Kollár Csaba

IoT a gyakorlatban, az információbiztonság fókuszában I. – Az IoT működése, fejlődési tendenciái

Az IoT polgári életben tapasztalt dinamikus elterjedése a digitális technológiák négy területére vezethető vissza. Ezek a következők: a szenzorok csökkenő ára, az internet elterjedésének növekedése, az adattárházak bővítése és az adatok szervezésének leegyszerűsödése, illetve a gépi tanulás, a mesterséges intelligencia és az algoritmusok révén az adatelemzés és az adatbányászat fejlődése. Teoretikus tanulmányomban a digitális kor fejlődési területei közül az IoT és az információbiztonság kapcsolatára fókuszálok. Az IoT működésének bemutatása után a terület biztonsági aspektusát, majd az IoT-t érintő fontosabb változásokat ismertetem.
Kulcsszavak: digitális kor, információbiztonság, IoT, trendek

Bevezetés

Ha az információs társadalom korával előbb párhuzamosan futó, majd azt folyamatosan leváltó digitális kor, más néven az adatok kora tendenciáit, irányait szeretnénk meghatározni, akkor több olyan területet azonosíthatunk, amelyek köré markánsan szerveződnek a fejlesztések, a műszaki megoldások, az üzleti modellek, a kereskedelmi aktivitások. Ezek a területek meglátásom szerint a következők:

- felhőalapú szolgáltatások és megoldások (cloud computing),
- robosztus mennyiségű adatok elemzése (big data analytics),
- mobileszközök és mobilalkalmazások (mobile),
- közösségi média (social media),
- informatikai és információbiztonság (security),
- kiterjesztett és egyéb (kevert) valóságok (augmented reality),
- a dolgok internete (Internet of Things – IoT),
- robotok és drónok (robots),
- mesterséges intelligencia (AI) és gépi tanulás.

Nevezett tendenciák természetesen nem elkülönülten fejlődnek, sőt a gyakorlatban megjelenő megoldásoknál már elképzelhetetlen, hogy csak egy területet érintsenek

a fejlesztések. Jelen tanulmány az IoT, illetve az információbiztonság metszéspontjainak polgári és második részében katonai lehetőségeit kívánja bemutatni; de ahogy később látni fogjuk, a téma tárgyalása során a felhőalapú szolgáltatások, a nagy mennyiségű adat (közel) valós időben történő elemzése, az önvezérelt robotok, illetve a mesterséges intelligencia is említésre kerül.

2017-re az élet szinte valamennyi területén – igaz, eltérő fontossággal, de – megjelent az IoT és a hozzá kapcsolódó technológiák, megoldások. Az IoT szenzorai által szolgáltatatott és feldolgozott adatok révén olyan területek kapták meg rendszerint az „intelligens" (smart) előtagot, mint az energiaellátás, az ipari vállalatok, a hálózatok, az élet, a lakások/háztartások, az egészség, a városok, a mezőgazdaság, a szállítás, a kereskedelem, illetve a védelem és a közbiztonság.

Az Ericsson 2015-ös technikai jelentése szerint a gép és gép közötti kommunikáció (M2M) mennyisége éves szinten 25%-kal fog nőni 2020 végéig, ami azt jelenti, hogy a vállalatok 3 milliárd dollárt, a fogyasztók 900 millió dollárt fognak költeni az IoT és a hozzá kapcsolódó technológiák megvásárlására és bevezetésére.

A mérnököket egyesítő nemzetközi szervezet, az IEEE gondozásában megjelent tanulmány az IoT meghatározásával kapcsolatban leírja, hogy különböző definíciók és architektúrák léteznek az IoT modellezésére attól függően, hogy milyen üzleti érdekeket szolgálnak. Nevezett írásműben az IoT és a kapcsolódó témák definitív keretét elsősorban a nemzetközi szervezetek definíciói adják meg.

Az IEEE definíciója szerint IoT-nak tekinthetjük az összes olyan, szenzorokat tartalmazó hálózati elemet, amelyik az internetre csatlakozik. Az ETSI (Európai Távközlési Szabványügyi Intézet) 2010-es dokumentumában nem említi az IoT kifejezést, helyette az M2M-mel kapcsolatban úgy fogalmaz, hogy a gép–gép-kommunikáció során nem szükséges direkt emberi beavatkozás, mivel az M2M szolgáltatások automatizálni kívánják a döntéshozatalt és a kommunikációs folyamatokat. Az ITU (Nemzetközi Távközlési Egyesület) 2005-ös értelmezése szerint az IoT egy olyan hálózat, ami bárhol, bármikor, bárki és bármi számára elérhető. Ebben a kontextusban a fogyasztók által vásárolt termékek nyomon követhetőek a rájuk, a csomagolásukba vagy csomagolásukra helyezett apró rádióadók vagy érzékelők segítségével. Az amerikai szabványügyi és technológiai hivatal, a NIST a CPS (cyber-physical system, kiberfizikai rendszer) és az IoT fogalmát egymás szinonimájaként használja. Definíció helyett az NIST is inkább leírást ad az IoT-ra, két külön dokumentumban. A városok globális kihívásaival foglalkozó Smart America (Intelligens Amerika, 2014) szerint a CPS magában foglalja a különböző ágazatokban és iparágakban (szállítás, energia, gyártás, egészségügy) található intelligens eszközöket és rendszereket. Az intelligens városok/közösségek egyre inkább elfogadják a CPS/IoT-technológiákat, melyeknek segítségével működésük hatékonysága fokozható és fenntartható, az életminőség pedig javítható. A másik dokumentum az NIST CPS felsővezetőjének, Chris Greernek 2014-ben írt blogjából származik. Meglátása szerint a CPS, más néven IoT lehetővé teszi

a komplex rendszerek visszacsatolását és ellenőrzését, ami révén például a mentési műveletekben össze lehet hangolni a robotokat, a keresőkutyákat és a mentésben részt vevő embereket, vagy figyelemmel lehet kísérni a betegek gyógyulását azt követően is, hogy elhagyták a kórházat. A World Wide Web Konzorcium (W3C) álláspontja szerint az IoT a WoT (web of things – a dolgok webje) ernyője alatt helyezkedik el. A WoT gyakorlatilag a webes technológiák szerepét emeli ki azzal a céllal, hogy megkönnyítse az IoT-alkalmazások és -szolgáltatások fejlesztését.

Az internet vezető testületének mérnököket tömörítő szervezete, az IETF 2010-ben a következő leírást adta az IoT-val kapcsolatban: az alapötlet az, hogy az IoT kapcsolja össze a körülöttünk levő elektronikus, elektromos és nem elektromos tárgyakat, biztosítva a zökkenőmentes kommunikációt és az eszközök/tárgyak által nyújtott szolgáltatások elérhetőségét. Az RFID-val (Radio Frequency IDentification, termékek, eszközök egyedi megjelölésére használt rádiófrekvenciás azonosítás), szenzorokkal, aktuátorokkal, mobiltelefonokkal foglalkozó fejlesztések teszik lehetővé, hogy megvalósuljon az IoT, az eszközök/tárgyak egymással kölcsönhatásba lépjenek és együttműködjenek annak érdekében, hogy a kínált szolgáltatások egyre jobbak legyenek, bármikor és bárhonnan elérhetővé váljanak.

Az IETF szakembereinek véleménye szerint az IoT „dolgok" nagyon különbözőek lehetnek, mint például számítógépek, szenzorok, aktuátorok, emberek, hűtőszekrények, televíziók, járművek, mobiltelefonok, ruhák, élelmiszerek, gyógyszerek, könyvek stb. A dolgokat három kategóriába lehet sorolni, úgymint: (1) emberek, (2) gépek (szenzorok, aktuátorok), (3) információk (ruhák, élelmiszerek, gyógyszerek, könyvek).

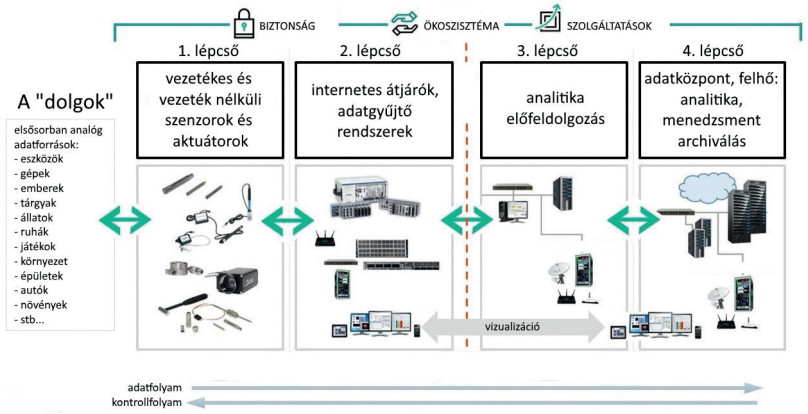
Tanulmányom aspektusában elsősorban Haig 2015-ös értelmezését veszem alapul az IoT fogalmának meghatározásakor: *„Az IoT egyedileg címezhető, saját IP-címmel rendelkező, egymással összekapcsolt objektumok világméretű hálózata, amely egységesen elfogadott címzési és kommunikációs protokollokon alapszik."* Ezek az eszközök nem szükségszerűen, de rendszerint egy vagy több szenzort is tartalmaznak, melyek a környezetben levő fizikai, kémiai, biológiai jellemzőket mérik, majd ezeket az adatokat feldolgozás céljából a felhőbe küldik, s az így keletkezett információ, tudás valamilyen formában megjelenik a felhasználó számára, illetve a mérési adatok összegződnek, s azokat csoportosan/tömegesen feldolgozzák, majd értékelik.

Atzori, Iera és Morabito [1] az IoT három dimenzióját (dologorientált, internetorientált, szemantikaorientált) különböztetik meg tanulmányukban, kiemelve, hogy e három metszéspontja maga az IoT. A dologorientált nézőpontba tartozik többek között az RFID, a UID (Unique Identifier, felhasználóazonosító), az intelligens áruk, az NFC (Near Field Communication, egymástól maximum néhány deciméterre levő informatikai eszközök között biztosít vezeték nélküli kapcsolatot és adatcserét), a WISP (Wireless Internet Service Provider – vezeték nélküli internetszolgáltató), a vezeték nélküli szenzorok és aktuátorok. Az internetorientált nézőpontba az IPSO (IP for Smart Objects, IP-címet az okos-

eszközöknek), maga az internet, illetve a WoT, míg a szemantikaorientáltba a szemantikus technológiák, az adatbányászat és -elemzés, illetve a szemantika alapú végrehajtás tartozik.

Az IoT működése

Az IoT felépítésével, architektúrájával, szerkezetével kapcsolatban a nagyobb vállalatok (DELL, Cisco, IBM, Fujitsu) saját elképzelésük szerinti modelleket vázoltak fel. Ezekben a modellekben, ha vizuális megjelenésükben el is térnek egymástól, de a szenzorok, az aktuátorok, a kapcsolódást elősegítő eszközök, az átjárók, a hálózat, a menedzselt szolgáltatások és az alkalmazások rendszerint megtalálhatók.



1. ábra: Az IoT négylépcsős architektúrája ([4] alapján saját szerkesztés)

Az IoT négylépcsős architektúráját [4] az 1. ábrán ismertetem. Látható, hogy a „dolgok" alapvetően analóg formában vannak jelen a rendszerben. Ez azt jelenti, hogy az analóg világ jeleit, tulajdonságait és jellemzőit át kell alakítani annak érdekében, hogy azok továbbíthatók, feldolgozhatók legyenek (2., 3., 4 lépcső). Sahoo [12] a szenzorokat a következő fontosabb kategóriákba gyűjtötte:

- akusztikus, hang és rezgés,
- autóipari, szállítás,
- kémiai,
- elektromos áram, elektromos potenciál, mágneses, rádiófrekvencia,
- környezetvédelmi, időjárás, nedvesség, pára,
- áramlás, folyadékok sebessége,
- ionizáló sugárzás, szubatomi részecskék,
- navigáció.

Az aktuátor Minerva, Biru és Rotondi [9] szerint olyan mechanikus eszköz, aminek az a feladata, hogy mozgasson vagy ellenőrizzen egy mechanizmust, egy rendszert. Az aktuátor – működésétől függően – a beérkező energiát arra használja, hogy megváltoztasson egy állapotot, aminek hatása lesz egy vagy több fizikai egységre/dologra. Halmai [7] a fizikai működési módjuk alapján az aktuátorokat az alábbiak szerint csoportosítja:

- mechanikus (villamos érintkezők és kapcsolók),
- elektronikus (teljesítménytranzisztor, tirisztor, triak),
- elektromágneses (egyen- és váltakozó áramú motorok, lineáris motorok),
- termikus (bimetallok, halmazállapot-változással működő aktuátorok),
- pneumatikus (pneumatikus hengerek, motorok),
- hidraulikus (hidraulikus hengerek, motorok),
- piezoelektromos (transzlátorok, motorok),
- emlékező fémes (mesterséges izom),
- magnetostrikciós (transzlátorok).

Hiba lenne azt állítani, hogy a szenzor–aktuátor együttműködés érdekében minden esetben szükség van arra, hogy a szenzorokkal érzékelt jelek adatok formájában továbbítódjanak az adatközpontba azzal a céllal, hogy az onnan induló kontrollfolyam (beavatkozás) révén az aktuátor működésbe lépjen. Az IoT-t megelőző technikai korszakokban is számtalan olyan megoldás létezett, amikor az automatizált rendszereknél a szenzor által mért értéket a rendszer „helyben" dolgozta fel, majd hozta működésbe az aktuátort (például ha a szobában a hőmérséklet bizonyos szint alá csökkent, akkor automatikusan bekapcsolt a fűtésrendszer). Ha egy ilyen klasszikus modellt az IoT szellemében szeretnénk modernizálni (például távfelügyelet, távvezérlés), akkor rendszerint lehetőség van a helyben hozott döntések felülbírálatára (például az elvárt hőmérsékleti szint megemelése távolról, okostelefonon keresztül). Általánosságban elmondható azonban, hogy sem az adatok mennyisége, sem azok feldolgozási ideje nem kritikus, hiszen az adatok alapján képzett adatsorok vizuális megjelenítése (táblázat, idősoros grafikon) inkább csak informatív jelleggel bír, illetve ha a távvezérlésben némi késés van, annak nincs semmilyen komoly hatása sem a rendszerre, sem a környezetére. Az olyan területeken azonban, mint a robotkarral végzett műtétek vagy a gépjárművek és repülőgépek, ahol nagyon sok adatot kell nagyon gyorsan feldolgozni, majd ugyancsak nagyon gyorsan kell beavatkozni a működésbe, alapvető fontosságú a gyorsaság, illetve a távoli elérések miatt a hálózati és az információbiztonság.

A szenzorok rendszerint az alábbi módon csatlakoznak a második lépcsőben található átjárókhoz és adatgyűjtő rendszerekhez:

- ODB2/EOBD (on board diagnostics/European on board diagnostics, fedélzeti diagnosztika),

- PLC (powerline communication, kisfeszültségű elektromos elosztóhálózaton történő adattovábbítás),
- RS-232 (Recommended Standard 232, pont–pont kapcsolatot biztosító távközlési adatátviteli szabvány),
- RS-458 (szabvány, mely a szimmetrikus adatátviteli módot írja le),
- Modbus (kommunikációs protokoll),
- USB (Universal Serial Bus, univerzális soros busz),
- SPI (Serial Peripheral Interface, nagy sebességű soros szinkron busz),
- RJ-45 (négy érpárból álló vezetékes adatátvitel),
- vezeték nélküli megoldások (wifi, Bluetooth stb.).

A második lépcsőnél találhatók az internetes átjárók, valamint az adatgyűjtő rendszerek. Ezek feladata a következő:

- a szenzoroktól érkező adatok összegyűjtése és digitalizálása,
- az összegyűjtött és digitalizált adatok továbbítása feldolgozásra, elemzésre, a beavatkozáshoz szükséges döntések meghozatalára, megjelenítéshez, archiváláshoz,
- gyors és biztonságos információáramlás biztosítása az aktuátorok felé.

Az adatok továbbítása egyaránt történhet vezetékes és vezeték nélküli kommunikációs protokollok segítségével, akár WAN-, akár LAN-hálózatokon. A fontosabb protokollok:

- Ethernet („helyi hálózatok kommunikációs technikája”),
- Bluetooth (nyílt, vezeték nélküli szabvány rövid hatótávolságú adatcseréhez),
- IEEE 802.11 (az OSI modell fizikai és adatkapcsolati rétegét definiáló vezeték nélküli protokoll, ahol az alap sávszélesség 2 Mb/s, a használt frekvencia 2,4 GHz),
- IEEE 802.15.4 (a vezeték nélküli személyi hálózatok működését leíró szabvány),
- Zigbee (rövid hatótávolságú, vezeték nélküli kapcsolódási technológia),
- GSM (Global System for Mobile Communications, a digitális kommunikációt az egész világon lehetővé tevő mobilkommunikációs szabvány),
- LTE (Long Term Evolution, negyedik generációs, azaz 4G vezeték nélküli mobilinternetes szabvány),
- 3G, 4G, 5G (a növekvő számmal egyre nagyobb adatátviteli sebességet lehetővé tevő vezeték nélküli mobilinternet-szabványok),
- RFID,
- NFC.

A konkrét kapcsolat megvalósításánál az adat- és információbiztonság mellett mérlegelni kell, hogy ezek az eszközök fizikailag mennyire messze találhatók a 3. lépcsőnél megnevezett elemző és előfeldolgozó rendszerektől, illetve, hogy a meglevő vezetékes vagy vezeték nélküli infrastruktúra képes-e megfelelni (akár gyorsaságban, akár sávszélességben) az el-

várásoknak. Előfordulhat az is, hogy a szenzorok által mért adatokat egy hordozható adatgyűjtő és előfeldolgozó eszköz (például céltablet) együttesen kezeli úgy, hogy a szenzorok közelében elhaladó operátor gépe és a szenzorok között az adattovábbítás megtörténik, majd a hordozható eszközről az előfeldolgozott adatok vezeték nélküli kapcsolaton keresztül továbbítódnak a felhőbe, további feldolgozás és egyéb feladatok elvégzése érdekében.

A harmadik lépcső feladata az, hogy elvégezze az összegyűjtött adatok elemzését, illetve előfeldolgozását. Az itteni eszközök és berendezések fizikailag megtalálhatók például a vállalatnak azon a telephelyén, amelynél a fizikai környezet folyamatos monitorozása zajlik, de arra is találhatunk megoldást, hogy inkább a 4. lépcsőnél megnevezett eszközökhöz és rendszerekhez van közel vagy azokkal egy helyen van. Biztonsági szempontból fontos kérdés lehet az, hogy mi a kisebb kockázattal járó megoldás: a helyben keletkezett nagy adatmennyiség előfeldolgozása is helyben történjen meg (tehát a 2. és 3. lépcső egymás mellett van), majd az így előfeldolgozott, strukturált adatokat továbbítsák a távoli 4. lépcső felé, vagy a nyers adatok az összegyűjtést követően a fizikailag távol levő 3. (majd 4.) lépcső felé továbbítódjanak.

Ha a fejlesztést az első megközelítés szerint realizálják, akkor olyan esetekben, amikor a rendszer működésébe be kell avatkozni (üzemzavar), nem történhet meg az, hogy a távoli hozzáférés megszűnése vagy akadozása miatt a beavatkozás nem vagy időben csak lényegesen később valósul meg. Az egyszerűbb hibák tehát helyben és hatékonyan kezelhetők, a mélyrehatóbb, komparatív és szemantikai elemzésekre pedig később kerül sor. A második esetben – a nagy számítási kapacitások igénybevétele miatt – egy összetettebb üzemzavar esetén pontosabban, komplexebb módon, több, egymással összefüggő területen lehet beavatkozni a rendszer működésébe, feltéve, hogy a meghibásodás (teljes áramkimaradás, beázás, robbanás) nem érinti az adattovábbítással és a feldolgozott adatok fogadásával foglalkozó hálózati infrastruktúrát.

A negyedik lépcső az adatközpont és a felhő helye. Itt történik meg az adatok komolyabb elemzése és menedzselése, az adatbányászat, a nagy számítási kapacitást igénylő műveletek alapján az algoritmusok, az adatok közötti kapcsolatok (korreláció), a trendek vizsgálata, a vizsgálati eredmények alapján az akár automatikus, akár ember által jóváhagyott döntések meghozatala, majd a döntések alapján az aktuátorok felé a kontrollparancsok kiadása. A negyedik lépcső feladata továbbá az adatok biztonságos tárolása akár archiválás, akár további feldolgozás céljából, illetve az is, hogy az adatbázisból a helyi adatgyűjtő rendszerek számára könnyen és gyorsan értelmezhető vizuális állapotjelentéseket szolgáltasson.

Az adatmenedzsment fontosabb részei, rendszerei és feladatai a következők [11]:

- OSS/BSS (operations support systems/business support systems, tevékenységi és üzleti támogató rendszerek), például termékmenedzsment, fogyasztómenedzsment, pénzügyi menedzsment, megrendelésmenedzsment,

- elemzőplatformok: statisztikai elemzés, adatbányászat, valós idejű elemzés, szövegbányászat, in-memory elemzés, prediktív elemzés,
- adatok: adatirányítás, adatanonimitás, adatraktározás, adatminőség-menedzsment,
- biztonság: hozzáférési jogosultságok kezelése, titkosítás, hozzáférés monitorozása,
- BRM (Business rules management, üzleti szabályok menedzselése): definíciók, szabálymodellek, szabályszimulációk, szabályvégrehajtások,
- BPM (business process management, üzleti folyamatok menedzselése): munkafolyamat, folyamatmodellezés, folyamatszimulációk, folyamatok végrehajtása.

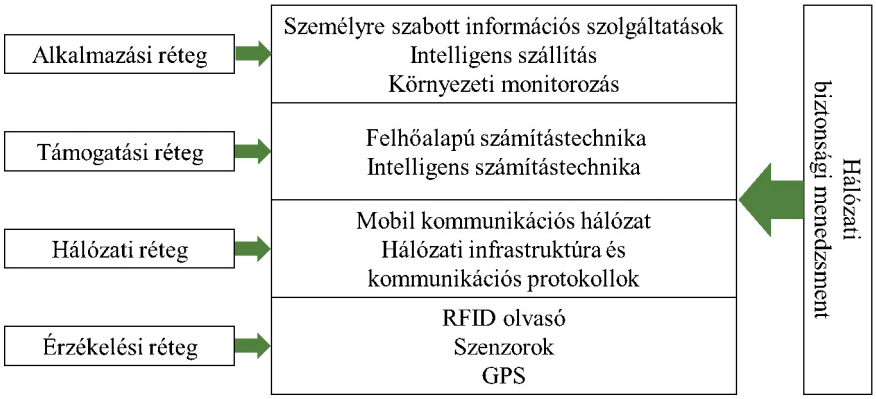
Fuller négylépcsős modelljénél már többször esett szó az IoT és a biztonság kapcsolatáról. Tanulmányom következő alfejezetében ezzel a témával foglalkozom részletesebben.

Az IoT és a biztonság

Kaur [8] az OWASP (Open Web Aplication Security Project) jelentésére hivatkozva tíz olyan biztonsági tényezőt nevez meg, amelyek közvetve vagy közvetlenül az IoT-ra, a rá épülő technológiára és alkalmazásokra is hatással lesznek. Ezek a következők:

1. nem biztonságos webes felületek,
2. nem megfelelő szintű azonosítási és engedélyezési eljárások,
3. nem biztonságos hálózati szolgáltatások,
4. hiányzó vagy gyenge algoritmust használó titkosítás az adatok továbbítása során,
5. adatvédelmi problémák,
6. nem biztonságos felhő interfész,
7. nem biztonságos mobil interfész,
8. nem megfelelő biztonsági konfigurálhatóság,
9. bizonytalan/kétes forrásból származó szoftverek és firmverek,
10. gyenge fizikai biztonság.

A továbbiakban az IoT biztonsági architektúrájának négy szintjét (rétegét) ismertetem, úgymint: érzékelési réteg, hálózati réteg, támogatási réteg, illetve alkalmazási réteg (2. ábra). Mind a négy réteg biztonsági követelményeinek kialakításánál figyelembe kell venni a hálózati biztonsági menedzsmentet.



2. ábra: Az IoT biztonsági architektúrája ([2] alapján saját szerkesztés)

A legalapvetőbb biztonsági réteg az érzékelési, más néven felismerési réteg. Ez a réteg segít azonosítani a fizikai világot, illetve ebben a rétegben történik meg a fizikai világ jellemzőinek érzékelése. Ebben a rétegben vannak az érzékeléshez szükséges szenzorok és egyéb eszközök is. Az érzékelési csomópontok rendszerint kis számítási kapacitással rendelkeznek, ezzel párhuzamosan a fogyasztásuk is csekély. Gyengeségük jelenti sebezhetőségüket, mivel a bonyolultabb titkosítási algoritmusokat nem képesek kezelni, így nagyon nehéz ezen a szinten megvalósítani a megfelelő informatikai biztonságot, illetve a hatékony védelmi rendszert. Az érzékelési rétegben levő eszközök ellen külső hálózatokból DoS (Denial of Service, túlterheléses támadás) támadásokat lehet indítani, ami az adatfolyamban okozhat fennakadásokat. További követelmény, hogy a szenzorok által mért adatokat meg kell védeni a CIA (confidentiality, integrity, availability, bizalmasság, sértetlenség és rendelkezésre állás) elve szerint is. Megoldás: a csomópontok hitelesítése, a csomópontokhoz történő illegális hozzáférések megakadályozása, kis erőforrásigényű titkosítási technológiák kidolgozása, a szenzorok adatvédelme, a szenzorok hitelesítése, megállapodások a biztonsági (kvázi) szabványok tekintetében az iparág szereplői között.

A hálózati réteg feladata az érzékelési rétegben keletkezett adatok és információk továbbítása, valamint az adatok kezdeti feldolgozása, illetve osztályozása is. A hálózati rétegben található az adatátvitellel kapcsolatos vezetékes és vezeték nélküli infrastruktúra (internet, mobil kommunikációs hálózat, műholdas hálózatok, vezeték nélküli hálózatok), illetve különböző kommunikációs protokollok. Dastikop [2] szerint e réteg törzshálózata viszonylag biztonságosnak tekinthető, de a közbeékelődéses támadás (man-in-the-middle attack) komoly veszélyforrás lehet, s nem lehet figyelmen kívül hagyni a rendszer terheléséből és hibájából (például tömegével érkező levelek, számítógépes vírusok) származó adattorlódást sem. Mivel úgy tűnik, hogy az érzékelési rétegen a biztonság a technikai korlátok miatt csak részlegesen oldható meg, ezért ezen a szinten (ahol ezek a korlátok nem jellemzőek) kell kidolgozni és alkalmazni a megfelelő biztonsági mechanizmusokat.

Megoldás: identitáshitelesítés annak érdekében, hogy az illegális csomópontok ne tudjanak a hálózathoz csatlakozni, a veszélyeztetett csomópontok feltérképezése, valamint a hálózatokra jellemző általános információbiztonsági előírások megtartása.

A támogatási, más néven hordozórétegben találhatók meg a különböző intelligens számítástechnikai megoldások, a grid technológia, illetve a felhőalapú számítástechnika. Feladata a kapcsolat biztosítása a hálózati és az alkalmazási réteg között. Ebben a rétegben történik az adatok tömeges feldolgozása és az intelligens döntéstámogatás, így az alapvető információbiztonsági kihívás a rosszindulatú/hamis információk felismerése, kiszűrése, kezelése. Megoldás: erős titkosítási algoritmusok alkalmazása, aktívan futó víruskeresők, a vírusadatbázisok folyamatos frissítése.

Az alkalmazás(i) réteg biztosítja a személyre szabott információs szolgáltatásokat, és ennek segítségével tud a felhasználó hozzáférni az olyan intelligens eszközökhöz, mint az okostévé vagy az okostelefon. Az alkalmazás(i) rétegben a biztonság a különböző alkalmazásoktól függ, így számos biztonsági problémával lehet számolni. Ezek közül a gyakoribbak: az adatok illetéktelen megosztása, a nem megfelelő hozzáférés, a hozzáférési adatok ellopása, illetve a felhasználó gyengeségét kihasználó különböző social engineering technikák. Megoldás: a felhasználók információbiztonság-tudatosságának fejlesztése, a biztonságtudatosság fejlesztésével kapcsolatban új pedagógiai és didaktikai módszerek kidolgozása és bevezetése.

A fentebb bemutatott biztonsági architektúra mellett másféle struktúra szerint is osztályozni lehet az IoT biztonsági kockázatait, illetve az általa használt technikák és megoldások ellen elkövetett támadásokat. Kaur [8] a támadási módszereket passzív és aktív támadásokra osztja.

A passzív támadások közé sorolhatóak a következők.

- Lehallgatás: a támadó elfogja a szenzorok által rögzített és továbbított adatokat, ennek alapján saját vagy megbízója elvárásai szerint tudja magát az adatokat elemezni.
- Forgalom elemzése: a támadó elemezni tudja a hálózaton folyó adatmennyiség változását, így meg tudja határozni a bázisállomások helyét, illetve a használt protokollokat is.
- Üzenetfecskendezés (message injection): a támadó hamis adatokat juttat a hálózatba, szofisztikáltabb támadás esetén az ellenőrző információkat módosítja.

A fontosabb aktív támadások a következők:

- Üzenet módosítása: a támadó a korábban rögzített adatokat módosítja.
- Csomópontelfogás (node capture): a támadó átveszi az irányítást a csomópontok felett.
- DoS-t támadások: például túlterhelés.

Az IoT-t érintő változások a közeljövőben

Oro [10] a Gartner kutatásai alapján tíz területet nevez meg, ahol az IoT jelenleg és a közeljövőt változni fog:

1. IoT és biztonság: az IoT tömeges elterjedésével egy időben megannyi biztonsági kockázat is megjelenik, melyek egyaránt érintik magukat az IoT-eszközöket, az operációs rendszereket, a kommunikációs csatornákat, valamint a kapcsolódó rendszereket. Komoly veszély, hogy jelenleg nincsenek még kiforrott és megfelelően biztonságosnak tartott rendszerek és megoldások ahhoz, hogy megvédjék a nevezett komponenseket. A biztonsági kockázatot az is növeli, hogy az eszközökben rendszerint egyszerű processzorok, illetve operációs rendszerek vannak, amelyek nem támogatják a kifinomult és fejlett biztonsági megoldásokat.
2. IoT és eszközfelügyelet: a fent leírtakkal összhangban a jövőben olyan megoldásoknak kell megjelenniük (lásd lentebb részletesebben), amelyek lehetővé teszik az eszközök monitorozását, firmware-, illetve szoftverfrissítését, diagnosztikáját, az ellenük elkövetett támadások elemzését, általánosságban és teljeskörűen a biztonságmenedzsmentet.
3. IoT és elemzés: azzal, hogy az IoT egyre több és több adatot gyűjt a felhasználókról, lehetővé teszi viselkedésük jobb és teljesebb megismerését, ami révén hatékonyabb üzleti modellekre épülve lehet majd a marketinget folytatni. Nagy valószínűség szerint a BDA (big data analytics, hatalmas mennyiségű adat feldolgozása) módszerei az IoT területén is megjelennek a közeljövőben.
4. Kis teljesítményű és rövid hatótávolságú IoT: a fejlesztések során az eddigihez képest hangsúlyosabban jelennek meg olyan elvárások, mint a megfelelő vezeték nélküli hálózat kiválasztása, a hálózat sávszélessége, az eszközök fogyasztása és az akkumulátorok kapacitása, az adott fizikai területen levő eszközök száma/sűrűsége, a végpontok és az üzemeltetés költségei. Bár Gartner egyértelműen a kis teljesítményű és rövid hatótávolságú eszközök elterjedését jósolja, egységes megoldásokról mégsem lehet beszélni az eltérő kereskedelmi, technikai elvárások és kompromisszumok miatt.
5. IoT és a kis teljesítményű WAN: a hosszabb távú cél az, hogy országos szinten az adatátviteli sebesség a bps-ből a kbps (kilobit per second) tartományba ugorjon olyan IoT-eszközök használata mellett, amelyek akkumulátora akár tíz évig is képes az eszközöket kiszolgálni. Költségoldalról az elvárás az, hogy egy végponthardver költsége 5 dollár körül mozogjon, s képes legyen biztosítani akár több százezer eszköz csatlakozását a bázisállomáshoz vagy azzal egyenértékű állomásokhoz. Ugyan az első LPWAN (low power wide area network, alacsony fogyasztású WAN) a tervek szerint már védett technológián fog alapulni, de nagy

valószínűség szerint az olyan szabványok fogják hosszabb távon uralni a piacot, mint az NB-IoT (Narrowband IoT, keskeny sávú IoT).

6. Az IoT-processzorok: a processzorok fejlesztésénél is számos szempontot figyelembe véve vázolhatók fel az irányok. Ilyen szempont többek között: erős biztonsági és titkosítási képességek, hatékony és alacsony energiafelhasználás, az operációs rendszerek akadásmentes támogatása, firmware frissítésének lehetősége, beágyazott megoldások támogatása. Az IoT-eszközök elterjedésénél – gazdasági aspektusból – fontos tényező a processzorok ára, aminél többek között a fejlesztési és a gyártási költségek csak akkor eredményeznek a vállalatoknak komolyabb nyereséget, ha az egy processzorra vetített költség alacsonyan marad.
7. Az IoT operációs rendszerek: a hagyományos operációs rendszereket, mint a Windows vagy az IOS nem arra tervezték, hogy hatékonyan együttműködjenek az IoT-technológiát használó eszközökkel és rendszerekkel. Az ok, hogy ezek az operációs rendszerek túl sok energiát fogyasztanak, gyors processzorra van szükségük, és bizonyos esetekben hiányzik az a képességük, hogy garantált valós idejű választ adjanak. Ezeknek az operációs rendszereknek nagy memóriára van szükségük a működéshez, ami nem egyezik az IoT-eszközök és -csipek fejlesztőinek az elképzeléseivel. Ez azt jelenti, hogy több olyan IoT-specifikus operációs rendszert fejlesztettek már eddig is, ami jobban megfelel a valós elképzeléseknek és igényeknek.
8. Eseményfolyam-feldolgozás: alapvetően nem az adatok robusztus mennyisége az elsődleges szempont az IoT elvárt működésével kapcsolatban, hanem az, hogy az adatok nagy adatátviteli sebességgel kerüljenek a feldolgozó egységhez, az adatfeldolgozás valós időben történjen meg, majd ugyanolyan nagy sebesség mellett továbbítódjanak a beavatkozó egységhez (például aktuátor). Ugyanakkor azzal is számolni kell, hogy a távközlési és a telemetriaipar egyre nagyobb adatmennyiség-igényeket támaszt (több tízezer, több millió esemény másodpercenként), ahol ugyancsak alapvető elvárás a valós idejű folyamatok realizálása.
9. IoT-platformok: az IoT-platformokban egyetlen eszközben számos infrastruktúra-összetevő található. A platformok által nyújtott szolgáltatások három kategóriába sorolhatók: (1) alacsony szintű eszközellenőrzés és műveletek, (2) adatgyűjtés, -átalakítás és -kezelés, (3) alkalmazásfejlesztés, értve ez alatt az eseményvezérelt logikát, az alkalmazásprogramozást, a megjelenítést, az elemzést és olyan csatolófelületeket, amelyek révén az eszközök a vállalati rendszerekhez képesek csatlakozni.
10. IoT-szabványok: olyan IoT-szabványok alakulnak ki és terjednek el, amelyek lehetővé teszik, hogy az eszközök egymással varratmentesen tudjanak kommunikálni, lehetővé téve az adatok megosztását számos eszköz és szervezet (felhasználó) között.

Következtetések

A technológiák fejlődését józansággal érdemes mérlegelni. Egy új technológia, mint amilyen az IoT is, elindítja a kreatív ötletekre épülő fejlesztéseket, s az innovatív, korai elfogadó fogyasztók örömmel és lelkesen kezdik el használni ezeket a kézzelfogható eredményeket. Az ipari felhasználók inkább racionális döntéseket hoznak, az IoT észszerű és tervszerű használata kimutatható előnyöket jelent a vállalatok számára. Az IoT-ban érintett szereplők – fejlesztők, kereskedők, vásárlók stb. – többségének a biztonságtudatossága vagy szűkebben értelmezve az információbiztonság-tudatossága nem tekinthető elfogadható szintűnek. A semmilyen vagy egyszerűbb titkosítási algoritmusokra épülő védelem nem jelent igazi megoldást a használat során, a támadások pedig – bár eltérő módszerek révén, de – valamennyi rendszerelemnél megjelenhetnek. Az IoT tömeges elterjedésének véleményem szerint az lesz a sarkalatos pontja, hogy a közeljövőben megjelennek-e olyan ajánlások/szabványok, amelyek használata és betartása biztosítani tudja az IoT-rendszerek biztonságos használatát. Az elvárások már most is világosak: biztonságos felhőalapú infrastruktúra, szabványokra épülő legjobb gyakorlatok népszerűsítése, biztonsági fókuszú terméktervezés, biztonságos csatlakozás a fizikai elemekhez és a hálózathoz, biztonságos szolgáltatások és alkalmazások, biztonságtudatos felhasználók és biztonságos hozzáférések.

Összefoglalás

Tanulmányom elsődleges célja az volt, hogy bemutassam a digitális kor egyik legdinamikusabban fejlődő területének, az IoT-nak a működését, illetve rávilágítsak a használata során felmerülő biztonsági problémákra, melyek az írásművemben ismertetett IoT biztonsági architektúrájának érzékelési, hálózati, támogatási, illetve alkalmazási rétegeinek szintjén értelmezhetők. Az érzékelési és a hálózati rétegekben a hitelesítés, a csomópontokhoz történő illetéktelen hozzáférés megakadályozása a nagyobb biztonság irányába mutat. A titkosítási algoritmusok ugyancsak pozitívan hatnak a biztonságra, különösen az érzékelési és a támogatási rétegekben, de az előbbinél csak a kis erőforrás-igényű titkosítási technológiák alkalmazhatók. A biztonságtudatosság humán aspektusával hangsúlyosan az alkalmazási rétegnél találkozhatunk, ahol számolni lehet social engineering típusú támadásokkal. A megoldást a felhasználók információbiztonság-tudatosságának a fejlesztése, a biztonságtudatosság fejlesztésével kapcsolatban új módszerek kidolgozása és bevezetése jelenti.

Irodalomjegyzék

[1] Atzori, Luigi – Iera, Antonio – Morabito, Giacomo: The Internet of Things: A survey. *Computer Networks*, 2010/54, 2787–2805.

[2] Dastikop, Ravindra: *Will Internet of Things (IoT) be secure enough?* www.slideshare.net/indravi/will-internet-of-things-iot-be-secure-enough

[3] *Ericsson Mobility Report on the Pulse of the Networked Society. Technical Report.* Ericsson, Stockholm, 2015. november.

[4] Fuller, J. R.: *The 4 stages of an IoT architecture.* https://techbeacon.com/4-stages-iot-architecture

[5] Haig Zsolt: *Információ, társadalom, biztonság.* Nemzeti Közszolgálati Egyetem, Budapest, 2015.

[6] Haig Zsolt – Várhegyi István: *Hadviselés az információs hadszíntéren.* Zrínyi Kiadó, Budapest, 2005.

[7] Halmai Attila: *Szenzor- és aktuátortechnika.* Edutus Főiskola, Tatabánya, 2011.

[8] Kaur, Ramnek: *Security IN IoT.* www.slideshare.net/gr9293/security-in-iot

[9] Minerva, Roberto – Biru, Abyi – Rotondi, Domenico: *Towards a definition of the Internet of Things (IoT) (rev.1).* Torino, IEEE Internet Initiative, Torino, 2015.

[10] Oro, David: *Gartner Identifies the Top 10 Internet of Things Technologies for 2017 and 2018.* www.iotcentral.io/blog/gartner-identifies-the-top-10-internet-of-things-technologies-for

[11] Pipara, Ankur: *Internet of things (IoT).* www.slideshare.net/AnkurPipara/internet-of-things-iot-2014

[12] Sahoo, Rashmi: *List of sensors.* http://forum.electronicsforu.com/forum/technologies-work/components/sensors-actuators/699-list-of-sensors

IoT in Practice, in the Focus of Information Security, part I. Operation of IoT, Tendencies of Development

KOLLÁR CSABA

The dynamic expansion of IoT in civil life can be led back to four areas of digital technologies. These are as follows: declining prices of sensors, increasing internet penetration, expansion of data warehousing, simplification of data organisation, as well as the development of data analysis and data mining due to mechanized learning, artificial intelligence and use of algorithms. Besides the development areas of digital age the present theoretical study focuses on the relation of IoT and information security. After introducing how IoT works, the security aspects of the area and the main changes regarding IoT are discussed in the study.

Keywords: digital age, information security, IoT, trends