Исследование и разработка методов интеллектуального анализа данных для задач компьютерной безопасности

Петровский М. И., Машечкин И. В., Трошин С. В.
Москва, МГУ им. М.В. Ломоносова

Под вторжением в компьютерную систему понимается любая деятельность, нарушающая целостность, конфиденциальность или доступность данных. Для обнаружения вторжений используется специальное программное обеспечение — intrusion detection systems (IDS). В традиционных IDS применяется сигнатурный подход, при котором правила распознавания атаки задаются экспертом «вручную» и хранятся в периодически обновляемой базе знаний. У такого подхода есть ряд серьезных недостатков, в частности, он не устойчив к новым типам атак, поскольку базы знаний еще не содержат соответствующих сигнатур; кроме того, для распределенных и для «замаскированных» атак определение их сценария в виде экспертных правил является нетривиальной задачей. В связи с этим в настоящее время специалистами по компьютерной безопасности большое внимание уделяется применению интеллектуальных методов в IDS. Идея применения этих методов основывается на предположении о том, что активность пользователя или программы может быть отслежена, и на основе прецедентных данных с помощью методов машинного обучения может быть построена либо модель нормального поведения (для подхода «обнаружения аномалий») либо модель распознавания атаки (для подхода «обнаружения нарушений»).

В рамках данного исследования ставились следующие задачи: разработать архитектуру распределенной интеллектуальной IDS; разработать интеллектуальные методы выявления вторжений, в основе которых лежит идея построения моделей поведения пользователей системы с целью обнаружения аномалий, а также распознавания следов вторжений.

В рамках указанных направлений получены следующие результаты. Был разработан экспериментальный прототип для сбора и анализа информации о поведении пользователей защищаемой компьютерной системы [1]. Он представляет собой мульти-агентную систему консолидации информации из системных журналов и лог-файлов защищаемой компьютерной системы и автоматизированное рабочее место аналитика безопасности (АРМ). Задачей системы консолидации является сбор, нормализация, предобработка и сохранение в едином хранилище в унифицированном XML-подобном представлении информации безопасности из различных источников. АРМ аналитика безопасности позволяет проводить анализ собранных данных с помощью статистических и интеллектуальных методов на предмет выявления следов вторжений, а также для построения моделей поведения пользователей. В состав АРМ включены

стандартные методы оперативного статистического анализа данных об активности пользователей с использованием технологии OLAP (online analytical processing), а также реализованы следующие алгоритмы интеллектуального анализа данных.

1. *Алгоритм обнаружения аномалий в разнородных структурированных данных* на основе ассоциативных правил [1]. Идея алгоритма базируется на том, что ассоциативные правила, описывающие корреляции между атрибутами событий, можно использовать для прогнозирования значений одних атрибутов по значениям других. Для этого на основе найденной системы правил строится функция, которая вычисляет распределение условной вероятности значений некоторого атрибута в зависимости от значений остальных атрибутов. В таком случае уровень «ожидаемости» (нормальности) значения этого атрибута события вычисляется как отношение условной вероятности реально наблюдаемого значения к условной вероятности наиболее ожидаемого значения. Аномальность всего события определяется как свертка значений аномальностей всех атрибутов. Такой подход дает возможность не только обнаружить аномальные события, но «интерпретировать» причину их аномальности, т. е. выявлять те атрибуты, которые являются ненормальными с точки зрения предыдущей активности пользователей.

2. *Алгоритм построения вероятностной модели поведения пользователей* позволяет прогнозировать следующее действие пользователя по последовательности предыдущих действий [2]. Он основан на использовании метода потенциальных функций для отображения последовательности событий в конечномерное вещественное пространство признаков, в котором применяется алгоритм построения деревьев решений типа CART для прогнозирования следующего события, при условии, что предыдущая активность описывается заданной последовательностью. В отличие от большинства существующих алгоритмов такой подход учитывает временные интервалы между событиями, а не только порядок событий, и одновременно допускает представление результирующей модели в понятном эксперту виде, в частности, в виде набора правил вида «ЕСЛИ . . . ТО».

3. *Алгоритмы анализа «сырого» сетевого трафика* (TCP/IP), основанные на комбинации методов потенциальных функций и теории нечетких множеств [3]. Алгоритм обнаружения аномалий в сетевом трафике базируется на методе поиска исключений, основанном на использовании потенциальных функций и вычислении нечеткой степени «типичности» объектов в анализируемой выборке. На базе данного метода поиска исключений и нечеткого метода опорных векторов (Fuzzy Support Vector Machines) разработан гибридный метод решения задачи бинарной

классификации для больших объемов данных в условиях наличия шума, который применяется для обнаружения атак по сетевому трафику в режиме обнаружения нарушений. Разработанные алгоритмы проверены на эталонных тестовых наборах данных DARPA Intrusion Detection Evaluation Program и показали высокую точность по сравнению с существующими методами.

В рамках работ по данному направлению также была спроектирована и реализована *мульти-агентная интеллектуальная подсистема обнаружения и защиты от атак, осуществляемых через несанкционированную рассылку электронных сообщений* [4]. Это потребовало разработать специальные алгоритмы моделирования электронной переписки пользователей защищаемой компьютерной системы и фильтрации нежелательных электронных сообщений на уровне почтового сервера. Эти алгоритмы используют методы машинного обучения на основе опорных векторов, а также оригинальные методы сокращения тренировочного набора и уменьшения размерности пространства признаков, что позволяет применять их в режиме реального времени. Данные алгоритмы были успешно верифицированы на эталонных тестовых наборах данных SpamAssasin и LinqSpam.

Работа выполнена при поддержке РФФИ, проекты № 05-01-00744 и № 06-07-08035-офи.

Литература

[1] *Машечкин И. В., Петровский М. И., Трошин С. В.* Система мониторинга и анализа поведения пользователей компьютерной системы // Программные системы и инструменты. — 2006. — № 7. — С. 95–113.

[2] *Petrovskiy M.* A Data Mining Approach to Learning Probabilistic User Behavior Models from Database Access Log // Proc. of ICSOFT, Portugal, 2006. — V. 2. — Pp. 73–79.

[3] *Петровский М. И.* Применение методов интеллектуального анализа данных в задачах выявления компьютерных вторжений // Труды конф. «Методы и средства обработки информации», Москва, 2005. — С. 158–167.

[4] *Mashechkin I., Petrovskiy M., Rozinkin A.* Enterprise Anti-spam Solution Based on Machine Learning Approach // Proc. of 7th Internat. Conf. on Enterprise Information Systems, USA, 2005. — V. 2. — Pp. 188–193.