Подсистема обеспечения безопасности в ОС

Общие сведения

Основные задачи ИБ – обеспечить:

– Конфиденциальность

– Целостность

– Доступность

Подсистема обеспечения безопасности ОС предназначена для решения этих задач.

Для определения требований к защите формируется модель угроз:

– Естественные и техногенные угрозы

– Антропогенные угрозы

Источники антропогенных угроз

- Внешние нарушители (не имеют легального идентификатора в системе). Доступ к атакуемой системе через терминал, разъемы ПЭВМ и сеть (при условии известности адреса компьютера). Цель – получить в системе идентификатор с максимальными правами доступа
- Внутренние нарушители (имеют легальный идентификатор и набор прав и привилегий)
  - Преднамеренные
  - Непреднамеренные

Защита от неантропогенных угроз

- Резервные копии ценной информации
- Зеркалирование
- Использование журналирования (для баз данных и файловых систем)
- Использование источников бесперебойного питания с обратной связью

Защита от внешних нарушителей

Процедура входа в систему:

– Предъявление идентификатора (имя, аппаратное устройство, биометрия)
– Предъявление аутентификатора (пароль, аппаратное устройство, биометрия)
– Проверка идентификатора
– Аутентификация
– Авторизация

Защита от внутренних нарушителей

Программы (субъекты), управляемые или неуправляемые человеком.

Для расширения прав используются:

– «Троянские кони»
– Перехват аутентификаторов
– Различные уязвимости операционной системы или субъектов с большими правами в системе (в первую очередь – переполнение буфера)

TCB

(высоконадежная вычислительная база)

Включает в себя аппаратное обеспечение, ядро ОС и драйверы устройств.

Обязана быть защищена от субъектов ОС.

На действия, осуществляемые TCB не распространяются ПРД.

В обязательном порядке содержит монитор обращений (диспетчер доступа)

Модели разграничения доступа

Дискреционная модель

– Домены защиты. Каждый субъект принадлежит одному домену безопасности. Домен определяется UID и GID субъекта.
– Списки доступа. Объект хранит в своем составе права доступа к нему субъектов. Субъект содержит маркер безопасности.

Мандатная модель

– Белла-Ла Падуллы (NRU, NWD)
– Биба

ОС Windows

Класс С2:

- Механизм безопасной регистрации – доступ только после аутентификации
- Дискреционная модель безопасности
- Аудит безопасности
- Очистка при повторном использовании
- Безопасная аутентификация
- Элементы ролевой модели

ОС Windows – ОУД 1+

Дополнительные требования :

- Функции управления дискреционным доступом – на основании криптографии(EFS)
- Политика управления избирательным доступом – для дополнительных объектов
- Внутренняя репликация для распределенных компонентов
- Утилизация ресурсов для дисков (NTFS)
- Блокировка интерактивного сеанса и безопасная аутентификация
- Защита передачи данных между распределенными компонентами
- Систематическое устранение уязвимостей

Компоненты системы защиты-1

- Монитор состояния защиты – обслуживание объекта маркера доступа, проверка прав, обработка привилегий и генерация сообщений аудита безопасности (SRM)
- Подсистема локальной AU – политика безопасности, AU пользователей, сообщения аудита для журнала
- База данных политики LSASS – содержит параметры политики, «секреты», список аутентифицирующих доменов, привилегии пользователей, виды выполняемого аудита

Компоненты системы защиты-2

- Диспетчер учетных записей безопасности
- База данных SAM – информация о локальных пользователях и их паролях
- AD – служба каталогов содержащая информацию об объектах в домене
- Пакеты аутентификации – сообщают в ответ на AU-информацию LSASS информацию для генерации маркера доступа
- Winlogon – управление сеансами интерактивного входа в систему
- LogonUI – GUI входа в систему

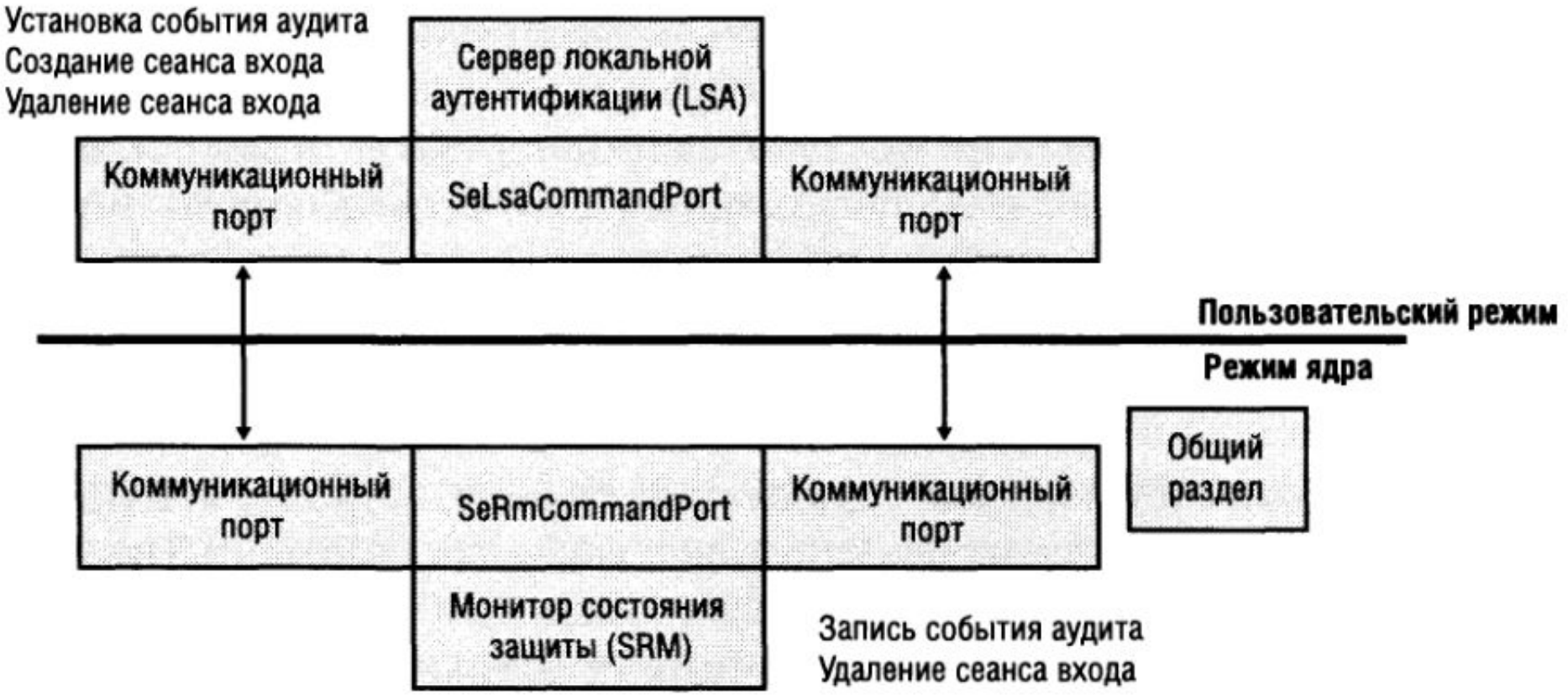
Компоненты системы защиты-3

- Поставщик учетных данных – компонент, определяющий процесс получения AU-информации от пользователя
- NetLogon – компонент, устанавливающий защищенный канал с контроллером домена и отвечающий за обмен AU-информацией
- KSecDD – библиотека функций, реализующая функции безопасности, используемые компонентами ядра
- AppLocker – средство организации ЗПС

Компоненты системы защиты

При инициализации системы устанавливается двусторонняя связь между SRM и LSASS.

В дальнейшем командные порты не используются



Защита объектов

Обращаться к объектам могут только прошедшие AU пользователи (есть маркер)

Отличие маркера защиты от базового – олицетворение

При открытии объекта субъект должен заранее сообщить о своих намерениях

На объект может распространяться нестандартная политика защиты

По результатам проверки может быть выдан описатель объекта

Ключевая функция – BOOL SeAccessCheck

Существуют также косвенные проверки прав

Идентификаторы защиты

Для идентификации субъектов применяется идентификаторы защиты.

S-[версия]-[код агента ID]-[коды субагентов]-[RID]

SID имеется у компьютера, каждого субъекта и группы

Некоторые встроенные участники

Локальные (S-1-2-0) Пользователи, вошедшие через локальный физический терминал

Анонимный вход (S-1-5-7) Пользователь, который подключился к компьютеру, не предъявив имя пользователя и пароль

Прошедшие проверку (S-1-5-11) Все пользователи и компьютеры, прошедшие проверку подлинности. Сюда не включаются пользователи, вошедшие с гостевой учетной записью, даже если они предъявляли пароль

Пакетные файлы (S-1-5-3) Все пользователи, вошедшие в систему с помощью какого-либо средства обработки очередей программ, такого как планировщик заданий.

Создатель-владелец (S-1-3-0) Прототип в наследуемой записи таблицы управления доступом. Когда эта запись наследуется, система заменяет данный прототип идентификатором безопасности текущего владельца объекта

Группа-создатель (S-1-3-1) Прототип в наследуемой записи таблицы управления доступом. Когда эта запись наследуется, система заменяет данный прототип идентификатором безопасности основной группы текущего владельца объекта

Удаленный доступ (S-1-5-1)Все пользователи, вошедшие в систему через подключение удаленного доступа

Все (S-1-1-0) На компьютерах, работающих под управлением Windows XP Professional, группа «Все» включает в себя группы «Прошедшие проверку» и «Гость»

Интерактивные (S-1-5-4) Все пользователи, входящие в систему на локальном компьютере или через подключение к удаленному рабочему столу

Локальная система (S-1-5-18)Учетная запись службы, используемая операционной системой

Сеть (S-1-5-2) Все пользователи, входящие в систему через сетевое подключение. Описатели доступа для интерактивных пользователей не содержат идентификатор безопасности «Сеть»

Self (S-1-5-1-0) Прототип в записи таблицы управления доступом для объекта Active Directory, обозначающего пользователя, группу или компьютер. В ходе проверки доступа операционная система заменяет данный прототип идентификатором участника безопасности, представленного объектом

Служба (S-1-5-6) Группа, в которую включаются все участники безопасности, вошедшие в систему в качестве службы. Членством в этой группе управляет операционная система

Пользователи сервера терминалов (S-1-5-13)Все пользователи, вошедшие на сервер Terminal Services 4.0, работающий в режиме совместимости приложений.

Модель обеспечения целостности

Процессы, запущенные от учетной записи пользователя разбиваются на субъектов по уровню целостности.

Уровни: недоверенный, низкий, средний, высокий и системный.

Определение уровня целостности процесса:

– Меньшее значение из уровня родителя и образа (если у родителя выше низкого)
– Задан родителем ниже
– Наследуется от родителя

Модель обеспечения целостности-2

У объектов имеется метка целостности.

Если у объекта не указан уровень, то считается средним.

При создании объекта уровень целостности средний или равный уровню создателя (для низкого и недоверенного уровня)

Объекты с метками: файлы, ключи, процессы, потоки, маркеры, задания.

Также объект содержит политику целостности: NWU, NRU (процессы), NEU (COM-классы)

Проверка целостности до поверки ACL

Маркер доступа содержит:

- Источник маркера – кто создал
- Тип олицетворения
- Идентификатор маркера, AU, модификации
- Время окончания действия(не используется)
- Основная группа по умолчанию (шаблон)
- DACL по умолчанию (шаблон)
- SID пользователя и SID’ы групп
- Уровень целостности
- Ограниченные SID’ы
- Привилегии

Специфические моменты:

- Олицетворение
- Ограниченные маркеры:
  - Удалить привилегии из основного маркера.
  - Пометить некоторые SID как проверяемые только на запрет.
  - Пометить некоторые SID как ограниченные.
- Фильтрованный административный маркер
  - Для администраторов и опытных пользователей
  - Для обладателей суперпривилегий
- Аудит

Дескриптор защиты

Дескриптор описывает права доступа к объекту.

Содержит:

- Номер версии для SRM
- Флаги (например, регулировка наследования)
- SID владельца
- SID группы
- Метка и политика целостности
- Список управления дискреционным доступом (ACL состоит из ACE)
- Системный список управления доступом

Присвоение ACL

1. Если явно задан дескриптор, то он используются. Если не задан запрет наследования, то копируются ACE контейнера
2. Если дескриптор не указан, то объект наследует от контейнера ACE
3. Если наследовать нечего, но есть DACL по умолчанию, то используется он
4. Иначе дескриптор становится NULL и права доступа не проверяются

Запрос максимальных прав

1. Если дескриптор NULL, то все разрешено
2. Если запрос от владельца, имеющего привилегию присвоения, то разрешается доступ для записи
3. Если запрос от владельца, то право на изменение DACL
4. Из маски доступа удаляются все запреты для запрашивающего
5. В маску доступа добавляются все разрешения для запрашивающего

Запрос желаемых прав доступа

1. Пункты 1-3 те же.
2. Проверка ACE от начала в конец:
   - SID в ACE совпадает с незаблокированным SID из маркера.
   - SID в ACE совпадает с ограниченным SID из маркера при втором проходе.
3. Проверка успешна в случае всех прав.
4. Если по окончанию просмотра какое-либо право не удовлетворено – отказ.
5. Если есть ограниченные SID, то п. 2-4 повторяются

Права

Указывают на возможность выполнения конкретных операций.

Права учетных записей регламентируют вход в систему и не содержатся в маркере. Ими руководствуется LSA при запросах AU.

Регламентируется:

– Интерактивный вход
– Сетевой вход
– Вход через клиент службы терминалов
– Вход как сервис
– Вход как пакетное задание

Привилегии

Определяются и применяются различными компонентами ОС. Проверяющий компонент вызывает стандартную функцию для проверки наличия привилегии.

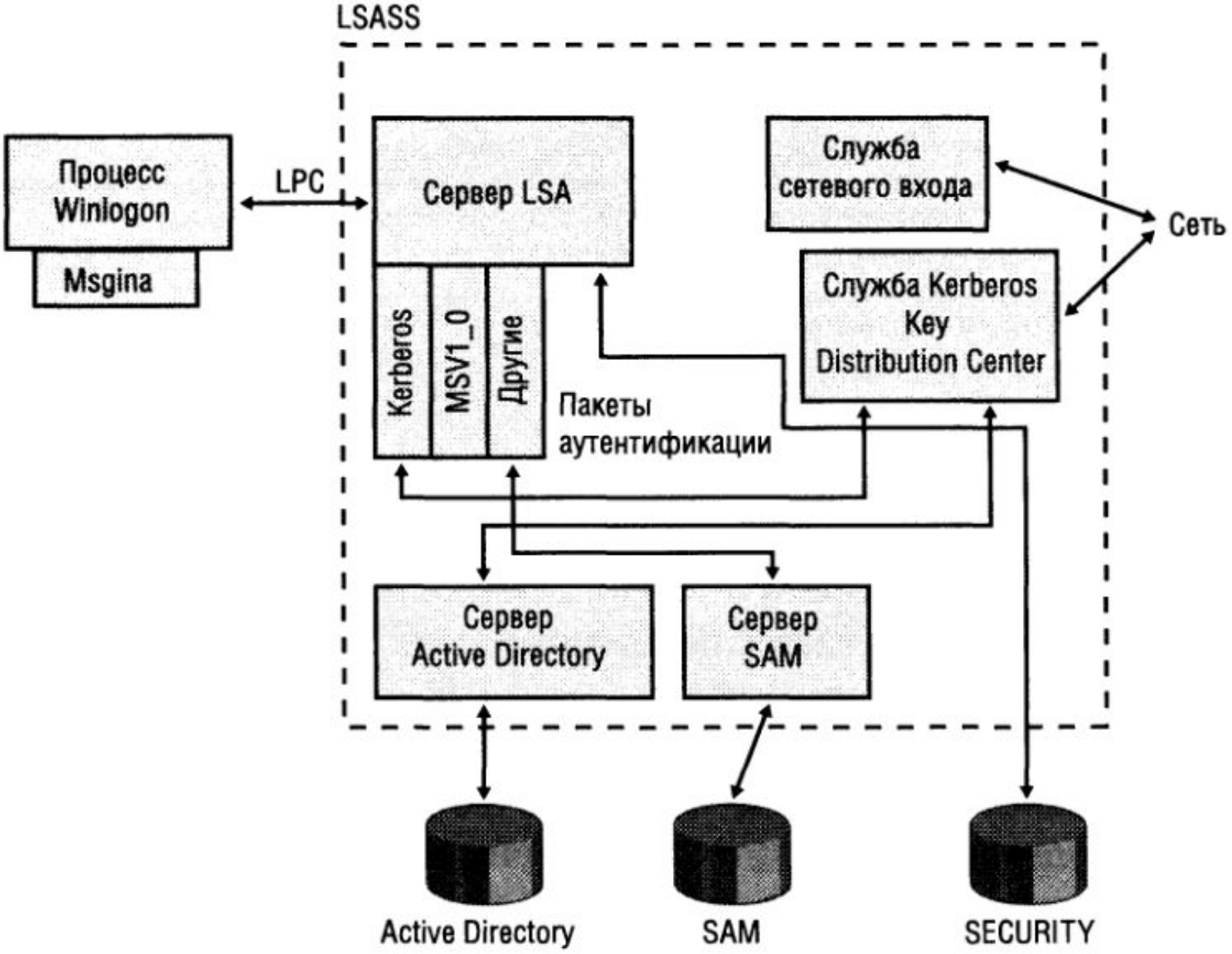
Привилегии могут находиться в неактивном состоянии. Применяется для защиты от случайного использования привилегий.

Суперпривилегии

Данные привилегии позволяют получить неограниченные права в системе:

- Отладка программ
- Смена владельца
- Восстановление файлов и директорий
- Загрузка/выгрузка драйверов
- Создание маркеров безопасности
- Работа в режиме операционной системы

Вход в систему



ОС Linux

Присутствует 4 основных механизма:

– ID/AU пользователей.
– Разграничение прав доступа в VFS.
– Способности процессов.
– Аудит.

ОС Linux

У каждого валидного пользователя имеется:

– ID пользователя – Имя пользователя

– Хеш-свертка в файле паролей

– UID.

При входе в систему на основании ID и AU процессу пользователя присваивается UID

У встроенного пользователя «root» UID = 0.

Проверка прав доступа для процессов с UID=0 не осуществляется.

Разграничение доступа в VFS

У каждого файла или директории присутствует описатель, содержащий:

– uid владельца.
– gid владельца.
– Три категории прав по 3 права в каждой.
– Флаг setuid – «программа с установкой идентификатора пользователя».

Права процесса

В дескрипторе процесса хранится:

– uid, gid – реальные идентификаторы.
– euid, egid – эффективные идентификаторы.
– fsuid, fsgid – идентификаторы для файлов.
– suid, sgid – сохраненные идентификаторы.
– groups – дополнительные идентификаторы групп.

В ходе работы процесса возможно изменение этих полей.

Способности процессов

определяют, разрешено ли процессу выполнение привилегированной операции.

Сведения о способностях **не** хранятся в образах программ.

У пользователя root «взведены» все способности.

LSM

Перед выполнением какой-либо функции, влияющей на безопасность системы вызывается перехватчик. Адреса всех функций-перехватчиков сведены в таблицу

Содержимое таблицы определяет текущую модель безопасности.

Перехватчики в модели безопасности по умолчанию либо проверяют способности, либо разрешают операцию.