MTA SZTAKI

Hálózatbiztonsági és Internet Technológiák Osztály

Vezető
Rigó Ernő

Telefon:
+36 1 279 6266

E-mail:
rigo.erno@sztaki.mta.hu

Cím:
H-1111 Budapest, Lágymányosi u. 11.

Web:
hbit.sztaki.mta.hu

BEMUTATKOZÁS

Részlegünk fejlesztési tapasztalatai az 1970-es évekre nyúlnak vissza. Az elmúlt négy évtized során számos hálózati architektúra, valamint szoftver- és hardvertechnológia jelent meg, terjedt el – majd némelyik fokozatosan elavult és el is tűnt. A kezdetleges gép-gép kommunikáció első napjait, majd az Internet megjelentését és széleskörű elterjedését követve új, összekapcsolt korszakba lépünk, melyben soha nem látott mennyiségű felhasználót, eszközt és információt kell kezelhetővé és biztonságossá tennünk.

FŐBB K+F IRÁNYOK

Fontosabb K+F irányok:

- autentikációs és jogosultsági infrastruktúrák (attribútum- és azonosító szolgáltatások)
- felhő infrastruktúrák menedzsmentje és biztonsága (OpenStack, OpenNebula)
- hálózatbiztonsági felügyeleti rendszerek, elosztott hálózati érzékelők
- automatikus és fél-automatikus hálózat-megfigyelés, helyzeti tudatosság
- speciális célú hálózati eszközök
- IT biztonság menedzsment és értékelési módszertanok (CobIT, ISO27k, OWASP)
- hálózatbiztonsági incidenskezelés és menedzsment

Kihívások: Az új technológiák aktív fejlesztése és alkalmazása során számos, a számítógépes rendszerek kezelésével és információbiztonságával kapcsolatos alapvető, általánosan felmerülő problémát azonosítottunk. Csoportunk az ezekkel kapcsolatos kulcsfontosságú területekre összpontosítja kutatási, vizsgálati és fejlesztési tevékenységét. Végső célunk, hogy szolgálatkész internetes technológiákat és biztonságosabb hálózati rendszereket eredményező, fejlett technológiákat hozzunk létre.

Megoldások: A szakmai kihívások gyakorlati megközelítésekor az eltérő megoldási lehetőségek, szabályok és folyamatok tényezőinek és hatásainak feltárására törekszünk. Saját tesztkörnyezeteinkben végzett, részletes vizsgálataink során, az egyes alternatív technológiák integrációs lehetőségeinek felmérése mellett, gondosan megtervezett méréseket is végzünk. Mérnöki-tudományos kutatói megközelítésünk elősegíti a problémák mélyebb megértését, így teremt stabil alapot tervezési, fejlesztési és szolgáltatási tevékenységünk számára.

Implementáció: Megvalósítási tevékenységünk során, befektetett erőforrásaink gyors megtérülésének érdekében, fejlett technológiai ismereteinket hatékony, agilis fejlesztési módszerekkel kombináljuk. Belső folyamatainkat, termékeinket és szolgáltatásainkat folyamatosan felülvizsgáljuk és fejlesztjük. Előszeretettel alkalmazunk nyílt szoftvereket, nyílt hardvereket és nyílt protokollokat, azonban számos iparág vezető termék, technológia és környezet tekintetében is kiterjedt tapasztalattal rendelkezünk.

IPARI MEGOLDÁSOK

HEXAA (www.hexxa.eu) - mint szoftverfejlesztési eredmény egy alapvető hiányosságot pótol azzal, hogy lehetőséget teremt szabványosan, hiteles attribútumok biztosítására alkalmazásoknak kutatóhálózati azonosítási föderációkban, mint amilyen a hazai eduID, illetve a nemzetközi eduGAIN.

Hun-CERT - Részlegünk több mint egy évtizede üzemelteti a Hun-CERT (www.cert.hu) hazai hálózatbiztonsági incidenskezelő szolgáltatást. Az incidens-feltárási- és kezelési szolgáltatás mellett nemzetközi kapcsolatokat is fenntartunk. Elsődleges feladatunk a hazai internetes hálózat robusztusságának és a hazai internet felhasználók biztonságtudatosságának növelése.

REFERENCIÁK

- Internet Szolgáltatók Tanácsa
- Fővárosi Szabó Ervin Könyvtár
- MATEHETSZ – www.tehetseg.hu
- Magyar Tudományos Művek Tára
- MVM Paksi Atomerőmű
- NIIFI
- GEANT
- BOSCH

MUNKATÁRSAK

Részlegünkön jellemzően 15 fő, korszerű technológiákban naprakész mérnök-informatikus és mérnökjelölt munkatárs dolgozik. Munkánk során az idősebb kollégák tapasztalatára gyakran támaszkodunk, ám emellett hangsúlyt fektetünk az informatikai szakértők friss generációinak kinevelésére és foglalkoztatására is. Számos kollégánk több nemzetközileg elismert szakmai minősítéssel (CCNA, CCNP, CISSP, CISA, CEH) rendelkezik.

JELENTŐSEBB K+F PROJEKTEK

Adat Dióda - Létfontosságú és egyéb biztonságkritikus létesítmények esetén a jogosulatlan hálózati forgalom megakadályozása kiemelt prioritású. Eszközünk segítségével szokványos informatikai szolgáltatások (E-mail, FTP, HTTP), fizikailag garantált egyirányú adatforgalom mellett is használhatók.

ASTOR - A kutatási projekt célja az egyes szervezetek hálózatán fellépő biztonsági események és kockázatok automatikus elemzését és értékelését támogató kísérleti eszközkészlet kifejlesztése volt. Az eszközök adaptív, autonóm és felügyelő tanulási mechanizmusai a piacon akkor elérhető eszközöknél jobb riasztási hibaaránnyal rendelkeztek.

DBpedia Spotlight Live szolgáltatásunk segítségével új Wikipédia szócikkek azonnali elemzésére nyílik lehetőség. A projekt során kifejlesztett UIMA adapter és OpenLibrary eszköz az Apache Stanbol projektet egészíti ki.

Net-Sensor - A kutatási projekt keretében létfontosságú infrastruktúrák védelmét szolgáló korai figyelmeztető rendszer prototípusát dolgoztuk ki. A rendszer alhálózatok teljes forgalmának valósidejű elemzésére és felügyeletére alkalmas, a normál adatfolyam megszakítása nélkül. A visszaállított adatfolyamok folyamatos elemzésével a megfigyelt rendszerek biztonsági állapotáról valósidejű információ áll rendelkezésre.