РАЗРАБОТКА ИНФОРМАЦИОННОЙ ТЕХНОЛОГИИ ВЫЯВЛЕНИЯ ВНЕШНИХ ВОЗДЕЙСТВИЙ НА ИНФОРМАЦИОННО-ТЕЛЕКОММУНИКАЦИОННЫЕ СЕТИ

И.В. Рубан, д.т.н., проф.; Д.В. Прибыльнов
Харьковский университет Воздушных Сил имени Ивана Кожедуба

В настоящее время одной из угроз государственной безопасности и безопасности вооружѐнных сил являются информационные операции в кибернетическом пространстве. Как показывает анализ событий протекающих в информационном пространстве, связанных с хакерскими и вирусными атаками на информационные ресурсы разных государств (Британия, Сирия, США, Грузия, Россия), существующая система информационного противодействия в кибер-пространстве не является совершенной. Проведенный анализ методов информационного воздействия в кибер-пространстве указывает на то, что наиболее распространѐнными атаками являются атаки типа «Отказ в обслуживании» или DOS-атаки. В настоящий момент, нерешѐнной задачей является противодействие медленным DOS-атакам. Это вызвано тем, что обнаружение данного типа атак затруднено из-за отсутствия явных проявлений изменений интенсивности информационных потоков на начальной стадии выполнения атаки. Механизм действия медленной DOS-атаки основан на особенностях рестарта протокола транспортного уровня TCP, и реализуется за счѐт формирования служебных пакетов с протокольными характеристиками в части выбора временного интервала поступления на вход информационного узла распределѐнной системы. Для решения задачи противодействия медленным DOS-атакам предлагается разработка метода распознавания данного типа атак за счѐт использования механизмов пассивного анализа протокольных характеристик. Части оценки временных и информационных параметров входящего трафика и активных механизмов блокирования информационных направлений инициирующих процедуру отказа в обслуживании протоколом TCP. Данный подход позволяет обнаружить пассивную DOS-атаку, классифицировать еѐ и блокировать вредоносные информационные направления.

ТЕХНОЛОГИЯ УПРАВЛЕНИЯ ДОСТАВКОЙ ПАКЕТОВ В ИНФОРМАЦИОННО-ТЕЛЕКОММУНИКАЦИОННЫХ СЕТЯХ

И.В. Рубан, д.т.н., проф.; М.И. Литвиненко, к.т.н.; А.О. Смирнов
Харьковский университет Воздушных Сил имени Ивана Кожедуба

Современный этап развития общества характеризуется глобальным проникновением информационных технологий в нашу жизнь. Этот процесс сопровождается развитием способов обработки информации, важность и стоимость которой, зачастую, тяжело переоценить, а также ростом угроз информационной безопасности (ИБ). Следовательно, информационная безопасность становится обязательным условием и ставит перед нами новые задачи по еѐ обеспечению.

Одной из угроз информационной безопасности является несанкционированная деятельность нарушителя ИБ. На этапе организации атаки перед ним стоит задача получить максимум информации об атакуемой системе и среде еѐ функционирования. Для этого нарушителю, как правило, необходимо физически внедриться в атакуемую сеть и провести пассивный и активный сбор информации. Получить необходимую информацию возможно посредством проведения атак типа «Man-in-the-Middle», IP-спуфинг, сниффинг пакетов, подбор паролей. В основе данных атак лежат недостатки протоколов маршрутизации. Основными, на наш взгляд, являются необходимость создания виртуального канала связи между абонентами, и трансляция TCP-пакетов в

пределах всего сегмента сети (домена). Предлагается использовать подход, который позволит передавать данные без создания классического виртуального канала связи между абонентами, а именно: за счѐт ветвления трафика по возможным каналам связи между абонентами по заданному закону и распределѐнного подхода к маршрутизации. Это позволит исключить наличие всего сетевого трафика на одном маршруте, что сделает сниффинг пакетов нецелесообразным, выявлять пользование новыми IP-адресами, находящимся в пределах диапазона санкционированных IP-адресов сегмента сети (домена) при IP-спуфинге, снизит эффективность атаки типа DoS.

ПЕРЕДАЧА ДАННЫХ ОБРАТНОЙ СВЯЗИ RTCP ПАКЕТАМИ DNR ПЕРЕМЕННОЙ ДЛИНЫ

А.В. Бабич, к.т.н., доц.; А.Ю. Мова; Р.И. Усиченко
Харьковский национальный университет радиоэлектроники

Для решения задачи сокращения RTCP-трафика предлагается ввод диагностического узла (ДУ) в модель обратной связи RTCP, выступающего, в соответствии со стандартом, в качестве монитора – третьей стороны, не участвующей в мультимедиа сессии, но выполняющей анализ состояния и накапливание статистики для оценки каналов связи по данным отчетов в тренде. Принимая SR- и RR-отчеты от всех узлов-участников RTP-сессии одноадресным образом, ДУ выполняет их обработку и формирует из них пакет DNR (Diagnostic Node Report), который затем рассылается стандартным для RTCP-трафика образом всем участникам RTP-сессии. Анализ эффективности предложенной модели показал тенденцию сокращения объема RTCP-трафика в сравнении со стандартной моделью обратной связи RTCP при росте количества участников сессии видеоконференцсвязи (ВКС) от 5 и выше. Также предлагается формирование пакета DNR варьируемой длины, основанной на результатах статистической обработки диагностическим узлом характеристик качества обслуживания, пересылаемых в отчетах SR и RR. Другими словами, в теле DNR-пакета будет передаваться информация только от тех участников ВКС, анализ состояния которых показал необходимость более тщательного наблюдения для обеспечения должного уровня качества обслуживания в рамках сессии ВКС. Такой подход позволит, с одной стороны, более широко использовать возможности диагностического узла, а с другой – получить большее сокращение объемов RTCP-трафика, сохраняя, при этом, качество обратной связи на уровне стандартной модели RTCP.

РОЗПОДІЛЕНИЙ КОНТРОЛЬ ПОТОКІВ ДАНИХ В ТЕЛЕКОМУНІКАЦІЙНИХ СИСТЕМАХ НА РІВНІ ІНФРАСТРУКТУРИ МЕРЕЖІ

І.В. Кобзев, к.т.н., доц.; Ю.М. Онищенко
Харківській національний університет внутрішніх справ

Ідея реалізації функцій контролю та управління доступом на рівні інфраструктури мережі є аналогією мереж шифрованого зв'язку. Завдання розподіленого контролю потоків даних складається у моніторингу та управлінні передачею інформації між територіально розподіленими вузлами системи, які об'єднані мережею зв'язку. Завдання розподіленого контролю потоків даних може бути вирішено різними методами. Ідентифікація вузлів зв'язку може бути виконана на основі мережевої адреси, або з залученням засобів ідентифікації і аутентифікації користувачів. Віднесення потоків даних до сеансів зв'язку може бути виконане на основі аналізу даних, що пересилаються, маркування даних перед відправленням