Дәріс 6. Ақпараттық қауіпсіздік модельдері және оларды қолдану

Жоспары:

1 Операциялық жүйелерді қорғау механизмдері
2 Қазіргі операциялық жүйелердің қауіпсіздігін талдау
3 Windows амалдық жүйесінің қауіпсіздік жүйесі
4 Unix операциялық жүйесінде қорғау
5 Novell NetWare операциялық жүйесінде қорғау

Операциялық жүйелерді қорғау механизмдері

Операциялық жүйе-бұл жүйенің ресурстарын (компьютерлер, есептеу жүйелері, әуе кемелерінің басқа компоненттері) оларды тиімді пайдалану мақсатында басқаратын және ресурстармен пайдаланушы интерфейсін қамтамасыз ететін арнайы ұйымдастырылған бағдарламалар жиынтығы.

Операциялық жүйелер, компьютердің аппаратурасы сияқты, олардың даму жолында бірнеше ұрпақ өтті.

Бірінші буын ОЖ пайдаланушының бір тапсырмасынан екінші тапсырмаға (басқа пайдаланушыға) ауысуды жеделдетуге және жеңілдетуге бағытталған, бұл әртүрлі тапсырмаларға жататын деректердің қауіпсіздігін қамтамасыз ету мәселесін тудырды.

ОЖ-нің екінші буыны енгізу-шығару операцияларының бағдарламалық жасақтамасын құрумен және үзілістерді өңдеуді стандарттаумен сипатталды. Тұтастай алғанда деректердің қауіпсіздігін сенімді қамтамасыз ету шешілмеген мәселе болып қала берді.

60-жылдардың аяғында XX ғ. Вт қаражатын мультипроцессорлық ұйымдастыруға көшу басталды, сондықтан ресурстарды бөлу және оларды қорғау мәселелері өткір және шешілмейтін болды. Бұл мәселелерді шешу ОЖ-ны тиісті ұйымдастыруға және аппараттық құралдарды кеңінен қолдануға әкелді (жадты қорғау, аппараттық бақылау, диагностика және т.б.).

Есептеу техникасын дамытудың негізгі тенденциясы оның пайдаланушылар үшін максималды қолжетімділігі идеясы болды және болып қала береді, бұл деректердің қауіпсіздігін қамтамасыз ету талабына қайшы келеді.

ОЖ қорғау механизмдері деп ОЖ құрамында жұмыс істейтін деректерді қорғаудың барлық құралдары мен механизмдерін түсінеміз. Деректерді қорғау құралдары мен механизмдері жұмыс істейтін операциялық жүйелер көбінесе қорғалған жүйелер деп аталады.

ОЖ қауіпсіздігі деп ОЖ жұмысының кездейсоқ немесе қасақана бұзылуы, сондай-ақ ОЖ басқаруындағы жүйелік ресурстардың қауіпсіздігін бұзу мүмкін болмайтын ОЖ күйін түсінеміз. ОЖ қауіпсіздігін қамтамасыз ету мәселелерін ерекше санатқа бөлуге мүмкіндік беретін ОЖ-нің келесі ерекшеліктерін

көрсетейік:

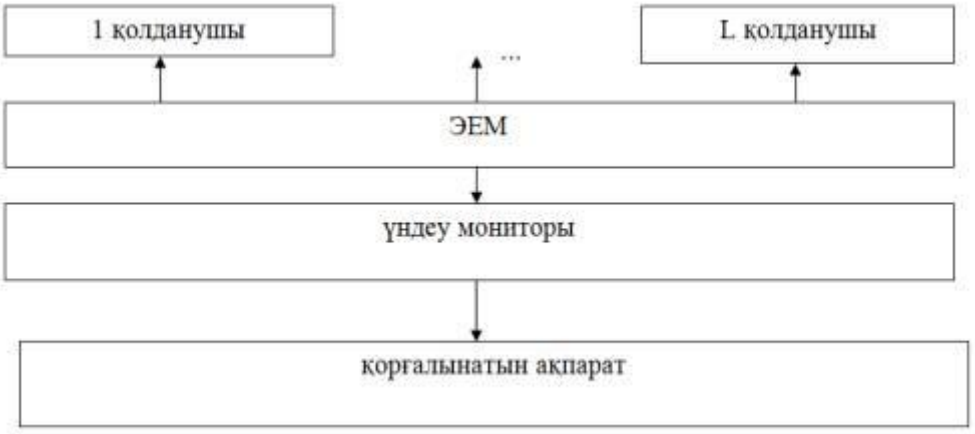
- жүйенің барлық ресурстарын басқару;

- ОЖ ортасында жұмыс істейтін бағдарламалар мен деректердің қауіпсіздігіне тікелей немесе жанама әсер ететін кіріктірілген механизмдердің болуы;

- жүйе ресурстарымен пайдаланушы интерфейсін қамтамасыз ету;

- ОЖ өлшемдері мен күрделілігі.

Көптеген қорғалған ОЖ құрастыру мен оны іс жүзінде іске асыру Харрисон, Руззо, Ульманды қорғалған жүйенің формалды моделін құрастыруға септігін тигізді. Харрисон – Руззо – Ульманның (HRU-моделі) моделдерінің сызбасы 1-суретте келтірілген.



Сурет 1. Харрисон, Руззо және Ульманның моделдер сызбасы

Қазіргі универсалды ОЖ көмегімен АС 1В қорғаныстық кластары үшін орындалатын процестерді анализдеу шын мәнінде маңызды емес. Көптеген ОЖ үшін негізгі мәліметтер қосымшаларына арналған ресурстарға деген қолжетімділікті басқарудың мандатты механизмі толық орындалмайды не болмаса оның ең негізгі мынадай талаптары орындалмауы мүмкін, ақпараттар ағынын басқару құпиялықты анықтау әдісімен жасалуы керек. Сонымен қатар жинағыштың құпиялық деңгейі соған жазылып отырған ақпараттың құпиялық деңгейінен кем болмауы тиіс. Осыған байланысты біз тек АС 1Г класстары үшін ОЖ қорғаныстық құралдарының мүмкін болатын сәйкестіктері туралы айтамыз (құпия ақпарттарды қорғау).

Берілген сызбада қолданушы тәжірибе жүзінде қорғаныс әкімшісі секілді сенімге ие болуға тиіс және сол секілді компьютер қорғанысын қамтамасыз етуге жауап беруі тиіс. Айта кететін жайт, берілген тұжырымдама көптеген кейінгі қосымшаларда қолданылады, нақты айтатын болсақ, деректер қорын басқару жүйесі (ДҚБЖ), мұнда қолданушы өзінің құқықтарын қорғалып отырған ресурстар қолжетімділігіне жұмсауы мүмкін. Сонымен қоса, үлкен көлемде

соңғы қолданушыдан компьютерлік ақпараттың қорғаныс механизмдері болмаса, берілген тұжырымдама бойынша қолданушыны потенциалды құқық бұзушы ретінде қарастыра алмаймыз.

Операциялық жүйелердің қауіпсіздігі

Компьютерлік жүйелердің қауіпсіздігін бұзудың көптеген жолдары бар. Мысалы, көптеген адамдар өздерінің PIN-кодтары үшін 0000 комбинациясын орнатады немесе пароль ретінде " password" сөзін қолданады — оларды есте сақтауоңай, бірақ қауіпсіздіктің жоғары деңгейін қамтамасыз етпейді. Кейбір адамдар естесақтау мүмкін емес өте күрделі парольдерді де ойлап табады және оларды мониторғанемесе пернетақтаға орналастырылған жапсырмаларға жазуға мәжбүр болады. Машинаға физикалық қол жетімділігі бар кез-келген адам (тазалаушылар, хатшыларжәне барлық келушілерді қоса) ондағы барлық нәрсеге қол жеткізе алады. Басқа да көптеген мысалдар бар, олардың ішінде жоғары лауазымды тұлғалардың құпия ақпараты бар USB дискілерін жоғалту, қоқыс тастамас бұрын дұрыс тазаланбаған өндірістік құпиялары бар ескі қатты дискілер және т. б.

Дегенмен, қауіпсіздікке қатысты ең маңызды оқиғалар күрделі кибершабуылдарға жатады. Бұл кітапта операциялық жүйелерге қатысты шабуылдарға ерекше назар аударылады. Басқаша айтқанда, біз веб-шабуылдарды немесе SQL дерекқорларына шабуылдарды қарастырмаймыз. Оның орнына, біз операциялық жүйелерге бағытталған немесе қауіпсіздік саясатын орындауда(немесе көбінесе орындауға кедергі келтіруде) маңызды рөл атқаратын шабуылдарғаназар аударамыз. Жалпы, біз ақпаратты пассивті түрде ұрлауға тырысатын шабуылдар мен компьютерлік бағдарламаның әрекетін бұзуға тырысатын шабуылдарды ажыратамыз.

Пассивті шабуылдың мысалы-желі трафигіне қосылған және деректерді алу үшін шифрды бұзуға тырысатын жау. Белсенді шабуыл кезінде зиянкес зиянды кодты орындауға мәжбүрлей отырып, мысалы, кредит картасының деректемелерін ұрлау үшін пайдаланушының веб-браузерін басқаруды ала алады. Сол сияқты, біз хабарламаны немесе файлды толығымен кілтсіз бастапқы деректерді қалпына келтіруді қиындататын жолмен араластыруға арналған криптографияны және бағдарламаларға қорғаныс механизмін қосатын, бұзушыларға олардың мінез- құлқын өзгертуді қиындататын бағдарламаларды (hardening) нығайтуды ажыратамыз.

Операциялық жүйе көптеген жерлерде криптографияны қолданады: желі арқылы деректерді қауіпсіз беру, файлдарды дискіде қауіпсіз сақтау, пароль файлындағы құпия сөздерді шифрлау және т. б. Бағдарламаларды нығайту да кеңінен қолданылады: бұзушылардың жұмыс істеп тұрған бағдарламаға жаңа кодтыенгізуіне жол бермеу үшін, әрбір процестің өзіне қажетті және ол үшін көзделген, 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 оқымау мүмкін емес. Бұл жағдайда сіз екі қарапайым және өте қисынды сұрақ қоя аласыз:

1. Қорғалған компьютерлік жүйені құру мүмкін емес пе?
2. Олай болса, неге ол әлі жасалмаған?

Бірінші сұрақтың жауабы: "Теориялық түрде мүмкін". Негізінде, бағдарлама қателіктерден құтылуы мүмкін және егер бұл бағдарлама тым үлкен немесе күрделіболмаса, біз оның қауіпсіздігін қамтамасыз ете 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 қауіпсіз емес, бірақ пайдаланушылар олардан бас тартқысы келмейді. Мысалы, егер Microsoft Windowsжүйесінен басқа, оның вирусқа қарсы иммунитеті бар, бірақ Windows қосымшаларын орындамайтын жаңа өнімі 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 сақтау. Функционалдылық мүмкіндіктер -қауіпсіздіктің жауы болып табылады. Көптеген технологиялық компаниялардағы маркетинг бөлімінің батыл жігіттері (дұрыс па, жоқ па) пайдаланушылар көбірек функционалдылықты, одан да кең және сапалы мүмкіндіктерді қалайды деп болжайды.

Олар өздерінің бағдарламалық өнімдерінің жүйелік құрылымдарын жасаушылар бұл үшін тиісті нұсқаулар алатынына сенімді. Бірақ мұның бәрі жүйенің күрделілігін, кодтың көбеюін, 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 болады. Пошта бағдарламаларында қателіктер болса да, ASCII хабары компьютерлік жүйенібұзуы мүмкін (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 компьютерде 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, қауіпсіздіктің маңызды мәселелерін ештеңе білдірмеді. Енді көптеген веб-беттерде пайдаланушы мазмұнды көру үшін іскеқосатын бағдарламалар (апплеттер мен JavaScript сценарийлері) болған кезде, қауіпсіздік жүйесінде барлық жаңа олқылықтар пайда болады. Олардың біреуін ғана жою керек, оның орнында екіншісі пайда болады. Бүкіләлемдік ғаламтор толығымен статикалық сипатқа ие болған кезде, пайдаланушылар динамикалық толтыруға дауыс беру кезінде екі қолын көтерді ме? Қауіпсіздіктің жақсы жүйесі сәнді қоңыраулар мен ысқырықтардан гөрі маңызды деп санайтын бірқатар ұйымдар бар, бұл ең алдымен әскери адамдарға қатысты. Келесі бөлімдерде бір сөйлемге келтіруге болатын бірқатар тиісті мәселелер қарастырылады. Қауіпсіз жүйені құру үшін сіз операциялық жүйенің өзегіндегі қауіпсіздік моделін қолдануыңыз керек, оны әзірлеушілер оның мәнін түсінуге оңай болар еді және кез-келген қысымға төтеп бере алады, жаңа функционалдылықты қосудан аулақ бола алады

Жоғары сенімді есептеу базасы компьютерлік қауіпсіздік мамандарының шеңберлерінде қорғалған жүйелер туралы емес, сенімді жүйелер туралы жиі айтылады. Бұл ресми түрде белгіленген қауіпсіздік талаптары бар және осы

талаптарды орындайтын жүйелер. Әрбір сенімді жүйенің негізінде барлық қауіпсіздік шараларын орындау үшін қажетті аппараттық және бағдарламалық қамтамасыз етуден тұратын TCB (Trusted Computing Basse) минималды базасы (сенімді есептеу базасы — жоғары сенімді есептеу базасы) орналасқан. Егер жоғарысенімді есептеу базасы техникалық шарттарға сәйкес жұмыс істесе, жүйенің қауіпсіздігі басқа қолайсыз жағдайларда бұзылмайды.

Әдетте, TCB негізінен аппараттық құралдардан тұрады (қауіпсіздікке әсер етпейтін кіріс құрылғыларынан басқа), операциялық жүйенің негізгі бөлігі және артықшылықты пайдаланушы өкілеттіктері бар көптеген немесе барлық пайдаланушы бағдарламалары (мысалы, UNIX жүйесінің түбірлік каталогында SETUID биті орнатылған бағдарламалар). TCB бөлігі болуы керек операциялық жүйенің функциялары мыналарды қамтиды: процесті құру, процестерді ауыстыру, жад дисплейін басқару, сонымен қатар файлдарды басқару және деректерді енгізу- шығару бөлігі. Сенімді жүйенің дизайнында TCB көбінесе оның мөлшерін азайту және оның дұрыстығын тексеру үшін операциялық жүйенің қалған бөлігінен толығымен бөлінеді. Жоғары сенімді

есептеу базасының маңызды бөлігі – үндеу мониторы (1-сурет). Ол қауіпсіздікке қатысты барлық жүйелік қоңырауларды қабылдайды, мысалы, файлдарды ашуға қоңырау шалып, оларды өңдеу керек пе, жоқ па, соны шешеді. Осылайша, үндеу мониторы барлық қауіпсіздік шешімдерін бір жерде орналастыруға мүмкіндік береді, оларды айналып өтуге жол бермейді. Көптеген операциялық жүйелерді ұйымдастыру осы схемадан ерекшеленеді, бұл олардың сенімсіздігінің себептерінің бірі.

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
4. https://adilet.zan.kz/kaz/docs/Z990000349
5. https://adilet.zan.kz/kaz/docs/U060000199_

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