Дәріс 8. Операциялық жүйелердің қауіпсіздігі. Жоғары сенімді есептеу базасы

Жоспары:

1 Операциялық жүйелердің қауіпсіздігі
2 Қорғалған жүйелерді құруға бола ма?
3 Жоғары сенімді есептеу базасы

Операциялық жүйелердің қауіпсіздігі. Компьютерлік жүйелер қауіпсіздігінің беделін түсірудің көптеген жолдары бар. Мысалы, адамдардың көпшілігі өздерінің PIN-кодтары үшін 0000 комбинациясын орнатады немесе пароль ретінде "password" сөзін қолданады – бұларды есте сақтау оңай, бірақ олар қауіпсіздіктің жоғары деңгейін қамтамасыз етпейді. Керісінше, кейбір адамдар есте сақтау мүмкін емес өте күрделі парольдерді де ойлап табады және оларды мониторға немесе пернетақтаға орналастырылған жапсырмаларға жазуға мәжбүр болады. Машинаға физикалық қол жетімділігі бар кез-келген адам (тазалаушылар, хатшылар және барлық келушілерді қоса есептегенде) ондағы барлық нәрсеге қол жеткізе алады. Басқа да көптеген мысалдар бар, олардың ішінде жоғары лауазымды тұлғалардың құпия ақпараты бар USB дискілерін жоғалтуы, өндірістік құпиялары бар, бірақ қоқысқа тастамас бұрын дұрыс тазаланбаған ескі қатты дискілер және т.б.

Дегенмен, қауіпсіздікке қатысты ең маңызды оқиғалар күрделі кибершабуылдарға жатады. Кітапта операциялық жүйелерге қатысты шабуылдарға ерекше назар аударылады. Басқаша айтқанда, біз веб-шабуылдарды немесе SQL дерекқорларына жасалатын шабуылдарды қарастырмаймыз. Оның орнына, біз операциялық жүйелерге бағытталған немесе қауіпсіздік саясатын орындауда (немесе көбінесе орындауға кедергі келтіруде) маңызды рөл атқаратын шабуылдарға назар аударамыз.

Жалпы, біз ақпаратты пассивті түрде ұрлауға тырысатын шабуылдар мен компьютерлік программаның әрекетін бұзуға тырысатын шабуылдарды ажыратып қарастырамыз. Пассивті шабуылдың мысалы – желі трафигіне қосылған және деректерді алу үшін шифрды бұзуға (егер ол бар болса) тырысатын жау. Белсенді шабуыл кезінде қаскүнем зиянды кодты орындауға мәжбүрлей отырып, мысалы, кредит картасының деректемелерін ұрлау үшін, пайдаланушының веб-браузерін басқаруды өзіне ала алады. Сол сияқты, біз толығымен хабарламаны немесе файлды кілтсіз бастапқы деректерді қалпына келтіруді қиындататын жолмен араластыруға арналған криптографияны және бағдарламаларға қорғаныс механизмін қосатын, бұзып кірушілерге олардың іс-әрекеттерін өзгертуді қиындататын программаларды нығайтуды (укрепление, hardening) ажыратамыз.

Операциялық жүйе криптографияны көптеген жерлерде қолданады: желі арқылы деректерді қауіпсіз жіберу, файлдарды дискіде қауіпсіз сақтау,

пароль файлындағы құпия сөздерді шифрлау және т. б. Программаларды нығайту да кеңінен қолданылады: бұзып кірушілердың жұмыс істеп тұрған программаға жаңа кодты енгізуіне жол бермеу үшін, әрбір процестің өзіне қажетті және ол үшін көзделген, және одан жоғары емес артықшылықтардың болуын қамтамасыз ету үшін және т.б. Қорғалған жүйелерді құруға бола ма? Бүгінгі таңда газет ашып, компьютерлік жүйелерге енген, ақпаратты ұрлаған немесе миллиондаған компьютерлерді бақылауға алған хакерлер туралы тағы бір оқиғаны оқымай қалу мүмкін емес. Бұл жағдайда сіз екі қарапайым және өте қисынды сұрақ қоя аласыз:

1. Қорғалған компьютерлік жүйені құруға болмай ма?
2. Егер олай болса, неге ол әлі жасалмаған?

Бірінші сұрақтың жауабы: "Теориялық түрде мүмкін". Негізінде, программа қателіктерден құтылуы мүмкін және егер бұл программа тым үлкен немесе күрделі болмаса, біз оның қорғалғанына көз жеткізе аламыз. Өкінішке орай, қазіргі компьютерлік жүйелер өте күрделі, бұл екінші сұрақтың жауабына сәйкес келеді.

Неліктен мүлдем қорғалған жүйелер әлі жасалмаған деген сұрақтың жауабы екі негізгі себепке байланысты. Біріншіден, бүгінгі жүйелер қорғалмаған, бірақ пайдаланушылардың олардан бас тартқысы келмейді. Мысалы, егер Microsoft Windows жүйесінен басқа, оның вирусқа қарсы иммунитеті бар, бірақ Windows қосымшаларын орындамайтын жаңа өнімі SecureOC бар деп мәлімдесе, онда барлық жеке пайдаланушылар мен компаниялар бірден Windows-тан бас тартып, жаңа жүйені сатып алуы екіталай. Microsoft корпорациясының қорғалған операциялық жүйесі бар (Fandrich et al., 2006), бірақ ол оны нарыққа шығармайды. *Екінші себеп соншалықты айқын емес*. Қорғалған жүйені құрудың жалғыз белгілі тәсілі – оның қарапайымдылығын сақтап қалу. Функционалдылық мүмкіндіктер – қауіпсіздіктің жауы болып табылады. Көптеген технологиялық компаниялардағы маркетинг бөлімінің батыл жігіттері (дұрыс па, жоқ па) пайдаланушылар көбірек, одан да кеңірек, сапалырақ функционалдық мүмкіндіктерді қалайды деп болжайды. Олар өздерінің бағдарламалық өнімдерінің жүйелік құрылымдарын жасаушылар бұл үшін тиісті нұсқаулар алатынына сенімді. Бірақ мұның бәрі жүйенің күрделілігінің арта түсуін, кодтың көбірек санын, қауіпсіздік жүйесіндегі ақаулар мен қателіктердің көбеюін білдіреді.

Екі қарапайым мысал келтіруге болады. Алғашқы электрондық пошта жүйелерінде хабарламалар ASCII-мәтіні ретінде жіберілді. Олар қарапайым болды және оларды мүлдем, яғни толығымен қауіпсіз етуге болатын еді. Пошта бағдарламаларында қателіктер болса да, ASCII-де жазылған хабарламаның компьютерлік жүйені бұзуы күмәнді шаруа болатын (кейінірек біз бірнеше ықтимал шабуылдарды талқылаймыз). Содан кейін хабарламалардың мүмкіндіктерін кеңейту және оларға макростар болуы мүмкін Word редакторының файлдары сияқты құжаттардың басқа түрлерін қосу идеясы пайда болды. Мұндай құжатты оқу сіздің компьютеріңізде біреудің бағдарламасын іске

қосуды білдіреді. Қолданылатын қауіпсіздік механизмдеріне қарамастан, компьютерде біреудің бағдарламасын іске қосу ASCII мәтінін қарауға қарағанда әлдеқайда қауіпті. Пайдаланушыларға пассивті құжаттардан белсенді бағдарламаларға электрондық пошта мазмұнын өзгерту мүмкіндігі қажет болды ма? Мүмкін емес, бірақ бұл өзгерістер біреуге керемет идея болып көрінді, ал ешкім қауіпсіздік үшін салдары туралы ойламады.

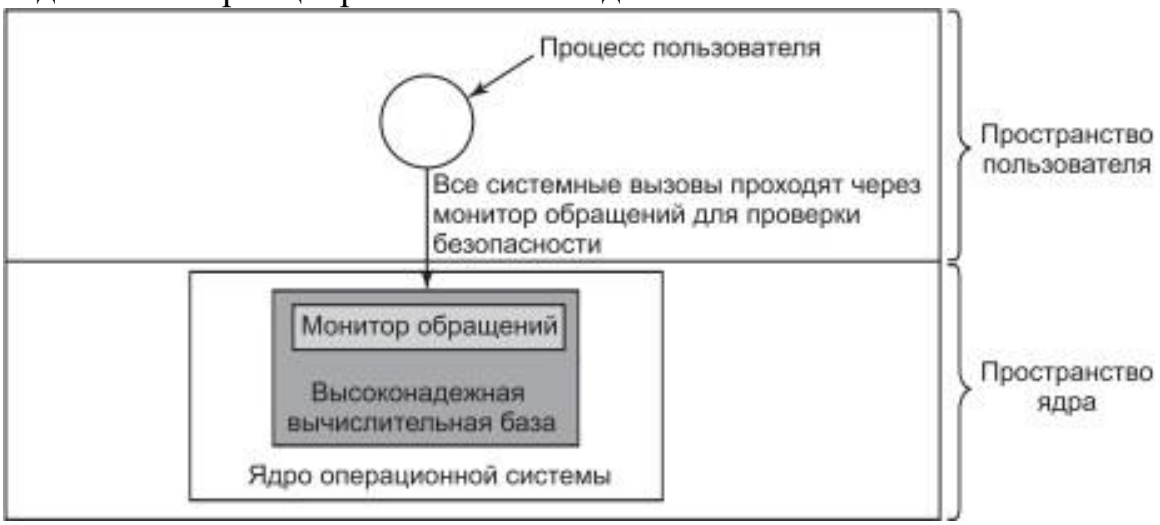
Екінші мысал веб-беттерге қатысты. Бүкіләлемдік ғаламторда пассивті HTML парақтары қолданылған кезде, қауіпсіздікке қатысты маңызды мәселелер туындайтыны ештеңе білдірмейді. Енді көптеген веб-беттерде пайдаланушы мазмұнды көру үшін іске қосатын бағдарламалар (апплеттер мен JavaScript сценарийлері) болған кезде, қауіпсіздік жүйесінде барлық жаңа олқылықтар пайда болады. Олардың біреуін жойғанда, екіншісі пайда болып жатты. Бүкіләлемдік ғаламтор толығымен статикалық сипатқа ие болған кезде, пайдаланушылар екі қолын көтеріп динамикалық толтыруға дауыс берген жағдай болды ма? Қауіпсіздіктің жақсы жүйесі сәнді қоңыраулар мен ысқырықтардан гөрі маңызды деп санайтын бірқатар ұйымдар бар, бұл ең алдымен әскери адамдарға қатысты.

Келесі бөлімдерде бәрін бір сөйлемге келтіруге болатын бірқатар тиісті мәселелер қарастырылады. Қорғалған жүйе құру үшін операциялық жүйенің ядросындағы, оның мәнін әзірлеушілердің түсінуіне оңай болатын қрапайым және кез-келген қысымға төтеп бере алатын, жаңа функционалдылық мүмкіндіктерді қосудан ада ететін қауіпсіздік моделін қолдану керек.

Жоғары сенімді есептеу базасы. Компьютерлік қауіпсіздік мамандарының ортасында қорғалған жүйелер туралы емес, сенімді жүйелер (trusted systems) жайында жиі айтылады. Бұл ресми түрде рәсімделген қауіпсіздік талаптары бар және осы талаптарды орындайтын жүйелер. Әрбір сенімді жүйенің негізінде барлық қауіпсіздік шараларын зорлап орындау үшін қажетті аппараттық және бағдарламалық қамтамасыз етуден тұратын жоғары сенімді есептеу базасы (высоконадежная вычислительная база – TCB (Trusted Computing Basse)) минималды базасы орналасқан. Егер жоғары сенімді есептеу базасы техникалық шарттарға сәйкес жұмыс істесе, жүйенің қауіпсіздігі басқа қолайсыз жағдайлардың бәрінде де бұзылмайды.

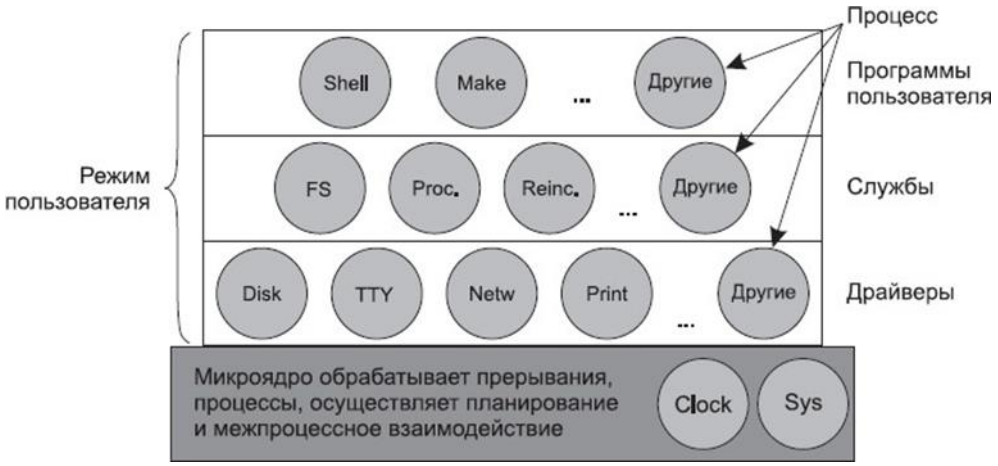
Әдетте, TCB негізінен аппараттық құралдардан (қауіпсіздікке әсер етпейтін енгізу-шығару құрылғыларынан басқа) тұрады, операциялық жүйенің ядросы бөлігінен және артықшылықтары бар пайдаланушы өкілеттіктері бар көптеген немесе барлық тұтынушы (мысалы, UNIX жүйесінің түбірлік каталогындағы SETUID биті орнатылған) программаларынан тұрады. Операциялық жүйенің TCB- ның бөлігі болуға тиіс функцияларына мыналар: үдерісті (процесті) құру, үдерістерді ауыстыру, жадты кескіндеуді басқару және, сонымен қатар, файлдар мен деректерді енгізу-шығаруды басқарудың белгілі бір бөлігі жатады. TCB көбінесе сенімді жүйенің конструкциясында, оның мөлшерін азайту және оның дұрыстығын тексеру үшін, операциялық жүйенің қалған құрылымынан толықтай бөлек ұйымдастырылады.

Жоғары сенімді есептеу базасының маңызды бөлігін қатынасу мониторы құрайды (1-сурет). Ол қауіпсіздікке қатысты барлық жүйелік шақыруларды (үзілімдерді) қабылдайды, мысалы, файлдарды ашуға жасалған жүйелік шақыруға қатысты, оларды өңдеу керек пе, жоқ па, соны шешеді. Осылайша, қатынасу мониторы барлық қауіпсіздік шешімдерін, оларды айналып өтуге жол бермей, бір жерде орналастыруға мүмкіндік береді. Көптеген операциялық жүйелерді ұйымдастыру осы схемадан басқаша боғандықтан, олардың сенімсіздігі себептерінің бірі болып табылады.



1-сурет. Қатынасу мониторы

Қауіпсіздік саласындағы кейбір заманауи зерттеулер мақсаттарының бірі – жоғары сенімді есептеу базасының көлемін бірнеше миллион жолдық кодтан ондаған мыңға дейін азайту. 2-суретте POSIX-үйлесімді жүйе, бірақ Linux немесе FreeBSD-ге қарағанда мүлдем басқа құрылымы бар, MINIX 3 операциялық жүйесінің құрылымы көрсетілген. MINIX 3 ядросында шамамен 10 000 жол бағдарламалық код жұмыс істейді. Қалған код пайдаланушы үдерістерінің жиынтығы ретінде іске қосылады. Ядро кодының бір бөлігі, мысалы, файлдық жүйе және үдеріс менеджері, жоғары сенімді есептеу базасына кіреді, өйткені бұл код жүйенің қауіпсіздігіне оңай нұқсан келтіруі мүмкін. Бірақ қалған бөліктер, мысалы, принтер драйвері және дыбыстық карта драйвері, жоғары сенімді есептеу базасына кірмейді және олардың барлық сәтсіздіктері маңызды емес (олар вирустан туындаған болса да), олар жүйенің қауіпсіздігіне ешқандай нұқсан келтіре алмайды. Жоғары сенімді есептеу базасын екі дәрежеге азайту арқылы MINIX 3 сияқты жүйелер дәстүрлі дизайн шешімдеріне қарағанда қауіпсіздіктің жоғары деңгейін қамтамасыз етуі мүмкін.



2-сурет. MINIX 3 жүйесінің жеңілдетілген құрылымы

Компьютерлік жүйеде қорғауды қажет ететін көптеген ресурстар немесе объектілер бар. Бұл объектілер құрал-жабдықтар (мысалы, орталық процессорлар, жад парақтары, диск жетектері немесе принтерлер) немесе бағдарламалық жасақтама (мысалы, үдерістер, файлдар, мәліметтер базасы немесе семафорлар) болуы мүмкін.

Әр объектінің оған қол жеткізуге болатын ерекше атауы және осы объектіге қатысты үдерістер орындай алатын операциялардың ақырлы жиынтығы болады.Файлға *read* және *write* операциялары, ал семафорға *up* және *down* операциялары тән.Оларға қол жеткізу құқығы жоқ объектілерге кіру үдерістеріне тыйым салу әдісі қажет екені анық. Сонымен қатар, бұл механизм қажет болған жағдайда рұқсат етілген операцияларды таңдау арқылы үдерістерді шектеуге мүмкіндік беруі керек.

Ұсынылған әдебиеттер:

Негізгі әдебиеттер:

1. Нестеров, С. А. Основы информационной безопасности: учебник для вузов/ С. А. Нестеров. - Санкт-Петербург : Лань, 2021., 324 с. — ISBN 978-5-8114-6738-9.

2. Зенков, А. В. Информационная безопасность и защита информации: учебное пособие для вузов / А. В. Зенков. — 2-е изд., перераб. и доп. — Москва: Издательство Юрайт, 2023. — 107 с. — (Высшее образование). — ISBN 978-5-534-16388-9

3. Суворова, Г. М. Информационная безопасность : учебное пособие для вузов / Г. М. Суворова. — 2-е изд., перераб. и доп. — Москва : Издательство Юрайт, 2023. — 277 с. — (Высшее образование). — ISBN 978-5-534-16450-3

Қосымша әдебиеттер:

1. Внуков, А. А. Защита информации : учебное пособие для вузов / А. А. Внуков. — 3-е изд., перераб. и доп. — Москва : Издательство Юрайт, 2023. — 161 с. — (Высшее образование). — ISBN 978-5-534- 07248-8

2. Казарин, О. В. Надежность и безопасность программного обеспечения : учебное пособие для вузов / О. В. Казарин, И. Б. Шубинский. — Москва : Издательство Юрайт, 2023. — 342 с. — (Высшее образование). — ISBN 978-5-534-05142-1

3. Корабельников, С. М. Преступления в сфере информационной безопасности : учебное пособие для вузов / С. М. Корабельников. — Москва : Издательство Юрайт, 2023. — 111 с. — (Высшее образование). — ISBN 978-5-534-12769-0