Шпилёв Сергей (гр. 011 , 24 марта 2004 г.)

Методы защиты авторских прав для цифрового видео.

1. Введение.

Эра интернета приносит новую парадигму для распространения видео в мире. Преимущества цифрового кино в отношении производителей и потребителей многочисленны: значительно понижается стоимость распространения и расходы на техническое обслуживание, обеспечивается немедленный доступ к архивам пленки, более высокое качество продукции, и сильный потенциал для развития новых моделей бизнеса. Несмотря на эти преимущества, студии все еще неохотно переходят к цифровым технологиям. Главным недостатком для цифрового кино остается опасность пиратства. Пиратство уже стоит Голливуду миллиарды долларов в год, и цифровое кино без правильного применения, и защиты авторских прав только увеличит эти цифры. В этом эссе, я представляю системы организации защиты авторского права которые направлены на обеспечение набора необходимых мер безопасности: стандартные криптографические основы и механизмы защиты авторского права, которые делают возможным надежное и безопасное распространение видео.

2. Модель и окружающая среда нападения

Цель этого раздела определить цели системы анти пиратства описанной в этом эссе. На абстрактном уровне, D.R.M.(Digital rights management) или подобная технология анти пиратства довольно распространена. Например, данный протокол аутентификации можно использовать независимо от типа содержания, которое передается (видео, тонально-звукового, книги и т.д.) и участников в системе (кино студия или розничный интернет продавец). Однако, конечный успех любой, защитной системы, зависит в первую очередь от своей финансовой осуществимости и применимости в определенных анти-пиратских целях и сильно зависит от окружающей среды, в которой должна работать система. В общем, пиратство в той или иной степени все равно будет присутствовать. Есть море критических факторов, среди которых: стоимость содержания системы и стоимость ее взлома для пиратов, количество пользователей в системе, возможность перераспределения каналов для защиты от пиратства, трудность определения пирата в системе, величина потерь от пиратства при отсутствии защиты. Технология защиты может учесть только часть из этих факторов.

Системы защиты разных типов данных развивались отдельно и независимо и применялись с разным процентом успеха (защита спутникового телевидения, защиты от копирования для видеоигр, содержимое, распространяемое через интернет). Однако оперативные среды этих систем отличаются существенно от среды для цифрового кино.

Первым важным различием является кривая стоимости содержания. Первоначально стоимость каждого нового продукта будет весьма высока (до сотни миллионов долларов для новых выпущенных пленок) и будет спадать очень быстро (миллионы долларов в день). Большинство доходов от фильма получается в течение первой пары недель после выпуска. Затем размеры аудитории заметно снижаются. Например, пленка 'Титаник' Джеймс Камерон принесла 600 миллионов долларов только в Соединенных Штатах, причем 400 миллионов - доход касс в пределах только 2 месяцев с момента своего выпуска. Резкий спад цены ограничивает время, в течение которого защита видео критична. Например, после того как пленка будет выпущена через другие каналы (такие как цифровая передача, DVD), эти слабо защищенные каналы снимают ограничения политики безопасности с продукта.

Вторым, относящимся к окружающей среде параметром, который отличает цифровое кино от наилучшим образом изученных сред анти пиратства, будет относительно малый и ограниченный набор участников (несколько сотен тысяч репроекторов во всем мире против 10 или, возможно, сотни миллионов ТВ спутников). Репроекторы содержат дорогую оптическую аппаратуру, и в меру сложные компоненты анти пиратства не сильно повлияют на суммарную стоимость.

Цель пирата - получить незащищенный экземпляр данной пленки, которую можно распространять без ограничения. В прошлом, пираты использовали разнообразие канала распространения для украденного видео- содержания, включая физическое (продукция и распространение видео - иногда

основано на экземплярах сделанных камерой в кино) и электронное распространение по интернету. Последнее становится особо актуально, в свете широкого распространения сервисов общего доступа, таких как "Gnutella" или "Napster" . Наличие общедоступного и высокого качества экземпляра фильма в интернете вскоре после выпуска в состоянии привести к мульти миллионным потерям для студии.

2.1. Содержимое Задачи Защиты

Основная цель - обеспечить надежное распространение содержания и обеспечить условный доступ к ней. В частность, система должна предотвратить получение пиратами незащищенного варианта, первоначального оттиска с подлинника или экземпляров полученных кино. В то же самое время, нужно понимать, что невозможно обеспечить совершенную защиту. Любой репроектор (и пленки, которые он может получить) можно обойти за определенную сумму. Более того, атака останется незамеченной до тех пор, пока полученный экземпляр не будет растиражирован. Мы предполагаем, что в случае коммерческого тиражирования пиратских пленок, мы можем обнаружить, что пролом происходил.

Точнее, мы должны сделать такую систему, чтобы она удерживала уровень пиратства, даже в случае единичного взлома системы значительно ниже стандартного уровня для обычных систем защиты (процент пиратства для большинства систем ТВ передач лежат между 3% и 10%). Мы увеличиваем робастность системы посредством следующих мер - использование других свойств окружающей среды цифрового кино:

1. Поднимите цену первоначально нападения посредством защитного оборудования. Как сказано выше, высокая цена оптической аппаратуры в сочетании с ограниченным набором участников даетвозможност ь использования более изощренного оборудования, чем был бы возможно в «розничной» окружающей среде. Это может включить так же механические барьеры вокруг репроекторов.
2. Сделайте возможным идентификацию пиратов. Имея экземпляр пиратской пленки, должно быть возможно определить скомпрометированный репроектор, от которого он был получен. Наша система обеспечивает это посредством простых «отпечатков пальцев». Комплиментарный подход лежит в основе тампер очевидного оборудования совместно с процедурой по проверке.
3. Включите дешевое и легкое возобновление системы. После того как взлом был обнаружен, система должна предотвратить скомпрометированные репроекторы от получения новых данных. И вообще, даже в отсутствии взлома, компоненты системы безопасности репроекторов должны изменяться периодически, для того чтобы представить движущуюся мишень для потенциальных атакующих.

Как сказано выше, доля пиратства зависит в основном от нескольких нетехнических параметров , таких как правовая среда и, самое важное, политика предпринимателя для обеспечения доступа операторов к пленке. Огульное распределение пленок неизбежно ведет к более частым актам пиратства, чем при высоко селективной политике.

В основном нападения на системе принимают следующие формы:

- Атакующий извлекает пленку (незащищенный вариант) от правомерного репроектора. Для этой цели, атакующий должен обойти тампер упорное оборудование защищающее репроектор. Наша первая задача - сделать это нападение трудновыполнимым и дорогостоящим. А 2 и 3 пункты направлены на определение и выведение из строя скомпрометированного репроектора.
- Атакующий извлекает секрет аутентификации, который хранят в репроекторе (см. ниже). Это позволяет произвольному приспособлению имитировать скомпрометированный репроектор. Оборона и ответная мера также же, как описано под первым нападением.

Несколькими других обстоятельств могут, в принципе, вести к взлому системы или защищенной пленки, даже если они не будут подвержены нападению в классическом понимании. Они включают:

- Открыто, что криптографический протокол или алгоритм небезопасны. Это очень маловероятно, если использованы стандартные, проверенные криптографические алгоритмы и протоколы.
- Открытие атаки против алгоритма «fingerprinting». Система предвидит эту возможность посредством возможностилегк ого изменения компонентов «fingerprinting».
- Социальное инженерство: Содержание украдено вне системы защиты (в производящей студии). Это тип нападения не влияет на цифровую систему кино и должен быть решен другими средствами.
- Брешь в защите одного репроектора делает возможным скомпрометировать любой репроектор в модели без существенного оборудования. Все подвергшиеся этому репроекторы должны быть заменены.
- Экземпляры копий сделаны от необработанных аналоговых вариантов пленки. Экземпляры, полученные таким образом, имеют относительно плохое качество, и нападение трудно для выполнения без сговора с персоналом кино. Методы fingerprinting (см. выше) могут помочь определить кино, где этот тип нападений происходит часто.

3. Описание Системы

Этот раздел описывает предложенную систему. Система состоит из комплекта безопасных хранилищ или *узлов*, которые используют D.R.M. функциональность, и которые эксплуатируются по-разному участниками (студиями, раздатчиками, кино). Раздел 3.1 определяет узлы и описывает их критические свойства и функциональности, которымиони должны обладать. Мы обращаем особое внимание на узлы внутри кино.

3.1. Возможности Узла

Узел – это хранилище для защищенной информации. Узлу предоставляется возможность доступа к определенной информации. Узел получает доступ только в соответствии с описанием прав доступа, которое происходит от владельца продукта. Мы называем комбинацию тайнописных ключей, которые позволяют доступ к содержимому, и описание прав доступа *лицензией*. A D.R.M. *система - это* набор узлов и их взаимодействий, которые позволяют содержимому передаваться между узлами.

Этот раздел опишет инженерные возможности, которые необходимы для D.R.M. узлов. Помимо этого, мы сфокусируемся на узлах в кино, включая взаимодействия между центральными сервером и отдельными репроекторами.

В общем, участвующие узлы необходимо снабдить следующими возможностями, для того чтобы выполнить цели функциональности и анти пиратства, перечисленные до сих пор:

- Аутентификация
- Правовая политика (лицензирование)
- Кодирование и раскодирование содержимого
- Fingerprinting

3.1.1. Аутентификация

В зависимости от своего места в цепи распределения, узел может действовать как передатчик или приемник содержания. Действуя, как передатчик, узел должен обеспечить проверку, что узел - получатель, которому он передает содержимое - авторизованный (лицензированный) узел, который имеет права доступа. Наоборот, действуя как приемник, узел должен мочь доказать передатчику, что он действительно авторизован. Это требует возможности аутентификации в узлах. Мы основываем аутентификацию на тайнописи открытого ключа. Каждый узел должен хранить (и оберегать) закрытый ключ, иметь соответствующий открытый ключ и выполнять основные виды деятельности с

открытым ключом (кодирование, раскодирование, подписание и проверка). Для этого всего можно использовать простейшие стандартные тайнописные протоколы аутентификации

3.1.2. Управление и лицензирование прав

Однаиз главных целей D.R.M. - позволить предпринимателям определить, как их имущество может быть получено, после того как оно было распространено. Это требует определения официального языка (цифрового языка прав), в котором предприниматели могут указать эти правила доступа и условия (лицензию). Перед тем, как предоставить доступ к любой, информации, D.R.M. узел проверит, позволен ли доступ лицензией.

Типичная лицензия определяет *права доступа* или действия, которые могут быть выполнены с данными. Каждое действие типично сопровождено комплектом *условий*, ограничивающих действия (по времени, количеству операций, оплате). Выполнение некоторых из этих ограничений может требовать наличия секретных счетчиков или скрытых часов. Помимо этого, лицензия может определить, что некоторые действия (ввод отпечатков пальцев) должен быть выполнен над содержимым. Другие элементы политики лицензии могут включить следующее:

- срок действия лицензии;
- ограничение показа по определенным дням и часам;
- выполнение журналов проверки, то есть автоматически записывать названия, времена, продолжительность, и т.д. каждоо показа для каждого репроектора;
- предотвращение показа полного содержания от начала до конца, поэтому кино не может пропускать некоторые места и разделы видео - в частности титры и предупреждения;
- использование определенного типа репроекторов (гарантирующих качество, размер индикации, размер аудиторий)
- Требования к некоторым характеристикам.

Более того, лицензия обычно определяет набор правил или вещей, к которым относится лицензия. Обычно, принцип определяется узлом или набором узлов.

Лицензия должна быть защищена тайнописными средствами, для того чтобы обеспечить свою целостность при передаче через незащищенные каналы от предпринимателя через промежуточные узлы к репроектору. Стандартной цифровой подписи достаточно для этой цели. Содержимое ключей раскодирование может связать с правилами лицензии таким же механизмом. Язык прав "XrML" имеет все свойства описанные в этом разделе.

3.1.3. Кодирование и раскодирование содержимого

Как сказано выше, узлы обеспечивают хранилища, которые могут доставлять содержимое (например, пленки). В незащищенном пространстве между узлами, содержимое защищается посредством кодирования с ключами, которые доступны только узлам, которым предназначено послание. Таким образом, узлы должны мочь кодировать и раскодировать содержимое (пленки). Способность узлов оберегать закрытые ключи - это дело стандартных тайнописных шифров. Требования к рабочим характеристикам и форме, в которой хранится пленка, могут привести к дополнительным ограничениям на шифр и могут заставить его обязательно оставить некоторые участки пленки незашифрованными.

3.1.4. Fingerprinting

Как описано в разделе 2, мы должны учесть возможность того, что некоторые отдельные узлы могут быть скомпрометированы. "Fingerprinting" данных, будет нашим главным инструментом для идентификации скомпрометированных узлов. Таким образом, по крайней мере, некоторые узлы должны мочь ввести водяные знаки в данные. Раздел 4 даст детальное описание fingerprinting в предложенной системе.

3.1.5. Восстанавливаемость и управление ключами

Цель восстанавливаемости - она должна позволить защитить всю систему от разных типов нападений, которые будут возможны всегда. Стратегия управления ключами должна быть такой, что по возможности в случае взлома, он должен быть ограничен в пределах конкретного узла, и восстановление должно быть быстрым и дешевым. В случае появления произвольного набора скомпрометированных узлов, должно быть, возможно, предотвращение получения ими нового содержимого без влияния на остальные узлы. Это означает, что каждый узел должен иметь *уникальную* пару ключей. Таким образом, если одиночный узел скомпрометирован, то его ключ можно аннулировать без влияния на любой другой узел. Аннулирование происходит во время аутентификации, когда проверка целостности открытого ключа приемника включает проверку, содержится ли этот открытый ключ в перечне аннулируемых скомпрометированных ключей. Данные по аннулированию должны криптографически быть связаны с содержимым.

Некоторые из нападений описанных в разделе 2 приводят к глобальным проломам, которые требуют, чтбы каждый узел был возобновлен. Нападения этого типа включают взлом одного из тайнописных алгоритмов используемых системой или нападения на уровне оборудования. Систему необходимо установить, так чтобы эти нападения были весьма редки и маловероятны. Выбор правильных тайнописных алгоритмов дает очень высокий уровень гарантии против взломов с этой точки зрения. Широко распространенное оборудование кодирования должно быть предохранено комбинацией технических и правовых механизмов. Во всяком случае, компоненты, которыми обеспечены узлы, должны быть сборными, чтобы их можно было заменить независимо от других компонентов (оптического оборудования репроектора).

Считается, что существующие алгоритмы watermarking и fingerprinting обычно гораздо менее крепки, чем тайнописные алгоритмы. Таким образом, компонент fingerprinting узлов должны быть легко обновляемы.

4. Содержание fingerprinting цифровое аудио/видео.

Для соблюдения авторского права для мультимедиа, мы не можем единственно положиться на традиционные методы защиты данных, такие как кодирование или перестановка, потому что мультимедиа окончательно будет сыграна в правильном порядке и раскодированой форме. Поэтому, во всех случаях возможно записать нормальное содержание, в худшем случае путем записи с аналогового выхода, воспроизводящего приспособления. Подходом, который может сдержать такие нападения перезаписи является введение watermarks/fingerprints в само содержание.

Отпечатки пальцев использованы для обеспечения соблюдения авторских прав посредством возможности автору определить происхождение объекта пиратства. В обычном сценарии защиты, всем потребителям предоставляется по разному экземпляру содержания, где каждый экземпляр содержит "fingerprint" - потребитель специфический водяной знак. Если неавторизованный клиент перераспространяет содержимое с отпечатками пальцев, уникальность их позволяет определить злостного клиента. "Fingerprints", как раз как водяные знаки, должны быть:

- **Надежными:** вероятность ложного обвинения потребителя в пиратстве должна быть как можно меньше (по крайней мере 10^{-12}), но сохранять твердую уверенность в обнаружении зложелательных потребителей даже после мощных атак на fingerprinted содержимое (по крайней мере 10^{-3}).
- **Крепким** к общему изменению (сжатие, преобразование формата, фильтрация) и различным злонамеренным нападкам (рассинхронизация и т.д.);
- **легка в обнаружении:** в отличие от watermark, которые проверяются на клиенте перед проигрыванием содержания, отпечатки пальцев обнаруживаются на сервере после того как пиратство было выявлено, таким образом они не обнаруживаются в реальном времени; помимо этого, детектор отпечатков пальцев позволяет сравнить 'атакованное' содержание с оригиналом;
- **Незаметность** для потенциальной аудитории и всех аналитических средств; важно усвоить что полная незаметность для статистических инструментов может быть трудна в

достижении особенно в случаях когда функция плотности вероятности первоначального сигнала хорошо известна.

В виду того, что группа клиентов может эффективно убирать втихомолку метки путем совместного использования своих экземпляров, важно чтобы шифрование отпечатков пальцев былокак можно лучше:

- **сопротивление сговору:** определено как число экземпляров которое можно совместно использовать с произвольным лучшим алгоритмом для того чтобы привести к в новому экземпляру все еще показывающему по крайней мере один из отпечатков пальцев,
- **отслеживаемость:** взяв пиратский экземпляр должно быть возможно указать по крайней мере одного из сговорщиков с некоторой незначительной вероятностью не заметить все злобные нападки примененные в процессе сговора (рассинхронизация, сжимание); и
- **Доказуемость:** не существует группы потребителей, которая могла бы создать пиратский экземпляр провоцирующий невиновного потребителя.

Важный асимптотический верхний предел на сопротивление fingerprinted материалу был установлен "Ergun":

$$K : O\left(\sqrt{\frac{n}{\ln(n)}}\right)$$

где K - сопротивление сговору и n соответствует к длине объекта. Очевидно, этот верхний предел устанавливает сильный предел эффективности любого механизма fingerprinting. В конце этого раздела, мы кратко рассматриваем методы watermarking как технологии маркировки для содержимого и методы "fingerprints" как методы для увеличения сопротивления сговору.

4.1. Watermarking

Схемы watermarking полагаются на несовершенство системы людского восприятия (НСЛВ). Многочисленные системы скрытия исследуют факт того, что НСЛВ (как для слухового, так и для визуального) нечувствительны к малым изменениям амплитуды, или даже временным или частотным областям, так же, как к вставке временных областей низкой амплитуды. Модуляция информации обычно использует: широкодиапазонную модуляцию (ШД) или модуляцию индекса квантования (МИК). Преимущества ШД и МИК watermarking включают: проверка водяных знаков не требует оригинала и трудно извлечь врезанную информацию, использующую оптимальный статистический анализ. Помимо этого, ШД обнаружение watermark исключительно упорно к нападениям, можно модулировать как масштабирование времени и частот с флуктуациями, так и добавлением или умножением на шум.

Недостатки включают: watermarked сигнал должен быть идеально синхронизирован с watermark, и нужно достигнуть достаточно малой вероятности ошибки, длины сигналов могут быть довольно большими, увеличивая сложность обнаружения и задержки. Наибольший недостаток обеих схем - то, что они не BORE -упорные (BORE - сломанный однажды отработает везде), то есть путем взлома одиночного видео можно извлечь втихомолку информацию (ключ, использованный для получения последовательности ШД или скрытых квантователей в МИК) и воссоздать оригинал (ШД) или создать новый экземпляр наведения МИК, для того чтобы обработать содержимое как непомеченное. Для того чтобы обойти эту проблему, недавно несколько асимметричных схем watermarking были начаты, но с меньшим успехом. Удачный способ решения - вопрос BORE -сопротивления не играет значительной роли, когда watermarks использованы как "fingerprints", по мере того как процесс обнаружения полностью выполнен на стороне сервера.

5. Заключения

В этом эссе я описал метод сокрытия для цифровых видео и мультимедиа вообще. Мы детализировали основные компоненты системы. Наша цель была предоставить обзор общего принципа защиты цифрового кино. Мы рассмотрели действительно мощную и высокоуровневую модель для безопасности оборудования.

6. Использованная литература.

1. “Digital rights management for digital cinema” (Darko Kirovski, Marcus Peinado[2], Fabien A. P. Petitcolas).

2. The Motion Picture Association of America (August 31, 2000). http://www.mpaa.org/dcinema.

2. B. Fox, ‘The pirate’s tale,’ New Scientist, December 1999. http://www.newscientist.com/ns/19991218/thepirates.html
3. M. G. Kuhn, ‘Attacks on Pay-TV Access Control Systems,’ Security Seminar, Computer Laboratory, Cambridge 9 December 1997. http://www.cl.cam.ac.uk/~mgk25/vc-slides.pdf