Reportáž

VIAC ÚROVŇOVÉ BEZPEČNOSTNÉ RIEŠENIA POKROK V OBLASTI OPERAČNÝCH SYSTÉMOV

Juraj POLÁK
SUN Microsystems Bratislava

Odvetvie informačných technológií čoraz intenzívnejšie zameriava svoje úsilie na bezpečnostné požiadavky prichádzajúce z komerčného sektora a bezpečnostné požiadavky vládneho sektora ustupujú na vedľajšiu koľaj. Dôsledok je taký, že v oblasti bezpečnosti počítačových sietí privátny sektor ďaleko predstihol vládny sektor.

Komunita informatikov ako aj komerčný sektor požadujú riešenia s viac úrovňovou bezpečnosťou operačných systémov, aby dokázali chrániť citlivé informácie pred vnútorným aj vonkajším ohrozením. Tieto riešenia musia uspokojiť aj protirečivé požiadavky, kde na jednej strane musia byť operačné systémy zabezpečené proti prístupu neoprávnených užívateľov, no na druhej strane musia zároveň umožňovať jednoduchý prístup oprávneným užívateľom.

Potreba chrániť prístup k citlivým informáciám, ktorá vznikla v komunite informatikov, vyvolala úsilie hľadať takéto riešenia, avšak v súčasnosti už požiadavky komerčného sektoru prichádzajúce z čoraz viac zosieťovaného sveta prerástli cez požiadavky komunity informatikov. Tieto požiadavky prichádzajú zo všetkých oblastí hospodárstva. Finančné inštitúcie potrebujú zabezpečiť prístupné služby pre zákazníkov a zároveň sa chrániť pred neoprávnenými užívateľmi. Organizácie v zdravotníctve sú povinné chrániť záznamy pacientov. Subjekty prevádzkujúce elektronické obchody musia chrániť účtovné údaje zákazníkov a výrobcovia musia strážiť návrhy nových produktov pred konkurenciou. Vzdelávacie inštitúcie sú povinné zachovať dôvernosť záznamov a protokolov a tiež zabezpečiť anonymitu darcov z rád absolventov.

Jednou zo spoločností, ktoré produkujú riešenia bezpečnostných požiadaviek vládneho aj komerčného sektora je spoločnosť Sun Microsystems Federal Incorporated.

Táto spoločnosť so sídlom v McLean vo Virgínii dodáva vládnym a komerčným zákazníkom distribuované počítačové technológie, produkty i služby.

Koncom minulého roka spoločnosť Sun ohlásila operačné prostredie Trusted Solaris 2.5.1, ktoré je nasledujúcou verziou operačného systému Trusted Solaris 2.5 (SIGNAL, október 1997, strana 31). Tento systém podporuje rad počítačového vybavenia na báze "interconnect" architektúry periférnych komponentov, ako aj nové prenosové média vrátane asynchrónneho režimu prenosu (ATM), distribuovaného rozhrania s optickým káblom, Token Ringu a gigabitového Ethernetu.

"V priebehu minulého roka orgány federálnej vlády zvýšili nákupy bezpečnostných systémov Trusted o 200%", uvádza Joe A. Alexander, manažér pre produktový rad Trusted Solaris. Predpovedá tiež, že v roku 1999 dôjde k ďalšiemu nárastu, a to hlavne zo strany Ministerstva spravodlivosti ako takého, a hlavne jeho zložky - Federálneho vyšetrovacieho úradu FBI. Joe Alexander takisto predpokladá, že najväčšia oblasť rastu medzi vládnymi inštitúciami bude medzi agentúrami nespadajúcimi pod Ministerstvo obrany. Avšak najväčším trhom pre Trusted Solaris bude komerčný sektor, a to hlavne oblasť elektronického obchodovania.

"V zásade možno povedať, že v hospodárstve práve prebieha revolúcia, ktorá nás privedie k sieťovému hospodárstvu," hovorí Joe Alexander. "Ako sa internet stáva nevyhnutnou súčasťou obchodu a sieťovo centrické počítačové spracovanie začína byť normou, otázky prístupu nadobúdajú na dôležitosti. Otázka, kto dostane prístup k akým informáciám, aby mohol vykonávať svoju prácu naznačuje, že bezpečnosť začína byť veľmi dôležitou témou. Práve preto sú príležitosti pre Trusted Solaris v oblasti komerčného sektora rovnako veľké, ak nie väčšie, ako vo vládnom sektore, v armáde alebo v informatike. Je tam jednoducho oveľa viac zákazníkov."

Operačný systém Trusted Solaris 2.5.1 je postavený na systéme Solaris 2.5.1, jednotnom desktopovom prostredí Common Desktop Environment 1.1 a balíku Solstice AdminSuite 2.1. Riadi užívateľský prístup k informáciám ako aj rozsah aktivít jednotlivých užívateľov v systéme. Ako uvádzajú predstavitelia spoločnosti, nový systém má lepšiu funkčnosť a vyššiu bezpečnosť ako prostredie Trusted Solaris 2.5 a poskytuje

ochranu proti interným aj externým ohrozeniam, ktorá predčí ochranu bežnú u štandardných UNIXových systémov.

Ďalší rozdiel medzi operačnými systémami 2.5 a 2.5.1 spočíva v tom, že Britská rada pre kritériá hodnotenia bezpečnosti informačných technológií (ITSEC) hodnotila operačné prostredie Trusted Solaris 2.5.1 a udelila mu hodnotenie E3/F-B1, čo je vyššie hodnotenie ako rating B1 udelený podľa amerických kritérií hodnotenia dôveryhodnosti počítačových systémov (TCSEC). Rada tiež prostrediu Trusted Solaris 2.5.1 udelila rating E3/F-C2, ktorý zahŕňa zoznamy kontroly prístupu a informatívne značenie dôveryhodnosti.

ITSEC je iniciatíva podporovaná Britskou vládou, ktorá certifukuje úroveň istoty, ktorú možno vkladať do testovaných produktov a systémov.

TSEC rating je uznávaný v Európe, Kanade a v Austrálii. Podľa kritérií ITSEC sa produkty môžu hodnotiť z hľadiska úrovne istoty a funkčnosti. Rating istoty sa pohybuje od najnižšieho hodnotenia E1 po najvyššie hodnotenie E6. Funkčnosť operačných systémov sa meria podľa amerických kritérií U.S. TCSEC, tiež známych ako ”Orange Book”, kde sa používa nepovinná kontrola prístupu. Rating E3/F-E1 je ekvivalent B1 pre povinnú kontrolu prístupu. Nepovinná kontrola prístupu umožňuje užívateľom prihlásiť sa do systému a po zadaní správneho hesla už nenarazia na žiadne obmedzenia prístupu k informáciám, ku ktorým majú prístup povolený.

Podľa Joea Alexandra sa spoločnosť sústredila na získanie ratingu ITSEC z dôvodu dlhého procesu hodnotenia systému Trusted Solaris 1.x podľa amerických kritérií hodnotenia dôveryhodnosti počítačových systémov (TCSEC) u národnej bezpečnostnej agentúry National Security Agency (NSA), ktorý sa vlastne nikdy neukončil. Dodal, že spoločnosť Sun úzko spolupracuje s programovým úradom pre jednotné operačné prostredie infraštruktúry obranných informácií (DIICOE) obrannej informačnej agentúry Defence Intelligence Agency, a v súčasnosti sa sústreďuje na partnerské riešenia, ktoré plnia požiadavky informatickej komunity. Parametre operačného prostredia Trusted Solaris 2.5.1 plnia a prekračujú všetky certifikačné požiadavky DIICOE na bezpečnosť. Joe Alexander prehlasuje, že pri výbere operačného prostredia pre špecifické požiadavky, sa americké informačné agentúry čoraz v širšej miere riadia ratingom ITSEC.

Spoločnosť Sun sa tiež rozhodla nezúčastniť sa programu hodnotenia dôveryhodnosti produktov agentúry NSA. Podľa vyjadrenia Joea Alexandra čas, ktorý mala spoločnosť na to, aby získala rating produktu Trusted Solaris, neumožnil spoluprácu s touto agentúrou.

Agentúra NSA však v súčasnosti spolupracuje s Národným inštitútom pre štandardy a technológiu na príprave procesu rovnocenného britskej certifikácii, čo by mohlo znamenať, že NSA bude v budúcnosti môcť akceptovať certifikáciu udelenú spoločnosti SUN podľa hodnotenia ITSEC.

Podľa vyjadrení predstaviteľov spoločnosti môžu organizácie produkt Trusted Solaris 2.5.1 využiť na vyladenie bezpečnostnej ochrany tak, aby zodpovedala ich špecifickým požiadavkám. V distribuovanom systéme typu klient/server možno spoločne konfigurovať pracovné stanice a servery, takže užívatelia môžu zdieľať súbory, odosielať poštu, na diaľku sa prihlásiť a spustiť tlač, a to všetko s viacerými úrovňami bezpečnosti. Zákazníci môžu zaviesť jednotnú celopodnikovú bezpečnostnú politiku, spoliehajúc sa na ochranu zabudovanú v prostredí Trusted Solaris vrátane **NIS4** – čo je ”trusted” verzia národného súborového systému spoločnosti Sun známeho ako NFS, ako aj bezpečnej sieťovej práce. Vybrané črty možno aktivovať alebo deaktivovať a tak pripraviť konfiguráciu systému, ktorá splní bezpečnostné požiadavky daného pracovného miesta a tiež požiadavky na použiteľnosť.

Operačné prostredie Trusted Solaris 2.5.1 možno upraviť tak, aby plnilo bezpečnostné požiadavky C2, B1 alebo bezpečnostné požiadavky pracovnej stanice v compartmented mode. Ponúka aj pokrokový multithreading a podporu pre symetrický multiprocessing, čo dáva organizáciám, ktoré prechádzajú na počítačové spracovanie na báze webu, možnosť zvládnuť zvýšený počet sieťových transakcií. Okrem toho má tento produkt už aj označenie citlivosti a systém okien bol rozšírený tak, aby prístup k dátam poskytoval podľa ich citlivosti.

Operačné prostredie podporuje zariadenia s procesorom UltraSPARC, a ponúka bezpečné počítačové spracovanie dimenzovateľné od desktopových pracovných staníc Sun Ultra 5 až po Sun Entreprise Server 6500 s 30 centrálnymi základnými jednotkami. Programové vybavenie sa v distribuovaných sieťach NFS a v systémoch Trusted Solaris

2.5.1 riadi rovnakými princípmi a atribútmi a podporuje štandard MAXSIX umožňujúci interoperabilitu so systémami Trusted Solaris 1.2.

Neoprávnení užívatelia, ktorí sa pokúsia o prístup k citlivým informáciám na servery s operačným prostredí Trusted Solaris 2.5.1, budú mať zamietnutý prístup bez toho, aby sa dozvedeli, či daná informácia existuje. Rieši sa to tak, že sa aktivuje povinná kontrola prístupu, ktorá pre dané miesto uplatní bezpečnostnú politiku definovanú pre konkrétneho zákazníka, ktorá určuje, k akým informáciám alebo aktivitám môže užívateľ tejto pracovnej stanice dostať prístup. Tieto kontrolné mechanizmy zvyšujú bezpečnostný rating systému z úrovne C na úroveň B. Podľa Joe Alexandra, prostredie Windows NT zatiaľ takúto črtu nemá.

Spoločnosť Sun Microsystems vyvíja a ponúka riešenia Trusted Solaris v spolupráci s viacerými partnerskými spoločnosťami. Patrí medzi ne i spoločnosť Trusted Computer Solutions so sídlom v Hemdone vo Virgínii, ktorá už má viacero komerčných aplikácií postavených na systéme Trusted Solaris 2.5.1. Jedna z týchto aplikácií je SecureOffice. Ide o produkt, ktorý umožňuje užívateľom vidieť, presúvať, vystrihnúť a prilepiť prvky z aplikácií Microsoft Windows vrátane aplikácií Word, Excel, Powerpoint, Access a z prehliadača Netscape Navigator, a to súbežne s prácou na životne dôležitých aplikáciách UNIX, pracujúc z toho istého počítača na viacerých bezpečnostných úrovniach.

SecureOffice sa dokáže súbežne napojiť na internetový protokol tajnej smerovacej siete (SIPRNET) a na internetový protokol neklasifikovanej prístupovej siete (NIPRNET), takže z jedinej stanice je možný prístup ku globálnemu systému príkazov a kontroly aj k internetu. Tento systém možno tiež napojiť na prísne tajné siete, ako spoločný celosvetový informačný komunikačný systém JWICS a siete spriatelených krajín.

Ďalšia aplikácia je TCSecure, čo je bezpečná brána proxy gateway, ktorá poskytuje webovské rozhranie k celej sérii back-end hostov s rôznymi informáciami. ”Prihlásite sa na webový server , riadne sa identifikujete a ak správne zadefinujete a lokalizujete informácie, ktoré potrebujete, démon bezpečného protokolu prenosu hypertextu (http) - čo je program, ktorý spracúva vašu požiadavku – vyhľadá túto informáciu a poskytne ju oprávnenému užívateľovi”, vysvetľuje Joe Alexander. Ďalším partnerom je spoločnosť Authentica

Security Technologies Incorporated so sídlom v Montgomery Village v Marylande, ktorá nedávno prišla s produktom PageVault. Ide o balík integrovaných nástrojov, ktoré možno použiť na zvýšenie ochrany a kontroly citlivých a autorských dokumentov vytvorených v prenosnom dokumentovom formáte Adobe Systems, a ktoré zároveň poskytujú vysokú pružnosť v distribúcii týchto dokumentov.

”PageVault umožňuje užívateľovi chrániť úseky alebo interné časti dokumentu”, tvrdí Joe Alexander. Užívatelia môžu napríklad publikovať podmienky výberového konania a použiť časový zámok systému PageVault, ktorý určí čas, keď sa majú tieto podmienky zverejniť na webe. Časový zámok tiež po uplynutí určeného času prístup uzavrie. Informácie sa neodstránia, no časový zámok PageVault určí, kedy sa prestanú zobrazovať.

Systém PageVault možno použiť aj na ochranu citlivých dokumentov s rôznymi časťami vysoko klasifikovaných dát. Použitím PageVault ”môžete ukryť časti dokumentu pred neoprávnenými užívateľmi, podľa toho, ako sa identifikovali pri prihlásení,” pokračuje Joe Alexander. ”Resumé možno, napríklad, považovať za otvorené informácie, zatiaľ čo ďalšie časti dokumentu možno pred jednotlivými osobami ukryť podľa toho, aké sú ich prístupové práva.”

Podľa vyjadrenia Joe Alexandra budú na jar uvedené na trh dva komerčné ochranné produkty typu firewall, ktoré bežia na operačnom systéme Trusted Solaris. Spoločnosť V-One so sídlom v Germantowne v štáte Maryland prišla s aplikáciou virtuálnej privátnej siete ponúkanej pod názvom SmartGate, ktorá poskytuje celoplošnú ochranu sieťových dát medzi vzdialenými pracovnými stanicami na úrovni aplikácie. Taktiež poskytuje dvojfaktorovú identifikáciu, vzájomnú identifikáciu, šifrovanie a kontrolu prístupu.

Divízia SunScreen spoločnosti Sun Microsystems v apríli alebo v máji uvedie na trh verziu 3.0 produktu SunScreen EFS. EFS možno v rámci organizácie použiť na dôsledné uplatňovanie zásad kontroly prístupu k sieťovým službám na vlastnom intranete.

Ďalším produktom radu Trusted spoločnosti Sun bude Trusted Solaris 7 s cieľovým termínom v septembri. Tento produkt bude postavený na operačnom prostredí Solaris 7 spoločnosti Sun.

MHK

SIGNAL, február 1999, oficiálna publikácia AFCEA