Современные тенденции в области контентной фильтрации

Alex Ott

23 июля 2007 г.

1 Введение

В настоящее время контентную фильтрацию нельзя выделить в отдельную область компьютерной безопасности, настолько она переплелась с другими направлениями. В обеспечении компьютерной безопасности контентная фильтрация очень важна, поскольку позволяет вычленять потенциально опасные вещи и корректно их обрабатывать. Подходы, появившиеся при разработке продуктов для контентной фильтрации, находят применение в продуктах для предотвращения вторжений (IDS), распространения вредоносного кода и других негативных действий.

На основе новых технологий и продуктов в области контентной фильтрации создаются дополнительные услуги для пользователей, повышается качество защиты и обеспечивается возможность не только обрабатывать существующие угрозы, но и предотвращать целые классы новых угроз.[1]

2 Новые тенденции в области контентной фильтрации

Одна из общих тенденций развития продуктов информационной безопасности — стремление реализовать различные функции в одном устройстве или программном решении. Как правило, разработчики стараются выполнить решения, которые кроме функций контентной фильтрации еще выполняют и функции антивируса, межсетевого экрана и/или системы обнаружения и предотвращения вторжений. С одной стороны, это позволяет снизить затраты компаний на покупку и сопровождение систем безопасности, но с другой — функциональность таких систем часто оказывается ограниченной. Например, во многих продуктах функции фильтрации Web-трафика сведены только к проверке адресов сайтов относительно какой-либо базы данных категорий сайтов.

К этому же направлению можно отнести и развитие продуктов в соответствии с концепцией Unified Threat Management (UTM), которая обеспечивает унифицированный подход к предотвращению угроз независимо от того, какой из протоколов или какие данные обрабатываются.

[1] Первоначально данная статья была опубликована в октябрьском номере журнала JetInfo http://www.jetinfo.ru. В данную статью были внесены некоторые изменения, отражающие современное состояние дел. Кроме того, убран раздел, описывающий продукты компании "Инфосистемы Джет о которых вы можете прочитать на продуктовом сайте компании http://www.jetsoft.ru.

Этот подход позволяет избежать дублирования функций защиты, а также обеспечить актуальность данных с описанием угроз для всех контролируемых ресурсов.

В существующих уже достаточно давно областях контентной фильтрации — контролепочты и Интернет-трафика — также происходятизменения, появляются новые технологии.

В продуктах для контроля почтового обмена стала выходить на первый план функция защиты от фишинга. А в продуктах для контроля Интернет-трафика происходит смещение от использования заранее подготовленных баз адресов к категоризации по содержимому, что является очень актуальной задачей при работе с разнообразными портальными решениями.

Кроме двух указанных выше областей, возникают и новые области применения контентной фильтрации — некоторое время назад начали появляться продукты для контроля за передачей мгновенных сообщений (instant messaging) и peer-to-peer (p2p) соединений. В настоящее время активно разрабатываются также продукты для контроля за VoIP-трафиком.

Во многих странах активно стали развивать средства для перехвата и анализа многих видов информации, которая используется для различного вида расследований (lawful interception). Данные мероприятия проводятся на государственном уровне и наиболее часто привязываются к расследованию террористических угроз. Такие системы перехватывают и анализируют не только данные, передаваемые по каналам Интернет, но также и по другим видам связи — телефонным линиям, радиоканалам и т.п. Наиболее известной системой для перехвата информации является Echelon — система, использовавшаяся американской разведкой для сбора информации. В России также существуют различные реализации системы оперативно-розыскных мероприятий (СОРМ), которые используются для захвата и анализа информации в интересах спецслужб.

В качестве одной из тенденций на рынке продуктов контентной фильтрации можно отметить массовую консолидацию компаний-производителей таких решений. Хотя эта тенденция в большей мере отражает организационную сторону процесса, но она может привести к появлению новых продуктов и направлений для компаний, у которых этих направлений не было, либо они занимали незначительную часть сектора рынка таких компаний. Иллюстрацией вышесказанного могут служить следующие случаи объединения/поглощения компаний:

1. компания Secure Computing, которая в прошлом году купила компанию Cyberguard, обладающую хорошим набором средств фильтрации Интернет-трафика, летом объединилась с другой компанией — CipherTrust, имеющей большой опыт разработки средств для фильтрации почтового трафика;

2. компания MailFrontier, производившая средства для защиты почтового трафика, была поглощена компанией SonicWall, у которой до этого не было решений с таким качеством разработки;

3. в конце июля 2006 г. компания SurfControl, известная своими решениями в области контентной фильтрации, купила компанию BlackSpider, которая предоставляла расширенные сервисы в части компьютерной безопасности;

4. в конце августа 2006 г. произошло самое грандиозное поглощение — компания Internet Security Systems (ISS) подписала соглашение о слиянии с компанией IBM. Это слияние является примером большого интереса к информационной безопасности со стороны крупных компаний-разработчиков программного обеспечения;

5. В январе 2007 г. компания Cisco поглотила компанию IronPort, имеющую хорошую линейку продуктов для безопасности электронной почты;

6. компания Microsoft за последние несколько лет провела поглощение нескольких компаний, занимавшихся информационной безопасностью. Самым крупным из них было поглощение компании Sybari с ее линейкой средств защиты от вирусов и другого вредоносного кода, а также средств для контентной фильтрации почтовых и мгновенных сообщений. Поглощение Sybari и других компаний позволяет Microsoft успешно конкурировать на новом для нее рынке компьютерной безопасности.

Стоит также отметить, что в последние годы начали появляться продукты для контентной фильтрации с открытым исходным кодом. В большинстве случаев они не достигают такого функционала как коммерческие приложения, однако есть конкретные решения и области применения, где они могут составить реальную угрозу.

3 Современные угрозы

Современная ИТ-инфраструктура подвергается множеству атак, целью которых становятся и простые пользователи, и компании независимо от их размера. Наиболее актуальными являются следующие виды угроз:

1. Фишинг (Phishing) — распространившиеся в последнее время способы перехвата важных данных пользователей (паролей, номеров кредитных карт и т.п.) с помощью техник социальной инженерии, когда пользователя ложным письмом или сообщением от той или иной организации пытаются заставить ввести определенные данные на сайте, контролируемом злоумышленником;

2. Spyware & Malware — различные средства, позволяющие перехватывать данные или устанавливать контроль над компьютером. Существует множество разновидностей таких средств, которые различаются по степени опасности для компьютера — от простого показа рекламных сообщений до перехвата данных, вводимых пользователями, и захвата контроля над операциями с компьютером;

3. вирусы и другой вредоносный код — вирусы, черви и троянцы — давно известная угроза для ИТ-инфраструктуры. Но с каждым годом появляются новые модификации вредоносного кода, которые часто эксплуатируют уязвимости в существующем программном обеспечении, что позволяет им распространяться автоматически;

4. SPAM/SPIM — нежелательные сообщения, передаваемые с помощью электронной почты (SPAM) или средств обмена мгновенными сообщениями (SPIM) заставляют пользователей тратить свое время на обработку нежелательной корреспонденции.

В настоящее время СПАМ составляет более 70% всех передаваемых почтовых сообщений;

5. атаки на инфраструктуру — ИТ-инфраструктура компаний имеет очень важное значение, атаки с целью выведения ее из строя предельно опасны. Для них могут быть задействованы целые сети компьютеров, зараженных каким-либо вирусом, используемым для перехвата управления. Например, некоторое время назад был распространен вирус, содержавший в себе код, который должен был в определенное время начать распределенную атаку на сайты компании Microsoft с целью выведения их из строя. Зараженными оказались несколько миллионов компьютеров, и только ошибка в коде вируса не позволила выполнить планируемую атаку;

6. утечка бизнес-информации — предотвращение таких утечек является одной из главных задач продуктов контентной фильтрации. Утечка важной информации может нанести компании непоправимый ущерб, порой сравнимый с потерей основных средств производства. Поэтому во многих продуктах развиваются средства для определения каналов скрытой передачи данных, таких например, как применение стеганографии;

7. угроза судебного преследования — этот вид угроз крайне актуален для компаний, если их сотрудники могут пользоваться файлообменными сетями, скачивая и/или распространяя музыку, фильмы и другое содержимое, защищенное авторским правом. Судебное преследование возможно и за распространение клеветнической и/или порочащей информации, касающейся третьих лиц.

Первым пяти видам угроз подвергаются как домашние компьютеры, так и компьютеры корпоративных сетей. А вот последние две угрозы являются особенно актуальными для компаний всех видов.

4 Фильтрация Интернет-трафика

В последнее время в области фильтрации Интернет-трафика происходят различные изменения, обусловленные появлением новых технологий фильтрации и изменением технологий, которые используются для построения Интернет-сайтов.

Одной из наиболее важных тенденций развития продуктов контентной фильтрации в части контроля Интернет-трафика является переход от использования баз данных категорий сайтов к определению категории сайта по его содержимому. Это стало особенно актуально с развитием различных порталов, которые могут содержать наполнение разных категорий, изменяющееся во времени и/или подстраиваемое под настройки клиента.

Ставшие в последнее время популярными технологии и инструменты построения Интернет-сайтов, такие как Ajax, Macromedia Flash и другие, требуют внесения изменений и в технологии фильтрации Интернет-трафика.

Использование шифрованных каналов для взаимодействия с Интернет-сайтами обеспечивает защиту данных от перехвата третьими лицами, но в то же время, по этим каналам передачи данных могут происходить утечка важной информации или проникновение вредоносного кода в компьютерные системы.

Актуальной остается проблема интеграции средств защиты с системами, обеспечивающими функционирование ИТ-инфраструктуры, такими как прокси-серверы, веб-серверы, почтовые серверы, серверы каталогов и т.п. Разными компаниями и некоммерческими организациями разрабатываются протоколы для взаимодействия между различными системами.

О современном положении дел в этой области пойдет речь ниже.

4.1 Подходы к категоризации сайтов и данных

Категоризация сайтов и данных, на них размещенных, может выполняться разными способами. В настоящее время выделяются следующие виды категоризации:

1. использование предопределенных баз категорий сайтов с регулярным обновлением списков сайтов и категорий;
2. категоризация данных на лету путем анализа содержимого страниц;
3. использование данных о категории, информацию о принадлежности к которой предоставляет сам сайт.

Каждый из этих методов имеет свои достоинства и недостатки.

4.1.1 Предопределенные базы категорий сайтов

Использование заранее подготовленных баз адресов сайтов и связанных с ними категорий — давно используемый и хорошо зарекомендовавший себя метод. В настоящее время такие базы предоставляют многие компании, такие как Websense, Surfcontrol, ISS/Cobion, Secure Computing, Astaro AG, NetStar и другие. Некоторые компании используют эти базы только в своих продуктах, другие позволяют подключать их к продуктам третьих фирм. Наиболее полными считаются базы, предоставляемые компаниями Websense, Secure Computing, SurfControl и ISS/Cobion, они содержат информацию о миллионах сайтов на разных языках и в разных странах, что особенно актуально в эпоху глобализации.

Категоризация данных и формирование баз категорий обычно производится в полуавтоматическом режиме — сначала выполняются анализ содержимого и определение категории с помощью специально разработанных средств, которые даже могут включать в себя системы распознавания текстов в картинках. А на втором этапе полученная информация часто проверяется людьми, принимающими решение о том, к какой категории можно отнести тот или иной сайт.

Многие компании автоматически пополняют базу категорий по результатам работы у клиентов, если обнаруживается сайт, не отнесенный еще ни к какой из категорий.

В настоящее время используются два способа подключения предопределенных баз категорий сайтов:

1. использование локальной базы категоий с регулярным ее обновлением. Данный метод очень удобен для больших организаций, имеющих выделенные серверы фильтрации и обслуживающие большое количество запросов;

2. использование базы категорий, размещенной на удаленном сервере. Данный метод часто применяется в различных устройствах — небольших межсетевых экранах, ADSL-модемах и т.п. Использование удаленной базы категорий немного увеличивает нагрузку на каналы, но обеспечивает использование актуальной базы категорий.

К преимуществам применения предопределенных баз категорий можно отнести то, что предоставление или запрет доступа производится еще на этапе выдачи запроса клиентом, что может существенно снизить нагрузку на каналы передачи данных. А главный недостаток использования данного подхода — задержки в обновлении баз категорий сайтов, поскольку для анализа потребуется некоторое время. Кроме того, некоторые сайты достаточно часто меняют свое наполнение, из-за чего информация о категории, хранящаяся в базе адресов, становится неактуальной. Некоторые сайты также могут предоставлять доступ к разной информации, в зависимости от имени пользователя, географического региона, времени суток и т.п.

4.1.2 Категоризация данных на лету

Категоризация сайтов на лету также осуществляется самыми разными способами. Особенно часто используются методы, основанные на статистическом подходе к анализу содержания.

Один из простых вариантов реализации такого решения — использование байесовских алгоритмов, которые себя достаточно хорошо зарекомендовали в борьбе со спамом. Однако у этого варианта есть свои недостатки — необходимо его периодически доучивать, корректировать словари в соответствии с передаваемыми данными. Поэтому некоторые компании применяют более сложные алгоритмы определения категории сайта по содержимому в дополнение к простым способам. Например, компания ContentWatch предоставляет специальную библиотеку, которая выполняет анализ данных согласно лингвистической информации о том или ином языке и на основании этой информации может определять категорию данных.

Категоризация данных на лету позволяет быстро реагировать на появление новых сайтов, поскольку информация о категории сайта не зависит от его адреса, а только от содержания. Но такой подход имеет и недостатки — необходимо проводить анализ всех передаваемых данных, что вызывает некоторое снижение производительности системы. Второй недостаток — необходимость поддержания актуальных баз категорий для различных языков. Тем не менее, некоторые продукты применяют этот подход с одновременным использованием баз категорий сайтов. Сюда можно отнести использование Virtual Control Agent в продуктах компании SurfControl, механизмы определения категорий данных в СКВТ "Дозор-Джет".

4.1.3 Данные о категории, предоставляемые сайтами

Кроме баз данных адресов и категоризации содержимого на лету существует и другой подход к определению категории сайтов — сайт сам сообщает о том, к какой категории он относится.

Этот подход в первую очередь предназначен для использования домашними пользователями, когда, например, родители или учителя могут задать политику фильтрации и/или отслеживать, какие сайты посещаются.

Существует несколько путей реализации данного подхода к категоризации ресурсов:

1. PICS (Platform for Internet Content Selection) — спецификация, разработанная консорциумом W3 около десяти лет назад и имеющая различные расширения, направленные на обеспечение надежности рейтинговой системы. Для контроля может использоваться специальное разработанное программное обеспечение, доступное для загрузки со страницы проекта. Более подробную информацию о PICS можно найти на сайте консорциума W3.org (http://www.w3.org/PICS/).

2. ICRA (Internet Content Rating Association) — новая инициатива, разрабатываемая независимой некоммерческой организацией с тем же названием. Основная цель данной инициативы — защита детей от доступа к запрещенному содержимому. Данная организация имеет соглашения с множеством компаний (крупные телекоммуникационные и компании-разработчики ПО) для обеспечения более надежной защиты.

   ICRA предоставляет программное обеспечение, которое позволяет проверять специальную метку, возвращаемую сайтом, и принимать решение о доступек этим данным. Программное обеспечение работает только на платформе Microsoft Windows, но благодаря открытой спецификации существует возможность создания реализаций фильтрующего ПО и для других платформ. Цели и задачи, решаемые данной организацией, а также все необходимые документы можно найти на сайте ICRA — http://www.icra.org/.

К достоинствам этого подхода можно отнести то, что для обработки данных нужно только специальное программное обеспечение и нет необходимости обновлять базы адресов и/или категорий, так как вся информация передается самим сайтом. Но недостатком является то, что сайт может указывать неправильную категорию, а это приведет к неправильному предоставлению или запрещению доступа к данным. Однако эту проблему можно решить (и она уже решается) за счет использования средств подтверждения правильности данных, таких как цифровые подписи и т. п.

4.2 Фильтрация трафика в мире Web 2.0

Массовое внедрение так называемых технологий Web 2.0 сильно усложнило контентную фильтрацию веб-трафика. Поскольку во многих случаях данные передаются отдельно от оформления, существует возможность пропуска нежелательной информации к пользователю или от пользователя. В случае работы с сайтами, применяющими такие технологии, необходимо делать комплексный анализ передаваемых данных, определяя передачу дополнительной информации и учитывая данные, собранные на предыдущих этапах.

В настоящее время ни одна из компаний, выпускающих средства для контентной фильтрации веб-трафика, не позволяет производить комплексный анализ данных, передаваемых с использованием технологий AJAX.

4.3 Интеграция с внешними системами

Во многих случаях достаточно острым становится вопрос об интеграции систем контентного анализа с другими системами. При этом системы контентного анализа могут выступать как клиентами, так и серверами или в обеих ролях сразу. Для этих целей было разработано несколько стандартных протоколов — Internet Content Adaptation Protocol (ICAP), Open Pluggable Edge Services (OPES). Кроме того, некоторые производители создавали собственные протоколы для обеспечения взаимодействия конкретных продуктов друг с другом или со сторонним программным обеспечением. Сюда можно отнести протоколы Cisco Web Cache Coordination Protocol (WCCP), Check Point Content Vectoring Protocol (CVP) и другие.

Некоторые протоколы — ICAP и OPES — разработаны так, что могут использоваться для реализации как сервисов контентной фильтрации, так и других сервисов — переводчики, размещение рекламы, доставка данных, зависящая от политики их распространения, и т.п.

4.3.1 Протокол ICAP

В настоящее время протокол ICAP пользуется популярностью среди авторов ПО для контентной фильтрации и создателей программного обеспечения для определения вредоносного содержимого (вирусы, spyware/malware). Однако стоит отметить, что ICAP в первую очередь разрабатывался для работы с HTTP, что накладывает много ограничений на его использование с другими протоколами.

ICAP принят группой Internet Engineering Task Force (IETF) в качестве стандарта. Сам протокол определяется документом "RFC 3507"с некоторыми дополнениями, изложенными в документе "ICAP Extensions draft". Эти документы и дополнительная информация доступны с сервера ICAP Forum — http://www.i-cap.org.

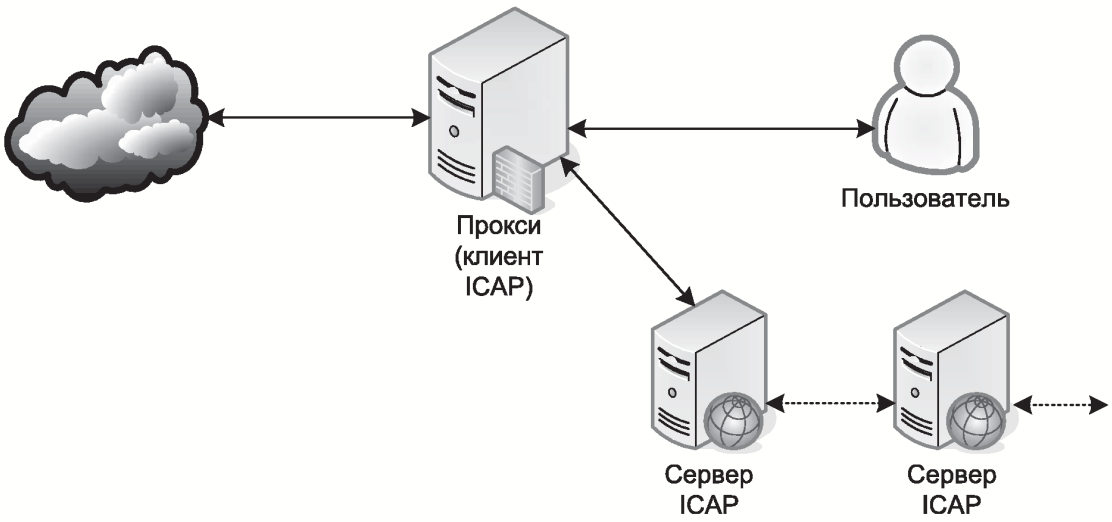

Рис. 1. Схема взаимодействия серверов и клиентов ICAP

Архитектура системы при использовании протокола ICAP изображена на рисунке

Схема взаимодействия серверов и клиентов ICAP. В качестве клиента ICAP выступает система, через которую передается трафик. Система, выполняющая анализ и обработку данных, называется сервером ICAP. Серверы ICAP могут выступать в роли клиентов для других серверов, что обеспечивает возможность стыковки нескольких сервисов для коллективной обработки одних и тех же данных.

Для взаимодействия между клиентом и сервером используется протокол, похожий на протокол HTTP версии 1.1, и те же способы кодирования информации. Согласно стандарту ICAP может обрабатывать как исходящий (REQMOD — Request Modification), так и входящий (RESPMOD — Response Modification) трафик.

Решение о том, какие из передаваемых данных будут обрабатываться, принимается клиентом ICAP, в некоторых случаях это делает невозможным полный анализ данных. Настройки клиента полностью зависят от его реализации, и во многих случаях невозможноих изменить.

После получения данных от клиента сервер ICAP выполняет их обработку, а если это необходимо, то и модификацию данных. Затем данные возвращаются клиенту ICAP, и он их передает дальше серверу или клиенту, в зависимости от того, в каком направлении они передавались.

Наиболее широкое применение протокол ICAP нашел в продуктах для защиты от вредоносного кода, поскольку он позволяет использовать эти проверки в различных продуктах и не зависит от платформы, на которой выполняется клиент ICAP.

К недостаткам использования ICAP можно отнести следующее:

1. дополнительные сетевые взаимодействия между клиентом и сервером несколько замедляют скорость передачи данных между внешними системами и потребителями информации;

2. существуют проверки, которые необходимо выполнять не на клиенте, а на сервере ICAP, такие как определение типа данных и т.п. Это актуально, поскольку во многих случаях клиенты ICAP ориентируются на расширение файла или на тип данных, сообщенный внешним сервером, что может стать причиной нарушения политики безопасности;

3. затрудненная интеграция с системами, использующими протоколы, отличные от HTTP, не позволяет использовать ICAP для глубокого анализа данных.

4.3.2 Протокол OPES

В отличие от ICAP протокол OPES разрабатывался с учетом особенностей конкретных протоколов. Кроме того, при его разработке учитывались недостатки протокола ICAP, такие как отсутствие установления подлинности клиентов и серверов, отсутствие аутентификации и др.

Так же как и ICAP, OPES принят группой Internet Engineering Task Force в качестве стандарта. Структура взаимодействия сервисов, протокол взаимодействия, требования к сервисам и решения по обеспечению безопасности сервисов изложены в документах RFC 3752, 3835, 3836, 3837 и других. Список регулярно пополняется новыми документами, описывающими применение OPES не только к обработке интернет-трафика, но и к обработке почтового трафика, а в будущем, возможно, и других видов протоколов.

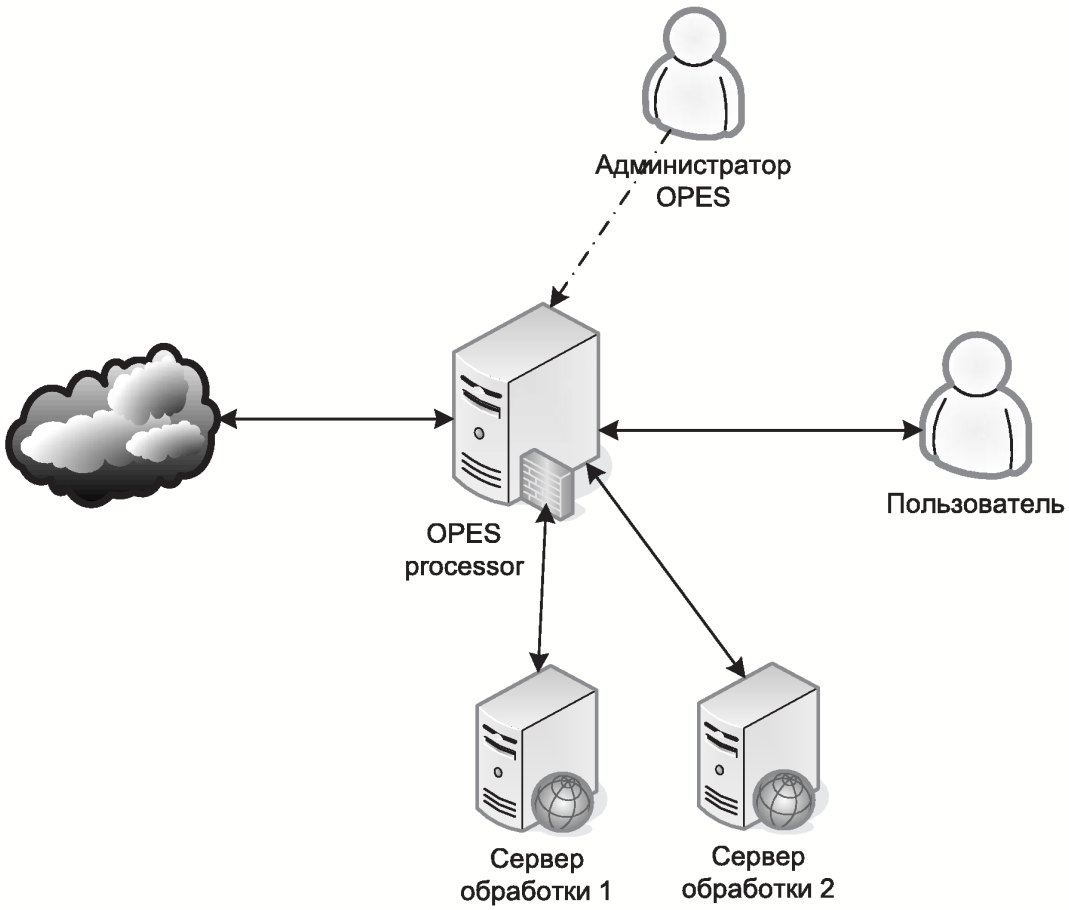

Рис. 2. Схема взаимодействия клиентов и серверов OPES

Структура взаимодействия серверов OPES и клиентов (OPES Processor) изображена на рисунке Схема взаимодействия клиентов и серверов OPES. В общих чертах она подобна схеме взаимодействия серверов и клиентов ICAP, но есть и существенные отличия:

1. имеются требования к реализации клиентов OPES, что делает возможным более удобное управление ими — задание политик фильтрации и т.п.;

2. потребитель данных (пользовательили информационная система) может оказывать влияние на обработку данных. Например, при использовании автоматических переводчиков получаемые данные могут автоматически переводиться на тот язык, который используется пользователем;

3. системы, предоставляющие данные, также могут оказывать влияние на результаты обработки;

4. серверы обработки могут использовать для анализа данные, специфичные для протокола, по которому данные были переданы клиенту OPES;

5. некоторые серверы обработки данных могут получать более важные данные, если они находятся в доверительных отношениях с клиентом OPES, потребителями и/или

поставщиками информации.

Все перечисленные возможности зависят исключительно от конфигурации, применяемой при внедрении системы. За счет этих возможностей использование OPES более перспективно и удобно, чем использование протокола ICAP.

В скором будущем ожидается появление продуктов, поддерживающих OPES наравне с протоколом ICAP. Пионером в разработке и использовании OPES является компания Secure Computing со своей линейкой продуктов Webwasher.

Поскольку в настоящее время нет полноценных реализаций, использующих OPES, то нельзя делать окончательные выводы о недостатках данного подхода, хотя теоретически пока остается лишь один недостаток — увеличение времени обработки за счет взаимодействия между клиентами и серверами OPES.

4.4 HTTPS и другие виды шифрованного трафика

По расчетам некоторых аналитиков, до 50% Интернет-трафика передается в зашифрованном виде. Проблема контроля шифрованного трафика сейчас актуальна для многих организаций, поскольку пользователи могут применять шифрацию для создания каналов утечки информации. Кроме того, шифрованные каналы могут использоваться и вредоносным кодом для проникновения в компьютерные системы.

Существует несколько задач, связанных с обработкой шифрованного трафика:

1. анализ данных, передаваемых по зашифрованным каналам;
2. проверка сертификатов которые, используются серверами для организации шифрованных каналов.

Актуальность этих задач возрастает с каждым днем.

4.4.1 Контроль передачи шифрованных данных

Контроль передачи данных, пересылаемых по зашифрованным каналам, является, наверное, самой важной задачей для организаций, сотрудники которых имеют доступ к Интернет-ресурсам. Для реализации этого контроля существует подход, называемый "Man-in-the-Middle"(в некоторых источниках его также называют "Main-in-the Middle"), который может использоваться злоумышленниками для перехвата данных. Схема обработки данных для данного метода дана на рисунке Процесс обработки шифрованных данных.

Процесс обработки данных выглядит следующим образом:

1. в Интернет-броузер пользователя устанавливается специально выписанный корневой сертификат, который используется прокси-сервером для подписывания сгенеренного сертификата (без установки такого сертификата, броузер пользователя будет выдавать сообщение о том, что подписывающий сертификат выдан недоверенной организацией);

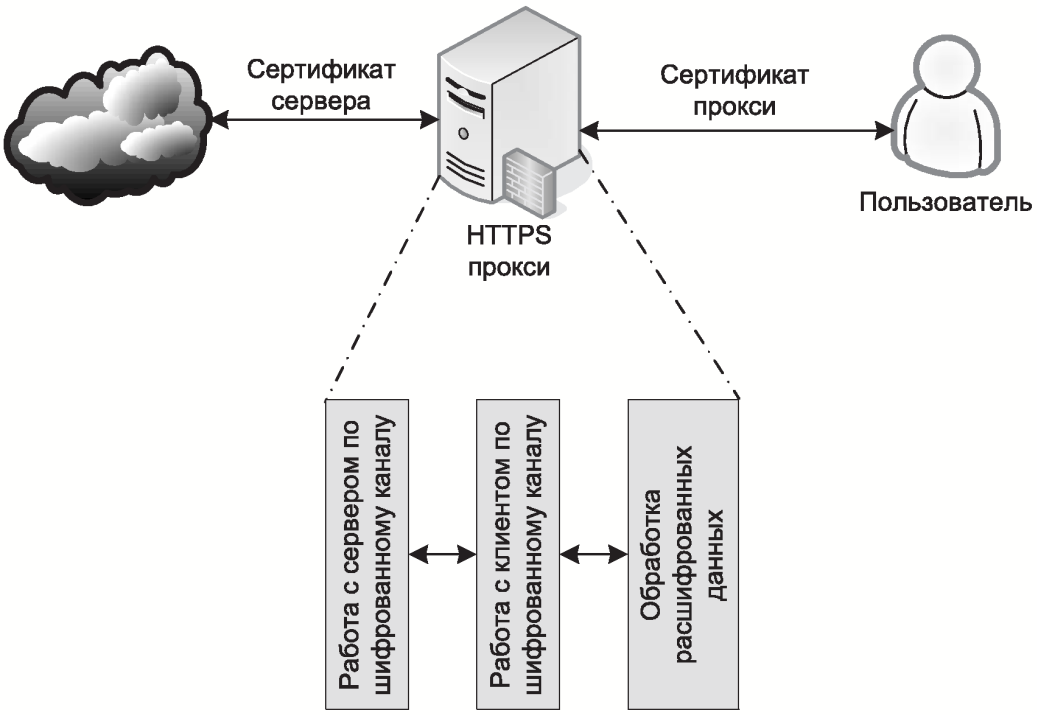

Рис. 3. Процесс обработки шифрованных данных

2. при установлении соединения с прокси-сервером происходит обмен данными, и в браузер передается специально сгенерированный сертификат с данными сервера назначения, но подписанный известным ключем, что позволяет прокси-серверу расшифровывать передаваемый траффик;

3. расшифрованные данные анализируются так же, как и обычный HTTP-трафик;

4. прокси-сервер устанавливает соединение с сервером, на который должны быть переданы данные, и использует для шифрации канала сертификат сервера;

5. возвращаемые от сервера данные расшифровываются, анализируются и передаются пользователю, зашифрованные сертификатом прокси-сервера.

При использовании данной схемы обработки шифрованных данных могут возникать проблемы, связанные с подтверждением истинности пользователя. Кроме того, требуется выполнение работы по установке сертификата в Интернет-броузеры всех пользователей (если не установить такой сертификат, то у пользователя будет появляться сообщение о том, что сертификат подписан неизвестной компанией, что даст пользователю информацию о наблюдении за передачей данных).

Сейчас на рынке предлагаются следующие продукты для контроля передачи шифрованных данных: Webwasher SSL Scanner компании Secure Computing, Breach View SSL, WebCleaner.

4.4.2 Проверка подлинности сертификатов

Вторая задача, возникающая при использовании шифрованных каналов передачи данных, — проверка подлинности сертификатов, предоставляемых серверами, с которыми работают пользователи.

Злоумышленники могут осуществлять атаку на информационные системы, создавая ложную запись в DNS, перенаправляющую запросы пользователя не на тот сайт, который им необходим, а на созданный самими злоумышленниками. С помощью таких подставных сайтов могут быть украдены важные данные пользователей, такие как номера кредитных карт, пароли и т.п., а также под видом обновлений программного обеспечения может быть загружен вредоносный код.

Для предотвращения подобных случаев и существует специализированное программное обеспечение, выполняющее проверку соответствия сертификатов, предоставленных сервером, тем данным, о которых они сообщают.

В случае несовпадения система может заблокировать доступ к таким сайтам или осуществить доступ после явного подтверждения пользователем. Обработка данных при этом выполняется практически тем же способом, что и при анализе данных, передаваемых по шифрованным каналам, только в этом случае анализируются не данные, а сертификат, предоставляемый сервером.

5 Фильтрация почтового трафика

При использовании электронной почты, организации сталкиваются с необходимостью обеспечения защиты как для входящего, так и для исходящего трафика. Но задачи, решаемые для каждого из направлений, довольно сильно различаются. Для входящего трафика необходимо обеспечить контроль вредоносного кода, фишинга и нежелательной почты (спама), в то время как в исходящей почте контролируется содержимое, передача которого может привести к утечке важной информации, распространению компрометирующих материалов и тому подобных вещей.

Большинство продуктов, существующих на рынке, предоставляют контроль только входящего трафика. Это осуществляется за счет интеграции с антивирусными системами, реализации различных механизмов защиты от нежелательной почты и фишинга. Многие из этих функций уже встраиваются в почтовые клиенты, но полностью решить задачу они не могут.

Для защиты пользователей от спама в настоящее время существует несколько способов:

1. сравнение получаемых сообщений с имеющейся базой сообщений. При сравнении могут применяться различные методики, включая использование генетических алгоритмов, которые позволяют вычленить ключевые слова даже в случае их искажения;

2. динамическая категоризация сообщений по их содержимому. Позволяет очень эффективно определять наличие нежелательной корреспонденции. Для противодействия этому методу распространители спама используют рассылку сообщений в виде изображения с текстом внутри и/или наборы слов из словарей, которые создают шум, мешающий работе данных систем. Однако уже сейчас для

борьбы с таким спамом, начинают использовать различные методы, такие как вейвлет-анализ и/или распознание текста в изображениях;

3. серые, белые и черные списки доступа позволяют описывать политику приема почтовых сообщений с известных или неизвестных сайтов. Применение серых списков во многих случаях помогает предотвратить передачу нежелательных сообщений за счет специфики работы ПО, рассылающего спам. Для ведения черных списков доступа могут использоваться как локальные базы данных, управляемые администратором, так и глобальные, пополняемые на основе сообщений пользователей со всего мира. Однако использование глобальных баз данных чревато тем, что в них могут попасть целые сети, в том числе и содержащие "хорошие"почтовые сервера.

Для борьбы с утечками информации используются самые разные способы, основанные на перехвате и глубоком анализе сообщений в соответствии со сложной политикой фильтрации. В этом случае возникает необходимость корректного определения типов файлов, языков и кодировок текстов, проведения семантического анализа передаваемых сообщений.

Еще одно из применений систем для фильтрации почтового трафика — создание шифрованных потоков почты, когда система автоматически подписывает или шифрует сообщение, а на другом конце соединения производится автоматическая расшифровка данных. Этот функционал очень удобен, если вы хотите обрабатывать всю исходящую почту, но она должна доходить до адресата в зашифрованном виде.

6 Фильтрация мгновенных сообщений

Средства для передачи мгновенных сообщений (Instant messaging) постепенно переходят в разряд активно используемых инструментов во многих компаниях. Они обеспечивают быстрое взаимодействие с сотрудниками и/или клиентами организаций. Поэтому совершенно закономерно, что развитие средств, которые, кроме прочего, могут оказаться и каналом для утечки информации, привело к появлению инструментов для контроля передаваемой информации.

В настоящее время для обмена мгновенными сообщениями наиболее часто используются протоколы MSN (Microsoft Network), AIM (AOL Instant Messaging), Yahoo! Chat, Jabber и их корпоративные аналоги — протоколы Microsoft Live Communication Server (LCS), IBM SameTime и Yahoo Corporate Messaging Server. На территории СНГ широкое распространение получила система ICQ, которая сейчас принадлежит компании AOL и использует практически такой же протокол, что и AIM. Все указанные системы выполняют практически одно и то же — передают сообщения (как через сервер, так и напрямую) и файлы.

Теперь почти у всех систем появились возможности и для звонков с компьютера на компьютер и/или на обычные телефоны, что создает определенные трудности для систем контроля и требует поддержки VoIP для реализации полноценных прокси-серверов.

Обычно продукты для контроля IM-трафика реализуются как прикладной шлюз, выполняющий разбор передаваемых данных и блокирующий передачу запрещенных

данных. Однако есть и реализации в виде специализированных серверов IM, которые осуществляют необходимые проверки на уровне сервера.

Наиболее востребованные функции продуктов для контроля IM-трафика:

1. управление доступом по отдельным протоколам;
2. контроль используемых клиентов и т.п.;
3. контроль доступа отдельных пользователей:
4. разрешение пользователю общения только в пределах компании;
5. разрешение пользователю общения только с определенными пользователями вне компании;
6. контроль передаваемых текстов;
7. контроль передачи файлов. Объектами контроля являются:
   (a) размер файла;
   (b) тип и/или расширение файла;
8. направление передачи данных;
9. контроль наличия вредоносного содержимого;
10. определение SPIM;
11. сохранение передаваемых данных для последующего анализа.

В настоящее время контроль за передачей мгновенных сообщений позволяют выполнять следующие продукты:

1. CipherTrust IronIM компании Secure Computing. Данный продукт имеет поддержку протоколов AIM, MSN, Yahoo! Chat, Microsoft LCS и IBM SameTime. Сейчас это одно из самых полных решений;
2. IM Manager компании Symantec (разработан компанией IMLogic, которая была поглощена Symantec). Этот продукт имеет поддержку следующих протоколов — Microsoft LCS, AIM, MSN, IBM SameTime, ICQ и Yahoo! Chat;
3. Antigen for Instant Messaging компании Microsoft также позволяет работать практически со всеми популярными протоколами для передачи мгновенных сообщений.

Продукты других компаний (ScanSafe, ContentKeeper) обладают меньшими возможностями по сравнению с перечисленными выше.

Стоит отметить, что две российские компании — "Гран При"(продукт "SL-ICQ") и "Мера.ру"(продукт "Сормович") — предоставляют продукты для контроля за передачей сообщений с использованием протокола ICQ.

7 Фильтрация VoIP

Растущая популярность средств для передачи звуковой информации между компьютерами (называемых также Voice over IP (VoIP)) заставляет принимать меры к контролю передачи такой информации. Есть разные реализации для звонков с компьютера на компьютер и/или на обычные телефоны.

Существуют стандартизированные протоколы для обмена такой информацией, сюда можно отнести Session Instantiation Protocol (SIP), принятый IETF и H.323, разработанный ITU. Эти протоколы являются открытыми, что делает возможным их обработку.

Кроме того, существуют протоколы, разработанные конкретными компаниями, которые не имеют открытой документации, что сильно затрудняет работу с ними. Одной из самых популярных реализаций является Skype, завоевавший широкую популярность во всем мире. Эта система позволяет выполнять звонки между компьютерами, делать звонки на стационарные и мобильные телефоны, а также принимать звонки со стационарных и мобильных телефонов. В последних версиях поддерживается возможность обмена видеоинформацией.

Большинство имеющихся на данный момент продуктов можно разделить на две категории:

1. продукты, которые позволяют определить и блокировать VoIP-трафик;
2. продукты, которые могут определить, захватить и проанализировать VoIP-трафик.

К первой категории можно отнести следующие продукты:

1. продукты компании "Dolphian позволяющие определить и разрешить или запретить VoIP-трафик (SIP и Skype), который инкапсулирован в стандартный HTTP-трафик;
2. продукты компании Verso Technologies;
3. разные виды межсетевых экранов, обладающие такой возможностью.

Ко второй категории продуктов относятся:

1. продукт российской компании "Сормович"поддерживает захват, анализ и сохранение голосовой информации, которая передается по протоколам H.323 и SIP;
2. библиотека с открытым кодом Oreka (http://oreka.sourceforge.net/) позволяет определить сигнальную составляющую звукового трафика и выполнить захват передаваемых данных, которые затем можно проанализировать другими средствами.

Недавно стало известно, что разработанный фирмой ERA IT Solutions AG продукт позволяет перехватывать VoIP-трафик, передаваемый при помощи программы Skype. Но для выполнения такого контроля необходимо установить специализированный клиент на компьютер, на котором работает Skype.

8 Фильтрация peer-to-peer

Использование сотрудниками различных peer-to-peer (p2p) сетей несет следующие угрозы для организаций:

1. распространение вредоносного кода;
2. утечка информации;
3. распространение данных, защищенных авторским правом, что может привести к судебному преследованию;
4. снижение производительности труда;
5. повышенная нагрузка на каналы передачи данных.

Существует большое количество сетей, работающих в формате peer-to-peer. Есть сети, имеющие центральные серверы, используемые для координации пользователей, а есть сети полностью децентрализованные. Во втором случае их особенно трудно контролировать с помощью таких стандартных средств как межсетевые экраны.

Для решения данной проблемы многие фирмы создают продукты, позволяющие детектировать и обрабатывать p2p-трафик. Для обработки p2p-трафика существуют следующие решения:

1. SurfControl Instant Messaging Filter, который обрабатывает p2p наравне с обработкой мгновенных сообщений;
2. пакет Websense Enterprise также предоставляет пользователям средства для контроля p2p-трафика;
3. Webwasher Instant Message Filter позволяет контролировать доступ к различным p2p-сетям.

Использование этих или других, не перечисленных здесь, продуктов резко сокращает риски, связанные с доступом пользователей к p2p-сетям.

9 Unified Threat Management

Решения, соответствующие концепции Unified Threat Management, предлагаются многими производителями средств защиты. Как правило, они построены на базе межсетевых экранов, которые кроме основных функций выполняют еще и функции контентной фильтрации данных. Как правило, эти функции сосредоточены на предотвращении вторжений, проникновения вредоносного кода и нежелательных сообщений.

Многие из таких продуктов реализуются в виде аппаратно-программных решений, которые не могут полностью заменить решения для фильтрации почтового и интернет-трафика, поскольку работают лишь с ограниченным числом возможностей, предоставляемых конкретными протоколами. Обычно их используют для того, чтобы

избежать дублирования функций в разных продуктах, и для обеспечения гарантий, что все прикладные протоколы будут обрабатываться в соответствии с одной базой известных угроз.

Наиболее популярными решениями концепции Unified Threat Management являются следующие продукты:

1. SonicWall Gateway Anti-Virus, Anti-Spyware and Intrusion Prevention Service обеспечивает антивирусную и другую защиту данных, передаваемых по протоколам SMTP, POP3, IMAP, HTTP, FTP, NetBIOS, протоколам Instant Messaging и многим потоковым протоколам, применяемым для передачи аудио- и видеоинформации;

2. серия устройств ISS Proventia Network Multi-Function Security, выполненных в виде программно-аппаратных комплексов, обеспечивает блокировку вредоносного кода, нежелательных сообщений и вторжений. В поставку включено большое число проверок (в том числе и для VoIP), которые могут быть расширены пользователем;

3. аппаратная платформа Network Gateway Security компании Secure Computing, кроме защиты от вредоносного кода и нежелательных сообщений, также имеет поддержку VPN. В составе этой платформы объединены практически все решения Secure Computing.

Существуют и другие продукты, но перечисленные выше имеют массовое распространение.

10 Перехват данных

Перехват данных (Lawful interception) практически всегда использовался спецслужбами для сбора и анализа передаваемой информации. Однако в последнее время вопрос перехвата данных (не только Интернет-трафика, но и телефонии, и других видов) стал очень актуальным в свете борьбы с терроризмом. Даже те государства, которые всегда были против таких систем, стали использовать их для контроля за передачей информации.

Поскольку перехватываются различные виды данных, часто передаваемые по высокоскоростным каналам, то для реализации таких систем необходимо специализированное программное обеспечение для захвата и разбора данных и отдельное программное обеспечение для анализа собранных данных. В качестве такового может использоваться ПО для контентной фильтрации того или иного протокола.

Пожалуй, самой известной из таких систем является англо-американская система Echelon, которая долго использовалась для перехвата данных в интересах различных ведомств США и Англии. Кроме того, агенство национальной безопасности США использует систему Narus, которая позволяет выполнять мониторинг и анализ Интернет-трафик в реальном времени.

Среди российских продуктов можно упомянуть решения от компании "Сормович позволяющее захватывать и анализировать почтовый, звуковой, а также разные виды Интернет-трафика (HTTP и другие).

11 Заключение

Развитие информационных систем приводит к возникновению все новых и новых угроз. Поэтому развитие продуктов контентной фильтрации не только не отстает, но иногда даже и предвосхищает возникновение новых угроз, уменьшая риски для защищаемых информационных систем.