INFORMATIKA A VERSENYKÉPESSÉGÉRT • ALAPÍTVA 1969

A KÉTHETI SZAKLAP

# COMPUTERWORLD

2023. március 22. • LIV. évfolyam 6. szám

www.computerworld.hu

MALLÁSZ
JUDIT

TECHNOLÓGIA

# Újszerű védelem kicsiknek is

Ha egy okosotthont meghekkelnek, és éjszaka dübörgő zenére ébrednek a lakók, az roppant bosszantó. Az IoT rendszerek feltörése és megtámadása azonban ennél sokkal nagyobb károkat is okozhat. Érdemes elgondolkozni azon, hova vezethet például az, ha az önvezető autók vezérléséhez férnek hozzá illetéktelenek, vagy a háztartási erőművek hálózatát éri támadás.

Vajon mennyire biztonságosak azok a rendszerek, amelyekben nagyszámú egyszerű eszköz, például szenzor működik hálózatba kapcsolva? Vannak olyan IoT rendszerek, ahol elegendő az alapszintű, például felhasználónév/jelszó védelem, de vannak olyanok is, ahol a személyes és egyéb érzékeny adatokat a legmagasabb szinten kell védeni. Egy magyar vezetésű nemzetközi konzorcium ez utóbbira kíván létrehozni olyan IoT architektúrát, amely rugalmas és ellenálló IoT szolgáltatási környezetek fejlesztését és működtetését teszi lehetővé. Az Európai Unió által finanszírozott IOTAC projektben hét európai ország 13 ipari szereplője, kutatási központja és egyeteme dolgozik együtt. A konzorcium hazai résztvevői az Atos Magyarország Kft. (koordinátor), a Budapesti Műszaki és Gazdaságtudományi Egyetem (BME) és a SafePay Systems Kft. A projekt futamideje 36 hónap, befejezése 2023 augusztusában várható. Nulláról indult a fejlesztés, vagy voltak már alapmegoldások, amelyekre építeni lehet? – tettük fel a kérdést *Vilmos András* projektvezetőnek és *Vajta Lászlónak*, a BME c. egyetemi tanárának.

Vilmos András: Mielőtt a pályázatot benyújtottuk, döntően koncepcióink, és alapmegoldásaink voltak. Arra vállalkoztunk, hogy a projekt során kifejlesztjük az elképzeléseinket megvalósító modulokat.

Vajta László: Egyértelmű tendencia, hogy az IoT rendszerekben drasztikusan megnő a védendő, adott esetben nagyon egyszerű elemek száma, amelyek kapacitásukban nem alkalmasak rá, hogy drága, szofisztikált védelmet kapjanak. Ilyen körülmények között szükségessé vált, hogy újszerűen közelítsük meg a nagy végpontszámú IoT rendszerek védelmét.

**Computerworld: Mennyiben új a megközelítés?**

VA: Rugalmas rendszerről van szó, amelyben egy központi elemként működő átjáróhoz csatlakoznak a védelmi modulok, nevezetesen a front-end jogosítás-ellenőrzés, valamint többfajta runtime biztonsági funkció: mesterséges intelligencia-alapú észlelési modellek, mézesbödönök (honeypotok), visszalépési pontok, továbbá a valós idejű felügyeleti rendszer. Ezek a technológiák hardver- és szoftverszinten is megfelelő védelmet nyújtanak. Mivel a rendszer rugalmasan konfigurálható, nem feltétlenül csak nagy ipari környezetekben alkalmazható, hanem olyan kis- és középvállalati vagy akár háztartási környezetben is, ahol hiányzik a megfelelő szakértelem, illetve biztonsági támogatás a védelem kialakításához. A rendszer alapja a tervezett biztonság paradigmája. Az ajánlott irányelvek és eljárások a biztonságos szoftverfejlesztés teljes életciklusát lefedik a tervezéstől a fejlesztésen és a tesztelésen át, az értékelésig és a tanúsításig. Nagyon fontos, hogy a projekt során nemcsak egyes technológiai elemek fejlesztése történik, hanem azok gyakorlatorientált, életszagú pilotprojekteken keresztül meg is valósulnak.

**Vilmos András**

**CW: Milyen IoT szolgáltatási környezetben próbálják ki a fejlesztések eredményeit?**

VL: A konzorciumi tagok együttműködésével vannak pilotprojektjeink ipari (prosumer rendszer), lakossági (intelligens otthon), autóipari (autonóm jármű) és légi (drónüzemeltetés) IoT szolgáltatási környezetben. A BME részvételével a megújuló energiák, energiatárolók együtteséből kialakítunk egy háztartási méretű, önálló energiagazdálkodó egységet, amely termel és fogyaszt is energiát. Ezen az úgynevezett prosumer egységen teszteljük a technológiák alkalmazhatóságát, valamint vizsgáljuk a biztonságtechnikai kérdéseket. Figyelemre méltó, hogy a háztartási erőművek szaporodása komoly biztonsági veszélyeket rejt magában. Ha például sok háztartási erőművet ér egyidejű támadás, akár nagyobb területek energiaellátása is súlyos veszélybe kerülhet. Az IOTAC projektnek tehát egyfajta missziója is van: felhívni a figyelmet az IoT rendszerek speciális kihívásaira, feltárni a potenciális veszélyeket, illetve felhívni a figyelmet a veszélyeztetettségek csökkentésének lehetőségeire. Szerencsére egyre több döntéshozó is felismeri a problémát, és keresi a megoldást.

VA: A BME más pilotprojektekben is részt vesz: a drónüzemeltetésben francia, az autonóm járműveknél spanyol, az okosotthonoknál görög cég a partnerünk. Érdekes, mindenki számára a legmagasabb szintű védelmet nyújtó, vadonatúj megoldást készít a chipkártyás beléptető rendszerre az Atos. Lényege, hogy a fizikai chipkártyákat a felhőben tárolják, így azokhoz minden kártyatulajdonos bárhol és bármikor, külön eszköz nélkül hozzáférhet.

**Vajta László**

**CW: Valós vagy szimulált környezetben folynak a tesztek?**

VA: Vannak valós, szimulált és vegyes pilotok. A prosumer és az okosotthon tesztek például valós környezetben zajlanak, Athénban. Az önvezető autók számára félig valós, félig emulált környezetet alakítottunk ki. Ez azt jelenti, hogy a részben valódi, részben számítógéppel szimulált autók valódi, zárt tesztpályán haladnak. A drónpilot teljes mértékben szimuláció.

**CW: Durván fél év van még hátra a projektből. Hol tartanak a munkában?**

VA: A fejlesztések többé-kevésbé befejeződtek. Jelenleg a pilotokat telepítjük és teszteljük. A tesztek eredményeit visszacsatoljuk a fejlesztőkhöz, akik a jelzések alapján finomhangolják a rendszereket, kielégítik az esetleg menet közben felmerült új igényeket. Teljes mértékben a terveknek, az ütemezésnek megfelelően haladunk.

**CW: A BME részéről bevonnak hallgatókat a kutatás-fejlesztési munkába?**

VL: Igen, mesterhallgatókat és doktoranduszokat. Tevékenységüket minden esetben tutorok irányítják. Jellemzően kisebb részfeladatokat bízunk rájuk. Mivel a feladatok meglehetősen magas szintűek és bonyolultak, viszonylag kevés hallgatót tudtunk bekapcsolni a munkába.

**CW: Az IOTAC konzorcium nemrégiben kiállítóként vett részt a barcelonai Kiberbiztonsági Kongresszuson, amit az IoT Megoldások Világkongresszusával (IOTSWC) együtt rendeztek. Mik voltak a tapasztalataik?**

VA: Egyre többekben tudatosul, hogy valamit tenni kell, mivel rohamosan nő a hálózatba kapcsolt eszközök száma, következésképpen fokozódik a veszély. Az IoT biztonság a fókuszban van, egyre nagyobb az igény a védelmi megoldásokra. Az IOTWSC-n egyébként nemcsak az IOTAC projekttel vettünk részt, hanem más, az IoT technológiákhoz szorosan vagy érintőlegesen kapcsolódó EU-s projekteket is bemutattak partnereink.

**CW: Más fórumokon is népszerűsítik az IoT rendszerek védelmének fontosságát?**

VA: Harmadik éve szervezzük az IoT Day Roundtable-t, ahol minden alkalommal egy speciális témát választunk. Tavaly általában a szabványosításról volt szó, idén egy új európai uniós törvény, az EU Cyber Resilience Act lesz a fő téma. Lényege, hogy miként kell a különböző fogyasztási IoT eszközöket úgy elkészíteni, hogy azokban a biztonság alapértelmezetten szerepeljen. Az idei rendezvényen természetesen az IOTAC projektet is bemutatjuk. Az IoT Day Roundtable-re (április 17.) meghívjuk az Európai Bizottság, az ENISA (European Union Agency for Cybersecurity) és különböző iparági szakai szervezetek képviselőit is. A hazai szereplőkön kívül Európa több országából lesznek előadók, sőt az Egyesült Államokból is előad a NIST *(National Institute of Standards and Technology)* egyik szakértője. A virtuális eseményt bárhol a világon online lehet majd követni.

**CW: Az IOTAC projekt befejezését követően mi lesz a fejlesztések eredményeinek a sorsa?**

VA: A projekt során létrehoztuk az IOTAC Egyesületet, aminek az a feladata, hogy koordinálja az eredmények hasznosítását. Az egyesület üzleti tevékenységet nem végez, de támogatja az iparági szervezetekben való megjelenést, a partnerekkel való kommunikációt, a projekttagok kereskedelmi tevékenységét. Egyértelmű cél tehát, hogy a projekt eredményeiből a résztvevők üzletet csináljanak. Az üzleti modellt úgy dolgoztuk ki, és az IOTAC keretrendszer úgy épül fel, hogy egységesen, egy rendszerként legyen értékesíthető. Flexibilitásra törekedtünk, azaz az egyes modulokat külön-külön is lehet aktiválni, de többségük önállóan is alkalmazható. Az IOTAC Egyesületnek a szabványosítás területén is vannak feladatai. Az ETSI-vel karöltve olyan szabványok megalkotásán fáradozunk, amelyek leírják, hogy miként kell védeni az IoT környezeteket, milyen feltételeknek kell megfelelni, és az ehhez szolgáló eszközöket hogyan kell elkészíteni. Feladataink közé tartozik ezen ismeretek és elvárások terjesztése.

**CW: Várhatóan kik, milyen szervezetek lesznek majd a vevők, a fő felhasználók?**

VL: Vegyünk egy példát! Manapság minden háztartási vagy kiserőmű a működése során keletkező adatokat – részben biztonsági megfontolásokból – elküldi az inverter gyártójának a felhőjébe. Ezután minden adathozzáférés (amit mi a saját erőművünkkel való kommunikációként érzékelünk) a külföldi gyártó tudtával, illetve engedélyével történik. Az IOTAC projekt egyik eredménye, hogy lehetővé teszi a kiserőművek leválását a gyártói felhőről a szükséges adatvédelem és adathozzáférés biztosítása mellett. Jó példa ez arra, hogy miként hozhat egy kutatás-fejlesztési projekt hasznosítható, kézzelfogható eredményt.

VA: Nagy potenciált látunk az okosotthonokban. Azokkal a gyártókkal, szolgáltatókkal, integrátorokkal kell majd felvennünk a kapcsolatot, amelyek okosotthonokat telepítenek. Azt kell elérnünk, hogy megoldásunkat opcióként vagy alapértelmezett lehetőségként kezeljék. Általánosságban nem a végelhasználók a mi közvetlen partnereink, hanem azok a rendszerintegrátorok, amelyek adott esetben az IoT rendszert telepítik. Az IOTAC projektben létrehozott eredmény tehát nem közvetlenül egy B2C, hanem inkább egy B2B2C megoldás. CW