intel, mind AMD processzorokba implementált utasítás végrehajtást gátló indikátor bit, amelynek feladata, hogy az irányítás egy olyan utasítássorozatra kerüljön át, amelyet a DMA biztonsági gyengeségeit kihasználva írtak a memóriába, tulajdonképpen a bit nem tesz mást, mint azt jelzi, hogy mely memóriatartomány hajtható végre az adott környezetben és mely nem.

Ezt követően a virtualizáció teljesítménymérésének egy lehetséges megoldását próbáltam tanulmányozni, illetve alkalmazni. A hardveresen támogatott virtualizációt jól jellemzik az olyan periodikusan végrehajtható utasítások, mint a VMEntry-VMExit, mivel ezek az események jelentős környezetváltásokkal járnak és sok száz vagy több ezer órajel ciklusig tartanak, ezért kellőképpen jellemzik a virtualizációs állomás teljesítményállapotát, ha sok van vergődik a rendszer, lassúak a virtuális gépek, ha kevés kellő számítási teljesítmény jut a virtuális gépeknek. Ezen jellemzők mérésére is megoldás nyújt a Linux operációsrendszerek alá írt perfmon monitorozó csomag, sajnos az alkalmazás telepítése egy kernel oldali illesztőt is igényel, amelyet csak az IA-64 architektúrára írt disztribúciók kernelei tartalmaznak alapértelmezetten, más esetben manuálisan kell telepíteni és konfigurálni, amely meghiúsult.

A félév nagy részét ezek után az energia hatékony informatika témakörében való kutatással, forráselemzéssel töltöttem. Megpróbáltam megvizsgálni, hogy a mai és a közelmúltban alkalmazott eszközök milyen fogyasztási paraméterekkel rendelkeznek, milyen módon menedzselhető az, így került képbe az APM és az ACPI mint a két legelterjedtebb szabvány, mivel az utóbbi a korszerűbb és időt állóbb megoldás ezért ezt tanulmányoztam tüzetesebben. A forrástanulmányozásból arra a megállapításra jutottam, hogy mindezen technikák, megoldások csak az otthoni, illetve kisvállalati környezetben járnak jelentős megtakarítással, ahol nem alkalmaznak többszörös redundanciát a szolgáltatások biztosítására, nagyvállalati környezetben ez a nyereség elenyésző a terheletlen rendszer alapfogyasztásához képest. Ebben az esetben csak az egyes szerverek leállítása jár energiatakarékossgal. Ahhoz hogy a szolgáltatás fenntartása mellett ezt megtehessek virtualizált rendszert kell alkalmazni energiamentes funkciókkal. Erre a VMWare ESX Server termékcsaládjában találtam megoldást az DPM modul formájában.