В результате объединения IDS Snort и МСЭ IPTables получается двухуровневая система защиты: на первом уровне iptables проверяет входящий пакет на соответствие своим правилам фильтрации, если пакет получил разрешение на прохождение через межсетевой экран, его проверяет система обнаружения вторжений на наличие вредоносного кода в теле входящего пакета. Представлен скрипт конфигурирующий Snort_inline и IPTables для совместной работы.

ОБ ОДНОЙ МОДИФИКАЦИИ АЛГОРИТМА XOR

И.В. Молчанов, М.А. Калугина

Обратимость логической операции исключающего ИЛИ позволила успешно использовать ее в синхронном шифровании. Однако основанный на ней классический алгоритм XOR рекомендуется применять лишь однократно из-за его уязвимости к криптоанализу при достаточно большом количестве перехваченных зашифрованных данных.

Реализованный в утилите для Windows алгоритм на основе простого XOR предназначен для приложений, использующих уникальный ключ для шифрования каждого конкретного блока информации. Он состоит из шифрования данных простым алгоритмом XOR и добавления «шума» с использованием специальной рекуррентной последовательности псевдослучайных чисел. Эта последовательность формируется заранее по следующей схеме: $a_0=A$, $a_1=B$, $a_{i+1}=\alpha \bullet a_{i-1}+ \beta \bullet a_i$, − где A, B, α, β – псевдослучайные числа, которые вычисляются до исполнения.

Ключ генерируется как последовательность псевдослучайных байтов или как ключевая фраза, задаваемая пользователем (данная реализация включает псевдослучайный ключ на основе вычисления количества байтов в шифруемом файле). Частью ключа являются значения A, B, α, β.

Шифрование. Пусть M , K , E – массивы символов (байтов) в файле ввода, в ключе и в файле вывода соответственно. Тогда $E_i = M_i$ xor K_i, если i не совпадает с каким-либо элементом последовательности, $E_i = T$ – псевдослучайный символ, если совпадает. Расшифровка. Пусть E, K, M – массивы символов (байтов) в файле ввода (зашифрованная информация), в ключе и в файле вывода соответственно. Тогда $M_i = E_i$ xor K_i, если i не совпадает с каким-либо элементом последовательности, E_i игнорируется, если совпадает.

Таким образом, попытка узнать длину ключа путем циклического сдвига (первый шаг по взлому XOR) не осуществима из-за разных дистанций между a_i и a_{i+1}. Кроме того, при разработке утилиты особое внимание было уделено не только реализации данного алгоритма, но и распространению такого подхода на асинхронный алгоритм шифрования.

ИСПОЛЬЗОВАНИЕ КОДОВ ХЭММИНГА ДЛЯ ОБНАРУЖЕНИЯ И ИСПРАВЛЕНИЯ ОШИБОК В DWDM СЕТЯХ

Б.А. Монич

В системах оптических магистралей, которые работают на терабитных и мультигигабитных скоростях, используется уплотненного волнового мультиплексирования (DWDM). Алгоритм обнаружения и исправления ошибок методом кодов Хэмминга на DWDM транспортной системы Optix OSN 8800 компании Huawei был впервые опробован на одном из 10G каналов. В Республике Беларусь данная транспортная система также является частью сети передачи данных. Функции выявления ошибок реализуются на транспортировке в составе блока избыточной служебной информации, по которой смотрят степень достоверности принятой информации.

Для обнаружения ошибок разработаны и применяются различные алгоритмы. Среди них основными являются следующие.

1. Контроль по паритету. Представляет собой наиболее простой метод контроля данных. Метод заключается в суммировании по модулю 2 всех бит контролируемой информации. Существуют горизонтальный и вертикальный контроль по паритету.

2. Циклический избыточный контроль. Метод основан на рассмотрении исходных данных в виде одного многоразрядного двоичного числа. В качестве контрольной информации рассматривается остаток от деления этого числа на известный делитель R.