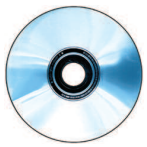
DSI: Biztonságos Linux a távközlésben



Az Ericsson Research újfajta szerkezetet fejleszt a Linux-telepeken futó adatátviteli rendszerekhez alkalmazásokhoz.

A távközlési ipar érdeklődése a telepek iránt azért nagy, mert olyan távközlési tulajdonságokkal bírnak, mint magas rendelkezésre állás, megbízhatóság és méretezhető teljesítmény, ráadásul mindehhez költséghatékony gépeket és programokat használnak. Ezekhez a komoly követelményekhez most a kifinomultabb biztonság kérdése is csatlakozott. Ennek ellenére igen kevés próbálkozás folyik a telepeken is megfelelő biztonsági szintet nyújtó egységes osztott keretrendszerek felépítésére.

Munkánk az Ericsson Researchnél jelenleg olyan programkód-megoldott valós idejű (soft real-time) osztott alkalmazások fejlesztése, amelyek nagyméretű Linux-alapú távközési telepeken futnak. Ezeknek a telepeknek folyamatos működés mellett kell lehetővé tenniük, hogy a karbantartók futás közben cseréljék le az alkatrészeket és programokat, anélkül, hogy zavarnák a rajtuk futó alkalmazások működését. Az ilyen telepekben a telep csomópontjai közötti és a külső gépekre irányuló kapcsolattartás korlátozott.

Írásunkban az új biztonsági szerkezet fejlesztése mögötti alapokat mutatjuk be, azaz a DSI (Distributed Security Infrastructure) rendszert. A DSI többféle biztonsági módszert is támogat a távközlésben használt linuxos telepeken futó alkalmazások igényeinek megfelelően. A DSI ezeket az osztott módszerrel ellátott alkalmazásokat ruházza fel az elérési jogosultság, az azonosítás, a hitelesítés és a kapcsolattartási épség ellenőrzésének képességeivel.

Igény újfajta biztonsági megközelítésre

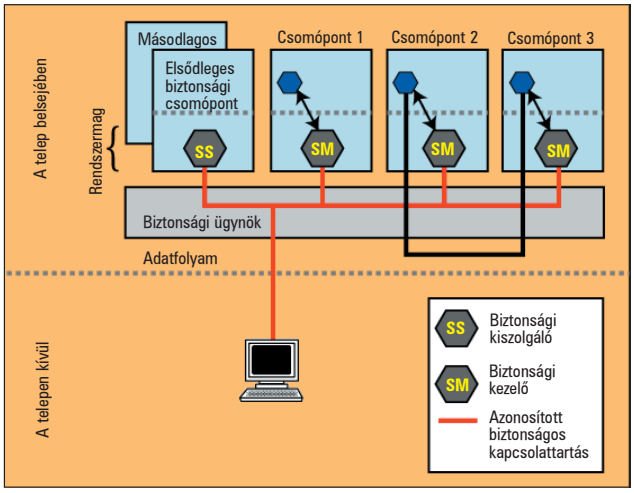
A telepekre számos biztonsági megoldás létezik, de semelyik ilyen megoldás nem kifejezetten telepek számára készült.

A leggyakrabban használt biztonsági megközelítés több létező megoldás összevonása. Csakhogy a különböző biztonsági csomagok egybeépítése és karbantartása igen összetett feladat, és gyakran kiderül, hogy a különböző biztonsági módszerek egyáltalán nem képesek együttműködni. További nehézségek léphetnek fel sok csomag egyesítésekor, például a rendszerkarbantartás és -fejlesztés esetében, hiszen a számos biztonsági folttal igen nehéz lépést tartani.

A távközlésben használt telepekkel szemben ugyanakkor igen szigorú teljesítmény- és válaszidő-követelmények vannak érvényben, ami a biztonsági megoldások tervezését igencsak megnehezíti. Valójában számos biztonsági megoldás egyszerűen nagy erőforrásigénye miatt nem használható.

A jelenleg létező biztonsági megoldások felhasználói jogosultságokon alapulnak, és nem támogatják az egyazon rendszeren, de különböző processzorokon futó folyamatok közötti kapcsolattartás hitelesítését és jogosultságait. A távközlési alkalmazások esetében ugyanazt az alkalmazást kevés felhasználó futtatja igen hosszú ideig, megszakítás nélkül.

A fenti elképzelés megvalósítása a különböző csomópontokon készült folyamatokhoz ugyanazokat a biztonsági előjogokat rendeli. Ez pedig oda vezet, hogy az osztott rendszer számos tevékenységére nem fogunk biztonsági ellenőrzést végezni.



1. ábra A DSI osztott szerkezete

A DSI jellemzői

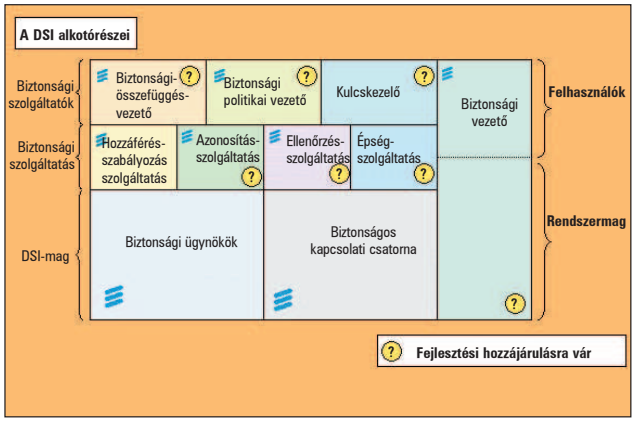
Minthogy a DSI maga is egy távközlésben használt Linux-telep része, meg kell felelnie a megbízhatóság, a méretezhetőség és a magas rendelkezésreállás távközlési követelményeinek. Ezen kívül a DSI a következő elvárásokat is teljesíti:

1. Egységes keretrendszer: a biztonságnak egységesnek kell lennie a heterogén alkatrészek, az alkalmazások, a köztes réteg (middleware), az operációs rendszer és a hálózati megoldások különböző szintjén keresztül. Minden szerkezetnek illeszkednie kell a másikhoz, hogy a rendszeren található minden kihasználható biztonsági rést kiküszöböljön.
2. Folyamatszintű megközelítés: a DSI kicsiny alapegységen, a folyamaton alapul.
3. A legkisebb teljesítménycsökkentő hatás: a biztonsági képességek bevezetésének nem lehet komoly teljesítménymérséklő hatása. A teljesítmény ideiglenes csökkenése a biztonsági összefüggések kezdeti telepítésekor engedélyezett; ugyanakkor a további elérésekre gyakorolt hatásának elhanyagolhatónak kell lennie.
4. Időosztásos biztonság: a biztonsági összefüggések megváltoztatása a futó biztonsági szolgáltatásokban azonnali hatást eredményez. Valahányszor a cél biztonsági beállításai megváltoznak, a rendszer az új biztonsági összefüggéseknek megfelelően újraértelmezi a jelenlegi erőforrás felhasználását.
5. Menet közben frissíthető szabályok: lehetővé kell tenni az osztott biztonsági rendszabályok futásidejű megváltoztatását. Az adatátviteli kiszolgáló csomópontoknak folyamatos és hosszú távú elérhetőséget kell biztosítani; ezért lehetetlen egy szolgáltatást pusztán azért megszakítani, hogy az új biztonsági rendszabályokat beállítsuk.
6. Áttetsző kulcskezelés: a kapcsolatok biztosítása érdekében titkosítási kulcsok készülnek. Ez nagy mennyiségű kulcsot jelent, amelyeket biztonságosan kell kezelni és tárolni.

A DSI szerkezete

A DSI kétféle összetevővel bír: a kezelőfelülettel és a szolgáltatással. A DSI-kezelőfelület egy vékony réteg, amelybe a biztonsági kiszolgáló, a biztonsági és a biztonsági kapcsolattartó csatorna tartozik (*1. ábra*). A DSI-szolgáltatás egy rugalmas réteg, amely a szolgáltatások helyettesítésével és eltávolításával igény szerint módosítható vagy frissíthető.

A DSI kezelőfelületének központi eleme a biztonsági kiszolgáló. Ez ugyanis a biztonsági műveletek és a kezelőfelület,



2. ábra A DSI elemei

illetve a betörésérzékelő rendszerek belépési pontja. Itt határozzuk meg a teljes telepre vonatkozó dinamikus biztonsági környezetet azáltal, hogy osztott környezetben minden biztonsági kezelőnek szétsugározzuk a változásokat.

A telep minden csomópontján a biztonsági kezelők gondoskodnak a biztonsági szabályok betartásáról. Ők felelősek a biztonsági környezet megváltozásának helyi érvényesítéséért is. A biztonsági kezelők kizárólag a biztonsági kiszolgálóval cserélnek (biztonsági) adatot.

A biztonságos kapcsolattartási csatorna a biztonsági ügynökök közötti titkosított és hitelesített kapcsolattartásért felelős.

A biztonsági kiszolgáló és a külvilág között áramló minden adat a biztonságos csatornán halad keresztül. Két csomópont (hogy elkerüljük az egyetlen csomópont meghibásodásával járó gondokat) ad otthont a biztonsági kiszolgálónak és a különféle biztonsági szolgáltatóknak, például a bizonyítvány-hitelesítőnek.

A biztonsági módszer széles körben elterjedt és kipróbált algoritmusokon alapul. A felhasználók nagy valószínűséggel képtelenek áttörni ezeket a megoldásokat; ezért a biztonság végrehajtására a magszint a legmegfelelőbb. Minden biztonsági döntés – amikor szükségessé válik – rendszermagszinten kerül megvalósításra, akárcsak a fő biztonsági kezelőelem, amely a rendszermagba ágyazva található meg. Ezeket a beágyazásokat modulok betöltésével végezzük.

A DSI-szerkezet minden egyes csomóponton lazán összeillesztett szolgáltatásokból áll. Minden szolgáltatás készítésétől fogva jelenléti jelzéseket küld a helyi biztonsági kezelőnek, amely bejegyzi a szolgáltatást, és elérési módszerüket a belső modulok által elérhetővé teszi. Kétfajta szolgáltatás: az egyik a biztonsági szolgáltatások (jogosultságellenőrzés – access control), az azonosítás (authentication), az egységesítés (integration), az ellenőrzés (auditing); a másik a biztonsági szolgáltatók (például a biztonsági kulcskezelő) már felhasználói szinten futva szolgálja ki a biztonsági kezelőket.

A jelenlegi eredmények

A jelen pillanatig a lemeznélküli Linux-kiszolgálók biztonságos indítási rendszere készült el. A csomópontok indulásakor a digitális aláírásokkal támogatott biztonságos indítás (secure boot) és az osztott megbízható számítási bázis (DTCB) érhető el. A biztonsági indításhoz használt rendszermag elég kis méretű ahhoz, hogy sérülékenységét alapos vizsgálatnak vethessük alá. Továbbá a futtatható állományok digitális aláírás hitelesítése, illetve a helyi biztonsági hitelesítő (local certification authority) megakadályozza a DTCB rosszindulatú módosítását.

A Linux Security Module (LSM) modul alapján készítettünk egy biztonsági modult is, amely a DSI-elérési jogosultság szolgáltatás részeként betartatja a biztonsági szabályokat. Ezt a modult egybeépítettük az SCC-vel, így hozva létre az osztott eléréskezelési szerkezetet. A DSI jelenleg a teljes telepben folyamatszinten támogatja az időosztásos és a menet közben frissíthető biztonsági rendszabályokat.

Hogy megkönnyítsük az osztott biztonsági rendszabályok felügyeletét és karbantartását, tanulmányokat végeztünk a csomagkezelő rendszerekben (például az RPM-ben) is megtalálható adat-újrahasznosító módszerek kifejlesztésére, hogy a biztonsági rendszabályok egy részét így állítsuk elő, vagy ezt az adatot a csomagba helyezzük (ha ez a legmegfelelőbb megadási forma). Ezek az erőfeszítések egyben azt is célozzák, hogy a rendszabályokat a program telepítéskor, beállításakor, működésbe lépésekor és végrehajtásakor teljesen más jogosultságok kiadására használjuk. A rendszabályok, a fordítási és betöltési módszerek kifejezésére használt pontos nyelvezet még kiegészítésre szorul.

Részlegesen a biztonságos kapcsolattartási csatornát is elkészítettük az OmniORB, a CORBA nyílt forrású változata alapján. Az SCC-logika a hordozható rétegre (portability layer) került, ezáltal a megvalósítást sikerült a felhasznált kapcsolattartó középrétegtől (middleware) függetleníteni. A CORBA választását SCC kapcsolattartó középrétegként több tényező is indokolta, többek között az osztott, valós idejű és beágyazott rendszerek támogatása és a jó együttműködés.

A DSI mint nyílt forrású projekt

A DSI-vel az a tervünk, hogy a teljes keretrendszert nyílt forrásúvá tegyük, hogy a különböző szervezeteket és nyílt forráskódon munkálkodó fejlesztőket is bevonhassuk a különféle elemek tervezésébe és fejlesztésébe. A *2. ábra* a DSI különféle elemeit ábrázolja. Minden kérdőjellel jelölt elem még tervezésre és fejlesztési hozzájárulásokra vár.

Összegzés

A projekt honlapja 2002 júniusától érhető el. Itt a DSI jelentései, a bemutatók, a forráskódok és a további támogatók honlapjaira történő hivatkozások találhatók. Természetesen bárki kapcsolatba léphet a DSI-csapat (alább felsorolt) tagjaival, ha a DSI szerkezetének részletes leírására, a stratégiára vagy a forráskódokra kíváncsi, esetleg az együttműködés lehetőségeiről szeretne beszélgetni. Ezen kívül a DSI-csapat „Further Details on DSI: a New Architecture for Secure Carrier-Class Linux Clusters" című cikkét a Linux Journal honlapján (➲ http://www.linuxjournal.com/article/6053) meg lehet tekinteni.

A csapat névsora és egy kiegészítő szöveg a 41. CD Magazin/DSI könyvtárában megtalálható.

Linux Journal 2002. július, 99. szám

Ibrahim F. Haddad (Ibrahim.Haddad@Ericsson.com)