Дисциплина: «Основы информационной безопасности»

Раздел 3.

§ 15. Автоматизированная система как объект информационной защиты

План

15.1. Система аутентификации пользователей
15.2. Подсистема контроля целостности
15.3. Подсистема антивирусной защиты
15.4. Криптографические системы

Семинар № 2.

1.История криптологии.
2.Понятие криптографии и ее методы.
3.Симметричные системы шифрования
4.Ассиметричные системы шифрования
5.ХЭШ-функция: понятие, назначение, виды, случаи использования.

15.1. Процессы аутентификации можно разделить на следующие категории

1. На основе знания чего-либо (пароль, PIN..)

2. На основе обладания чем- либо (магнит карты, смарт-карты..)

3. На основе каких- либо неотъемлемых характеристик (биометрическая характеристика)

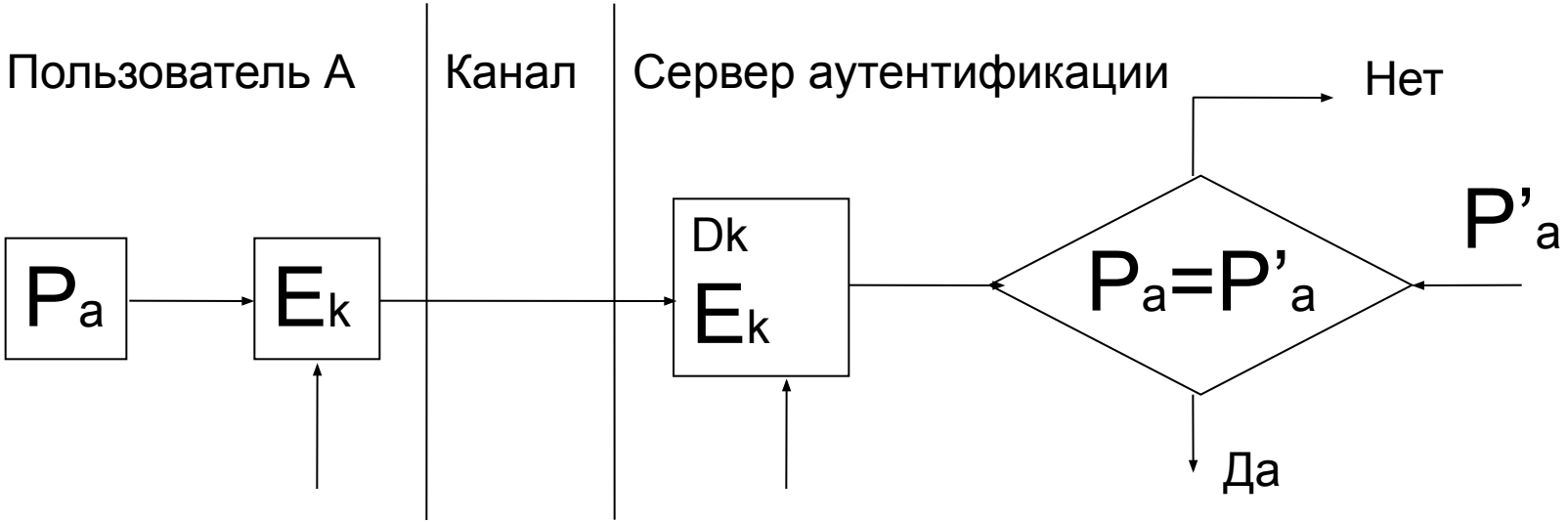
BioAPI, AAMVA, CBEFF, ANSI x9.84-2002
CDSA, CJIS-RS, HA-API, ISO/IEC JTC1/SC37,
XCBF, CDSA/HRS, ANSI/NIST-ITL-1-2000
Fingerprint Standart Revision

Рис. 2.9. Блок-схема общего алгоритма идентификации и установления

15.1. Парольные методы

Методы проверки на основе простого пароля.
Пароль не изменяется от сеанса к сеансу на протяжение установленного администратором временем его существования.

На основе динамически изменяющегося пароля.
Для каждого сеанса или периода работы, пароль изменяется по правилам зависящим от используемого метода.



I. Способы повышения стойкости системы защиты на этапе аутентификации

- Увеличение степени нетривиальности пароля;
- Увеличение длины последовательности символов пароля.
- Увеличение длины времени задержки между разрешёнными попытками повторного ввода неправильного пароля.
- Увеличение ограничений на минимум и максимум t действий пароля.

TP=(AS*tn)/2; где TP- ожидаемое время раскрытия пароля(в днях), A- число символов в алфавите, S- длина пароля в символах, tn- время ввода пароля в секундах с учётом времени задержки между попытками повторного ввода неправильного пароля.

II. Динамически изменяющиеся пароли

1. Метод модификации схемы простых паролей

   А. Случайная выборка символов: длинный пароль – выборка для опознавания при каждом сеансе

   Б. Одноразовое использование пароля: список паролей - № пароля (случайно, по порядку)

2. Метод «запрос-ответ»

   Взаимная проверка подлинности объектов и субъектов: в системе создается защищаемый массив вопросов общего и частного характера.

3. Функциональные методы

3.1. метод функционального преобразования

Функция F: удовлетворяющая условиям:

- для заданного числа (слова) X легко вычислить Y=F(X)
- зная X и Y, сложно или невозможно определить функцию Y=F(X)

Пример: F(x)=(x mod 100)*D+W, где (x mod 100) – остаток целочисленного деления x на 100, D – текущий № дня недели, W - № текущей недели

II. Динамически изменяющиеся пароли

3.2. метод «рукопожатия»

Наличие функции F, известная пользователю и системе

При входе система генерирует случайное число (слово) X

Система вычисляет F(X)

Вывод X пользователю

Пользователь вычисляет F1(X) и вводит в систему

Система сравнивает F(X) и F1(X)

«+» между системой и пользователем не передается никакой конфиденциальной информации

III. Аутентификация на основе сертификатов

Сертификат – электронная форма, содержащая: открытый ключ владельца, сведения о нем, наименование сертифицирующей фирмы, ее ЭЦП (информация о ней зашифрованная закрытым ключом)

Основана на стандарте X.509

15.2. Общие сведения о КИЦ

Основные действия при выполнении контроля информационной целостности:

- Создание эталонной характеристики (по V существенно меньше контролируемой информации)
- Определение текущей характеристики обнаружения модификаций по тому же способу, по которому формировалась эталонная характеристика.
- Сравнение текущей и эталонной характеристик, при совпадении - считают что контролируемая на целостность информация модификации не подвергается.

Примеры

- ФИКС-Unix 1.0, программа фиксации и контроля целостности информации для Unix-подобных ОС
- Программа контроля целостности файлов «ПКЦ» (для Windows Server 2003)

15.2. Способы определения модификаций

Определение случайных модификаций

Определение преднамеренных модификаций

Этапы установки и использования программных средств КИЦ:

- Анализ всех файлов конфигурирования и настройки на отсутствие вызовов несанкционированных программ.
- Анализ вычислительной техники на наличие вирусов и обезвреживание обнаруженных вирусов.
- Установка требуемых режимов и параметров рабочей среды компьютера.
- Формирование эталонных характеристик
- Периодическая проверка соответствия реальных характеристик элементов компьютерной системы их эталонным

Причины возникновения несоответствия реальных и эталонных характеристик

- После обновления не была обновлена эталонная характеристика;
- Произошло повреждение контролируемых элементов данных из-за сбоев или отказов программно-аппаратных средств;
- Произошла несанкционированная модификация файлов;
- Произошло заражение программ компьютерным вирусом.

15.2. Способы функционирования

Транзитный

Режимы работы:
- первый запуск для форматирования эталонных характеристик;
- ежедневный запуск в процессе загрузки операционной системы для проверки всех контролируемых объектов и форматирования эталонных характеристик;
- запуск по мере необходимости для формирования эталонных характеристик программ, поступающих извне.

Резидентный

При регистрации сведений рекомендуется фиксировать:

- Время поступления запроса;
- Идентификатор пользователя – автора запроса;
- Идентификатор компьютера – источника запроса;
- Содержание сообщения в составе запроса;
- Реквизиты защиты(полномочия пользователя, пароли, коды, ключи);
- Время окончания использования ресурса

Задачи, решаемые использованием регистрационных журналов

- Наблюдение за использованием реквизитов защиты;
- Регулирование использования средств защиты в процессе функционирования вычислительной системы;
- Фиксация всех нарушений правил обращения к защищаемым ресурсам;
- Восстановление информации и работоспособности ВС после сбоев и отказов программно-аппаратных средств;
- Анализ процесса поддержания безопасности информации и процесса её обработки с целью совершенствования системы защиты;
- Настройка компонентов системы защиты и других компонентов ВС

Функции системы регистрации

1. Своевременное уведомление о НСД, нарушении работоспособности, возникновении сбоев и отказов в работе программно аппаратных средств;
2. Предупреждение пользователей о необходимости соблюдения предосторожностей при работе с секретными данными

15.3. Методы обнаружения ЗПО

1. Встраивание в BIOS -

2. Метод сравнения с эталоном - просмотр (сканирование) проверяемых объектов (системных областей дисковой и оперативной памяти, а также файлов заданных типов) в поиске **сигнатур** известных вирусов.

Примеры: программы –сканеры (удаление обнаруженных вирусов — полифаги):

«-»:

- необходимость постоянного обновления баз данных сигнатур известных вирусов, которые используются при поиске;

- неспособность обнаружения новых компьютерных вирусов;

- недостаточная способность обнаружения сложных полиморфных вирусов.

Обычно сканеры запускаются при загрузке ОС или после обнаружения признаков вирусного заражения другими средствами.

15.3. Методы обнаружения ЗПО

3. Метод обнаружения изменений - обнаружение изменений в объектах КС путем сравнения их вычисленных при проверке хеш-значений с эталонными (или проверки ЭЦП для этих объектов).

Примеры: программы - ревизорами или инспекторы.

«+»:

+ могут обнаружить новые вирусы.

+ могут обнаружить заражение вирусом новых объектов.

«-»:

- не могут помочь при записи на жесткий диск компьютера пользователя уже зараженного файла

4. Эвристический анализ — проверка системных областей памяти и файлов с целью обнаружения фрагментов исполнимого кода, характерного для ЗПО.

«+»: способны обнаружить любые новые разновидности компьютерных вирусов.

15.3. Методы обнаружения ЗПО

5. Антивирусный мониторинг **-** постоянное присутствие в оперативной памяти компьютера с целью контроля всех подозрительных действий других программ.

Примеры: программы - мониторы.

«+»: автоматически проверяют на наличие известных вирусов все устанавливаемые внешние носители и открываемые файлы и т. п.

«-»:

- назойливость;

- снижение эффективности работы КС (потребляют процессорное время и уменьшают размер свободной ОП).

6. Вакцинирование — присоединение к защищаемому файлу специального модуля контроля, следящего за целостностью данного файла с помощью вычисления его хеш-значения и сравнения с эталоном.

«-»:

- не могут противостоять вирусам-невидимкам;

- не защищают файлы документов

15.3. Классификация АВ ПО

Большинство современных АВ программ являются комплексными т.е. Включают: сканеры - дополнительной функцией избыточного сканирования и эвристического анализа, мониторы, инспекторы.

Виды антивирусных программ:

- программы-фаги (сканеры);
- программы-ревизоры (CRC-сканеры);
- программы-блокировщики;
- программы-иммунизаторы.

15.4. Цели и задачи криптологии

Причины актуальности криптологии

1. Расширение использования КС
2. Увеличение V конфиденциальных данных передаваемых по КС
3. Появление новых устройств, технологий и способов вычислений, способных вскрывать ранее стойкие криптосистемы

Криптология *– наука, занимающаяся проблемой ЗИ путем ее преобразования (kryptos – тайный, logos – наука)*

Криптография (криптографы)
Цель: поиск и исследование математических методов преобразования нформации:
- симметричные криптосистемы
- ассиметричные криптосистемы
- системы электронной цифровой подписи
- управление ключами

Криптоанализ (криптоаналитики)
Цель: исследование возможности расшифровки информации без знания ключа

15.4. Основные понятия

Алфавит - конечное множество символов, используемых для преобразования.

Текст - упорядоченный набор из элементов алфавита;

Текст : открытый, закрытый (шифротекст)

P – открытый текст

C - шифротекст

Шифрование - преобразовательный процесс: исходный(открытый) текст, заменяется шифротекстом, на основе ключа. *E(P)=C*

Дешифрование - обратный шифрованию процесс. На основе ключа шифрованный текст преобразовывается в исходный. *D(C)=P*

ВЕРНО D(E(P))=P

Ключ - Информация, необходимая для беспрепядственного шифрования и дешифрования текстов.

Ek(P)=C, Dk(C)=P верно ***Dk(Ek(P))=P***

Ek1(P)=C, Dk2(C)=P верно ***Dk2(Ek1(P))=P***

Если ключ получен не с помощью криптоанализа (краден, куплен) называется ***скомпрометированным***

15.4. Основные понятия

Криптографическая система - представляет собой семейство преобразований открытого текста.

Криптостойкость - характеристика шифра, определяющая его стойкость к дешифрованию без знания ключа (криптоанализу).

Показтели криптостойкости:

1. Количество всех возможных ключей
2. Среднее время, необходимое для криптоанализа.

Правило А.Керкхоффа: надежность шифра определяется только секретностью ключа

Величины оценки **сложности криптоаналитической атаки:**

- Сложность по данным
- Вычислительная сложность
- Сложность по памяти

Процесс криптографического закрытия информации может осуществляться программно и аппаратно.

15.4. Классификация методов криптографического закрытия

1. Шифрование
   1.1. Замена(подстановка)
      1.1.1. Простая(одноалфавитная)
      1.1.2. Омофонная (одна буква - несколько замен)
      1.1.3. Многоалфавитная одноконтурная обыкновенная, одноконтурная монофоническая, многоконтурная
      1.1.4. Блочная замена
   1.2. Перестановка
      1.2.1. Простая
      1.2.2. Усложнённая по таблице
      1.2.3. Усложнённая по маршрутам
   1.3. Аналитическое преобразование
      1.3.1. С использованием алгебры матриц
      1.3.2. По особым зависимостям
   1.4. Гаммирование
      1.4.1. С конечной короткой гаммой
      1.4.2. С конечной длинной гаммой
      1.4.3. С бесконечной гаммой

- 1.5. Комбинированные методы
  - 1.5.1. Замена и перестановка
  - 1.5.2. Замена и гаммирование
  - 1.5.3. Перестановка и гаммирование
  - 1.5.4. Гаммирование и гаммирование
- 2. Кодирование
  - 2.1. Смысловое
    - 2.1.1. По специальным таблицам (Словарям)
  - 2.2. Символьное
    - 2.2.1. По кодовому алфавиту
- 3. Другие виды
  - 3.1. Рассечение – разнесение
    - 3.1.1. Смысловое
    - 3.1.2. Механическое
  - 3.2. Сжатие - растяжение

Домашнее задание №6: Дать определение/раскрыть суть каждого метода

1. Шифрование
   1.1. Замена(подстановка)
      1.1.1. Простая(одноалфавитная)
      1.1.2. Омофонная (одна буква - несколько замен)
      1.1.3. Многоалфавитная одноконтурная обыкновенная, одноконтурная монофоническая, многоконтурная
         1.1.4. Блочная замена
   1.2. Перестановка
      1.2.1. Простая
      1.2.2. Усложнённая по таблице
      1.2.3. Усложнённая по маршрутам
   1.3. Аналитическое преобразование
      1.3.1. С использованием алгебры матриц
      1.3.2. По особым зависимостям
   1.4. Гаммирование
      1.4.1. С конечной короткой гаммой
      1.4.2. С конечной длинной гаммой
      1.4.3. С бесконечной гаммой
   1.5. Комбинированные методы
      1.5.1. Замена и перестановка
      1.5.2. Замена и гаммирование
      1.5.3. Перестановка и гаммирование
      1.5.4. Гаммирование и гаммирование
2. Кодирование
   2.1. Смысловое
      2.1.1. По специальным таблицам (Словарям)
   2.2. Символьное
      2.2.1. По кодовому алфавиту
3. Другие виды
   3.1. Рассечение – разнесение
      3.1.1. Смысловое
      3.1.2. Механическое
   3.2. Сжатие - растяжение