SAJTÓKÖZLEMÉNY

MŰEGYETEM 1782

Félidőnél tart a SETIT[1] projekt –
Rövid beszámoló az eddig elért eredményekről

Buttyán Levente, BME
Ferenc Rudolf és Nagy Gábor Péter, SZTE
Huszti Andrea, DE

Az Internet ma már több beágyazott eszközt köt össze, mint hagyományos PC-t és szervert. A beágyazott eszközökkel kiterjesztett Internetet nevezzük Internet-of-Things-nek, vagy röviden IoT-nek. Az IoT számos alkalmazási területen biztosíthatja az új megoldások és a dinamikus fejlődés lehetőségét. IoT technológiákat használva otthonainkat *okos otthonokká*, városainkat *okos városokká*, gyárainkat *okos gyárakká*, és közlekedési rendszereinket *intelligens közlekedési rendszerekké* alakíthatjuk. Mindez azonban alakulhat máshogyan is, ha nem gondoskodunk arról, hogy az a technológia, amire a jövőnket építjük, kellően biztonságos és megbízható legyen. „Okos" otthonaink személyes szokásaink és adataink kiszivárogtatójává, „okos" városaink és „intelligens" közlekedési rendszereink masszív megfigyelési platformmá válhatnak.

A fenti problémákat az IoT rendszerek biztonságossá tételével kerülhetjük el. Ezt a célt tűzte ki a SETIT projekt (2018-1.2.1-NKP-2018-00004), melyben a Budapesti Műszaki és Gazdaságtudományi Egyetem, a Szegedi Tudományegyetem és a Debreceni Egyetem együttműködésében olyan új biztonsági megoldások kutatása és fejlesztése folyik, melyek jelentősen csökkentik az IoT rendszerek biztonsági kockázatait. A 4 éves projekt 2018 őszén indult és a „Nemzeti Kiválósági Program: 2018-1.2.1-NKP" pályázati program keretében, a Nemzeti Kutatási és Innovációs Alapból biztosított támogatással valósul meg. Az elmúlt 2 évben számos érdekes és hasznos új eredmény született a projektben; ezekről adunk rövid tájékoztatást az alábbiakban.

IoT eszközök platform szintű biztonsága

A teljes projekt koordinálása mellett, a BME vezeti azt a munkacsomagot, ami maguknak a beágyazott IoT eszközöknek, valamint az eszközökön megvalósított program végrehajtási környezetnek a biztonságával foglalkozik. Ez alapvető fontosságú terület, mert az eszköz és a végrehajtási környezet

[1] Security Enhancing Technologies for the Internet of Things

sikeres támadása az IoT eszköz feletti teljes uralom átvételét teszi lehetővé, és ez egyben hatással van *minden* azon futó vagy azt használó alkalmazásra is.

A projektben intenzíven foglalkozunk malware detekciós módszerek és a malware mentes állapot igazolására használható protokollok fejlesztésével. Olyan új rootkit detekciós módszert javasoltunk[2], ahol a detekciót végző ellenőrző algoritmusok futtatása egy izolált, megbízható végrehajtási környezetben történik, melyben a rootkit nem tudja befolyásolni az ellenőrző algoritmusok működését. Kidolgoztuk továbbá az első, erőforrás korlátozott IoT eszközökön futó anti-vírus megoldást[3], amit SIMBIoTA-nak neveztünk el. A SIMBIoTA anti-vírus rendszer bináris hasonlóság alapján dönti el egy fájlról, hogy az vírust tartalmaz vagy nem. A módszer gyors és – méréseink alapján – 90%-nál jobb hatékonysággal felismer korábban nem látott vírusokat is. Ugyanakkor, az ehhez szükséges erőforrás felhasználás az IoT eszközön meglepően alacsony. Ezek a tulajdonságok kifejezetten alkalmassá és versenyképessé teszik a SIMBIoTA rendszert az IoT világban. Kidolgoztunk továbbá egy elemző módszert[4], a már azonosított kártékony programok analízisére, melynek segítségével automatizált módon megállapítható, hogy bizonyos rosszindulatú viselkedési minták milyen környezeti feltételek teljesülése mellett aktiválódnak a programban.

Szoftverhibák előrejelzése

Az IoT eszközök biztonságossá tételében kitüntetett szerepet tölt be a rajtuk futó szoftverek minőségének és biztonságának kérdése. A fejlesztők által akaratlanul elkövetett programozási hibák biztonsági réseket nyithatnak a szoftvert futtató IoT eszközön, melyeket rosszindulatú támadók kihasználhatnak. Az SZTE vezetésével olyan módszerek kidolgozásán fáradozunk, amelyek segíthetnek az IoT eszközökre szánt szoftverekben előforduló hibák mesterséges intelligenciával támogatott automatikus előrejelzésében azok forráskódjának analizálásával. Mivel az IoT eszközök programozása már egyáltalán nem csak a hardver közeli, alacsonyszintű programnyelvekhez kötött, ezért kutatásainkban első sorban a JavaScript programokban levő hibák előrejelzésére koncentráltunk. Annál is inkább, mert ezen technológia népszerűsége robbanásszerűen nő az olyan JavaScript futtató-környezetek megjelenésével, mint a NodeJS, vagy a kifejezetten IoT környezetre szánt JerryScript, illetve Espruino.

Kutatásunk során létrehoztuk a BugsJS JavaScript hibaadatbázist[5,6], amely kézzel validált valós JavaScript programhibákat, azokhoz tartozó unit teszteket, valamint a hibákat javító kódmódosításokat tartalmaz. Ezt az adathalmazt felhasználva gépi tanuló modellek segítségével automatikus szoftverhiba

---

[2] R. Nagy, K. Németh, D. Papp, L. Buttyán, Rootkit Detection on Embedded IoT Devices, accepted for publication in *Acta Cybernetica*, 2021.
[3] Cs. Tamás, D. Papp, L. Buttyán, SIMBIoTA: Similarity-Based Malware Detection on IoT Devices, International Conference on IoT, Big Data, and Security (IoTBDS), April 2021.
[4] D. Papp, T. Tarrach, L. Buttyán, Towards Detecting Trigger-based Behavior In Binaries: Uncovering the Correct Environment, International Conference on Software Engineering and Formal Methods (SEFM), Oslo, Norway, September 2019.
[5] P. Gyimesi et al., BugsJS: a Benchmark of JavaScript Bugs, 12th IEEE Conference on Software Testing, Validation and Verification (ICST), Xi'an, China, 2019.
[6] P. Gyimesi et al., BUGSJS: a Benchmark and Taxonomy of JavaScript Bugs, *Journal of Software: Testing, Verification and Reliability*, John Wiley & Sons, October 2020.

előrejelző módszert[7] dolgoztunk ki. Külön is foglalkoztunk a sérülékenységekkel, melyek jellegükben sokszor eltérnek a klasszikus szoftver-hibáktól. Több gépi tanuláson alapuló előrejelző modellt dolgoztunk ki, amelyeket kifejezetten a szoftverhibák ezen speciális típusára finomhangoltunk. Az előrejelzés pontosságának növelése érdekében a statikus programanalízisből származó programjellemzőket ún. folyamat metrikákkal egészítettük ki[8], melyek jelentősen megnövelték az előrejelző modellek hatékonyságát. A sérülékenység előrejelző modellek hatékonysága mellett fontos szempont volt a gépi tanuló modellek által adott előrejelzések alátámasztása megfelelő magyarázattal[9], amely alapján a fejlesztők a javasolt forráskód részeket javítani tudják.

Kriptográfiával kapcsolatos eredmények

Az IoT eszközökről származó adatok többnyire a felhőben tárolódnak vagy ott kerülnek feldolgozásra. Elengedhetetlen az IoT eszközök és a felhőszolgáltatás közötti biztonságos kommunikáció és a felhő oldali biztonságos adatkezelés. A Debreceni Egyetem Informatikai Karának kutatócsoportja az IoT eszközök kriptográfiai algoritmusaival, valamint kriptográfiai protokollok tervezésével és elemzésével foglalkozik. Egy olyan felhasználó hitelesítési protokollt[10] terveztünk, amivel a felhasználók egy token segítségével és jelszavukkal férhetnek az adataikhoz. Az általunk javasolt protokollban azonban a felhasználó hitelesítését több felhő szerver együttesen végzi el, a sikeres támadáshoz ezért több szervert kell egyszerre kompromittálni. Kidolgoztunk továbbá egy olyan hitelesítő protokollt[11], melyben a felhasználó PIN kódját vagy jelszavát bilineáris leképezés segítségével tároljuk, ami ellehetetleníti a jól ismert off-line szótár alapú támadásokat. A protokoll megvalósítását segítendő, elkészítettük a bilineáris leképezések egy platformfüggetlen implementációját[12]. Az implementáció az általunk fejlesztett CryptID programcsomag része. A programcsomag nyílt forráskódú és további, az identitás-alapú kriptográfiához szükséges primitíveket is megvalósít.

Több évtizede ismert az az elméleti eredmény, mely szerint a jelenleg használt publikus kulcsú algoritmusok feltörhetők kvantum-számítógépen futó algoritmusokkal, de magának a kvantumszámítógépnek a megalkotása sokáig technikailag nem tűnt lehetségesnek. Ezen a téren azonban az utóbbi években több jelentős áttörés is történt. Ez irányította rá a figyelmet a poszt-kvantum kriptográfiára, mely a beágyazott IoT eszközök esetében is releváns, hiszen ezek az eszközök sokszor évtizedekig működnek egy alkalmazásban, és ennyi idő alatt a kvantum veszély reálissá válhat.

---

[7] G. Antal, Z. Tóth, P. Hegedűs, R. Ferenc, Enhanced Bug Prediction in JavaScript Programs with Hybrid Call-Graph Based Invocation Metrics, *Technologies*, 9(1):3, 2021.
[8] T. Viszkok. Sérülékenység előrejelzés JavaScript programokban folyamat metrikák segítségével, Student Scientific Conference (TDK), Szeged, September 2020.
[9] B. Mosolygó, N. Vándor, G. Antal, P. Hegedűs, R. Ferenc, Towards a Prototype Based Explainable JavaScript Vulnerability Prediction Model, accepted for publication at the 1st International Conference on Code Quality (ICCQ), 2021.
[10] A. Huszti, N. Oláh, Provably Secure Scalable Distributed Authentication for Clouds. In: Krenn S., Shulman H., Vaudenay S. (eds), *Cryptology and Network Security (CANS)*, LNCS 12579, 2020.
[11] A. Huszti, Sz. Kovács, N. Oláh, Scalable, Password-based and Threshold Authentication for Smart Homes, submitted for publication
[12] Á. Vécsi, A. Bagossy, A Pethő, Cross-platform Identity-based Cryptography using WebAssembly, *Infocommunications Journal*, Vol. XI, No 4, December 2019.

Az SZTE matematikus kutatói poszt-kvantum kriptográfiai algoritmusokhoz szükséges matematikai objektumok vizsgálatával foglalkoznak.[13,14,15]

A SETIT projekt megbeszélései és rendszeres találkozói adták a motivációt arra is, hogy közös BME-SZTE csapattal elinduljunk az NSUCRYPTO'2020 nemzetközi kriptográfiai olimpián.[16] A felkészülés sikerét mutatja a professzionális kategóriában elért I. helyezésünk (Nagy Gábor Péter, Nagy V. Gábor, Győrffy Lajos), valamint a hallgató kategóriában és az egyéni fordulóban elért III. helyezéseink és dicséreteink. Jelen pillanatban is folyik a felkészülésünk NSUCRYPTO'2021 őszi versenyeire. Ugyanez a verseny motiválta egyik MSc hallgatónkat (Kiss Rebeka) két korábban kitűzött, de mindeddig megoldatlan NSUCRYPTO probléma megoldására.[17]

Projekt adatok

A projekt címe: loT 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.

[13] G. Korchmáros, G. P. Nagy, M. Timpanella, Codes and Gap Sequences of Hermitian Curves, accepted for publication in *IEEE Transactions on Information Theory* (doi:10.1109/TIT.2019.2950207)
[14] S. El Khalfaoui, G. P. Nagy, On the Dimension of the Subfield Subcodes of 1-point Hermitian Codes, accpeted for publication in *Advances in Mathematics of Communications* (doi:10.3934/amc.2020054, arxiv.org/abs/1906.10444)
[15] S. El Khalfaoui, G. P. Nagy, Estimating The Dimension Of The Subfield Subcodes of Hermitian Codes, *Acta Cybernetica* — online first paper version, 2020. (DOI: 10.14232/actacyb.285453, arXiv:2004.05896)
[16] https://nsucrypto.nsu.ru/
[17] R. Kiss, G. P. Nagy, On the Nonexistence of Certain Orthogonal Arrays of Strength Four, to appear in *Prikladnaya Diskretnaya Matematika*, 2021. (arXiv:2011.09935)