Программно-аппаратные средства обеспечения информационной безопасности.

Лекция №1

Методы обеспечения информационной безопасности компьютерных систем

Рахманенко И.А.

ОСНОВНЫЕ ПОНЯТИЯ И ОПРЕДЕЛЕНИЯ

Основные понятия и определения

- ***Политика безопасности (Security Policy).*** Совокупность норм и правил, обеспечивающих эффективную защиту системы обработки информации от заданного множества угроз безопасности.

Основные понятия и определения

- ***Модель безопасности (*Security *Model).*** Формальное представление политики безопасности.

Основные понятия и определения

- ***Дискреционное, или произвольное управление доступом (Discretionery Access Control).*** Управление доступом, осуществляемое на основании заданного администратором множества разрешенных отношений доступа (например в виде "троек" – <объект, субъект, тип доступа>).

Основные понятия и определения

- ***Мандатное, или нормативное, управление доступом (Mandatory Access Control).*** Управление доступом основанное на совокупности правил предоставления доступа, определенных на множестве атрибутов безопасности субъектов и объектов, например, в зависимости от грифа секретности информации и уровня доступа пользователя.

Основные понятия и определения

- ***Ядро безопасности (Trusted Computing Base (TCB)).*** Совокупность аппаратных, программных и специальных компонент ВС, реализующих функции защиты и обеспечения безопасности.

Основные понятия и определения

- ***Идентификация (Identification).*** Процесс распознания сущностей путем присвоения им уникальных меток (идентификаторов).

Основные понятия и определения

- ***Аутентификация (Autentification).*** Проверка подлинности предъявленных идентификаторов сущностей.

Основные понятия и определения

- ***Адекватность (Assurance).*** Показатель реально обеспечиваемого уровня безопасности, отражающий степень эффективности и надежности реализованных средств защиты и их соответствия поставленным задачам (в основном политике безопасности).

Основные понятия и определения

- ***Квалификационный анализ, квалификация уровня безопасности (Evaluation).*** Анализ системы с целью определения уровня ее защищенности и соответствия требованиям безопасности на основе критериев стандарта безопасности.

Основные понятия и определения

- ***Прямое взаимодействие (Trusted Path).*** Принцип организации информационного взаимодействие (как правило, между пользователем и системой), гарантирующий, что передаваемая информация не подвергается перехвату или искажению.

УГРОЗЫ БЕЗОПАСНОСТИ И МЕТОДЫ ВЗЛОМА КОМПЬЮТЕРНЫХ СИСТЕМ

Угрозы безопасности КС

- **Угроза безопасности** вычислительной системе (ВС) - воздействия на систему, которые прямо или косвенно могут нанести ущерб ее безопасности.

Виды угроз

- Конфиденциальности;
- Целостности;
- Доступности.

Угрозы безопасности КС

- Цель защиты АС – противодействие угрозам безопасности

Методы взлома АС

- Атаки на уровне:
  - ОС;
  - Сетевого ПО;
  - СУБД.

Атаки на уровне ОС

- Структура ОС сложна -> защитить сложно.
- Эффективны не только сложные виды атак.
- Успех атаки зависит от архитектуры и конфигурации ОС.

Атаки на уровне ОС

- Кража пароля
  - подглядывание за пользователем;
  - из файла на компьютере ;
  - записан возле рабочего места;
  - кража носителя;
  - атака с перебором.

Атаки на уровне ОС

- Сканирование жесткого диска
- Сборка мусора
- Превышение полномочий
  - Запуск от имени администратора;
  - Подмена системных библиотек;
  - Модификация системы защиты ОС.

Атаки на уровне ОС

- Отказ в обслуживании
  - Захват ресурсов;
  - Бомбардировка запросами;
  - Использование ошибок ПО или администрирования.

Атаки на уровне сетевого ПО

- Прослушивание сегмента локальной сети
- Перехват сообщений на маршрутизаторе
- Создание ложного маршрутизатора
- Навязывание сообщений
- Отказ в обслуживании

Защита на уровне сетевого ПО

- Максимальное ограничение размеров компьютерной сети
- Изоляция сети от внешнего мира
- Шифрование сетевых сообщений
- Электронная цифровая подпись сетевых сообщений
- Использование межсетевых экранов

Атаки на уровне СУБД

- СУБД, содержащая ошибки в программном обеспечении;
- Грубые ошибки при определении политики безопасности.

ЗАЩИТА АВТОМАТИЗИРОВАННЫХ СИСТЕМ ОТ ВЗЛОМА

Защита АС от взлома

- постоянно повышайте квалификацию в области защиты компьютерных систем;
- руководствуйтесь принципом разумной достаточности (чем мощнее защита, тем больше ресурсов компьютерной системы она требует);

Защита АС от взлома

- храните в секрете информацию о принципах действия защитных механизмов АС;
- постарайтесь максимально уменьшить размеры АС и без крайней необходимости не подключайте ее к Internet;

Защита АС от взлома

- перед покупкой нового ПО поищите информацию о нем в сети Internet;
- размещайте серверы в охраняемых помещениях, не подключайте к ним клавиатуру и дисплеи, чтобы доступ к ним осуществлялся только через сеть;

Защита АС от взлома

- Сообщения, нуждающиеся в защите и передаваемые по незащищенным каналам связи, должны шифроваться;
- При стыковке защищенной сети с незащищенной все сообщения должны проходить через межсетевые экраны;

Защита АС от взлома

- не пренебрегайте возможностями аудита (интервал просмотра журнала аудита не должен превышать одних суток);
- если окажется, что число событий в журнале аудита велико, изучите новые записи, так как не исключено, что КС подверглась атаке взломщика;

Защита АС от взлома

- регулярно проводите проверку целостности программного обеспечения АС, проверяйте АС на наличие в ней программных закладок;
- регистрируйте все изменения в политике безопасности в обычном бумажном журнале (регулярная проверка поможет обнаружить присутствие программной закладки);

Защита АС от взлома

- пользуйтесь защищенными ОС;
- создайте несколько ловушек для взломщиков;
- регулярно тестируйте КС с помощью специальных программ оценки степени защищенности КС.

ЗАЩИТА АВТОМАТИЗИРОВАННЫХ СИСТЕМ ОТ ПРОГРАММНЫХ ЗАКЛАДОК

Программные закладки

- Преднамеренно внесенный в ПО функциональный объект, который при определенных условиях инициирует реализацию недекларированных возможностей ПО.

Программные закладки

- Выполняют одно из действий:
  - Искажают коды программ, загруженных в оперативную память;
  - перемещают фрагменты информации из одних областей оперативной или внешней памяти компьютера в другие;
  - искажают выводимую на внешние устройства или в канал связи информацию.

Программные закладки

- По методу внедрения делятся на:
  - программно-аппаратные закладки (BIOS);
  - загрузочные закладки (в загрузочных секторах ЖД);
  - драйверные закладки;
  - прикладные закладки (в прикладном ПО);
  - исполняемые закладки (сами по себе);
  - закладки-имитаторы (копируют элементы интерфейса, например окно ввода пароля);
  - замаскированные закладки.

Программные закладки

- Для выполнения предназначения, процессор должен исполнить код закладки.
- Закладку может запустить пользователь.
- У всех программных закладок имеется одно общее свойство: они обязательно выполняют операцию записи в оперативную или внешнюю память системы.

Программные закладки

- Действия закладок:
  - копирование информации пользователя;
  - изменение алгоритмов работы системных, прикладных и служебных программ;
  - навязывание определенных режимов работы (например, блокирование записи на диск).

Программные закладки

- Разновидностью программных закладок являются программы типа **троянский конь**.

Троянская программа

- Программа, которая является частью другой программы с известными пользователю свойствами, способная втайне от него выполнять некоторые дополнительные функции с целью причинения ущерба;
- Программа с известными пользователю свойствами, в которую были внесены изменения, чтобы помимо известных функций, она могла втайне от него выполнять некоторые разрушительные действия.

Воздействие программных закладок на АС

- Перехват;
- Искажение;
- Сборка мусора;
- Наблюдение и компрометация.

Защита от программных закладок

- Предотвращение внедрения программной закладки;
- Обнаружение внедренной программной закладки;
- Удаление программной закладки.

Предотвращение внедрения закладок

- Изолированная среда:
  - BIOS и операционная система не содержат программных закладок;
  - гарантированно установлена неизменность BIOS и операционной системы в данном сеансе работы компьютера;
  - на компьютере не запускалось и не запускается никаких других программ, не проверенных на закладки;
  - исключен запуск проверенных программ вне изолированного компьютера.

Обнаружение внедренной программной закладки

- Обнаружение признаков присутствия в системе:
  - качественные и визуальные признаки (обнаруживаются пользователем);
  - обнаруживаемые средствами диагностики.

Удаление программной закладки

- Определяется методом внедрения.
- **Программно-аппаратная** закладка – перепрограммировать ПЗУ;
- **Загрузочная, драйверная, прикладная, замаскированная, закладка-имитатор** – произвести замену на соответствующее ПО от доверенных источников.
- **Исполняемая** - убрать код закладки из исходного кода программного модуля и откомпилировать модуль заново.

Рассмотренные вопросы

- Основные понятия.
- Угрозы безопасности и методы взлома компьютерных систем.
- Защита автоматизированных систем от взлома.
- Защита от программных закладок.