**Дәріс 7. Ресурстарға қол жеткізуді басқару. Қорғау домендері. Қол жеткізуді басқару тізімдері. Мүмкіндіктер тізімі**

Жоспары:

1 Қауіпсіздік ресурстарына қол жеткізуді басқару
2 Кіруді басқару тізімдері
3 Қорғау жүйесінің жұмысы
4 Мүмкіндіктер тізімі

**Қауіпсіздік ресурстарына қол жеткізуді басқару**. Егер не қорғалуы керек, кімге және не істеуге рұқсат етілетіні туралы нақты модель болса, қауіпсіздікке қол жеткізу оңайырақ болып табылады. Бұл салада өте үлкен жұмыс жасалды, сондықтан осы қысқаша сипаттамада біз тек үстірт шолу жасайтын боламыз. Біз оларды қолданудың бірқатар жалпы модельдері мен тетіктеріне ғана назар аударамыз.

**Қорғау домендері**. 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. Мысалы, *A* процесіне *F* файлынан деректерді оқу құқығы берілуі мүмкін, бірақ оған бұл файлға жазуға рұқсат етілмейді. Қорғаудың әртүрлі механизмдерінқарастыру үшін домен ұғымын енгізген пайдалы. **Домен** (*domain*) жұптар жиынынан(объект, қол жеткізу құқығы) тұрады. Әр жұп объектіні және сол объектіге қатысты орындалуы мүмкін операциялардың ішкі жиыны болып табылады. **Қол жеткізу құқығы** (*rights*) осы контексте белгілі бір операцияны орындауға берілетін рұқсат түрін анықтайды. Көбінесе домен жеке қолданушымен байланысты болады, бұл пайдаланушы не істей алатындығы немесе, керісінше, не істей алмайтындығы туралы хабарлайды, бірақ ол жеке пайдаланушыға ғана емес, жалпы сипатқа да иеболуы мүмкін. Мысалы, бір жобада жұмыс істейтін бір бағдарламашылар тобының қызметкерлері толығымен бір доменге тиесілі және жоба файлдарына қол жеткізеалады.

Объектілерді домендер бойынша бөлу кімге және олардың не туралы білуі керек екеніне байланысты

Дегенмен, іргелі ұғымдардың бірі – ең төменгі билік принципі (Principle of Least Authority (POLA)) немесе қажетті білім принципі. Жалпы, әр доменде олармен жұмыс істеу үшін минималды объектілер мен артықшылықтар болған кезде және артық ештеңе болмаған кезде қауіпсіздікті сақтау оңайырақ.

2-суретте әр объектіге қатысты әрқайсысында объектілері бар және оқу, жазу және орындау құқықтары бар үш домен көрсетілген (Read, Write, eXecute). Printer1 объектісі бір уақытта екі доменде болатындығын және олардың әрқайсысында бірдей құқықтарға ие екенін ескеріңіз. File1 объектісі екі доменде де бар, бірақ олардың әрқайсысында әртүрлі құқықтарға ие.

Кез-келген уақытта әр процесс қандай да бір қорғаныс доменінде жұмыс істейді. Басқаша айтқанда, оған қол жеткізуге болатын объектілердің белгілі бір жиынтығы болады және әр объект үшін белгілі бір құқықтар жиынтығы көзделген. Жұмыс кезінде процесстер бір доменнен екіншісіне ауыса алады. Домендер арасында ауысу ережелері белгілі бір жүйеге байланысты.


2-сурет. Үш қорғау домені

Қорғау домені идеясын нақтылау үшін UNIX жүйесінен мысал келтіруге болады (Linux, FreeBSD және оларға ұқсас клондарға да қатысты). UNIX-те процестің домені оның UID және GID идентификаторларымен анықталады. Пайдаланушы кірген кезде оның қабығы пароль файлындағы жазбасында бар UID және GID алады және олар оның барлық ұрпақ үдерістеріне мұра болады. Кез-келген комбинацияны (UID, GID) ұсына отырып, сіз барлық объектілердің толық тізімін жасай аласыз (файлдар, соның ішінде арнайы файлдар түрінде ұсынылған енгізу- шығару құрылғылары және т. б. д.), оған қол жеткізудің мүмкін түрін (оқу, жазу, орындау) көрсете отырып, процесс жүгіне алады. Бірдей (UID, GID) комбинациясы бар екі процесс бірдей объектілер жиынтығына бірдей қол жеткізе алады. Дегенмен әр түрлі (UID, GID) мәндерге ие үдерістер әр түрлі файл жиындарына, бұл жиындардың айтарлықтай қабаттасуымен де, қол жеткізе алады.

Сонымен қатар, UNIX-тегі әр процесс екі бөліктен тұрады: тұтынушылық және жүйелік (ядрода орындалатын) режимдерде жұмыс істейтін. Процесс жүйелік шақыруды жүзеге асырған кезде, ол пайдаланушы бөлігінен жүйеге ауысады. Пайдаланушымен салыстырғанда, жүйелік бөлік басқа объектілер жиынтығына қол жеткізе алады. Мысалы, процестің жүйелік бөлігі физикалық жадтағы барлық беттерге, бүкіл дискіге және барлық басқа қорғалған ресурстарға қол жеткізе алады. Осылайша, жүйелік шақыру қорғаныс домендерін ауыстырудың себебі болып табылады.

Процесс exec жүйелік жүйелік шақыруды жүзеге асырған кезде, ол SETUID биті немесе SETGID биті орнатылған файлға қатысты, ол жаңа жарамды UID немесе GID идентификаторын алады. Басқа комбинациямен (UID, GID) ол қол жетімді файлдар мен операциялардың басқа жиынтығына ие болады. Орнатылған SETUID битімен немесе SETGID битімен бағдарламаны іске қосу доменнің ауысуына себеп болады, өйткені кіру құқықтары өзгереді. Жүйе объектінің белгілі бір объектіге тиесілігін қалай қадағалайтынын білу маңызды. Концептуалды түрде үлкен матрицаны елестетуге болады, ондағы жолдар домендер, ал бағандар объектілер болады. Әрбір ұяшықта, егер бар болса, домен объектіге қатысты иеленетін құқықтар тізімделеді. 3-суретте 2-сурет үшін құрылған матрица көрсетілген. Осы матрица мен ағымдағы домен нөмірінің көмегімен операциялық жүйе белгілі бір доменнен берілген объектіге кірудің белгілі бір түріне рұқсат етілгенін анықтай алады. Егер сіз enter кіру операциясына рұқсат етілуі мүмкін доменнің өзін объект ретінде елестетсеңіз, домендер арасындағы ауысуды сол кестелік модельге оңай қосуға болады. 4-суретте қайтадан 3-суреттегі матрица көрсетілген, бірақ бұл жағдайда объектілер ретінде үш доменнің өзі пайда болады. 1-домендегі үдерістер 2-доменге ауыса алады, бірақ олар енді қайта орала алмайды.

Бұл жағдай UNIX-те орнатылған SETUID битімен бағдарламаның орындалуын модельдейді. Бұл мысалда басқа домендерді ауыстыруға рұқсат етілмейді.

| | Объект | | | | | | | |
|---|---|---|---|---|---|---|---|---|
| Домен | Файл 1 | Файл 2 | Файл 3 | Файл 4 | Файл 5 | Файл 6 | Принтер 1 | Плоттер 2 |
| 1 | Чтение | Чтение<br>Запись | | | | | | |
| 2 | | | Чтение | Чтение<br>Запись<br>Исполнение | Чтение<br>Запись | | Запись | |
| 3 | | | | | | Чтение<br>Запись<br>Исполнение | Запись | Запись |

3-сурет. Қорғаныс матрицасы

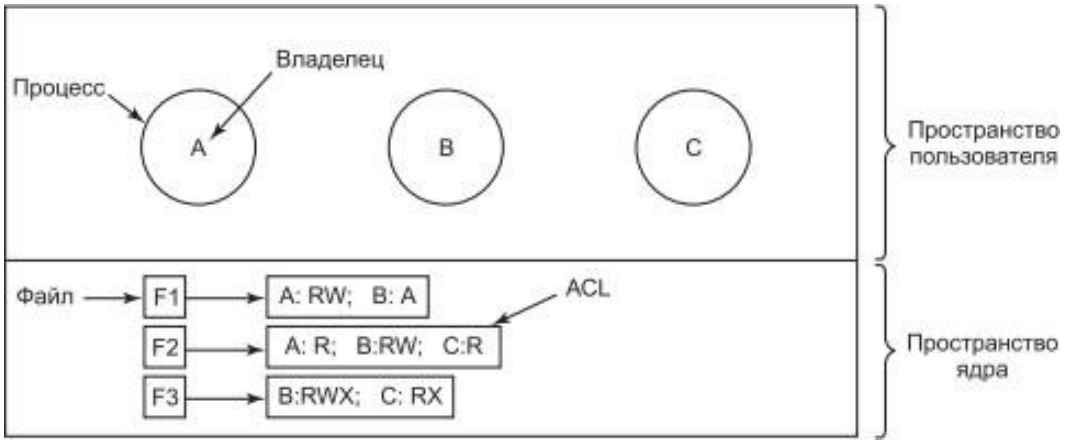

4-сурет. объектілер ретінде домендермен анықталған қорғаныс матрицасы

**Кіруді басқару тізімдері**

Іс жүзінде 4-суретте көрсетілген матрица, ол үлкен мөлшерде және таусылған сипатқа байланысты сирек қолданылады. Көптеген домендерде көптеген объектілерге мүлдем қол жетімділік жоқ, сондықтан диск кеңістігі өте үлкен, іс жүзінде бос матрицаны сақтау үшін үлкен ысырап болады. Сондықтан келесі екі әдіс практикалық қолдану тапты: матрицаны жолдар немесе бағандар бойынша сақтау, содан соң тек толтырылған элементтерді сақтау. Бір таңқаларлығы, бұл екі тәсіл бір-бірінен ерекшеленеді. Бүгін (бұл бөлімде) ақпаратты бағандар бойынша, ал келесі бөлімде жолдар бойынша сақтау қарастырылады.

Бірінші әдісте әр объектімен белгілі бір объектіге кіруге рұқсат етілген барлық домендерді, сондай-ақ кіру түрін қамтитын реттелген тізім байланыстырылады. Мұндай тізім 5-суретте көрсетілген. Ол **ACL** (Access Control List – қол жеткізуді басқару тізімі) деп аталады. Мұнда *A, B* және *C* домендеріне жататын үш процесс, сонымен қатар үш файл көрсетілген: *F1, F2* және *F3*. Жағдайды жеңілдету үшін әр доменге тек бір қолданушы сәйкес келеді делік, бұл жағдайда *A, B* және *C* пайдаланушылары. Ақпараттық қауіпсіздік әдебиетінде тұтынушылар көбіне **субъектілер** (*subjects*), **принципиалдар** (*principals*) немесе осы ортада есептік жазбасы бар пайдаланушылар деп аталады (олардың иелерін белгілі бір жерлерден,

объектілерден **(objects)** ажырату үшін, мысалы, оларға файлдарды жатқызуға болады).




5-сурет. Файлдарға қол жеткізуді басқару үшін қол жеткізуді басқару тізімдерінпайдалану

Әр файлда онымен байланысты ACL бар. F1 файлының ACL тізімінде екі жазбабар (нүктелі үтірмен бөлінген). Бірінші жазбада А пайдаланушысының кез-келген процесі осы файлға қатысты оқу және жазу операцияларын жүргізе алады. Екінші жазбада В пайдаланушысының кез-келген процесі осы файлды оқи алады.Пайдаланушы деректеріне қол жеткізудің барлық басқа түрлеріне және басқа пайдаланушыларға қол жеткізудің барлық түрлеріне тыйым салынады. Құқықтар процеске емес, пайдаланушыға берілетініне назар аударыңыз. Қорғау жүйесінің жұмысының нәтижесінде А пайдаланушысының кез-келген процесі *F1* файлына қатысты оқу және жазу операцияларын орындай алады. Мұндай үдерістер қанша болуы маңызды емес. Процестің идентификаторы емес, процестің иесі кім екендігі маңызды.

*F2* файлының ACL тізімінде үш жазба бар: *A, B* және *C* пайдаланушылары файлды оқи алады,ал В пайдаланушысы да оған жаза алады. Қол жеткізудің басқа түрлеріне рұқсат етілмейді. *F3* файлы орындалатын бағдарлама екені анық, өйткені*A* және *B* пайдаланушылары бұл файлды оқи да, орындай да алады. *B* пайдаланушысына оған жазба жүргізуге рұқсат етіледі. Бұл мысал ACL тізімдері арқылы қорғаудың жалпы формасын көрсетеді. Іс жүзінде неғұрлым күрделі жүйелер жиі қолданылады. Бастау үшін, мұнда тек үш кіру құқығы көрсетілген: оқу, жазу және орындау. Олардан басқа, басқа қол жетімділік құқықтары болуы мүмкін. Құқықтардың бір бөлігі жалпы сипатқа ие болуы мүмкін, яғни барлық объектілергетаралуы мүмкін, ал бір бөлігі объектіге нақты байланысты болуы мүмкін. Жалпы сипаттағы құқықтардың мысалдары **объектіні жою** (*destroy object*) және **объектіні көшіру** (*copy object*) құқығы болуы мүмкін, олар түріне қарамастан кез-келген объектіге тиесілі болуы мүмкін. Нысанға ерекше қатысы бар құқықтарға пошта жәшігі объектісіне

**хабарлама қосу** құқығы (*append message*) және каталог объектісі үшін **алфавиттік ретпен сұрыптау** құқығы (*sort alphabetically*) кіреді.

Осы уақытқа дейін ACL тізіміндегі жазбалар жеке пайдаланушыларға тиесілі болды. Көптеген жүйелер пайдаланушылар тобы (group) тұжырымдамасын қолдайды. Топтардың атаулары бар және оларды ACL тізімдеріне де қосуға болады. Топтардың семантикасында екі мүмкін нұсқа бар. Кейбір жүйелерде әр процесте UID пайдаланушысының идентификаторы және GID тобының идентификаторы бар. Мұндай жүйелерде ACL тізімдерінде көрініс жазбалары бар UID1, GID1: Құқық 1; UID2, GID2: Құқық 2;...

Нысанға кіру туралы сұрау түскен жағдайда, осы сұрауды берген адамның UID және GID тексерісі жасалады. Егер бұл идентификаторлар ACL тізімінде болса, онда тізімде көрсетілген құқықтар беріледі. Егер комбинациялар(UID, GID) тізімде болмаса, кіруге рұқсат етілмейді.

Негізінде, топтарды қолдану рөл (role) ұғымын енгізеді. Tana жүйелік әкімші болып табылатын есептеу орталығын қарастырсақ, ол sysadm тобына кіреді. Бірақ компанияда қызметкерлерге арналған клубтар бар делік және Тана– көгершін әуесқойлары клубының мүшесі болсын. Клуб мүшелері pigfan тобына жатады және көгершін деректер базасын жүргізу үшін компанияның компьютерлеріне қол жеткізе алады. ACL тізімінің бөлігі 2-кестеде көрсетілген көрініске ие болуы мүмкін.

2-кесте. Қол жеткізуді басқарудың екі тізімі

| **Файл** | **Қолжетімділікті басқару тізімі** |
|---|---|
| Password | tana, sysadm: RW |
| Pigeon data | bill, pigfan: RW; tana, pigfan: RW; |

Егер Тана осы файлдардың біріне кіруге тырысса, нәтиже оның қай топқа кіргеніне байланысты болады. Тіркеу кезінде жүйе өзінің қай тобын пайдаланғысы келетінін немесе топтарға кіруді бөлек сақтау үшін әр түрлі атаулар және/ немесе парольдер болуы мүмкін екенін сұрауы мүмкін. Бұл схеманың мәні-Тана өзінің Көгершін хоббиімен айналысқан кезде пароль файлына қол жеткізе алмауы. Ол жүйеде жүйелік әкімші ретінде тіркелген жағдайда ғана пароль файлына қол жеткізе алады.

Кейбір жағдайларда пайдаланушыға белгілі бір файлдарға қол жетімділік берілуі мүмкін, ол қазіргі уақытта топқа жатады. Мұны кез-келген нәрсені білдіретін топтық таңбаны (wildcard) пайдалану арқылы ұйымдастыруға болады. Мысалы,

tana,* :RW

жазбасы пароль файлындағы Таняға қазіргі уақытта қай топқа жататынына қарамастан қол жеткізуге мүмкіндік береді.

Тағы бір мүмкіндік – кез-келген топқа кіретін және белгілі бір қол жетімділік құқығы бар пайдаланушы осы құқықтарды алады. Артықшылығы – бір уақытта бірнеше топқа кіретін пайдаланушы тіркелу кезінде қай топты пайдалану керектігін көрсетпеуі керек. Олардың барлығы оның бүкіл жұмысы барысында ескеріледі. Бұл тәсілдің кемшілігі–бұл инкапсуляцияның аз дәрежесін қамтамасыз етеді.

Топтар мен топтық таңбаларды пайдалану белгілі бір пайдаланушының файлға кіруін іріктеп бұғаттауға мүмкіндік береді. Мысалы,

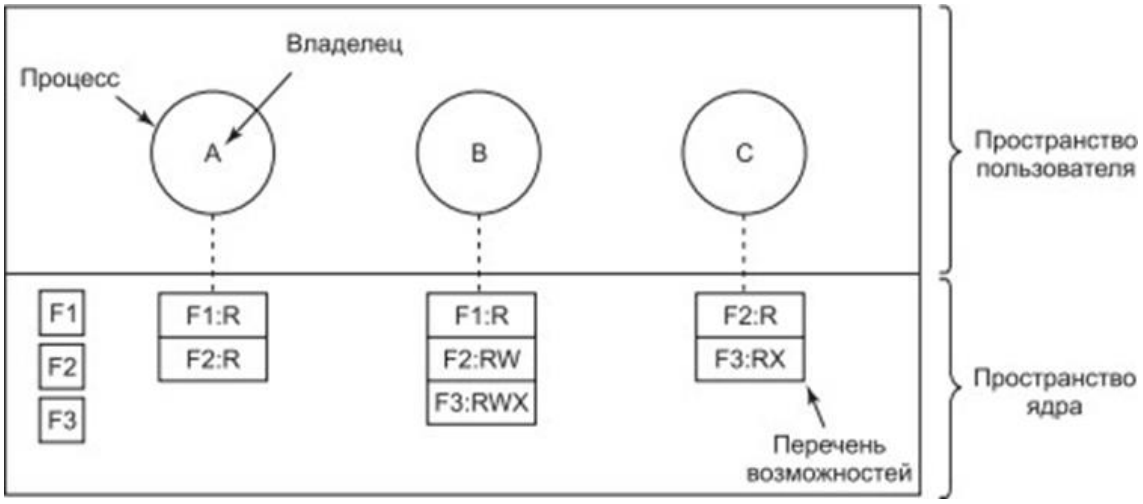
virgil, *: (none); *, *: RW

жазбасы оқуға арналған файлды оқу және жазу құқын немесе мүмкіндігін Вирджил (Virgil) атты тұтынушыдан басқа барлық пайдаланушыға береді. Бұл жазба рет-

ретімен жазылғандықтан жұмыс істейді және олардан бірінші сәйкес келеді, ал кейінгі жазбалар тіпті талданбайды.

5-суретте көрсетілген матрицаны, сондай-ақ жолдармен жазуға болады. Бұл әдісті қолданған кезде әр процеске қол жеткізуге болатын объектілердің тізімі, сондай-ақ әр объектімен қандай операцияларға рұқсат етілгені туралы ақпарат, басқаша айтқанда, оның қорғау домені байланысты болады. Мұндай тізім мүмкіндіктер тізімі (capability list, C-list) деп аталады, ал оның элементтері – мүмкіндіктер (capabilities) (Dennis and Van Horn, 1966; Fabry, 1974).

6-суретте үш процестің жиынтығы және олардың мүмкіндіктер тізімі көрсетілген.




6-сурет. Мүмкіндіктерді пайдалану кезінде әр процесс олардың тізімін алады

Мүмкіндіктер тізімінің әр элементі иесіне белгілі бір объектіге қатысты белгілі бір құқықтар береді. Мысалы, 6-суретте А пайдаланушысы иелік ететін процесс F1 және F2 файлдарын оқи алады. Әдетте, мүмкіндіктер тізімінің элементі файл идентификаторынан (немесе жалпы жағдайда объекттен) және

әртүрлі құқықтарға арналған бит массивінен тұрады. UNIX отбасылық (семейства) операциялық жүйелерінде файл идентификаторы ретінде оның і-ші түйінінің нөмері пайдаланылуы мүмкін. Мүмкіндіктер тізімі өздері объектілер болып табылады және оларды басқа мүмкіндіктер тізімдері көрсете алады және, осылайша, қосалқы домендерді (субдомендерді) пайдалануды жеңілдетеді.

**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