NEMZETI KÖZSZOLGÁLATI EGYETEM
LUDOVIKA

A TÉRINFORMATIKA SZEREPE AZ OKOSVÁROSOK FEJLESZTHETŐSÉGÉBEN (kiberbiztonsági nézőpontból)

Orbók Ákos
tanársegéd
Kiberbiztonsági és E-közigazgatási Tanszék

eivok

Mi az okos város?

Adatvezérelt város

- szenzorhálózatok,
- IoT
- mobil appok
- …

A kihívás

Az okos város biztonsági kihívásai (részlet)

Kiberbiztonság:

- A használt eszközök milyen védelemmel rendelkeznek?
- A felhasználók menyire tudatosan használják?
- Milyen időközönként vizsgálják felelül a védelmi képességeket?

Üzembiztonság:

- A használt technológia mennyire megbízhatóan működik?
- Ha elromlik milyen következményei lehetnek?

Adatvédelem:

- A helyadatokból és a szenzorok adataiból mennyire lehet profilozni a polgárokat?
- A gyártó figyelheti-e a felhasználó eszközének paramétereit? Mihez férhet hozzá?

Adatforrások kihívásai az okosvárosokban

Adatforrások

IoT-szenzorok

GNSS

Kiberbiztonság

Információ-biztonság

Adatkezelés

Digitális ikrek

Helyhez kötött döntéstámogatás

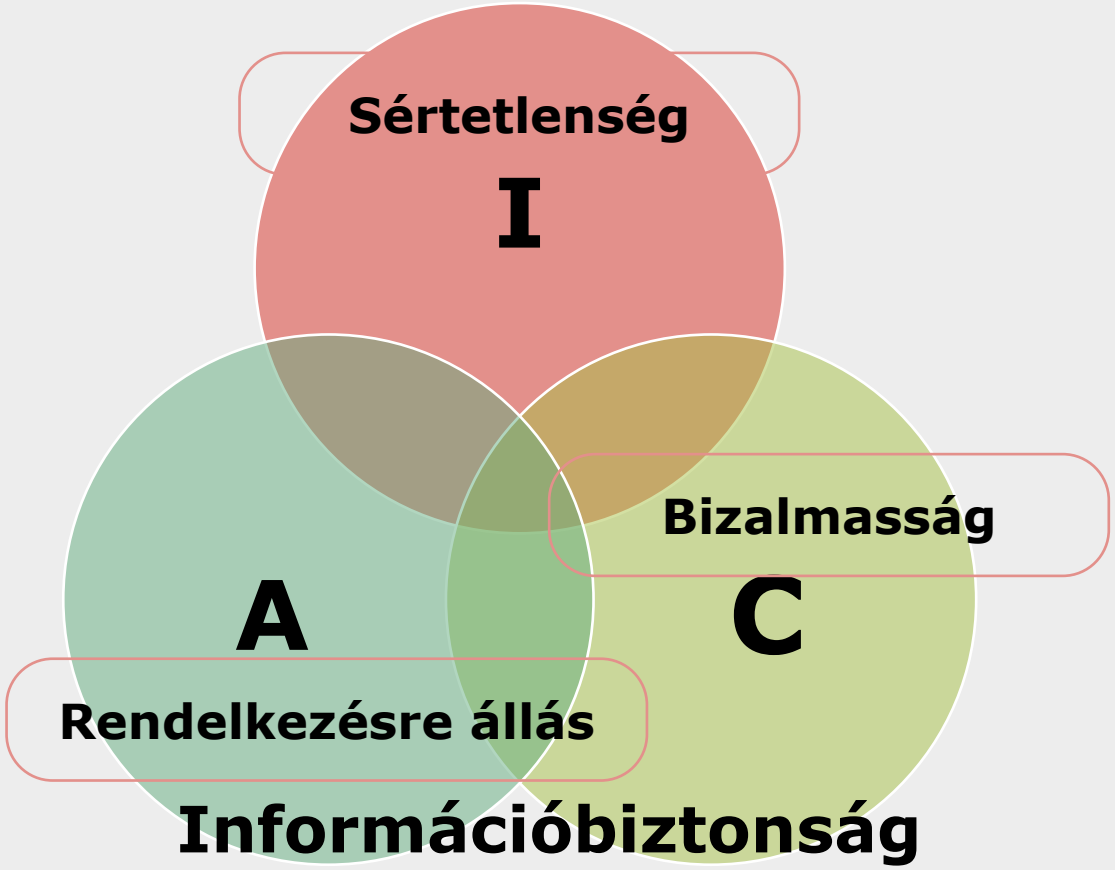
Térinformatika

Adatintegráció

Adatminőség

Adatvédelem

Hol sérülhet a rendszer?



Információbiztonság (CIA elv)

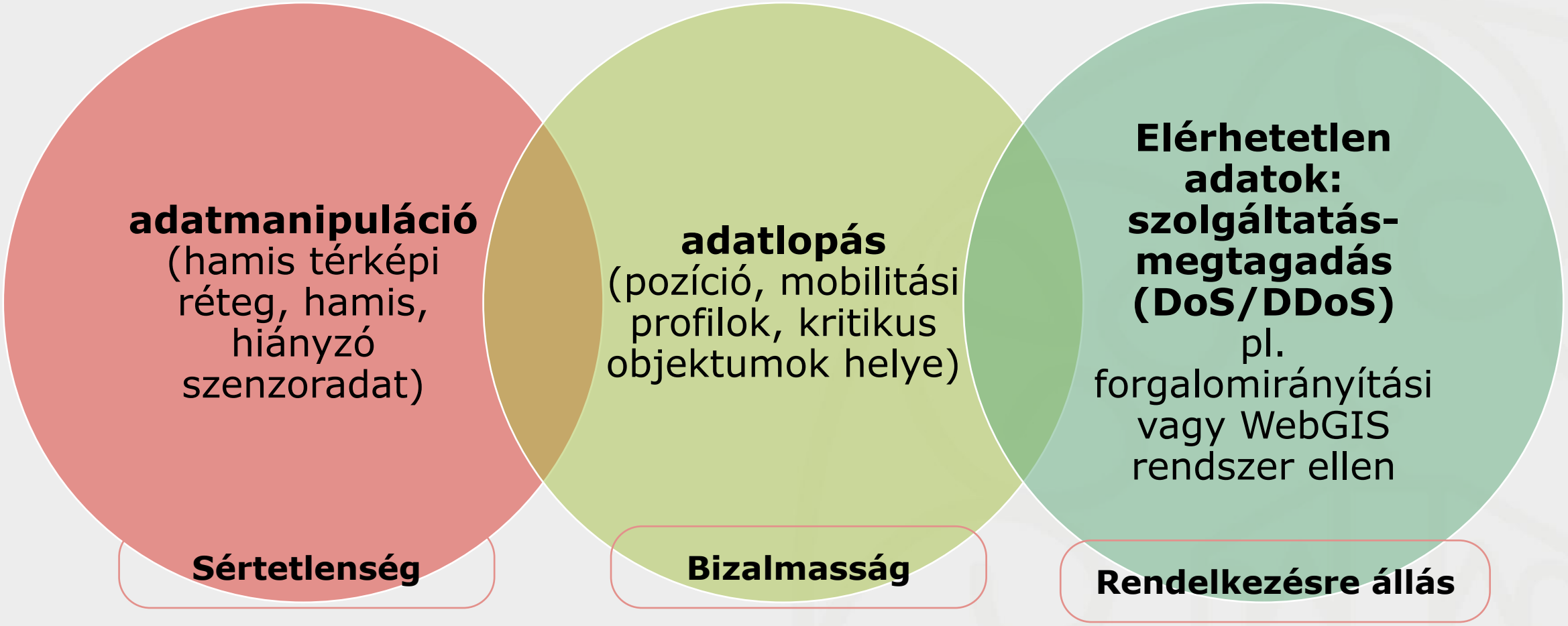
Alkalmazási réteg
WebGIS, döntéstámogató rendszerek, nyílt adatos portálok

Platform/adatréteg
városi adatplatform, idő-sor adatbázisok, téradatbázisok, felhő

Kommunikációs réteg
LoRaWAN, NB-IoT, 4G/5G, Wi-Fi, optika

Eszköz/szenzor réteg
IoT, kamerák, mérőállomások, drónok

Fenyegetési környezet *röviden*



Kiber-fizikai hatás:
a rossz geoadat **fizikai kockázattá** válhat (baleset, torlódás, üzeműzavar)

Fenyegetési környezet
(motiváció alapján)

- Szervezett bűnözés (zsarolóvírus, adatlopás, kémkedés)

Kiberbűnözés

- államilag támogatott szereplők (kritikus infrastruktúrák ellen)

Kiberhadviselés

Kiberterrorizmus

- Félelemkeltés

Hacktivizmus

- hacktivisták, script kiddie-k, insider (hibázó vagy rosszindulatú munkatárs/alvállalkozó)

Eszköz- és szenzorszintű kockázatok

IoT-eszközök tipikus gyengeségei:

- gyári alapértelmezett jelszók, frissítetlen firmware, gyenge titkosítás
- fizikai hozzáférhetőség (utcai szekrény, oszlopra szerelt szenzor)

Geospecifikus fenyegetések:

- **GNSS-zavarás és –spoofing**: járművek, drónok, időszinkron tévesztése
- hamis szenzorok vagy klónozott eszközök beillesztése a hálózatba

Lehetséges következmények:

- hibás forgalommodellek, rosszul hangolt közlekedési lámpák
- szennyezés „eltüntetése” adatmódosítással

Hálózati és kommunikációs fenyegetések

Városi IoT-hálózatok:

- **LoRaWAN, Sigfox, NB-IoT**:
  eltérő biztonsági modell, kulcskezelés
- 4G/5G hálózati szeletek: elkülönítés kérdése

Tipikus támadások:

- lehallgatás, közbeékelődés (MITM), replay támadások
- DoS a gateway-ek és broker-ek ellen (MQTT, AMQP stb.)

GIS-re gyakorolt hatás:

- hiányos idő-sorok, „lyukas” idősor
  hibás tér-idő elemzések
- késleltetett vagy duplikált események
  téves riasztások, döntések

Adatplatform, WebGIS és API-k sérülékenysége

Városi adatplatform / digitális iker:

sok alrendszerből integrált, gyakran **felhő + on-prem** hibrid rendszerek

Tipikus hibák (OWASP):

- gyenge autentikáció (megosztott felhasználók, API-key nyilvános repo-ban)
- rossz hozzáférés-kezelés (mindenki „admin”, tesztrendszerben éles adatok)
- input-validáció hiányosságai – SQL/NoSQL/command injection a téradatbázisban
- rosszul konfigurált OGC-szolgáltatások (WMS/WFS/WFS-T), túl tág lekérdezési lehetőségek

Következmények:

- kritikus térbeli adatok (pl. rendőrségi, energetikai rétegek) kiszivárgása
- téradat-bázis módosítása (map defacement, geoadat „poisoning”)

Geoadat-specifikus fenyegetések: privacy, profilozás, re-identifikáció

- Helyadat, mint „szuper” személyes adat:
  - lakcím, munkahely, rutin (útvonalak) - könnyű profilozás
- Okos városi példák:
  - közösségi kerékpár / roller adatok, tömegközlekedési kártyák, parkolási appok
- Kockázatok:
  - felhasználók újra azonosítása anonimnak hitt adatbázisokból
  - érzékeny csoportok (iskolák, kórházak, kissebségek) helyének, viselkedésének feltérképezése
- Milyen feladatot jelent ez a térinformatikusnak:
  - térbeli aggregáció,
  - generalizálás,
  - k-anonimitási küszöb,
  - adatminimalizálás szükségessége

Kiber-fizikai rendszerek, digitális ikrek és geoadat-integritás

Smart city, mint **kiber-fizikai rendszer**:

- forgalomirányítás, közvilágítás,
  víz- és energiahálózat, vészkezelés
- ICS/SCADA biztonság irányelvei:
- NIST SP 800-82 – ipari irányítórendszerek kiberbiztonsága
- geoadatok gyakran **vezérlési logikát**
  is befolyásolnak (zónák, prioritások)

Kiber-fizikai rendszerek, digitális ikrek és geoadat-integritás

Lehetséges támadások:

- digitális iker adatainak manipulálása
  hibás szabályok, rossz optimalizáció
- hamis geoadat alapján automatikus átirányítás, lezárás, erőforrás-átcsoportosítás

Pl: ukrán áramszolgáltatók elleni támadások (2015–2016)
ICS/SCADA sérülékenységek, geo.infó rendszerekkel összefüggő folyamatok is érintettek voltak

Jogi és szabványos keretek a geoadatokra

- **Adatvédelem:**
  GDPR – helyadat, mint személyes adat;
  célhoz kötöttség, adattakarékosság, elszámoltathatóság
- **Információbiztonsági keretrendszerek**:
  ISO/IEC 27001:
  információbiztonság irányítási rendszere
  NIST Cybersecurity Framework:
  azonosítás, védelem, detektálás, reagálás, helyreállítás
  IoT-specifikus: ETSI/EN szabványok fogyasztói IoT eszközökre
- **Smart city / urbanisztikai keretek**:
  ISO 37120/37122:
  smart city indikátorok (közvetve geoadat-intenzív rendszerek)
- **GIS-eknél**:
  jogosultság-kezelés téradat-rétegek szintjén
  adatkezelési nyilvántartás,
  DPIA (adatvédelmi hatásvizsgálat) geoadat-projekteknél

Mit tehet a térinformatikai szakember?

1. Tervezési fázisban

- Vegyen részt **fenyegetésmodellezésben**:
  - Milyen geoadat? Ki fér hozzá? Mi történik, ha módosul/eltűnik/kiszivárog?
- **Privacy-by-design**:
  - tényleg kell-e egyedi szintű helyadat, vagy elég aggregált?
  - szükséges-e pontos cím, vagy elég cellaszint, rács, zóna?

Mit tehet a térinformatikai szakember?

2. Megvalósításkor

- WebGIS / API biztonság:
  - erős autentikáció, szerepkör-alapú hozzáférés (RBAC, ABAC)
  - „least privilege” elve rétegszinten
  - naplózás, audit trail térbeli műveletekről
- Adatintegritás:
  - ellenőrző összegek, aláírás, forrás metaadatok
  - anomália-detektálás (görbülő idősorok, váratlan minták)

Mit tehet a térinformatikai szakember?

3. Üzemeltetés és együttműködés

- rendszeres sérülékenység-vizsgálat, patch-kezelés (beleértve térinformatikai szoftvereket is)
- együttműködés a város **CISO / IT-biztonsági csapatával** (nem „külön világ” a GIS)
- fókusz a **képzésen**: GIS-csapat alap kiberhigiénéje (phishing, jelszókezelés, adathordozók)

Összefoglalás

- Az okos város **nem csak IT-rendszerek halmaza**, hanem egy kiber-fizikai ökoszisztéma. (Lesz…)
- A **térinformatika** a legtöbb smart city use case „kritikus magja” ezért **támadási felület is**.
- A geoadatokra egyszerre érvényes a **kiberbiztonság** és az **adatvédelem** is.
- A geoinformatikus mint kulcsszereplő:
  - fenyegetésmodellezés
  - adatarchitektúra
  - privacy-by-design, security-by-design
  - együttműködés a kiberbiztonsági csapattal

Irodalom

- Batty, M., Axhausen, K. W., Giannotti, F., et al. (2012). Smart cities of the future. *European Physical Journal Special Topics*, 214(1), 481–518.
- Gubbi, J., Buyya, R., Marusic, S., & Palaniswami, M. (2013). Internet of Things (IoT): A vision, architectural elements, and future directions. *Future Generation Computer Systems*, 29(7), 1645–1660.
- Kitchin, R. (2014). The real-time city? Big data and smart urbanism. *GeoJournal*, 79, 1–14.
- Krumm, J. (2007). Inference attacks on location tracks. In A. LaMarca, M. Langheinrich & K. N. Truong (Eds.), *Pervasive 2007*, Lecture Notes in Computer Science, 4480, 263–278. Springer.
- de Montjoye, Y.-A., Hidalgo, C. A., Verleysen, M., & Blondel, V. D. (2013). Unique in the Crowd: The privacy bounds of human mobility. Scientific Reports, 3, 1376.
- Roman, R., Zhou, J., & Lopez, J. (2013). On the security of Internet of Things: A survey. Computer Networks, 57(10), 2266–2279.
- Sicari, S., Rizzardi, A., Grieco, L. A., & Coen-Porisini, A. (2015). Security, privacy and trust in Internet of Things: The road ahead. Computer Networks, 76, 146–164.
- Zanella, A., Bui, N., Castellani, A., Vangelista, L., & Zorzi, M. (2014). Internet of Things for Smart Cities. IEEE Internet of Things Journal, 1(1), 22–32.
- ISO/IEC 27001:2013. Information technology — Security techniques — Information security management systems — Requirements. International Organization for Standardization.
- ISO 37120:2018. Sustainable cities and communities — Indicators for city services and quality of life. International Organization for Standardization.
- ISO 37122:2019. Sustainable cities and communities — Indicators for smart cities. International Organization for Standardization.
- ETSI EN 303 645 V2.1.1 (2020-06). Cyber Security for Consumer Internet of Things: Baseline Requirements. European Telecommunications Standards Institute.NIST (2015). Guide to Industrial Control Systems (ICS) Security.
- NIST Special Publication 800-82, Revision 2. National Institute of Standards and Technology.
- NIST (2018). Framework for Improving Critical Infrastructure Cybersecurity (Version 1.1). National Institute of Standards and Technology.
- European Union. (2016). Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation).
- E-ISAC & SANS ICS. (2016). Analysis of the Cyber Attack on the Ukrainian Power Grid. Electricity Information Sharing and Analysis Center & SANS Institute.

KÖSZÖNÖM A FIGYELMET!

uni-nke.hu