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)

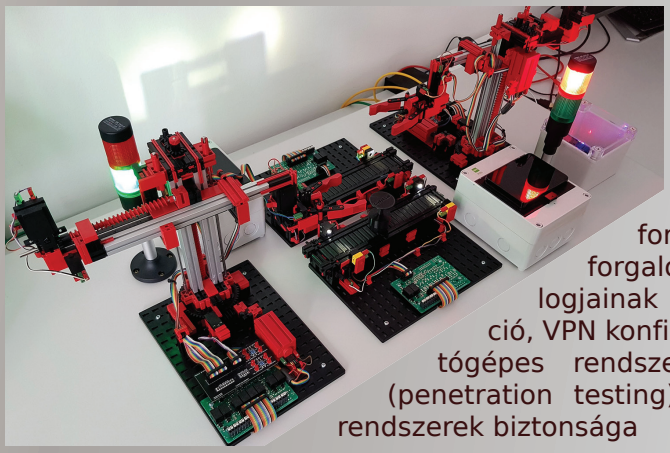
döntések manipulációja, tanító adat mérgezése, hátsó kapuk és trójaiak ML modellek ellen, tanító adat rekonstrukciója, modell-lopás, modellek megmagyarázhatóságának támadása

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)

Tehetséggondozás

A CrySyS Lab minden évben megrendezi a CrySyS Security Challenge nevű egyetemi hacker versenyt. A versenyen jól szereplő hallgatók meghívást kapnak a CrySyS Student Core nevű diákkörbe. A Student Core tagjai rendszeresen találkoznak, az IT biztonsággal kapcsolatos témákat dolgoznak fel, vitatnak meg, és nemzetközi hacker versenyekre készülnek. A Student Core hacker csapatai a !SpamAndHex és a c0r3dump számos versenyen értek el kiemelkedő eredményt. A Student Core-ba való bejutás segítésére IT Security Bootcamp névvel felkészítést tartunk, erről a lehetőségről érdeklődni a CrySyS Lab vezetőjénél lehet.

Specializáció felelős

Dr. Buttyán Levente, egyetemi tanár

BME Hálózati Rendszerek és Szolgáltatások Tanszék,
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, kutatás, és szakértői tevékenység mellett az IT biztonság területén. A laboratórium jelenlegi fő kutatási területe a kiber-fizikai rendszerek biztonsága. A laboratórium szakértői tevékenységet is végez ipari partnerei számára, mely főleg biztonsági teszteléseket és incidens kezelési feladatok megoldását jelenti. A laboratórium munkatársai fedezték fel és analizálták először a Duqu kémprogramot, és ők publikáltak először a Flame, a MiniDuke és a TeamSpy kártevőkről. A laboratórium részvétele különböző nemzetközi K+F projektekben intenzív és sikeres, publikációs tevékenysége kiemelkedő, szakértői tevékenysége pedig széles körben elismert. 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

Tanszéki tájékoztató

ideje: **2024. május 7., 13:00-17:00**
helye: **IB. 110.**

www.crysys.hu