Защита от сетевых атак на основе комбинированных механизмов анализа трафика

Чечулин А.А.
ООО “Центр специальной системотехники”, Санкт-Петербург
andreych@bk.ru

Актуальной задачей в области обеспечения безопасности информационных ресурсов является защита от сетевых атак. Существующие средства защиты не всегда справляются с новыми видами (экземплярами) атак, поэтому важным направлением исследований и разработок является создание систем защиты, способных защищать не от конкретных (экземпляров) атак, а от классов атак. Аргументом в пользу разработки подобных систем защиты также является то, что производители программного обеспечения не всегда выпускают обновления для закрытия замеченных уязвимостей. Пример – компания Microsoft [1,2].

Для решения данной проблемы предлагается использовать подход к защите от сетевых атак, основанный на использовании семейства отдельных (атомарных) методов (алгоритмов) анализа трафика и многоуровневого комбинирования алгоритмов в виде системы базовых классификаторов, обрабатывающих данные о трафике, и мета-классификатора, осуществляющего принятие решения о вредоносности трафика по данным от каждого алгоритма, что позволяет объединить достоинства отдельных методов и уменьшить их недостатки.

В работе существующие сетевые атаки (а так же методы сбора информации о жертве, что так же является одним из элементов сетевых атак) предлагается разделить на четыре основных класса: сбор информации, основанный на анализе результата обработки пакетов; атаки, основанные на ошибках в обработке пакетов; сканирование хостов и сетей, основанное на использовании ошибок в обработке сессий; сканирование, базирующееся на корректном установлении соединений.

Методы анализа трафика, применяемые для защиты, сгруппированы в два класса: методы, основанные на анализе отдельных пакетов [3-6], и методы, основанные на анализе последовательности пакетов [7,8].

Класс методов, основанных на анализе отдельных пакетов, состоит из следующих механизмов: механизмы фильтрации некорректных пакетов (обеспечивают защиту от атак, основанных на ошибках в обработке некорректных пакетов) и механизмы нормализации пакетов (обеспечивают защиту от сбора информации и сокрытия атак, основанных на разнице в обработке корректных пакетов).

Общими недостатками всех методов, основанных на анализе отдельных пакетов, являются: отсутствие дефрагментации пакетов и уязвимость к DoS-атакам (при слишком большом трафике пакеты либо задерживаются, либо пропускаются без обработки).

Достоинствами этих методов являются: высокая скорость работы; надежность; возможность работы на сетевом оборудовании; защита не от конкретных атак, а от классов атак.

Класс методов, базирующихся на анализе последовательности пакетов, состоит из следующих механизмов: механизмы фильтрации на основе данных об отдельных сессиях, механизмы, основанные на анализе статистики (например, “Virus Throttling” [7,8] базовый и на основе метода CUSUM) и механизмы Data Mining.

В работе дается характеристика указанных методов анализа трафика.

Фильтрация некорректных пакетов. Данный механизм предназначен для защиты от сбора информации и реализации атак с помощью ошибок в обработке некорректных сетевых пакетов. Для организации защиты используется фильтрация пакетов, имеющих некорректные заголовки.

В заголовках протоколов IP, TCP, UDP и ICMP около 40 различных полей. Практически в каждом из них, согласно спецификации, возможны некорректные значения. Для таких полей можно разработать правила фильтрации. Правила фильтрации можно разделить на две группы:

обязательные (основанные на RFC или блокирующие конкретные атаки) и рекомендуемые (зависящие от параметров защищаемой сети и необходимые для блокирования конкретных атак с учетом конфигурации защищаемой сети).

Примером работы механизма может служить защита от атаки Land – защита осуществляется с помощью фильтрации пакетов, у которых IP-адрес источника совпадает с IP-адресом получателя.

Нормализация трафика. Данный механизм служит для защиты от сбора информации и сокрытия атак с помощью разницы в реализации обработки сетевых пакетов. Для организации защиты используется нормализация пакетов, т.е. приведение полей заголовков пакетов к стандартному виду.

Примером работы механизма может служить защита от сканирования топологии сети с помощью утилиты tracert – защита осуществляется с помощью изменения значения поля TTL протокола IP у всех входящих в сеть пакетов, например, на 128.

Использование нормализации трафика в дополнение к фильтрации позволяет значительно снизить возможности злоумышленника, поскольку блокируются практически все виды сканирований и большинство видов атак, основанных на ошибках и особенностях реализации обработки заголовков пакетов.

Проводимые автором исследования направлены на повышение эффективности механизмов защиты на основе нормализации трафика, увеличение списка поддерживаемых протоколов. Осуществляется разработка методики нормализации протоколов уровня приложений (HTTP, FTP и пр.), позволяющей защититься также от использования некоторых видов скрытых каналов передачи информации.

Фильтрация на основе данных о сессиях. Данный механизм предназначен для защиты от сбора информации и сокрытия атак с помощью TCP-пакетов, относящихся к несуществующим сессиям. Для организации защиты используется фильтрация пакетов, не имеющих отношение к корректно созданным сессиям и не являющихся частью корректного установления соединения.

Примером работы механизма может служить защита от скрытого сканирования Stealth FIN (при сканировании данным методом используется отправка пакетов TCP с установленным флагом FIN для получения списка закрытых портов). Защита осуществляется с помощью фильтрация пакетов, не принадлежащих корректно созданным сессиям.

Недостатками механизма являются: сложность установки механизма на сетевом оборудовании в сетях с высокой сетевой активностью; уязвимость к DoS-атакам (при слишком большом трафике пакеты либо задерживаются, либо пропускаются без обработки); пропуск атак, использующих корректное создание сессий.

Фильтрация на основе сбора статистики. Методика “Virus throttling” (“дросселирование/регулирование вирусов”), предложенная Вильямсоном, основывается на том, что легитимное приложение обычно демонстрирует стабильное число соединений с ограниченным числом внешних узлов.

Достоинствами механизмов основанных на методах “Virus Throttling” являются: простота реализации; эффективное обнаружение быстрого сканирования при условии “медленных” легитимных приложений; адаптивность – в процессе выполнения методики происходит регистрация наиболее часто используемых адресов.

Недостатками механизмов являются: блокировка хостов, на которых установлены приложения, генерирующие много запросов на соединение (web-браузеры, менеджеры закачки, P2P, прокси-сервера); невозможность обнаружения медленного сканирования; невозможность обнаружения сканирования, основанного на протоколе UDP; отсутствие обработки результата установления соединений.

В работе реализуются следующие улучшения механизмов защиты на основе сбора статистики: реализация анализа протокола UDP, представляя отдельный пакет как соединение; обработка ответов на запросы (TCP SYN-ACK), например, для игнорирования успешных соединений; использование для анализа не только IP-адресов, но других полей пакета, например, портов (для обнаружения сканирования портов).

Фильтрация на основе методов Data Mining. Методы Data Mining в настоящее время использовать в полностью автоматизированных системах не представляется возможным, так как процент ошибок слишком высок. Предполагается, что подобные методы могут быть использованы частично для обнаружения неизвестных атак путем поиска аномалий в сетевом трафике.

Объединение механизмов защиты. Общий механизм обнаружения и противодействия сетевым атакам можно представить как совокупность следующих компонентов: сенсор – анализатор сетевого трафика; детектор – механизм обнаружения, принимающий на вход данные от анализаторов сетевого трафика и дающий на выходе правила фильтрации; мета-классификатор – модуль, принимающий на вход правила фильтрации от детекторов и дающий на выходе итоговые правила фильтрации, учитывающие вычисленные на основе данных от анализаторов весовые коэффициенты каждого детектора; фильтр – компонент блокирования, модификации или сдерживания трафика на основе правил, полученных от мета-классификатора.

В работе предлагается комплексный подход к защите от сетевых атак, базирующийся на использовании механизмов нормализации и фильтрации сетевых пакетов. На основе проведения имитационных экспериментов на разработанном программном средстве моделирования проанализированы механизмы защиты от сетевых атак, основанных на протоколах транспортного и сетевого уровней модели OSI, в том числе методики “Virus throttling” (базовый “virus throttling” и “virus throttling” для реализации на свитче на основе метода CUSUM), методики фильтрации трафика на основе данных о сессиях, методики нормализации и фильтрации некорректных пакетов и другие. Выявлены основные достоинства и недостатки предложенных механизмов защиты.

Планируется проведение большой серии исследований на основе моделирования различных сетевых атак и предлагаемых механизмов защиты от них. Также предполагается осуществить следующие улучшения механизмов: оптимизация механизмов для возможности их работы на сетевом оборудовании; создание механизмов фильтрации для работы в сетях с P2P-трафиком; разработка системы фильтрации и нормализации протоколов верхнего уровня стека TCP/IP.

Работа выполнена при финансовой поддержке РФФИ (проект № 10-01-00826-а) и программы фундаментальных исследований ОНИТ РАН (проект № 3.2).

Литература

1. Microsoft Security Bulletin MS09-048 – Critical. http://en.securitylab.ru/notification/384898.php
2. Security lab. http://www.securitylab.ru/news/385475.php.
3. Handley M., Paxson V. Network Intrusion Detection: Evasion, Traffic Normalization, and End-to-End Protocol Semantics // Proceedings of USENIX Security Symposium, 2001.
4. Lemonnier E. Protocol Anomaly Detection in Network-based IDSs // Defcom. 2001.
5. Mahoney M.V. Network Traffic Anomaly Detection Based on Packet Bytes // Proceedings of the 2003 ACM symposium on Applied computing. 2003.
6. Mahoney M. V., Chan P. K. PHAD: Packet Header Anomaly Detection for Identifying Hostile Network Traffic // Department of Computer Sciences Florida Institute of Technology.
7. Williamson M., Twycross J., Griffin J. Virus Throttling // Virus Bulletin, 2003. http://www.hpl.hp.com/techreports/2003/HPL-2003-69.pdf
8. Котенко И.В., Чечулин А.А. Исследование механизмов защиты от сетевых червей на основе методик Virus Throttling // Защита информации. Инсайд, № 3. 2008.