М. Р. Мухтаров

ИСПОЛЬЗОВАНИЕ ПРОТОКОЛА IPFIX ДЛЯ РЕГИСТРАЦИИ РАСПРЕДЕЛЕННЫХ АТАК «ОТКАЗ В ОБСЛУЖИВАНИИ»

Современные методы обнаружения аномалий основаны на регистрации отклонения профиля сетевого трафика от заданных заранее пороговых значений [1–4]. Пороговые значения обычно получаются в результате обучения алгоритма или же устанавливаются администратором системы вручную на основе объективных показателей [1, 2, 4].

Главным преимуществом подходов на основе регистрации аномалий в профиле сетевого трафика является способность к обнаружению новых типов атак, в том числе атаки «нулевого дня» [1, 2, 5]. Недостаток данного подхода — большое количество ложных срабатываний и неспособность многих методов идентифицировать, какой именно трафик вызывает аномалию, или сопоставить данную аномалию с известной сетевой атакой [5].

Несмотря на указанные недостатки, в последние годы эти методы вновь привлекли внимание исследователей, а также стали активно применяться известными производителями систем сетевой безопасности [6, 7]. Причиной популярности данного типа систем является способность эффективно на ранней стадии оповещать о распределенных атаках «отказ в обслуживании» [1, 2, 7].

В данной работе было проведено сравнение следующих методов: метод авторегрессионной модели, кумулятивной суммы, метод оценки энтропии. Основным недостатком методов обнаружения аномалии, применимых к регистрации распределенных атак «отказ в обслуживании», является невозможность регистрации атак, развивающихся с низкой интенсивностью. Кроме того, реализация указанных методов подразумевает анализ трафика, полученного в результате работы пакетного анализатора трафика, и прямой перехват сетевого трафика. Для обеспечения раннего оповещения распределенных атак «отказ в обслуживании» необходимо использовать распределенный подход и получать информацию о сетевом трафике из всех возможных точек сбора трафика. Прямой перехват трафика потребует размещения большого количества устройств перехвата по всей сети.

В работе в качестве источника информации заголовков сетевого и транспортного уровня IP-пакетов предлагается использовать информацию, предоставляемую протоколом IPFIX [8, 9]. Сетевое оборудование: маршрутизаторы, межсетевые экраны, некоторые коммутаторы — проводят измерения сетевого трафика в определенных точках сети и отправляют полученные данные по протоколу IPFIX в специализированный приемный компонент протокола, который называется «коллектор». Из коллектора информация поступает для последующей обработки, анализа и хранения [9].

При использовании данного протокола существует возможность построить эталонный профиль сетевого трафика; для регистрации отклонений сетевого трафика от эталонного профиля предлагается применять метод оценки максимальной энтропии [1].

В докладе предложен способ анализа результатов работы протокола IPFIX, сведений о потоках трафика с помощью предварительного разбиения трафика по классам и подсчета вхождения каждого из пакетов в выбранный класс. На основе проведенной классификации было получено распределение трафика по классам.

Для предварительного обучения нормального профиля сетевого трафика используется метод оценки максимальной энтропии. Для сравнения нормального профиля сетевого трафика с текущим значением используется оценка расстояния Кульбака–Лейблера.

СПИСОК ЛИТЕРАТУРЫ:

1. *Gu Y., McCallum A., Towsley D.* Detecting anomalies in network traffic using maximum entropy // Tech. rep. Department of Computer Science. UMASS. Amherst, 2005.
2. *Lee W., Xiang D.* Information-theoretic measures for anomaly detection // Proceedings of the IEEE Symposium on Security and Privacy. IEEE Computer Society. 2001.
3. *Zhang H.* Study on the TOPN Abnormal Detection Based on the NetFlow Data Set // Computer and Information Science. 2009. Vol. 2. № 3.
4. Distributed Change-Point Detection of DDoS Attacks: Experimental Results on DETER Testbed // USENIX Association Berkeley. CA, USA.
5. *Maselli G., Deri L.* Design and Implementation of an Anomaly Detection System: an Empirical Approach // Terena TNC. Zagreb, Croatia, 2003.
6. *Sekar V., Duffield N., Spatscheck O., Van der Merwe J., Zhang H.* Lads: Large-scale automated DDoS detection system // USENIX Annual Technical Conference. 2006.
7. Cisco-Arbor Clean Pipe Solution 2.0 White Paper. URL: http://www.arbornetworks.com/index.php?option=com_docman&task=doc_download&gid=448.
8. Cisco Systems NetFlow Services Export Version 9 / Claise B., Ed. // RFC 3954. October 2004.
9. *Leinen S.* Evaluation of Candidate Protocols for IP Flow Information // RFC 3955. 2004.

А. Р. Орлов, Е. Б. Маховенко

АНАЛИЗ КРИПТОСИСТЕМ С ОТКРЫТЫМ КЛЮЧОМ, ПОСТРОЕННЫХ НА ОСНОВЕ ЗАДАЧ ТЕОРИИ РЕШЕТОК

Для построения криптосистем обычно применяются следующие задачи теории решеток:

1. По базису решетки найти кратчайший ненулевой вектор (SVP).

2. По базису решетки найти ближайший вектор $\bar{b}$ к заданному вектору $\bar{j}$ (CVP).

3. Найти m линейно независимых векторов B_m, для которых $\max_i \|Bx_i\| \le \lambda_n$ ($SIVP$).

4. Поиск кратчайшего расстояния между векторами в базисе решетки; по заданному базису определить, не превосходит ли кратчайший вектор норму N ($GapSVP$).

5. По базису решетки и заданному $\varepsilon > 0$ определить, существует ли в решетке вектор $\bar{v}$, близкий к заданному вектору $\bar{j}$ с точностью до ε ($GapCVP$).

6. По базису решетки, в котором кратчайший вектор в k раз меньше другого кратчайшего линейно независимого вектора, найти кратчайший вектор ($uSVP$).

7. Дана решетка с минимальным расстоянием l (необязательно известным); по базису B и вектору $\bar{j}$, такому, что $\rho(B, \bar{j}) \le \gamma l$, найти вектор в решетке (BDD).

8. Дан базис B q-нарной (модулярной) m-мерной решетки $L_q^{m \times n}$. Принадлежность вектора к решетке L определяется: $L(B) = \{B^T s \bmod q \subseteq Z^m, s \in Z^n\}$. На решетке равномерно распределен шум e (обычно с математическим ожиданием, равным 0, и дисперсией $\sqrt{q}$), q задан некоторым многочленом. $\bar{s} \in Z_q^n$ — некоторый исходный вектор без шума. Найти исходную точку в решетке (исключить шум) по некоторому множеству известных $(B\bar{s}_i + \bar{e}_i)$ — задача обучения с ошибками (LWE).

Все исследуемые криптосистемы можно условно разделить на два типа: имеющие строго доказанную криптостойкость, но неэффективные по времени работы и/или характеризующиеся быстрым ростом размеров ключей от параметров шифрования. К таким относятся системы на основе SVP, $uSVP$, $SIVP$ - задач [1]; эффективные по времени работы и затратам на хранение ключей, но не обладающие строго доказанной криптостойкостью. К таким относятся системы, основанные на частных случаях задач теории решеток или на решетках с цикличностью образующего их базиса [2], например криптосистема $NTRU$ (Draft standard IEEE 1363.1) [3].