IT biztonság mellékspecializáció

MSc Mérnökinformatikus szak

Célkitűzés

Az IT biztonság mellékspecializáció célja, hogy megismertesse a hallgatókkal az IT rendszerek biztonsággal kapcsolatos problémáit és az azok megoldására alkalmazott korszerű módszereket és technológiákat. A mellékspecializáció a hangsúlyt a praktikus alkalmazásokra fekteti, ám azok részletes elemzésén keresztül a hallgatók betekintést nyernek az analízis módszerek és a tervezés kérdéseibe is. Olyan mérnök-informatikusok képzésére törekszünk, akik képesek a modern IT rendszerekben felmerülő biztonsági problémák azonosítására, feltárására, a problémák megoldásához szükséges praktikus tervezési és fejlesztési feladatok elvégzésére, valamint a mélyebb elméleti alapokra (pl. kriptográfiára) épülő módszerek és rendszerek megértésére és alkalmazására.

Illeszkedés a főspecializációkhoz

A biztonság ma az egyik fő kihívás az információs rendszerekben, a kommunikációs hálózatokban és a beágyazott rendszerekben. Legyen szó akár felhő alapú szolgáltatásokról, mobil platformokról, az Internetről és a Webről, közösségi alkalmazásokról, vezeték nélküli hálózatokról, ipari folyamatirányítási rendszerekről, vagy a tárgyak internetéről (IoT), nap mint nap hallhatunk az ezekkel kapcsolatos biztonsági problémákról, az újabb és újabb sérülékenységekről és az ezeket kihasználó sikeres támadásokról. Ezért az IT biztonság mellékspecializáció nagyszerű kiegészítője lehet bármelyik főspecializációnak. Az IT biztonság mellékspecializáció olyan hozzáadott értéket biztosít, mely egyedivé és keresetté teszi az itt végző hallgatókat bármely főspecializáció által képviselt szakmai területen.

https://www.hit.bme.hu/page/68

HIT
HÁLÓZATI RENDSZEREK
ÉS SZOLGÁLTATÁSOK
TANSZÉK

Szaktárgyak

A szaktárgyak gyakorlat-orientáltak, és minden tárgynak vannak házi feladatai is, melyeket az avatao on-line gyakorló platformon (www.avatao.com) kell megoldani.

Biztonsági protokollok (VIHIMA05)
kriptográfiai primitívek és alapprotokollok, véletlenszám-generálás, kulcscsere protokollok, publikus kulcs infrastruktúra, biztonságos kommunikációs protokollok (TLS, Wi-Fi biztonság), biztonsági protokollok erőforrás -korlátozott környezetben és felhő alapú rendszerekben, anonim kommunikációs rendszerek

Számítógép-biztonság (VIHIMA06)
jogosultságok és hozzáférés-védelem, memória-korrupció (stack és heap overflow, integer overflow, DEP, ASLR, return-to-LibC, ROP), biztonságos szoftverek fejlesztése, rosszindulatú szoftverek (malware), browserek biztonsága, mobil platformok biztonsága (Android, iOS), virtualizáció biztonsága, bontásellenálló eszközök, incidenskezelés

Hálózatbiztonság (VIHIMB00)
hálózati behatolási módszerek (ethical hacking), tűzfalak, behatolást detektáló rendszerek (IDS/IPS), logelemzés, honeypot-ok alkalmazása, hálózati infrastruktúra biztonsága, botnet-ek, spam és DDoS, webes rendszerek biztonsága, vállalati hálózatok biztonsága, ipari és beágyazott hálózatok biztonsága, privátszféra védelme a weben és közösségi hálózatokban

Mérés labor

IT biztonság laboratórium (VIHIMB01)
jogosultságkezelés, szoftver implementációs biztonsági rések vizsgálata, malware analízis, hálózatok és webes rendszerek biztonsági ellenőrzése (ethical hacking), hálózati forgalom analízise lehallgatással, tűzfal és IDS konfigurációja, PKI és elektronikus aláírás, Internet-of-Things (IoT) biztonság

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.

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

- Biztonságos szoftverfejlesztés (VIHIAV33)
- Programok visszafejtése és védelme (VIHIAV05)
- Számítógép hálózatok biztonságos üzemeltetése (VIHIAV14)
- Személyes adatok védelme (VIHIAV35)
- Security and Privacy: an Economic Approach (VIHIAV34)
- Kriptográfia (VIHIAV30)
- Biztonság a gépi tanulásban (VIHIAV45)

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 korábbi és jelenlegi hackercsapata, a !SpamAndHex és a c0r3dump, számos versenyen ért el kiemelkedő eredményt. A Student Core-ba való bejutás segítésére az IT Security Bootcamp témalabor keretében tartunk felkészítést az őszi félévekben. A legmotiváltabb hallgatók felvételt nyerhetnek a tanszék PARIPA-programjába. A három féléves hallgatói képzési és ösztöndíjprogram keretében a hallgatók versenyképes K+F problémák megoldásában szereznek értékes tapasztalatokat az ipari partnereinknél tanszéki és ipari témavezető felügyelete alatt, illetve a gyakorlati munkához szükséges szakmai ismereteken túl „soft skill”-képességeiket is fejleszthetik.

Mellékspecializáció-felelős

Dr. Buttyán Levente, docens

BME Hálózati Rendszerek és Szolgáltatások Tanszék,
CrySyS Adat- és Rendszerbiztonság Laboratórium

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

www.crysys.hu

CrySyS Lab

A CrySyS Adat- és Rendszerbiztonság Laboratórium elkötelezett a nemzetközi színvonalú oktatás és kutatás mellett az IT biztonság területén. A laboratórium jelenlegi fő kutatási területe a kiber-fizikai rendszerek biztonsága, ezen belül az ipari folyamatirányítási rendszerek, az IoT, és más beágyazott rendszerek biztonsága. Kiemelt kutatási terület még a gépi tanulás biztonsága és a biztonság közgazdasági megközelítése. A laboratórium legjobban talán arról ismert, hogy 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

Várunk benneteket a HIT-es tanszéki tájékoztatóra.
Időpont: május 9, hétfő, 16-17 óra,
helyszín: IB 110.
Nézd meg a specializációnkat bemutató prezentációt itt:

www.crysys.hu

www.hit.bme.hu