Vránics Dávid Ferenc, Palik Mátyás, Bottyán Zsolt

ESETTANULMÁNY EGY NYÍLT REPÜLÉSTÁMOGATÓ RENDSZER BIZTONSÁGÁRÓL

Az Open Glider Network (OGN) nyílt, vitorlázó repülést támogató rendszer, mely egyre nagyobb népszerűségnek örvend világszerte. Az idő múlásával azonban az átviteli biztonság kialakítására tett intézkedései elavulttá váltak, jelenleg a hálózat felé küldött adatok egyszerű módszerekkel meghamisíthatóak. A cikk célja megmutatni, hogy egy nyilvános, nyílt repüléstámogató rendszer is lehet biztonságos. Javító szándékú kritikával, "fehér kalapban" vizsgálja a rendszer jelenlegi hibáit, és javaslatokkal szolgál azoknak javítására, a napjainkban elterjedt átviteli biztonsági eljárásoktól az adatok heurisztikus vizsgálatát megvalósító mesterséges intelligenciáig.

***Kulcsszavak**: repüléstámogatás, biztonság, esettanulmány*

AZ OGN RÖVIDEN

Az OGN[1] nyílt, vitorlázó repülést támogató rendszer, mely egyre nagyobb népszerűségnek örvend világszerte. Jelenleg több mint 10 000 fedélzeti jeladó eszköz [1] van regisztrálva a hálózatba, vitorlázó repülőgépektől kezdve, kisméretű légcsavaros repülőgépeken át pilóta nélküli légijárművekig. A rendszer kifejlesztésének célja az volt, hogy azokról a repülőgépekről, melyek nem rendelkeznek transzponderrel, közel valós idejű 3D-ós pozíció és alapvető telemetriai adatok legyenek elérhetők egy publikus web felületen. A vitorlázó repülő közösségtől eredő kezdeményezés, ma már széles körben elterjedt és az OGN hálózatból nyert adatok, akár bajba jutott légijárművek felkutatásakor is felhasználásra kerülhetnek.

Jelenleg egy kutatócsoporttal azon dolgozunk, hogy a fenti rendszert felhasználva, meteorológiai információt juttassunk el magába az OGN rendszerbe, illetve ezzel párhuzamosan, az OGN hálózat felhasználásával egy új repüléstámogatási rendszer numerikus prognosztikai alrendszerét is támogassuk ezzel az információval [2][3][4].

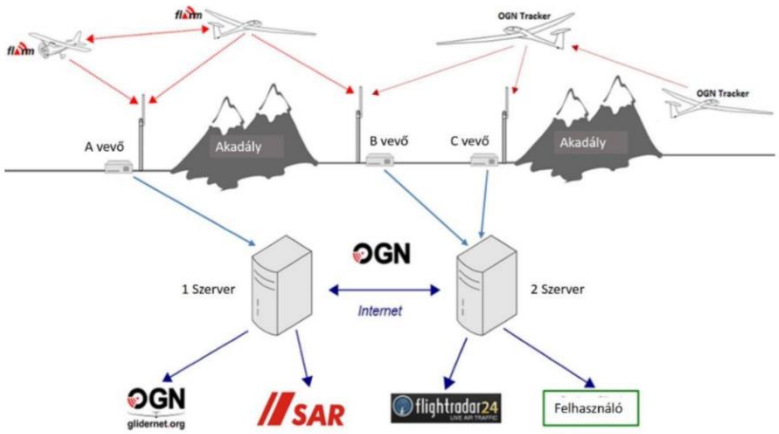
A hálózat [5] a FLARM[2] rendszerre épül. Utóbbinak alapvető célja a kisgépes repülés támogatása ütközés elkerülés lehetőségének megvalósításával. Az OGN ennek kiterjesztése, földi vevő állomások beiktatásával biztosítja interneten át a légijárművek „láthatóságát”, online térképes felületet biztosítva a biztonságosabb repülés tervezéséhez.

Az OGN hálózat felépítése

A repüléstámogató rendszereket légi, földi és adatkapcsolati alrendszerekre oszthatjuk. [6]

Az OGN és FLARM esetén a légi alrendszer alapeleme a tracker (nyomkövető egység), ami a pozíció és egyéb repülési adatok továbbítására képes. Ez általában egy kis méretű, kis energia igényű, 868 MHz-en üzemelő rádiós eszköz [5].

[1] Open Glider Network – Nyílt Vitorlázórepülő Hálózat
[2] Flight Alarm – „Légi Riasztó”



1. ábra FLARM és OGN TRACKER az OGN-hálózatban [5]

A kihelyezett földi vevőállomás a rádiós jeleket fogadja és dekódolja, majd ezeket APRS[3] csomagok formájában, interneten át továbbítja a központi szerverekre.

2. ábra Az „InfoPark” szoftveres vevő (balra) és a „PETRA-D” tracker (jobbra), a képet készítették a szerzők

A szerverekre különböző kliens alkalmazások iratkozhatnak fel és jeleníthetik meg tetszőleges formában az adatokat.

Az „OGN flavoured APRS” protokoll

Az APRS egy szöveges protokoll, eredetileg pozíció, időjárás adatok és egyéb szöveges közlemények rádió alapú digitális átvitelére lett tervezve.Az OGN rendszeren belüli kommunikáció egységesítésére különböző üzenetformátumok kerültek rögzítésre [7].

Köztük szerepelnek a szerverre történő bejelentkezéshez, a vevő azonosítására használt üzenetek, vagy éppen a vevő státuszát, technikai információit (földrajzi pozíció, rendelkezésre álló processzor és memória, hőmérséklet stb.) közlő üzenetek. Ezeken felül természetesen a közeli trackerektől vett pozíció, vagy időjárási adatok is APRS formában továbbításra kerülnek.

[3] Automatic Packet Reporting System – Automata Csomag Jelentő Rendszer

A sebezhető pontok

Gyenge hitelesítés

A jelszó valójában a felhasználónév (vevő azonosító) hasításával jön létre. [8] A vevő azonosítók maximum 10 alfanumerikus karakter hosszúak, a jelszó generáló algoritmus kis és nagybetűre nem érzékeny. Első lépésként maximum 10 karakter hosszúvá és nagybetűssé alakítjuk a vevő azonosítót. Ezután vesszük a 73e2 hexadecimális kezdőszámot, és az azonosítóval 2 bájtosával (azaz 2 karakterenként) az elejétől kezdve kizáró vagyoljuk. A végén lemaszkoljuk az előjelbitet, hogy biztosan pozitív legyen a szám, azaz a jelszó.

Az algoritmus levezetve az „InfoPark” vevőkódra:

a jelszó *kezdőszám XOR „IN” XOR „FO” XOR „PA” XOR „RK”* azaz

$$73e2_{16} \oplus 494e_{16} \oplus 464f_{16} \oplus 5041_{16} \oplus 524b_{16} = 32489_{10}$$

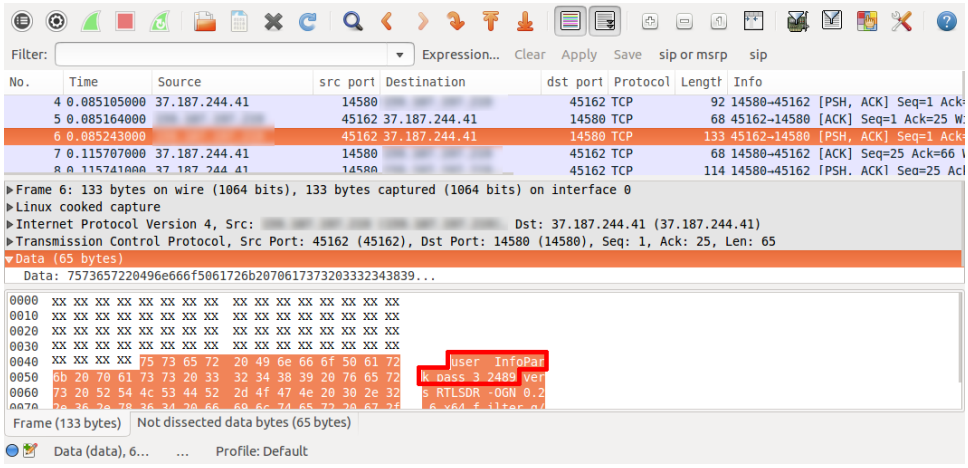
Gyenge engedélyezés

Adatküldés során nem is kell online lennie a vevőnek, azaz nem kell státusz üzeneteket küldenie. Elég, ha a vevő egyszer bejelentkezik az APRS szerverre felhasználónév/jelszó párossal, onnantól nincs is szükség sem a földrajzi hely megadására konfigurációs csomagokkal, sem státuszüzenetek küldésére, vagyis elég légi eszközök adatait továbbítania. Így előállhat az a furcsa helyzet, hogy a megjelenítő alkalmazásokon a vevőállomás vörösen, offline, vagy egyáltalán meg sem jelenik, viszont az általa továbbított adatok alapján megjelennek légijárművek.

A légijármű adatok sincsenek igazán validálva, az eszköz által sugárzott, a fizika törvényeit meghazudtoló hamis vagy hibás adatokat is megjeleníti a legtöbb kliens alkalmazás. Lásd 4. ábra.

Titkosítatlan átvitel

Ha egy kiszolgálón vagyunk a vevőt megvalósító ogn-rf és ogn-decode szoftverrel, könnyedén kielemezhetjük a vevő és az APRS szerver közti adatforgalmat.



3. ábra APRS csomag megjelenítése a Wireshark eszközzel, a képet készítették, szerkesztették a szerzők

Ugyanígy lehallgathatjuk egy hálózati forgalom analizáló eszközzel, például Wiresharkkal, ha egy hálózaton vagyunk vele, és sikerül egy MITM-jellegű[4] támadással például DNS[5] gyorsí-

[4] Man in the middle – közbeékelődéses támadás

tótár mérgezés vagy ARP[6] mérgezés [9] módszerével a két végpont közé férkőznünk. Ezután akár egyszerűen le is másolhatjuk, meghamisíthatjuk és meg is módosíthatjuk a csomagokat. Vegyük észre, hogy a 3. ábrán kiemelt részben tényleg a fentebb általunk is kiszámolt jelszó található. Tapasztalataim szerint a légiirányítás fenntartásokkal kezeli az OGN-t emiatt a sebezhetőség miatt.

Egy támadás vektora

- Kiválasztjuk az trackert a regisztrált eszközök listájából. [1] Legyen ez a példa kedvéért OGN132528 (a tracker bármelyik lehetne, ez az általam használt, kölcsön kapott valódi tracker).
- Kiválasztjuk a vevőt a vevők listájából, [10] vagy egy térképes megjelenítőből. [11] Legyen ez most InfoPark (a vevő bármelyik lehetne, ez az általam telepített valós, ideiglenes vevő a munkahelyemnél).
- Kitöltjük a bejelentkező csomagot.
    - Felhasználónév a vevő azonosító; a jelszó generálható online, [12] vagy a korábbi fejezetben mutatott módszerrel ki is számolható, sőt, akár lehallgatható, ezért nem is féltem jelen cikkben nyilvánossá tenni.

```
user InfoPark pass 32489 vers RTLSDR-OGN 0.2.6.x64 filter g/ALL
```

- A további csomagokban időbélyeg dinamikus előállítására, megfelelő formázására van szükség. Ez Linux operációs rendszereken, bash-ben például a következőképp történhet.

```
date +%H%M%S
```

- Kitöltünk egy konfigurációs sort, hogy megjelenjünk a térképen. GPS pozíciót, és egyéb paramétereket adunk meg a vevőről, a protokollnak megfelelően. [7]

```
InfoPark>APRS,TCPIP*,qAC,GLIDERN2:/`date
+%H%M%S`h4728.26NI01903.78E&000/000/A=000390
```

- Kitöltünk egy státusz riport sort is, hogy online-nak tűnjünk.

```
InfoPark>APRS:>`date        +%H%M%S`h        v0.2.6.x64        CPU:0.2
RAM:13350.9/16730.0MB  NTP:0.1ms/+11.9ppm  +25.0C  1/1Acfts[1h]  RF:-
2+0.3ppm/+9.16dB
```

- Kitöltünk pár eszköz által lesugárzott sort. Nem muszáj a valódi eszköznek bejelentkezve lennie. Nem is muszáj logikus adatoknak lennie (például szürreális 999 csomó sebességet is megadhatunk egy szimulált vitorlázó vagy pilóta nélküli repülőgépnek). Lásd majd a 4. ábrán.

```
OGN132528>APRS,qAR:/`date
+%H%M%S`h4728.26N/01903.80E'000/999/A=000390 !W54! id07132528 +000fpm
+0.0rot 45.2dB 0e -2.6kHz gps5x7
```

- Csatlakozunk az egyik APRS szerverhez a listából, példaként a másodikhoz, a megfelelő publikus, ismert portjára.
    - glidern1.glidernet.org
    - glidern2.glidernet.org
    - glidern3.glidernet.org

[5] Domain Name System – tartománynév rendszer
[6] Address Resolution Protocol – cím feloldási protokoll

- glidern4.glidernet.org

```
telnet 37.187.244.41 14580
```

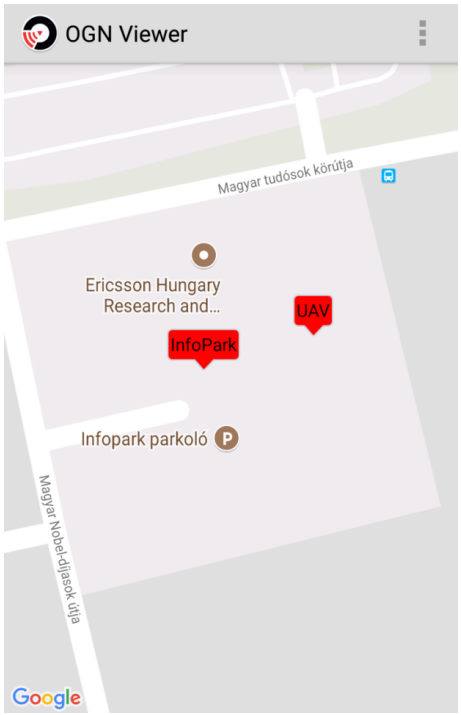
✈ Beküldjük az összeállított csomagokat.

Sikeresen eltérítettük vagy megzavartuk a céltárgy nyomkövető jelét a rendszerben.

4. ábra Sikeres megjelenítés a glidertracker.org [11] honlapon, a képet készítették a szerzők

Tapasztalataink szerint a glidertracker.org megjelenítő jobban megengedő. A live.glidernet.org csak akkor jeleníti meg, ha elég ideje aktív a vevő.

Az OGN Viewer App-on is látszik a sikeres támadás. Lásd 5. ábra.



5. ábra Sikeres megjelenítés az OGN Viewer alkalmazáson, [13] a képet készítették a szerzők

Javaslatok a biztonság növelésére

Átviteli biztonság (TRANSEC[7])

„[Az átviteli biztonság] mindazon védelmi rendszabályok összességének az eredménye, amelyek végrehajtásával biztosítjuk a híradó adatátviteli utakon, csatornákon az információk sértetlenségének, rendelkezésre állásának, bizalmasságának meglétét, valamint adott esetekben a hitelességét illetve letagadhatatlanságát." [14]

A megvalósításhoz javasoljuk az SSL[8]/TLS[9] titkosítást TCP[10] fölött. Ez az elterjedten használt módszer nyilvános (aszimmetrikus) kulcsú rejtjelezésen alapul. Aszimmetrikus kulcsú rejtjelezés alatt olyan kódolást értünk, ahol a kódoló kulcs és a dekódoló kulcs különbözik. Egy ilyen kulcspárral gyakorlatban megvalósíthatjuk nem csak az üzenetek titkosítását, hanem a digitális aláírását is a hitelesség biztosítására.

Ezek során mind a két fél (A és B) is rendelkezik saját privát és publikus kulccsal is. Abban az esetben, ha A küld B-nek, az üzenetét B publikus kulcsával titkosítja, és a kódolt üzenetet egy hasító (hash) algoritmus és saját privát kulcsának segítségével írja alá. B a kódolt és aláírt üzenet fogadása után ellenőrzi az üzenet integritását A publikus kulcsának segítségével és az üzenet saját oldalán történő hasításának végrehajtásával. Ezután a titkosított üzenetrészt dekódolja saját privát kulcsának felhasználásával.

Azt, hogy egy publikus kulccsal kódolt üzenetet csakis egy megfelelő privát kulccsal lehessen dekódolni, az RSA[11] algoritmus biztosítja.

Az SSL/TLS eljárás a fentiek informatikai megvalósítását, biztonságos kulcscserét illetve további képességeket biztosít a megfelelő biztonsági szint kialakításához.

Hitelesítés

Az APRS jelszó a már ismertetett okok miatt nem megbízható, ezért egy regisztrációs felület megvalósítását javaslom.

Az átviteli biztonság fenti megvalósítása igaz, nyújt hitelesítési lehetőségeket, de gondoljunk bele, ez átviteli, nem alkalmazói szinten történik a hálózatban, vagyis csak azt biztosítja alap esetben, hogy a szerver oldal az, akinek mondja magát. Ezért az APRS bejelentkezést is erősíteni érdemes, vagy bevezetni a kliens oldali tanúsítványok alkalmazását a SSL/TLS hitelesítés során.

Az APRS jelszót generáló algoritmus kifejlesztése során a fejlesztők elkövettek egy rég óta felismert hibát. A Kerckhoff-elv [15] alapján a titkosítási algoritmusok során egyedül a kulcsok kellene, hogy titkosak legyenek. Auguste Kerckhoff, a 19. századi matematikus szerint nem szabad egyedül arra alapozni egy eljárást, hogy a lehetséges támadók nem ismerik az algoritmust. Sőt, az algoritmus legyen publikus, hogy minél többen használhassák, illetve megismerhessék, ez is hozzájárul ahhoz, hogy biztonságosan lehessen alkalmazni, hiszen ha valami sérülékenység van az algoritmusban, annál hamarabb kiderül. A fejlesztők pont fordított logika mentén az algoritmust tartották titokban, és igazi jelszót nem is kérnek a felhaszná-

[7] Transport Security – átviteli biztonság
[8] Secure Sockets Layer
[9] Transport Layer Security
[10] Transmission Control Protocol
[11] Rivest–Shamir–Adleman (az algoritmus kidolgozói után)

lótól. Felteszik, hogy mert „ismeri” az algoritmust, biztosan a megbízható, hivatalos szoftvert használja, aminek titokban tartják a forráskódját.

Ha már javaslom a vevő regisztráció megvalósítását választott jelszóval, érdemes említést tenni a jelszavak tárolásának módjáról. Ne tároljunk a kiszolgálón nyers jelszavakat, hiszen ha ezeket megszerzi valaki, máris be tud jelentkezni a felhasználók nevében. Ebből az okból kifolyólag szokás a jelszavakat szerver oldalon hasítva, vagyis hash, lenyomat formájában tárolni.

A hasító eljárások jellemzője, hogy olyan függvények (egy bemenő adatból determinisztikusan ugyanaz az egy kimenet képződik minden esetben), amelyek nagy valószínűséggel nem generálják több különböző bemenetből ugyanazt a lenyomatot (csekély az ütközés esélye), illetve nem invertálhatóak (a kimenetet nem lehet, illetve nehéz közvetlen visszaalakítani az eredeti bemenetté). Még egy gyakori jellemzőjük, hogy a bemenő adatok kis mértékű módosítása a lenyomat nagy mértékű módosulásával jár, így nem lehet következtetni „ránézésre hasonló”, ismert bemenetű lenyomatok alapján az eredeti bemenetre.

Megjegyzés: a lenyomat általában jóval rövidebb, mint a bemenet volt. [15]

Engedélyezés

Heurisztikával segített mesterséges intelligenciával vizsgálható lehet, hogy valós adatokat küld-e a légijármű vagy az adó egység. Akár neuronhálóval, tanuló, evolúciós algoritmussal felkészíthetjük a szervereket, hogy kiszűrjék a valótlan adatokat. Megfelelő mennyiségű valós adat betáplálásával megtanítható a szűrő algoritmus, hogy melyek a valósnak tűnő adatok, így nem lehetne például a korábban bemutatott módszerrel szuperszonikus vitorlázó repülőgépet szimulálni a rendszerben.

Próbálkozásaink során kezdetleges szűrési próbálkozást véltünk felfedezni, amikor a Budapesten bejelentkezett vevőhöz Szolnok környékén mozgó járművet próbáltunk szimulálni. Bár az is lehetséges, hogy csak egy újabb programhibát fedeztünk fel, hiszen egy idő után furcsa módon a szimulált légijármű hirtelen megjelent Szlovákia fölött, pontosan északi irányban a vevőállomástól, Szolnok helyett. Ennek az is lehet egy feltételezhető oka, hogy a gyakran használt előjel nélküli, 16 biten ábrázolt egész számok maximális értéke 65 535. A vevő és a légijármű közti távolságot az OGN megjelenítők általában méterben számolják, Budapest és Szolnok távolsága nagyjából 90 km, vagyis a 16 biten ábrázolt egész szám vélhetően túlcsordult, és ez ábrázolási hibákat okozott. Ez gyakorlatban nem szokott előfordulni, hiszen a szokásos 868 MHz antennák hatótávolsága általában csak pár kilométer.

ÖSSZEGZÉS

A cikk által bemutatott, ma már széles körben elterjedt, és minden számítógépes platformon támogatott SSL/TLS eljárásnak köszönhetően könnyedén áthidalható lenne a titkosítatlan átvitel problémája. Ennek a kisebb fejlesztői feladatnak a megvalósítása évtizedek lemaradását hozná be a rendszer szempontjából. Egy modernebb jelszó politikával és ellenőrzött adatokkal megbízhatóbb szolgáltatást nyújthatna. Továbbá a trackerek regisztrációját megvalósító felülethez hasonlóan a vevő egységek regisztrációja is megoldható lenne, így a cikkben bemutatott támadás nem lenne ilyen könnyen, illetve ilyen formában kivitelezhető.

Az OGN hálózat meglátásunk szerint egy nagyszerű, egyre növekvő, közösségformáló kezdeményezés, melynek gyakorlati haszna felbecsülhetetlen a vitorlázó repülő pilóták számára.

FELHASZNÁLT IRODALOM

[1] GliderNet: OGN DDB - registered devices, url: http://wiki.glidernet.org/ddb-list

[2] Bottyán Z, Wantuch F, Gyöngyösi Z, Tuba Z, Hadobács K, Kardos P, Kurunczi R.: Development of a Complex Meteorological Support System for UAVs. WORLD ACADEMY OF SCIENCE ENGINEERING AND TECHNOLOGY 7:(4) pp. 646-651. 2013.

[3] Bottyán Z, Zénó András Gyöngyösi, Wantuch F, Tuba Z, Kurunczi R, Kardos P, Istenes Z, Weidinger T, Hadobács K, Szabó Z, Balczó M, Varga Á, Bíróné Kircsi A, Horváth Gy.: Measuring and Modeling of Hazardous Weather Phenomena to Aviation Using the Hungarian Unmanned Meteorological Aircraft System (HUMAS). IDŐJÁRÁS / QUARTERLY JOURNAL OF THE HUNGARIAN METEOROLOGICAL SERVICE 119:(3) pp. 307-335. (2015).

[4] Gyongyosi AZ, Kardos P, Kurunczi R, Bottyan Z.: Development of a complex dynamical modeling system for the meteorological support of unmanned aerial operation in Hungary. In: Kimon P Valavanis, Pascual Campoy (szerk.) 2013. International Conference on Unmanned Aircraft Systems (ICUAS): Conference Proceedings. 1172 p. Konferencia helye, ideje: Atlanta (GA), Amerikai Egyesült Államok, 2013.05.28-2013.05.31. Atlanta (GA): IEEE, 2013. pp. 8-16. (ISBN:978-1-4799-0815-8)

[5] Makkay Imre: Ütközések elkerülése a kisgépes és a pilóta nélküli repülésben. Repüléstudományi Közlemények (1997-TŐL) XXIX:(1), 2017, pp. 59–66. url: http://www.repulestudomany.hu/folyoirat/2017_1/2017-1-04-0378_Makkay_Imre.pdf

[6] Palik Mátyás: Pilóta nélküli légijármű rendszerek légi felderítésre történő alkalmazásának lehetőségei a légierő haderőnem repülőcsapatai katonai műveleteiben. PhD értekezés, Budapest, Zrínyi Miklós Nemzetvédelmi Egyetem, 2007. pp. 14–18, url: http://m.ludita.uni-nke.hu/repozitorium/bitstream/handle/11410/9778/Teljes%20sz%C3%B6veg%21?sequence=1&isAllowed=y

[7] Github: OGN flavoured APRS, url: https://github.com/svoop/ogn_client-ruby/wiki/OGN-flavoured-APRS

[8] Github: magicbug/PHP-APRS-Passcode, url: https://github.com/magicbug/PHP-APRS-Passcode/blob/master/aprs_func.php

[9] Haig Zsolt: In. Kovács László (szerk.) Információ - társadalom – biztonság. NKE Szolgáltató Kft., Budapest, 2015. (ISBN:978-615-5527-08-1)

[10] GliderNet: List of OGN Receivers, url: http://wiki.glidernet.org/list-of-receivers

[11] GliderTracker: Welcome, url: http://glidertracker.org

[12] APRS Passcode Generator: Techical Example of Passcode Generation using PHP, url: https://apps.magicbug.co.uk/passcode/index.php

[13] GooglePlay: OGN Viewer - FLARM Radar, url: https://play.google.com/store/apps/details?id=com.meisterschueler.ognviewer&hl=en

[14] Kerti András: Átviteli út biztonság. HADMÉRNÖK II:(4) 2007, pp. 60–65. url: http://www.hadmernok.hu/archivum/2007/4/2007_4_kerti.html

[15] Spala Ferenc: Bluetooth eszközök biztonsági kérdései, diplomamunka, Eötvös Loránd Tudományegyetem, Budapest, 2008. http://krasznay.hu/presentation/diploma_spala.pdf

A CASE STUDY ON OPEN FLIGHT SUPPORT SYSTEM SECURITY

Open Glider Network (OGN) is an open, glider flight support system, gaining ever growing recognition around the globe. Eventhough, with time its transport security measures have become outdated, with some simple steps it is possible to inject fraudulent data into the network. The aim of this article is to show that an open, public flight support system can also be secured. The article covers some now-existing security issues, and with constructive critique and white-hat approach it points out possible practices to mitigate the found problems, including common transport security solutions and heuristically aided artificial intelligence to validate flight data.

***Keywords**: flight support, security, case study*

Vránics Dávid Ferenc (MSc) doktoranduszhallgató, informatikus Nemzeti Közszolgálati Egyetem Hadtudományi és Honvédtisztképző Kar Katonai Műszaki Doktori Iskola vranicsd@gmail.com orcid.org/0000-0003-0637-476X	Vránics Dávid Ferenc (MSc) PhD Student, computer scientist National University of Public Service Faculty of Military Science and Officer Training Doctoral School of Military Engineering vranicsd@gmail.com orcid.org/0000-0003-0637-476X
Palik Mátyás (PhD) intézetigazgató, egyetemi docens Nemzeti Közszolgálati Egyetem Hadtudományi és Honvédtisztképző Kar Katonai Repülő Intézet palik.matyas@uni-nke.hu orcid.org/0000-0002-2304-372X	Palik Mátyás (PhD) Director of institute, associate professor National University of Public Service Faculty of Military Science and Officer Training Institute of Military Aviation palik.matyas@uni-nke.hu orcid.org/0000-0002-2304-372X
Bottyán Zsolt (PhD) tanszékvezető, egyetemi docens Nemzeti Közszolgálati Egyetem Hadtudományi és Honvédtisztképző Kar Katonai Repülő Intézet Repülésirányító és Repülő-hajózó Tanszék bottyan.zsolt@uni-nke.hu orcid.org/0000-0003-0729-2774	Bottyán Zsolt (PhD) Head of department, associate professor National University of Public Service Faculty of Military Science and Officer Training Institute of Military Aviation Department of Aerospace Controller and Pilot Training bottyan.zsolt@uni-nke.hu orcid.org/0000-0003-0729-2774

A GINOP 2.3.2-15-2016-00007 „A légiközlekedés-biztonsághoz kapcsolódó interdiszciplináris tudományos potenciál növelése és integrálása a nemzetközi kutatás-fejlesztési hálózatba a Nemzeti Közszolgálati Egyetemen – VOLARE” című projekt az Európai Unió támogatásával, az Európai Regionális Fejlesztési Alap társfinanszírozásával valósul meg.

A kutatás a fenti projekt „UAS_ENVIRON” nevű kiemelt kutatási területén valósult meg.

http://www.repulestudomany.hu/folyoirat/2018_1/2018-1-13-0460_Vranics_D_F-Palik_M-Bottyan_Zs.pdf