Котенко И.В.

ПРОАКТИВНЫЕ МЕХАНИЗМЫ ЗАЩИТЫ ОТ БЫСТРО РАСПРОСТРАНЯЮЩИХСЯ СЕТЕВЫХ ЧЕРВЕЙ

Санкт-Петербург, СПИИРАН

В докладе рассматривается проактивный подход к защите от быстро распространяющихся сетевых червей в сети Интернет.

Подход базируется на комбинировании различных механизмов обнаружения и сдерживания сетевых червей и автоматической динамической адаптации механизмов защиты в соответствии с изменением сетевой конфигурации и сетевого трафика.

Предлагаемый подход предназначен для обнаружения сетевых червей (посредством выявления их действий по сканированию уязвимых хостов) и сдерживания их дальнейшего распространения за счет ограничения и блокирования посылаемых инфицированными узлами сетевых пакетов.

В докладе описываются особенности данного подхода и программной реализации разработанной авторами системы моделирования механизмов защиты от сетевых червей.

Предполагается, что проактивное обнаружение и реагирование против сетевых червей основывается на автоматических механизмах, которые используют информацию об “истории” анализируемых сетевых событий и прогнозе будущих событий.

Для разработки проактивного подхода к обнаружению и сдерживанию сетевых червей предлагается использовать комбинацию следующих особенностей [1, 2]:

- “многорезолюционный” способ обнаружения и сдерживания сетевых червей, сочетающий использование нескольких интервалов времени (“окон”) наблюдения сетевого трафика и применение различных порогов для отслеживаемых параметров [3];
- использование различных алгоритмов и математических методов, в том числе учитывающих события, характеризующие как аномальную, так и нормальную сетевую активность хоста;
- многоуровневое комбинирование используемых алгоритмов в виде системы базовых классификаторов, обрабатывающих данные о трафике, и мета-классификатора, осуществляющего выбор решения;
- адаптация механизмов обнаружения и сдерживания сетевых червей, заключающаяся в возможности изменять критерии обнаружения и сдерживания на основе статистических параметров сетевого трафика.

В работе исследуются следующие механизмов обнаружения и сдерживания, а также их модификации:

- различные механизмы Virus throttling (например, для реализации на свитче (VT-S) [4] и на основе метода CUSUM (VT-C) [5];
- механизмы, основанные на анализе неудачных соединений (Failed Connection Basic, FC-B) [6];
- механизмы, базирующиеся на методе “порогового случайного прохождения” (Threshold Random Walk, TRW) [7];

- механизмы, основанные на методе упрощенного “порогового случайного прохождения” (Simplified Threshold Random Walk, TRWS) [8];
- механизмы, применяющие кредиты доверия (Credit Based, CB) [9];
- механизмы, основанные на DNS-статистике (DNS) [10].

Программно реализованная методика исследования механизмов защиты от сетевых червей использует следующие элементы программной среды (рис.1):

- источники трафика, формирующие нормальный трафик и трафик сетевого червя;
- анализатор трафика, предназначенный для синхронизации и стандартизации различных источников;
- контрольные задачи, включающие спецификацию сценариев тестирования, которые определяют способы использования среды моделирования и интерпретации результатов;
- библиотеки предобработки трафика и механизмов защиты от сетевых червей;
- модели средств тестирования, содержащие все элементы, необходимые для исследования реалистичных сценариев в программной среде, с том числе набор метрик (показателей) оценки, описывающих свойства исследуемых механизмов защиты.

Рис.1. Обобщенная архитектура среды исследования механизмов защиты

Пользовательский интерфейс разработанной среды моделирования представлен на рис.2.

В докладе приводятся результаты экспериментов, полученные при исследовании применения предлагаемого подхода для обнаружения и сдерживания как известных, так и потенциально возможных сетевых червей.

Эксперименты позволяют сделать вывод о том, что универсального метода защиты от сетевых червей среди исследованных нет.

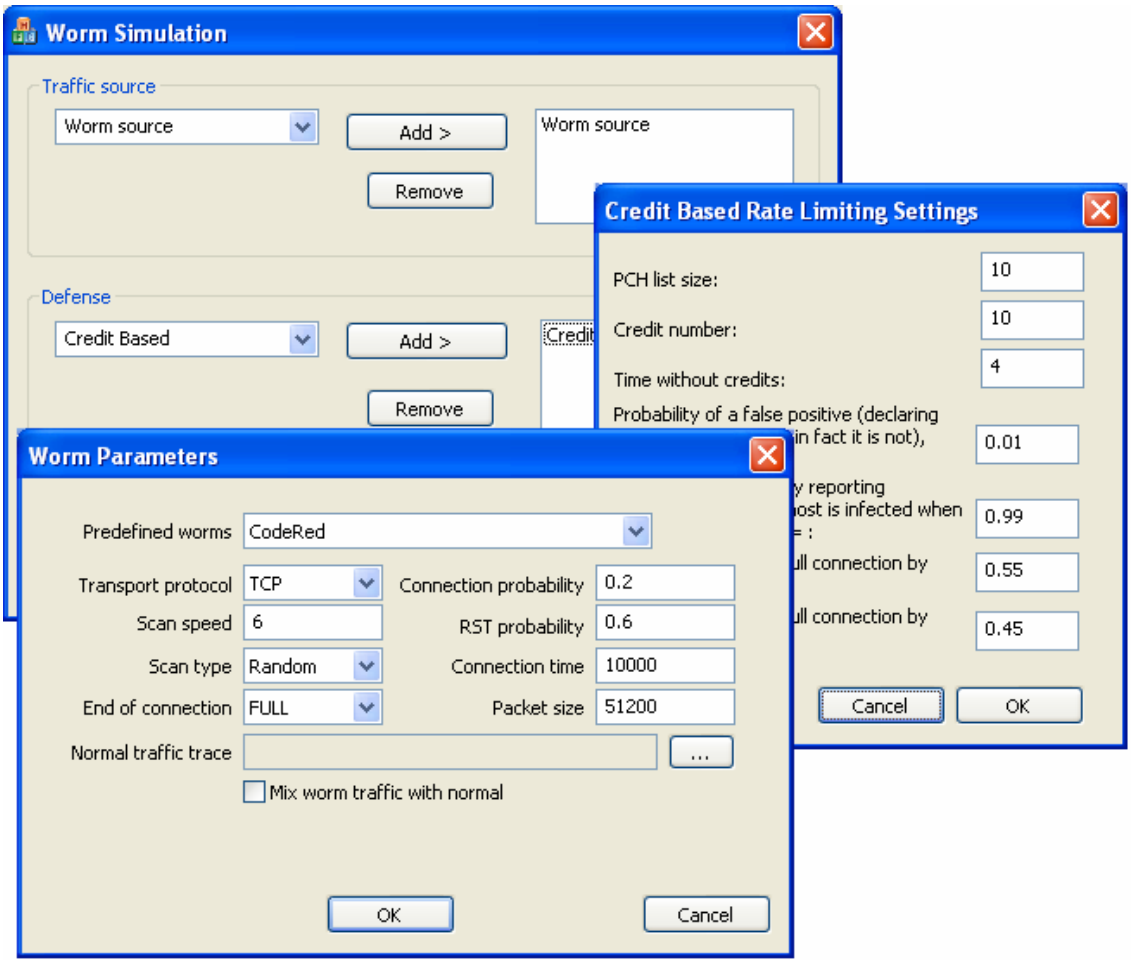

Рис.2. Пользовательский интерфейс разработанной среды моделирования

В этих условиях возможны три направления улучшения защиты:

- выбор наилучшего механизма для данного вида трафика;
- комбинирование механизмов и принятие решения на основе голосования нескольких методов;
- совершенствование существующих механизмов.

Работа выполнена при финансовой поддержке РФФИ (проект №07-01-00547), программы фундаментальных исследований ОИТВС РАН (контракт №3.2/03), Фонда содействия отечественной науке и при частичной финансовой поддержке, осуществляемой в рамках проекта с фирмой Hewlett-Packard и проекта Евросоюза RE-TRUST (контракт № 021186-2).

Литература

1. Котенко И.В., Воронцов В.В. Проактивный подход к обнаружению и сдерживанию сетевых червей // Труды Международных научно-технических конференций “Интеллектуальные системы (AIS'07)” и “Интеллектуальные САПР (CAD-2007)”. М.: Физматлит, 2007.
2. Воронцов В.В., Котенко И.В. Модели обнаружения и сдерживания сетевых червей на основе проактивного подхода // V Санкт-Петербургская межрегиональная конференция

«Информационная безопасность регионов России (ИБРР-2007). Материалы конференции. СПб, 2007. С.47-48.
3. Sekar V., Xie Y., Reiter M.K., Zhang H. A Multi-Resolution Approach for Worm Detection and Containment // IEEE/IFIP DSN'06. 2006. P.189-198.
4. Sanchez M. Virus Throttle as basis for ProActive Defense // Communications in Computer and Information Science (CCIS). Springer. Vol.1, 2007. P.57-74.
5. Peng T., Leckie C., Kotagiri R. Proactively Detecting DDoS Attack Using Source IP Address Monitoring // Networking 2004, Athens, Greece, May, 2004. Lecture Notes in Computer Science. V.3042, 2004, P.771-782.
6. Chen S., Tang Y. Slowing Down Internet Worms // 24th International Conference on Distributed Computing Systems (ICDCS '04), March 2004. IEEE Computer Society. P.312 – 319.
7. Jung J., Paxson V., Berger A.W., Balakrishnan H. Fast portscan detection using sequential hypothesis testing // Proceedings of the 2004 IEEE Symposium on Security and Privacy, Oakland, California, USA, 2004. IEEE Computer Society. P.211-225.
8. Weaver N., Staniford S., Paxson V. Very fast containment of scanning worms, Revisited // Advances in Information Security, V.27. Malware Detection. Springer. 2007, P.113-145.
9. Schechter S., Jung J., Berger A.W. Fast Detection of Scanning Worm Infections // Proceedings of the Seventh International Symposium on Recent Advances in Intrusion Detection, French Riviera, France, September 2004. Lecture Notes in Computer Science, Springer, V.3224, 2004. P.59-81.
10. Wong C., Bielski S., Studer A., Wang C. Empirical Analysis of Rate Limiting Mechanisms // 8th International Symposium on Recent Advances in Intrusion Detection (RAID 2005), Seattle, Washington, September 7-9, 2005. Lecture Notes in Computer Science, Springer, V.3858, 2006. P.22-42.