# Лекция 3. Моделирование угроз и нарушителей

Цель – заставить разработчиков при проектировании систем конструктивно (**на основе формального описания**) мыслить **с точки зрения безопасности**.

## Моделирование угроз (6 этапов)

1. Определение **активов** (что?)

Кто определяет:

* конструктор;
* владелец (руководители бизнеса, использующего систему).

Что определяют:

* ресурсы,
* секретная информация,
* средства контроля безопасности (какие нужны?)

2. Описание **архитектуры** (где?)

Кто описывает:

* конструктор;
* архитектор;
* специалист по безопасности.

Что описывают:

* перечисление границ системы;
* функциональных особенностей;
* возможностей;
* используемых технологий.

3. **Декомпозиция** системы, приложения (как?)

Кто описывает (последние 3 стадии):

* конструктор;
* инфраструктурщик;
* разработчик;
* тестировщик;
* технические писатели (разработчики документации);
* руководитель проекта.

Включает:

1. Выделение **областей для защиты** в информационной сфере
2. Формирование **политик безопасности** приложения (определение правил)
   1. Проверки входных данных (минимизировать, так как это уязвимость)
   2. Проверки подлинности (использовать сертифицированные средства)
   3. Авторизации (разграничение доступа – изоляция защищаемых ресурсов)
   4. Управления конфигурацией (тщательная разработка интерфейсов между компонентами-инфраструктурой и приложениями)
   5. Выделения конфиденциальных данных
   6. Управления сеансом (перехват сеансового обмена между конечными точками сеанса – XSS-атаки (cross-site scripting))
   7. Шифрования (использовать стандартные и сертифицированные протоколы и алгоритмы)
   8. Управления параметрами (при передаче между компонентами)
   9. Управления исключениями (обработка – что сообщать клиенту, что логировать, а что глушить – эта информация содержит много сведений, полезных взломщику)
   10. Аудита и входа в систему (инструкции, подтверждение проведения транзакций, защита этих подтверждений)
3. Важные **события** (что проверять)
   1. Потоки данных (между компонентами) - ресурс
   2. Точки входа (внутренние и внешние интерфейсы, которые разработчики стремятся снабдить максимальным числом функций)
   3. Границы доверия (проверка подлинности данных при обмене между компонентами)
   4. Код (части программы) с высоким приоритетом (минимизация прав: отвечаем на вопрос – очень ли нужен такой код?)

Определение угроз

- подмена идентификатора (незаконное получение учетных данных)

- фальсификация данных (незаконное изменение)

- отказ от авторства действий

- разглашение (явное и неявное – следы редактирования в офисных документах)

- отказ в обслуживании (Deny Of Service)

- расширение прав

- и др.

Источники угроз:

1. Природные (наводнения, пожары, радиоактивное излучение)
2. Техногенные (отключение питания, скачки напряжения, сбои в работке аппаратуры)
3. Антропогенные
   1. Умышленные (целенаправленные)
      1. Проникновение в систему
      2. Маскировка под легального пользователя
      3. Подкуп, шантаж
      4. Искажение программ и данных
   2. Случайные (ошибки сотрудников разного уровня и клиентов)

Документирование угроз

Для каждой определяется

- цель

- категория (в модели STRIDE)

- риск

- метод борьбы

Модель STRIDE

-

<http://msdn.microsoft.com/ru-ru/magazine/cc163519.aspx#S2>

Оценка серьезности угроз

Выяснение

- потенциального ущерба

- воспроизводимости угроз

- доступность начать атаки

- затронутые пользователи и ресурсы (активы)

- легкость обнаружения

*---------------------------------------------------45 минут----------------------------------------------------*

## Проблемы технической защиты информации

- перехват электронных излучений (решается обеспечением защиты информации, передаваемой по радиоканалам связи и обмена данными информационной системы);

- принудительное электромагнитное облучение (подсветка) линий связи с целью получения паразитной модуляции несущей (решается с помощью инженерной защиты информации или физической защиты информации, передаваемой по кабельным линиям передачи данных)

- защита информации в локальных сетях, в интернете и технические средства информационной безопасности;

- применение подслушивающих устройств;

- дистанционное фотографирование;

- перехват акустических излучений;

- восстановление текста принтера;

- копирование носителей информации с преодолением мер защиты;

- маскировка под зарегистрированного пользователя;

- маскировка под запросы системы;

- использование программных ловушек;

- использование недостатков языков программирования и операционных систем;

- незаконное подключение к аппаратуре и линиям связи специально разработанных аппаратных средств, обеспечивающих доступ к информации;

- злоумышленный вывод из строя механизмов защиты;

- расшифровка специальными программами зашифрованной информации;

- информационные инфекции.

## Модель нарушителя

Классификация (по уровню возможностей)

1. Низкий – запуск средств из предопределенного набора, реализующих заранее предусмотренные функции
2. Средний – создание и запуск собственных средств с новыми функциями
3. Высокий – управление функционированием системы (воздействие на базовое ПО, изменение конфигурации ПО и аппаратуры)
4. Абсолютный – проектирование и реализация системы, ее ремонт, обновление, доработка и замена с использованием новых компонентов собственной разработки

## Компьютерное пиратство

Хакеры (Hack – разбивать, разрубать) – компьютерные пираты, злоумышленники.

Классы хакеров:

1. Увлеченные и начинающие

Мотивы:

1. добиться доступа к системе, чтобы выяснить ее строение
2. получить доступ к развлекательному ресурсу
3. показать свою крутизну миру
4. досадить руководству за недооцененность
5. заработать деньги
6. Профессионалы
7. заработать деньги

Профессионалы, преимущественно, используют **некомпьютерные средства**:

- вербовка служащих

- изучение открытой информации о системе

- перехват электронной почты

- анализ распечаток и выписок

- кража документов, носителей и т.п.

Этапы внедрения в систему

|  |  |
| --- | --- |
| Этап | Пример |
|  | для выявления номеров, которые слушают модемы, выполняется автонабор через модем с проверкой тональности ответа |
|  | определение протокола ответа |
| определение процедуры входа в систему | Сведения о процедуре входа в систему могут быть в формате приглашении или доступны по команде help |
| получение (подбор) пароля |  |
| повышение приоритета доступа | * 1. просмотр файлов (системных или просто файлов с реквизитами доступа)   2. создание экранных имитаторов для получения пароля от пользователя   3. анализ содержимого оперативной памяти |
| нарушение штатной работы системы | 1. распространение вирусов 2. лавинообразная рассылка |

## Классификация АС с точки зрения требований безопасности (9 классов)

По руководящему документу Гостехкмиссии России:

- **группа 3**(3А, 3Б)

-- однопользовательские АС

-- пользователь допущен ко всей информации

-- носители одного уровня конфиденциальности

- **группа 2** (2А,2Б)

**--** несколько пользователей

**--** права доступа у всех **одинаковые -** ко всей информации

-- носители различного уровня конфиденциальности

- **группа 1**(1А-1Д; 1А – самые жесткие требования)

-- многопользовательские АС

-- обрабатывается и хранится информация различных уровней конфиденциальности

-- разные пользователи имеют доступ к разной информации

| **Подси-стемы** |  | **3Б** | **3А** | **2Б** | **2А** | **1Д** | **1Г** | **1В** | **1Б** | **1А** |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| Управление (идентификация и контроль) доступом | Субъектов к терминалам, узлам сети, внешним устройствам |  |  |  |  |  |  |  |  |  |
| Субъектов к программам, томам, файлам |  |  |  |  |  |  |  |  |  |
| Потоками информации с помощью меток конфиденциальности |  |  |  |  |  |  |  |  |  |
| Регистрация и учет | Входа/выхода в систему |  |  |  |  |  |  |  |  |  |
| Вывода на печать |  |  |  |  |  |  |  |  |  |
| Запуска программ |  |  |  |  |  |  |  |  |  |
| Доступа к узлам сети (связи), внешним устройствам |  |  |  |  |  |  |  |  |  |
| Изменения полномочий |  |  |  |  |  |  |  |  |  |
| Создания защищенных объектов доступа |  |  |  |  |  |  |  |  |  |
| Криптографическая подсистема | Шифрование конфиденциальных данных |  |  |  |  |  |  |  |  |  |
| Шифрование информации, принадлежащей различным субъектам |  |  |  |  |  |  |  |  |  |
| Использование сертифицированных криптографических средств |  |  |  |  |  |  |  |  |  |
| Обеспечение целостности | Программных средств и данных |  |  |  |  |  |  |  |  |  |
| Физическая охрана |  |  |  |  |  |  |  |  |  |
| Наличие административной защиты |  |  |  |  |  |  |  |  |  |
| Периодическое тестирование СЗИ |  |  |  |  |  |  |  |  |  |
| Наличие средств восстановления |  |  |  |  |  |  |  |  |  |
| Использование сертифицированных средств защиты |  |  |  |  |  |  |  |  |  |

## Подсистемы защиты информации в АС

1. Управление доступом к (системе, терминалам, линиям связи, программам, носителям)
   1. идентификация и проверка подлинности субъектов (
   2. использование матрицы доступа или меток конфиденциальности
2. Регистрация и учет
   1. вход-выход
   2. вывод информации
   3. изменение полномочий
   4. доступа к программам, ресурсам, информации
   5. изменение журналов
3. Криптографическая
   1. шифрование всей конфиденциальной информации, записываемой на разделяемые носители
   2. разные ключи для разных групп доступа
   3. использование сертифицированных средств
4. Обеспечения целостности
   1. физическая охрана помещений, оборудования, носителей (пропуска, режим)
   2. недоступность средств управления доступом, учета и контроля
   3. целостность информации и ПО
   4. периодическое тестирование СЗИ
   5. восстановление средств защиты при отказах и сбоях
   6. наличие администратора ИБ
   7. применение сертифицированных средств защиты

## Типичная процедура установления подлинности в Unix (логин, проль)

Вызов процедуры установления подлинности

Запрос идентификатора

Правильно?

Уведомление о несоответствии

Отключение терминала

Превышено число попыток?

Процедура установления подлинности

Подтвер-ждена?

Уведомление

Работа…

## Модели доступа

Контроль доступа

Установление полномочий (разрешение на доступ):

- дается в зависимости от уровня полномочий

- разделяется по категориям ресурсов.

Матрица доступа

- Объект

- Субъект

- Права

--Вид доступа (R-W-E-D)

-- Время дня

-- Произвольное условие (например, не показывать зарплаты больше млн рублей)

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Субъект\Объект | ФИО сотрудника | Адрес | Наименование товара | Зарплата |
| Директор | R | RW | R | R |
| Кадровик | RWD | RWD | R | RWD |
| Бухгалтер | R | R | RWD | - |

Является сердцем системы обеспечения безопасности и хранится в зашифрованном виде!

Настраивается с помощью специальной (привилегированной) программы. При обращении извлекается по частям и удаляется из памяти после использования.

Модель (классическая) Харрисона-Рузо-Ульмана

Дискретная модель, избирательное управление доступом

Описание системы:

- активные субъекты

- пассивные объекты

- права доступа (R-W-E)

Пользователь 1

Пользователь 2

Объект доступа 2

Объект доступа 3

Объект доступа 1

Модель HRU (Харрисона – Руззо - Ульмана) используется для анализа системы защиты, реализую-щей дискреционную политику безопасности, и ее основного элемента - матрицы доступов. При этом система защиты представляется конечным ав-томатом, функционирующим согласно определенным правилам перехода.

Модель HRU была впервые предложена в 1971 г. В 1976 г. появилось формальное описание модели.

В рамках этой модели система обработки информации представляется в виде совокупности активных сущностей — субъектов (множество S), которые осуществляют доступ к информации, пассивных сущностей - объектов (множество О), содержащих защищаемую информацию, и конечного множества прав доступа R - {г1р ..., г„}, означающих полномочия на выполнение соответствующих действий (например, чтение, запись, выполнение).

Мандатная модель Белла - ЛаПадулы

1. Уровни полномочий устанавливаются пользователям и объектам доступа.

2. Система защиты отвергает запрос, если уровень полномочий пользователя ниже уровня полномочий объекта.

Доступ настраивается индивидуально для каждого пользователя глобально и навсегда.

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| ***Уровень допуска пользователя/ Уровень секретности объекта*** | **Совершенно секретно особой важности** | **СС** | **С** | **ДСП** |
| *ССОВ* |  |  |  |  |
| *СС* |  |  |  |  |
| *С* |  |  |  |  |
| *ДСП* |  |  |  |  |

Мандатная модель регулирует не операции, а потоки информации

Одна из первых моделей безопасности - и впоследствии наиболее часто используемой - была разработана Дэвидом Беллом и Леонардо Ла Падула для моделирования работы компьютера

Мандатная модель управления доступом основана на правилах секретного документооборота, принятых в государственных и правительственных учреждениях многих стран. Основным положением политики Белла-ЛаПадулы, взятым ими из реальной жизни, является назначение всем участникам процесса обработки защищаемой информации, и документам, в которых она содержится, специальной метки, например, секретно, сов. секретно и т. д, получившей название уровня безопасности. Все уровни безопасности упорядочиваются с помощью установленного отношения доминирования, например, уровень сов. секретно считается более высоким чем уровень секретно, или доминирует над ним. Контроль доступа осуществляется в зависимости от уровней безопасности взаимодействующих сторон на основании двух простых правил:

1. Уполномоченное лицо (субъект) имеет право читать только те документы, уровень безопасности которых не превышает его собственный уровень безопасности.

2. Уполномоченное лицо (субъект) имеет право заносить информацию только в те документы, уровень безопасности которых не ниже его собственного уровня безопасности. .

Первое правило обеспечивает защиту информации, обрабатываемой более доверенными (высокоуровневыми) лицами, от доступа со стороны менее доверенных (низкоуровневых).

Второе правило (далее мы увидим, что оно более важное) предотвращает утечку информации (сознательную или несознательную) со стороны высокоуровневых участников процесса обработки информации к низкоуровневым.

Модель совместного доступа

Доступ (модификация прав доступа) разрешается в результате совместных действий нескольких ответственных лиц (два ключа поворачиваются одновременно).

Ролевая модель

Субъект (пользователь) – Роль (минимальный необходимый набор полномочий)

Пользователь может иметь несколько ролей.

Управляется назначением ролей пользователям.

## Регистрация (журналирование)

Должен вестись в любой многопользовательской системе. В ЕС ЭВМ регистрационный журнал выводился на консоль оператора.

Регистрируемые параметры:

- время

- выполняемое задание

- реквизиты пользователя

- используемые ресурсы

Лица, ответственные за безопасность, должны регулярно просматривать журнал.

Система регистрации также позволяет:

- выявить часто используемые ресурсы для доработки системы

- выявить часто ошибающихся пользователей и их обучение (или увольнение)

- восстановить разрушенные ресурсы по последовательности действий

- оказать психологическое воздействие.

*--------------------------------------------------------45 минут------------------------------------------------*