ИМИТАЦИОННОЕ МОДЕЛИРОВАНИЕ МЕХАНИЗМОВ ОБНАРУЖЕНИЯ И СДЕРЖИВАНИЯ СЕТЕВЫХ ЧЕРВЕЙ В КОМПЬЮТЕРНЫХ СЕТЯХ*

И. В. Котенко, А. В. Уланов, А. В. Тишков, В. С. Богданов, В. В. Воронцов, А. А. Чечулин (Санкт-Петербург)

Характерной чертой сегодняшней ситуации в области сетевой безопасности является не только огромный ущерб, наносимый атаками сетевых червей и вирусов, но и непрекращающийся рост числа самих вредоносных кодов. Существующие средства защиты не всегда оперативно справляются с эпидемиями сетевых червей (вирусов), поэтому становится актуальной проблема создания систем обнаружения и защиты нового поколения, способных предотвратить или сдержать эпидемию на ранних стадиях.

В настоящее время экспертами выделяются *три обобщенных взаимодополняющих класса механизмов защиты от сетевых червей* [1]: *предотвращение*, состоящее в устранении уязвимостей, которые потенциально могут быть использованы сетевыми червями (вирусами), и недопущении самого инцидента заражения; *лечение,* начинаемое уже после того, как заражение произошло; *сдерживание*, направленное на снижение возможностей взаимодействия между инфицированными и потенциально уязвимыми хостами.

Методы сдерживания, в свою очередь, могут быть классифицированы следующим образом: *карантин*, заключающийся в изоляции инфицированного хоста от других хостов в сети; *фильтрация контента*, сводящаяся к отбрасыванию сетевых пакетов на основе сопоставления их содержимого с сигнатурами известных червей; *ограничение интенсивности соединений*, состоящее в ограничении скорости установления хостами соединений.

В статье рассматривается *проактивный подход к защите от сетевых червей, базирующийся на использовании механизмов обнаружения и ограничения интенсивности соединений сетевых червей, и описывается подход и программный прототип для имитационного моделирования механизмов обнаружения и сдерживания сетевых червей*.

Сущность проактивного подхода к защите от сетевых червей

Предлагаемый проактивный подход к защите от сетевых червей базируется на комбинировании различных механизмов обнаружения и сдерживания сетевых червей и автоматической настройке основных параметров механизмов обнаружения и сдерживания в соответствии с текущей сетевой конфигурацией и сетевым трафиком.

Проактивный подход к обнаружению и сдерживанию сетевых червей в проекте предполагает реализацию следующих особенностей:

- во-первых, *применение «многорезолюционного» подхода* – использование нескольких интервалов времени («окон») наблюдения сетевого трафика и применение различных порогов для отслеживаемых параметров;
- во-вторых, *использование различных алгоритмов и математических методов*;
- в-третьих, *многоуровневое комбинирование алгоритмов* в виде системы базовых классификаторов, обрабатывающих данные о трафике, и метаклассификатора, осуществляющего выбор решения;
- В-четвертых, применение *адаптивных механизмов* обнаружения и сдерживания сетевых червей, способных изменять критерии обнаружения на основе статистических параметров сетевого трафика.

* 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 проектов Евросоюза POSITIF (контракт IST-2002-002314) и RE-TRUST (контракт № 021186-2).

Средство для моделирования, рассматриваемое в данной работе, создано с учетом данного подхода и позволяет в дальнейшем его применить путем *интеграции и координации* различных реализованных механизмов (алгоритмов) обнаружения и сдерживания сетевых червей и добавления новых.

Общая архитектура программного комплекса моделирования

При реализации программного средства, предназначенного для моделирования механизмов обнаружения и сдерживания сетевых червей, использовалась архитектура (рисунок), включающая следующие компоненты:

- *Модели источников трафика (Traffic source models)*. Эти модели предназначены для предоставления сетевого трафика для механизмов обнаружения и сдерживания сетевых червей. Они включают как модели трафика атаки, так и модели обычного сетевого трафика. Модели трафика задаются следующим образом. В трафике атаки описывается набор вредоносных пакетов, направленных жертве. Он может влиять на систему защиты (использование памяти, скорость обработки). Сложные атаки могут подражать легитимному трафику и, таким образом, обходить систему защиты. Легитимный трафик задается записями трафика. Трафик атаки также может быть задан записью.
- *Модели предобработки и синхронизации источников трафика (Preprocessing models/Sources synchronization).* Модели предобработки предназначены для приведения трафика из формата источников в формат, удобный для анализа механизмами обнаружения и сдерживания. При одновременном использовании нескольких источников трафика возникает проблема их синхронизации и передачи механизмам обнаружения и сдерживания в упорядоченном во времени виде. Для этого служит модель синхронизации источников.
- *Модели механизмов обнаружения и сдерживания трафика червя (Worm traffic detection and response models).* Модели состоят из алгоритмов методов и используемых протоколов. Вспомогательными элементами являются таблица фильтрации метода и генератор отчетов. Входными параметрами метода являются те поля пакета, полученного от источника трафика, которые им обрабатываются. В качестве управляющих параметров вводятся различные внутренние параметры каждого метода, которые влияют на его эффективность.

Обобщенная архитектура средств моделирования механизмов обнаружения и сдерживания сетевых червей

Особенности моделирования сетевых червей

Для моделирования методов защиты от сетевых червей используются специально разработанные генераторы трафика, которые способны формировать как нормальный трафик (на основе «проигрывания» ранее записанного трафика), в том числе трафик быстрых приложений, так и трафик различных типов сетевых червей, как ранее известных, так и неизвестных, которые могут появиться в будущем.

Деятельность ранее известных червей предлагается моделировать путем задания в генераторе трафика сетевых червей предопределенных параметров их функционирования, соответствующих известным червям.

Действия новых червей предлагается моделировать на основе задания произвольных параметров функционирования. Такими параметрами являются следующие:

- *Тип соединения.* Соединения могут быть двух типов: на основе TCP или на основе UDP.
- *Частота генерации пакетов* (число пакетов (соединений), генерируемых в секунду).
- *Изменение скорости сканирования.* Скорость, с которой червь производит сканирование, может быть постоянной или изменяться (в том числе, случайным образом).
- *Тип сканирования (стратегия сканирования)* (методика выбора адреса узла-получателя и порта):
  - случайное сканирование (random-scanning);
  - последовательное сканирование (sequential-scanning);
  - сканирование на основе перестановок (permutation-scanning);
  - частичное сканирование (partition-scanning);
  - локальное сканирование или сканирование на основе предпочтения локальных адресов (local-preference-scanning);
  - топологическое сканирование (topological-scanning);
  - сканирование по хит-листам, т.е. по заранее составленным спискам уязвимых узлов (hitlist-scanning);
  - комбинация этих методов.
- Вероятность установления успешного TCP-соединения.
- Размер пакета.
- Число используемых адресов (Number of addresses used) и т. д.

Особенности моделирования механизмов защиты

При реализации описываемого программного средства для моделирования в качестве базовых используются следующие методы обнаружения сетевых червей:

- «дросселирования/регулирования вирусов» («virus throttling») и ее модификации [2];
- основанные на ограничении интенсивности соединений на основе DNS-статистики (DNS-based Rate Limiting) [3];
- основанные на анализе неудачных соединений (Failed Connection, FC) [4];
- использующие ограничение интенсивности на базе метода «порогового случайного прохождения» (Threshold Random Walk, TRW) [5], [6];
- базирующиеся на ограничении интенсивности соединений на основе кредитов доверия (Credit Based Rate Limiting) [7].

Все описанные модели объединяются в средстве моделирования.

Для оценки механизмов обнаружения и сдерживания сетевых червей задаются различные сценарии моделирования, включающие набор экземпляров источников трафика и механизмов обнаружения и сдерживания.

В результате моделирования определяются следующие основные параметры работы механизмов защиты: количество ложных срабатываний (False positives), т. е. количество отброшенных пакетов, которые не были сгенерированы червем; количество сгенерированных червем пакетов, которые не были обнаружены защитой (False negatives); время реакции (Reaction time), т. е. время от начала работы метода до первого срабатывания; количество полученных пакетов (Packets processed); минимальное время обработки пакета (Minimal processing time); максимальное время обработки пакета (Maximal processing time); среднее время обработки пакета (Average processing time).

Заключение

Предложен подход к имитационному моделированию проактивной защиты от сетевых червей. Разработано средство для моделирования трафика сетевых червей, как уже известных, так и будущих; это достигается путем возможности генерировать трафик с предопределенными параметрами и характеристиками (определенной частоты генерации пакетов, размера генерируемого пакета и т. д.). Реализованное средство позволяет тестировать методы защиты в различных условиях и при различных предустановленных параметрах.

В работе не предполагается моделировать все взаимодействия, происходящие на пакетном уровне, а также эффекты сетевой перегрузки. При этом предполагаемый генератор трафика сетевых червей «теряет» в степени точности моделирования, так как не учитывает все эффекты, но при акценте проведения экспериментов на начальной стадии сетевой эпидемии (когда заражено небольшое количество узлов) эти потери минимальны.

В дальнейшем планируется проведение большой серии экспериментов по моделированию различных сетевых червей и методов защиты от них.

Литература

1. **Воронцов В. В., Котенко И. В.** Исследование подходов к автоматическому обнаружению и предотвращению вирусных атак на основе комбинированных механизмов ограничения сетевого трафика//Десятая Санкт-Петербургская международная конференция "Региональная информатика-2006" ("РИ-2006"). СПб., 2006.
2. **Twycross J., Williamson M. M.** Implementing and testing a virus throttle//Proceedings 12th USENIX Security Symposium, 2003.
3. **Wong C., Bielski S., Studer A., Wang C.** Empirical Analysis of Rate Limiting Mechanisms//Proceedings of 8th International Symposium on Recent Advances in Intrusion Detection, 2005.
4. **Chen Z., Gao L., Kwiat K.** Modeling the Spread of Active Worms//IEEE INFOCOM’03, 2003.
5. **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. IEEE Computer Society, 2004.
6. **Weaver N., Staniford S., Paxson V.** Very fast containment of scanning worms//Proceedings of the 13th USENIX Security Symposium, 2004.
7. **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, 2004.