



A Tudomány Kapujában

A drónok kiberbiztonsági kihívásai

Katona Gergő

Nemzeti Közszerológati Egyetem

A drón infrastruktúrákat számos kiberbiztonsági kihívás fenyegeti, amelyeket fielembé kell venni, akkor mikor egy ilyen rendszer kialakítása előtt állunk. A kockázatok a következőkben a CIA triád alapján kerülnek kategorizálásra. A CIA triád kifejezés a kiberbiztonság három legfőbb alapelvét tartalmazza. A támadók ha egy elektronikus információs rendszer működését szeretnék befolyásolni, akkor ezen három alapelvet Bizalmasságot, Sértelességet, Rendelkezésreállást szeretnék megtörni különböző támadásokkal.

A támadások csoportosításánál ez elsődleges hatás került megvizsgálásra, ami azt jelenti, hogy az egyes támadások nem csak arra az alapelvre hathatnak, de első körben ezen elv megsértése következik be.

Bizalmasság

Személyazonosság-hamisítás: Az azonosság-hamisítás lehetővé teszi a támadó számára, hogy olyan identitásnak álcázza magát, amely jogosan helyezkedik el a rendszerben, rendelkezik megfelelő jogosultsággal, hogy hozzáférjen a rendszer adataihoz.

Üzenet visszajátszása: A visszajátszási támadások során a jogos adatokat a támadó észleli, és elfogja, amit később újra és újra továbbít. Mivel az adatok hitelesek, nehéz eldönteni, hogy az eredeti forrás ismét elküldte-e az üzenetet, vagy az újraküldött adatokat támadásra használják.

Lehallgatás: A lehallgatás a drónok kommunikáció jogosulatlan valós idejű lehallgatását jelenti, amely lehetővé teszi a támadó számára, hogy lekérje az eszközök közötti bizalmas információkat. Ezen támadás elősegítheti az üzenet visszajátszási támadást is többek között.

Sértelesség

Az információ helyettesítése vagy módosítása: Ezen támadásnak a lényege, hogy a kommunikációban jelenlévő hiteles adatokat fals információkra cserélik. A módosítások különféle formái magukban foglalják a módosítást, gyártást, helyettesítéseket és adat injektálást is.

Hozzáférés kezelés módosítása: A hozzáférés kezelés azon a szabályok és házirendek összessége, amelyek szabályozzák, hogyan kommunikálnak egyes eszközök a rendszerben, és hogyan fér hozzá a felhasználó az adatokhoz. Ha egy támadó hozzáfér ezen rendszerhez, akkor megváltoztathatja az jogosultsági engedélyeket, így átvéve az irányítást a rendszer felett.

Man-in-the-Middle támadások: lehetővé teszik a támadók számára, hogy rögzítsék a drónok és vezérlő, szenzorok közötti kommunikáció adatait. A támadó egy vezeték nélküli hozzáférési ponton keresztül kikényszeríti a közeli eszközöknél, hogy csatlakozzanak domainjéhez a kommunikáció során. Ezen a hozzáférési pontokon keresztül a hálózati forgalmat a támadó manipulálhatja.

Üzenethamisítás: A drón rendszerek üzenethamisító támadása alatt a nyilvános/nyitott csatornán végrehajtott korábbi munkamenetekben lévő bejelentkezési kérelmet hamisítják a hitelesítés lefutása során. Ezt követően a támadó módosíthatja és továbbíthatja az üzenetet a felhasználónak.

Rendelkezésre állás

A GPS-adatok zavarása vagy hamisítása: A drón navigálása a fedélzeti GPS-vevő által fogadott és feldolgozott GPS-jelektől függ. A GPS adások szabadon hozzáférhetőek, titkosítatlan és nem hitelesített jelek. A GPS-jelek nyílt jellege lehetővé teszi a hamisítási támadásokat, ahol hamis jeleket lehet generálni és a megtámadott drónnak továbbítani azzal a céllal, hogy az eszköz megváltoztassa a GPS-vevője által kiszámított földrajzi koordinátákat.

Fizikai támadás: Ezen támadások a hardverek fizikai megkárosítását, illetve megsemmisítését helyezik a középpontba.

Szolgáltatás megtagadás: Ennél a támadásnál az elkövető a célpontot folyamatos és nagy számú kéréssel árasztja el, amelyet a célpont nem tud feldolgozni és így nem lesz az adott szolgáltatás elérhető. A DoS támadás egyik fajtája az elosztott szolgáltatásmegtagadással járó támadás (Distributed Denial of Service), amely során nem egy eszköztől történik a támadás, hanem eszközök hálózatról úgynevezett botnet hálózatról. Mivel a drónok megfelelő működéséhez folyamatos kommunikáció szükséges, ezért ha ezen csatornákat egy támadó elárasztja akkor az eszközök elérhetetlenek lesznek.

A féreglyuk-támadások: úgy működnek, hogy kapcsolatot hoznak létre két csomópont között. Ez a kapcsolat olyan két csomópont között fordulhat elő, amelyek tipikusan nem közvetlenül egymás mellett vannak. A féreglyuk adatokat fogad a forráscsomóponttól és továbbítja a

célállomásnak. Mivel a célállomás a féreglyukon keresztül fogad adatokat, feltételezi, hogy a forrás most egy ugrásvira van. Egy támadó két dolgot tehet ezzel a féreglyukkal: a szolgáltatás megtagadása támadást eszközölhet vagy lehallgatja a csatornát.

Feketelyuk támadás: Ez abban különbözik a féreglyuk támadástól, hogy itt a támadó, mikor hálózati csomóponttá válik nem továbbítja a csomagokat, hanem eldobja azokat.

Támadások csoportosítása céljaik alapján

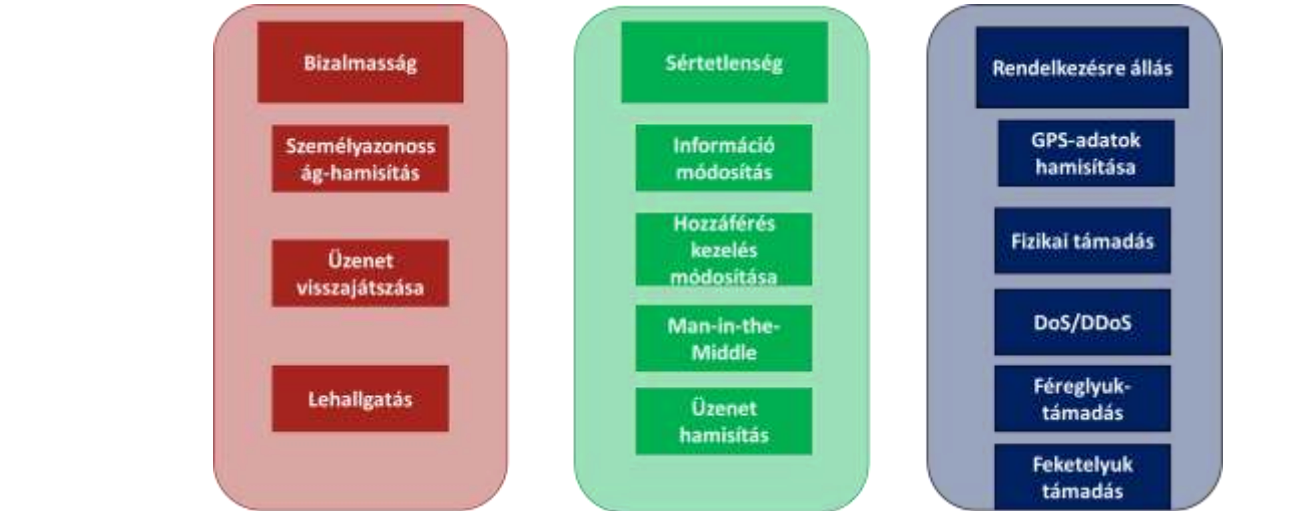
Egy svéd tanulmány alapján megvizsgáltam, hogy az előzőekben bemutatott támadásokat az elkövetők milyen céllal használták fel. Az esettanulmányokból az látszik, hogy 4 fő célja volt a támadásoknak. Amelyek a következők voltak: repülési útvonal eltérítés; lezuhanás/leszállás; hozzáférés a drón rendszer fájljaihoz; lehallgatás. A vizsgálat eredménye a 2. sz. ábrán látható. A fő cél inkább a drónok eltérítése volt. Ezt követte a leszállásra vagy lezuhanásra kényszerítés. A fájllokhoz való hozzáférés és a lehallgatás azonos megoszlásban látható. Ebből arra lehet következtetni, hogy a támadók főleg a drónok irányítását akarják átvenni, az információ szerzés, mint cél csak másodlagos. Ezen eredmény fontos lehet egy leendő akár autonóm drón rendszer kialakításakor. Mivel az egyes fenyegetések kockázatait valósabban fel lehet mérni, így könnyebb meghatározni a megfelelő ellenintézkedést is.

Források

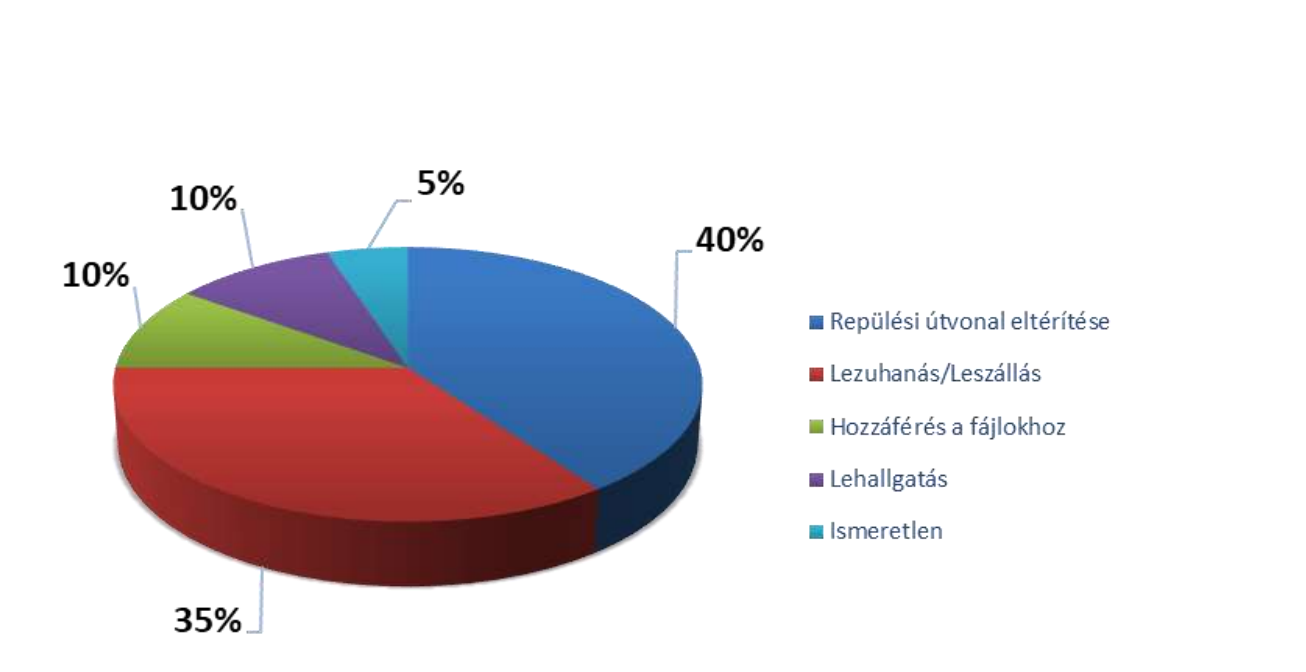
- [1] Lamia CHAARI, Sana CHAHBANI, és Jihene REZGUI, Vulnerabilities Assessment for Unmanned Aerial Vehicles Communication Systems, 2020 International Symposium on Networks, Computers and Communications, 2020. október, 1–6, <https://doi.org/10.1109/ISNCC49221.2020.9297293>
- [2] Shashank Kamthan, Harpreet Singh, és Thomas Meitzler, UAVs: on development of fuzzy model for categorization of countermeasures during threat assessment, in Unmanned Systems Technology XIX, köt. 10195 (Unmanned Systems Technology XIX, SPIE, 2017), 407–15, <https://doi.org/10.1117/12.2275551>
- [3] CHAARI, CHAHBANI, és REZGUI, Vulnerabilities Assessment for Unmanned Aerial Vehicles Communication Systems
- [4] Riham Altawy és Amr Youssef, Security, Privacy, and Safety Aspects of Civilian Drones: A Survey, ACM Transactions on Cyber-Physical Systems 1 (2016. 09.): 1–25, <https://doi.org/10.1145/3001836>
- [5] E. Dahlman és Karin Lagrelius, A Game of Drones: Cyber Security in UAVs, Undefined, 2019, <https://www.semanticscholar.org/paper/A-Game-of-Drones-%3A-Cyber-Security-in-UAVs-Dahlman-Lagrelius/3119bc3f5f4282210ab46a25ce86b3c6124b26d5>

Katona Gergő

„AZ INNOVÁCIÓS ÉS TECHNOLÓGIAI MINISZTERIUM ÚNKP-21-2-I-NKE-111 KÓDSZÁMÚ ÚJ NEMZETI KIVÁLÓSÁG PROGRAMJÁNAK A NEMZETI KUTATÁSI, FEJLESZTÉSI ÉS INNOVÁCIÓS ALAPBÓL FINANSZÍROZOTT SZAKMAI TÁMOGATÁSÁVAL KÉSZÜLT.”



1.sz. ábra: Drón támadások csoportosítása; Saját szerkesztés



2.sz. ábra: Drón támadások céljainak csoportosítása; Saját szerkesztés