Введение в информационную безопасность

Лекция 2, Введение

Лаборатория вычислительных комплексов ВМК МГУ

2010 г.

План лекции

- Задачи информационной безопасности. Конфиденциальность, целостность, доступность данных и программ. Понятие политики безопасности.
- Методы обеспечения информационной безопасности – криптография, модели безопасности, контроль поведения.
- Программные уязвимости, виды уязвимостей. Эксплуатация уязвимостей.
- Практические аспекты эксплуатации уязвимостей. Взаимодействие аппаратного обеспечения, ядра ОС, загрузчика, прикладных программ и библиотек. Размещение объектов в памяти.
- Инструменты. Статический и динамический анализ программ. Информация о процессах в системе.

Информационная безопасность

- ***Информационная безопасность*** – состояние защищённости информации, обрабатываемой средствами вычислительной техники или автоматизированной системы, от внутренних или внешних угроз: нарушения конфиденциальности, нарушения целостности, нарушение доступности, а так же её незаконного тиражирования, которые приводят к материальному или моральному ущербу владельца или пользователя информации.
- ***Угроза безопасности компьютерной системы*** – это потенциально возможное происшествие, преднамеренное или нет, которое может оказать нежелательное воздействие на саму систему, а также на информацию, хранящуюся в ней.

Проблемы информационной безопасности

- Обеспечение:
  - Конфиденциальности
  - Целостности
  - Доступности

Нарушения информационной безопасности

- ***Уязвимость компьютерной системы*** – некая ее характеристика, которая делает возможным возникновение угрозы.
- ***Атака на компьютерную систему*** – это действие, предпринимаемое злоумышленником, которое заключается в поиске и использовании той или иной уязвимости.
  - Нарушения конфиденциальности информации – ситуация, когда информацией обладает посторонний субъект.
  - Нарушения целостности информации – ситуация, когда произошло умышленное искажение (модификация или удаление) данных, хранящихся в вычислительной системе или передаваемых из одной системы в другую.
  - Отказ от обслуживания.

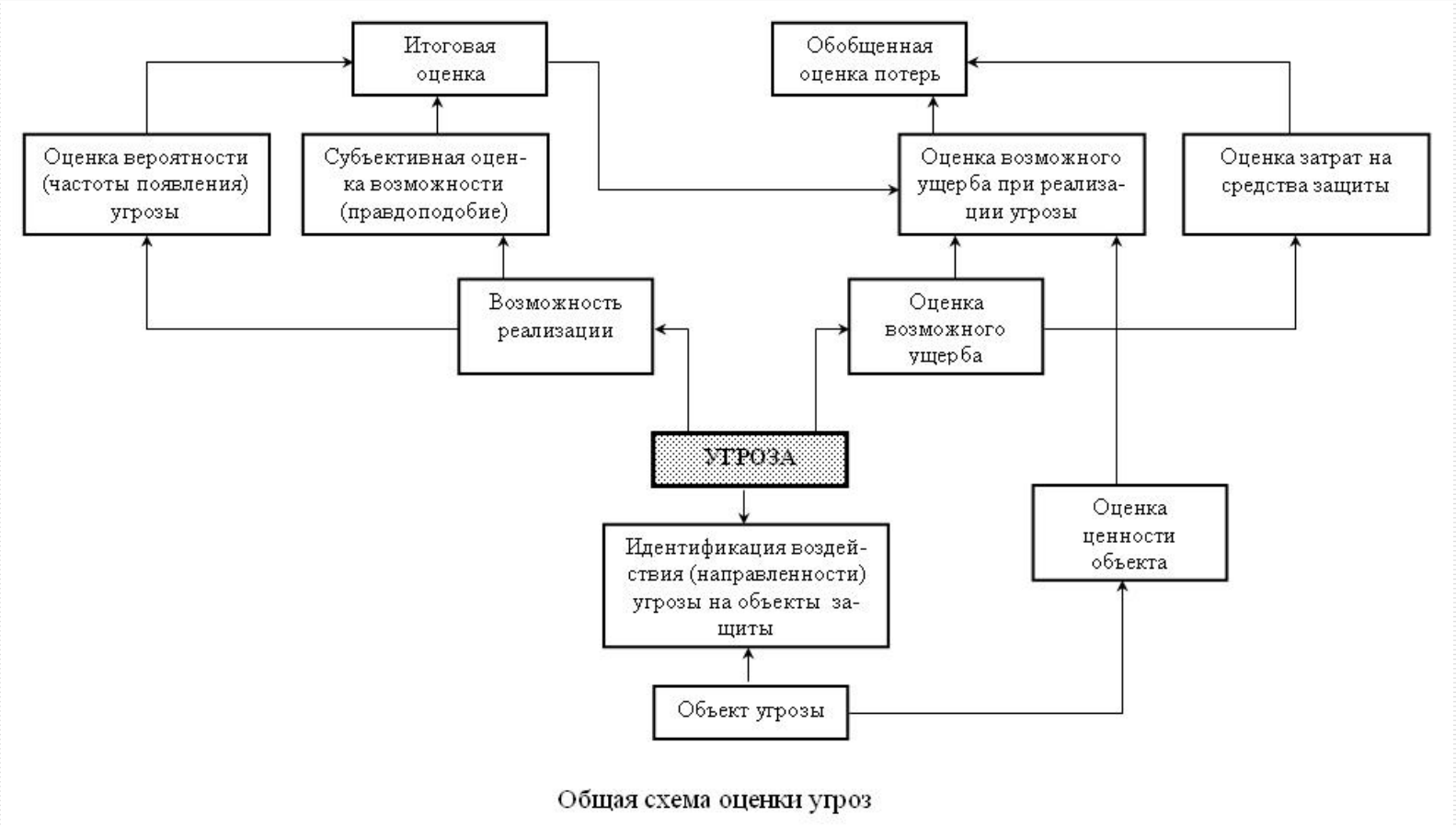
Задачи обеспечения безопасности

- Секретность
  - несанкционированный доступ к информации
  - несанкционированное изменение информации
- Идентификация подлинности пользователей
- Идентификация подлинности документа
- Надежность управления
  - несанкционированное использование ресурсов
  - отказ в обслуживании

Политика безопасности

- **Политика безопасности организации**
  - совокупность руководящих принципов, правил, процедур, практических приемов или руководящих принципов в области безопасности, которыми руководствуется организация в своей деятельности (ГОСТ Р ИСО/МЭК 15408)
- **Политика безопасности компьютерной системы**
  - интегральная (качественная) характеристика, описывающая свойства, принципы и правила защищенности информации в КС в заданном пространстве угроз
- **Модель безопасности**
  - формальное (*математическое*, *алгоритмическое*, *схемотехническое* и т.п.) выражение политики безопасности
- **Модель угроз** – составная часть политики безопасности, описывает возможные угрозы, возможности нарушителя, может содержать оценку угроз

Угрозы безопасности



Общая схема оценки угроз

Различные роли нарушителей

- «Студент» - развлечения ради
- «Хакер» - тестирование защиты, кража данных
- «Коммивояжёр» - выдать себя за более солидную фирму
- «Бизнесмен» - промышленный шпионаж
- «Уволенный работник» - отомстить
- «Кардер» - украсть данные о кредитных картах
- «Шпион» - узнать военные секреты
- «Террорист» - найти уязвимые места для точечного удара

Методы решения задач безопасности

- Организационные
- Технические
  - Криптография
  - Формальные модели безопасности
  - Pentesting/Аудит безопасности
  - Контроль доступа

Криптография

- Шифрование
  - Симметричные алгоритмы, хэширование, алгоритмы с открытыми ключами
  - SSL, VPN, тунеллирование
  - Авторизация и аутентификация
- Электронная подпись
  - Удостоверение подлинности
  - PEM, PGP
  - Проблема PKI (Public key infrastructure)

Формальные модели безопасности

- Модели доступа
  - Дискреционные
  - Мандатные
  - Ролевые
  - Комбинированные

Пример – стандарты на управление безопасностью

- ГОСТ Р ИСО/МЭК 17799-2005: Практические правила управления информационной безопасностью
- ГОСТ Р ИСО/МЭК 15408-2008: Критерии оценки безопасности информационных технологий

ГОСТ Р 17799

- Набор рекомендаций по организации управления безопасностью
- Ключевые меры контроля безопасности:
  - обеспечение конфиденциальности персональных данных
  - защита учетных данных организации и коммерческой тайны
  - защита прав на интеллектуальную собственность

Основные аспекты управления безопасностью

- Организационные
- Управление активами
- Управление персоналом
- Физическая защита
- Управление передачей данных и операциями
- Контроль доступа
- Разработка и обслуживание систем
- Управление непрерывностью бизнеса
- Соответствие требованиям законодательства

Организационный аспект: взаимодействие с другими организациями

- Анализ «внешнего мира» и его влияния на защищенность предприятия
  - Контроль доступа посторонних лиц к ресурсам
  - Включение темы безопасности во все договоры по предоставлению услуг
  - Вопросы аутсорсинга
  - Пример: Redspin

Пример: Redspin

- Независимый аудит защищенности банка
- Аутсорсинг публичных IT-сервисов (web, почта)
- Хостинг ABCHosting оказался уязвимым к атаке directory traversal
- Загрузка файла SYSTEM, с помощью которого зашифрован файл SAM, в котором хранятся все локальные учетные записи и пароли к ним. Получен доступ с правами администратора хостинга.
- Загружена копия реестра Windows Registry Hive, в котором найдена информация об используемом почтовом ПО. Учетные записи и пароли хранятся в Hive, алгоритм шифрования паролей очень прост (Vegerine).
- Получен доступ к почтовым аккаунтам вице-президентов и CFO — в некоторых найдены заявления на получения ссуды и финансовые истории клиентов.
- Среди 15 учетных записей найдены администраторские, пароль от которых также подходит к VPN Банка. Получены права администратора домена VPN Банка.
- Сеть банка взломана.

Управление активами

- Информационные активы должны быть учтены и закреплены за людьми
  - Инвентаризация
  - Классификация
  - Маркировка – в случае информационных активов представляет собой сложную проблему.
    - ЭЦП

Управление персоналом

- Обеспечение безопасности – часть должностных обязанностей
- Схемы доверия, проверка при найме
- NDA (соглашение о конфиденциальности)
- Условия трудового соглашения
- Обучение, информирование
- Ответственность, дисциплинарные меры

Физическая защита

- Охраняемые зоны
- Периметр
- Контроль доступа в зоны
- Безопасность помещений
- Снабжение – электропитание, кабельные сети, водопровод и т.д.
- Политика «чистого стола» и «чистого экрана»

Управление потоками данных и операционной деятельностью

- Документирование основных бизнес-процессов
- Контроль изменений
- Процедуры по инцидентам нарушения безопасности
- Разделение обязанностей – никто не должен обеспечивать технологический процесс в одиночку
- Планирование нагрузки и производительности
- Защита от вредоносного программного обеспечения
- Резервирование
- Управление сетевыми ресурсами
- Безопасность носителей информации
- Безопасность электронной почты и документооборота
- Системы публичного доступа

Контроль доступа

- Регистрация пользователей
- Идентификация и аутентификация
- Управление паролями
- Управление привилегиями
  - Дискреционные политики
  - Мандатный доступ
  - Ролевой доступ

Разработка и обслуживание систем

- Спецификация требований безопасности
- Контроль корректности вводимых данных, целостности обрабатываемых данных
- Контроль изменений
- Регламент использования СКЗИ
  - Взаимодействие с регуляторами
  - Организация и поддержка PKI

Управление непрерывностью бизнеса

- Анализ последствий нарушения непрерывности деятельности
- Планы обеспечения непрерывности бизнеса
- Тестирование, поддержка и пересмотр планов

Соответствие требованиям законодательства

- Авторское право и интеллектуальная собственность
- Критичная для бизнеса информация, учетные данные
- Персональные данные

Программные уязвимости и их эксплуатация

- Уязвимости проектирования
  - «Слабые» протоколы
  - Неправильные значения «по-умолчанию»
- Уязвимости реализации
  - Ошибки переполнения буфера
- Уязвимости конфигурации

Ошибки переполнения

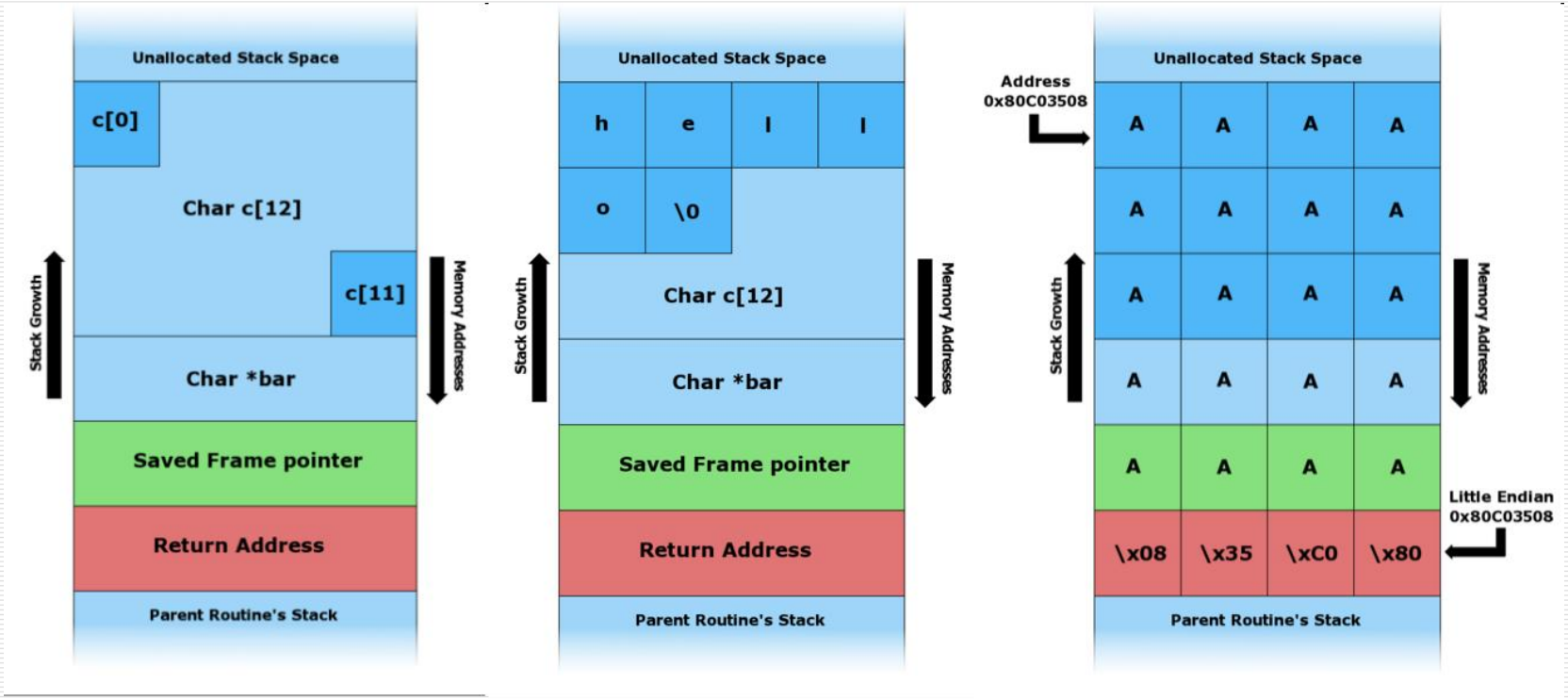
- Stack, Heap, Форматная строка

```
#include <string.h>   *

void foo (char *bar) {
   char c[12];
   strcpy(c, bar); // без проверки границ
}

int main (int argc, char **argv) {
   foo(argv[1]);
}
```

* © wikipedia.org

Ошибки переполнения

- Stack



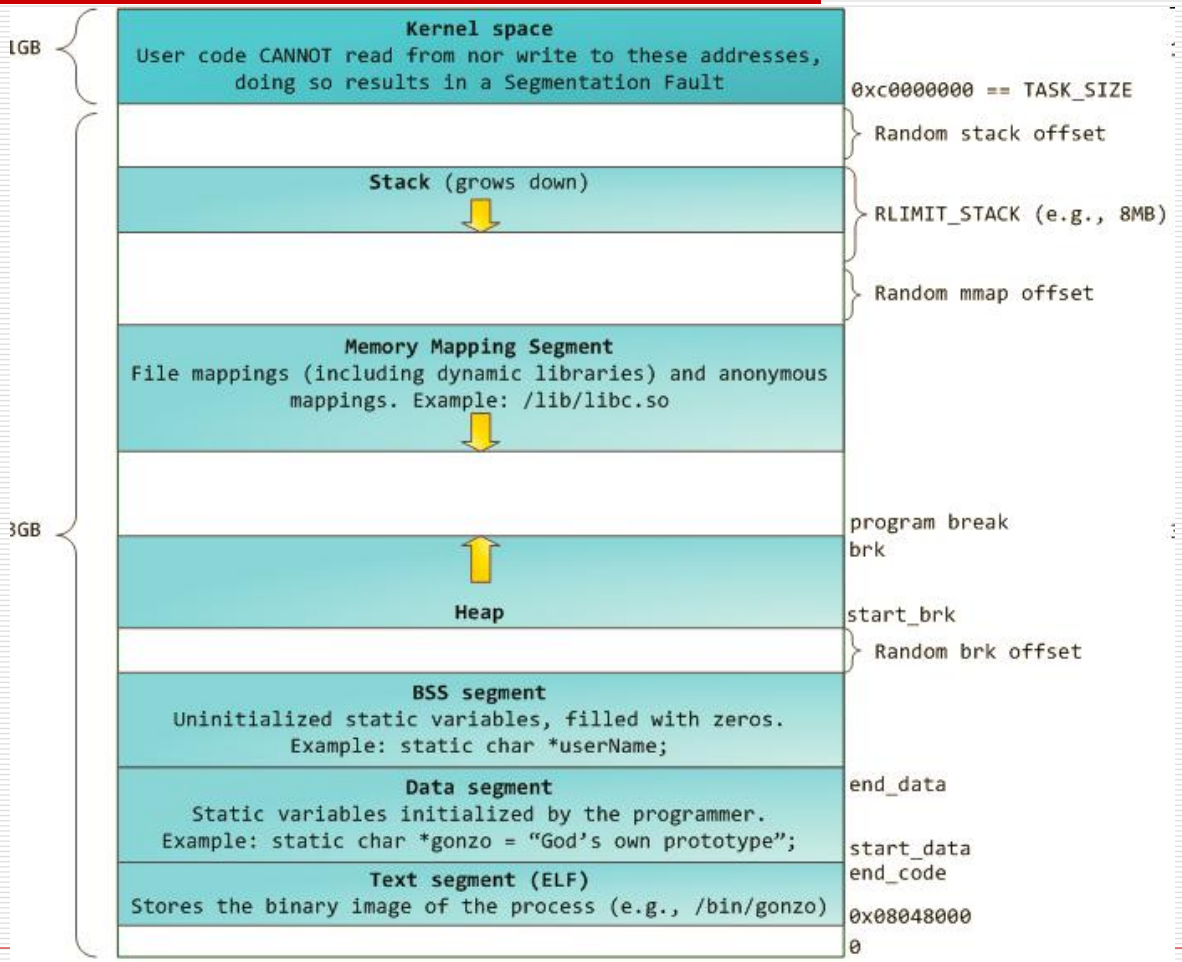
*

аргумент – "hello"

аргумент – "AAAAAAAAAAAAAAAAAAAA\x08\x35\xC0\x80"

* © wikipedia.org

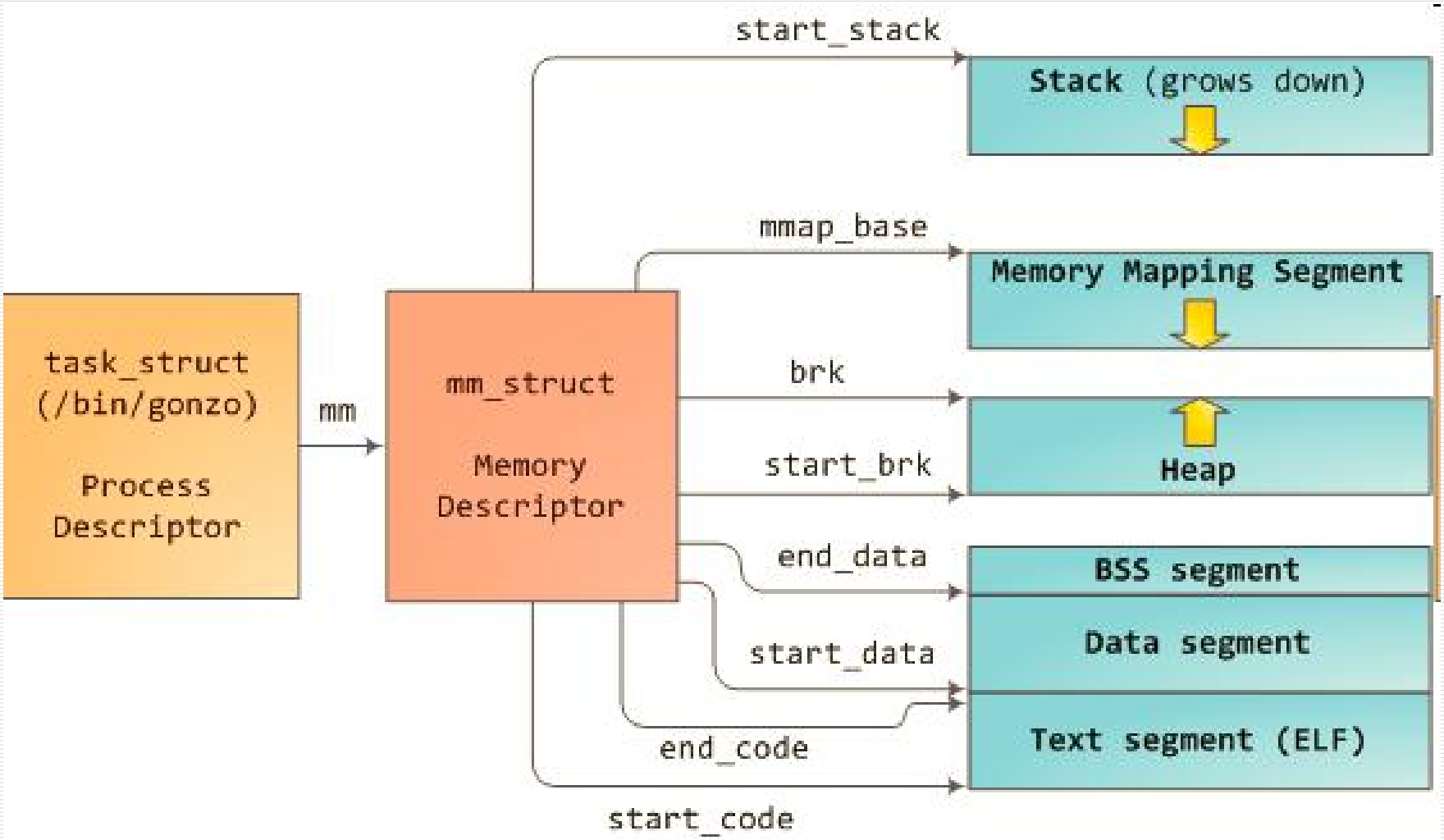
Структура процесса в Linux



*

* © http://duartes.org/gustavo/blog/

Структура процесса в Linux



Инструментарий

- Linux
  - DVL – Damn Vulnerable Linux http://www.damnvulnerablelinux.org/ (ftp://trac.redsecure.ru/)
- Отладчик – gdb
- Работа с исполнимыми файлами – binutils (objdump etc)
- Трассировка - strace

Модель информационной системы

- Основные сущности:
  - ресурсы (объекты)
  - пользователи (субъекты)
  - права доступа
  - операции доступа

Информационные ресурсы

- Под ресурсами понимаются любые информационные объекты, представляющие ценность для их владельца. В ресурсы входят аппаратные ресурсы, программные ресурсы и данные.
  - Аппаратные ресурсы: процессорное время, пропускная способность канала, объёмы оперативной или постоянной памяти.
  - Программные ресурсы: сервис электронной почты, сервис обмена мгновенными сообщениями, трансляция потокового видео, клиент-банк, межбанковские переводы и т.д.
  - Данные: персональные данные физических лиц, банковские реквизиты, личная переписка, оцифрованное видео, текст мгновенных сообщений, конфигурационные файлы сервисов, новости и т.д.

Операции над ресурсами

- Аппаратные ресурсы: «использование объема аппаратных ресурсов».
  - Для каналов связи – часть пропускной способности, для файловой системы – объем дискового пространства, для процесса – объем занимаемой оперативной памяти и процессорного времени и т.д.
- Программные ресурсы: запуск и останов, изменение функциональности (добавление модулей, применение обновлений), непосредственно получение сервиса.

Примеры информационных систем

- Google Documents – сервис хранения и редактирования документов. В случае хранения программный ресурс в соответствии со своей логикой работы предоставляет доступ к использованию аппаратных ресурсов, а именно дискового пространства. В случае редактирования программный ресурс в соответствии со своей логикой работы проводит определенные операции над входными данными, тем самым изменяя их структуру и значение.
- Сеть предприятия. В такую информационную систему входит целый набор программных ресурсов (сетевых сервисов) таких как маршрутизация, управление потоком, удаленное управление устройствоми, фильтрация, трансляция адресов и т.д. Данные, с которыми работают сервисы, следующие: пакеты, конфигурационные файлы, таблицы маршрутизации, базы топологии каждого протокола маршрутизации, таблицы ARP, таблицы DHCP-клиентов, таблицы трансляций NAT и т.д.

Пользователи

- Люди или автономные программы, выполняющие некоторые операции над ресурсами с использованием доступных интерфейсов
- Базисные цели:
  - получение (использование) некоторого объема аппаратных ресурсов;
  - получение некоторого сервиса (в соответствии с требованиями к доступности);
  - изменение функциональности некоторого сервиса;
  - запуск/останов некоторого сервиса;
  - чтение данных;
  - изменение состава (структуры) данных или самих данных.

Злоумышленник

- Лицо или группа лиц, которое:
  - заинтересовано в реализации базисных целей, не имея соответствующих прав (например, кража информации)
  - заинтересовано в нарушении возможностей по достижению базисных целей легитимными пользователями (DoS-атаки)
  - заинтересовано в злоупотреблении ресурсом (спам, сканирование сети)

Вектор атаки

- Конкретная цель злоумышленника может быть достигнута различными способами. Например, злоумышленник имеет цель нарушить доступность сервиса. Этого можно достичь следующими способами:
  - Получить некий объем аппаратных ресурсов, от которых зависит сервис (используя другой сервис на том же узле);
  - Модифицировать или удалить данные, от которых зависит сервис (например, сломать конфигурационный файл);
  - Передать сервису некорректные входные данные, вызвав тем самым ошибку времени исполнения, которая приведет к аварийному останову сервиса;
  - Нагрузить сервис бесполезными запросами, что приведет к исчерпанию пула свободных соединений для обслуживания остальных клиентов.
- **Вектор атаки** = [**конечная цель**] + [**последовательность шагов**]

Пример сценариев атаки

- Пусть имеется ИТС, состоящая из двух серверов, один из которых имеет доступ в Интернет. На сервере работает веб-сервер Apache, в составе которого выполняется веб-приложение. На втором узле работает СУБД, которая используется веб-сервисом для хранения данных. Второй сервер не доступен из сети Интернет. У первого сервера извне доступны только 22 (SSH) и 80 (HTTP) порты. Пусть конечная цель злоумышленника – вывод из строя всей ИТС. Злоумышленник может рассматривать среди прочих следующие сценарии атаки:
  - Захват группы узлов через распространение троянской программы (генератора ключей) со своего хостинга и осуществление DDoS атаки (легитимные запросы главной страницы) с этих узлов;
  - Использование уязвимости веб-сервера Apache, получение терминального доступа на первый сервер, считывание из исходных кодов веб-приложения параметров доступа к СУБД, доступ к СУБД и удаление всей информации;
  - Использование уязвимости SQL injection веб-приложения для внедрения команды «DROP TABLE», которая удалит информацию из СУБД.

Продолжение примера

- **Первый сценарий** = [Захват плацдарма] N раз ***потом*** [реализация конечной цели] (без повышения привилегий в отношении атакуемого сервиса).
- **Второй сценарий** = [Разведка] (открытые порты и версия Apache на первом сервере) ***потом*** [захват плацдарма] (первого сервера) ***потом*** [реализация конечной цели] (с повышением привилегий в отношении атакуемого сервиса).
- **Третий сценарий** = [Реализация конечной цели] (с повышением привилегий в отношении атакуемого сервиса).

Классификация угроз и вредоносной активности

- В общем случае злоумышленник, заинтересованный в проведении атаки на информационные ресурсы, может обладать двумя типами возможностей:
  - Находится на пути взаимодействия пользователя(-ей) с информационными ресурсами;
  - Находится вне пути взаимодействия пользователя(-ей) с информационными ресурсами.

Верхние уровни классификации

- активные «In-Flow» (класс «AIF», Active In-Flow);
- пассивные «In-Flow» (класс «PIF», Passive In-Flow);
- [активные] «Out-of-Flow» (класс «AOF», Active Out-of-Flow).

Соответствие целей классам

Базисная цель злоумышленника	Способы достижения цели
Приведение аппаратных ресурсов к загруженности заданного объема	AOF
Останов заданного сервиса	AOF
Запуск заданного сервиса	AOF
Изменение функциональности заданного сервиса	AIF, AOF
Получение заданного сервиса	AOF
Чтение данных	PIF, AOF
Изменение состава (структуры) данных	AIF, AOF
Изменение данных	AIF, AOF
Снижение качества обслуживания программного ресурса до заданного уровня	AOF, AIF

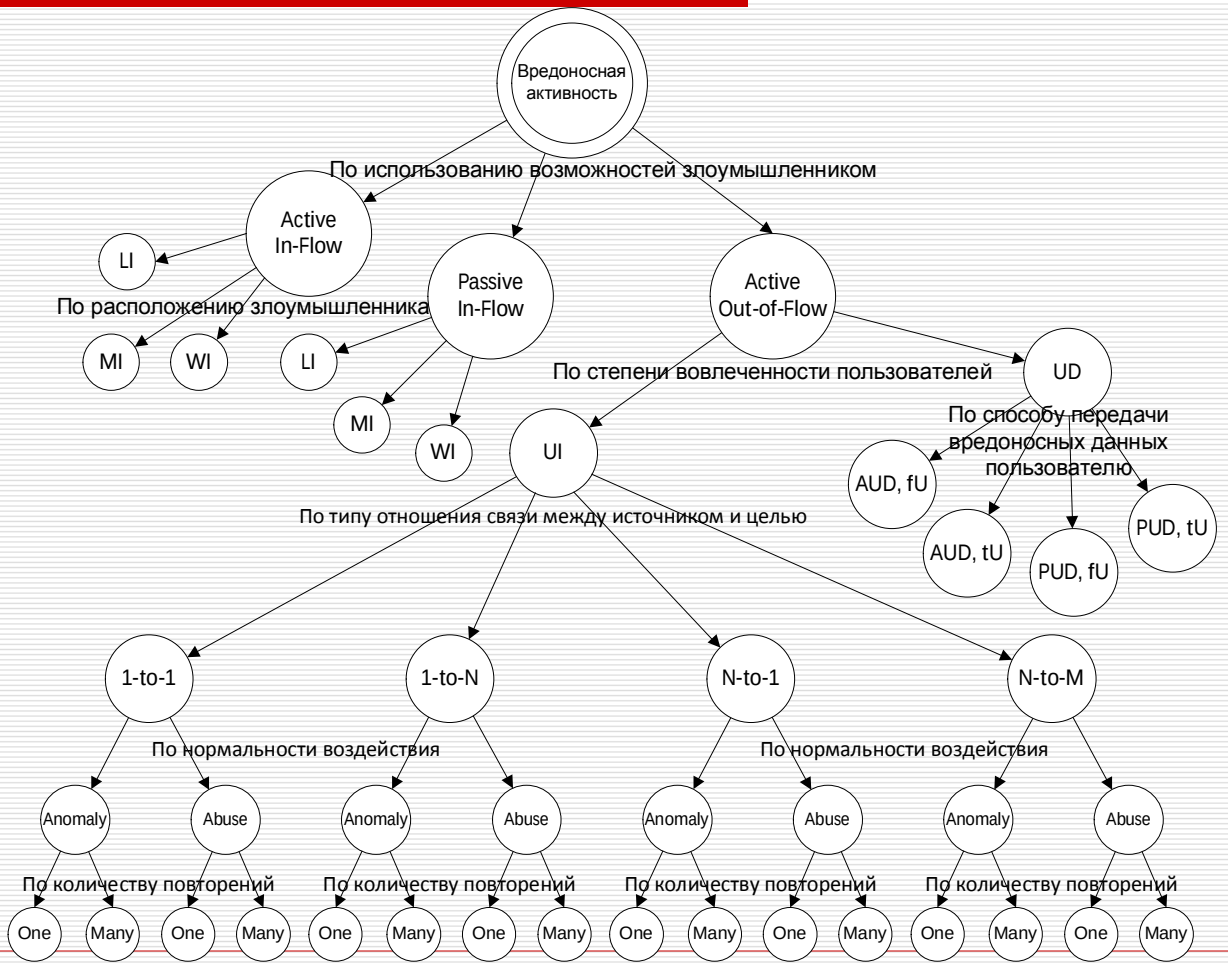
Группа In-Flow

- Локальная сеть пользователя, класс LAN Intruder, или LI.
  - Атаки, связанные с прослушиванием и/или модификацией трафика, проводимые в локальных сетях. Данные атаки возможны либо вследствие физического доступа к каналу (прослушивания эфира, внедрения сетевого оборудования), либо после нарушения целостности служебных сетевых сервисов ARP, STP, DTP и VTP (закрытые протоколы Cisco), DHCP, внутренней маршрутизации (RIP, EIGRP, IS-IS, OSPF и т.д.) или локального DNS.
- Между периметром локальной сети и оборудованием провайдера, класс Last mile Intruder, или MI.
  - Атаки, связанные с прослушиванием и/или модификацией трафика, которые становятся возможными вследствие получения злоумышленником доступа к каналу передачи данных от абонента к провайдеру. Здесь можно выделить две основные подгруппы: прослушивание эфира при наличии беспроводных способов передачи данных и внедрение в канал специализированного оборудования.
- В глобальной сети на пути маршрутизации, класс WAN Intruder, или WI.
  - Атаки, связанные либо с наличием у злоумышленника доступа к магистральным каналам (владеет автономной системой), либо вследствие нарушения целостности глобальных служебных сервисов Интернет: BGP и DNS.

Группа «Active Out-of-Flow»

- «User-Dependent» (UD) – воздействия, успешность которых зависит от решений пользователей ресурсов.
  - Фишинг, установка троянских программ и прочего вредоносного ПО (malware), CSRF (Cross Site Request Forgery), Reflected XSS.
- «User-Independent» (UI) – воздействия, которые не опираются на действия пользователей.
  - Переполнение буфера, сканирование, DDoS, рассылка спама.

Дерево классов



Направленные и ненаправленные атаки

- Направленные – цель выбирается явно, все векторы атаки нацелены на одну цель
  - Классические атаки на сети организаций: компрометация ресурсов, DoS/DDoS-атаки.
- Ненаправленные – цель выбирается неявно, векторы атаки могут иметь сколь угодно много целей
  - Распространение сетевых червей, спам.

Задания

- 1. Посмотреть на память процесса с помощью gdb (надо расписать + взять из howto по gdb простейшие команды для просмотра секций)
- 2. strace ls сравнить с strace ls -l, выделить те системные вызовы, которые работают с файлами, выписать их реальную наблюдаемую последовательность в обоих случая.
- 3. Собрать и сравнить определения конфиденциальности, целостности и доступности в orange book 1980-х, в common criteria, ISO 27001 и стандарте Банка России

Задания

- Программа
  - Собрать с отладочной информацией
- Запустить без параметров
- Запустить под gdb:
  - вывести backtrace после SIGSEGV
  - вывести листинг секции кода в момент SIGSEGV
  - вывести список локальных переменных и их значений
  - вывести аргументы запуска
  - поставить breakpoint на main, выполнить программу пошагово
  - вывести на экран значение переменных bad_message, good_message
- objdump:
  - вывести заголовки всех секций
  - дизассемблировать, найти участок, соответствующий main, сравнить с выводом диассемблирования в gdb, отметить адреса инструкций, сравнить.
- Сохранить листинг от начала до конца и отправить на проверку

```
#include "stdio.h"
void print_scrambled(char *message)
{
int i = 3;
do { printf("%c", (*message)+i); }
while (*++message);
printf("\n");
}

int main() {
char * bad_message = NULL; char *
good_message = "Hello, world.";
print_scrambled(good_message);
print_scrambled(bad_message);
}
```