Взаимодействия прикладной программы и программы с потенциально опасными последствиями

Выполнила: Аюрова Д.Ч.
Проверил: Тенгайкин Е.А.

Взаимодействие прикладных программ

- **Взаимодействие прикладных программ** происходит следующим образом. Обмен информацией во всех сетях осуществляется по логическим каналам (ЛК), следовательно, между взаимодействующими программами должен быть установлен ЛК. Выделяются программа-источник и программа-приемник. После установления ЛК программы становятся равноправными. Между двумя или более взаимодействующими программами может существовать по одному или более логических каналов.

- **Прикладная программа** или **приложение**-программа, предназначенная для выполнения определённых задач и рассчитанная на непосредственное взаимодействие с пользователем. В большинстве операционных систем прикладные программы не могут обращаться к ресурсам компьютера напрямую, а взаимодействуют с оборудованием и другими программами посредством операционной системы. Также на простом языке — вспомогательные программы.
- К **прикладному программному обеспечению** относятся компьютерные программы, написанные для пользователей или самими пользователями для задания компьютеру конкретной работы. Программы обработки заказов или создания списков рассылки-пример прикладного программного обеспечения. Программистов, которые пишут прикладное программное обеспечение, называют ***прикладными программистами***.

Программы с потенциально опасными последствиями

- **Потенциально опасные программы** – это программное обеспечение, которое может нанести косвенный вред компьютеру, на котором установлено или другим компьютерам в сети: легальные программы, содержащие ошибки, программы удаленного администрирования, клавиатурные шпионы, программы вскрытия паролей, программы автоматического дозвона на платные сайты, рекламные движки и т.д.

Программой с потенциально опасными последствиями назовем некоторую самостоятельную программу (набор инструкций), которая способна выполнять любое непустое подмножество перечисленных функций:

- - скрывать признаки своего присутствия в программной среде ПЭВМ;
- - обладать способностью к самодублированию, ассоцииро-ванию себя с другими программами и/или переносу своих фрагментов в иные области оперативной или внешней памяти;
- - разрушать (искажать произвольным образом) код программ в оперативной памяти;
- - сохранять фрагменты информации из оперативной памяти в некоторых областях внешней памяти прямого доступа (локальных или удаленных);
- - искажать произвольным образом, блокировать и/или подменять выводимый во внешнюю память или в канал связи массив информации, образовавшийся в результате работы прикладных программ, или уже находящиеся во внешней памяти массивы данных.

Программы с потенциально опасными последствиями можно условно подразделить на:

- классические программы-"вирусы";
- программы типа "программный червь" или "троянский конь" и фрагменты программ типа "логический люк";
- программы типа "логическая бомба";
- программные закладки - обобщенный класс программ с потенциально опасными последствиями.

- Компьютерным вирусом называется программа, которая может создавать свои копии (не обязательно совпадающие с оригиналом) и внедрять их в файлы, системные области компьютера, сети и так далее. При этом копии сохраняют способность дальнейшего распространения.

- Люком называется не описанная в документации на программный продукт возможность работы с этим программным продуктом. Сущность использования люков состоит в том, что при выполнении пользователем некоторых не описанных в документации действий он получает доступ к возможностям и данным, которые в обычных условиях для него закрыты (в частности - выход в привилегированный режим).

- Существуют программы, реализующие, помимо функций, описанных в документации, и некоторые другие функции, в документации не описанные. Такие программы называются "троянскими конями".

- Логической бомбой обычно называют программу или даже участок кода в программе, реализующий некоторую функцию при выполнении определенного условия.

- Программная закладка — скрытно внедрённая в защищенную систему программа, либо намеренно измененный фрагмент программы, которая позволяет злоумышленнику осуществить несанкционированный доступ к ресурсам системы на основе изменения свойств системы защиты. Закладка может быть внедрена самим разработчиком программного обеспечения.

Кроме того, такие программы можно классифицировать по методу и месту их внедрения и применения (то есть по "способу доставки" в систему):

- закладки, связанные с программно-аппаратной средой (BIOS);
- закладки, связанные с программами первичной загрузки;
- закладки, связанные с драйвером DOS, командным интерпретатором, сетевыми драйверами, то есть с загрузкой и работой операционной среды;
- закладки, связанные с прикладным программным обеспечением общего назначения (встроенные в клавиатурные и экранные драйверы, программы тестирования ПЭВМ, утилиты, файловые оболочки);
- исполняемые модули, содержащие только код закладки (как правило, внедряемые в пакетные файлы типа BAT);
- модули-имитаторы, совпадающие по внешнему виду с легальными программами, требующими ввода конфеденциальной информации;
- закладки, маскируемые под программные средства оптимизационного назначения (архиваторы, ускорители и т.д.);
- закладки, маскируемые под программные средства игрового и развлекательного назначения (как правило, используются для первичного внедрения других закладок; условное название - "исследователь").