Papp Attila (Kürt Zrt.)

BIZTONSÁGI MEGOLDÁSOK INTEGRÁCIÓJA

„A biztonsági fenyegetettségek sokrétűsége számos különböző védelmi mechanizmus egyidejű működését kívánja meg, ugyanakkor a hatékony védelem szükségessé teszi ezen mechanizmusok együttműködését és integrálását is.”

Az utóbbi évek, évtizedek során alapvetően változott meg a biztonsággal kapcsolatos vélekedés. Ma már természetes, hogy a legkülönbözőbb élethelyzetekben merül fel a biztonság és a kockázatarányos védelem kérdése, a közlekedéstől, a személyes adatok védelmén keresztül egészen a banki adatkezelésig. A szervezeteknek ma már nem jó termékekre van szükségük, hanem biztonságra. Nem biztonsági eszközöket akarnak, hanem biztonságos működést, nem riasztókat, hanem betörésmentes infrastruktúrát, nem vírusirtót, hanem vírusmenetes működést. Ezt az állapotot elérni csak megfelelő integrált biztonsági megoldások alkalmazásával lehet. Egy szervezetnél ma már rengeteg különböző – fizikai, informatikai és szervezeti – biztonsági megoldást alkalmaznak. Ezeknek az önállóan működő megoldásoknak az adattartalma együttesen igen nagy érték…

Manapság a szervezetek legnagyobb részénél az informatikai és a biztonságtechnikai rendszerek még két különálló hálózaton működnek. Ennek megfelelően az informatikai üzemeltetők és a biztonsági üzemeltetői csapatok is elkülönülnek egymástól. Miután azonban a biztonságtechnikai rendszerek egyre inkább átköltöznek az IP alapú hálózatra, várhatóan mind a két rendszer üzemeltetése, karbantartása, fejlesztése egy kézbe, a szervezet informatikai szervezetéhez kerül. A biztonságiak feladatai magára a megfigyelésre, az őrzés-védésre, a beléptetésre szorítkoznak majd. Ezzel minden szervezet egyértelműen csak jobban járhat, hiszen minden érintett szakterület csak azzal foglalkozik, amihez valóban ért. Következésképpen a teljes szervezet fenyegetettségei is mérsékelhetők ill. a biztonsági szint javítható. Az integrált biztonsági rendszer attól lesz intelligens, hogy a különböző biztonsági rendszerek nemcsak megvannak egymás mellett, hanem össze vannak kapcsolva, összehangoltan működnek. Az esetek nagy részében ezt az összehangolást még emberek végzik. Csakhogy tudható: az ember rossz abban, amiben a számítógép jó. Az ember a monoton, ismétlődő dolgokat nem tudja lankadatlanul és hibátlanul figyelemmel kísérni. A számítógép nem gondolkodik. Ha egyszer az a feladata, hogy mindenkit azonosítson, akkor csak annak fog kaput nyitni, aki – megfelelő módon – azonosította magát. Nem lehet rábeszélni semmire, nem megy el elszívni egy cigarettát, nem is kávézik. Célszerűnek látszik tehát valamiképpen automatizálni minden olyan biztonsági megoldást, amit csak lehet.

Biztonsági megoldások integrációja

Az elosztott intelligenciájú integrált biztonsági rendszerek elsősorban ott érhetnek el jelentős biztonsági szint növekedést, ahol nagy számú különböző érzékelő működik egyidejűleg. Tipikusan ilyenek lehetnek a nagyvállalatok telephelyei, a pénzintézetek, a repülőterek és kikötők, a bevásárlóközpontok, az államigazgatási intézmények és kormányhivatalok, valamint a meghatározó infrastrukturális szolgáltatók (elektromos áram, vezetékes gáz, víz, távhő, telefon). Ahol sok telephely/helyiség egyidejű megfigyelése a feladat, ott jelentős mértékben segíthetik a biztonsági szervezet tevékenységét az elosztott intelligenciával rendelkező integrált biztonsági megoldások.
Egy integrált biztonsági rendszer megtervezésekor, telepítésekor és bevezetésekor magától értetődő kérdés, hogy mindez mekkora költségnövekedéssel jár a szervezet számára. Kétségtelen tény, hogy az integrált biztonsági megoldások drágábbak a hagyományos biztonságtechnikai eszközöknél, azonban a tapasztalatok azt mutatják, hogy nem lehet a kétféle megoldást, illetve a segítségükkel elérhető biztonsági szintet összehasonlítani, hiszen nem ugyanazt a minőséget nyújtják. Az integrált rendszerek üzemeltetése lényegesen olcsóbb, mint a hasonló funkcionalitást nyújtó független biztonsági megoldásoké, így mindezzel jelentős idő és költség takarítható meg. Az elosztott intelligenciával rendelkező, öntanuló biztonsági rendszerek alkalmazásával csökkenthető a felügyelő személyzet létszáma, a biztonsági vezetőknek lehetőségük van a védelmi szolgálat rugalmasabb szervezésére, így azonos létszámú személyzettel több feladat látható el, magasabb szinten.

Az integrált biztonsági rendszer koncepciója

A technikai fejlődéssel párhuzamosan az intézmények, gazdasági szervezetek életében egyre fontosabb szerepet tölt be, egyúttal növekvő értéket képvisel a tárolt adatok, dokumentumok formájában megjelenő, tárgyalások, telefonos megbeszélések során elhangzó, vagy konkrét termékekben, prototípusokban megtestesülő információ. Az információ egy vagyonelem, és ugyanúgy, mint más vagyonelemeknek, jelentős értéke van a szervezetben. Az információ minden formája hordozhat értéket, amelyet védeni kell a – szándékos károkozás, vagy valamilyen véletlen esemény hatására bekövetkező – illetéktelen kezekbe kerüléstől, vagy az elvesztéstől, esetleg használhatatlanná válástól.

Az intézmények, vállalkozások és magánszemélyek pótolhatatlan, gyakran felbecsülhetetlen értékű adatokkal, információkkal rendelkeznek, a használt és kezelt információk köre és értéke évről évre nő. A szervezetek információs rendszerei és hálózatai egyre inkább szembekerülnek a biztonságukat fenyegető veszélyek széles skálájával, beleértve a számítógépes csalásokat, a kémkedést, a szabotázst, a szándékos visszaéléseket, a vandalizmust, a tűzeseteket, az árvizet, illetve más

környezeti fenyegetettségeket, és igen nagy részük használ is különféle eszközöket, megoldásokat védelmi, megelőzési céllal. Lényegesen kevesebb azonban azoknak a száma, akik valamennyi fenyegetést, illetve a kockázatokat figyelembe véve rendszerbe foglalják, és annak megfelelően a működést/működtetést szabályozva alkalmazzák azokat. Kutatási eredményeink eddigi tapasztalatai megerősíteni látszanak azt a feltételezést, hogy jelenleg még nincs valódi együttműködés a különböző biztonsági területek között. A saját területén mindenki jól és eredményesen dolgozik, de nem csatolják vissza egymás számára az információkat. Ezzel párhuzamosan – az eleinte az orwelli látomás eszközének tekintett – integrált biztonsági megoldások sem keltenek már különösebb visszhangot – úgy tűnik tehát, a közhiedelemmel ellentétben, hogy az emberek legnagyobb része hajlandó a privát szféra részleges feláldozására a biztonsága érdekében.

A biztonsági rendszerek bonyolultsága mára összemérhetővé vált más komplex ipari rendszerekével. Ugyanakkor a biztonsági rendszerek tervezéséhez nem állnak rendelkezésünkre olyan, matematikailag megalapozott, bizonyítható eredményt szolgáltató módszertanok, mint például ipari termelő folyamatok szintézisére. Így erősen megkérdőjelezhető, hogy az ügyfél a számára legjobb, legbiztonságosabb, legmegbízhatóbb megoldást kapja-e. Ez elsősorban onnan ered, hogy az integrált biztonsági rendszer kialakítására nem létezik egyféle, mindenre jó megoldás, hanem átfogó módon, a szabályozástól kezdve egészen az adott infrastruktúrához és szervezeti felépítéshez illeszkedően kell a megfelelő biztonsági szintet és a kockázatarányos védelmet megteremteni.

A különböző biztonsági megoldások (fizikai, logikai, szervezeti/humán) területén az a bevett gyakorlat, hogy egy-egy adott célcsoport a veszélyelemzés alapján feltárja a lehetséges fenyegetettségek, illetve támadások körét és ezekre szinte egymástól függetlenül alkalmaz biztonsági/védelmi megoldásokat. Ezek a védelmi intézkedések közvetlenül a rendszerelemekhez kapcsolódnak és általában semmi kapcsolatuk nincs egymással. Lényegesen magasabb biztonsági szintet érhetünk el – a költségoldal csökkentése mellett, ha az összes fenyegetésnek kitett rendszerelemet úgy látjuk el a kockázattal arányosan kiépített védelemmel, hogy megvalósítjuk e rendszerek közötti kapcsolatot is, hiszen ebben az esetben jelentős szinergikus hatással számolhatunk. Egy ilyen komplex rendszer esetén számos olyan új elvárás is megfogalmazható, amely a korábbi rendszerek esetében fel sem merülhetett.

A biztonsági fenyegetettségek sokrétűsége ugyanakkor számos különböző védelmi mechanizmus egyidejű működését kívánja meg, miközben a hatékony védelem szükségessé teszi ezen mechanizmusok együttműködését és integrálását is. Az integrált biztonsági megoldások kidolgozásának alapkoncepciója az, hogy az egyedi, egyes

részterületeket érintő, sürgető problémákra adott megoldások a legtöbb esetben nem nyújtják azokat az előnyöket, amelyeket a nagyobb területekre összpontosító, komplex, a kockázatokkal arányos megoldások nyújtanak, mivel külön-külön a feltárt problémák kis csoportját képesek csak lefedni. A KÜRT eddigi kutatási eredményei azt látszanak igazolni, hogy összetett biztonsági kérdések esetén a tapasztalat és az emberi intuíció önmagában már nem elég a legjobb, leghatékonyabb megoldás megtalálására, hanem ehhez szisztematikus és bizonyítható eljárásokon nyugvó módszertanra van szükség. A gyakorlati életben ez azt jelenti, hogy minél fáradtabb a biztonsági őr, annál többet téveszt. Intelligens megfigyelő rendszerekkel és a hozzájuk kapcsolódó integrált biztonsági megoldásokkal növelhető a biztonság és tehermentesíthető a személyzet.

Az integrált biztonsági módszertanok és eszközök alkalmazásának célja, hogy a különböző szervezetek működésében található biztonsági réseket azonosítva, azokra kompakt termék és szolgáltatás csomagokkal megoldásokat nyújtson egy egységes és egyenszilárdságú körkörös védelmi vonalat létrehozva, amely optimalizálja és hatékonyabbá teszi a szervezetek védelmi rendszerét. A biztonságtechnikai megoldások alkalmazásának célja megakadályozni az információkhoz, eszközökhöz és erőforrásokhoz való jogosulatlan hozzáférést, a károkozást és a szervezet helyiségeibe való illetéktelen behatolást. A biztonságtechnikai megoldások kialakítása során alapkövetelmény, hogy a nyújtott védelem arányos legyen a megállapított kockázatokkal.

Az adatok integritását, a vírus- és számítógépes behatolás-védelmet és titkosítási eljárásokat is magában foglaló **logikai biztonság**; a beléptetést, szünetmentes energiaellátást, térfigyelést, tűz- és vízkár-elhárítást egyesítő **fizikai biztonság**; valamint a belső csalások, visszaélések, szándékos és vétlen károkozások megelőzését szolgáló **szervezeti (humán) biztonság** integrálása jelentősen csökkenti a szervezetek biztonsági kockázatait. Az integrált biztonsági rendszer üzemeltetésével lehetővé válik a kockázatok egységes értékelése és kezelése, az eltérő fenyegetettség-típusokkal szemben homogén védelmi szinttel rendelkező rendszer kialakítása, a szűk keresztmetszetek és párhuzamosságok kiküszöbölése, illetve valamennyi fenyegetettség figyelembe vétele. Ennek eredményeként a szervezet működési hatékonysága és versenyképessége is jelentős mértékben emelkedhet.

Gyakorlati tapasztalataink azt mutatják, hogy biztonságtechnikai szempontból nem feltétlenül az a jó rendszer, amely rengeteg paramétert ellenőriz és dolgoz fel egyszerre. A jó rendszer az, amely folyamatosan, megbízhatóan és – lehetőség szerint – téves riasztásoktól mentesen dolgozik. Egy optimális integrált biztonsági megoldás tehát annyi és csak annyi jó minőségű érzékelőt, jelfeldolgozó, rögzítő és visszacsatoló egységet tartalmaz, amennyit a biztonságtechnikai igények feltétlenül megkövetelnek és amennyit a gazdasági érdekek megengednek.

Biztonsági megoldások integrációja

A biztonsági rendszerek jellegükből adódóan folyamatos fejlesztésre szorulnak, annak érdekében, hogy ellent tudjanak állni az újabbnál újabb támadásoknak, meg tudjanak felelni az újabb és újabb kihívásoknak. Egy rendszer biztonságát alapvetően meghatározza az újonnan felmerülő kihívásokra adott válaszok gyorsasága. Ezért tűzte ki célul a KÜRT és a Pannon Egyetem Műszaki Informatikai Kara, hogy közös kutatási tevékenységünk eredményeként olyan megoldásokat nyújtsunk az integrált biztonsági rendszerek építéséhez, amelyek lokális intelligenciájukkal tanulásra képesek. A védelem különböző aspektusait megvalósító eszközök együttes alkalmazásával egy lényegesen jobb biztonsági rendszer építhető fel. Így biztosítható, hogy a telepítés pillanatában kockázatarányos védelmet garantáló biztonsági rendszer tulajdonságait hosszú távon – akár a biztonsági rendszer teljes életciklusa alatt is – képes legyen megőrizni.

Az integrált biztonsági rendszerek kidolgozásához kapcsolódó új elem az intelligens ágensek megjelenése, amelyek lehetővé teszik, hogy – a lehető legnagyobb fokú flexibilitás érdekében – a különböző biztonsági rendszerelemeket egymástól elválasszuk és egy közös szabványos kommunikációs protokollon keresztül kapcsoljuk egymáshoz. Az így létrejövő lokális intelligenciák megjelenése egyben hatékony elosztott megvalósításokat tesz lehetővé, ahol minimális a kockázatot jelentő kommunikáció. Egy lokális intelligencia nem válik működésképtelenné a kommunikáció elvesztésével, hanem számára ezen esemény bekövetkezése is információt hordoz. Az integrált biztonsági megoldások kidolgozása nemzetközi szinten is olyan egyedülálló tudományos eredményeket képes produkálni, amelyek széles körben kerülhetnek felhasználásra, hozzájárulva ezzel a biztonsági incidensekből származó potenciális károk csökkentéséhez, illetve a szervezeti biztonságtudatosság növeléséhez.

A spirális életciklus modell

A biztonsági megoldások integrációjára irányuló kutatási tevékenységünk egy spirális életciklus modellen keresztül valósul meg, amelynek fókuszába a kockázatelemzést helyezzük, és amelynek keretében a projekt minden egyes szakaszát a kockázat-minimalizálás elérésének rendeljük alá. A modell alkalmazásának előnye, hogy rendkívül világos a tevékenységek struktúrája, egyszerű a megvalósítás és biztos alapot nyújt a tervezési fázisok feladatainak egységes szemléletű végrehajtásához. A koncepciókészítésnél az a cél, hogy a fejlesztési munkát az elképzeléseinkre alapozhatjuk, a tervezés fázisában pedig arra törekszünk, hogy az általunk elképzelt rendszer megvalósítható legyen, és a felhasználók igényeit a megoldások maradéktalanul kielégítsék. A spirális életciklus modell lényeges sajátossága, hogy a kidolgozandó

megoldások, valamint a fejlesztéseket támogató módszerek és eszközök kiválasztásának kritériuma a funkció rizikófaktoron alapuló hasznossága.

A spirálmodell szerinti megközelítésmód esetében a kiindulási pont a követelmények meghatározása és a kockázatok specifikálása. Ezt követi a fejlesztések tervének a kidolgozása, a költségek becslése és a megvalósíthatósági alternatívák elkészítése. Az első körben kidolgozott tervek alapul szolgálnak a felhasználói oldal által is minősíthető prototípusok fejlesztéséhez, majd a programtervezési és tesztelési munkák elvégzéséhez. A prototípuskészítés elv alkalmazása nagymértékben csökkenti a kutatás-fejlesztési tevékenységek bizonytalanságát, hiszen olyan folyamatok végrehajtására kerül sor, amelyekben a nagyvonalú felhasználói elképzelések és a rendszerről feltárt ismeretek alapján kidolgozhatók a kívánt modellek. Ezeket a prototípusokat úgy készítjük el, hogy bemutathassuk a fejlesztés szempontjából kritikus komponensnek minősített eredményeket, folyamatokat, bonyolult algoritmusokat, ember-gép kommunikációkat, amelyeket előre nem lehet egyértelmű igényként megfogalmazni. A fejlesztés során a valóságos rendszer egy részének a felhasználói oldal által érzékelhető funkcióihoz készítünk megoldásokat.

Egy kívánt célra felépíthető rendszerek körét meghatározzák az elérhető építőelemek, illetve azok szükséges és lehetséges kapcsolódásai. Az elérhető elemek köre és az összes megengedett kapcsolódásuk – gyakorlati feladatok esetén – a felépíthető rendszerek egy beláthatatlanul nagy halmazát jelentheti. Ezért a biztonsági rendszerek szükséges strukturális és topológiai tulajdonságainak vizsgálata, formális megadása, alapja lehet olyan eljárásoknak, amelyek a keresési teret – a figyelembe veendő rendszerek halmazát – azok szükséges strukturális tulajdonságai alapján szűkítik. A strukturális tulajdonságok a szintézis módszer vezérlő szempontjai között kiemelt szerepet töltenek be.

Kutatásaink ezen része Fan és Friedler professzorok ún. P-gráf modelljére épül [1], mely a szakirodalomban folyamathálózat szintézis (PNS, Process Network Shynthesis) néven vált ismertté. A kidolgozott matematikai modell segítségével leírhatók a különféle „nyersanyagok” és az ezeket felhasználó „műveleti egységek” közötti kapcsolatok, oly módon, hogy az egyes műveleti egységeket valamely alkalmas módon összekapcsoljuk. Vizsgálatunk során ezt a leírást adaptáltuk a biztonsági rendszer matematikai modelljének megkonstruálásához, úgy hogy a műveleti egységeket az egyes ágensek, a különféle rendszer-állapotokat pedig az anyag jellegű csomópontok jelölik.

A biztonsági rendszerek kvantitatív értékeléséhez mértékekre van szükség, amely segítséget nyújt nem csak létező rendszerek minősítéséhez, de a tervezés során felmerülő alternatívák közti választáshoz is. A biztonsági rendszer legfontosabb mértékei

a rendelkezésre állása, és bizonyos események kockázata. A megfelelő rendelkezésre állás biztosításához kritikus kérdés a szükséges erőforrások méretezése. A tervezett biztonsági megoldások esetében meg kell vizsgálni, hogy valóban képes-e a tervezett erőforrások segítségével a várható igények kiszolgálására. Ezt olyan ütemezési és erőforrás allokációs feladatként lehet leképezni, amely megadja, hogy a rendelkezésre álló eszközökkel a kért szolgáltatások a kívánt válaszidőn belül kielégíthetőek-e. Összetett rendszerek esetén, a különböző elemek kiesése vagy korlátozott használhatósága nem csak lokális eseményekhez vezet, hanem a rendszer összefüggései mentén tovább terjedhet. Ilyen események együttes kockázatának elemzése nem lehetséges a biztonsági rendszer strukturális elemzése nélkül. A biztonsági rendszerek szintéziséhez alapkutatásként megvalósuló formális leírás és strukturális elemzés jó alapot ad a biztonsági rendszer struktúrájából adódó kockázatok felméréséhez is.

A biztonsági rendszerek formális leírása, strukturális tulajdonságai és mértékei alapján adott szempontok szerint optimális rendszerek algoritmikusan szintetizálhatóak. Ilyen szintézis eljárások bemenete a felhasználható rendszerelemek leírása és a felépítendő rendszerrel szemben támasztott követelmények megfogalmazása. Az integrált biztonsági megoldások alkalmazásának végeredményeként olyan eszközök jöhetnek létre, amelyek alkalmasak a környezetből érkező összetett információk rögzítésére, értékelésére, elemzésére, illetve ezek alapján döntések, intézkedések kezdeményezésére, valamint mindezek kommunikációjára. Ezen technikai eszközök képesek a kifinomult, illetve összetett fenyegetettségek időben történő azonosítására, megelőzésére, és mindezen eszközök összefogására.

Az integrált biztonság helyzete Magyarországon

És hogy mi a helyzet az integrált biztonság terén Magyarországon? A tapasztalatok azt mutatják, hogy a hazai piac egyelőre nem igazán érett a komoly rendszerek bevezetésére, ez köszönhető egyrészt a még nem kiforrott technológiai megoldásokból származó hátrányoknak, másrészt a viszonylag magas bevezetési, megvalósítási költségeknek.

Hasonló jellegű, a különféle biztonsági fenyegetettségek kezelését egyesítő módszertani és a módszertanok alkalmazását segítő eszközök kifejlesztését célzó kutatás Magyarországon jelenleg nem folyik. Az integrált biztonsági megoldások kidolgozása nemzetközi szinten is egyedülálló tudományos eredményeket képes produkálni, amelyek nemcsak hazai, de nemzetközi viszonylatban is széles körben kerülhetnek felhasználásra,

hozzájárulva ezzel a biztonsági incidensekből származó potenciális károk csökkentéséhez, illetve a hazai tudományos kutatási eredmények nemzetközi elismertségének növeléséhez.

A projekt a biztonsági rendszerek integrációjának elősegítésével, információk védelmével kapcsolatban szorosan illeszkedik a tudásintenzív iparágak fejlődését segítő, illetve a K+F kapacitásokat koncentráló, ezen keresztül a versenyképességet növelő hazai fejlesztési célokhoz. A projekt keretében előálló eredmények az EU 2007-ben induló FP 7 K+F keretprogramjaihoz is szorosan illeszkednek, valamint az Amerikai Egyesül Államok HSPD-12 (Homeland Security Presidential Directive), a fizikai és informatikai biztonság konvergenciáját, a biztonsági rések feltárását, és intelligens fizikai biztonsági megoldások kialakítását célzó direktívájában megfogalmazott célokkal is szoros összefüggésben állnak.

Irodalmi hivatkozás

[1] Friedler, F., J. B. Varga, E. Feher, and L. T. Fan, Combinatorially Accelerated Branch-and-Bound Method for Solving the MIP Model of Process Network Synthesis, Nonconvex Optimization and Its Applications, State of the Art in Global Optimization, Computational Methods and Applications (Eds: C. A. Floudas and P. M. Pardalos), 609-626, Kluwer Academic Publishers, Norwell, MA, U.S.A. (1996).