Tóth András

Az IoT-eszközök[1] védelmi célú alkalmazásának információbiztonsági kihívásai

Bevezetés

Jelen tanulmány célja átfogó képet adni az Internet of Things- (továbbiakban: IoT-) eszközök és -rendszerek védelmi célú alkalmazásának biztonsági kérdéseiről, valamint a kialakítható védelmi megoldások lehetőségeiről, az alkalmazásuk során felmerülő kihívásokról.

A mobil számítástechnika, a szociális hálózati technológiák fejlődése, valamint az internetes alkalmazások és szolgáltatások exponenciális növekedése miatt széles körben elterjedt, majd rohamosan fejlődő IoT-eszközöknek köszönhetően kiemelten fontos a védelmi szférában is komoly hangsúlyt fektetni az alkalmazott rendszerek védelmére. Ezek komoly kihívásokkal járnak az IoT-képességek és -alkalmazások egyre nagyobb térnyerésének köszönhetően. A szerző a tanulmány elkészítéséhez az elemző-értékelő módszert alkalmazta, megvizsgálta a jelenleg rendelkezésre álló releváns szakirodalmakat az IoT kialakulásának, módszereinek, képességeinek és védelmi lehetőségeinek vonatkozásában. A tudományos cikkek és művek összegyűjtéséhez a szerző a Harzing's Publish or Perish szoftvert alkalmazta, amely segítségével elsősorban a Google Scholar adatbázisában kereste a releváns irodalmakat, könyveket, amelyek más akadémiai keresőmotorokban nincsenek indexelve. Ezt követően megvizsgálta az Elsevier Scopus adatbázisát is, és a két adatbázisból kapott szakirodalmakat vetette össze. A duplikált irodalmak kiszűrését kulcsszavas szűkítéssel hajtotta végre olyan szavakkal, mint például IoT-fenyegetések, hardveres védelem, szoftveres védelem, nyílt kulcsú titkosítás, átvitelbiztonság. Ezt követően a már szűkített szakirodalmakat elemezve készítette el ezt az összefoglaló tanulmányt.

Az IoT kialakulása, képességei, kommunikációs megoldásai

Az infokommunikációs megoldások rohamos fejlődésének köszönhetően az elmúlt évtizedben egyre több olyan eszköz került mindennapi használatba a közvetlen környezetünkben, amely adatgyűjtésre, tárolásra, esetleg elemzésre alkalmas. Ezek mindegyike hálózati kapcsolódásra alkalmas, ezáltal képesek egymással kommunikálni az interneten keresztül, valamint információt megosztani a jogos és jogosulatlan felhasználókkal. Ezek

[1] Dolgok Internete: az internet napjainkban már nemcsak az emberek, hanem rengeteg hétköznapi eszköz közötti kommunikációt is biztosítja.

https://doi.org/10.36250/00973_05

az eszközök és rendszerek az IoT-technológiát alkalmazzák, és valamilyen hálózati entitást alkalmaznak a fizikai világgal történő kapcsolatok kialakításához, fenntartásához. Az IoT-technológia alapvető jellemzői:

– az IoT-összetevőket valamilyen hálózat kapcsolja össze, ami lehetővé teszi a redundáns kapcsolatok kialakítását az összetevők között;
– az egyes elemek érzékelőkkel, továbbá működtető, vezérlő elemekkel rendelkeznek, amelyek lehetővé teszik az eszközök számára, hogy megfigyeljék (adatokat gyűjtsenek), elemezzék és értékeljék a fizikai világot érintő egyes hatásokat.[2]

Az IoT-rendszerek egyes elemeit az 1. ábra szemlélteti, amelyen az egymástól elkülönült elemek csoportosítása jól látható. A bal oldalon látható elemek minden egyes szektorban alkalmazott szolgáltatásnál, a felhasználandó eszközöknél és megoldásoknál egyaránt kötelező érvényűek. A biztonság és a kapcsolat fontos az adatok begyűjtéséhez, feldolgozásához, tárolásához, valamint rendelkezésre bocsátásához. A szabványosítás biztosítja, hogy az egyes elemek közötti kommunikáció megvalósítható legyen, azok olyan technikai megoldásokat használjanak, amelyek minden felhasználó számára ugyanazokat a lehetőségeket és képességeket biztosítják. A nemzeti és nemzetközi szabványügyi szervezetek konkrét követelményrendszert fogalmaznak meg a gyártók irányába, akiknek ezekhez a szabványokhoz már a tervezés időszakától szigorúan tartaniuk kell magukat.

		Fogyasztó	Épületek	Kiskereskedelem	Szállítás	Egészségügy	Ipar
Kapcsolat, Biztonság, Szabványosítás	Alkalmazások	➢ Kontextusérzékeny információ ➢ Központosított alkalmazásirányítás ➢ Szórakozás ➢ Okoskészülékek	➢ Okoshőmérő ➢ Erőforrás-menedzsment ➢ Biztonság	➢ Ellátásilánc-menedzsment ➢ Célzott reklám ➢ Készletgazdálkodás ➢ Raktár-automatizálás ➢ Szállító drónok	➢ Önvezető autók/okosautók ➢ Járműkarbantartás ➢ Forgalomkezelés ➢ Flottakezelés	➢ Távorvoslás ➢ Hálózati implantátumok, gyógyszeradagolók ➢ Összekapcsolt egészségügyi monitoring ➢ Robotsebészet	➢ Erőforrás-elosztó rendszer ➢ Hatékonyság-figyelés ➢ Kibocsátásfigyelés ➢ Biztonsági figyelmeztetések ➢ Ipari robotok
	Eszközök	Okostelefonok, tabletek	Számítógépek	Autók	TV, videojátékok, konzolok	Háztartási gépek	Fitnesz okoseszközök
	Szenzorok	Audioszenzorok	Lézer	Infravörös / elektrooptikai	Helymeghatározás	Bioszenzorok	Sugárzási és kémiai detektorok
		RF detektor	Kamerák	RFID	Hőmérséklet-érzékelők	Motorfigyelés	Energiafelhasználás
	Analitika	Anomáliaészlelés	Viselkedéselemzés	Termékkövetés	Prediktív elemzés		Hatékonyságelemzés
	Infrastruktúra	Szerverek			Felhőszolgáltatások (számítás és tárolás)		

1. ábra: Az IOT-technológia alapelemei

Forrás: Denise E. Zheng – William A. Carter: Leveraging the Internet of Things for a more efficient and effective military. Center for Strategic & International Studies, 2015. alapján a szerző szerkesztése

Az 1. ábrán látható alapelemek az IoT-rendszerek és -hálózatok felépítésében általában négy, egymástól fizikailag vagy szolgáltatásilag elhatárolt szinten jelennek meg,

[2] Kovács László: *A kibertér védelme.* Budapest, Dialóg Campus, 2018. 82.

amelyekben megtalálhatók a szenzorok, a vezérlők, a kommunikációs eszközök, a hálózati átjárók, a kezelt szolgáltatások, valamint alkalmazások. Az utóbbiak vonatkozásában elsősorban a kritikus infrastruktúrák néhány elemében történő felhasználási lehetőségük van feltüntetve. Ezekből látható, hogy az IoT egyre nagyobb teret nyer a védelmi szféra egyes elemeinél, mind növekvőbb kihívást jelent a biztonságos környezetek kialakításában. Ahhoz, hogy ezek az eszközök, szolgáltatások, alkalmazások megfelelően tudjanak működni, a kapcsolat és biztonság szempontjából kiemelten fontos a megfelelő szabványok alkalmazása.[3]

Az IoT-alkotóelemek képességei

Az amerikai Nemzeti Szabványügyi és Technológiai Intézet[4] által 2018-ban készített jelentésben a tárgyak internetének nemzetközi kiberbiztonsági szabványosításának helyzetéről az alábbiakat fogalmazta meg az IoT képességeivel kapcsolatosan. A jelentés szerint a különböző IoT-rendszerek képességeinek több típusa is létezik:

- a különböző szenzorok, kamerák és egyéb érzékelők kölcsönhatásba lépnek a fizikai világgal;
- az adatképességek közvetlenül részt vesznek a rendszer funkcionalitásának biztosításában;
- az interfészképességek lehetővé teszik az egyes elem számára, hogy kölcsönhatásba lépjen más IoT-elemekkel (beleértve az embereket is);
- a támogatóképességek közvetetten részt vesznek a rendszer funkcionalitásának biztosításában, például a megfigyelésben, a menedzsmentben, a biztonság szavatolásában vagy az összehangolásban (az IoT összetevőinek elrendezése és irányítása az IoT-rendszerben);
- a rejtett képességek olyan átalakító-, adat-, interfész- vagy támogatóképességek, amelyek jelenleg nem engedélyezettek és hozzáférhetők az IoT-összetevőn kívül.

Működtetői képesség

A működtetői képesség lehetővé teszi a külső fizikai környezet vagy elemek megváltoztatását az IoT-összetevőre küldött vagy az azt irányító információk alapján. Példák: fűtőtekercsek (hőmérséklet-szabályozás), áramütés (szívritmus), elektronikus ajtózár (reteszelés/feloldás), pilóta nélküli légi jármű (UAV), működtetés (távirányító), szervomotorok (egyszerű mozgás, mozgás) és robotkar (összetett mozgás, mozgás).

[3] Zheng–Carter (2015) i. m. 6.
[4] National Institute of Standards and Technology.

Alkalmazási felület

Az alkalmazás interfészképessége más számítástechnikai eszközök (alkatrészek, rendszerek stb.) számára teszi lehetővé a kommunikációt az IoT-összetevővel IoT-alkalmazásokon keresztül. Példa egy alkalmazási felületre az alkalmazásprogramozási felület (API).[5]

Adatfeldolgozás

Az adatfeldolgozási képesség lehetővé teszi az adatok algoritmus alapján történő átalakítását. A transzformáció lehet nagyon egyszerű, egyetlen bemeneti változóval és egyetlen kimenettel, vagy lehet bonyolult több bemenettel és kimenettel. A vezérlőalgoritmusok a feldolgozás fontos elemei, amelyek az érzékelő(k), működtető(k) vagy előprocesszor(ok) kimenetén működnek, és olyan kimenetet biztosítanak, amelyek egy működtető vagy utófeldolgozó elembe illeszthetők. Az ilyen vezérlőalgoritmusra példa egy proporcionális-integrált-származékos (PID)[6] vezérlő (amelyet ipari vezérlőrendszerekben széles körben használnak). Egy másik példa egy algoritmus, amely modellezi az emberi inzulinválaszt egy valós idejű rendszerben, ami befolyásolja a mesterséges hasnyálmirigy működését. Az adatfeldolgozás további példái az alábbiak: adataggregációs képesség, prediktív elemzés és bináris (igen/nem) elemzés.

Adattárolás

Az adattárolási képesség lehetővé teszi az adatok tárolását és visszakeresését későbbi felhasználás céljából. Példa erre az összetevők bemeneti adatainak tárolása, valamint az összetevők által generált adatok, például elektronikus betegnyilvántartások tárolása.

Adatátvitel

Az adatátviteli képesség lehetővé teszi az adatok áthelyezését egyik fizikai vagy logikai helyről a másikra. Az adatátviteli képesség lehetővé teszi a hálózat „elrejtését”, és információkat szolgáltat a hálózatról anélkül, hogy az adott hálózati topológia nyilvánosságra kerülne. Az egyes IoT-elemek adatátviteli képessége befolyásolja az információáramlás késleltetését, valamint sebességét. Az adatátviteli képesség néhány példája az Ethernet protokollra és az IEEE 802.11 vezeték nélküli protokollra épülő adathálózatokon alapul.

[5] Application programming interface.
[6] Proportional–integral–derivative.

Emberi felhasználói felület (UI)[7]

Az emberi felhasználói felület képessége biztosítja az IoT-elemek közvetlen kapcsolatba lépését az emberekkel. Nem minden komponens rendelkezik emberi felhasználói felülettel. Ezek az összetevők továbbítják az információkat a többi rendszerösszetevőhöz az UI képességének támogatása érdekében. Példák: optikai és tapintható kijelzők, valamint audio be- és kimenet.

Rejtett képességek

A rejtett képességek azt jelentik, hogy egy IoT-elemhez való külső hozzáférés nincs engedélyezve vagy kihasználva. Például egy összetevőnek lehet USB-portja, de ehhez a porthoz semmi nincs bedugva. Ebben az állapotban az USB-port rejtett képességnek tekinthető. Megvan a lehetőség arra, hogy bármikor felhasználható legyen, és ha valaki hozzákapcsol valamit, az lehetővé teszi akár az eszköz többi képességének kihasználását is. Ha például valaki csatlakoztat egy wifiadaptert az USB-porthoz, akkor az IoT-összetevőnek egy további hálózati interfészképessége is lesz.

Hálózati felület

A hálózatifelület-képesség biztosítja az adatátvitelhez szükséges digitális kommunikációs hálózati összetevők közötti interfészt. Minden IoT-elemnek legalább egy hálózati interfészképességgel kell rendelkeznie. Noha a hálózati interfész képessége lehetővé teszi egy komponens csatlakoztatását a kommunikációs hálózathoz, önmagában nem biztosítja az adatátviteli képességet. A hálózati interfész lehet: Ethernet adapter, mobil vagy ZigBee rádióadapter.

Támogatás

A támogatóképesség további funkcionális képességeket biztosít az IoT-rendszer támogatásához. Példák: hangrendezés, időszinkronizálás, távoli menedzsment, rendszermemória-titkosítás, hitelesítés és megbízható végrehajtás.[8]

[7] User interface.

[8] National Institute of Standards and Technology: *NISTIR 8200 Interagency Report on the Status of International Cybersecurity Standardization for the Internet of Things (IoT).* 2018. 7.

IoT-szabványok és -protokollok

Az IoT-rendszerek kialakításánál elengedhetetlen, hogy olyan eszközöket alkalmazzanak, amelyekkel interoperábilis környezetek alakíthatók ki. Ezek eredményeképpen alkalmasak lesznek az egymással való kommunikációra, ezáltal az információmegosztásra, valamint egy olyan biztonságos környezet kialakítására, amelyben minden egyes elem képes az alkalmazott titkosítási eljárások kezelésére. Ezek kialakítására szabványfejlesztő és szabványügyi szervezetek jöttek létre, amelyek az IoT vonatkozásában is számos kötelező érvényű, illetve ajánlott követelményt fogalmaztak meg. Ezek közül a legjelentősebbek az IETF,[9] ITU-T,[10] IEEE,[11] TSI,[12] ISO/IEC,[13] ISA.[14] Az általuk elkészített szabványokat a gyártóknak már a tervezés folyamán figyelembe kell venniük, azokat a termékeikbe be kell építeniük, így lesznek az eszközeik használhatók a világ szinte minden pontján. Az egyes nemzetek további szabályozásokat vezethetnek be, ezek okozhatnak problémát az interoperábilis környezet kialakításában. Az alábbi szabványok a fenti szervezetek által meghatározott alapvető kommunikációs és titkosítási protokollok, amelyek segítségével megbízható infokommunikációs környezet alakítható ki az IoT-rendszerek számára.

- 6LoWPAN (IPv6 over Low-Power Wireless Personal Area Networks) – egy kommunikációs protokoll az IPv6-csomagok energiatakarékos vezeték nélküli hálózatokon történő továbbítására;
- Bluetooth és BLE[15]– kis energiaigényű, de a hagyományos Bluetooth-technikához hasonló hatótávolságot biztosító átviteli protokoll;
- Mobil cellás hálózatok (LTE/5G);
- CoAP (Constrained Application Protocol) – egy ügyfélszerver-protokoll, amelyet telemetriai adatok gyűjtésére használhatnak, elsősorban alacsony fogyasztású végponti eszközökről, például kihelyezett szenzorokról gyűjt adatokat;
- LoRaWAN (Long Ranged Wide Area Network) – kis fogyasztású szenzoroknak biztosít nagy távolságú és nehéz körülmények között is működő kommunikációt.

[9] IETF (Internet Engineering Task Force) – feladata, hogy kidolgozza, frissítse és fenntartsa az internet-, valamint a TCP/IP-technológiákat.

[10] ITU-T (International Telecommunications Union Telecommunications Standardization Sector) – az egyik legnagyobb és legrégebbi kommunikációs szabványügyi szervezet.

[11] IEEE (Institute of Electrical and Electronics Engineers) – egy szakmai szövetség, amely kidolgozza, meghatározza és felülvizsgálja az elektronikai, illetve informatikai szabványokat.

[12] ETSI (European Telecommunications Standards Institute) – világszerte alkalmazható szabványokat állít elő az infokommunikációs technológiákra (ICT) vonatkozóan, beleértve a vezetékes, a rádió-, a mobil, a mikrohullámú és az internetes technológiákat.

[13] ISO/IEC (International Organization for Standardization/ International Electrotechnical Commission) – az ISO egy független, nem kormányzati szervezet és a világ legnagyobb önkéntes nemzetközi szabványok kidolgozója. Az IEC a világ vezető szervezete az elektromos, elektronikus és kapcsolódó technológiák nemzetközi szabványainak elkészítésében és közzétételében.

[14] ISA (International Society of Automation) – egy nonprofit szakmai szövetség, amely az ipari és a kritikus infrastruktúra területén használt modern automatizálási és vezérlőrendszerek irányításának, biztonságának és kiberbiztonságának javítása érdekében határoz meg mérnöki/technológiai szabványokat.

[15] Bluetooth Low Energy – BLE.

Előnyei a kétirányú kommunikáció, az adatbiztonság, a mobilitás és a pontos helymeghatározás. Elsősorban az okosvárosokban alkalmazzák ezt a protokollt;
- MQTT (Message Queue Telemetry Transport) – egy egyszerű üzenetküldő protokoll, amely alacsony sávszélességű korlátozott eszközökhöz ajánlott, lehetővé teszi parancsok küldését kimenetek vezérlésére, érzékelő csomópontok adatainak olvasására és közzétételére;
- RFID (Radio Frequency Identification) – a rádiófrekvenciás tartományt használja fel beágyazott címkékben tárolt adatok kiolvasására. A technológia lényege a rádiófrekvenciás adó-vevő egység kommunikációja a megfigyelt tárgyakon vagy személyeken elhelyezett RFID-címkékkel. A kommunikáció automatikusan történik, akár emberi beavatkozás nélkül;
- X.509 – a nyilvános kulcsú infrastruktúra (PKI)[16] szabványa a digitális tanúsítványok és a nyilvános kulcsú titkosítás kezelésére. A szállítási réteg biztonsága (TLS)[17] a protokoll kulcsfontosságú része, amelyet a webes és e-mailes kommunikáció biztonságára használnak;
- Wifi – az IEEE 802.11 szabványon alapuló, széles körben használt, helyi hálózati hozzáférést biztosító, vezeték nélküli szabvány, amely lehetővé teszi, hogy az eszközök megosztott hozzáférési ponton keresztül kommunikáljanak egymással;
- Wifi Direct – a hagyományos wifi egy változata, ahol az eszközök hozzáférési pont nélkül képesek egymással kommunikálni;
- Z-Wave – a wifinél alacsonyabb energiaigényű, kis hatótávolságú, rövid késleltetésű és kisebb adatsebességű kommunikációs protokoll, amelyet elsősorban otthonok automatizálásnál alkalmaznak;
- ZigBee – az IEE 802.15.4 szabványon alapuló személyi hálózatokban alkalmazott kommunikációs protokoll, alacsony fogyasztás, adatsebesség, költség- és nagy áteresztőképesség jellemzőkkel.[18]

IoT-kommunikációs megoldások

Az IoT-rendszerek esetében az elsődleges kommunikációs megoldás a gépek közötti (M2M)[19] kommunikáció. Ebben a viszonylatban olyan eszközökről beszélhetünk, amelyek valamilyen információgyűjtő vagy -feldolgozó és -továbbító funkcióval rendelkeznek.

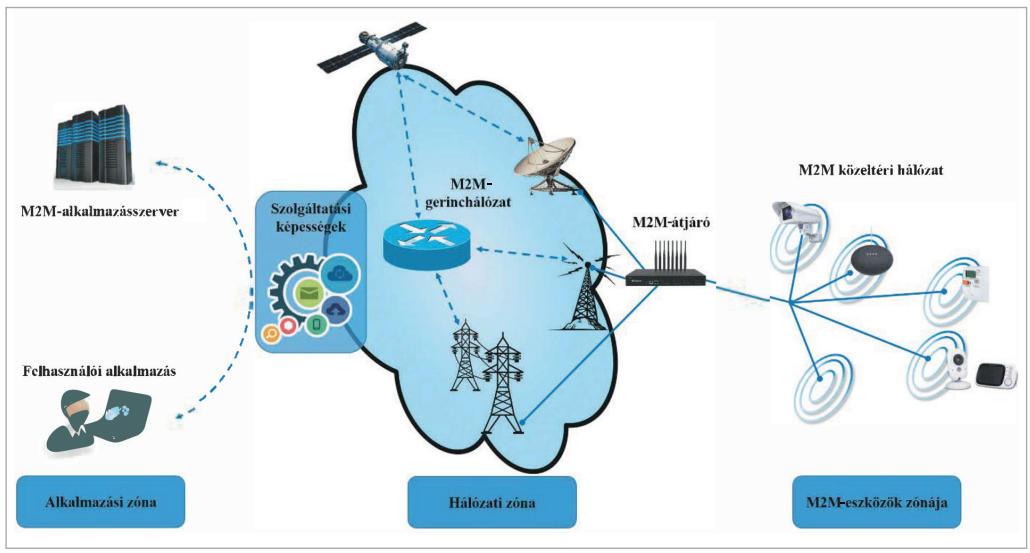
[16] PKI (Public Key Infrastructure) – a nyilvános kulcsú infrastruktúra az a rendszer, amelynek feladata a digitális aláíráshoz szükséges nyilvános kulcsok létrehozása, kibocsátása, közzététele, szervezése és visszavonása.

[17] TLS (Transport Layer Security) – a protokoll ügyfél/szerveralapú alkalmazások számára teszi lehetővé a biztonságos kommunikációt, elhárítva a lehallgathatóságot és az esetleges hamisítást.

[18] Balaji Yedle et al.: A survey: security issues and challenges in Internet of Things. In Asis Kumar Tripathy et al. (szerk.): *Advances in distributed computing and machine learning.* Proceeings of ICADCML, 2020. 78–80. (7586)

[19] M2M- (Machine-to-Machine-) kommunikáció – számos gazdasági területen és üzleti megoldásban használható, emberi beavatkozás nélkül adatok továbbítására, távmérésre, felügyeletre. A mobiltechnológia fejlődése, a cégek törekvése működési hatékonyságuk fejlesztésére.

A végponti elemek (szenzorok, kamerák, robotok stb.) alkalmasak a vezérlőegységektől vett feladatok alapján végrehajtani azokat a tevékenységeket, amelyekre az adott rendszerben rendeltetve lettek. Ezek általában olyan eszközök, amelyek alkalmasak a távmenedzsment fogadására, de léteznek olyanok is, amelyek csak egy előre felprogramozott feladat ellátására alkalmasak. Ebben az esetben az eszköz például gyűjti az információkat egy adott területről vagy RFID-címkéről, és a kialakított kommunikációs csatornákon továbbítja ezeket a feldolgozóközpontok felé. Nemcsak a begyűjtött adatokat kell továbbítani ezeken a hálózatokon, hanem az eszközök és azok környezete állapotával kapcsolatos információkat is.



2. ábra: Az M2M-kommunikáció

Forrás: Sallai Gyula – Abos Imre – Kósa Zsuzsanna – Adamis Gusztáv: *Felmérés-előkészítő tanulmány az M2M-alkalmazások számozási kérdéseiről.* Budapest, BME Távközlési és Médiainformatikai Tanszék, 2012. alapján a szerző szerkesztése

Az IoT-rendszerek egyre nagyobb kiterjedésűek és mind több eszköz található meg bennük. Vegyük példának az okosvárosok koncepcióját, ahol többek között okosközlekedésről, -környezetről, -gazdaságról, -kormányzásról, -életkörülményekről beszélhetünk. Ezek jól mutatják, hogy egy ilyen városi méret esetében akár több millió eszköz hálózatba kapcsolását kell megvalósítani. Ennek a kialakítására használják például a mesh-hálózatokat, ahol a központi irányítógépek szerepét már köztes hálózati elemek is képesek átvenni, amelyek önállóan szintén működőképes útválasztók, amelyek megosztják egymás közt a feladatokat. Ezzel a megoldással például elkerülhető, hogy egy csomópont kiesése esetén megszakadjon a kommunikáció a végberendezések és az irányítóközpont között. Maguk az IoT-eszközök is rendelkezhetnek olyan képességgel, hogy érzékeljék a környezetükben végbemenő forgalmi helyzetet, valamint az esetleges hálózati

meghibásodásokat, erről jelzést küldenek egymásnak, és reagálásképpen megváltoztatják a forgalomirányítást a hálózaton belül.

A Nemzeti Média- és Hírközlési Hatóság, valamint a BME Távközlési és Médiainformatikai Tanszék közötti együttműködés keretében készült tanulmány alapján az M2M-kommunikáció három különböző zónára különíthető el. Ezt a 2. ábra jeleníti meg:

- az M2M-eszközök zónája, amelyben az irányítandó gépek, eszközök vannak, mind egyedi irányíthatósággal és közeltéri kommunikációs képességgel. Az eszközzóna határán van az M2M-átjáró, amely a közeltéri jeleket összefogva küldi a távközlési hálózatokra, illetve szétosztja a hálózatok felől érkező jeleket;
- a hálózati zóna, amely többféle technológiával rendelkezhet: lehet vezetékes, vezeték nélküli, fix vagy mobil, különféle kapacitású;
- az M2M-alkalmazási zóna, ahol a távoli M2M-eszközök irányítása történik. Ebben az alkalmazási zónában van az M2M-alkalmazásszerver, amely a hálózatból jövő jeleket a felhasználó (kliens) számára transzformálja.[20]

Az IoT-rendszerek biztonsági kihívásai

Az IoT-rendszerek elleni átfogó támadások már évekkel ezelőtt megjelentek. Nagyon sok esetben olyan eszközöket alkalmaznak, amelyek nem vagy csak részben felelnek meg az előző fejezetben tárgyalt szabványoknak, követelményeknek, így azokban komoly sérülékenységek találhatók. A támadók ezeket a hibákat kihasználva hajthatnak végre szolgáltatásmegtagadásos támadásokat, felderíthetik és módosíthatják az információkat, megváltoztathatják az eszközökhöz vagy a hálózathoz rendelt rendszergazdai, illetve felhasználói jogosultságokat.

Az OWASP (Open Web Application Security Project) alapítvány IoT Sérülékenységek Projektje[21] (IoT Vulnerabilities Project) folyamatosan értékeli a dolgok internete területén meglévő biztonsági kihívásokat és sérülékenységeket. Ezek közül a legfontosabbakat és a legtöbbször előforduló sérülékenységeket egy adatbázisba rendezve, a támadási felületek alapján is kategorizálva nyilvánossá teszi. Az OWASP adatai alapján az IoT legfontosabb sérülékenységei közül a legjelentősebbek a következők:[22]

- gyenge jelszavak alkalmazása;
- kétfaktoros hitelesítés hiánya;
- titkosítatlan szolgáltatások;

[20] Sallai Gyula – Abos Imre – Kósa Zsuzsanna – Adamis Gusztáv: *Felmérés-előkészítő tanulmány az M2M-alkalmazások számozási kérdéseiről.* Budapest, BME Távközlési és Médiainformatikai Tanszék, 2012. 6.

[21] Az OWASP IoT-projekt célja segíteni a gyártókat, a fejlesztőket és a felhasználókat abban, hogy jobban megértsék a dolgok internetével kapcsolatos biztonsági kérdéseket, valamint hogy a felhasználók, legyen szó bármilyen környezetről is, biztonsági szempontból jobb döntéseket hozhassanak az IoT-technológiák építése, telepítése és értékelése során.

[22] Kovács (2018) i. m. 93–94.

– gyenge titkosítás;
– hiányzó frissítési mechanizmus;
– frissítés titkosítás nélkül;
– nem biztonságos szoftverek/firmware-ek;
– nem biztonságos külső gyártók;
– nem biztonságos interfészek.

A fentiekből jól látható, hogy a sérülékenységek nem feltétlenül csak a gyártók és szolgáltatók hibáiból adódnak, több esetben is felhasználói probléma okozza a bekövetkezett támadást. A védelmi szférában szintén jellemzően a biztonságtudatosság hiánya okozza a legtöbb hibát a kialakított infokommunikációs rendszerek zavartalan működésében. Ebben az esetben komoly problémát jelenthet az, hogy ezek a rendszerek kritikus információs infrastruktúrák részei lehetnek, ezzel veszélyeztetve akár a kritikus infrastruktúrák működését is. Ennek megfelelően komoly figyelmet kell fordítani a fenti veszélyek és fenyegetések megelőzésére, kivédésére. A fenti felsorolás alapján, valamint az elmúlt évek legjellemzőbb támadási vektorai és véghez vitt támadásai alapján a védelmi szférára a legveszélyesebb sérülékenységeket a továbbiak szerint lehet meghatározni.

Az első a gyenge, könnyen kitalálható jelszavak alkalmazása. Sajnálatos módon számos IoT-eszköz esetében nincs lehetőség az eszköz jelszavának megváltoztatására, ami biztonsági szempontból súlyos hibát jelent. Ez nagyon sok esetben azt jelenti, hogy a webes interfészek úgy vannak gyárilag beállítva, hogy nem teszik lehetővé a felhasználók számára az alapértelmezett jelszavak megváltoztatását, a rendszerbeállítások módosítását (hardveresen kódolt jelszavakat, a külső rootengedélyekkel futó szolgáltatásokat), és ez kiszolgáltatottá teszi őket a webes támadásokkal szemben. Ezenkívül sok IoT-terméket gyakran nem biztonságos firmware-rel[23] bocsátanak ki, amely hátsó kapukat tartalmaz, hogy hibakeresési célból hozzáférhessenek.

Az IoT-rendszerek biztonsága gyakran sérül az illetéktelen hozzáférés miatt, például a fentebb említett alapértelmezett jelszavak vagy a nyitott portok miatt. Ezek potenciálisan odavezethetnek, hogy ezeket az eszközöket egy nagyobb botnet[24] részeként használják fel. Hálózati biztonsági eszközök alkalmazásával, mint amilyen például tűzfalak, behatolásészlelő rendszerek (IDS),[25] behatolásmegelőző rendszerek (IPS),[26] egységes

[23] Közvetlenül a hardvereszközzel egybeépített memóriamodulban tárolt szoftver, amelynek feladata az eszköz működtetése, illetve az ahhoz szükséges alapvető be-/kimeneti rutinok biztosítása.

[24] A botnet vagy robothálózat egy fertőzött informatikai eszközökből álló hálózat, amelyet a botnet gazdája többféle károkozásra is alkalmazhat. A fertőzött munkaállomások felhasználásának célja főképp kéretlen levelek kiküldése, szolgáltatásmegtagadást okozó támadások (Denial-of-Service ─ DoS) indítása vagy éppen szenzitív adatok eltulajdonítása.

[25] IDS (Intrusion Detection System) – olyan hardveres, illetve szoftveres biztonsági megoldás, amely a hálózati forgalomba történő beavatkozás nélkül, válogatás nélkül figyeli az áthaladó csomagokat, ezzel szűrve az esetleges támadásokat.

[26] IPS (Intrusion Prevention System) – olyan aktív, a hálózat forgalmát áteresztő és vizsgáló eszköz, amely a hálózatba érkező csomagokat szoftveres átvizsgálást követően engedi át vagy dobja el. Amennyiben a behatolásmegelőző rendszer rosszindulatú forgalmat érzékel, lehetősége van az azonnali beavatkozásra. Riasztást küld a hozzá kapcsolódó felügyeleti állomásnak, majd a beállítások megváltoztatásával azonnal blokkolja a rosszindulatú forgalmat.

fenyegetéskezelő megoldások (UTM).[27] Ezek a védelmi szféra részére kiemelten fontosak, kiegészítve a következő néhány védelmi módszerrel, amelyekkel az IoT hálózati biztonsága növelhető:

- a felesleges használaton kívüli portok, valamint sérülékeny elemek kikapcsolása;
- külön hálózat kialakítása az intelligens eszközök részére;
- a távoli hozzáférést biztosító szolgáltatások letiltása;
- rendszeres frissítések telepítése.

A frissítések esetében elengedhetetlen olyan eszközök alkalmazása, amelyek rendelkeznek az ehhez szükséges funkciókkal. Ez alapkövetelmény a gyártók irányába, de még mindig megtalálhatók olyan IoT-elemek a piacon, amelyek nem alkalmasak például firmware-frissítésre. Ezekhez különböző frissítési mechanizmusokat alkalmazhatunk, amelyek nemcsak a javítások telepítéséről és a sebezhetőségek lezárásáról szólnak, hanem tartalmazhatnak olyan funkciókat is, mint például:

- az illesztőprogram-visszaállítást gátló mechanizmusok, amelyek célja, hogy megakadályozzák az eszköz szoftverének régebbi verzióra való visszaállítását, amely ismert sebezhetőségeket tartalmaz;
- a biztonságos kézbesítés (a frissítés egy zárt rendszeren keresztül jut el az egyes elemekhez, a frissítés aláírása stb.);
- a firmware-ellenőrzés az eszközökön.

A biztonságos vagy elavult alkatrészek, szoftverek használata, valamint a nem biztonságos könyvtárak hivatkozása az alkalmazott kódban az IoT-termékek általános biztonságának veszélyeztetéséhez vezethet. Az operációs rendszer nem biztonságos testre szabásától kezdve a sérülékeny, harmadik féltől származó hardver- vagy szoftverkomponensek használatáig az IoT biztonsági rései magukban foglalnak mindent, ami sebezhetővé teszi az eszközöket, belépési pontként használhatók, ezzel akár a teljes hálózatot veszélyeztetve a folyamatos támadási lehetőségeknek köszönhetően. A megfelelő biztonsági környezet kialakításához elengedhetetlen tudni, hogy milyen eszközök vannak a hálózaton, illetve ugyanolyan fontos azok hatékony kezelése is. Függetlenül az eszközök méretétől vagy egyedi költségeitől, ha kölcsönhatásban vannak a hálózattal, és hozzáférnek ahhoz, akkor az egyik legfontosabb feladat azok módszeres kezelésnek kialakítása. A hálózatok és rendszerek felügyeletének szerves részévé kell tenni az olyan jól bevált hálózatbiztonsági gyakorlatokat, mint például a frissítéskezelés, a biztonságos hardver- vagy szoftverkivonás. Ezenkívül komoly problémát jelentenek a kompromittált ellátási lánccal összefüggő kockázatok, amelyek esetében már a gyártási folyamat során olyan hátsó kapukat építenek be, amelyek észrevétlenek maradhatnak, így súlyosan befolyásolhatják az eszközök és rendszerek biztonságát.

[27] UTM (Unified Threat Management) – pontbiztonsági termékek összehangolt platformja, különösen a kis és közepes méretű vállalkozások számára. A jellemző szolgáltatáskészletek három fő részhalmazba sorolhatók, amelyek mindegyike az egységes fenyegetéskezelő megoldásokon belül van: tűzfal/behatolásmentesítő rendszer /virtuális magánhálózat, biztonságos web-átjáróbiztonság (URL-szűrés, webes vírusirtó) és az üzenetküldés biztonsága (antispam, mailvírusirtó).

2016 óta minden szervezetnek komoly figyelmet kell fordítania a személyes adatok védelmére, azonban a védelmi szférában emellett még számos olyan érzékeny adatot gyűjthetnek, dolgoznak fel vagy tárolnak, amelyek védelmére komoly hangsúlyt kell fektetni. A nem biztonságos adatátvitel és -tárolás komoly problémákat okozhat, éppen ezért a szakértők folyamatosan figyelmeztetnek a titkosításra, az adatok osztályozására és az érzékeny információk megfelelő kezelésére. Az adatokhoz való általános hozzáférés korlátozása mellett alapvető fontosságú az adatok titkosítása nyugalmi állapotban, szállítás vagy feldolgozás közben. Szigorú titkosítás és kulcsmenedzsment nélkül az adatok sebezhetőekké válnak, és jelentős IoT-biztonsági problémát okozhatnak. A fent említett aggályokon kívül a fogyasztói adatok gyűjtése – kifejezett hozzájárulás nélkül – mindvégig kérdés volt. Az ilyen adatok begyűjtése és megőrzése, különösen most, amikor az IoT a mindennapjaink részévé vált, szintén veszélyeztetheti a fizikai környezet biztonságát. Az adatvédelmet, különösen az IoT-t illetően, jogalkotási intézkedésekkel kezdik kezelni, amelyeket nemcsak nemzetközi és nemzeti, hanem vállalati szinten is szigorúan kell szabályozni.[28]

IoT-biztonsági megoldások és kihívásaik a védelmi szférában

Ahhoz, hogy a védelmi szférát esetleges érő támadások elkerülhetők legyenek, a legegyszerűbb megoldás az lenne, ha az eszközök nem csatlakoznának az internethez. Ez azonban az IoT-rendszerek esetében nagyon sokszor kivitelezhetetlen, így feltétlenül szükséges a következő megoldások alkalmazása. Minden körülmények között biztosítani kell, hogy a peremvédelmi lehetőségek olyan erősek legyenek, hogy lépést tudjanak tartani a körülöttük lévő gyorsan változó külső világból érkező veszélyekkel, újabb és újabb támadási módszerekkel. Napjainkban már nem elegendő csak az általános értelemben vett tűzfalakra támaszkodni, ezek már nem nyújtanak kellő védelmet, a támadók megtalálták azokat a biztonsági réseket, amelyek segítségével meg lehet kerülni a tűzfalakat, kihasználva az alkalmazások gyengeségeit. Éppen ezért szükséges a legújabb technológiák és szolgáltatások alkalmazása, folyamatosan felül kell vizsgálni az alkalmazott védelmi eljárásokat, módszereket annak biztosítása érdekében, hogy a rendszer, hálózat védelmi szintje megfeleljen a legújabb fenyegetések elleni kihívásoknak. Dinamikus és hatékony házirendet (policy) kell alkalmazni a gyanús tevékenységek folyamatos figyelemmel kísérése érdekében, amelybe foglalt rendszabályok a tevékenységek felfedezését követően gyorsan alkalmazhatók.

A felhasználók oktatására szintén komoly hangsúlyt kell fektetni. A felhasználói oktatás különösen fontos a mobil eszközök alkalmazásának területén, valamint az olyan alkalmazói helyeken, ahol a kíváncsi szemek könnyedén láthatják a jelszavakat vagy az adatokat. Fontos, hogy a felhasználók ismerjék a nem biztonságos hálózatokba történő bejelentkezésekkel járó fenyegetéseket, az eszközök elvesztésével járó kockázatokat, valamint a vezeték nélküli lehallgató kémprogramok működését, azok esetleges

[28] Open Web Application Security Project: Internet of Things Top 10.

felismerése céljából. Nem számít, hogy mennyire jól kialakított és kiépített hálózati biztonsági folyamatokat és rendszereket alkalmaztak, továbbra is a biztonság leggyengébb láncszeme a felhasználó. Megfelelő biztonságtudatosság kialakításával a kockázatok csökkenthetők, a biztonság szintje növelhető.

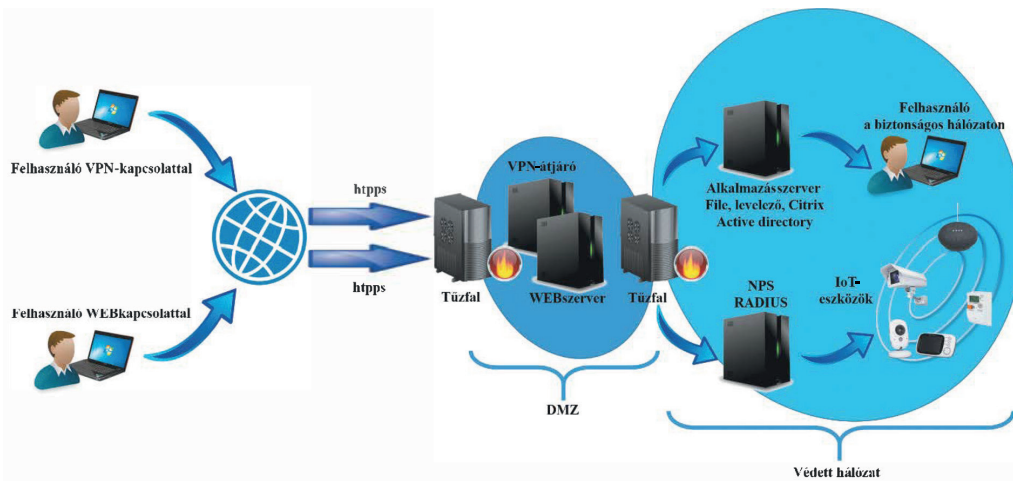
A következő komoly probléma, ami befolyásolja a rendszerek és különösen az IoT-rendszerek biztonságát, hogy az alkalmazott információs környezetek már nem csak az irodákra, intézményekre vagy otthonokra koncentrálódnak, így az adatforgalom nem feltétlenül a tűzfalak mögött zajlik. Az egyre szélesebb körben elterjedt és alkalmazott mobil informatika a hálózatok tradicionális határait nagyban kiszélesítette, aminek eredményeképpen a hálózatok biztonsági követelményeit feltétlenül újra kell gondolni. A hálózatok végponti peremei jelentősen eltolódtak, a mobil informatikai eszközök alkalmazásával a pontos határok nem meghatározhatók. Ennek eredményeképpen a hálózatok fizikai határai már nem tekinthetők a védelem végső vonalának, a nagy kiterjedésű peremvédelmi rendszerek sok esetben a biztonsági házirendek egy kritikus pontját eredményezik.

Éppen ezért a védelmi szférában az informatikai házirendet úgy kell meghatározni, hogy az a teljes hálózat minden szegmensére érvényes legyen. Így magában kell foglalnia minden olyan személyt, aki valamilyen szinten hozzáférhet a hálózathoz (felhasználó, rendszer-adminisztrátor, rendszer-üzemeltető, hálózatüzemeltető stb.), valamint minden olyan technikát és technológiát, amely a rendszerhez csatlakozhat vagy azon futtatható. Egy jól kialakított biztonsági házirend nem csupán egy dokumentum, hanem különböző intézkedések és rendszabályok összessége, amelyek egyes speciális területekre koncentrálódnak, mint például az eszközök és hálózatok használata, a felhasználóazonosítási formák, az e-mail-házirend, a távoli hozzáférési és mobil technológiák alkalmazása, valamint a webhasználati házirend. Kialakítása során minden körülmények között meg kell vizsgálni, hogy milyen erőforrásokat szükséges védeni (felhasználói pénzügyi vagy orvosi adatok, hitelkártya-információk stb.); hány felhasználó fog belépni a hálózatba (alkalmazottak, vállalkozók stb.); a hálózathoz történő hozzáférés csak bizonyos időpontokban vagy 24 órán keresztül a hét minden napján (és több időzónában és/vagy nemzetközi szinten) szükséges; milyen költségvetés áll rendelkezésre; a távoli felhasználók hozzáférnek-e a hálózathoz, és ha igen, hányan; lesznek-e földrajzilag távoli helyek (szükség van biztonságos mechanizmust, például replikációt igénylő adatok szinkronizálására a hálózaton keresztül).

A fentiek alapján kiemelten fontos a felhasználók számára a hálózat alapvető paramétereinek ismertetése a biztonságtudatosságuk növelése érdekében, ezzel csökkentve vagy akár megakadályozva egy esetleges támadás lehetőségét. Egy tipikus hálózati alaprajz látható a 3. ábrán, amelyen a nyílt és védett hálózat között tűzfalakkal elkülönített demilitarizált zóna (DMZ)[29] található, ami más néven peremhálózatként vagy átvilágított alhálózatként is ismert fizikai, illetve logikai alhálózat, amely elválasztja a belső helyi hálózatot a többi nem megbízható hálózattól, általában a nyilvános internettől. A külső kiszolgálók, az erőforrások és a szolgáltatások a DMZ-ben találhatók. Ezért elérhetők az internetről, de a belső hálózat többi része elérhetetlen marad. Szintén itt megoldható

[29] DMZ (Demilitarized Zone).

a virtuális magánhálózatok (VPN)[30] kialakításának lehetősége, ami a nyilvános hálózat fölött kiépített, titkosított hálózatot nyújt a külső felhasználók számára. Ez további biztonságot nyújt a védelmi szféra helyi hálózatai számára, mivel korlátozza a támadók azon képességét, hogy az interneten keresztül közvetlenül hozzáférjenek a belső szerverekhez, eszközökhöz és adatokhoz. A belső védett hálózatban helyezkednek el az olyan kiszolgálók, amelyek az ott elhelyezett eszközöket kezelik. Ilyen például a hálózatiházirend-kiszolgáló (Network Policy Server, továbbiakban: NPS),[31] amely lehetővé teszi az egész szervezetre kiterjedő hálózati hozzáférési házirendek létrehozását és kényszerítését az ügyfelek állapotára, a csatlakozási kérelmek hitelesítésére és engedélyezésére vonatkozóan.[32]



3. ábra: A védelmi szféra IoT-elvi hálózati diagramja

Forrás: Gemini George – Sabu M. Thampi: A graph-based security framework for securing industrial iot networks from vulnerability exploitations. *IEEE Access,* 6 (2018), 43586–43601. alapján a szerző szerkesztése

Ahhoz, hogy a fenti hardveres megoldások maradéktalanul megfeleljenek a biztonsági követelményeknek, minden esetben szoftveres védelmi megoldásokkal kell kiegészíteni. Ezek elengedhetetlenül szükségesek ahhoz, hogy a belső és a külső hálózat között biztonságos, védett kapcsolatot tudjunk létrehozni. Ilyen lehet például a hardverinterfészek tiltása, amivel megakadályozható, hogy egy fertőzött külső adathordozót csatlakoztassanak a hálózathoz. Feltétlenül szükséges a felhasználók hálózathoz való csatlakozása előtti hitelesítése, aminek minden esetben legalább kétfaktoros hitelesítésnek kell lennie hosszú élettartamú titkosítási kulccsal, ezzel garantálva a biztonságos kommunikációt. Szintén

[30] VPN (Virtual Private Network).
[31] NPS (Network Policy Server).
[32] Luís Costa – João Barros – Miguel Tavares: Vulnerabilities in IoT devices for smart home environment. In Paolo Mori – Steven Furnell – Olivier Camp (szerk.): *Proceedings of the 5th International Conference on Information Systems Security and Privacy.* Prague, 2019. 616–621.

kiemelten fontos a megbízható kulcskezelés az eszközök, átjárók és az M2M-összetevők között. Ez okozhat komoly fennakadást a védelmi szféra egyes elemei között az eltérő kulcsszabályozások miatt. Amennyiben kettő vagy több különálló szervezetnek kell együtt dolgoznia, és azok szeretnének egymás IoT-eszközeihez hozzáférni, feltétlenül szükséges a biztonsági kulcsok megosztása, amit nagy valószínűséggel minden szervezet biztonsági házirendje tilt. Erre alkalmazhatók például az olyan VPN-megoldások, amelyek a belső védett hálózaton belül kialakított alhálózatokhoz vagy virtuális alhálózatokhoz kapcsolódnak, amelyekben a használni kívánt IoT-eszközök elhelyezhetők.[33]

Összegzés

Az IoT biztonságának tanulmányozása közben egyértelműen megállapítható, hogy a rendszerek és hálózatok komplexitása miatt tökéletes megoldás nem garantálható. Az elemzések során meghatározott és megfogalmazott hardveres, illetve szoftveres megoldások csak együttes alkalmazás esetén lehetnek hatékonyak. Alapvetően megállapítható, hogy minden esetben alapkövetelmény a megbízható gyártótól és beszállítótól származó eszközök alkalmazása. Fontos komoly figyelmet fordítani az eszközök szoftvereinek, firmware-einek frissítéseire, amelyek hiánya komoly támadói potenciált jelenthet. Ugyancsak szükséges kiemelni a tűzfalak jelentőségét, amelyek segítségével demilitarizált zónák hozhatók létre a védett belső hálózatunk előtt, ami nagymértékben növelheti a rendszerek biztonságát. Szoftveres oldalról a legfontosabb a végponti eszközök és a kommunikációs csatornák titkosítása. A kialakított rendszernél feltétlenül figyelni kell a felhasználók rendszerbe lépése előtti hitelesítésére, ennek megfelelően olyan eljárásokat kell alkalmazni, amelyek többlépcsős hibrid hitelesítést alkalmaznak, ezzel elkerülve például az identitáshamisítást. Fontos szempont még a megfelelő kulcsmenedzsment kialakítása, amely az egyes IoT-eszközök, -átjárók és -kommunikációs összetevők közötti kulcsmegosztást, valamint kulcstárolást biztosítja. A tűzfalakkal megfelelően leválasztott belső hálózat esetében is mindenképpen célszerű szegregált hálózatokat kialakítani az IoT-összetevők menedzselésére, és minden egyéb kapcsolat más alhálózatra, esetleg virtuális alhálózatra történő áthelyezésére, hogy az egyes elemek kompromittálódása a lehető legkisebb negatív hatást gyakorolja a teljes hálózatra.

[33] Minhaj Ahmad Khan – Khaled Salah: IoT security: Review, blockchain solutions, and open challenges. *Future Generation Computer Systems,* 82. (2018), 400–402.

Felhasznált irodalom

Costa, Luís – João Barros – Miguel Tavares: Vulnerabilities in IoT devices for smart home environment. In Paolo Mori – Steven Furnell – Olivier Camp (szerk.): *Proceedings of the 5th International Conference on Information Systems Security and Privacy.* Prague, 2019. 615–622.

George, Gemini – Sabu M. Thampi: A graph-based security framework for securing industrial iot networks from vulnerability exploitations. *IEEE Access,* 6 (2018), 43586–43601.

Khan, Minhaj Ahmad – Khaled Salah: IoT security: Review, blockchain solutions, and open challenges. *Future Generation Computer Systems,* 82 (2018), May. 395–411.

Kovács László: *A kibertér védelme.* Budapest, Dialóg Campus, 2018.

National Institute of Standards and Technology: *NISTIR 8200 interagency report on the status of international cybersecurity standardization for the internet of things (IoT).* U.S. Department of Commerce, 2018.

Open Web Application Security Project: *Internet of Things Top 10,* 2018, Forrás: https://owasp.org/www-pdf-archive/OWASP-IoT-Top-10-2018-final.pdf

Sallai Gyula – Abos Imre – Kósa Zsuzsanna – Adamis Gusztáv: *Felmérés-előkészítő tanulmány az M2M-alkalmazások számozási kérdéseiről.* Budapest, BME Távközlési és Médiainformatikai Tanszék, 2012.

Yedle, Balaji – Gunjan Shrivastava – Arun Kumar – Alekha Kumar Mishra – Tapas Kumar Mishra: A survey: security issues and challenges in Internet of Things. In Asis Kumar Tripathy – Mahasweta Sarkar, Jyoti Prakash Sahoo – Kuan-Ching Li – Suchismita Chinara (szerk.): *Advances in distributed computing and machine learning.* Proceeings of ICADCML, 2020. 75–86.

Zheng, Denise E. – William A. Carter: *Leveraging the internet of things for a more efficient and effective military.* Center for Strategic & International Studies, 2015.