Az IoT-rendszerek, ezen belül az IoB-szenzorok, katonai alkalmazhatóságának és adattovábbításának egyes sebezhetőségei

DOI https://doi.org/10.29068/HO.2025.1-2.32-45

Szerzők **Surányi Zsolt Mihály őrnagy,** MH Egészségügyi Központ, a Nemzeti Közszolgálati Egyetem, Katonai Műszaki Doktori Iskola doktorandusza (ORCID: 0009-0001-8707-2765, MTMT: 10090221)
Knapp Gábor alezredes, Katonai Nemzetbiztonsági Szolgálat, a Nemzeti Közszolgálati Egyetem, Katonai Műszaki Doktori Iskola doktorandusza (ORCID: 0009-0001-0702-756X, MTMT: 10090220)

Kulcsszavak *IoB, IoT, sebezhetőség, digitális katona*

Absztrakt Napjainkban az IoT-rendszerek[1] térnyerésére alapozva egyre nagyobb igény mutatkozik a testünkbe ültethető eszközök vagy a testen elhelyezett szenzorok alkalmazására. Az ezen szenzorokból származó információk, az általuk továbbított adatok alkotják az IoB-t.[2] A valós idejű (real-time) adatgyűjtés, a nem helyben történő adatfeldolgozáshoz szükséges adatátvitel, az adatok feldolgozást követő, aggregált tárolása magában hordozza a sebezhetőség lehetőségét, hiszen szenzitív adatok kezeléséről kell beszélnünk. A cikk a szenzorok és adattároló – akár felhő alapú – képességek közötti lehetséges átviteli csatornák közül csak a kezdeti, nyers adatok átvitelét biztosító egyes megoldások fenyegetéseit vizsgálja.

AZ IOT-RENDSZEREK ÉS IOB-SZENZOROK KATONAI TÉRNYERÉSÉNEK LÉPCSŐFOKAI

A szenzorok által generált adatok kezdeti és teljes körű feldolgozása komoly kihívást jelent a gyűjtési pontokon lévő korlátozott számítási kapacitás miatt. A katonai alkalmazás során a rendszereknek képesnek kell lenniük nemcsak az egyes katonák fiziológiai állapotának önálló monitorozására, hanem a harctéri egységek és magasabb szintű alakulatok kollektív állapotjellemzőinek érté-

1 Internet of Things (IoT): a dolgok hálózata.
2 Internet of Bodies (IoB): a testek hálózata.

kelésére is. Az ehhez szükséges adatok kezelése és feldolgozása megfelelő védelmi intézkedések nélkül rendkívül magas kockázatot hordoz.

Az adatgyűjtés két fő módon valósulhat meg. Az online adatgyűjtés során – amely tipikus a sürgősségi ellátásban – fizikai felmérések vagy a harctéri állapot nyomon követése esetében a szenzoradatokat valós időben továbbítják és azok azonnali előzetes értékelésen esnek át. Ezzel szemben az offline adatgyűjtés esetében az adatok feldolgozása nem azonnali, hanem periodikus, például havi rendszerességgel történik. Az offline adatgyűjtés során a felhalmozott adatok aggregálása nagyobb fenyegetést jelenthet az adatok biztonságára nézve, mint a részletek külön-külön történő kezelése.

Az IoB-technológiában alkalmazott M2M kommunikáció[3]kiküszöböli az emberi beavatkozás szükségességét. Az automatizáció eredményeként a folyamatok felgyorsulnak, a manuális hibák kockázata pedig csökken. Az IoT-eszközökben elterjedt technológiai megoldások, mint az RFID,[4] NFC[5] vagy BTLE,[6] széles körű összeköttetést és adatátvitelt tesznek lehetővé. Egyes gyártók azonban egyedi, nem kompatibilis megoldásokat fejlesztenek, ami bár potenciálisan csökkentheti a fenyegetettségeket, egyben nagyobb erőforrásokat igényel a támogatás és a karbantartás fenntartásához.

RFID

Az RFID, és így az IoB, alkalmazási körébe tartozik a betegek nyomon követése, ellenőrzése, az alkalmazott berendezések és eszközök nyomon követése, valamint az érzékelőből származó adatok gyűjtése. „Ez a betegek számára az egészségügyi ellátás minőségének javítását jelenti a betegek és az egészségügyi személyzet közötti interakciók során elkövetett emberi hibák csökkentése révén."[7] Az RFID-technológia a kórházakban, főként a magas költségek és a beruházás indokoltságának nehézségei miatt, eddig nem nagyon terjedt el.

A technológia alkalmazása során veszélyt jelent az elektromágneses interferencia – például pacemakerrel rendelkező páciensek esetében –, így alkalmazása általánosságban megvalósítható, de csak kivételekkel. Emellett a jelen cikkben vizsgált információbiztonság, illetve az

3 Machine to Machine (M2M): gép és gép közötti, automatizált információátadási eljárás.

4 Radio Frequency Identification (RFID): automatikus azonosításhoz és adatközléshez használt technológia, melynek lényege adatok tárolása és továbbítása RFID-címkék és eszközök segítségével.

5 Near Field Communication (NFC): az RFID egy változata, ami egy rövid hatótávú kommunikációs szabványgyűjtemény okostelefonok és hasonló (általában mobil) eszközök közötti, egymáshoz érintéssel vagy egymáshoz nagyon közel helyezéssel (maximum néhány centiméter) létrejövő rádiófrekvenciás kommunikációja.

6 Bluetooth LE, BLE, korábbi nevén Bluetooth Smart (BTLE): olyan vezeték nélküli személyi hálózati technológia, amely az egészségügy, a fitnesz, a jeladók, a biztonsági és az otthoni szórakoztatóipar újszerű alkalmazásait célozza. A klasszikus Bluetooth-hoz képest a Bluetooth Low Energy célja, hogy jelentősen csökkentett energiafogyasztást és költséget biztosítson, hasonló kommunikációs hatótávolság fenntartása mellett.

7 Https://copperdigital.com/blog/all-about-rfid-solutions-technology-in-medical-industry.

adatvédelem oldaláról is felmerülnek kérdések. Az RFID-címkéken található érzékeny, titkosítatlan adatok meghamisítása, az adatátvitel közbeni lehallgatás vagy az érzékeny adatokhoz való jogosulatlan hozzáférés biztonsági problémákat jelentenek, amelyeket kezelni kell vagy elfogadni. Az RFID-címkék vezeték nélküli interfészei fizikai támadásoknak is ki lehetnek téve, illetve az adatátvitelnél a lehallgatás központi kérdése merül fel sebezhetőségként.

NFC

Az RFID egyik speciális változataként is emlegetett NFC kizárólag a közeli adatátvitelre korlátozódik. Az RFID-hoz hasonlóan az átvitelhez nem szükséges saját külön áramforrás, azt a vevő egységből generálja le az áramkör. Az NFC-technológiát Thomas Edison fejlesztette ki egy rádiófrekvenciás kísérlet során az 1800-as évek végén, melyet Charles Walton szabadalmaztatott 1983-ban. Lényegében egy érintésmentes kommunikációs technológia, amely a 13,56 MHz-es frekvenciatartományban működik.[8] Ezen technológia része az NFC-adatcsere-formátum (NDEF),[9] ahol a formázott adatok tarolása NFC-címkéken valósul meg, majd peer-to-peer (P2P)[10] kapcsolaton keresztül továbbítják azokat.

Az orvosbiológiai alkalmazásokban a leggyakrabban használt információtípusok a hőmérséklet és a nyomás, amelyek méréséhez az NFC egy kiváló megoldást biztosíthat kis helyigénye, illetve a jelzett áramforrásmentes alkalmazása miatt. Ugyanakkor az egészségügyi alkalmazás során is felmerül az NFC NDEF formátumának biztonsági problémája, amelyet szükséges kezelni.

„A harcmezőn megjelenő – tableteken kezelhető – digitális egészségügyi alkalmazások használata nem csupán fikció manapság. A 2023 októberében kirobbant gázai konfliktusban már bizonyítottan használja az IDF egészségügyi hadteste[11] ezen innovatív alkalmazást, amelynek célja, hogy forradalmasítsa a sérült katonákról szóló orvosi információk megosztását a csatatérről az egészségügyi ellátást végző kórházak irányába. Az új alkalmazás tavaly novemberi bevezetése kiváltotta az eddig megszokott, az első ellátó által kézzel kitöltött űrlapokat és dokumentációkat. A terepen dolgozó egészségügyi személyzet által használt táblagépekre telepített alkalmazás lehetővé teszi a sérült egészségi állapotának és a megkezdett ellátás (kimentés, akut sürgősségi beavatkozás) tényének digitális rögzítését. Ezeket a létfontosságú adatokat azután NFC-kártyákon keresztül zökkenőmentesen továbbítják a sérült kiürítését végzőknek, majd a további ellátást végrehajtó egészségügyi intézmény irányába. Így biztosítva, hogy részletes és pontos egészségügyi információk kísérjék végig a

8 Kang, Sung-Gu és mások: *Near-Field Communication in Biomedical Applications*.

9 NFC Data Exchange Format.

10 Egyenrangú hálózati architektúra, az informatikai végpontok közvetlenül egymással kommunikálnak, dedikált szerver(ek) nélkül.

11 Israel Defense Forces Medical Corps: az Izraeli Védelmi Erők egészségügyi hadteste.

sérült katonát az evakuálási folyamat során. Ez a digitális megoldás nemcsak a létfontosságú egészségügyi adatok átvitelét egyszerűsíti, hanem elősegíti a sérültek állapotváltozása miatt megkövetelt folyamatos osztályozást is, ezzel is növelve az ellátás hatékonyságát."[12]

Bluetooth

A Bluetooth egy master-slave alapú vezetéknélküli (IEEE[13] 802.15.1) ipari szabvány, amelyet az 1990-es években rádiófrekvenciás adatátvitelre fejlesztettek ki. A szabvány feladata az alacsony teljesítményű rádióhullámok segítségével történő információs tevékenységek támogatása volt. Ezzel az új eljárással szerették volna kiváltani az 1960-as évek óta alkalmazott RS-232 vezetékes soros port szabványt, a 2,4 és 2,485 GHz közötti UHF-rádiófrekvenciatartományban.[14] A cél a két vagy több eszközt összekötő kábelcsatlakozások kiváltása volt. Továbbá olyan összeköttetést szerettek volna megalkotni, amely megszünteti a vezetékek helyhez kötöttsége általi korlátozást és ezzel párhuzamosan megfelelő sebességű adatátvitelt biztosít. Bár ez nagyon hasonló frekvenciákat foglal el, mint a WiFi,[15] a Bluetootht mindig is sokkal rövidebb hatótávolságú és alacsonyabb fogyasztású alternatívaként tervezték és szánták. A Bluetoothtechnológia fejlődését az átviteli sebesség és átviteli távolságok növekedésével mutatja be az *1. ábra*.

Annak érdekében, hogy a különböző gyártók készülékei között létrejöjjön a megfelelő interoperabilitás és kompatibilitás, a Bluetootht saját protokollkészlettel látták el. A működési sáv 79 darab 1 MHz sávszélességű csatornára osztódik 2,402 GHz és 2,480 GHz között. A Bluetooth frekvenciaugratásos spektrumkiterjesztést (FHSS)[16] alkalmaz a kommunikációja során, ezzel is elkerülve az interferenciát az ISM-frekvenciatartományban[17] üzemelő további eszközökkel. A széles frekvenciaspektrum, illetve az előre meghatározott protokoll a védelmi és együttműködési feladatok mellett a támadó felek részére biztosítja a támadási vektorok megismerési – és ezáltal hatékony támadási – lehetőségét is.

A Bluetoothszabvány fejlesztése a 4.0 verziónál kettévált, így jött létre a Classic és a Low Energy. A Classic továbbra is nagyobb adatátviteli sebességet biztosít az állandó kapcsolatot igénylő eszközökhöz

12 Surányi Zsolt Mihály; Ollári Viktor Szilárd: *A medikai rendszer használatának infokommunikációs lehetőségei az első ellátás helyszínén.*

13 Institute of Electrical and Electronics Engineers (IEEE): napjaink legnagyobb elektronikai fejlesztéssel és szabványosítással foglalkozó szervezete.

14 Ultra High Frequency (UHF): ultrarövid hullám, 300 MHz és 3 GHz közti frekvenciasáv.

15 Wireless Fidelity (WiFi): vezeték nélküli mikrohullámú kommunikációt megvalósító szabvány (IEEE 802.11).

16 Frequency Hopping Spread Spectrum (FHSS).

17 Industrial, Scientific, and Medical (ISM): ipari, tudományos és egészségügyi célra fenntartott, nem engedélyköteles frekvenciatartomány.

A szabvány neve (a bevezetés éve)	Adatátviteli sebesség	Maximális átviteli távolság (méter)	Főbb új funkciók (az angol megnevezés)
Bluetooth 1.0 (1999)	0,7 Mbps	~10 m	–
Bluetooth 2.0 (2004)	1 Mbps core 3 Mbps EDR	~30 m	Fokozott adatátviteli sebesség (Enhanced Data Rate, EDR)*
			Egyszerű biztonsági párosítás (Secure Simple Pairing) (BT 2.1)
Bluetooth 3.0 (2009)	3 Mbps EDR (24 Mbps over HS 802.11 link)	~30m	Nagy sebesség (High Speed, HS)
			Továbbfejlesztett módok (Enhanced Modes) (L2CAP)
			Továbbfejlesztett teljesítményszabályozás (Enhanced Power Control)
Bluetooth 4.0 (2013)	3 Mbps EDR 1 Mbps alacsony energiával (Low Energy)	~60 m	Alacsony energia (Low Energy) (BLE)
			Alapspecifikáció-kiegészítések 1–4 (Core Specification Addenda 1–4) (BT 4.1)
			IoT-funkciók (IoT features) (BT 4.2)
Bluetooth 5 (2017)	3 Mbps EDR 2 Mbps alacsony energiával (Low Energy)	~240 m	Rés elfedésének lehetősége (Slot Available Masking) (SAM)
			Nagy hatótávolság, alacsony energiával (LE Long Range)
			Alapspecifikáció-kiegészítések 6 (Core Specification Addenda 6) (BT 5.1)
			Alacsony energiájú hangátvitel (LE Audio) (BT 5.2)

* Enhanced Data Rate (EDR): továbbfejlesztett/megnövelt adatátvitel-sebesség.

1. ábra. *A Bluetoothtechnológia fejlődése*
(Triggs, Robert; Wankhede, Calvin: *A little history of Bluetooth.)*

(pl. vezeték nélküli fejhallgató), míg a BLE[18] sorozatszerű kommunikációra lett optimalizálva. Lényege az alacsony energiafogyasztáson alapuló, vezetéknélküli adatátvitel, mely magas rendelkezésre álló idővel párosul.

Internet of Bodies (IoB)

Napjainkban az IoB-t folyamatosan és egyre növekvő arányban alkalmazzák – rendkívül innovatív módon – az emberi életminőség javításának érdekében. Az IoB az internet olyan részhalmaza, melyben a különböző eszközök kötik az emberi testet a hálózathoz. Régebbi megnevezése a BAN[19] volt, melynek az alapja a centrális (pl. okoseszköz) és perifériás eszközök (szenzorok) közötti vezetéknélküli kapcsolat és összeköttetés.

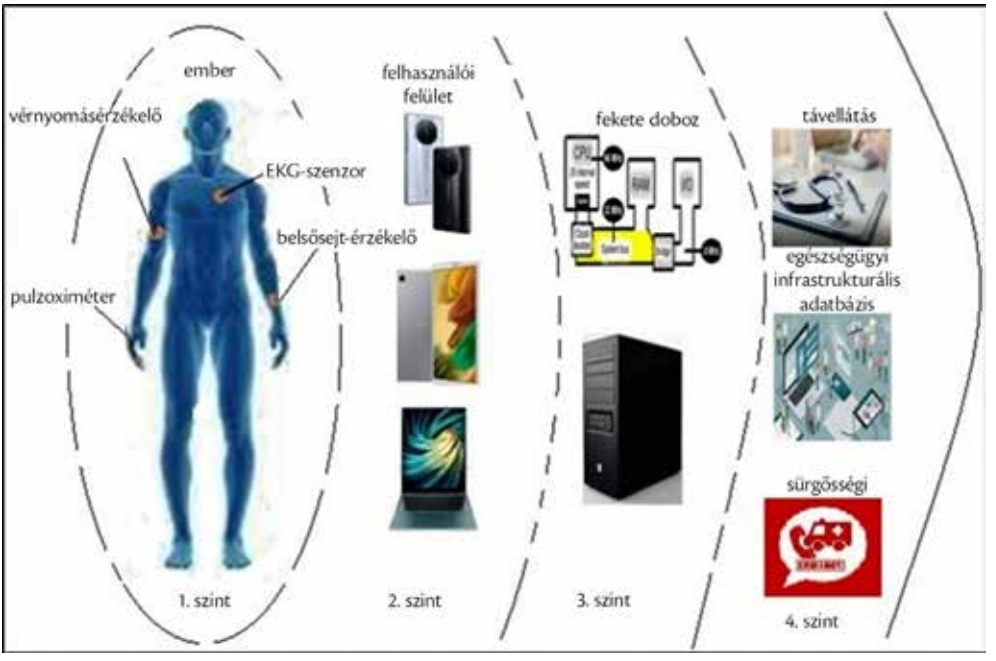
18 Bluetooth Low Energy (BLE)/Bluetooth Smart.

19 Body Area Network (BAN): testközeli hálózat. Alapja a centrális és perifériás eszközök közötti kapcsolat és összeköttetés.

Kritériumok	Low Energy (LE)	Classic
Csatornák száma	40 csatorna (3 hirdető, 37 adatátviteli) 2,4 MHz ISM	79 csatorna 1 MHz térközzel
Adatátviteli sebesség	BLE 5: 2 Mbps BLE 4.2: 1 Mbps BLE 5 nagy távolságú (S=2): 500 Mbps BLE 5 nagy távolságú (S=8): 125 Mbps	EDR (8DPSK): 3 Mbps EDR (π/4 DQPSK): 2 Mbps Alap adatátviteli sebesség: 1 Mbps
Teljesítmény- és rádióprofilok	Profil 1: 100 mW (+20 dBm) Profil 1.5: 10 mW (+10 dbm) Profil 2: 2,5 mW (+4 dBm) Profil 3: 1 mW (0 dBm)	Profil 1: 100 mW (+20 dBm) Profil 2: 2,5 mW (+4 dBm) Profil 3: 1 mW (0 dBm)
Energiafelhasználás	~0,01×-től 0,5×-ig	Rádióosztály alapján
Hálózati topológiák	Ponttól pontig (beleértve a piconetet is) Adás Hálózat	Ponttól pontig (beleértve a piconetet is)

2. ábra. *Technológiai különbségek a Bluetooth LE és Classic között (*Triggs, Robert; Wankhede, Calvin: *A little history of Bluetooth.)*

Ezen eszközök lehetnek beültetett implantátumok, testhez csatlakoztatott szenzorok vagy lenyelt kapszulák is. Az alkalmazott technológia a felhasználási időszaktól (ideiglenes vagy állandó), helyszíntől, illetve a felügyelt katonai szervezet nagyságától (egyes harcos vagy akár magasabb harci egység) függ. Ezen eszközök vizsgálják az emberi test egyes funkcióinak működését, majd az összegyűjtött adatokat továbbítják monitorozás vagy elemzés céljából.



3. ábra. *A vezetéknélküli IoB- (BAN) hálózat elvi felépítése szintenként (forrás: https://www.researchgate.net/figure/General-architecture-of-healthcare-monitoring_fig2_363896736)*

A technológia továbbra is létfontosságú szerepet tölt be a végleges gyógymódok keresése, valamint a beteg állapotának javítására történő törekvések terén. Az elmúlt évszázad során a technológiai fejlődés forradalmasította az egészségügyi ellátást. Olyan áttörések jelentek meg, mint az őssejtkutatás, a génterápia, a biotechnológia, a regeneratív gyógyászat, az immunterápia, a digitális terápia, a nanoterápia és a telemedicina. Az orvostudomány fellendülésére kétségkívül jelentős hatással van az ipari fejlődés. Napjaink legújabb vívmányai, mint a mesterséges intelligencia (MI),[20] a 3D-nyomtatás (bioprinting), a kibővített és a virtuális valóság, valamint az IoT bejutnak a mainstream[21] egészségügyi ellátásba

A beépített szenzorok által kinyert adatokat fel is kell dolgozni. A feldolgozás történhet helyben, például egy vércukormérő szenzorhoz kapcsolt mobiltelefonon vagy céleszközön való megjelenítéssel,[22] vagy akár az adatok továbbításával, amely során a fentebb említett hálózati kapcsolatok további alkalmazására van szükség. További kapcsolat lehet az adatgyűjtők tárhellyel vagy akár központi adatbázissal való szinkronizációja, amely során az adatok megfelelő védelme érdekében már az informatikai biztonság különböző sebezhetőségeit kell kezelni. A cikk ezen hálózati végpontok közötti adatátviteli problémákra és azok kezelésére nem tér ki.

Kiberbiztonság az IoB esetében

Technológiai értelemben az ember egészségi állapotát monitorozó, felügyelő hálózatok még nem veszélytelenek, hisz adatvédelmi, vagy átfogó jogi környezeti, szempontból még nem tökéletesítettek. A Nemzetközi Orvosi Eszközszabályozók Fóruma[23] által 2020-ban rendezett munkacsoport egyeztetésén, melynek témája az orvosi eszközök kiberbiztonsági kitettsége volt, az alábbi iránymutatást tette: „Az egészségügyi ágazatban érdekelt felek közös felelősséggel tartoznak az orvostechnikai eszközökkel kapcsolatban a kiberbiztonság növelésében. Minden érdekelt fél részére segítséget kell nyújtani a téma jobb megértésében, hisz nekik van szerepük a proaktív kiberbiztonság támogatásában, amely segít megvédeni és biztonságossá tenni az orvosi eszközöket a jövőbeli támadásokkal szemben és a lehetséges problémák vagy események előrejelzésében."[24]

A kiberbiztonságot az alábbiak szerint határozza meg az ISO:[25] „Olyan állapot, ahol az információk és rendszerek olyan mértékben védettek a különféle jogosulatlan tevékenységektől, mint a hozzáférés, felhasználás, nyilvánosságra hozatal, megzavarás, módosítás vagy megsemmisítés, hogy a kockázatok, a bizalmasság, a sértetlenség és a rendel-

20 Artificial Intelligence (AI): mesterséges intelligencia.

21 Mainstream: fősodor. A célközönség és a szakértők többsége által elfogadott és támogatott irányzat.

22 Hevesi Judit; Haig Zsolt: *A folyamatos glükózmonitorozó rendszer katonai környezetben való alkalmazhatósága és sebezhetősége.*

23 International Medical Device Regulators Forum (IMDRF): Nemzetközi Orvosi Eszközszabályozók Fóruma.

24 International Medical Device Regulators Forum: *Principles and Practices for Medical Device Cybersecurity.*

25 International Organization for Standardization (ISO): Nemzetközi Szabványügyi Szervezet.

kezésre állás megsértésével kapcsolatos kockázatok az életciklus során elfogadható szinten maradjanak."[26]

Az orvostechnikai eszközöket veszélyeztető kiberbiztonsági fenyegetések egyik kiinduló forrása az lehet, hogy a kezelés, az orvosi felügyelet időszakában alkalmazott eszköz átesett-e a megfelelő kezdeti teszteléseken, illetve, hogy megoldható-e a később felmerülő fenyegetések esetén az alkalmazott eszközökhöz való nem csak fogadó oldali hozzáférés, beavatkozás akár hardveres, akár szoftveres oldalról. Nem szabad megfelejtkezni arról sem, hogy az információbiztonsági szempontú megközelítés mellett felmerülhet a páciensek emberi létének tiszteletben tartása, napi életüknek a lehető legkisebb mértékű befolyásolása. Természetesen amennyiben az intézkedések meghozatala nélkül az érintettek élete is veszélybe kerül, akkor a beavatkozás prioritást kell, hogy élvezzen, mint minden egészségüggyel összefüggő orvosi beavatkozás során.

A digitális katona (DIKA) koncepciójában megjelenő szenzortechnológia

A technológia jól kapcsolódhat a digitális katona koncepciójához, amelynek egyik fontos eleme a katona fiziológiai/egészségi állapotának valós idejű, folyamatos monitorozása. A katonán elhelyezhető különböző szenzorok ma már alkalmasak többek között a légzés, a szívműködés, a vérnyomás, a testhőmérséklet, az alvás-ébrenléti ciklus stb. megfigyelésére. A mért paraméterek alapján mind a katona, mind a parancsnok képet kaphatnak a katona állapotáról (pl. lehűlés, oxigénhiány, anyagcsereromlás, folyadékhiány, pszichés stressz, kialvatlanság stb.).

Ebbe a rendszerbe illeszthető és képességeit kiterjesztheti a CGMS,[27] amivel akár az egészséges katona vércukorszint-ingadozása is nyomon követhető. Normál szénhidrátanyagcsere-állapot esetén a vércukorszint általában stabil marad, de bizonyos esetekben, mint például tartós éhezésnél, extrém fizikai megterhelés vagy érzelmi stressz hatására, esetleg súlyos fertőző betegség fennállásakor, kórosan alacsony vagy magas vércukorértékek is előfordulhatnak. Ebben az esetben a szenzortechnika alkalmas lehet a teljesítmény optimalizálására, valamint változó tápanyag-összetételű ételeknek, illetve a fizikai aktivitást jellemző minőségi és mennyiségi paramétereknek a vércukorszintet befolyásoló egyéni hatásainak elemzésére is. A félig invazív technológia azonban magában hordozza a fertőzés veszélyét, mely szélsőséges környezeti helyzetben fokozottabb. Ebből a szempontból előnyösebbek lennének a még fejlesztés alatt álló, nem invazív vércukormérési eljárások, mint pl. a spektroszkópia, bioimpedancia, optikai koherencia tomográfia stb., amelyek során a vércukor-koncentráció meghatározása nem vérmintából történik. Katonai környezetben emellett fokozottabban kell számolni a CGMS elleni szándékos fenyegetésekkel, különösen a szenzort használó katonai vezetők körében.

A CGMS mint példa alapján úgy véljük, hogy minden, a katonai állomány aktuális, nem csak az orvosi vizsgálatok

26 ISO 81001-1: https://www.iso.org/obp/ui/en/#iso:std:iso:81001:-1:ed-1:v1:en.

27 Continuous Glucose Monitor Sensor (CGMS): folyamatos visszajelzésű vércukorszint-ellenőrző szenzor.

4. ábra. *Afganisztán Helmand tartományában 2018-ban települő katonai bázisnak a Strava fitneszalkalmazásban rögzített adatok alapján kirajzolt útvonalainak hőtérképe (forrás: https://www.theguardian.com/world/2018/jan/28/fitness-tracking-app-gives-away-location-of-secret-us-army-bases)*

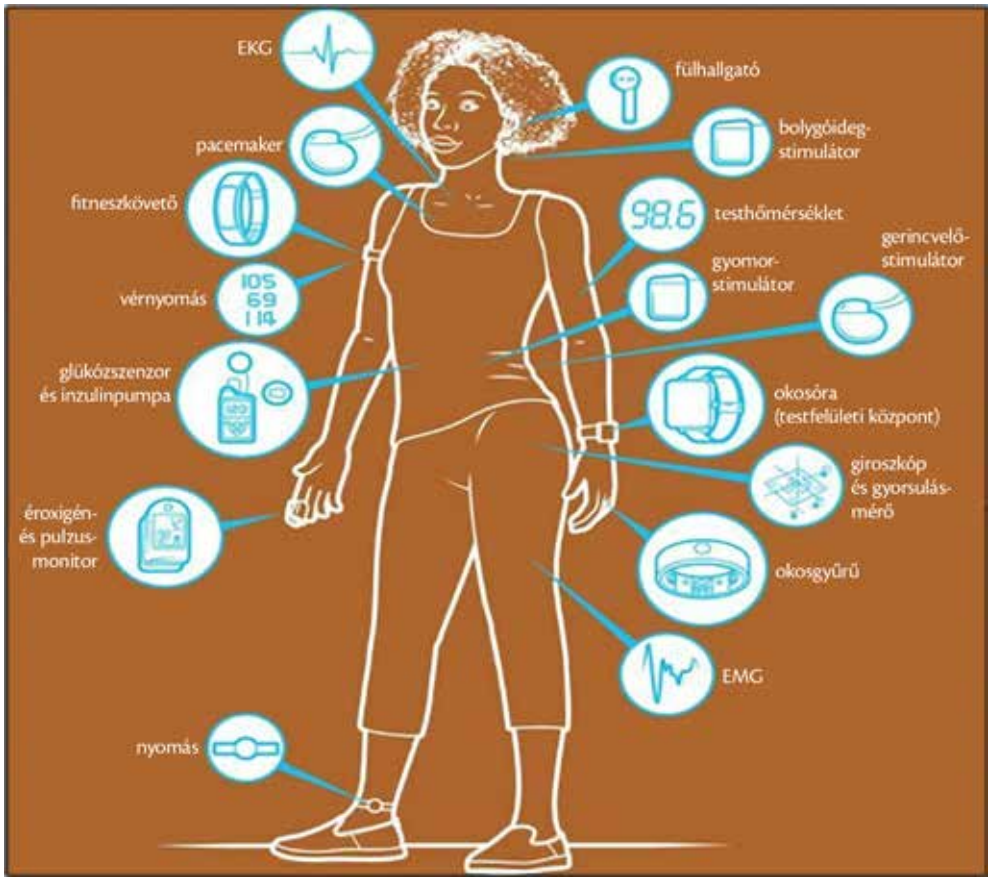
során felmért és megállapított egészségügyi állapotára vonatkozó információ, potenciális célpont lehet a támadók részéről. Amennyiben az (egyéni) egészségügyi állapot felmérése olyan megoldásokon keresztül történik, amelyeknek alkalmazása nem kellően körültekintő biztonsági megoldásokhoz van kötve, az biztonsági problémákat is eredményezhet. A Guardian cikke[28] alapján, ha nem is közvetlenül a szenzorokból származó adatok, és nem is a közvetlen személyek, de egyes fitneszapplikációk a cikkben megjelentek alapján adatokat szolgáltathatnak a vezetők helyzetéről, amelyet a *4. ábra* mutat be. Mivel ezen applikációk a helyzet mellett egészségügyi adatokat is tárolhatnak, nem megfelelő konfigurálásuk esetén illetéktelenek is hozzáférhetnek az edzettségre utaló és így – elemző-értékelő eljárásokat követve – akár az egészségügyi állapotra vonatkozó adatokhoz is.

A Bluetoothtechnológia sebezhetősége

Kijelenthetjük, hogy napjainkra a Bluetoothtechnológia mindennapi életünk részévé vált, mely a különböző infokommunikációs eszközök közötti zökkenőmentes és vezetéknélküli kapcsolatot teremti meg. Bármennyire elterjedt is a használata, számos sebezhetőségi pont húzódik meg mögötte, melyek láthatatlan, de valós kockázatot jelentenek a felhasználók számára. Mosolygó szerint:

„Minden fejlesztőcsapat törekszik a lehető legnagyobb minőség, és biztonság elérésére, ennek ellenére azonban, gyakran előfordul, hogy kisebb-nagyobb hibák keletkeznek. Ezek észlelése és javítása azonban, csak az első lépések a hiba eltüntetésében, ugyanis a felhasználókat, legyenek azok más fejlesztők, vagy végfelhasználók, értesíteni kell arról, hogy szükséges lehet az újabb verzióra frissíteniük. A különböző projektekben alkalmazott rutinok eltérése miatt az ilyen tájékoztatás egy rendkívül komoly kihívás. A célból, hogy az információ megosztása könnyebb legyen a Mitre Vállalat 1999-ben létrehozta a CVE (Common

28 Https://www.theguardian.com/lifeandstyle/2024/oct/29/strava-problem-fitness-app-locate-worlds-most-powerful-people.



5. ábra. *A testünk akár egy okos otthon. (Chris Philpot illusztrációja) (forrás: https://read.nxtbook.com/ieee/spectrum/spectrum_na_december_20 20/assets/9b9856dce4358b35109df1dbc66fb124.jpg)*

Vulnerabilities and Exposures)[29] koncepciót, aminek lényege egy publikus adatbázis készítése volt, ahol egységes nevezési konvenciók segítségével könnyítették a sérülékenységekkel, és azok javításával kapcsolatos adatok rendszerezését. Egy CVE egy konkrét projekt sérülékenységét írja le, és rendel hozzá egy egyedi azonosítót, míg egy CWE (Common Weakness Enumeration)[30] sérülékenységek egy csoportját jelöli. Habár az adatbázis rengeteg hasznos információt tartalmaz, mint például bizonyos hibák leírása, súlyossága és rövid leírása, nem ad minden kérdésre választ."[31]

29 Common Vulnerabilities and Exposures (CVE): gyakori sebezhetőségek és kitettségek. Https://cve.mitre.org.

30 Common Weakness Enumeration (CWE): gyakori gyengeségek felsorolása. https://cwe.mitre.org.

31 Mosolygó Balázs József: *Biztonsági sérülékenységek javításának empirikus vizsgálata és az ehhez szükséges eszközök fejlesztése.*

A sérülékenység fenyegetettségi szintjét a CVSS-számmal[32] értékelik és adják meg.

A teljesség igénye nélkül az alábbiakban olyan technikai támadási formákat sorolunk fel, amelyek informatikai kitettségük miatt véleményünk szerint kihasználhatók lehetnek az IoB-technológiák esetén:

1. Bluesnarfing

A bluesnarfing során a támadó egy eszköz Bluetoothkapcsolatának biztonsági réseit használja ki, hogy hozzáférjen az eszközhöz és bizalmas információkat lopjon el. A bluesnarfing során kihasznált sebezhetőség a Bluetooth Object Exchange (OBEX) protokolljához kapcsolódik. A Bluetoothképes eszközök ezt a protokollt használják a kommunikációhoz. A bluesnarfing támadások csak akkor működnek, ha az eszköz Bluetoothfunkciója be van kapcsolva, és „észlelhető" értékre van állítva. Így a hatótávolságon belüli többi eszköz párosítható, és a támadó hozzáférhet az eszközhöz. Miután a támadó hozzáférést szerez az eszközhöz (többnyire egy okostelefonhoz), hozzáférhet olyan adatokhoz, mint a fényképek, névjegyek, e-mailek és jelszavak.[33]

2. Bluejacking

A bluejacking egy egyszerűbb, potenciálisan kevésbé káros kibertámadás (ha egyáltalán nevezhetjük annak). A bluejacking során egy támadó kéretlen üzeneteket küld az áldozat Bluetoothképes eszközére.

A kiberbűnözők általában akár 9 méter távolságból is ellophatnak egy eszközt, miközben fizikailag távol vannak a címzettől, kihasználva a Bluetooth üzenetküldési lehetőségeiben található kiskaput. Ha laptopról van szó, ez a 9 méteres távolság körülbelül tízszeresére, akár 100 méterre is megnőhet. A bluejacking során a célpont kéretlen üzeneteket, névjegykártyákat vagy képeket kap a feladótól.

3. BIAS[34]

Úgynevezett MITM,[35] vagyis közbeékelődéses támadási fajta. Lényege, hogy a támadó egy másik eszközt megszemélyesítve, a küldő és fogadó eszköz közé beépülve, az adatfolyamot átjátszva, hoz létre kapcsolatot. A hitelesítési folyamatot veszi célba, megkerülve a Bluetooth azonosítási mechanizmusát.

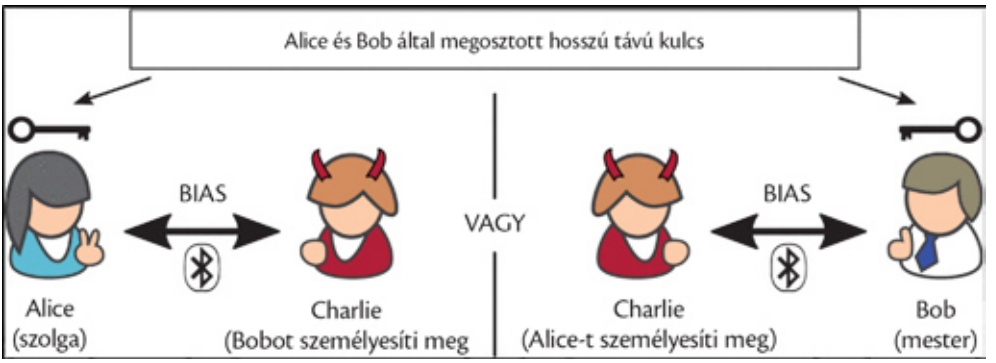
A *6. ábrán* látható a Bluetooth-os megszemélyesítési támadás áttekintése. Alice és Bob, az áldozatok, egy hosszú távú kulcsot osztanak meg, amely a támadó számára ismeretlen. A támadó (Charlie) célja, hogy „biztonságos kapcsolatot" létesítsen Bobbal, miközben Alice-t személyesíti meg, vagy Aliceszel, miközben Bobot személyesíti meg. Mivel Alice-nek és Bobnak különböző Bluetoothszerepkörei vannak, a támadó nem használhatja ugyanazt a megszemélyesítési támadást mindkettőjük ellen. Feltételezzük, hogy Alice és Bob már megosztanak egy hosszú távú kulcsot, az úgynevezett kapcsolati kulcsot. A kulcsot a Bluetooth biztonságos egyszerű párosításának befejezésével (vagy hagyományos biztonságos kapcsolatok, vagy biztonságos kapcsolatok haszná-

32 Common Vulnerability Scoring System (CVSS): általános sebezhetőségi pontozási rendszer.

33 Https://www.spiceworks.com/it-security/endpoint-security/articles/bluesnarfing-vs-bluejacking.

34 Bluetooth Impersonation AttackS (BIAS): Bluetooth megszemélyesítési támadás.

35 Man in the Middle (MITM): emberközpontú.



6. ábra. *A BIAS elméleti ábrázolása (forrás: https://ieeexplore.ieee.org/document/9152758)*

latával), valamint egy erős asszociációs modell (például jelszó megadása) használatával egyeztették.[36]

4. KNOB[37]

A Bluetooth specifikációja tartalmaz egy titkosítási kulcsot a végpontok közötti azonosítási protokollhoz, amely lehetővé teszi a titkosítási kulcsok 1 bájt entrópiájú egyeztetését anélkül, hogy megvédené a szinkronizációs folyamat integritását. A távoli támadó manipulálhatja az entrópia-egyeztetést, és lehetővé teheti bármely szabványos Bluetooth-eszköz számára, hogy valós időben kényszerítse ki az entrópiájú kulcsok használatának csökkentését vagy mellőzését. Az alacsony entrópiájú kulcsot könnyebb feltörni, hisz a kulcs lekicsinyítése segít a támadóknak a titkosítás gyorsabb és erőszakosabb kikényszerítésében, ezáltal a továbbított adatok megszerezhetővé válnak.[38]

ÖSSZEFOGLALÁS

Az IoB-eszközök gyártói a kiberbiztonság érdekében saját programozási nyelvek használatával, illetve a kapcsolatok szabványalapon, de biztonsági célokat teljesítő formában tudnak védekezni. Amennyiben a külső kapcsolat felépítéséhez a cikkben jelzett protokollok segítségét veszik igénybe, kiemelt figyelmet kell fordítani a publikus fenyegetések nyomon követésére, azok mielőbbi javítására.

A kiberbiztonsági fenyegetések egyik gyűjtőhelye a MITRE-adatbázis, amely a CVE-program® küldetésével összhangban nyilvánosan közzétett kiberbiztonsági sebezhetőségek azonosítását, meghatározását és katalogizálását végzi. A feltárt sebezhetőségekre a gyártók közvetlenül vagy az adatbázis segítségével nyújthatnak javítási megoldásokat.

36 Antonioli, Daniele és mások: *BIAS: Bluetooth Impersonation Attacks.*

37 Key Negotiation of Bluetooth (KNOB): Bluetooth-azonosítókulcs egyeztetése.

38 Antonioli, Daniele és mások: *The KNOB is Broken: Exploiting Low Entropy in the Encryption Key Negotiation of Bluetooth BR/EDR.*

Felhasznált irodalom

Antonioli, Daniele és mások: *BIAS: Bluetooth Impersonation AttackS*. IEEE Xplore. Https://francozappa.github.io/about-bias/publication/antonioli-20-bias/antonioli-20-bias.pdf.

Antonioli, Daniele és mások: *The KNOB is Broken: Exploiting Low Entropy in the Encryption Key Negotiation of Bluetooth BR/EDR*. In: 28th Usenix Security Symposium (USENIX Security 19), 1047–1061. o.

Hevesi Judit; Haig Zsolt: *A folyamatos glükózmonitorozó rendszer katonai környezetben való alkalmazhatósága és sebezhetősége*. In: Hadtudományi Szemle, 2024/17, 85–102. o. DOI: 10.32563/hsz.2024.2.8.

Hodzic, Migdat; Muhic, Indira: *Internet of Things: Current Technological Review*. In: Periodicals of Engineering and Natural Sciences, 2014/2. DOI:10.21533/pen.v2i2.1.

International Medical Device Regulators Forum: *Principles and Practices for Medical Device Cybersecurity*. 2020. március 18. Https://www.imdrf.org/sites/default/files/docs/imdrf/final/technical/imdrf-tech-200318-pp-mdc-n60.pdf.

Kang, Sung-Gu és mások: *Near-Field Communication in Biomedical Applications*. Sensors (Basel), 2021. január 20. DOI: 10.3390/s21030703.

Mosolygó Balázs József: *Biztonsági sérülékenységek javításának empirikus vizsgálata és az ehhez szükséges eszközök fejlesztése*. BsC disszertáció, Szegedi Tudományegyetem Informatikai Intézet Szoftver-fejlesztés Tanszék. Https://www.crysys.hu/publications/files/setit/thesis_szte_Mosolygo21bsc.pdf.

Roland, Michael; Langer, Josef: *Digital Signature Records for the NFC Data Exchange Format*. 2010 Second International Workshop on Near Field Communication (2010. április 20), Institute of Electrical and Electronics Engineers. DOI: 10.1109/NFC.2010.10.

Surányi Zsolt Mihály; Ollári Viktor Szilárd: *A medikai rendszer használatának info-kommunikációs lehetőségei az első ellátás helyszínén*. In: Hadmérnök, 2024/19, 149–163. o. DOI: 10.32567/hm.2024.2.11.

Triggs, Robert; Wankhede, Calvin: *A little history of Bluetooth*. Androidauthority.com, 2023. szeptember 1. Https://www.androidauthority.com/history-bluetooth-explained-846345.

Zbrog, Matt: *The hottest medical technologies in 2024*. Https://www.medicaltechnologyschools.com/medical-lab-technician/top-new-health-technologies.

SOME VULNERABILITIES IN THE MILITARY APPLICABILITY AND DATA TRANSMISSION OF IOT SYSTEMS, INCLUDING IOB SENSORS

AUTHORS **Maj. Zsolt Mihály Surányi,** HDF Medical Centre
Lt. Col. Gábor Knapp, Military National Security Service

KEYWORDS *IoB, IoT, vulnerability, digital soldier*

ABSTRACT Today, with the rise of the importance of IoT systems, there is a growing need for devices or sensors to be implanted or placed in our bodies. The information from these sensors is now commonplace, and the data they transmit constitute the IoB (Internet of Bodies). However, the real-time collection of data, the transmission of data for off-site processing, and the aggregated storage of data after processing all carry the potential for vulnerabilities, as sensitive data are handled and transmitted in an unencrypted form. This article will only consider the threats posed by some of the possible transmission channels between sensors and data storage, including cloud-based capabilities, and the initial solutions that provide for the transmission of raw data.