Зияутдинов В.С., Корнев П.А., Малыш В.Н. Методы борьбы с атаками на сеть через переполнение буфера. // Проблемы информатики в образовании, управлении, экономике и технике: Сб. статей VIII Всерос. научно-техн. конф. – Пенза: ПДЗ, 2008. – С. 108-110.

МЕТОДЫ БОРЬБЫ С АТАКАМИ НА СЕТЬ ЧЕРЕЗ ПЕРЕПОЛНЕНИЕ БУФЕРА

В.С. Зияутдинов, П.А. Корнев, В.Н. Малыш

Липецкий государственный педагогический университет,
г. Липецк

В современном информационном мире весьма актуальна проблема защиты от атак, которые основываются на переполнении буфера.

Известны следующие виды атак, которые осуществляются посредством переполнения буфера:

- атаки на стек;
- атаки на формат строки;
- атаки на хип.

Рассмотрим данные виды атак более подробно.

Стек представляет собой определенную часть памяти ЭВМ с методом доступа к элементам LIFO («последним пришел – первым вышел»). Очень часто возникает ситуация, когда для корректной работы некоторой программе по замыслу программиста выделяется небольшая область адресного пространства памяти компьютера, которая расположена в стеке. Риск подобной ситуации с точки зрения информационной безопасности заключается в следующем.

Как правило, адресное пространство стека предназначено для хранения некоторых исполняемых инструкций. Однако в памяти ЭВМ выделяется «рабочее пространство» не только для инструкций программы, но и для данных, с которыми эта программа непосредственно работает. Современные злоумышленники (хакеры) придумали использовать некорректную запись данных с тем, чтобы обмануть программу, написанную «незадачливым» программистом. К примеру, пользователю при заполнении некоторой анкеты предлагается ввести свое имя, и ожидается, что оно по количеству вводимых символов не превысит 50. Но совершенно неожиданно для программы в поле для имени вводится 256 букв «D» и некоторый набор команд. В результате происходит переполнение буфера данных, и команды злоумышленника попадут в стек. Так как по существу программа является «бездумным исполнителем», то в случае корректности передаваемых хакером инструкций произойдет их выполнение с фатальным финалом для атакуемого компьютера, информационной системы или некоторого Интернет-сервиса.

При проведении атак на формат строки злоумышленник использует специфические особенности оформления строковых данных, которые позволяют передавать некоторые инструкции в память. Фактически хакер в формате строки указывает исполняемой программе (процессу) на определенную ссылку, по которой расположен вредоносный программный код.

В противоположность стеку хип представляет собой определенную область памяти, которая должна быть готова к использованию в течение всей работы

программы. При атаке на хип происходит запись вредоносных инструкций в страницы хипа, которые затем будет вынужден выполнить компьютер. Технически реализация данного вида атак не отличается от атаки на стек.

Среди наиболее эффективных мер противодействия перечисленным видам атак необходимо выделить следующие:

- своевременная проверка данных;
- внедрение «точек предупреждения»;
- применение современных межсетевых экранов.

Первый способ противодействия атакам переполнения буфера предполагает, что в процессе разработки программного обеспечения будет предусмотрена проверка наличия в стеке и хипе только лишь данных, а не каких-либо посторонних инструкций.

Другой способ защиты рекомендует внедрять в программу так называемых «канареек». Такое красивое название носит определенный участок кода, который имплантируется в критические области памяти. В процессе выполнения программа периодически проверяет целостность «канареек». Если было отмечено нарушение целостности «канарейки», то не происходит перенаправления на очередной блок исполняемых инструкций после завершения текущей функции. Программа просто аварийно завершает работу и выдает соответствующее сообщение об ошибке.

Современные межсетевые экраны обеспечивают довольно качественную проверку чрезвычайно больших входных данных для защищаемых сервисов (E-mail, FTP, HTTP, DNS). Службы прокси межсетевых экранов функционируют следующим образом: они тщательно исследуют протоколы, за которыми призваны наблюдать. Если передаваемые пакеты отличаются от стандартных, то служба прокси разрывает соединение с подозрительным источником. При включении специальной службы обнаружения аномалии протокола служба прокси не только разорвет соединение, но и добавит адрес клиента в список заблокированных источников. После чего любые попытки злоумышленника возобновить свои вредоносные действия будут обречены в течение времени автоматического блокирования.

В завершение рассмотрения основных методов борьбы с атаками переполнения буфера следует отметить, что, безусловно, самым действенным и одновременно самым труднореализуемым способом остается грамотное программирование. Именно качественно составленный код сможет наиболее эффективно противостоять всевозможным попыткам взлома извне.

Библиографический список

1. Касперски, К. Ошибки переполнения буфера извне и изнутри как обобщенный опыт реальных атак [Электронный ресурс]. – http://www.wasm.ru/print.php?article=virii_worm_overbuff_part1.

2. Третьяков, К. Переполнение буфера [Электронный ресурс]. – http://www.codenet.ru/progr/asm/overflow.php.

3. Фэрроу, Р. Атаки на сеть через переполнение буфера: технологии и способы борьбы // Защита информации. INSIDE. – 2006. – № 4.