IT biztonság főspecializáció

MSc Mérnökinformatikus szak

Célkitűzés

A specializáció célja olyan mérnök-informatikusok képzése, akik

- értik az IT rendszerek különböző architektúrális szintjein felmerülő informatikai biztonsági problémákat,
- képesek egy adott rendszerben felmerülő releváns biztonsági problémák azonosítására és elemzésére,
- értik és alkalmazni tudják a problémák megoldására szolgáló tipikus biztonsági technológiákat és módszereket, és
- képesek új biztonsági architektúrák és mechanizmusok tervezésére és megvalósítására is.

https://www.hit.bme.hu/page/itbiztonsag

HÁLÓZATI RENDSZEREK
ÉS SZOLGÁLTATÁSOK
TANSZÉK

www.hit.bme.hu

Szaktárgyak

Szoftverbiztonság (A1 tárgy)

webes és mobil alkalmazások biztonsága, alacsony szintű és menedzselt nyelvek biztonsága, hitelesítés és engedélyezés, szoftverek biztonsági tesztelése

Számítógép- és hálózatbiztonság (A2 tárgy)

OS és firmware biztonság, mobil platformok biztonsága, virtualizációs és konténer technológiák biztonsága, malware, hálózati behatolástesztelés (ethical hacking), tűzfalak és behatolás detektáló rendszerek, hálózati forgalom monitorozása, logelemzés

Kriptográfiai protokollok (B tárgy)

szimmetrikus és aszimmetrikus kulcsú kriptográfiai primitívek tulajdonságai, kulcsmenedzsment, véletlenszám generálás, TLS (web), WPA2 (WiFi), háttértár rejtjelezés, egyéb kriptográfiai alkalmazások

A gépi tanulás biztonsága (C tárgy)

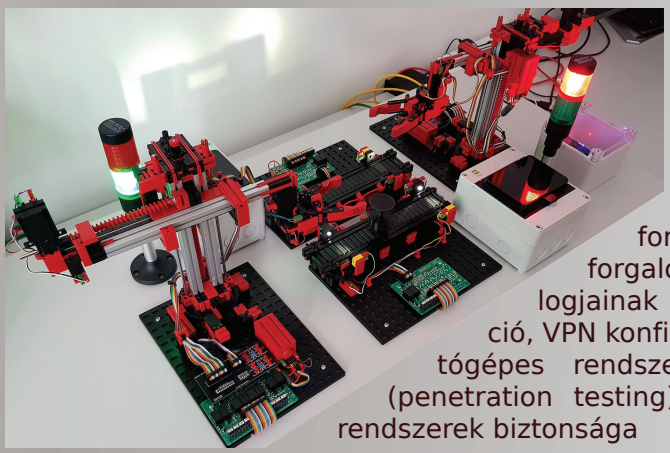
döntések manipulációja, tanító adat mérgezése, hátsó kapuk és trójaiak ML modellek ellen, tanító adat rekonstrukciója, modell-lopás, modellek megmagyarázhatóságának támadása

Mérés labor

Szoftverbiztonság laboratórium

alkalmazások biztonsági tesztelése, programkód digitális aláírása, webes alkalmazások biztonsága (kliens és szerver oldal, menedzselt nyelvek biztonsága, mobil alkalmazások biztonsága, memóriakorrupció (támadások, védekezési technikák)

Számítógép- és hálózatbiztonság laboratórium



konténerek biztonsági beállításai, jogosultságkezelés Linux alapú operációs rendszereken, memóriában végzett digitális elemzés (memory forensics), háttértár digitális elemzése (disk forensics), rögzített hálózati forgalom és hálózati eszközök logjainak elemzése, tűzfal konfiguráció, VPN konfiguráció, hálózatok és számítógépes rendszerek biztonsági tesztelése (penetration testing), Internet of Things (IoT) rendszerek biztonsága

Önálló laboratórium és diplomatervezés

Az önálló laboratórium és a diplomaterv témák tipikusan a CrySyS Lab kutatás-fejlesztési tevékenységéhez kapcsolódnak, vagy külső ipari partner által javasolt feladatok, s ezáltal lehetőséget teremtenek a hallgatóknak a labor kutatási és ipari fejlesztési munkáiban történő részvételre, illetve az ipari partnerekkel történő együttműködésre. Lehetőség van saját hozott témán is dolgozni, amennyiben annak témavezetését a CrySyS Lab valamelyik munkatársa elvállalja.

Szakmai gyakorlat, ipari kapcsolatok

A CrySyS Lab számos olyan ipari céggel áll kapcsolatban, melyek az IT biztonsághoz kapcsolódó tevékenységet végeznek, és melyek szívesen fogadnak hallgatókat szakmai gyakorlatra.

Ajánlott választható tárgyak

- Számítógépes rendszerek biztonságos üzemeltetése (VIHIAV43)
- Privacy-Preserving Technologies (VIHIAV35)
- Security and Privacy: an Economic Approach (VIHIAV34)
- Kriptográfia (VIHIAV30)

Mentoráció

A CrySyS Lab számára kiemelten fontos a hallgatók mentorálása, amely kiterjed az önlab, szakdolgozat és diplomaterv projektek témavezetésére, valamint számos további tevékenységre is. A soft skills tréningjeinken (7 alkalom, kéthetente) megtanítjuk, hogy hogyan indíts el sikeresen egy projektet, menedzseld jól az idődet, tarts hatékony megbeszéléseket, írj profi projekt riportot vagy műszaki dokumentumot, valamint tarts hiteles szakmai előadást. A heti rendszerességű CrySyS Student Cloud mentoring foglalkozásainkon elmélyedhetsz továbbá olyan szakmai témakörökben is, mint a binárisok exploitálása, reverse engineering vagy az AI biztonság gyakorlati oldala. Lehetőség van csatlakozni CTF versenyekhez, ezzel is erősítve a szakmai elmélyülést és a csoportos problémamegoldást. Ezen felül számos önismereti témakört is feldolgozunk ezeken az alkalmakon, melyek felvérteznek az élet kihívásaira.

Specializációfelelős

Dr. Buttyán Levente, egyetemi tanár

BME Hálózati Rendszerek és Szolgáltatások Tsz.
CrySyS Adat- és Rendszerbiztonság Laboratórium

e-mail: buttyan@crysys.hu
tel: +36 1 463 1803

CrySyS Lab

A CrySyS Adat- és Rendszerbiztonság Laboratórium elkötelezett a nemzetközi színvonalú oktatás és kutatás mellett az IT biztonság területén. A laboratórium szakértői tevékenységgel és hallgatók mentorálásával is foglalkozik. A kutatás fókuszában a hálózatba kötött beágyazott rendszerek biztonsága, a mesterséges intelligencia biztonsági kérdései, és a biztonság közgazdaságtana áll. A laboratórium kiemelkedő korábbi eredményei közé tartozik a Duqu malware felfedezése és első részletes elemzése, a !SpamAndHex hallgatói CTF csapat DEFCON CTF döntőbe jutása (3 alkalommal is), az első Raspberry Pi-n is futó antivírus megoldás, a SIMBIoTA kifejlesztése, és számos kiemelkedő tudományos eredmény. A laboratóriumból több spin-off cég is indult, többek között a Tresorit, az Ukatemi Technologies, és az Avatao. További információ elérhető a CrySyS Lab weboldalán: www.crysys.hu

www.crysys.hu