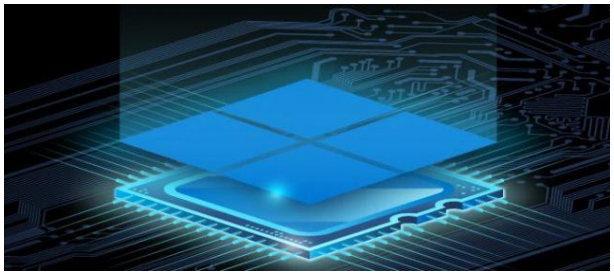
Új biztonsági funkciók kerülnek a windowsos PC-kbe



Egy új különleges processzor megalkotásában számos chipgyártó vett részt.

A Microsoft, az AMD, az Intel és a Qualcomm közösen fejlesztették ki a Pluton nevű biztonsági chipet a windowsos számítógépekhez. Az eszköz azon a chip-felhő biztonsági technikán alapul, amelyet a redmondi óriáscég már alkalmaz az Azure Sphere rendszerében és az Xbox konzolban. A Pluton új biztonsági funkciók integrálását teszi lehetővé a windowsos PC-kbe.

A tervek alapján a Pluton a jövőben része lesz az AMD, az Intel és a Qualcomm processzorainak, s az integráció a Trusted Platform Module (TPM) biztonsági hiányosságait küszöbölheti majd ki. Az új termék eleinte egy TPM-et fog emulálni és támogatni fogja a meglévő alkalmazásprogramozási interfészeket.

A Microsoft kiemelte, hogy az általa megálmodott jövőképben a biztonság részét képezi a processzornak, s a hardver és a szoftver szorosan kapcsolódik egymáshoz. A biztonsági processzorok ilyen szinten forradalmi dizájnja jelentősen nehezebbé teszi majd a támadók számára az operációs rendszer feltörését és az abban való elrejtőzést. A napjainkban használt TPM-et a Windows operációs rendszerek több mint tíz éve támogatják és olyan funkciókat tesz lehetővé, mint a Windows Hello és a BitLocker. A bűnözők azonban új módszereket fejlesztettek ki a processzor és a TPM közötti kommunikációs csatorna megtámadására, az utóbbi viszont a Pluton megakadályozza.

Az architektúrát használó windowsos PC-k esetében a felhasználók azonnal profitálhatnak majd az új funkciókból és alkalmazhatják a bejelentkezési információk, a személyazonosságok, a titkosítási kulcsok és a személyes adatok védelmére. Ezen információk egyike sem távolítható el, még akkor sem, ha egy támadó kártevőt telepít fel az adott számítógépre vagy fizikailag teljes mértékben átveszi az ellenőrzést a PC felett.

A chip a bizalmas adatokat külön fogja tárolni a rendszer többi részétől. A Secure Hardware Cryptography Key biztosítja majd, hogy a használt kulcsok a védett hardveren kívül soha ne legyenek láthatók, sőt, még a Pluton firmware-jétől is izolálva lesznek. A Pluton a firmware-frissítéstől kezdve a teljes PC-ökorendszer frissítésén át számos folyamatot egyszerűsíthet. Rugalmas és aktualizálható platform lesz, s integrálni fogják a Windows frissítési folyamatába.

Forrás: https://sg.hu/cikkek/it-tech/143397/uj-biztonsagi-funkciok-kerulnek-a-windowsos-pc-kbe

Válogatta: Berke Barnabásné