Министерство образования Республики Беларусь
Учреждение образования
Белорусский государственный университет
информатики и радиоэлектроники

УДК 004.056:681.5

Хасеневич
Борис Бекирович

Методы и алгоритмы шифрования информационных потоков в сети Интернет

АВТОРЕФЕРАТ

на соискание степени магистра технических наук
по специальности 1-98 80 01 – Методы и системы защиты, информационная безопасность

Научный руководитель
Скудняков Юрий Александрович
кандидат технических наук, доцент

Минск 2017

КРАТКОЕ ВВЕДЕНИЕ

Постоянное развитие и совершенствование переносной персональной электроники: планшетов, смартфонов за последнее несколько лет породило огромный потребительский рынок. Сейчас мобильные устройства являются одними из самых популярных способов доступа в сеть Интернет. Ожидается, что через пару лет персональные компьютеры будут генерировать менее половины Интернет трафика, уступая место переносным мобильным устройствам. С распространением Интернета кинотеатрам и телевидению пророчили быструю погибель. Но всемирная сеть не только не привела к краху индустрии, но даже укрепила ее позиции, лишь несколько преобразовав формат: инициативу у «традиционных» телекомпаний перехватывают компании-поставщики фильмов и сериалов на основе потокового мультимедиа, распространяющие свой контент через Интернет.

Защита видео контента остается актуальной темой отрасли. Для того, чтобы защитить видеоданные при передаче через публичные незащищенные сети, существует несколько технических решений. Выбор варианта зависит от множества факторов.

Во-первых, от бизнес-модели вещателя — ставит ли он задачу продавать доступ.

Во-вторых, от того, кто отвечает за сохранность контента. Если защита делается для правообладателя и нужно убедить его, что его контент в безопасности, и за каждый просмотр он получит свои материальные отчисления, то нужно использовать механизмы, которым доверяет правообладатель. Если защита делается для собственных нужд, то можно использовать любые решения.

В-третьих, выбор зависит от бюджета.

Таким образом, необходимо обеспечить защиту контента, при которой доступ будут иметь только те, кто получил на это право, например, кто оплатил просмотр или находится в правильном регионе, для которого поставщик закупает контент и продает рекламу.

ОБЩАЯ ХАРАКТЕРИСТИКА РАБОТЫ

Цель и задачи исследования

Целью настоящей работы стало исследование текущих технических решений на слабые места, выявление потенциально опасных узлов в области информационной безопасности. А также поиск и реализация способов защиты контента на основе алгоритмов и методов шифрования для парирования

потенциальных уязвимостей. Для достижения поставленной цели в этой диссертации решены следующие задачи:

- проведен обзор накопленного опыта в области использования систем защиты контента;
- проведены исследования о области информационной безопасности при передаче видео контента в сети Интернет;
- разработаны технические решения для обеспечения информационной безопасности на основе методов и алгоритмов шифрования информационных потоков в сети Интернет.

Объектом исследования является методы и алгоритмы шифрования информационных потоков в сети Интернет.

Предметом исследования является комплексное техническое решение для обеспечения информационной безопасности при передаче видеоконтента через сеть Интернет с использование шифрования.

Основной *гипотезой*, положенной в основу диссертационной работы, является возможность разработки комплексного технического решения для обеспечения информационной безопасности видео ресурсов в сети Интернет, на основе методов и алгоритмов шифрования информационных потоков. Что предоставляет требуемый уровень безопасности, при минимальных ресурсных затратах. Так же дает возможности для бизнеса получить материальный доход.

Личный вклад магистранта в выполненную работу

Работа полностью выполнена лично магистрантом на базе его исследований, проводимых на работе и на кафедре ЗИ БГУИР.

Публикации результатов диссертации

По теме диссертации опубликовано пять работ в сборниках трудов и материалов международных конференций. Еще одна работа представлена на республиканский конкурс.

Структура и объем диссертации

Диссертация состоит из введения, общей характеристики работы, трех глав, заключения, списка использованных источников, списка публикаций автора и приложения. В первой главе представлен анализ уже существующих подходов, методов защиты видеоконтента в сети Интернет. Вторая глава посвящена анализу угроз информационной безопасности, которыми подвергнуты Интернет

ресуры. В третьей главе предложены алгоритмы и методы шифрования информационных потоков в сети Интернет. Построена комплексная система защиты видеоконтента.

Общий объем работы составляет 70 страниц, из которых основного текста 58 страниц, 16 рисунков на 15 страницах, 2 таблицы и на 2 страницах, список использованных источников из 45 наименований на 5 страницах и 1 приложение на 5 страницах.

ОСНОВНОЕ СОДЕРЖАНИЕ

Во **введении** определена область и указаны основные направления исследования, показана актуальность темы диссертационной работы, дана краткая характеристика исследуемых вопросов, обозначена практическая ценность работы.

В **первой главе** проведен анализ уже существующих решений, используемых для защиты видеоконтента. Выполнен анализ применяемых методов и алгоритмов для обеспечения информационной безопасности.

Было рассмотрено потоковое видео и живая трансляция. Принцип организации ресурсов и их методы работы. Были определены требования к системе защиты контента. Разобрались в современных видео форматах подлежащих защите. Таких как стандарт H. 264, отличающейся высокой эффективностью сжатия видео, относительно предыдущих стандартов, благодаря расширенному списку возможностей обработки исходного видео, таких как:

- Многокадровое предсказание, включающее в себя: использование предыдущего кадра в качестве основы для последующего, обработку только изменяющегося фрагмента кадра с возможностью ссылки на предыдущий кадр до 32 раз и многие другие улучшения;
- Сжатие макроблоков без потерь, за счет более точного описания области макроблока;
- Переменные размеры блока сжатия, что позволяет точно выделить края движущихся объектов;
- Функции устойчивости к ошибкам.

Так как протокол RTP не имеет возможности установления соединения, его использование невозможно без применения дополнительных протоколов, таких как RTSP или SIP:

- Протокол RTSP (Real Time Streaming Protocol), являясь прикладным протоколом, используется для удаленного управления потоком данных с сервера. Как клиент, так и сервер могут создать запрос, используя определенный

формат. Запрос передается в текстовом виде и может содержать дополнительные поля с указанием параметров передачи. Итогом взаимодействия сервера и клиента является установление соединения

- Протокол SIP (Session Initiation Protocol), так же является протоколом прикладного уровня и используется для описания способа установки соединения между двумя и более узлами с целью передачи мультимедийного содержимого. Протокол имеет клиент-серверную архитектуру: клиент запрашивает определенную информацию с сервера; сервер обрабатывает запрос клиента и формирует ответ о возможности установки соединения.

Кроме RTP существует возможность передачи мультимедиа через HTTP, а именно HLS (HTTP Live Streaming). В таком случае установка соединения и передача мультимедийной информации происходят внутри одного протокола. Синтаксис команд схож с RTSP и содержится в заголовке HTTP пакета. Поддержка HLS интегрирована в большинство современных мобильных устройств и медиа проигрывателей, что позволяет широко использовать этот способ передачи потокового мультимедиа, а отсутствие сложностей при использовании портов нестандартных портов снимает ограничение на использование потокового мультимедиа в неподготовленных сетях.

Вторая глава посвящена анализу угроз информационной безопасности. Определены термины и классификация угроз. По природе возникновения принято выделять естественные и искусственные угрозы. Естественными принято называть угрозы, возникшие в результате воздействия на ИС объективных физических процессов или стихийных природных явлений, не зависящих от человека. В свою очередь, искусственные угрозы вызваны действием человеческого фактора. Примерами естественных угроз могут служить пожары, наводнения, цунами, землетрясения и т. д. Неприятная особенность таких угроз – чрезвычайная трудность или даже невозможность их прогнозирования [1, с. 32].

По степени преднамеренности выделяют случайные и преднамеренные угрозы. Случайные угрозы бывают обусловлены халатностью или непреднамеренными ошибками. Преднамеренные угрозы обычно возникают в результате направленной деятельности злоумышленника. В качестве примеров случайных угроз можно привести непреднамеренный ввод ошибочных данных, неумышленную порчу оборудования. Пример преднамеренной угрозы – проникновение злоумышленника на охраняемую территорию с нарушением установленных правил физического доступа [1, с. 41].

В зависимости от источника угрозы принято выделять:

Угрозы, источником которых является природная среда. Примеры таких угроз – пожары, наводнения и другие стихийные бедствия. Угрозы, источником

которых является человек. Угрозы, источником которых являются санкционированные программно-аппаратные средства. Пример такой угрозы – некомпетентное использование системных утилит. Угрозы, источником которых являются несанкционированные программно-аппаратные средства. К таким угрозам можно отнести, например, внедрение в систему «троянских коней» [2, с. 21–25].

По положению источника угрозы выделены:

А) Угрозы, источник которых расположен вне контролируемой зоны. Примеры таких угроз:

– перехват побочных электромагнитных излучений (ПэМИН) или перехват данных, передаваемых по каналам связи;

– дистанционная фото- и видеосъемка;

– перехват акустической информации с использованием направленных микрофонов.

Б) Угрозы, источник которых расположен в пределах контролируемой зоны.

Выделены основные особенности:

- территориальная разнесенность компонентов системы и наличие интенсивного обмена информацией между ними;

- широкий спектр используемых способов представления, хранения и протоколов передачи информации;

- интеграция данных различного назначения, принадлежащих различным субъектам, в рамках единых баз данных и, наоборот, размещение необходимых некоторым субъектам данных в различных удаленных узлах сети;

- абстрагирование владельцев данных от физических структур и места размещения данных;

- использование режимов распределенной обработки данных;

- участие в процессе автоматизированной обработки информации большого количества пользователей и персонала различных категорий;

- непосредственный и одновременный доступ к ресурсам (в том числе и информационным) большого числа пользователей (субъектов) различных категорий;

- высокая степень разнородности используемых средств вычислительной техники и связи, а также их программного обеспечения;

Проведен анализ атак и рисков. На основе чего выработаны методы борьбы с потенциальными угрозами и рисками в области информационной безопасности.

В третьей главе рассмотрена практическая реализация алгоритмов обеспечения безопасности используя общедоступные технологии, которые не нужно покупать, система сможет обеспечить безопасность на должном уровне,

при минимальных денежных вложениях. Нет необходимости приобретать дорогостоящие готовые решения. Также собственная система имеет более гибкое управление и диагностику, за счет отсутствия посредников и открытости компонентов. Архитектура состоит из трех основных частей:

– сервис шифрации контента (сервер) — выполняет предварительную шифрацию контента для распространения по открытым каналам (Интернет) исключительно в защищенном виде;

– сервис выдачи лицензий (сервер) — принимает решение о выдаче (или невыдаче) ключа на дешифрацию видеоконтента в соответствии с бизнес-логикой (правилами распространения контента). Проверяется наличие активной оплаты или достаточность денежных средств у зрителя. Доставка контента осуществляется независимо от его защиты и определяется, прежде всего, бизнес-моделью. Так, один и тот же защищенный контент в разных случаях может предоставляться, как и для скачивания, так и только для потокового вещания. Произведена оценка алгоритма шифрования и реализована система с использованием виртуальной сети доставки контента.

ЗАКЛЮЧЕНИЕ

На основании проведенного анализа были описаны принципы работы интернет ресурсов, актуальные форматы видеоконтента, выявлены возможные угрозы, а также стали понятны текущие принципы и решения по защите видеоконтента. Исходя из этого сформировалось понимание требуемого уровня безопасности на основе текущей ситуации при использовании ресурсов, когда важно обеспечить удобство и ожидание пользователей, требования бизнеса и видение маркетинга. Стал ясен подход других технических решении в обеспечении информационной безопасности. Была реализовано комплексное решение по обеспечению информационной безопасности при передаче информационных потоков в сети Интернет на основе методов и алгоритмов шифрования. Разработаны принципы, алгоритмы и методика функционирования системы защиты видеоконтента и сети доставки контента. Разработана защищенная виртуальная сеть доставки видеоконтента.

СПИСОК ПУБЛИКАЦИЙ СОИСКАТЕЛЯ

Б. Б. Хасеневич, К. А. Володько, А. В. Ковальчук Анализ преимуществ использования платформы Arduino // Информационные системы и технологии: 51-я научная конференция аспирантов, магистрантов и студентов. (Минск, 18 апреля 2015 г.). – Минск : БГУИР, 2015. – С. 70 – 71.

Б. Б. Хасеневич, К. А. Володько, А. В. Ковальчук Опыт создания платформы для обработки и передачи потокового видео через сеть интернет // Информационные системы и технологии: 51-я научная конференция аспирантов, магистрантов и студентов. (Минск, 18 апреля 2015 г.). – Минск : БГУИР, 2015. – С. 72 – 73.

Б. Б. Хасеневич, Ю. А. Скудняков Перспективы использования потокового видеовещания в дистанционном образовании // Дистанционное обучение – образовательная среда XXI века : материалы IX международной научно-методической конференции (Минск, 3-4 декабря 2015 года). – Минск : БГУИР, 2015. – С. 255.

Б. Б. Хасеневич, Ю. А. Скудняков Опыт внедрения системы динамического шифрования видео потоков в сети Интернет // XXII международная научно-техническая конференция «Информационные системы и технологии» ИСТ-2016.-Нижний Новгород: Нижегородский государственный технический университет им. Р. Е. Алексеева, 22 апреля 2016. - С . 316.

Хасеневич, Б. Б. Подходы к созданию защищенной сети доставки контента // Информационные системы и технологии: 52-я научная конференция аспирантов, магистрантов и студентов. (Минск, 16 апреля 2016 г.). – Минск : БГУИР, 2016. – С. 61 – 62.

Ю. А. Скудняков, Б. Б. Хасеневич, И. И. Шпак. Один из подходов организации сетевой образовательной среды // Высшее техническое образование: проблемы и пути развития = Engineering education:challenges and developments: материалы VIII международной научно-методической конференции. (Минск, 17-18 ноября 2016 г.). В 2 ч. Ч. 2 / редкол. Е. Н. Живицкая и др. – Минск: БГУИР, 2016. – С. 182 – 184.