УДК 004.7; 004.492.3

Ограничения современных программных средств глубокого анализа сетевого трафика и способы их преодоления

Ю.В. Маркин, В.А. Падарян, А.Ю. Тихонов
Институт системного программирования РАН, г. Москва

В настоящее время задача анализа сетевого трафика приобретает все большую актуальность: этому способствует как развитие и внедрение новых сетевых технологий, так и появление большого количества новых сетевых протоколов прикладного уровня. В соответствии со спецификой практических задач выделяют два принципиальных подхода:

- анализ трафика, поступающего в режиме реального времени (online)
- анализ предварительно сохраненного трафика (offline)

В online-режиме инструмент должен работать непрерывно с производительностью, достаточной для разбора трафика, поступающего на сетевой интерфейс. При этом должна обеспечиваться возможность обработки потенциально бесконечного входного потока данных. В offline-режиме инструмент получает входные данные (конечного размера) из файла. Поэтому может проводиться более детальный анализ по сравнению с online-анализом на аналогичном трафике.

Большинство существующих сетевых анализаторов реализует оба подхода. При этом offline-режим, как правило, полностью повторяет работу в online-режиме за одним исключением: вместо сетевого интерфейса пакеты считываются из файла. В то же время, отсутствие требований к скорости обработки данных в offline-режиме открывает дополнительные возможности: визуализировать структуру всех разобранных данных, проводить интерактивный разбор, расследовать инциденты нарушения ИБ. Кроме того, существующие opensource-решения [1] не учитывают в полной мере всех особенностей передачи данных по сети. Не проводится анализ восстановленных сессий (Snort [2], The Bro Network Security Monitor [3]): восстановленный поток является окончательным результатом и не подлежит дальнейшему разбору. Затруднена работа с туннельными протоколами.

В работе предлагается подход, состоящий в разработке и реализации двух отдельных инструментов: для проведения online- и offline-анализа соответственно. Инструменты опираются на общую инфраструктуру, построенную на основе

разработанной объектной модели представления данных, учитывающей особенности передачи сетевого трафика. Инфраструктура также включает модули разбора заголовков сетевых протоколов.

Разработанная модель позволяет учитывать семантику сборки данных любых потоковых протоколов: потоковые данные из пакетов записываются в новый единый буфер, к которому в дальнейшем применяются разборщики. Ключевая особенность подсистемы разбора – независимость модулей разбора и распознавания (как следствие, расширяемость без внесения изменений в уже написанный код). Для добавления возможности разбора какого-либо неподдерживаемого протокола необходимо создать дополнительный модуль. Взаимодействие разборщиков осуществляется посредством механизма распознавания данных: реализованы методы автоматического распознавания, что, в частности, позволяет анализировать многоуровневые туннели с различным стеком протоколов без какого-либо дополнительного конфигурирования.

Разработана и реализована инфраструктура анализа сетевого трафика, способная восстанавливать и разбирать сессии, разбирать туннелированный трафик. В настоящий момент поддерживаются только базовые протоколы. Целесообразно расширение функциональных возможностей системы за счет импорта модулей разбора протоколов из анализатора Wireshark [4]. Кроме того, разработан подход к анализу закрытых протоколов. Задача восстановления формата сообщений проприетарных протоколов может быть решена посредством программной среды для динамического анализа бинарного кода [5, 6]. Восстановленный формат (некоторое промежуточное представление) будет использоваться в качестве шаблона модуля поддержки соответствующего протокола.

Работа поддержана грантом РФФИ 15-07-07652 А.

Литература

1. *Ю.В. Маркин, А.С. Санаров*. Обзор современных инструментов анализа сетевого трафика. // Препринты ИСП РАН, №27, 2014.
2. Snort. http://www.snort.org/, дата обращения 07.10.2015
3. The Bro Network Security Monitor. http://www.bro.org/, дата обращения 07.10.2015
4. Wireshark. http://www.wireshark.org/, дата обращения 07.10.2015
5. *В.А. Падарян, А.И. Гетьман, М.А. Соловьёв*. Программная среда для динамического анализа бинарного кода. // Труды Института системного программирования, том 16, 2009, с. 51-72.
6. *А.И. Гетьман, Ю.В. Маркин, В.А. Падарян и др*. Восстановление формата данных. // Труды Института системного программирования, том 19, 2010, с. 195-214.