Üzemirányító rendszerek üzembiztonsága szeminárium

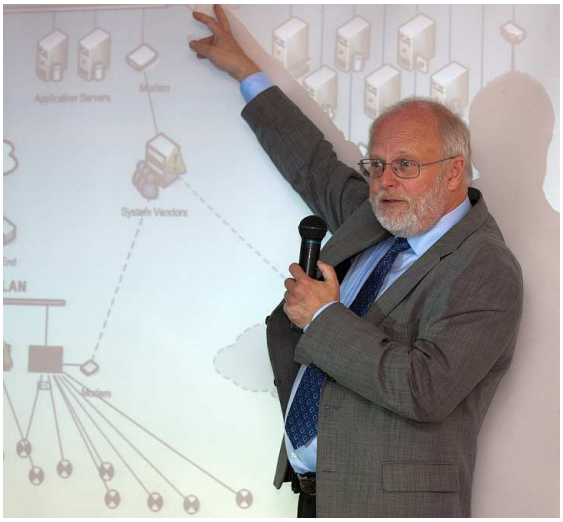
A MEE Energetikai Informatikai Szakosztály (EISZ) és az Astron Informatikai Kft. 2011. október 12-én az üzemirányító rendszerek üzembiztonsága témájában szemináriumot tartott. A szeminárium jelentős szakmai érdeklődés, „telt ház” mellett zajlott. Külön öröm, hogy a rendezvényen a szorosan vett villamos üzemirányítás szakemberei mellett más, az üzemirányító rendszerek maximális biztonságában érintett szakterületek is képviseltették magukat.

A rendezvény apropóját az adta, hogy a zavartalan villamosenergia-ellátás egyre nagyobb mértékben függ a számítógépes üzemirányító rendszerek folyamatos rendelkezésre állásától, megfelelő működésétől. Ezekben a korábbi zárt kommunikációs kapcsolatok és folyamatirányító architektúrák helyét fokozatosan veszik át az olyan nyilvános rendszerekben is használatos megoldások, mint az internet protokoll, a web-alapú megjelenítés, vagy a nagykiterjedésű hálózatok. Így a kritikus infrastruktúrák üzemirányítóinak idővel a publikus rendszereknél már "megszokott" IT biztonsági fenyegetésekkel kell szembesülniük. A védekezés első lépése a cyber-támadások hatásmechanizmusának, következményeinek megértése lehet. A szeminárium ebben kívánt segítséget nyújtani átfogó képet adva a témában indított nemzetközi információ-biztonsági projekt (VIKING) eredményeiről éppúgy, mint az amerikai Idaho National Laboratory éles támadásokat elemző tréningjéről.

A rendezvényt **Görgey Péter**, az EISZ elnöke nyitotta meg. Jelezte, hogy a szakosztály hangsúlyos célja a szakirányú hazai vállalkozások támogatása és a nemzetközi legjobb gyakorlatok bemutatása. Örömét fejezte ki, hogy a rendezvény mindkettőre egyszerre ad módot. Elemi érdeknek nevezte az üzemirányító hálózatok, ezzel az általuk irányított folyamatok, szolgáltatások üzemének a bármilyen – szélsőséges esetben terrorista – szándékkal való megzavarása elleni minden eszközzel és a legszélesebb nemzetközi összefogással történő fellépést.

Görgey Péter

A bevezetőt követően elsőként **Gunnar Björkman** (VIKING project manager) ”VIKING, A Security Project for the Protection of Vital Infrastructures” címmel tartott előadást. Az előadó a villamos hálózatok üzemirányító rendszereinek rövid áttekintését követően e rendszerek biztonsági kérdéseire fókuszált. Bemutatta az e rendszerek biztonsági aspektusainak vizsgálatára európai együttműködésben megindított VIKING projektet. Ismertette azt a modellt, amelyet a project az üzemirányító rendszerek biztonságnövelése kapcsán alkalmaz, továbbá bemutatta azt a virtuális „város szimulátort” (ViCiSi – Virtual City Simulator), amely az üzemirányító rendszerek elleni támadások miatti zavarok kritikus infrastuktúrákra gyakorolt sokirányú (közte költség-) hatásainak a modellezésére hivatott. A VIKING projekt az ABB és az EU együttműködésében 2008. novemberében indult úgy, hogy ahhoz tovább cégek (E.ON, Astron, MML Analysis & Strategy) is csatlakoztak. A projektet egyetemek (a svéd Royal Institute of Technology, a svájci ETH Zurich, valamint az amerikai University of Maryland) is támogatják. A projekt becsült költsége mintegy 2.6 millió €, melyből mintegy 1.8 millió € az EU hozzájárulás.



Gunnar Björkman

Ezt követően **Dr. Dán György**, a Stockholmi Királyi Műszaki Egyetem docense tartott előadást „A SCADA állapotbecslés biztonsági vonatkozásai” címmel. Az üzemirányító rendszerek alapvető funkcióinak az áttekintését követően az előadó a hibás adatok detektálásának a lehetőségeivel foglalkozott hangsúlyosan. Bemutatta az üzemirányítás alapjául szolgáló folyamatadatok megváltoztatásával megvalósuló támadások lehetséges fajtáit, helyeit, a támadások felismerési, elhárítási lehetőségeit. Míg az ún. naív támadás könnyen felismerhető, addig az ún. lopakodó (nagy rendszer- és szakismeretet, ráfordítást) igénylő támadások elleni védekezés komoly erőfeszítéseket igényel. Az előadó bemutatta e védelem matematikai modellezési alapjait. Az előadás kitért az adatátviteli hálózatra, mint amelynek támadása éppúgy meg tudja zavarni az üzemirányítás működését, mint annak közvetlen támadása. Végül bemutatta a támadhatósági vizsgálat általuk, a stockholmi egyetemen kialakított keretrendszerét.

Dr. Dán György

Bakos Béla, a MAVIR Zrt. alkalmazás szolgáltatási osztályvezetője „Folyamatirányító rendszer IT támadása „élesben”” címmel számolt be az Idaho Falls-ban tartott nemzetközi biztonsági tréningről, melyen módja volt részt venni. Először sorra vette az elmúlt évek nagyobb, ismertebb fenyegetéseit, támadásait (2007, Észtország; 2008, Grúzia-Oroszország; 2010, Stuxnet; 2011, Mitsubishi Heavy Industries) és azok alapvető jellemzőit, tanulságait. Ismertette, hogy a tréning célja a fenyegetések, tényleges támadások, a támadó és védekező eszközök megismerése volt. A tréning keretében a két csoportra (támadók és védők) osztott résztvevők egy e célra kialakított hálózati modellen „küzdöttek meg” egymással, az élvonalbeli informatikai támadó és védekező eszközök igénybevételi lehetősége mellett. A védőknek nem csak az IT védelem volt a dolga, hanem az általa felügyelt technológia (adott esetben egy „vegyigyár”) üzemének a fenntartása. Különösen elgondolkodtatóak voltak az előadónak a tréning alapján levont egyes végkövetkeztetései (pl. internetről letölthető eszközökkel már 1-2 nap tanulás után „eredményeket” lehet elérni; nincs feltörhetetlen rendszer; ipari protokollok sem jelentenek plusz védettséget).

Bakos Béla

Ezt követően **Gaál Róbert**, az Astron Informatikai Kft. üzletág igazgatója „VIKING projekt tesztalkalmazás (Test-bed)” címmel tartott előadást. Előadása bevezetőjében röviden bemutatta az informatika térhódításának folyamatát a villamosenergia-rendszerek üzemirányításában, melynek eredményeként napjainkban a hackerek már a villamosenergia-szolgáltatást is megzavarhatják. A Test-bed, amely egy képzeletbeli ország (Vikingia) villamosenergia-rendszerét modellezi, a hacker támadások villamosenergia-ellátásra gyakorolt hatásainak szimulációját végzi. A tesztalkalmazás, mely az erőművektől kezdve az átviteli hálózaton át a főelosztó és elosztó hálózaton keresztül a fogyasztókig követi az energia útját, több szimulátor és egy rendszerirányító SCADA rendszer laza összeintegrálásából született meg. Képes a hackerek által okozott kiesések valósághű szimulációjára és végeredményként az általuk okozott közvetlen és közvetett anyagi kár nagyságát is szolgáltatja.

Gaál Róbert

Fodróczi Csaba (Astron Informatikai Kft.) „VIKING biztonsági esettanulmányok” címmel tartott előadást. Az előadás első részében bemutatásra került, hogy a VIKING projekt kereteiben mit is jelentenek az esettanulmányok (történet és műszaki forgatókönyv), hogyan épülnek fel, és milyen megkötéseket alkalmaznak a biztonsági vizsgálatokkor (fizikai támadások és social engineering korlátozása). Az első esettanulmány történetében a támadást egy jól szervezett „terrorista” csoport hajtja végre. Céljuk az átviteli hálózat megbénítása, célpontjuk a SCADA rendszerben megvalósított automatikus kapcsolási sorrendek. A kártékony kódot egy preparált pendrive segítségével juttatják a SCADA rendszerbe, ahol az, előre megadott időpontban tömeges megszakító kikapcsolásokat hajt végre két lépcsőben, megnehezítve a kárelhárítást. A vizsgált esetben a „siker” esélye magas, ennek csökkentésére két alapvető intézkedést javasol. Ezt követően további négy esettanulmány kerül röviden bemutatásra. Különösen elgondolkodtató volt, hogy bár az esettanulmányok a képzelet szüleményei, a felvetett problémákra nem volt nehéz ráismerni a gyakorlatból.

Fodróczi Csaba

A szemináriumot **Dr. Kovács Attila** ügyvezető igazgató (Astron Informatikai Kft.) „EU-s K+F projekt tapasztalatok egy magyar résztvevő szemszögéből” című előadása zárta. Bemutatta a projekt igen kedvező pályázati jellemzőit, úgymint támogatási arány, adminisztrációs kötelezettségek, a tender eljárás során szükséges pályázati ráfordítások. Részletesen ismertette a létrejövő műszaki-tudományos eredmények publikációjának módját és fórumait is.

Dr. Kovács Attila

Az előadásokat követően az Astron Informatikai Kft. ebéden látta vendégül a szeminárium résztvevőit.