SAJTÓKÖZLEMÉNY

IoT eszközök informatikai biztonságát növelő kutatások

Az intelligens beágyazott eszközökkel kibővült Internet, azaz az Internet of Things (dolgok Internete, IoT) rendszerek biztonságát növelő technológiák fejlesztését kezdték meg a Budapesti Műszaki és Gazdaságtudományi Egyetem, a Szegedi Tudományegyetem és a Debreceni Egyetem kutatói egy közös projektben.

A kutatók arra keresik a választ, hogyan lehet megfelelő egyensúlyt kialakítani a költségek és a rendszer által nyújtott biztonság szintje között.

A 2018. október 1-én indult és 4 évig futó SETIT[1] projekt célja olyan technológiák kutatása és fejlesztése, melyek az IoT biztonsági kockázatait csökkentik, és ezzel lehetővé teszik az IoT alkalmazások szélesebb körű elterjedését.

A SETIT projekt (azonosító: 2018-1.2.1-NKP-2018-00004) a „Nemzeti Kiválósági Program: 2018-1.2.1-NKP" pályázati program keretében, a Nemzeti Kutatási és Innovációs Alapból biztosított támogatással valósul meg.

Az Internet ma már nem csak nagy teljesítményű szerverekből, személyi számítógépekből és mobil eszközökből áll, hanem számtalan intelligens beágyazott eszközt is magában foglal. Az előrejelzések szerint 2020-ra 25 milliárd ilyen eszköz lesz hálózatba kötve, és ez számos új és érdekes alkalmazás előtt nyitja meg az utat.

Az egyik ilyen alkalmazás a gyárak digitalizálása. Az ipari folyamatokat vezérlő beágyazott számítógépek, szenzorok és aktuátorok összekötése és Internetre kapcsolása lehetővé teszi a masszív adatgyűjtést, a különböző forrásból származó adatok korrelációját, és olyan adatelemzési feladatok végrehajtását, melyek segítségével jobban optimalizálhatóvá válnak a gyártási, a beszállítási, és a karbantartási folyamatok. Mindez hatással van az üzleti modellekre is, olyan változásokat előidézve, amit többen a negyedik ipari forradalomnak tartanak és ezért *Ipar 4.0*-nak neveznek.

Egy másik terület ahol a beágyazott intelligens eszközök hálózatba kötése forradalmi változást hozhat a közlekedés. A modern járművek már rendelkeznek Internet kapcsolattal, a jövő járművei pedig

[1] Security Enhancing Technologies for the Internet of Things

egymással és az útmenti intelligens infrastruktúrával is kommunikálni fognak. Ez lehetővé teszi az utak állapotával és a forgalommal kapcsolatos adatok folyamatos gyűjtését, feldolgozását és az eredmények visszacsatolását, ami a forgalom optimalizálását és a balesetek számának csökkenését eredményezi. Az önvezető (autonóm) járművek számára szintén hasznos információforrást jelenthet az Internet, valamint a közelben levő többi jármű és egyéb okos eszköz. Több gyártó központi helyen gyűjti és dolgozza fel az autonóm járműveiből származó információt, ezzel növelve az önálló vezetésért felelős gépi tanulási modellek pontosságát. Ezen modellek paramétereit aztán vissza kell juttatni a járművekbe. Mindez nem lenne lehetséges a jármű beágyazott vezérlői és a gyártó közötti hálózati kapcsolat nélkül.

Az intelligens beágyazott eszközökkel kibővült Internet, azaz az *Internet of Things* (dolgok Internete) vagy röviden IoT, azonban számos informatikai biztonsági kockázatot is magában rejt. Az IoT előre törését a beágyazott számítógépek és a vezeték nélküli kommunikáció fejlődése, illetve ezen technológiák árának folyamatos csökkenése teszi lehetővé. Az alacsony ár, a költségek minimalizálása azonban általában az informatikai biztonság hiányát eredményezi. Ugyanakkor, egyes IoT alkalmazásokban (pl. a fent említettekben) a biztonság hiánya fizikai és anyagi károkhoz vezethet, adott esetben emberéleteket követelhet. Ezekben az alkalmazásokban tehát meg kell találni a megfelelő egyensúlyt a költségek és a rendszer által nyújtott biztonság szintje között. A nagyléptékű bevezetéshez mindenképpen szükséges az IoT eszközök árának alacsony szinten tartása, ami azt jelenti, hogy ezek az eszközök erősen erőforrás-korlátozottak is egyben. Fontos kutatási kérdés, hogy hogyan lehet a lehető legnagyobb fokú biztonságot elérni az ilyen olcsó, erőforrás-korlátozott beágyazott eszközökön, illetve az ilyen eszközökből létrehozott nagyobb IoT rendszerekben.

A SETIT projekt célja ezen kérdések vizsgálata, és **olyan technológiák kutatása és fejlesztése, melyek az IoT biztonsági kockázatait csökkentik, és ezzel lehetővé teszik az IoT alkalmazások szélesebb körű elterjedését.**

A projekt koordinátora a BME, de minden résztvevő intézmény jelentős felelősséggel rendelkezik a projekthez kapcsolódó egy-egy kulcsterületen. A Szegedi Tudományegyetem az IoT rendszerekben használt beágyazott eszközök alkalmazás szintű biztonságával foglalkozó munkacsomagot vezeti. Ez a terület azért fontos, mert a IoT rendszerekben használt beágyazott eszközökön végső soron szoftver valósítja meg az alkalmazás logikáját, és ismert tény, hogy a szoftverekben található programozási hibák elsődleges kiinduló pontjai a rendszerek ellenei sikeres támadásoknak. Ezért ezen a területen a projekt szoftveres sérülékenységek detektálásával foglalkozik programanalízis módszerek alkalmazásával. Ez magában foglalja a sérülékenységek azonosítását magukban az alkalmazásokban, valamint az alkalmazások által használt, általában harmadik fél által fejlesztett programkönyvtárakban is. A hagyományos statikus és dinamikus programanalízis módszerek továbbfejlesztése mellett, az SZTE kutatói új statisztikai és gépi tanulási algoritmusokat is fejlesztenek az alkalmazások forráskódjában történő hiba-előrejelzés céljára.

A BME vezeti azt a munkacsomagot, ami az alkalmazások futtatására szolgáló beágyazott számítási platform biztonságával foglalkozik. Ez a terület azért fontos, mert a platform sikeres támadása a

beágyazott eszköz feletti teljes uralom átvételét teszi lehetővé, és ez egyben hatással van *minden* azon futó alkalmazásra is. A platform biztonságának egyik fontos eleme a biztonságos boot folyamat kialakítása, mely során az eszköz úgy tölti be és indítja el az operációs rendszert és az alkalmazásokat, hogy előtte ellenőrzi azok sértetlenségét. A biztonságos boot folyamat garantálja, hogy újraindítás után helyes állapotba kerül az eszköz, ám továbbra is fennáll annak lehetősége, hogy futási időben kompromittálódik egy platform szintű sebezhetőségnek köszönhetően. Ezért fontos további feladat az operációs rendszer megerősítése (hardening), mint preventív lépés, és a futási időben történő folyamatos integritás-ellenőrzés, mint detekciós módszer. Szükséges lehet továbbá az integritás bizonyítása egy távoli fél (pl. a rendszer üzemeltetője) számára, melyre különböző ún. távoli igazolás (remote attestation) protokollok adnak lehetőséget. Végül alapvető fontosságú a biztonságos távoli szoftverfrissítés, hiszen a felfedezett sérülékenységek javítása csak így oldható meg hatékonyan folyamatosan működő rendszerekben. A platform biztonságon túl, a BME kutatói foglalkoznak még IoT eszközök és rendszerek biztonsági tesztelési módszertanának kifejlesztésével és alkalmazásával (azaz egy speciális, IoT fókuszú, etikus hacker eszköztár kialakításával).

A projekt harmadik munkacsomagja, amit a Debreceni Egyetem vezet, IoT környezetben használható kriptográfiai algoritmusok és protokollok tervezésével és elemzésével, illetve az azokhoz szükséges algebrai kutatásokkal foglalkozik. Ez magában foglalja például az identitás-alapú kriptográfia és a bilineráris párosítások alkalmazását IoT rendszerekben, valamint az algebrai számelmélet és absztrakt algebra kriptográfiai alkalmazásainak vizsgálatát. Fontos feladat továbbá a véletlenszám generálás problémáinak vizsgálata beágyazott környezetben. Elméleti kutatásaik mellett az egészségi állapotot monitorozó IoT eszközök, például szív- és izomaktivitás, véroxigén szint, stb., kétirányú, biztonságos kommunikációját támogató tűzfal kidolgozását is tervezik.

A SETIT projekt nemzetközi szinten is elismert eredmények elérését és az eredmények rangos fórumokon történő publikációját tűzte ki célul, ezzel biztosítva, hogy a projekt mérhető hatást érjen el az IoT biztonság területén. Ezt segíti a konzorcium összetétele, az eddig is kiváló eredményeket elérő budapesti[2], szegedi[3], és debreceni[4] kutatócsoportok, valamint az NKFIA által nyújtott jelentős összegű támogatás.

A projekt címe: IoT rendszerek biztonságát növelő technológiák
A projekt azonosító száma: 2018-1.2.1-NKP-2018-00004
Kedvezményezett: Budapesti Műszaki és Gazdaságtudományi Egyetem, mint konzorcium vezető, Szegedi Tudományegyetem és Debreceni Egyetem mint konzorciumi tagok
A támogatási összeg: 299 971 567 Ft
A projekt időtartama*:* 2018.10.01. - 2022.09.30.

Információ: Dr. Buttyán Levente, BME CrySyS Lab, buttyan@crysys.hu, +36 1 463 1803

[2] www.crysys.hu
[3] www.sed.inf.u-szeged.hu
[4] inf.unideb.hu/hu/node/38