

Horcsin Bálint
Informatikai Kar**Virtualizáció biztonsága**

Kutatásom során futó virtuális gépek hatékony klónozásának módjával, felhasználási területeivel és azok esetleges veszélyeivel foglalkoztam. Korábbi kutatásom során hiányoltam olyan megoldást, amely segítségével lehetőség lenne klónozott virtuális gépekkel gyorsan kommunikációs csatornát kialakítani. Erre bemutattam egy elméleti lehetőséget. Virtuális gépek hatékony klónozását fel lehet például használni olyan esetekben, hogyha egy felhőben működő fejlesztői környezetet szeretnének kialakítani, ugyanakkor ennek a megoldásnak mindössze annyi az előnye a korábbi megoldásokhoz képest (pl. FireCracker), hogy nem kell megvárni, míg az operációs rendszer beindul, ami csak akkor releváns, hogyha a virtuális gép rövid ideig létezik. Így például olyan esetekre is lehet használni, hogyha egy elavult, elsősorban kliensoldali alkalmazást szeretnének futtatni szerveroldalon.

Ugyanakkor ebben a felhasználási esetben különös problémát okoz, hogy mivel a magas hardverenkénti költség miatt a szerverszolgáltatók kevés fizikai gépet használnának, így egy támadó könnyen kerülhetne ugyanazon hardverre, mint a célpontja. Ha ugyanazon hardverre tud kerülni, akkor sok x86_64 utasításkészletű processzoron lehetősége van arra a támadónak, hogy a számítógép memóriája ellen terheléses támadást hajtson végre, és ezzel drasztikusan lecsökkentse az áldozat számára elérhető számítási teljesítményt. Az ilyen jellegű támadás detektálásáról már több különböző kutatás is készült. Ezeknek 1 másodperc is kellett a támadás detektálásához, valamint az eredmények 10%-a fals pozitív volt. Én a korábbiaktól eltérő mérési és adatfeldolgozási módokat vizsgáltam, és javasolt módszeremmel kb. 80 µs alatt el tudtam vetni a támadás tényét, illetve kb. 1 ms alatt meg tudtam állapítani, hogy az érintett hardver támadás alatt volt. Mivel a támadás detektálható volt mind a gazdagépen, mind a többi hardveren futó virtuális gépen, így megállapítottam, hogy a két virtuális gép között lehetőség van rejtett kommunikációra is. Ezzel mintegy 832 bit/s adatátviteli sebességet értem el virtuális gépek között, így ez egy hatékony rejtett kommunikációs csatorna. Az elért eredményeimet a 2023-2024-es tanév tavaszi félévében az ELTE IK Informatikatudományi TDK-konferenciáján bemutattam, amellyel első helyezést értem el, és nomináltak az OTDK-ra.

A kutatásom kiindulásaként egy olyan felhasználási területet jelöltem ki, amelyben a virtuális gépeken belül adatbáziskezelés-feladatok automatikus értékelését végeztem. Korábbi ÚNKP kutatásomban bemutattam erre egy stratégiát. Ezt adaptáltam az ELTE IK Adatbázisok I gyakorlatának oktatására. Ezt követően nem volt szükség teljes virtuális gépeket létrehozni, hanem elegendő volt konténerizációt alkalmazni. A módszer alkalmazhatóságát pilot program keretében vizsgáltuk. Itt vizsgáltuk, hogy a módszer mennyire adott pontos eredményt az értékelésre, miképpen módosította az oktatói munkát, valamint azt is, hogy mi volt a hallgatók véleménye. Az értékelés pontossága 98% fölötti volt, az oktatói munkát hatékonyabbá tette, a hallgatók pedig pozitívan értékelték a rendszert. Így javaslatot tettem a rendszer bevezetésére. Az elért eredményeimet a 2023-2024-es tanév tavaszi félévében az ELTE IK Szakmódszertani TDK-konferenciáján bemutattam, amellyel első helyezést értem el, és nomináltak az OTDK-ra.