Biomatika és Alkalmazott Mesterséges Intelligencia Intézet			Választható tárgy 2025-26-2			
Tantárgy neve:	Kódja:	Kredit:	Óraszám			
				ea	tgy	lab
Beágyazott rendszerek biztonsága	NBWBA1HBNF	5	nappali heti	2	0	2
Tárgyfelelős: Dr. Bánáti-Baumann Anna			Beosztás: egyetemi adjunktus			
Oktató(k): Bringye Zsolt						
Előtanulmányi feltételek:	szakmai szigorlat vagy MSc					
Számonkérés módja:	évközi jegy					

A tananyag	
Oktatási cél:	Beágyazott rendszerek biztonsági vizsgálatához szükséges módszerek, technikák megismertetése a hallgatókkal. A megszerzett ismeretek segítik a beágyazott rendszerek működésének mélyebb megismerését, ami általános (nem biztonság-specifikus) tesztelés, hibakeresés során is jelentős segítség lehet. A tananyagban az elméleti ismeretek és azok gyakorlatban való kipróbálását célzó feladatok szerves egységet alkotnak.
Tematika:	Bevezetés, korábban tanultak felfrissítése: az IT biztonság alapjai; beágyazott rendszerek áttekintése; program kód létrehozásának folyamata fordító alapú nyelvek esetén. Fenyegetési modellek beágyazott rendszerek esetén. Biztonság tesztelési módszerek. Vizsgálati eszköztár szoftver sérülékenységek felderítésére. Interfészek felderítése, támadási lehetőségek. Statikus kód elemzés. Dinamikus kód elemzés. „Firmware hacking”.

Féléves ütemezés	
Oktatási hét (konzultáció)	Témakör
1.	Ea: IT Security alapok, kockázatok, kockázatkezelés Lab: FMEA alapú kockázatelemzés áttekintése példákon keresztül
2.	Ea: Beágyazott rendszerek áttekintése, hardver, szoftver rétegek, beágyazott rendszerek biztonsága, threat modeling (4 óra) Lab: -
3.	Ea: - Lab: a laborokon használt mikrovezérlő ISA áttekintése. Hogyan lesz a C kódból gépi kód? Eszközkészlet beágyazott fejlesztéshez (4 óra)
4.	Ea: Biztonsági tesztelési módszerek Lab: Vizsgálati eszköztár megismerése
5.	Ea: Hardver interfészek (klasszikus soros interfészek típusai, jellemzői) Lab: UART (azonosítás, „lehallgatás”)
6.	Ea: - Lab: SPI és I2C (azonosítás, „lehallgatás”, SPI memória) (4 óra)
7.	Ea: Szoftver felderítés, támadás – statikus és dinamikus elemzés (4 óra) Lab: -
8.	Ea: Kód elemzés eszközei Lab: Statikus kód elemzés
9.	Szünet
10.	Ea: - Lab: Dinamikus kód elemzés (4 óra)
11.	Ea: ZH, Kód analízis operációs rendszer (pl. Linux) esetén

	Lab: Kód analízis operációs rendszer (pl. Linux) esetén
12.	Ea: Kód analízis operációs rendszer (pl. Linux) esetén Lab: Komplex órai feladat
13.	Ea: - Lab: Komplex órai feladat II. (4 óra)
14.	Pót ZH, Házi feladatok bemutatása

Félévközi követelmények	
Évközi jegy / aláírás megszerzésének feltételei:	Az előadásokon és a laborgyakorlatokon való részvétel kötelező. A félév során egy házi feladat kerül kiosztásra, ezt a megadott időpontig önállóan vagy párban meg kell oldani, valamint a megoldásról dokumentációt kell készíteni és a 14. hétig bemutatni.

Zárthelyi dolgozatok	
Oktatási hét	Témakör
11.	ZH (az elmélet anyagából)
14.	pót ZH (az elmélet anyagából)

Az *évközi jegy* kialakításának módszere (csak évközi jegyes tárgyak esetében töltendő ki)
A ZH és a házi feladatra kapott érdemjegyek átlaga.

Pótlás módja	
A ZH / évközi jegy / aláírás pótlásának módja:	Az aláíráspótló időszakban meghirdetett alkalommal a ZH megírása és a házi feladat bemutatása pótolható.

Vizsga módja (csak vizsgás tantárgy esetében töltendő ki)
-

Vizsgajegy kialakítása (csak vizsgás tantárgy esetében töltendő ki)
-

Az egyes érdemjegyek ponthatárai:
91% … 100%: jeles (5) 81% … 90%: jó (4) 66% … 80%: közepes (3) 51% … 65%: elégséges (2) 0% … 50%: elégtelen (1)

Irodalom	
Kötelező:	Az óra anyagát képző diasorok és segédletek, valamint az alkalmazott eszközök gyártói dokumentációi
Ajánlott:	– Jasper van Woudenberg és Colin O'Flynn: The Hardware Hacking Handbook: Breaking Embedded Security with Hardware Attacks, No Starch Press (December 21., 2021) – Fotios Chantzis et al., Practical IoT Hacking: The Definitive Guide to Attacking the Internet of Things, No Starch Press (April 9, 2021)
Egyéb segédletek:	