МЕЖДУНАРОДНЫЙ СОЮЗ ЭЛЕКТРОСВЯЗИ

МСЭ-Т

СЕКТОР СТАНДАРТИЗАЦИИ
ЭЛЕКТРОСВЯЗИ МСЭ

X.1244

(09/2008)

СЕРИЯ X: СЕТИ ПЕРЕДАЧИ ДАННЫХ,
ВЗАИМОСВЯЗЬ ОТКРЫТЫХ СИСТЕМ
И БЕЗОПАСНОСТЬ

Безопасность электросвязи

Общие аспекты противодействия спаму в мультимедийных IP-приложениях

Рекомендация МСЭ-Т X.1244

РЕКОМЕНДАЦИИ МСЭ-Т СЕРИИ X

СЕТИ ПЕРЕДАЧИ ДАННЫХ, ВЗАИМОСВЯЗЬ ОТКРЫТЫХ СИСТЕМ И БЕЗОПАСНОСТЬ

СЕТИ ПЕРЕДАЧИ ДАННЫХ ОБЩЕГО ПОЛЬЗОВАНИЯ	
Службы и услуги	X.1–X.19
Интерфейсы	X.20–X.49
Передача, сигнализация и коммутация	X.50–X.89
Сетевые аспекты	X.90–X.149
Техническое обслуживание	X.150–X.179
Административные предписания	X.180–X.199
ВЗАИМОСВЯЗЬ ОТКРЫТЫХ СИСТЕМ	
Модель и обозначение	X.200–X.209
Определения служб	X.210–X.219
Спецификации протоколов с установлением соединений	X.220–X.229
Спецификации протоколов без установления соединений	X.230–X.239
Проформы PICS	X.240–X.259
Идентификация протоколов	X.260–X.269
Протоколы обеспечения безопасности	X.270–X.279
Управляемые объекты уровня	X.280–X.289
Испытание на соответствие	X.290–X.299
ВЗАИМОДЕЙСТВИЕ МЕЖДУ СЕТЯМИ	
Общие положения	X.300–X.349
Спутниковые системы передачи данных	X.350–X.369
Сети, основанные на протоколе Интернет	X.370–X.379
СИСТЕМЫ ОБРАБОТКИ СООБЩЕНИЙ	X.400–X.499
СПРАВОЧНИК	X.500–X.599
ОРГАНИЗАЦИЯ СЕТИ ВОС И СИСТЕМНЫЕ АСПЕКТЫ	
Организация сети	X.600–X.629
Эффективность	X.630–X.639
Качество обслуживания	X.640–X.649
Наименование, адресация и регистрация	X.650–X.679
Абстрактно-синтаксическая нотация 1 (ASN.1)	X.680–X.699
УПРАВЛЕНИЕ В ВОС	
Структура и архитектура управления системами	X.700–X.709
Служба и протокол связи для общего управления	X.710–X.719
Структура управляющей информации	X.720–X.729
Функции общего управления и функции ODMA	X.730–X.799
БЕЗОПАСНОСТЬ	X.800–X.849
ПРИЛОЖЕНИЯ ВОС	
Фиксация, параллельность и восстановление	X.850–X.859
Обработка транзакций	X.860–X.879
Удаленные операции	X.880–X.889
Общие приложения ASN.1	X.890–X.899
ОТКРЫТАЯ РАСПРЕДЕЛЕННАЯ ОБРАБОТКА	X.900–X.999
БЕЗОПАСНОСТЬ ЭЛЕКТРОСВЯЗИ	**X.1000–**

Для получения более подробной информации просьба обращаться к перечню Рекомендаций МСЭ-Т.

Рекомендация МСЭ-Т X.1244

Общие аспекты противодействия спаму в мультимедийных IP-приложениях

Резюме

В Рекомендации МСЭ-Т X.1244 определяются базовые понятия, характеристики и технические вопросы, связанные с противодействием спаму в мультимедийных IP-приложениях, таких как IP-телефония, мгновенная передача сообщений и т. д. Классифицированы различные типы спама мультимедийных IP-приложений, и каждая группа этой классификации описана в соответствии с ее характеристиками. В данной Рекомендации описаны различные угрозы безопасности, которые может создавать спам в мультимедийных IP-приложениях. Разработаны различные технологии управления спамом в электронной почте, который уже стал социальной проблемой. Некоторые из этих методов могут использоваться для противодействия спаму в мультимедийных IP-приложениях. В данной Рекомендации проанализированы механизмы борьбы с обычным спамом и рассматривается их применимость для противодействия спаму в мультимедийных IP-приложениях. В данной Рекомендации путем упоминания различных аспектов сделан вывод о том, что следует считать спамом в мультимедийных IP-приложениях.

Источник

Рекомендация МСЭ-Т X.1244 одобрена 19 сентября 2008 года 17-й Исследовательской комиссией МСЭ-Т (2005–2008 гг.) в соответствии с процедурой, описанной в Резолюции 1 ВАСЭ.

Ключевые слова

Спам в мгновенных сообщениях, спам в мультимедийных IP-приложениях, спам, спам при передаче голоса по IP.

ПРЕДИСЛОВИЕ

Международный союз электросвязи (МСЭ) является специализированным учреждением Организации Объединенных Наций в области электросвязи. Сектор стандартизации электросвязи МСЭ (МСЭ-Т) – постоянный орган МСЭ. МСЭ-Т отвечает за изучение технических, эксплуатационных и тарифных вопросов и за выпуск Рекомендаций по ним с целью стандартизации электросвязи на всемирной основе.

На Всемирной ассамблее по стандартизации электросвязи (ВАСЭ), которая проводится каждые четыре года, определяются темы для изучения Исследовательскими комиссиями МСЭ-Т, которые, в свою очередь, вырабатывают Рекомендации по этим темам.

Утверждение Рекомендаций МСЭ-Т осуществляется в соответствии с процедурой, изложенной в Резолюции 1 ВАСЭ.

В некоторых областях информационных технологий, которые входят в компетенцию МСЭ-Т, необходимые стандарты разрабатываются на основе сотрудничества с ИСО и МЭК.

ПРИМЕЧАНИЕ

В настоящей Рекомендации термин "администрация" используется для краткости и обозначает как администрацию электросвязи, так и признанную эксплуатационную организацию.

Соблюдение положений данной Рекомендации носит добровольный характер. Однако в Рекомендации могут содержаться определенные обязательные положения (например, для обеспечения возможности взаимодействия или применимости), и соблюдение положений данной Рекомендации достигается в случае выполнения всех этих обязательных положений. Для выражения необходимости выполнения требований используется синтаксис долженствования и соответствующие слова (такие, как "должен" и т. п.), а также их отрицательные эквиваленты. Использование этих слов не предполагает, что соблюдение положений данной Рекомендации является обязательным для какой-либо из сторон.

ПРАВА ИНТЕЛЛЕКТУАЛЬНОЙ СОБСТВЕННОСТИ

МСЭ обращает внимание на вероятность того, что практическое применение или реализация этой Рекомендации может включать использование заявленного права интеллектуальной собственности. МСЭ не занимает какую бы то ни было позицию относительно подтверждения, обоснованности или применимости заявленных прав интеллектуальной собственности, независимо от того, отстаиваются ли они членами МСЭ или другими сторонами вне процесса подготовки Рекомендации.

На момент утверждения настоящей Рекомендации МСЭ не получил извещение об интеллектуальной собственности, защищенной патентами, которые могут потребоваться для выполнения этой Рекомендации. Однако те, кто будет применять Рекомендацию, должны иметь в виду, что это может не отражать самую последнюю информацию, и поэтому им настоятельно рекомендуется обращаться к патентной базе данных БСЭ по адресу: http://www.itu.int/ITU-T/ipr/.

© ITU 2009

Все права сохранены. Ни одна из частей данной публикации не может быть воспроизведена с помощью каких бы то ни было средств без предварительного письменного разрешения МСЭ.

СОДЕРЖАНИЕ

		Стр.
1	Сфера применения	1
2	Справочные документы	1
3	Определения	1
	3.1 Термины, определенные в других документах	1
	3.2 Термины, определенные в данной Рекомендации	2
4	Сокращения и акронимы	3
5	Условные обозначения	4
6	Принципы и типовые виды мультимедийного IP-спама	4
	6.1 Спам в услугах VoIP	4
	6.2 Спам в мультимедийных IP-сообщениях	5
	6.3 Спам в мгновенных сообщениях	5
	6.4 Спам в чате	5
	6.5 Мультимодальный спам	6
	6.6 Распространение спама в службе обмена файлами на базе одноранговых (P2P) сетей	6
	6.7 Спам на веб-сайте	6
7	Классификация мультимедийного IP-спама	6
	7.1 Голосовой спам в режиме реального времени	7
	7.2 Текстовый спам в режиме реального времени	8
	7.3 Видеоспам в режиме реального времени	8
	7.4 Голосовой спам не в режиме реального времени	8
	7.5 Текстовый спам не в режиме реального времени	9
	7.6 Видеоспам не в режиме реального времени	9
8	Технические проблемы противодействия мультимедийному IP-спаму	9
	8.1 Создание и доставка спама	10
	8.2 Обнаружение и фильтрация спама	11
	8.3 Действия, когда спам уже получен	12
9	Угрозы безопасности, связанные со спамом	12
	9.1 Угрозы безопасности, связанные со спамом	12
	9.2 Классификация угроз безопасности, обусловленных спамом	14
	9.3 Меры противодействия	14
10	Применимость хорошо известных механизмов противодействия спаму в мультимедийных IP-приложениях	15
	10.1 Фильтрация по идентификации	16
	10.2 Маскировка адреса	18
	10.3 Доказательство взаимодействия с человеком	19
	10.4 Фильтрация по содержанию	19
	10.5 Аутентификация посредством обмена ключами	19

10.6 Фильтрация спама на основании сетевых связей 20
10.7 Онлайновая марка 21
10.8 Фильтрация спама на основе авторизации 21
10.9 Юридические действия и правила 22
11 Аспекты противодействия спаму в мультимедийных IP-приложениях 23
11.1 Пользователь услуги (абонент услуги) 23
11.2 Поставщик услуг 23
11.3 Оператор сети 24
11.4 Общественная организация 25
11.5 Другие аспекты 25
Библиография 26

Введение

Спам является социальной проблемой в сетевой системе электронной почты. Разработаны и внедрены различные варианты решения этой проблемы, но ни одно из них не решает этой проблемы. Мультимедийное IP-приложение состоит из различных видов услуг, таких как IP-телефония, мгновенная передача сообщений и т. д. Эти мультимедийные IP-услуги становятся новой целью для спаммеров, поскольку они являются технически более простой и экономически более дешевой средой для рассылки спама. Проблемы со спамом в мультимедийных IP-приложениях должны быть решены до того, как спам станет общественной проблемой.

В данной Рекомендации описываются принципы и характеристики различных видов спама, который может появляться в мультимедийных IP-приложениях. В ней с технической точки зрения и с точки зрения безопасности рассматриваются некоторые вопросы противодействия спаму в мультимедийных IP-приложениях, и, таким образом, она предоставляет некоторые аспекты, требующие учета со стороны некоторых участников процесса предоставления мультимедийных IP-услуг, таких как поставщики услуг, пользователи услуг и т. д. в процессе противодействия спаму в мультимедийных IP-приложениях.

Рекомендация МСЭ-Т X.1244

Общие аспекты противодействия спаму в мультимедийных IP-приложениях

1 Сфера применения

В данной Рекомендации дается обзор спама в мультимедийных IP-приложениях, причем особое внимание уделено следующим вопросам:

– принципы и характеристики мультимедийного IP-спама;

– технические вопросы, связанные с мультимедийным IP-спамом;

– угрозы безопасности, связанные со спамом;

– методы противодействия спаму и их применимость для противодействия мультимедийному IP-спаму;

– различные аспекты, которые должны быть рассмотрены в отношении противодействия спаму в мультимедийных IP-приложениях.

ПРИМЕЧАНИЕ. − Термин "идентичность" в данной Рекомендации употребляется не в своем основном значении. В частности, он не выражает никакой положительной достоверности.

2 Справочные документы

Нет.

3 Определения

3.1 Термины, определенные в других документах

В настоящей Рекомендации используются следующие термины, определенные в других документах:

3.1.1 список контроля доступа (access control list (ACL)) [b-ITU-T X.741]: Атрибут список контроля доступа используется для хранения идентичностей инициаторов, которым либо специально предоставлен доступ к информации управления, либо которым специально отказано в доступе к информации управления.

3.1.2 орган сертификации (certification authority) (CA) [b-ITU-T X.509]: Орган, которому один или несколько пользователей доверили создание и присвоение сертификатов открытых ключей. Дополнительно орган по сертификации может создавать ключи пользователя.

3.1.3 конференция (conference) [b-ITU-T T.124]: Множество узлов, которые объединены вместе и которые способны обмениваться аудиографической и аудиовизуальной информацией посредством различных сетей электросвязи.

3.1.4 почта с идентифицированными ключами домена (Domain Keys identified mail (DKIM)) [b-IETF RFC 4871]: Механизм, посредством которого подписываются сообщения электронной почты, позволяющий подписывающему домену брать на себя ответственность за введение сообщения в почтовый поток. Получатели сообщения могут проверить подпись, непосредственно запросив домен подписавшего для получения соответствующего открытого ключа, и, тем самым, подтвердив, что сообщение проверено стороной, владеющей секретным ключом для подписывающего домена.

3.1.5 мгновенная передача сообщений (instant messaging (IM)) [b-IETF RFC 3428]: Обмен содержанием между несколькими участниками в режиме времени, близком к реальному. Как правило, содержанием являются короткие текстовые сообщения, хотя это и не обязательно.

3.1.6 одноранговые взаимоотношения (peer-to-peer (P2P) relationship) [b-ITU-T T.180]: В одноранговых взаимоотношениях пользователи могут договориться о характеристиках своего взаимодействия и, после этого, общаться, подчиняясь правилам, которые были согласованы обоими пользователями. Объект и равноправный с ним объект имеют потенциально равные права. В документе [b-IETF RFC 4981] указано, что сети P2P – это такие сети, которым присущи три характеристики: самоорганизация, симметричное общение и распределенное управление.

3.1.7 довольно хорошая секретность (pretty good privacy (PGP)) [b-IETF RFC 1991]: PGP использует комбинацию открытого ключа и обычного шифрования для предоставления услуг безопасности сообщений электронной почты и файлов данных. Эти услуги включают в себя конфиденциальность и цифровую подпись. PGP создан Филиппом Циммерманом и впервые выпущен в виде Версии 1.0 в 1991 году. Последующие версии, например open PGP, которые описаны в

документе [b-IETF RFC 4880], разработаны и реализованы в результате полностью добровольных совместных усилий под общим руководством Филиппа Циммермана. *"PGP" и "Pretty Good Privacy" – торговые марки Филиппа Циммермана*.

3.1.8 инфраструктура открытых ключей (public key infrastructure (PKI)) [b-ITU-T X.509]: Инфраструктура, способная поддерживать управление открытыми ключами для поддержки услуг аутентификации, шифрования, целостности или сохранности информации.

3.1.9 безопасность транспортного уровня (transport layer security (TLS)) [b-ITU-T Q.814]: Протокол TLS обеспечивает дополнительную секретность связи. Этот протокол позволяет приложениям клиент/сервер связываться таким способом, который разработан для предотвращения подслушивания, мошенничества и вмешательства. Протокол TLS также обеспечивает сильную равноправную аутентификацию и целостность потока данных.

3.2 Термины, определенные в данной Рекомендации

В настоящей Рекомендации определяются следующие термины:

3.2.1 спам-ловушка (bait spam): Это название получено в результате игры слов по аналогии с рыбалкой (фишинг 0 – см. п. 3.2.10), спам-ловушка – это вид спама, в котором имеется элемент, например адресат электронной почты или встроенная ссылка, который "ловит" пользователей. Спам-ловушка атакует пользователя, попавшего в нее.

3.2.2 блог (blog): Сокращение от слова "web-log", блог – это онлайновый, возможно мультимедийный, перечень интересов владельца, который доступен для широкой общественности, которая может его просматривать, и иногда дополнять.

3.2.3 бот (bot): Бот – это сокращение от "робот", он представляет собой программу, которая работает, как агент для пользователя или другой программы для моделирования деятельности человека.

3.2.4 искажение кэш-памяти DNS (DNS cache poisoning): Искажение кэш-памяти DNS это метод, который хитростью заставляет сервер доменных имен (сервер DNS) поверить в то, что DNS адрес определенного сервера изменился, хотя на самом деле этого не произошло. После того, как сервер DNS обманут, эта информация, как правило, хранится в кэш-памяти в течение некоторого периода времени, распространяя действие атаки на пользователей сервера.

3.2.5 мультимедийное IP-сообщение (IP multimedia message): Текстовое, голосовое или видеосообщение, которое доставляется и хранится в мультимедийном IP-терминале или сервере, для того чтобы его впоследствии проверил получатель. Оно аналогично голосовой почте в телефонии, но предоставляется в составе мультимедийной IP-услуги.

3.2.6 мультимедийный IP-спам (IP multimedia spam): Не запрашиваемые сообщения или вызовы в мультимедийных IP-приложениях. В отличие от традиционного спама в электронной почте, мультимедийный IP-спам обозначает спам, передаваемый с помощью новейших методов электросвязи по сетям IP, таких как мгновенная передача сообщений (IM), присутствие, или голосовая связь по IP-каналу (VoIP).

3.2.7 модальность (modality): В общем смысле этот термин обозначает коды, протоколы или условия, которые окружают официальную связь. В контексте данной Рекомендации она означает код(ы) информации, содержащий(е) информацию, воспринимаемую человеком. Примерами модальности являются текстовые, графические, звуковые или осязательные данные, используемые в интерфейсах человек-компьютер. Мультимодальная информация может создаваться или быть предназначенной для мультимодальных устройств. Примерами интерфейсов человек-компьютер являются микрофоны для голосового (звукового) входного сигнала, ручки для тактильного входного сигнала, клавиатуры для текстового входного сигнала, мышки для двигательного входного сигнала, громкоговорители для выходного сигнала в виде синтезированного голоса, экраны для графического, текстового выходного сигнала, вибрирующие устройства для тактильного выходного сигнала, или устройства Брейля, предназначенное для чтения и письма для людей с дефектами зрения.

3.2.8 мультимодальное сообщение (multimodal message): Это мультимедийное сообщение, которое содержит различным образом кодированную информацию для взаимодействия посредством множества модальностей. Например, MMS (услуга передачи мультимедийных сообщений) сообщение может содержать текстовую, графическую и звуковую модальность. Веб-страница также может содержать мультимедийный модальный контент, например текст или видео. Аналогично электронная почта может содержать вместе с текстом графическое приложение. Мультимодальность,

дает пользователю возможность выбрать предпочтительную модальность в зависимости от условий, удобства и содержания.

3.2.9 онлайновая игра (online game): Игра в реальном времени, в которую играют по сетям.

3.2.10 фишинг (phishing): Попытка преступным или мошенническим путем завладеть важной информацией, например именем пользователя, паролем и данными финансового счета путем маскировки под заслуживающий доверия объект в электронной связи.

3.2.11 перехват сеанса связи (session hijacking): Механизм кражи правильного сеанса связи пользователя с целью получения доступа к информации или услугам.

3.2.12 распространение спама при мгновенной передаче сообщений (spam over instant messaging (SPIM)): Спам, нацеленный на пользователей услуги мгновенной передачи сообщений.

3.2.13 распространение спама в интернет-телефонии (spam over internet telephony (SPIT)): Спам, нацеленный на пользователей услуг интернет-телефонии.

3.2.14 спаммер (spammer): Отправитель спама.

3.2.15 спамминг (spamming): Последовательность действий, выполняемых спаммером для рассылки спама. Например, сбор списков целевой рассылки, создание спама, доставка спама и т. д.

3.2.16 спиммер (spimmer): Отправитель спама при мгновенной передаче сообщений (SPIM).

3.2.17 спиттер (spitter): Отправитель спама в интернет-телефонии (SPIT).

3.2.18 контент, создаваемый пользователем (user created contents (UCC)): UCC – это любая форма контента, например видео, блог, изображения, звуки и т. д., которая создается оконечными пользователями (населением), и которая доступна для широкой публики.

3.2.19 контент, генерируемый пользователем (user generated contents (UGC)): То же, что UCC.

3.2.20 вишинг (vishing): Незаконные действия с целью получения доступа к секретной персональной и финансовой информации при помощи услуги голосовая связь по IP-каналу (VoIP). Термин вишинг представляет собой комбинацию слов "voice" (голос) и "phishing" (финшинг).

4 Сокращения и акронимы

В настоящей Рекомендации используются следующие сокращения и акронимы:

ACL	Access Control List	Список контроля доступа
APEC	Asia-Pacific Economic Cooperation	Азиатско-тихоокеанское экономическое сотрудничество
ARP	Address Resolution Protocol	Протокол распознавания адреса
ASCII	American Standard Code for Information Interchange	Американский стандартный код обмена информацией
CA	Certification Authority	Орган по сертификации
DB	Database	База данных
DKIM	DomainKeys Identified Mail	Почта с идентифицированными ключами домена
HTTP	HyperText Transfer Protocol	Протокол передачи гипертекста
IM	Instant Messaging	Мгновенная передача сообщений
IP	Internet Protocol	Протокол Интернет
IPTV	Internet Protocol Television	Телевидение по протоколу Интернет
IPv4	Internet Protocol version 4	Протокол Интернет версия 4
IPv6	Internet Protocol version 6	Протокол Интернет версия 6
IRC	Internet Relay Chat	Трансляция чатов в интернет
ISP	Internet Service Provider	Поставщик услуг интернета
ITSP	Internet Telephony	Поставщик услуг интернет-телефонии
IVR	Interactive Voice Response	Интерактивный голосовой ответ
MAC	Media Access Control	Контроль доступа к среде передачи данных
MIPv4	Mobile IPv4	Мобильный протокол Интернет версия 4

MIPv6	Mobile IPv6		Мобильный протокол Интернет версия 6
NDP	Neighbour Discovery Protocol		Протокол обнаружения соседа
OS	Operating System		Операционная система
P2P	Peer-to-Peer		Одноранговый
PGP	Pretty Good Privacy		Довольно хорошая секретность
PKI	Public Key Infrastructure		Инфраструктура открытых ключей
PSTN	Public Switched Telephone Network	КТСОП	Коммутируемая телефонная сеть общего пользования
RTP	Real-time Transport Protocol		Протокол транспортирования реального времени
SMS	Short Message Service		Служба коротких сообщений
SMTP	Simple Mail Transfer Protocol		Упрощенный протокол передачи сообщений электронной почты
SQL	Structured Query Language		Язык структурированных запросов
TCP	Transmission Control Protocol		Протокол управления передачей
TLS	Transport Layer Security		Безопасность на транспортном уровне
URI	Uniform Resource Identifier		Унифицированный идентификатор ресурса
URL	Uniform Resource Locator		Унифицированный указатель ресурсов
VoD	Video on Demand		Видео по запросу
VoIP	Voice over IP		Голосовая связь по IP-каналу

5 Условные обозначения

Нет.

6 Принципы и типовые виды мультимедийного IP-спама

Несмотря на то, что не существует согласованного на глобальном уровне определения спама, этот термин широко используется для описания незапрашиваемых объемов электронной корреспонденции, передаваемых по электронной почте или в подвижных службах передачи сообщений с целью рекламы коммерческих продуктов или услуг. В настоящее время спам не ограничен электронной почтой или подвижными службами передачи сообщений. Он распространяется на мультимедийные IP-приложения, такие как VoIP и мгновенная передача сообщений. Мультимедийный IP-спам можно определить, как незапрашиваемые большие объемы электронной корреспонденции, передаваемые посредством мультимедийных IP-приложений с целью рекламы коммерческих продуктов или услуг. Спам в мультимедийных IP-приложениях может возникать в различных видах мультимедийных IP-приложений, таких как VoIP и мгновенная передача сообщений.

В данном разделе перечислены некоторые типовые виды мультимедийного IP-спама, который может появиться в мультимедийных IP-приложениях. Для каждого вида спама приведено описание его характеристик.

6.1 Спам в услугах VoIP

Спам в услугах VoIP – это спам, возникающий в услугах VoIP. Спам в услугах VoIP – это голосовой спам в реальном времени, например телемаркетинг, который предусматривает общение с оператором службы телемаркетинга и взаимодействие с системами IVR (интерактивного голосового ответа). Поскольку с быстрым внедрением услуг VoIP по всему миру службы телемаркетинга с использованием услуг VoIP быстро расширяются, угроза спама VoIP также увеличивается. В частности, создавать большое число вызовов несложно. В качестве операторов службы телемаркетинга можно использовать рабочую силу в других странах, стоимость которой ниже, чем в стране, на которую спам нацелен, поскольку при использовании услуг VoIP стоимость международных звонков значительно снижается. Спаммеру намного проще собирать информацию о целевых пользователях мультимедийных IP-приложений. Имея такие сильные стороны, спам в услугах VoIP может стать реальной угрозой для поставщиков и пользователей услуг VoIP.

6.2 Спам в мультимедийных IP-сообщениях

Мультимедийное IP-сообщение это текстовое, голосовое или видеосообщение, которое доставляется и хранится в мультимедийных IP-терминалах или серверах, для того чтобы его впоследствии проверил получатель. Оно аналогично голосовой почте в телефонии, но предоставляется в составе мультимедийной IP-услуги. Спам в мультимедийных IP-сообщениях – это спам, который использует услугу передачи мультимедийных IP-сообщений. Получатель спама проверяет сообщение и удаляет спам, как спам в электронной почте или в сообщениях на мобильном телефоне. Многие терминалы мультимедийных IP-приложений, например телефоны VoIP, поддерживают функции передачи мультимедийных сообщений, и, следовательно, являются хорошей мишенью для спаммера, рассылающего спам в мультимедийных IP-сообщениях.

Спам в мультимедийных IP-сообщениях можно разделить на спам в текстовых сообщениях и спам в голосовых/видео сообщениях. Спам в виде текстового сообщения – это короткое сообщение, содержащее рекламу или приглашающий текст. Его характеристики аналогичны характеристикам спама в электронной почте или SMS-спама в службах подвижной связи, поскольку он имеет текстовую форму. Однако, как ожидается, стоимость рассылки спама в виде текстовых сообщений будет намного ниже, чем спам в SMS подвижной связи. Спам в виде голосового/видеосообщения – это сообщение в форме голосового/видеофайла, содержащее рекламу или приглашения. Ожидается, что при использовании мультимедийных IP-приложений этот тип спама будет широко распространен. Можно ожидать, что голосовые/видеосообщения будут занимать большую часть почтового ящика для голосовых/видеофайлов пользователей IP-приложений или памяти хранилища данных поставщика IP-услуг, поскольку размер мультимедийного сообщения очень велик по сравнению со спамом в виде текстового сообщения. Спам в виде мультимедийных сообщений может использоваться злонамеренными спаммерами для доставки вредоносного программного обеспечения, например червей, компьютерных вирусов, программ-шпионов, троянских коней и т. п.

6.3 Спам в мгновенных сообщениях

Спам, распространяемый посредством услуги мгновенной передачи сообщений, а именно SPIM, это еще один вид передачи спама в мультимедийных IP-приложениях, который нацелен на пользователей услуги мгновенной передачи сообщений. Многие пользователи используют услугу IM для удобного общения с другими пользователями сетей. Большая часть спама IM – это короткие текстовые сообщения, которые имеют много общего со спамом в электронной почте, но спам IM – это сообщение, передаваемое в реальном времени, что может быть более раздражающим. Спам в виде мультимедийных сообщений может возникать в IM, поскольку служба IM поддерживает множество функций, дополняющих доставку текстовых сообщений в реальном времени.

Рассылка спама IM не может быть простой и не может быть выполнена без незаконных технических манипуляций, поскольку для большинства услуг IM принимаются согласованные списки контактов, содержащий только тех пользователей, которым разрешено передавать сообщения. Однако слабая система безопасности IM-услуг может дать спаммерам возможность украсть у целевого получателя список контактов или белый список для передачи сообщений спама, выдавая себя за члена списка контактов.

Хотя доставка сообщения допускается только между пользователями, включенными в списки контактов, любой может запросить разрешения присоединиться к списку контактов. Во многих IM-услугах, сообщения запроса на разрешение присоединиться к списку контактов могут содержать несколько предложений, которые представляют запрашивающего пользователя, которые должны помочь пользователю услуги IM узнать, кто просит разрешения, и определить, разрешить ли ему присоединиться к списку контактов. Спаммер, не включенный в список контактов, может передавать спам-сообщения, используя эту функцию IM-услуги.

6.4 Спам в чате

Спам в чате может возникать в различных видах мультимедийных IP-приложений, которые предоставляют пользователям функцию переписки в онлайновом режиме (чат). Функции переписки в онлайновом режиме и функция передачи сообщений предоставляются во многих мультимедийных IP-приложениях, например в услугах онлайновой переписки, услугах онлайновых игр и т. п. Спам в чате, как правило, имеет формат короткого текстового сообщения, содержащего одно и то же сообщение, которое многократно рассылается всем участникам переписки. Поэтому некоторые услуги онлайновой переписки и услуги онлайновых игр ограничивают количество повторной доставки одного и того же сообщения, для того чтобы противостоять доставке сообщений, являющихся спамом. Однако действенность этого метода ограничена и необходимы дополнительные контрмеры для противодействия различным видам спама в чате.

Услуги онлайновой переписки имеют те же характеристики, что и услуга IM, но типы спама, которые могут появляться в этих услугах, различны. Пользователь услуг IM обычно общается с корреспондентами из списка контактов, которым этот пользователь IM разрешает передавать сообщения. Таким образом, для того чтобы передать спам, спаммер должен проникнуть в список контактов. Услуга онлайновой переписки предоставляется в виде онлайновой услуги, в которой участники общения, обычно, неизвестны. Кто угодно может участвовать в онлайновой переписке, следовательно, спаммеры могут присоединиться к переписке с целью рассылки спама. Тип спама, который можно встретить в онлайновой переписке, многократно передает одно и то же сообщение. Таким образом, рассылать спам в услуге онлайновой переписки намного проще, чем в услуге IM.

6.5 Мультимодальный спам

Проблема безопасности, обусловленная "спаммингом" распространяется и на ситуацию с мультимодальным взаимодействием, в котором отдельное мультимедийное "спамовое" сообщение может достигать множества целей на интерфейсе пользователя, которые меняются с изменением модальности. "Спамовое" сетевое сообщение может привести к звучанию "спамового" звукового клипа, воспроизведению "спамового" видеоклипа или показу на экране "спамового" текстового сообщения; все они могут иметь либо одно и то же, либо даже разное содержание. Следовательно, мультимодальность увеличивает незащищенность от мультимедийного "спама", и, значит, когда мультимодальные взаимодействия станут более распространенными, можно ожидать, что проблема мультимодального "спама" увеличится.

6.6 Распространение спама в службе обмена файлами на базе одноранговых (P2P) сетей

Спам в мультимедийных IP-приложениях также может появляться в мультимедийных IP-приложениях на базе одноранговых (P2P) сетей, имея своей целью пользователей услуги на базе одноранговых (P2P) сетей, например службы обмена файлами в одноранговых сетях. Люди, которые соединяются с IP-сетью, используя программное обеспечение P2P, помогают пользователям использовать одноранговую связь для обмена компьютерными файлами различного вида. В таких службах спаммер может хитростью убедить других пользователей загрузить файлы со спамом под именем популярного кинофильма, популярной песни и т. п. Спаммерам не требуется искать целевую аудиторию. Им требуется только поделиться файлами со спамом и заставить других пользователей обратиться к ним. Ожидается, что многие загруженные файлы будут выполнены, поскольку получатели спама загружают их добровольно. Поэтому ущерб от спама в службе P2P может быть очень велик, если спам вместо рекламы содержит вредоносное программное обеспечение, такое как черви и вирусы.

6.7 Спам на веб-сайте

Спаммеры могут рассылать статьи или файлы, содержащие рекламный контент на множество веб-сайтов, движимые разного рода целями. Спам, который рассылается на доски объявлений, могут видеть многие посетители веб-сайта. Например, спамом на веб-сайте могут быть комментарии статей на веб-порталах с рекламным содержанием и рекламные статьи в блогах. Кроме текстовых статей спаммеры могут загружать рекламные звуковые и видеофайлы на сайтах обмена видео/аудиоматериалами, таких как UCC и UCG, или на досках объявлений, чтобы заставить других пользователей посмотреть рекламные видеофайлы. Спам на веб-сайте может быть прочитан или просмотрен огромным количеством пользователей услуг данного веб-сайта. Для того чтобы спам такого типа достиг своего назначения, спаммерам не требуется собирать целевую аудиторию для рассылки большого объема спама.

7 Классификация мультимедийного IP-спама

Спам в мультимедийных IP-приложениях подразделяется на две группы в соответствии с его возможностями. Спам в мультимедийных IP-приложениях можно разделить в соответствии с различными критериями, например по типу мультимедийных IP-приложений, в которых появляется спам, по типам среды передачи, используемой для передачи спама, по виду протокола, используемого для предоставления услуги, по типу протокольного сообщения и т. п. В данном разделе мультимедийный IP-спам подразделяется в соответствии со следующими характеристиками мультимедийных IP-приложений, с учетом того, что в соответствии с этими характеристиками могут применяться анти-спамовые методы.

– Мультимедийный IP-спам в режиме реального времени и не в режиме реального времени. Услуги мультимедийных IP-приложений могут быть подразделены по критерию использования режима реального времени для их предоставления.

– Тип среды передачи мультимедийного IP-спама. Услуга мультимедийного IP-приложения может поддерживать текст, голос, видео или их комбинацию. В категорию видео входит как неподвижные, так и подвижные изображения.

В услугах мультимедийных IP-приложений реального времени соединение устанавливается, сообщение доставляется, и получатель проверяет сообщение в режиме реального времени. Типичными примерами мультимедийных IP-приложений реального времени являются услуга VoIP и услуга IM. В услугах мультимедийных IP-приложений не реального времени, получатель может проверить сообщение, когда он или она захочет. Примерами мультимедийных IP-приложений не реального времени являются веб-услуги, услуга P2P, услуги онлайновых игр и т. п. Классификация спама в мультимедийных IP-приложениях и типичные примеры приведены в таблице 7-1.

Таблица 7-1 – Классификация спама в мультимедийных IP-приложениях

	Текстовый	**Голосовой**	**Видео**
В режиме реального времени	• Спам в мгновенных сообщениях • Спам в чате	• Спам в услугах VoIP • Спам в мгновенных сообщениях	• Спам в мгновенных сообщениях
Не в режиме реального времени	• Текст/спам в виде мультимедийных сообщений • Текстовый спам, распространяемый в службе однорангового (P2P) обмена файлами • Текстовый спам на веб-сайте	• Голос/спам в виде мультимедийных сообщений • Голосовой спам, распространяемый в службе однорангового (P2P) обмена файлами • Голосовой спам на веб-сайте	• Видео/спам в виде мультимедийных сообщений • Видеоспам, распространяемый в службе однорангового (P2P) обмена файлами • Видеоспам на веб-сайте

7.1 Голосовой спам в режиме реального времени

Голосовой спам в режиме реального времени можно определить как незапрашиваемое голосовое общение в режиме реального времени с целью рекламы коммерческих продуктов или услуг. Типичным примером голосового спама в режиме реального времени является спам в услугах VoIP. Голосовой спам в режиме реального времени может встречаться менее часто, чем спам в электронной почте, но, считается, что ущерб от такого спама для пользователя услуг намного больше. Голосовой спам в режиме реального времени чрезвычайно раздражает получателей спама. В услугах электронной почты пользователи могут проверять почту по своему желанию, могут быстро идентифицировать спам в электронной почте и могут удалить его, не затрачивая больших усилий. Но голосовой спам в режиме реального времени более навязчив, поскольку он требует от получателя спама немедленного ответа. Более того, для того чтобы понять, что принятое сообщение представляет собой голосовой спам, требуется больше времени. Голосовой спам в режиме реального времени более эффективен, чем спам в электронной почте и спам в мобильных SMS-сообщениях. Как правило, спаммеры пытаются убедить получателя спама купить конкретный продукт или услугу. Операторы службы телемаркетинга, используя голосовой спам в режиме реального времени, стараются убедить получателя спама в ходе интерактивного общения, что более убедительно, чем спама в электронной почте или SMS, с помощью которых можно лишь доставить короткие текстовые или видеосообщения в не интерактивном формате. Поскольку убедительность спама растет, ущерб от спама, в общем случае, тоже увеличивается. Поэтому, ущерб от голосового спама в режиме реального времени может быть относительно велик, учитывая количество спама.

Голосовой спам в режиме реального времени может пытаться повысить эффективность спама, используя различные дополнительные IP-услуги в дополнение к базовому голосовому общению. Голосовой спам в режиме реального времени, как правило, доставляется получателю спама через терминалы, которые поддерживают услугу VoIP. Многие терминалы такого вида могут поддерживать множество дополнительных функций, например передачу мультимедийных сообщений, видеотелефонию и, как функции по умолчанию, отображение на экране дополнительной информации во время голосовой связи. Спаммеры могут пытаться повысить эффективность спама, комбинируя голосовой спам в режиме реального времени с дополнительными услугами передачи видео или текста.

Голосовой спам в режиме реального времени может быть незаконным или мошенническим спамом, который является злонамеренным, каковой встречается также в традиционных службах проводной или подвижной телефонии. Более того, невысокая стоимость услуг VoIP может сделать незаконный

спам в услугах VoIP более активным, чем в традиционных телефонных услугах. Например, злонамеренные спаммеры могут стараться получить финансовую информацию, доставляя фишинговые сообщения VoIP, называемые "вишингом", на незаконно полученные адреса пользователей услуги. Злонамеренные спаммеры могу передавать спам-ловушку, заставляя получателей спама пользоваться более дорогими услугами, чего сами пользователи делать не собирались. Например, спаммеры могут использовать "программу автоматического одноразового звонка". Эта программа формирует соединение с получателем спама и завершает вызов после одного или двух звонков или быстро разъединяет соединение, произнеся только одно короткое слово типа "Привет". Многие получатели будут стремиться перезвонить, используя информацию об ID вызывающего абонента. Получатель спама соединяется с автоответчиком, на который записана рекламная информация, или с какой-нибудь очень дорогостоящей услугой. Этот вид спама более привлекателен для спаммера, поскольку стоимость рассылки спама очень мала. Спам ловушка может доставляться злонамеренными спаммерами, которые используют в своих целях уязвимость системы безопасности услуги VoIP. Например, спаммеры могут маскировать себя, используя перехваченный сеанс связи VoIP. Спаммеры могут заставить пользователя услуги VoIP соединиться со спаммером, который выдает себя за другого пользователя, когда первый пользователь хочет соединиться с другими пользователями услуги, аналогично в мультимедийных IP-приложениях могут появляться различные виды спама ловушек, заманивающих получателей спама.

7.2 Текстовый спам в режиме реального времени

Текстовый спам в режиме реального времени может быть определен как незапрашиваемое значительное по объему текстовое сообщение, переданное в режиме реального времени, например, с целью рекламы коммерческих продуктов или услуг. Текстовый спам в режиме реального времени может появляться во многих мультимедийных IP-приложениях, которых доставляют текстовые сообщения между пользователями услуги в режиме реального времени. Характеристики текстового спама в режиме реального времени аналогичны характеристикам спама в электронной почте, поскольку этот спам основан на тексте. Однако текстовый спам в режиме реального времени является более раздражающим, чем спам в электронной почте, поскольку в момент доставки спама получатель спама вынужден прерваться и обратить на него внимание. Примерами текстового спама в режиме реального времени являются спам IM и спам в чате.

Во многих услугах мультимедийных IP-приложений, включая услугу IM, услугу онлайнового чата, и онлайновых игр, возможность использовать функцию доставки сообщений предоставляется пользователям бесплатно или по очень невысокой цене. Поэтому спаммеры могут очень дешево передавать спам в виде текстового сообщения. Спаммеры, зачастую, могут при помощи различных методов получить общую или специальную информацию о пользователях услуги. Эта информация может повысить ожидаемый доход от спама для спаммеров по сравнению со спамом в электронной почте, который не направлен на конкретных людей.

7.3 Видеоспам в режиме реального времени

Видеоспам в режиме реального времени можно определить как незапрашиваемое визуальное общение с целью рекламы коммерческих продуктов или услуг. Видео включает себя как неподвижные, так и подвижные изображения. Видеоспам в режиме реального времени может встречаться в услугах мультимедийных IP-приложений, которые предусматривают функцию визуального общения между пользователями услуги в реальном времени.

На ранних стадиях развития спама в мультимедийных IP-приложениях, текстовые и голосовые спамовые сообщения, которые можно создавать без особых трудностей, могли доставляться с небольшими затратами, и не являлись обременением для IP-сети. Голосовой спам в режиме реального времени в форме телемаркетинга мог быть большей частью спама в мультимедийных IP-приложениях. Однако с развитием технологий обмена и доставки мультимедийных данных среди пользователей услуг мультимедийных IP-приложений и с ростом пропускной способности, видеоспам в режиме реального времени может стать столь же широко распространенным явлением.

7.4 Голосовой спам не в режиме реального времени

Голосовой спам не в режиме реального времени можно определить как незапрашиваемое голосовое сообщение, например, с целью рекламы коммерческих продуктов или услуг. Типичным примером голосового спама не в режиме реального времени является спам в виде записанного голосового сообщения.

Во многих случаях услуга VoIP может поддерживать услугу передачи мультимедийных сообщений, например передачу и прием текстовых, звуковых и видеосообщений, в дополнение к функции голосовой связи в реальном времени. Используя эту функцию услуги VoIP, спаммеры могут передавать спам в виде голосового сообщения, которое уже записано в терминал получателя спама. Этот тип спама в виде голосового сообщения причиняет большой ущерб пользователям услуг VoIP и провайдерам услуг VoIP, занимая место в почтовом ящике или хранилище данных, поскольку голосовое сообщение, обычно, имеет большой размер.

7.5 Текстовый спам не в режиме реального времени

Текстовый спам не в режиме реального времени может быть определен как незапрашиваемое значительное по объему текстовое сообщение, переданное не в режиме реального времени, например, с целью рекламы коммерческих продуктов или услуг. Характеристики текстового спама не в режиме реального времени аналогичны характеристикам спама в электронной почте. Текстовый спам не в режиме реального времени может появляться в различных мультимедийных IP-приложениях, поскольку создать и доставить текстовое сообщение нетрудно, и стоимость рассылки спама, обычно, мала.

Текстовый спам не в режиме реального времени может быть доставлен на IP-терминалы, которые способны принимать длинные тестовые сообщения типа электронной почты, или на телефоны VoIP, способные принимать короткие текстовые сообщения типа SMS в подвижных службах. Он может быть доставлен посредством множества услуг мультимедийных IP-приложений, включая IM и различные онлайновые услуги. Кроме этих типов текстового спама, который может быть доставлен получателям спама вне зависимости от намерений получателя спама, существуют другие типы текстового спама, который доставляется пользователям IP-услуги, например рекламный материал, размещенный на веб-сайтах. Характеристики текстового спама не в режиме реального времени аналогичны характеристикам спама в электронной почте и, как ожидается, некоторые методы противодействия спаму в электронной почте могут применяться к этому виду спама. Применимость этих методов может снижаться, когда длина текстового спама мала.

7.6 Видеоспам не в режиме реального времени

Видеоспам не в режиме реального времени можно определить как незапрашиваемое значительное по объему видеосообщение, переданное не в режиме реального времени, например, с целью рекламы коммерческих продуктов или услуг. Этот тип спама может быть одного из двух видов: пользователи IP-услуги получают или загружают спам в виде видеофайла, или пользователи IP-услуги получают доступ к видеоспаму в услугах мультимедийных IP-приложений посредством услуги видео-по-запросу (VoD). Методы доставки видео спама не в режиме реального времени можно разделить на две группы. Первая, получатели спама могут получить незапрошенные ими рекламные видеофайлы, переданные спаммером. Другой случай, когда пользователи мультимедийной IP-услуги загружают файлы, содержащие спам, посредством служб обмена файлами, не подозревая, что этот файл является спамом.

Когда получатель спама загружает спам в виде видеофайла, усилия и время, затраченные на загрузку файла со спамом могут быть потрачены впустую. Когда доставляется спам в виде видеосообщения, вне зависимости от желания получателя спама, спам причиняет ущерб пользователям услуги, занимая место в почтовом ящике или хранилище данных, поскольку видеосообщение обычно имеет большой размер.

8 Технические проблемы противодействия мультимедийному IP-спаму

Подобно спаму в электронной почте или в SMS для мобильных устройств, последовательность процедур, связанных с созданием, рассылкой и предотвращением передачи спама в услугах мультимедийных IP-приложений, является следующей:

– создание и доставка спама;
– обнаружение и фильтрация спама пользователем услуги и/или поставщиком услуги мультимедийных IP-приложений;
– противодействие принятому спаму.

До определения технических правил противодействия спаму в мультимедийных IP-приложениях, требуется исследовать слабые стороны предотвращения спама в мультимедийных IP-приложениях для соответствующей описанным выше процедурам. Учитывая это, на каждом этапе противодействия спаму в мультимедийных IP-приложениях необходимо рассмотреть типы технических проблем.

Анализ влияния этих проблем на процесс создания и доставки мультимедийного IP-спама приведен ниже. Анализ проблем, выполненный в данном разделе, может быть полезен в процессе изучения технических основ и технических средств противодействия мультимедийному IP-спаму, с целью определения эффективного способа противодействия спаму в мультимедийных IP-приложениях.

8.1 Создание и доставка спама

Базовое предположение о широком распространении мультимедийного IP-спама заключается в том, что стоимость рассылки спама должна быть низкой по сравнению с той выгодой, которую ожидает получить спаммер от мультимедийного IP-спама. Стоимость рассылки спама включает в себя не только стоимость в деньгах, но также и ресурсы различного вида, такие как время, усилия и техническая сложность, требуемая для создания и доставки мультимедийного IP-спама. Факторами, которые влияют на стоимость рассылки спама, являются следующие:

– стоимость сбора целевых адресов или целевых телефонных номеров: требуемая стоимость сбора адресов и телефонных номеров целевой аудитории спама;

– стоимость создания и доставки спама: требуемая стоимость создания и доставки спама для спаммера.

8.1.1 Составление списка целевой аудитории

До рассылки спама, прежде всего, требуется составить списки целевой аудитории. Спаммеры могут без особого труда сформировать список целевой аудитории для рассылки спама в электронной почте при помощи словарной атаки, программы сбора адресов электронной почты и незаконного доступа к собранным спискам целевой аудитории. В случае рассылки спама в виде SMS на мобильные телефоны список целевой аудитории может быть собран в виде простых комбинаций номеров, поскольку число номеров мобильных телефонов ограничено.

Тип идентификатора конкретного объекта, используемый для связи и обмена сообщениями между пользователями мультимедийной IP-услуги, может меняться в соответствии с типом мультимедийных IP-приложений, протоколом, национальными регламентарными правилами и т. п. Идентификаторы объекта, которые могут использоваться для услуги VoIP, могут иметь вид телефонных номеров, по аналогии с услугой КТСОП, IP-адресов, учетные записи IP-услуг, учетные записи электронной почты и т. п. Для услуги IM в качестве идентификатора объекта, как правило, используется адрес электронной почты и другие виды информации, например, может использоваться также номер мобильного телефона.

Когда для VoIP и IM используются такие виды идентификаторов объекта, спаммеры могут собрать идентификаторы объекта и счета услуг для этих услуг, используя существующие методы сбора списка целевой аудитории, используемые при рассылке спама в электронной почте. Адреса пользователей для VoIP и IM, как ожидается, могут быть собраны без особых усилий при помощи словарной атаки, программы сбора идентификаторов во время поиска в сети и т. п.

Помимо VoIP и IM различные виды спама могут существовать во вновь возникающих мультимедийных IP-приложениях, услугах онлайновой переписки, услугах онлайновых игр, услугах на базе P2P и т. п. Представляется также, что для создания списков целевой аудитории с целью рассылки спама для этих мультимедийных IP-приложений не требуется особых усилий. Во многих этих мультимедийных IP-приложениях, таких как онлайновые услуги, в качестве идентификаторов объекта применяются широко используемые типы счетов, например адреса электронной почты и номера телефона. Как правило, не трудно зайти в список пользователей услуги мультимедийных IP-приложений, которая позволяет передавать файлы или сообщения всем разрешенным пользователям. Учитывая эти соображения, если не принимать специальных мер, которые затрудняли бы сбор идентификаторов пользователей услуг мультимедийных IP-приложений, то спаммерам будет не сложно создать идентификаторы объекта IP-услуг, ни технически, ни экономически.

8.1.2 Создание и доставка спама

Как ожидается, затраты, необходимые для создания и доставки спама в мультимедийных IP-приложениях, будут составлять наибольшую часть расходов рассылки мультимедийного IP-спама. Услуги VoIP или голосовая связь в мультимедийных IP-приложениях различного вида, как правило, стоят дешевле, чем услуги проводной телефонии с коммутацией каналов или услуги подвижной телефонной связи. Для традиционных спаммеров, которые для активного маркетинга используют телемаркетинг в традиционных службах проводной или беспроводной телефонии, VoIP или голосовая связь в мультимедийных IP-приложениях является привлекательной целевой услугой для доставки спама. Более того, междугородние и международные звонки здесь намного дешевле, чем в

традиционных телефонных службах. Поэтому телемаркетинговый спам может распространяться в других странах, в которых говорят на том же языке, и телемаркетинговый спам может приходить из других стран, где очень мала стоимость труда оператора службы телемаркетинга и доставки спама.

В дополнение к услуге VoIP, многие мультимедийные IP-приложения, например услуги IM, услуги P2P и услуги онлайновой переписки предоставляются бесплатно или по очень маленькой цене. Ожидается, что создание и доставка спама в этих приложениях не потребует больших усилий или затрат, поскольку они обычно не требуют много денег, времени и не представляют технической трудности.

8.2 Обнаружение и фильтрация спама

Обнаружение и фильтрация спама в мультимедийных IP-приложениях является наиважнейшей, с технической точки зрения, частью эффективной противодействия спаму. Спам в электронной почте на сервере поставщика интернет-услуг (ISP), или в интранете, или на терминале получателя электронной почты можно отфильтровать еще до того, как получатель спама проверит спам, поскольку услуга электронной почты использует механизм хранения и дальнейшей передачи. Объем спама в электронной почте может быть отфильтрован с применением различного рода методов фильтрации, например анализа содержания и т. п., поскольку большинство сообщений электронной почты имеет текстовое содержание. В отличие от спама в электронной почте, фильтровать мультимедийный спам представляется чрезвычайно сложным, благодаря следующим функциям мультимедийного IP-приложения:

– связь в режиме реального времени;
– сложность анализа звукового и видеосодержания;
– сложность аутентификации спаммера.

Некоторые мультимедийные IP-приложения, такие как VoIP и IM, обеспечивают связь между пользователями услуги в режиме реального времени. Спам в таких приложениях доставляется получателю спама в реальном времени без промежуточного хранения на сервере. В некоторых случаях, содержание VoIP и IM не проходит через сервер провайдера услуг. Вместо этого оно доставляется непосредственно пользователю услуги. Следовательно, до установления соединения или до доставки сообщения трудно получить достаточную информацию о сообщении и проанализировать содержание сообщения для обнаружения спама. Например, когда установлено соединение отправителем и получателем спама, и получатель спама понял, что этот звонок является спамом, уже слишком поздно фильтровать спам, поскольку соединение уже установлено. В случае спама IM может иметься возможность проанализировать содержание IM сообщения в течение очень короткого времени, поскольку сообщения IM, обычно, текстовые. Однако краткость IM-сообщений может снизить эффективность традиционных методов фильтрации, разработанных для противодействия спаму в электронной почте. Терминалы пользователей услуги берут на себя ответственность фильтрации спама, когда содержание мультимедийных IP-приложений не проходят через сервер ISP. Но добавление в терминалы пользователей услуги фильтрации спама и управление функциями фильтрации спама со стороны пользователей является непростой задачей. Следовательно, обнаружение и фильтрация в режиме реального времени спама в мультимедийных IP-приложениях, например спама в услугах VoIP и спама IM, при помощи фильтрации на основе анализа содержания, может и не получиться.

В некоторых мультимедийных IP-приложениях, где связь в режиме реального времени не столь важна, например в услугах передачи мультимедийных сообщений или доставки файлов P2P, может использоваться механизм хранения и дальнейшей передачи для противодействия спаму посредством анализа содержания, когда это требуется поставщиками или пользователями услуг. Однако обнаружение и фильтрация спама посредством анализа содержания остается сложной задачей, поскольку технологии распознавания звуков и изображений до конца не разработаны, и применение таких технологий может привести к значительной загрузке сети.

Можно использовать также возможности идентификации спама на основе информации отправителя, а не информации о самом сообщении. Можно идентифицировать, является ли отправитель спаммером или нет, используя методы различного вида, например черные списки, белые списки, систему репутаций и т. п. Применение этих методов к спаму в мультимедийных IP-приложениях имеет несколько слабых пунктов. Во-первых, создание счетов услуги или идентификаторов объекта для мультимедийных IP-приложений не представляет трудности, и их может быть создано очень много. Спаммеры легко могут создавать новый идентификатор, когда их старый идентификатор определен как идентификатор спаммера. Спаммер может также выдать себя за обычного пользователя услуги, используя слабые стороны системы безопасности мультимедийных

IP-приложений. Учитывая эти факторы, необходимо комбинировать методы противодействия спаму, которые идентифицируют спам на основе информации об отправителе, с эффективными механизмами аутентификации.

8.3 Действия, когда спам уже получен

Получатели спама, после того как спам уже принят, могут предпринять несколько действий. Они могут добавить идентификатор спаммера в черный список, для того чтобы запретить спаммеру передавать спам в дальнейшем им или другим пользователям. Они также могут дать спаммеру плохую оценку, которая будет отражена в системах репутаций. Можно также сообщить о незаконном спаме, для того чтобы спаммеры понесли наказание. Однако, как упоминалось ранее, во многих мультимедийных IP-приложениях идентифицировать спаммеров непросто, а создать новый идентификатор нетрудно. На данном этапе требуется также использовать эффективный механизм аутентификации для повышения эффективности действий, когда спам уже получен.

9 Угрозы безопасности, связанные со спамом

В данном разделе рассматриваются аспекты мультимедийного IP-спама, связанные с безопасностью. Определены и классифицированы некоторые угрозы безопасности и меры противостояния им.

9.1 Угрозы безопасности, связанные со спамом

В данном разделе рассматриваются некоторые угрозы безопасности, которые могут возникать в мультимедийных IP-приложениях. Угрозы безопасности определяются с точки зрения рассылки спама в сети. Спаммеры могут рассылать спам, используя следующие технические атаки в среде мультимедийных IP-приложений .

9.1.1 Сбор идентификаторов

Для того чтобы рассылать спам, спаммер собирает идентификаторы с целью отыскания целевой аудитории для рассылки спама. Следовательно, сбор идентификаторов является наиболее общим действием по рассылке и важнейшим подготовительным процессом. Спаммер стремится собрать максимально возможное количество идентификаторов, поскольку число идентификаторов означает число мишеней для атаки с точки зрения спаммера. Идентификаторы могут быть собраны различными способами. Они могут быть собраны при помощи поисковых машин, открытых групп и т. д. Идентификаторы могут быть сгенерированы из обычных слов и имен. Иногда они могут быть собраны в результате незаконного взаимодействия с компаниями или школами, которые имеют большое число клиентов и обладают их личной информацией.

Во многих мультимедийных IP-приложениях для идентификации пользователей используются уникальные идентификаторы, такие как адреса электронной почты и URI. В отличие от телефонных услуг, услуги в мультимедийных IP-приложениях имеют несколько преимуществ, таких как многоканальная связь, низкая цена и т. п. Спаммерам выгодно рассылать спам именно в среде мультимедийных IP-приложений. Следовательно, пользователи должны быть осмотрительны, сохраняя свои идентификаторы и не позволять раскрывать их для спаммеров.

9.1.2 Маскировка отправителя спама

Маскировка – это один из видов перехвата. Злоумышленник создает веб-сайт и завлекает людей для его посещения для сбора данных об аутентификации пользователя, используя организационный недостаток протокола TCP/IP для кражи их личной информации. Кроме того, если спаммер рассылает спам, маскируясь под известную компанию, получатель может подумать, что сообщение получено от заслуживающего доверия отправителя. Высока вероятность того, что такой спам будет принят. Эти действия называются также "спуффингом"'.

Рассылка спама посредством маскировки ("спуффинга") отправителя – это угроза, в которой спаммер выдает себя за кого-то иного, подделывая поле заголовка сообщения или идентификатор отправителя, используемый в мультимедийных IP-приложениях. Эта угроза может разрушить возможность применения таких хорошо известных решений противодействия спаму, как белый список и черный список. Например, если спаммеры заменяют свой идентификатор идентификатором существующего пользователя, который внесен в список контактов или белый список получателя, то спаммер сможет обойти правила, основанные на белом списке. Более того, благодаря природе мультимедийной связи, до того, как соединение установлено, очень трудно определить, является ли данное сообщение спамом или нет. Следовательно, в данном случае, получатель ничего не может поделать, кроме как получить спам.

9.1.3 Анализ трафика для получения регистрационной информации

Анализ трафика – это действие, при помощи которого спаммер подслушивает существующий сеанс связи между другими пользователями. Инструмент, используемый для анализа трафика, называется анализатором трафика.

В условиях мультимедийного IP-взаимодействия, спаммер может рассылать незаконный спам, используя анализатор трафика. Во-первых, спаммер перехватывает регистрационную информацию действительного пользователя для конкретных приложений, в которых используется анализатор трафика, и, используя полученную информацию, генерирует фальшивую регистрационную информацию. Затем спаммер вводит в регистрационное сообщение IP-адрес атакующего вместо IP-адреса действительного пользователя. Затем спаммер может рассылать спам, используя фальшивую регистрацию.

9.1.4 Перехват сеанса связи

Перехват сеанса связи – это метод, при помощи которого один человек перехватывает сеанс связи между другими пользователями. Он может использоваться для рассылки спама в условиях мультимедийного IP-взаимодействия. Спаммеры могут заставить систему разорвать текущее соединение между двумя пользователями в середине сеанса связи. В этом случае пользователи стремятся восстановить предыдущие сеансы связи. После этого спаммеры могут перехватить сеанс связи и ввести в середину восстановленного сеанса связи сообщение протокола транспортирования реального времени (RTP), содержащее спам.

9.1.5 Введение запроса SQL

Введение запроса SQL – это метод перехвата, который выдает анормальный результат за счет введения синтаксиса запроса, который не использовался запрашивающей стороной. В условиях мультимедийных IP-приложений введение запроса SQL может использоваться, когда для аутентификации применяются механизмы дайджеста HTTP. Спаммер изменяет аутентификационный заголовок и вводит поддельный запрос SQL. Затем спаммер подделывает аутентификационный заголовок сообщения на прокси-сервере таким образом, который используется для аутентификации механизмом дайджеста HTTP, и вводит поддельный запрос SQL. Если эта атака завершается успехом, спаммер может выдать себя за аутентифицированного пользователя и передавать спам с настоящей авторизацией, подделав регистрационную информацию пользователя.

9.1.6 Спам-бот

Спам-бот – это злонамеренный бот, имеющий форму программы или кода, который может управляться из удаленного места, но который не может быть запущен сам собой. Как правило, он управляется по каналу связи при помощи протокола IRC. Сеть, состоящая из ботов, называется BotNet. Спаммер может управлять многими зараженными системами, используя всего лишь одну команду, потому что сеть BotNet может быть соединенной. Следовательно, спаммер, используя этот метод, может без труда рассылать большое количество спама в мультимедийных IP-приложениях.

9.1.7 Искажение кэш-памяти

Искажение кэш-памяти – это атака, которая заменяет адреса доменов другими фальшивыми адресами. Искажение кэш-памяти может использоваться в мультимедийных IP-приложениях для ARP и NDP. ARP используется для проверки соответствия IP и MAC адреса в сетях IPv4, а NDP используется для отыскания соседей в сетях IPv6. Пакеты ARP и NDP ретранслируются на все устройства, которые соединены в отдельную линию. Спаммеры могут использовать метод искажения кэш-памяти для изменения содержания кэш-памяти в ARP или в NDP посредством перехвата пакетов.

Например, используя искажение кэш-памяти ARP, спаммер может замаскироваться под шлюз, для того чтобы перехватывать все пакеты в этом канале связи. Таким образом, если пользователь инициирует соединение, то спаммер может ввести в текущий сеанс связи заранее подготовленное содержащее спам сообщение RTP. Спаммеры могут изменить идентификатор цели своей атаки. Если меняется идентификатор пользователя, пользователь может попытаться установить другое соединение с другой стороной, которая имеет идентификатор, к которому обращается спаммер, но который не является исходной стороной. Посредством этой атаки спаммеры могут передавать спам пользователю, который запрашивает соединение.

9.1.8 Контроль за маршрутизацией

Предполагая, что между маршрутизаторами и пользователями существует соединение для мультимедийных IP-приложений, спаммер при помощи перехвата играет роль маршрутизатора в соединении по данной сети. Если пользователь пытается установить соединения с другим пользователем, принадлежащим определенной сети, то спаммер отвечает на запрос, выдавая себя за действительного пользователя, и передает спам пользователю, который запрашивает соединение.

9.1.9 Уязвимая система управления

Могут существовать другие угрозы, которые используют уязвимые точки системы управления. В случае такой угрозы спаммеры могут изменить регистрационную информацию действительного пользователя и передать спам, используя данные действительного пользователя.

9.2 Классификация угроз безопасности, обусловленных спамом

Вышеперечисленные угрозы безопасности, обусловленные спамом, можно разделить на классы в соответствии с методом атаки. Классификация угроз безопасности, обусловленных спамом, показана в таблице 9-1.

Таблица 9-1 – Классификация угроз безопасности, обусловленных спамом, в соответствии с методом атаки

Методы атаки	Угрозы безопасности, обусловленные спамом
Злонамеренное программное/ дистанционное управление	Спам-бот
Перехват сеанса связи	Перехват сеанса связи
Введение запроса SQL	Введение запроса SQL
Анализ трафика	Анализ трафика для получения регистрационной информации
Маскирование	Маскирование отправителя, искажение кэш-памяти, управление маршрутизацией
Другие	Сбор идентификаторов, уязвимая система администрирования

Злонамеренное программное/дистанционное управление – это метод, при помощи которого можно без труда разослать большие объемы спама. Спаммеры могут распространять злонамеренные программы различными способами и давать зараженным устройствам команды рассылки спама. Одним из примеров является спам-бот.

Перехват сеанса связи – это метод перехвата, который крадет чужой сеанс связи. Как правило, это можно сделать, просто угадав ID сеанса связи и используя маркеры ID сеанса связи. Спаммеры могут подслушать связь между сервером и пользователем без процедур аутентификации или с разрешения сервера.

Введение запроса SQL – это метод перехвата, который использует уязвимость баз данных. Он может изменить обычный запрос SQL и незаконно пройти аутентификацию. Как правило, этот метод используется при взломе веб-сайта для кражи информации пользователя.

Анализ трафика – это метод, в котором хакер перехватывает пакеты, передаваемые между двумя или несколькими пользователями.

Маскирование – это метод, в котором один человек выдает себя за другого человека. Это действие может заставить компьютер другой стороны поверить в то, что спаммер – это другое лицо, заслуживающее доверия.

9.3 Меры противодействия

Существует три метода противодействия для решения вышеописанной проблемы спама: аутентификация, авторизация и управление безопасностью. Управление безопасностью означает противодействие, которое может применяться для соответствующей конфигурации безопасности путем установки в систему обеспечивающей безопасность программной вставки для обслуживания, восстановления и расширения осведомленности пользователя о безопасности. Существуют различные меры противодействия, например управление потоком, шифрование и т. д., которые можно использовать. В данном разделе рассматриваются три основных меры противодействия.

Взаимосвязь между мерами противодействия и угрозами безопасности, обусловленными спамом, сведена в таблицу 9-2.

Таблица 9-2 – Взаимосвязь между мерами противодействия и угрозами безопасности мультимедийной связи, обусловленными спамом

Меры противодействия / Угрозы	Аутентификация	Авторизация	Управление безопасностью
Сбор идентификаторов			X
Маскировка отправителя	X		
Анализ трафика для получения регистрационной информации	X		
Перехват сеанса связи	X		
Введение запроса SQL		X	X
Спам-бот			X
Искажение кэш-памяти	X		
Управление маршрутизацией	X		
Уязвимая система администрирования		X	X

Аутентификация может решить многие обусловленные спамом угрозы безопасности путем разрешения проблем маскировки. Маскировка используется в различных угрозах, таких как маскировка отправителя, анализ трафика для получения регистрационной информации, перехват сеанса связи, искажение кэш-памяти и контроль за маршрутизацией. Для противодействия атакам с маскировкой отправителя каждый отправитель аутентифицируется посредством процедуры аутентификации после того, как сообщение принято. Для противодействия атакам в виде анализа трафика для получения регистрационной информации, не аутентифицированному пользователю запрещается изменять регистрационную информацию в процессе аутентификации. Для противодействия атаке вида перехвата сеанса связи и искажения кэш-памяти только аутентифицированные пользователи могут присоединиться к соединению. Для противодействия атаке управления маршрутизацией только аутентифицированный пользователь может управлять маршрутизатором.

Однако обусловленные спамом угрозы безопасности при введении запроса SQL не могут быть разрешены посредством аутентификации. Соответственно, в таких случаях требуется определить правила авторизации. К этому случаю могут принадлежать также и уязвимые системы администрирования. Системный администратор должен давать различные права доступа различным пользователям в соответствии с их счетами.

И, наконец, некоторые обусловленные спамом угрозы безопасности требуют тщательного управления безопасностью. К этому случаю относятся сбор идентификаторов, введение запроса SQL, спам-бот и уязвимые системы администрирования. Спаммеры могут получать идентификаторы пользователей и передавать спам по многим каналам. Следовательно, требуется тщательное управление идентификаторами. Разработчики системы должны учитывать это при разработке системы, поскольку угрозы введения запроса SQL иногда возникают из-за ошибочного кода. Спам-бот создается посредством злонамеренного заражения со стороны другого бота. Следовательно, пользователи компьютеров должны быть осторожны при загрузке файлов или доступе к веб-сайтам, и должны защищать свою ОС. В ситуации с уязвимой системой администрирования системные администраторы должны быть осторожны в управлении своими системами.

10 Применимость хорошо известных механизмов противодействия спаму в мультимедийных IP-приложениях

Проведено множество исследований различных механизмов борьбы с обычным спамом в электронной почте. Некоторые из решений, использованных для спама в электронной почте, могут также применяться для противодействия мультимедийному IP-спаму. Прежде чем обратиться к пространству решений для мультимедийного IP-спама, необходимо проанализировать механизмы борьбы с обычным спамом и обсудить их применимость для противодействия мультимедийному IP-спаму. Следовательно, в данном разделе будут обсуждаться некоторые из хорошо известных

механизмов противодействия спаму в свете их применимости для противодействия мультимедийному IP-спаму.

10.1 Фильтрация по идентификации

10.1.1 Черный список

Черным списком называется список идентификаций (например, адресов электронной почты), которые подозреваются в том, что они являются спаммерами, или которые определены как спаммеры. Механизм черного списка предназначен для фильтрации сообщений или звонков от отправителей из этого списка. Списками идентификаций могут быть списки IP-адресов, доменных имен, идентификаторов или адресов вызывающей стороны, содержания заголовков или основного текста сообщений, или некоторые комбинации этих различных типов, которые могут использоваться для идентификации спама.

Использование только черного списка для противодействия спаму может не быть эффективной мерой в IP-приложениях. Спаммер может воспользоваться идентификацией других ничего не подозревающих людей и обмануть приемник. Эта проблема может быть решена за счет использования механизмов аутентификации адреса источника. Другой проблемой этого метода является то, что пользователь может без труда создавать новые идентификации. Различные мультимедийные IP-приложения, созданные для электросвязи, используют адреса электронной почты. Адрес электронной почты может быть без труда создан на известных порталах. Средний пользователь, не занимающийся спамом, в большинстве случаев тоже использует адреса, созданные на известных порталах, таким образом, доменное имя портала не может быть внесено в черный список. Для того чтобы решить эту проблему, поставщик услуг портала должен несколько увеличить сложность процесса создания новых адресов. Если время и усилия на создание нового адреса велики, спаммер, несомненно, будет использовать другой метод создания новых адресов для рассылки спама. Эти новые адреса имеют больше шансов быть отфильтрованными с использованием черного списка доменов. Следовательно, метод черного списка становится эффективным, если используется в сочетании с другими методами.

Метод черного списка применятся только в самом начале соединения, когда впервые встречается идентификационная информация источника. Следовательно, метод черного списка можно применять для мультимедийных IP-приложений любого вида, в которых используется идентификация по адресу источника. Этот метод может использоваться для приложений веб-сайта, поскольку имеется возможность применения метода черного списка для предоставления права передачи сообщений только не спаммерам, т. е. пользователям, не включенным в черный список. Таким образом, метод черного списка может использоваться для блокировки мультимедийного IP-спама любого вида, в котором используется идентификация любого вида, как в приложениях реального времени, так и в приложениях нереального времени.

10.1.2 Белый список

Белый список – это список, обратный черному списку. Этот список содержит информацию о доверенных пользователях. Электронные сообщения, созданные из адресов отправителей из белого списка, будут всегда приняты. В отличие от черного списка, массированное создание адресов электронной почты с целью изменения идентификатора, не поможет попасть в белый список, но он все же уязвим для маскировки адресов. Спам с маскированным адресом можно легко отфильтровать, используя методы сильной аутентификации.

Хотя метод белого списка позволяет отфильтровать почти весь спам, обычному человеку требуется связь с другими людьми, не указанными в белом списке. Если отправителю, не указанному в белом списке, потребуется связь с пользователем, то необходим некоторый метод авторизации, для того чтобы попасть в белый список данного пользователя. Пользователям придется проверить отправителя посредством идентификации или по каким-либо вводным замечаниям со стороны отправителя. Пользователь может принять или отклонить запрос на соединение. Принятый отправитель может попасть в белый список данного пользователя. Если пользователям приходится принимать или отклонять каждый новый запрос, это может быть раздражающим, поскольку большая часть новых запросов является спамом. Еще одна проблема этого подхода заключается в том, что пользователь при смене условий работы вынужден переконфигурировать белый список, что требует затрат времени и энергии.

Принципы белых списков уже включены в систему IM, которая известна как список контактов. Многие системы IM разрешают соединение только пользователям, внесенным в список контактов,

оставляя новым пользователям возможность получить согласие на присоединение к списку контактов. Таким образом, при использовании сильных механизмов аутентификации этот метод может быть полезен для противодействия спаму IM. Однако VoIP имеет функции, отличные от функция систем IM. Как и в системах электронной почты, белые списки могут быть полезны в качестве дополнительного метода при использовании других методов, поскольку пользователи все равно принимают звонки от неизвестных абонентов.

Метод белого списка применятся только в самом начале соединения, т. е. он приемлем как для приложений реального времени, так и для приложений не реального времени. Этот метод может использоваться для приложений веб-сайта, поскольку имеется возможность применения метода белого списка для предоставления права передачи сообщений только пользователям, включенным в белый список.

10.1.3 Система репутаций

Система репутаций используется совместно с белым или черным списком. Если отправитель, который не входит ни в черный, ни в белый список получателя, желает связаться с получателем, то принимающий терминал отображает его оценку репутации. Оценка репутации помогает приемнику принять решение, должен ли он принять или отклонить вызов. Если пользователь принимает запрос на соединение и понимает, что отправитель является спаммером, он или она может сообщить о спаме системе репутаций и не добавлять идентификатор отправителя в белый список данного пользователя. Эти отчеты накапливаются на сервере репутаций и образуют оценку репутации.

Проблема этого метода заключается в том, что спаммер с отрицательной оценкой репутации может сменить свою идентификацию и начать рассылку спама с новой идентификацией. Эта новая идентификация не будет иметь отрицательной оценки репутации, и потребуется некоторое время, чтобы этого пользователя признали спаммером после накопления отрицательных баллов. Еще одна проблема этого подхода заключается в том, что некоторая группа злоумышленников может травить невинную жертву, создавая ей отрицательную оценку репутации. Эта невинная жертва с отрицательной оценкой репутации будет иметь трудности в ведении своего бизнеса в IP-сетях.

Другой тип системы репутаций – это система положительных репутаций. Приемник прибавляет положительные баллы не спаммерам. При этом новый идентификатор затруднит рассылку спама, поскольку новый идентификатор будет иметь очень маленькую оценку репутации. Проблема этого метода заключается в том, что несколько спаммеров могут объединиться и ставить друг другу положительные баллы. Однако для того чтобы сделать это, спаммерам потребуется создать некоторый вид консорциума, что может быть очень дорогостоящим. Следовательно, система положительных репутаций является более эффективной, чем система отрицательных репутаций.

Для того чтобы система репутаций работала, необходима централизованная и единая система управления электросвязью. Этот метод может хорошо работать с приложениями типа IM, которые, как правило, управляются одним поставщиком услуг. Однако в приложениях VoIP предполагается связь между различными поставщиками услуг. Оценка репутации у разных поставщиков услуг может быть различной, поскольку стандартизованного определения у нее нет. Следовательно, этот метод не пригоден для таких приложений как VoIP, если нет стандартизованного описания системы.

Система репутаций может использоваться также в приложениях, в которых используется какая-либо идентификация отправителей, поскольку оценка репутации может быть присвоена идентификатору. Если отправитель прошел систему репутаций, отправитель будет добавлен в белый список получателя. Таким образом, этот метод может использоваться в любых приложениях реального или не реального времени.

Этот метод может использоваться также для веб-приложений путем предоставления права передачи сообщений только пользователям, имеющим оценку репутации выше некоторого уровня. Этот веб-сайт может хранить данные об оценке репутации для каждого участника, сохраняя данные о предыдущих действиях.

10.1.4 Круги доверия

В методе кругов доверия группы доверенных людей или доверенных доменов объединяются, и совместно используют свои белые списки. Методика этого подхода заключается в том, что человек доверят другу доверенного друга. Эта группа может сформировать доверенные отношения, и она также соглашается исполнять некоторый тип наказания, если один из участников будет уличен в рассылке спама.

Одним из вариантов метода кругов доверия является подход на основании распределенного черного списка, в котором группа доверенных людей совместно использует свои черные списки. Этот подход очень эффективен для фильтрации вредоносного спама. Могут существовать сервера, которые собирают черные списки, основываясь на этом подходе, и открывают собранный черный список для всеобщего использования.

Этот вид данного метода хорошо работает с небольшими группами или при небольшом числе поставщиков услуг, где можно обеспечить совместное использование и реализацию этой политики. Если размеры доверенных кругов растут, может оказаться невозможным достигнуть реальной договоренности по необходимому уровню наказания за рассылку спама.

10.2 Маскировка адреса

Для использования различных мультимедийных IP-приложений требуется знать их адреса. Следовательно, важно чтобы чей-то адрес не стал доступным для всех. Но при использовании веб-услуг адрес должен быть виден новому пользователю, чтобы он мог легко связаться с владельцем сайта. Спаммеры используют эту слабую точку для сбора адресов для рассылки спама. Спаммеры просматривают различные веб-страницы и выбирают адреса, имеющие в своей структуре знаки "@" и ".". Собранные адреса используются для рассылки спама, и кроме того, собранные адреса распространяются среди других спаммеров, поскольку спаммеры стремятся совместно использовать адреса для рассылки спама.

Маскировка адреса – это метод, при котором адрес пользователя скрывается, поэтому спаммер не может получить адрес автоматически. Наиболее простым методом является замена знака "@" на AT, а знака "." на DOT. Адрес, записанный таким образом, выглядит как обычный текст, и, следовательно, он невидим для системы автоматического сканирования адресов, которую используют спаммеры.

Маскировка адреса – это не метод противодействия спаму, а метод предотвращения спама. Этот метод предотвращает возможность получения адреса пользователя системой автоматического сбора адресов, которую используют спаммеры для сбора адресов. Таким образом, этот метод пригоден для предотвращения спама в мультимедийных IP-приложениях, которые используют те же адреса, что и веб-услуга.

В данном разделе описываются некоторые другие методы, которые могут использоваться для маскировки адреса.

10.2.1 Коды Java

В среде JavaScript просто добавить тип адреса "abc@xyz.com", используя функции языка Java. Веб-страница будет показывать его в форме "abc@xyz.com" но при использовании его с функцией document.write() языка JavaScript, очень просто спрятать адрес электронной почты. Ниже приведен один из примеров.

```
<SCRIPT TYPE="text/javascript">
document.write("abc@" + "xyz.com")
</SCRIPT>
```

Для того чтобы скрыть адрес электронной почты, можно использовать и другие функции или методы в среде JavaScript. Однако цель данного раздела состоит в том, чтобы описать, что в среде JavaScript можно скрыть адреса электронной почты. Таким образом, при использовании JavaScript для скрытия адресов, спаммеры столкнутся с трудностями автоматического сбора адресов электронной почты, даже если на веб-странице явно показан обычный адрес электронной почты.

Этот метод может использоваться только в среде JavaScript. Но, если пользователь желает показать на веб-странице свой ID в системе передачи сообщений или контактный адрес услуги VoIP с использованием языка JavaScript, этот метод может помочь не стать мишенью для спаммеров.

10.2.2 Код ASCII

Метод кода ASCII заключается в том, чтобы скрыть важную информацию в виде кода ASCII. который имеет вид "&#number". Важной информацией может быть адрес электронной почты или номер телефона, который является мишенью для спаммера. Веб-страница будет показана не в виде обычного текста, а в виде изображения. Таким образом, когда веб-страница загружается, она показывает только код ASCII. Если у спаммера есть функция преобразования кода ASCII в его программе поиска веб-страниц, то код ASCII может быть легко декодирован.

10.3 Доказательство взаимодействия с человеком

Каждый участник сеанса связи получает задачу или вопрос, которые составлены так, что решить их может только человек, но не машина. Задача или вопрос – это картинка или звук, содержащий слово или цифру, которые понять может только человек, но не машина. Это может быть изображение, скрытое за различными цветами или звук, замаскированный различными шумами, которые машине очень трудно распознать. Сегодня в результате достижений в области автоматической обработки звуков и изображений, и в области искусственного интеллекта очень трудно создать задачу, которая была бы непонятна для машин.

Метод доказательства взаимодействия с человеком, как правило, используется в веб-приложениях на этапе подписки на услуги сети, и поэтому он пригоден для борьбы с веб-спамом. Этот метод может использоваться также при фильтрации вызовов, содержащих спам, если применять метод авторизации с использованием звуков. Когда вызывающая сторона, не внесенная ни в черный, ни в белый список, начинает голосовой вызов, приемник автоматически включает систему автоматического голосового ответа (IVR), которая просит вызывающего абонента ввести некоторый номер на клавиатуре телефона. Если вызывающий абонент вводит номер телефона правильно, то номер вызывающего абонента автоматически добавляется в белый список данного пользователя. Пользователь услуги чатов в сети может также пройти через интерактивный метод доказательства, чтобы присоединиться к разговору.

10.4 Фильтрация по содержанию

Фильтрация по содержанию в строке темы – наиболее общий и широко используемый метод противодействия спаму в электронной почте. Он просматривает строки темы, отыскивая в них подозрительные слова, которые обычно используются в спаме.

IM – это связь посредством коротких сообщений, поэтому этот механизм может легко применяться для противодействия спаму. Основной текст каждого сообщения IM можно просматривать на предмет наличия в нем строки с адресом электронной почты.

Однако этот метод неприменим для VoIP или другой мультимедийной IP-связи, которая в настоящее время включает в себя звуки и/или изображение. Мультимедийное содержание может быть передано уже после того, как соединение установлено, поэтому предварительная фильтрация содержания не даст никакого выигрыша. С другой стороны, хотя спам доставляется в форме голосовой или видео почты, которая может храниться на сервере, современные технологии сканирования еще недостаточно хороши, чтобы использоваться для противостояния спаму.

10.5 Аутентификация посредством обмена ключами

Аутентификация имеет возможность безопасной идентификации отправителя мультимедийных IP-сообщений, что помогает блокировать большую часть спама типа атак маскирования.

10.5.1 PKI и PGP

Можно аутентифицировать отправителей с целью блокировки запросов на соединение со стороны спаммеров, выдающего себя за кого-либо другого, в частности за человека из белого списка. Метод инфраструктуры открытого ключа (PKI) и довольно хорошей секретности (PGP) – это хорошо известные методы аутентификации, которые используют механизмы открытого ключа. PKI использует механизм открытого ключа, в котором отправитель может быть аутентифицирован при помощи открытого ключа, который сертифицирован органом по сертификации (CA). В PGP используется компьютерная программа, которая выполняет функцию подписи для аутентификации. В системах электронной почты эти механизмы используются для шифрования сообщения и добавления цифровых подписей. Это сильные механизмы для предотвращения спама.

Механизмы обмена ключами полезны почти в любой мультимедийной системе IP-связи. Они должны быть тщательно разработаны для услуг IP-конференций, поскольку имеется высокий риск кражи группового ключа конференции.

Методы PKI и PGP могут использоваться почти для любых типов мультимедийных IP-приложений, таких как VoIP и IM. Этот метод может использоваться также в веб-приложениях, которые разрешают загрузку файлов или сообщений только сертифицированному пользователю.

10.5.2 DKIM [b-IETF RFC 4871]

Почта с идентифицированными ключами домена (DKIM) – это метод, который разработан Комитетом по инженерным проблемам Интернет (IETF) и который может использоваться в процессе

аутентификации электронной почты. Сервер электронной почты присоединяет к почте криптографический знак, который подтверждает, что этот сервер действительно передал данное сообщение. Метод DKIM позволяет организации нести ответственность за то, что сообщение должно быть подтверждено получателем. Метод DKIM определяет правила аутентификации цифровой подписи на уровне домена для электронной почты за счет использования криптографии с открытым ключом и технологии сервера ключей. Фальсификация электронной почты может не только вызвать повреждение приемника, но и испортить репутацию большого предприятия или организации. Применение метода DKIM может защитить предприятие или организацию от таких угроз.

Метод DKIM может использоваться для предотвращения фальсификации связи посредством VoIP или IM. Получатель может проверить на сервере отправителя, действительно ли принятое сообщение или вызов созданы заявленным отправителем. Процесс аутентификации может быть выполнен в начале соединения, таким образом, он не будет влиять даже на те соединения, для которых важен режим реального времени.

10.5.3 Аутентификация HTTP и соединение TLS

Применение аутентификации дайджеста HTTP [b-IETF RFC 5090] вместе с соединением TLS (безопасность на транспортном уровне) с сервером очень эффективно для мультимедийных IP-приложений со структурой клиент-сервер. Сервер домена проверяет своих пользователей посредством аутентификации дайджеста HTTP. Аутентификация дайджеста HTTP используется для аутентификации пользователя мультимедийных IP-приложений обычно при помощи имени пользователя и пароля. Клиент, которым является пользователь, поддерживает устойчивое соединение TLS с сервером. Клиент проверяет идентичность сервера, поддерживая с сервером соединение TLS. Сервер аутентифицирует клиента, используя обмен дайджестом данных о клиенте по соединению TLS. Когда аутентифицированный пользователь передает сообщение в другой домен, передающий домен сертифицирует пользователя, вводя подпись для подтверждения достоверности этого сообщения. Передающий и приемный домены должны образовать взаимную аутентификацию, чтобы доверять друг другу.

Этот метод может использоваться для аутентификации пользователей, связывающихся посредством IM или VoIP. Процесс аутентификации может выполняться в начале соединения, таким образом, он не будет влиять даже на те соединения, для которых важен режим реального времени.

10.6 Фильтрация спама на основании сетевых связей

Механизмы фильтрации спама, рассмотренные выше, разработаны для использования на стороне сервера и стороне клиента услуги связи. Однако для предотвращения спама важно создать безопасную сеть. В данном разделе будут кратко рассмотрены методы фильтрации спама на основании сетевых связей.

10.6.1 Отбрасывание пакета на сетевом объекте

Для маршрутизатора или другого объекта сети можно определить некоторые правила, например ACL (список контроля доступа), отбрасывания по подозрению в спаме пакетов, пришедших от источников с определенными IP-адресами или имеющих определенный IP-префикс источника. Источник спама может находиться внутри сети ISP или за пределами сети ISP. Поставщики ISP, которые желают защитить свои сети от спама, должны будут решать обе проблемы, используя различные подходы.

Если источник спама находится внутри сети ISP, то ISP может установить сетевой объект источника так, чтобы исключить возможность IP-соединения с источником спама. Спаммер увидит, что соединение разорвано, и должен будет признать свои неправомерные действия. Однако необходимо определить некоторый критерий, для того чтобы предотвратить неправильное использование. Один человек может ложно обвинить невинного человека в том, что он является спаммером, тем самым отказывая ему в присоединении к сети. Злоумышленник может использовать IP-адрес невинного человека для рассылки собственного спама, что также приводит к тому, что невиновному отказывают в присоединении к сети, а спаммер продолжает рассылать спам в течение определенного периода времени.

Предположим, что сеть "A" ISP соединена с сетью "B" ISP, и спаммер использует сеть "B" ISP. Если источник спама находится за пределами сети ISP A, то ISP A должен проверить, не стремится ли сеть ISP B управлять спамом в его сети. Если сеть ISP B не имеет никаких правил по управлению спамом, то ISP A должен определить правила для спама на шлюзе с сетью ISP B для предотвращения распространения спама по сети ISP A. Используя такой подход, ISP A не может запретить спаммеру присоединиться к сети, но он может защитить от спама свою сеть, этот метод может защитить и

сберечь ресурсы его сети. Недостатком такого подхода является то, что он может запретить невинному пользователю из сети ISP B соединиться с его сетью.

Другая проблема этого подхода состоит в том, что спаммер может часто менять свой IP-адрес. Таким образом, для того чтобы этот метод работал, ISP на стороне спаммера должен управлять и аутентифицировать IP-адрес, используемый спаммером.

Метод отбрасывания пакета на сетевом объекте может использоваться в любых приложениях, поскольку этот подход не зависит от мультимедийных IP-приложений.

10.6.2 Распределенный черный список

Распределенный черный список – это черный список, который хранится в сети для совместного использования сетевым сообществом. Распределенные черные списки обычно реализуются в службе доменных имен (DNS). Пользователи могут добавлять в распределенный черный список адрес, который был уличен в рассылке спама. Многие сайты отбрасывают сообщения с IP-адреса после того, как он появляется в распределенном черном списке. Применимость этого метода к мультимедийным IP-приложениям такая же, как и для метода черного списка.

10.6.3 Брандмауэр для спама

Корпоративные сети или сети ISP используют брандмауэры для спама с целью защиты своей сети от спама. Брандмауэр для спама использует многие методики, упомянутые ранее, для блокирования спама до его проникновения в сеть. Пользователь в защищенной сети не страдает от большей части спама. Этот метод представляет собой соединение черного списка и метода фильтрации по содержанию, поскольку он поддерживает черный список и фильтрует содержание, когда пакет проходит по корпоративной сети.

В настоящее время брандмауэр для спама используется для электронной почты и IM. Этот метод может не быть эффективным для услуг VoIP, поскольку в начале вызовов VoIP ничего отловить невозможно. Этот метод может использоваться для фильтрации веб-спама, поскольку его можно фильтровать, исследуя содержание.

10.7 Онлайновая марка

В методе с онлайновой маркой отправитель, который не включен в белый список получателя, для отправки сообщения должен будет купить онлайновую марку. Если отправитель, не включенный в список, передает сообщение без онлайновой марки, оно будет отброшено сервером поставщика услуги. На терминал получателя приходят только те сообщения от отправителей, не включенных в список, которые имеют онлайновую марку. Если получатель принимает сообщение, он вернет онлайновую марку отправителю. Адрес отправителя автоматически добавляется в белый список получателя. Если получатель решает, что отправитель передал спам, он может оставить у себя деньги за онлайновую марку. Спаммер будет вынужден передавать дополнительные сообщения, увеличивая расходы на рассылку спама.

Этот метод может точно также применяться в услугах электронной почты, VoIP и IM. Поскольку отправитель должен будет покупать онлайновую марку только один раз, этот метод не является ни раздражающим, ни дорогостоящим. Следовательно, он эффективен в борьбе со спамом, когда применяется с соответствующей аутентификацией идентичности отправителя.

10.8 Фильтрация спама на основе авторизации

Одним из важных "кирпичиков" в системе фильтрования спама является создание механизма, который бы давал команды некоторым объектам сети "фильтровать" входящие запросы на соединение в соответствии с правилами пользователя или сети. Различные объекты сети, такие как пользователи или системные администраторы, могут создавать или изменять правила авторизации. Правила сети необходимы для определения потоков сообщений между доменами.

Правила авторизации могут применяться на оконечном хосте и/или сетевыми элементами. Создателем правил может быть оконечный пользователь, который владеет устройством, провайдер услуг VoIP, человек, связанный с оконечным пользователем (например, родители ребенка, использующего мобильный телефон). Это раздел основан на различных вариантах фильтрации спама на основе авторизации.

10.8.1 Связь на основе взаимного согласия

Связь на основе взаимного согласия основывается на прямой авторизации сообщения на приемнике. Она используется совместно с белым или черным списком. Если отправитель, не включенный ни в

черный, ни в белый список, пытается соединиться с пользователем, он передает идентификатор и/или какой-нибудь короткий текст этому пользователю для идентификации самого себя. Отправитель сначала отбрасывается. Затем пользователя информируют, что отправитель пытается с ним связаться. Пользователь может принять или отклонить отправителя по итогам изучения идентификатора и/или короткого текста, переданного отправителем.

Этот тип фильтрации в настоящее время используется в различных услугах IM. Он очень эффективен для управления белым списком. Этот подход реализуем при работе с вызовами, содержащими спам, за счет достижения соглашения в начале вызова, но неприемлем для веб-спама, который является однонаправленной услугой. Он может быть неприемлем для услуг, предусматривающих участие множества пользователей, поскольку было бы неэффективно добиваться согласия от всех участников предоставляемой услуги.

Проблема этого подхода состоит в том, что пользователю может надоесть отвечать на огромное число запросов на согласование. Таким образом, некоторые запросы на согласование должны быть отфильтрованы другой системой фильтрации.

10.8.2 Авторизация на основе правил пользователя

В методе авторизации на основе правил пользователя, пользователь мультимедийных IP-услуг определяет правила принятия для фильтрации запросов от неизвестного отправителя. Правила устанавливаются для терминала пользователя или сервера приложений, для того чтобы автоматически принимать запросы. Эти правила могут применяться к адресу источника спама, идентификации и/или короткому тексту, переданному вызывающим абонентом, как и в методе связи на основе взаимного согласия. Правила могут применяться также к принятому содержанию, изображению, звуку или тексту для автоматической фильтрации запросов на соединение, нарушающих установленные правила. Информация об отброшенных запросах должна регистрироваться в хранилище так, чтобы пользователь мог вернуться и проверить запросы, которые не должны были быть отброшены. Пользователь может менять правила для удовлетворения своих потребностей.

Проблема метода связи на основе взаимного согласия состоит в том, что пользователь должен отвечать на запрос на соединение. Но в методе авторизации на основе правил пользователя большая часть спама фильтруется автоматически, поэтому пользователя не будет раздражать необходимость отвечать на огромное число запросов на согласование. Создание правил будет зависеть от характеристик используемых мультимедийных IP-приложений. Метод фильтрации на основе правил пользователя следует определить для всех приложений, где возможен спам.

Этот подход очень эффективен для управления белыми списками. Этот метод представляет собой подход, основанный на пользователе, следовательно, он может использоваться для любого типа двусторонних услуг, таких как VoIP и IM.

10.8.3 Авторизация на основе правил сети

Оператор сети должен использовать авторизацию на основе правил сети при фильтрации спама с целью защиты сети. Правила сети могут использоваться в отдельной сети или между соседними сетями. Этот метод эквивалентен методу отбрасывания пакета на сетевом объекте.

Для того чтобы выполнить масштабную фильтрацию спама, оператор сети может наделять правами администратора квалифицированных оконечных пользователей и позволять им конфигурировать правила на своих линиях с поставщиком сети. На маршрутизаторе услуги может быть реализована необходимая аутентификация с целью проверки идентификации пользователя и прав администратора. Только законным пользователям разрешается определение соответствующих правил.

10.9 Юридические действия и правила

Для того чтобы предотвратить спам, важно определить соответствующие регламентарные положения и законы, запрещающие спам, хотя по поводу эффективности этой меры ведутся споры. Многие страны приняли законы, позволяющие жертвам спама предпринимать юридические действия против спама. В большинстве случаев рекламодатель может ввести специальный набор содержаний, из которых получатель сможет распознать спам как рекламу и понести наказание, если это правило нарушится.

Проблема этого метода состоит в том, что довольно трудно выполнять антиспамовые законы для спама, созданного в зарубежных странах. Для того чтобы сделать этот метод действительно эффективным, необходимо подписать некоторые международные соглашения между многими

странами. Международные организации, включая МСЭ-Т, OECD, APEC и т. д., прилагают усилия для определения эффективного антиспамового законодательства, международного сотрудничества и права применения.

Этот метод является не техническим методом, который не зависит от характеристик мультимедийных IP-приложений.

11 Аспекты противодействия спаму в мультимедийных IP-приложениях

Использование IP-сетей для рекламы – это не только экономически выгодно, но и очень эффективно. Спам – это проблема, которая возникает из-за неправильного использования рекламы. Серьезные социальные проблемы могут возникнуть из-за спама. Эти проблемы включают в себя массовость рекламы, фальсификация, обман, которые навязчивы для пользователей и причиняют им ущерб.

В данной Рекомендации описаны различные методы противодействия спаму в мультимедийных IP-приложениях. Мультимедийные IP-приложения имеют различные характеристики, таким образом, присущий им спам также имеет различные характеристики. Используя только один или два метода, невозможно бороться со всеми типами мультимедийного IP-спама. Для того чтобы действительно разрешить или, как минимум, облегчить проблему спама, необходимо провести подробное исследование различных типов спама в различных частях элементов мультимедийных приложений. Следовательно, метод противодействия спаму необходимо проанализировать в соответствии с характеристиками мультимедийных IP-приложений. В данном разделе сделана попытка показать некоторые вопросы, которые должны быть рассмотрены в процессе противодействия спаму в мультимедийных IP-приложениях.

Для того чтобы эффективно противостоять спаму в мультимедийных IP-приложениях, следует рассмотреть различные подходы в различных аспектах групп, участвующих в предоставлении услуги. Это пользователь услуги (и/или абонент услуги), поставщик услуг, оператор сети, общественная организация и рекламодатели. Таким образом, в данном разделе описаны некоторые проблемы, вопросы, которые должны быть рассмотрены в процессе противодействия спаму в мультимедийных IP-приложениях относительно этой проблемы.

11.1 Пользователь услуги (абонент услуги)

Пользователь услуги и/или абоненты услуги – это настоящие жертвы спама, и необходимо осознавать важность блокирования спама для защиты их прав. Существует несколько пунктов, которые должен учитывать пользователь услуги при борьбе со спамом, хотя применение этих предложений будет различным, в зависимости от среды передачи.

– Для блокирования нежелательного спама, пользователи должны использовать программы фильтрации спама и поддерживать их в состоянии, соответствующем современному уровню. Всегда может возникнуть новый спам, поэтому программу фильтрации спама необходимо обновлять, чтобы контролировать новый спам.

– Пользователи должны оформить подписку на различные фильтры спама, такие как черный список, белый список и т. д., и непрерывно обновлять списки в этих фильтрах.

– При появлении спама, пользователи должны его немедленно удалить и сообщить о проблеме, для того чтобы предотвратить появление еще одной такой же жертвы.

– Пользователи должны принимать участие в тренингах по предотвращению спама, для того чтобы узнать о новом спаме и новых методах борьбы. Новые типы спама могут появляться в обычных услугах, а также в новых услугах. Хотя нет необходимости использовать все методы борьбы, но необходимо стараться найти адекватное решение для того чтобы ограничивать спам.

– Пользователи должны быть внимательными, защищая свою личную информацию, которая не должна быть доступна спаммерам. Пользователи не должны применять простые для запоминания или для угадывания типы идентификационных номеров.

– Пользователи должны использовать превентивные методы, для блокировки запросов на соединение от спаммеров, и конфигурировать свою систему так, чтобы спаммеру было сложно установить соединение.

11.2 Поставщик услуг

Поставщики услуг могут получать большую выгоду от предоставления качественной услуги. Спам может причинить серьезный ущерб услуге, поскольку спаммеры используют услугу неправильно и

злонамеренно. Поставщики услуг должны знать о проблеме спама, для того чтобы защитить свою сеть и предоставлять более качественные услуги. Существует несколько пунктов, которые могут учитывать поставщики услуг при борьбе со спамом.

– Прежде чем запускать новую мультимедийную услугу, поставщик услуг может провести анализ возможности того, что новые мультимедийные IP-услуги или приложения станут мишенью для возможного спама. Не каждая мультимедийная IP-услуга является мишенью для спаммеров. Проведя анализ спама и найдя решения, затрудняющие рассылку спама, можно повысить вероятность успеха новых услуг. Если услуга, уязвимая для спама, выводится на рынок без выполнения такого процесса, то может быть очень трудно контролировать спам, и пользователи будут отказываться от новой услуги после того, как в ней будет большую часть составлять спам.

– Поставщики услуг должны проверить все объекты, такие как пользователь, сеть, компоненты услуги и т. д., которые образуют мультимедийную IP-услугу или приложение, и проанализировать различные методы рассылки спама для каждого объекта, для того чтобы найти наиболее простые и эффективные решения противодействия спаму. Можно использовать методы противодействия спаму только в пределах мультимедийной IP-услуги, но лучшие решения могут существовать, когда все элементы сети воспринимаются как единое целое.

– Поставщики услуг могут вести непрерывные исследование появления нового спама в обычных приложениях. Новые типы спама могут появляться даже в самых старых услугах. Поставщики услуг могут пожелать исследовать эти явления и стараться найти решения для борьбы с новыми типами спама, даже в самых старых услугах.

– Поставщики услуг могут использовать различные фильтры, такие как черный список и белый список, для управления доступом пользователей к услугам. Лучше всего не дать спаммеру возможности использовать услугу, поскольку спаммер использует услугу только для достижения своих злонамеренных целей.

– Если услуга содержит процесс подписки, поставщики услуг должны сделать подписку достаточно сложной, чтобы спаммеры не присоединялись к этой услуге. Многие спаммеры используют автоматизированные методы или нанимают дешевую рабочую силу, для того чтобы подписываться на различные услуги, что очень эффективно для рассылки спама. Процесс подписки должен содержать строгие методы аутентификации для проверки абонента и должен иметь некоторую схему для предотвращения многочисленных подписок одного пользователя и, для того чтобы спаммеры не присоединялись к этой услуге.

– Если услуга содержит список пользователей услуги, поставщик услуг может иметь метод оценки степени доверия пользователя услуги для гарантии того, что данный пользователь не будет использовать в своих целях услугу или других пользователей услуги. Поставщик услуг должен иметь метод защиты для предотвращения того, чтобы личная информация абонентов стала доступной внешним или внутренним пользователям.

– Если услуга содержит хранилище, то поставщик услуг может пожелать отслеживать, чтобы содержание веб-сайта контролировалось с целью удаления веб-спама. Анализ содержания может выполняться даже для видео и звуковых данных в целях обнаружения несоответствующего содержания.

– Поставщики услуг могут иметь метод, который использовался бы пользователем услуги для контроля над спамом. Это может быть программа фильтрации, список фильтрации, инструменты определения правил, руководство по борьбе со спамом или что-либо еще, что может применять пользователь для противодействия спаму.

11.3 Оператор сети

Спам может привести к растрате ресурсов сети, особенно, если спам содержит мультимедийный контент. Оператор сети должен стараться блокировать спам для защиты сети и для предоставления эффективных сетевых услуг. Существует несколько пунктов, которые должен учитывать оператор сети при борьбе со спамом.

– Операторы сети могут контролировать трафик в сети для обнаружения аномального трафика, который может считаться спамом. Оператор сети должен иметь возможность анализировать аномальный трафик и предпринимать соответствующие действия. Обнаружить спам путем анализа трафика может быть достаточно сложным делом. Тем не менее, различный злонамеренный спам или программы имеют вид аномального трафика.

– Операторы сети могут ограничивать трафик спаммера или выполнять какие-либо иные действия, для того чтобы остановить рассылку спама.

– Операторы сети могут взаимодействовать с поставщиком услуг, обмениваясь информацией относительно спама. Оператор сети действительно может остановить трафик рассылки спама, что делает саму рассылку бесполезной.

– Операторы сети могут использовать различные формы брандмауэров для защиты сети.

– Сети могут быть сконфигурированы для связи только с доверенными сетями, так что устанавливать соединения могут только аутентифицированные пользователи, которым разрешено это сделать доверенными сетями. Если между сетями существуют доверенные отношения, то сеть может управлять трафиком и пользователями. В итоге, вхождение в сеть может быть защищено от спама и другого злонамеренного трафика, когда все подсети доверяют трафику от своих одноранговых подсетей.

11.4 Общественная организация

Общественная организация может быть правительственной организацией или частной организацией, состоящей из заинтересованных групп, которые работают над проблемой управления спамом. Частная организация может быть коммерческой или некоммерческой организацией, которая обладает эффективными решениями для противодействия спаму. Существует несколько пунктов, которые могут учитывать общественные организации при борьбе со спамом.

– Общественные организации могут иметь систему, позволяющую жертве подать жалобу об ущербе от спама. Организация может предупредить или наказать спаммера. Эта организация может быть правительственной организацией или сильной частной организацией, имеющей власть, для того чтобы предупреждение спаммера было бы эффективным.

– Общественные организации могут иметь программу для обучения или давать какие-либо рекомендации по борьбе со спамом пользователю мультимедийной IP-услуги, поставщикам мультимедийных IP-услуг и операторам IP-сети. Навыки противодействия спаму требуют большего опыта, к чему поставщик мультимедийных IP-услуг или оператор могут быть не готовы.

– Общественные организации могут предоставить черный список или фильтры, которые могут использоваться совместно с широкой публикой. Публика может принимать участие в создании черного списка или фильтров.

– Для рекламных агентств было бы полезно иметь систему одобрения рекламы, которую нельзя подделать, и которая является аутентичной, которую рекламное агентство могло бы использовать, не опасаясь быть принятым за спаммера.

11.5 Другие аспекты

Другими аспектами, которые не зависят от перечисленного выше, могут быть следующие.

– Проблема спама вероятно не исчезнет, несмотря на различные усилия по исследованию проблемы противодействия спаму. Всегда будет появляться новый спам и будут выполняться новые исследования для борьбы с этими проблемами. Но если исследование методов противодействия спаму провести сначала, то можно создать лучшую прикладную среду для лучших прикладных услуг.

– Различные методы противодействия спаму должны использоваться совместно. Пока еще не существует суперрешения, которое способно решить проблему спама. Для борьбы с различными видами спама, которые могут создаваться в различных местах с применением различных методов, различные методы противодействия спаму должны использоваться совместно.

– Оптимальным решением может быть то, которое сделает рассылку спама трудной и дорогостоящей задачей. Окончательной целью спаммера является использование для рекламы дешевого и простого метода. Спаммер, в конце концов, прекратит рассылку спама, если это будет сложным и дорогостоящим делом или если наказание за рассылку спама будет достаточно строгим.

Библиография

[b-ITU-T Q.814] Recommendation ITU-T Q.814 (2000), *Specification of an electronic data interchange interactive agent*.

[b-ITU-T T.124] Recommendation ITU-T T.124 (1998), *Generic Conference Control*.

[b-ITU-T T.180] Recommendation ITU-T T.180 (1998), *Homogeneous access mechanism to communication services*.

[b-ITU-T X.509] Рекомендация МСЭ-Т X.509 (2005 г.) ИСО/МЭК 9594-8:2005, *Информационная технология – Взаимосвязь открытых систем – Справочник: Структуры сертификатов открытых ключей и атрибутов*.

[b-ITU-T X.741] Recommendation ITU-T X.741 (1995) | ISO/IEC 10164-9:1995, *Information technology – Open Systems Interconnection – Systems management: Objects and attributes for access control*.

[b-IETF RFC 1991] IETF RFC 1991 (1996), *PGP Message Exchange Formats*. <http://www.ietf.org/rfc/rfc1991.txt?number=1991>

[b-IETF RFC 3428] IETF RFC 3428 (2002), *Session Initiation Protocol (SIP) Extension for Instant Messaging*. <http://www.ietf.org/rfc/rfc3428.txt?number=3428>

[b-IETF RFC 4871] IETF RFC 4871 (2007), *DomainKeys Identified Mail (DKIM) Signatures*. <http://www.ietf.org/rfc/rfc4871.txt?number=4871>

[b-IETF RFC 4880] IETF RFC 4880 (2007), *OpenPGP Message Format*. <http://www.ietf.org/rfc/rfc4880.txt?number=4880>

[b-IETF RFC 4981] IETF RFC 4981 (2007), *Survey of Research towards Robust Peer-to-Peer Networks: Search Methods*. <http://www.ietf.org/rfc/rfc4981.txt?number=4981>

[b-IETF RFC 5039] IETF RFC 5039 (2008), *The Session Initiation Protocol (SIP) and Spam*. <http://www.ietf.org/rfc/rfc5039.txt?number=5039>

[b-IETF RFC 5090] IETF RFC 5090 (2008), *RADIUS Extension for Digest Authentication*. <http://www.ietf.org/rfc/rfc5090.txt?number=5090>

СЕРИИ РЕКОМЕНДАЦИЙ МСЭ-Т

Серия A	Организация работы МСЭ-Т
Серия D	Общие принципы тарификации
Серия E	Общая эксплуатация сети, телефонная служба, функционирование служб и человеческие факторы
Серия F	Нетелефонные службы электросвязи
Серия G	Системы и среда передачи, цифровые системы и сети
Серия H	Аудиовизуальные и мультимедийные системы
Серия I	Цифровая сеть с интеграцией служб
Серия J	Кабельные сети и передача сигналов телевизионных и звуковых программ и других мультимедийных сигналов
Серия K	Защита от помех
Серия L	Конструкция, прокладка и защита кабелей и других элементов линейно-кабельных сооружений
Серия M	Управление электросвязью, включая СУЭ и техническое обслуживание сетей
Серия N	Техническое обслуживание: международные каналы передачи звуковых и телевизионных программ
Серия O	Требования к измерительной аппаратуре
Серия P	Качество телефонной передачи, телефонные установки, сети местных линий
Серия Q	Коммутация и сигнализация
Серия R	Телеграфная передача
Серия S	Оконечное оборудование для телеграфных служб
Серия T	Оконечное оборудование для телематических служб
Серия U	Телеграфная коммутация
Серия V	Передача данных по телефонной сети
Серия X	**Сети передачи данных, взаимосвязь открытых систем и безопасность**
Серия Y	Глобальная информационная инфраструктура, аспекты протокола Интернет и сети последующих поколений
Серия Z	Языки и общие аспекты программного обеспечения для систем электросвязи

Отпечатано в Швейцарии
Женева, 2009 г.