А.Я. Шалаев

ОБЕСПЕЧЕНИЕ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ IMS НА УРОВНЕ ПРОТОКОЛА SIP

Мультимедийная IP подсистема IMS (IP Multimedia Subsystem) представляет собой сетевую архитектуру, основой которой является пакетная транспортная сеть, поддерживающая все технологии доступа и обеспечивающая реализацию большого числа инфокоммуникационных услуг. В настоящее время IMS рассматривается многими операторами и сервис-провайдерами, а также поставщиками оборудования как возможное решение для построения сетей следующего поколения NGN (Next Generation Network).

Оборудование, входящее в состав IMS-платформ, имеет уязвимости, присущие любым основанным на IP-протоколе решениям и, следовательно, подвержено атакам червей и вирусов, DDoS, спаму и различным видам фрода [1, 2]. Поэтому при применении сетей нового поколения NGN/IMS актуальной задачей является поддержание непрерывной информационной безопасности. Целью данной работы является анализ моделей обнаружения заранее неизвестных атак и соответствующих структурных решений для защиты домена IMS на уровне протокола инициирования сеанса связи SIP (Session Initiation Protocol).

Задача обнаружения неизвестных атак требует идентификации аномалий, связанных со злонамеренными действиями, в процессе сигнализации по протоколу SIP. Угрозы направлены, главным образом, на управляющий уровень IMS, в особенности, на различные типы функций управления сеансом вызова (CSCF), а также на серверы приложений (AS), находящиеся выше уровня управления. Средства обнаружения аномалий должны функционировать наряду с типичными компонентами стека SIP и определять отклонение от нормы во входящих сообщениях SIP. При этом логический анализ появления необычных событий (аномалий) требует дополнительной более тщательной, чем в нормальных условиях, обработки сигнализации SIP.

Одним из подходов, лежащих в основе обнаружения аномалий является вложение сообщений SIP в векторные пространства и измерение подобия. Этот подход, основывающийся на векторной модели – общем универсальном методе для формирования свойств (признаков), обычно используется в области информационного поиска [4]. Документ, в данном случае сообщения SIP, характеризуются частотами появления в них отличительных (характерных) комбинаций символов $k \in K$. Данная комбинация k и SIP сообщение s связаны количеством появления k в s, и таким образом можно получить значение частоты $f(s,k)$. Частота комбинации k действует как мера её значимости в s, например, $f(s,k) = 0$ указывает на отсутствие значимости, в то время как $f(s,k) > 0$ отражает определенное присутствие k в s. Функция вложения m получается посредством отображения сообщений SIP в $|K|$-мерное векторное пространство, заполненное частотами всех комбинаций множества K. Функция m определяется как [3]

$$m: S \mapsto R^{|K|},\ m(s) = f(s,k),$$

где S обозначает множество всех возможных сообщений SIP и $R^{|K|}$ - векторное вещественное пространство. Однако в отличие от текстовых документов, невозможно определить множество K априорно, поскольку образцы неизвестных и новых атак заранее неизвестны. Чтобы решить эту проблему, множество комбинаций K определяется неявно, например, используя определения "маркеров" и "N-грамм" (групп из N последовательных символов). В неявном представлении маркеры соответствуют всем возможным комбинациям, разделяемым определенными символами-разграничителями. Если обозначить все значения байта через B и определить множество D, как набор символов-разграничителей, то множество B, связываемое с маркерами, определяется как $X \coloneqq (B \backslash D)^*$, где знак * обозначает замыкание Kleene [4] к множеству X, соответствующее всем возможным объединениям символов.

Гранулярностью (степенью детализации) при выделении признаков можно управлять, используя множество D. В качестве примера рассмотрим как сообщение $s = BYE\_sip: sha@loniis.ru\_sip/2.0$ отображается, используя понятие маркеров. В этом случае набор разделителей $D = \{\_, @, :, /\}$. $K = \{BYE, sip, sha, loniis.ru, 2.0\}$, причем комбинация $k = sip$ встречается дважды. Тогда для данного K имеем $m(s) \rightarrow (1 \quad 2 \quad 1 \quad 1 \quad 1)$.

Функция вложения m отображает сообщения SIP в векторное пространство, для которого могут быть применены различные методы обучения с целью обнаружения аномалии. Можно использовать два метода, основанных на геометрических моделях нормального закона распределения [3]: глобальное и локальное обнаружение аномалии. Основой для таких геометрических моделей обучения является функция расстояния d, которая оценивает несходство двух сообщений x и z, как $d(x, z) = ||m(x) - m(z)||$, и соответствует Евклидову расстоянию в векторном пространстве. Основываясь на таком представлении расстояния для сообщений SIP, например, глобальная модель для обнаружения аномалии определяется путем размещения гиперсферы вокруг множества заданных SIP сообщений $S = \{s_1, \ldots, s_n\}$ отображенного в векторное пространство. В частности, отыскивается наименьшее отображение S соответствующее гиперсфере с минимальным объемом, которое может быть определено, решая следующую оптимизационную задачу:

$$\mu_{opt} = \arg\min_{\mu} \max_{1 \le i \le n} ||\mathrm{m}(\mathrm{s_i}) - \mu||$$

где μ_{opt} - центр оптимальной гиперсферы.

Аномалии лежат вне сферы из-за их большого расстояния от центра. Неизвестные атаки в S могут привести к гиперсферам с большим объемом. Эта проблема может быть ослаблена методом регуляризации, который "смягчает" границы гиперсферы таким образом, что выбросы и неизвестные атаки можно

компенсировать с помощью модели обучения, предложенной в [6]. А именно, как только центр μ_{opt} наименьшей гиперсферы найден, отклонение от этой глобальной модели нормальности определяется путем вычисления расстояния входящего сообщения z от μ_{opt}.

$$gd(z) = ||m(z) - \mu_{opt}||$$

Использование этой модели требует вычислений только единичного значения расстояния для каждого входящего сообщения, поскольку μ_{opt} полностью определяется из S во время предшествующей фазы обучения. Если трафик SIP, наблюдаемый в сетевом узле IMS, по своей природе неоднороден, например, в крупном шлюзе, глобальная модель нормальности может быть недостаточной для обнаружения неизвестных и новых атак. Чтобы обнаружить аномалии в таких условиях, применяется локальная модель обнаружения аномалии, которая оценивает отклонение сообщения, рассматривая только часть сообщений в обучающих данных.

Множество аномалий, обнаруживаемое на основе рассматриваемых моделей и методов, может служить основой для автоматической генерации сигнатур аномальных событий с целью применения в существующих системах обнаружения сетевых атак [5]. Такие сигнатуры (характерные признаки атак, используемые для их обнаружения) могут быть использованы далее для информирования (обучения) пограничных контроллеров сессий SBC (Session Border Controller). Типичный сценарий построения сети NGN/IMS предполагает размещение SBC на границах ядра (базовой сети) с сетями доступа, а также на границах с другими сетями. Контроллер транслирует сигнальный и медиапоток, обеспечивая единую точку входа/выхода сети. Кроме того, SBC с целью защиты функций ядра IMS от любых имеющих место при сигнализации угроз, поступающих извне, реализует широкий спектр функций по безопасности сети: сокрытие топологии сети, защиту от угрозы анализа трафика, контроль обмена сигнальными сообщениями и др.[2]. Структура рассматриваемой в данной

работе системы защиты против нападений предполагает введение в состав контроллеров SBC домена IMS средств, которые в процессе сигнализации по протоколу SIP могут идентифицировать аномалии, связанные с злонамеренными действиями. Основа этих средств – программные средства обнаружения аномалий, которые развернуты в SBC наряду с типичными компонентами стека SIP. Как только новая ранее неизвестная атака была идентифицирована с помощью рассмотренных выше моделей обнаружения аномалии, автоматически генерируется соответствующая сигнатура атаки и распределяется по всем SBC домена IMS. Такое структурное решение может использоваться для обеспечения информационной безопасности домена IMS в целом.

Список литературы:

1. Колесник В., Ехриель И., Баженов Э. Безопасность и фрод-контроль в сетях NGN/IMS // ИнформКурьерСвязь «ИКС». - 2012. - № 3. – С. 64-66.
2. Морозов А.М. Анализ уязвимости сети SIP к угрозам фрода // Электросвязь. - 2013, №7. – С. 10-13.
3. S. Wahl, K. Rieck, P. Laskov, P. Domschitz, K-R. Muller. Securing IMS Against Novel Threats // Bell Labs Tech. J. - 2009. V. 14, Number 1. – P. 243-258.
4. T. Joachims. Learning to Classify Text Using Support Vector Machines. Kluwer Academic Pub., Boston, MA, 2002.
5. Чипига А.Ф., Пелешенко В.С., Лазарев Н.В. Методика обнаружения сетевых атак на базе сигнатурных и статических методов // Успехи современного естествознания. – 2008. – № 8 – С. 61-62.
6. P. Lascov, C. Gehl, S. Kruger, K.-R. Muller. Incremental Support Vector Learning: Analysis, Implementation and Applications // J. Mach.Learn. Res., 7 (Sept. 2006). – p.1909 – 1936.

Shalaev Aleksandr Y.

Information security protection of IMS on SIP layer

The article presents an analysis of models for detection malicious attacks at the level of the session initiation protocol (SIP). The structure of system of protection of the IMS domain, using session border controllers (SBC) is considered.

Key words: IP Multimedia Subsystem IMS, information security, SIP (Session Initiation Protocol), vector space model, signature analysis, SBC (Session Border Controller)

Аннотация. Проведен анализ моделей обнаружения «злонамеренных» атак на уровне протокола инициирования сеанса связи (SIP). Рассмотрена структура системы защиты домена IMS, использующая пограничные контроллеры сессий (SBC).

Ключевые слова:
Мультимедийная IP подсистема IMS, информационная безопасность, протокол SIP, векторная модель, сигнатурный анализ, SBC