После выполнения рассмотренных выше операций исходный массив сетевого трафика оказывается разбит на множество отдельных структурных элементов – потоков, после чего может быть произведено вычисление необходимых для используемой модели статистических характеристик как отдельных потоков, так и массива СТ в целом.

Одним из наиболее важных достоинств предлагаемого в данной работе механизма выделения структурных элементов СТ является его расширяемость: благодаря отсутствию привязки к конкретной реализации сетевой адресации, он легко может быть модернизирован для работы с трафиком IPv6, а разработка дополнительных подпрограмм для выделения потоков STCP и RTP позволит корректно обрабатывать трафик и этих протоколов транспортного уровня.

Библиографические ссылки

1. http://frozentux.net/documents/iptables-tutorial/
2. http://www.ietf.org/rfc/rfc792.txt

БРАНДМАУЭР ВЕБ-ПРИЛОЖЕНИЙ – ОБЗОР, НЕДОСТАТКИ

А. В. Адамов, А. В. Бабич
(Тюмень, ТюмГУ)

Введение

На сегодняшний день одной из самых быстроразвивающихся сфер деятельности человека является Интернет. Неудивительно, что наряду с его развитием теми же темпами развиваются и угрозы безопасности сервисов, работающих в среде Интернет. По данным статистики WASC (Web Application Security Consortium) [1] более 13 % сайтов могут быть скомпромитированы полностью автоматически, 80–96 % из которых имеют высокую степень уязвимостей, 86 % – среднюю степень уязвимостей, 37 % – низкую.

В данной работе хотелось бы поговорить о части Интернета, являющейся его непосредственным лицом и касающейся практи-

чески каждого пользователя, – это веб-сайты и их безопасность. Актуальность проблемы безопасности такого вида приложений растет с каждым днем, а большинство уязвимостей, существующих на данный момент в этой сфере, связаны с ошибками и недочетами, допущенными на этапе разработки сайта.

Обусловлено это тем, что порог вхождения в сферу создания веб-сайтов минимальный, благодаря упрощенным языкам веб-программирования и развивающимся технологиям, делающим процесс создания сайта простым, но эффективным с точки зрения достижения цели заказчиком. В то же время роль сайтов и их влияние на бизнес постоянно растет, а перенасытившийся рынок неквалифицированных веб-программистов, зачастую роль которых выполняют студенты, пагубно влияет на качество программных продуктов и сайтов в частности. Проблема безопасности у таких исполнителей, к сожалению, стоит далеко не на первом месте. Положение усугубляется и тем, что заказчик порой остается в неведении, что его сайт и все располагающиеся там данные являются слабо защищенными или не защищенными вообще.

Что делать?

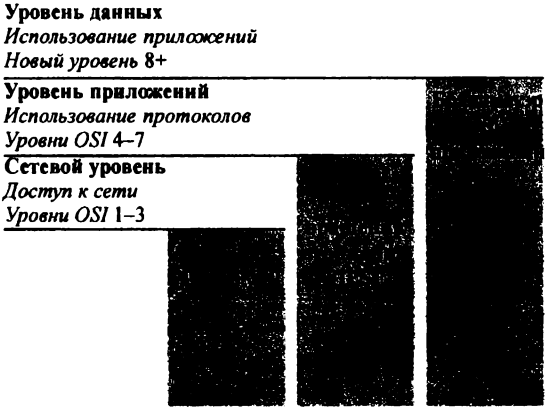
Таким образом, мы подошли к вопросу о необходимости решения указанной проблемы. Возможных вариантов несколько. Первый – обучить всех веб-программистов основам безопасности при создании сайтов, но данный способ не масштабируем и трудно реализуем с учетом темпов роста количества программистов. Наиболее оптимальным вариантом компенсации человеческого фактора, – ошибок программиста в процессе создания веб-сайтов – на сегодняшний день является технология WAF (Web Application Firewall).

WAF – Брандмауэр веб-приложений

WAF – это межсетевой экран, накладывающий определенный набор правил на то, как происходит взаимодействие сервера и клиента путем обработки HTTP-запросов. В основе лежит тот же принцип, что и в обычных фаерволах – контроль и анализ всех пакетов, поступающих от клиента. WAF опирается на набор правил,

с помощью которых выявляется факт атаки по сигнатурам – признакам активности пользователя, которые могут означать нападение.

Брандмауэр web-приложений еще называют третьей линией обороны. В такой парадигме первой линией обороны являются межсетевые экраны, второй – системы IPS и, наконец, третьей – WAF (рисунок).



Типы WAF

Web Application Firewall разделяют на 2 типа: аппаратный и программный. Наибольшее распространение получил второй ввиду более простой реализации.

По принципу действия WAF можно разделить на 3 типа:

1. Реализованные в виде обратного прокси-сервера;
2. Работающие в режиме маршрутизации/моста;
3. Встроенные в веб-приложения.

Обратный прокси-сервер

В данном типе WAF все данные сначала обрабатываются прокси-сервером, который уже решает, пропускать пакеты или блокировать. В случае положительного результата данные перенаправляются к веб-серверу без изменения либо с частичной правкой.

К данному типу относятся: mod_security [2], Barracuda [3], nevisProxy [4].

Режим маршрутизации/моста

К этому типу чаще всего относят аппаратные WAF. У данного типа реализации есть как плюсы, так и минусы. К первым можно отнести прирост производительности, ко вторым – более сложную и тонкую настройку.

Примером данного типа WAF является Impreva SecureSphere [5].

Встроенные в веб-приложения

Данный тип WAF встраивается непосредственно в веб-приложение в качестве дополнительного функционала и работает на программном уровне.

Наиболее распространенным подобным WAF в России является брандмауэр, встроенный в CMS Битрикс [6].

Обработка правил в WAF может осуществляться по принципу blacklist (производится сопоставление со списком недопустимых условий), whitelist (принимаются только разрешенные действия) или смешанно.

Типы угроз

На сегодняшний день почти все брандмауэры веб-приложений призваны защитить от основных типов угроз, свойственных веб-сайтам.

- SQL-инъекция;
- Межсайтовый скриптинг (XSS);
- Межсайтовые подделки запросов (CSRF);
- Спам в комментариях;
- Распределенный отказ в обслуживании (DDoS-атаки);
- Отсутствие таймаута сессии;
- Обратный путь в директориях.

Недостатки WAF

Основной проблемой, существующей на данный момент, являются ограниченные возможности существующей технологии WAF в обеспечении защиты от широкого спектра угроз, а также возможность обхода существующих на данный момент брандмауэров.

Каждый брандмауэр имеет отличительную особенность и оставляет за собой след. Для обнаружения того или иного firewall используется метод распознавания fingerprint, что в переводе означает «отпечаток пальца». Например:

- специальные коды ответа при передаче особых данных или вызове ошибок;
- специальные переменные, хранимые в Cookie;
- изменение HTTP-заголовков, в частности данных, передающихся в Server;
- незамедлительное завершение соединения при срабатывании недопустимого условия;
- встроенный набор базовых правил, поддающийся раскрытию.

После того как WAF обнаружен, остается только найти его уязвимость и использовать ее. Стопроцентной защиты не существует, и WAF – не исключение. На сегодняшний день имеется множество вариантов обхода WAF, и этот список постоянно пополняется. В качестве примера можно взять исследование компании Positive Technologies, которая нашла более 30 возможностей обхода существующих WAF [7].

Заключение

Основная проблема современных WAF кроется в их архитектуре, основанной на общем принципе использования сигнатурного анализа для определения типа угроз.

Недостаток такого подхода очевиден: его легко обнаружить и относительно легко обойти.

Один из возможных вариантов решения этой проблемы я вижу в применении методов поведенческого анализа. Принцип такого подхода в корне отличается от сигнатурного. За основу берется нормальное поведение, скажем, в скрипте С чтение из таблицы А – нормально, а чтение из таблицы Б считается аномальным. Данный подход в теории может избавить от уязвимостей, связанных с сигнатурным анализом. Данное направление я вижу наиболее перспективным в решении проблем безопасности веб-сайтов.

Библиографические ссылки

1. Статистика уязвимостей Web-приложений за 2008 год [Электронный ресурс]. Режим доступа: http://ru.scribd.com/doc/21324267/WASC-Web-Application-Security-Statistics-2008-Russian

2. ModSecurity [Электронный ресурс]. Режим доступа: http://modsecurity.org

3. Barracuda Networks, Inc. (US) [Электронный ресурс]. Режим доступа: http://barracudanetworks.com

4. AdNovum Informatik AG [Электронный ресурс]. Режим доступа: http://adnovum.ch

5. A division of Virtual Graffiti, Inc. [Электронный ресурс]. Режим доступа: http://impervaguard.com

6. Компания «1С-Битрикс» [Электронный ресурс]. Режим доступа: http://1c-bitrix.ru

7. *Евтеев Д.* Методы обхода Web Application Firewall [Электронный ресурс]. Режим доступа: http://www.ptsecurity.ru/download/PT-devteev-CC-WAF.pdf

ВОЗМОЖНОСТИ ПРОГРАММНОГО УПРАВЛЕНИЯ СМАРТФОНОМ В ТЕХНОЛОГИЧЕСКИХ РЕЖИМАХ

В. В. Бакланов, И. А. Бильдинов
(Екатеринбург, УрФУ, banbmw@k66.ru)

По данным аналитической компании Strategy Analytics на конец 2-го квартала 2013 г. компания Google контролирует 67 % рынка операционных систем (ОС) планшетов. За год популярность операционной системы Android поднялась почти в 2 раза: с 18,5 млн поставленных устройств до 34,6 млн планшетных ПК, в то время как доля присутствия операционной системы Apple iOS за квартал упала с 47,2 % до 28,3 %. И это падение обусловлено популярностью Android [1]. Еще одна аналитическая компания J'son & Partners Consulting сообщает, что ОС Android лидирует на рынке ОС для смартфонов в России с долей в 77 %. Второе место, как в России, так и по миру, занимает iOS с долей 11 % по России и 13 % по миру [2].