Спутниковое телевидение, нелегальный просмотр

Обзор Videocrypt

подготовил Андрей Б. Аюпов 917группа

Введение

Videocrypt – это система скремблирования платного телевидения, разработанная Thomson Consumer Electronics совместно с News Datacom. Более миллиона пользователей получают зашифрованный Videocrypt сигнал и эта система, и сейчас, остается достаточно безопасной из многих подобных ей структур, защищающих права компаний спутникового телевидения.

Требования.

Videocrypt – стандарт многоформатного вещания, который подходит для PAL, NTSC и SECAM передач. Язык – также не барьер для VideoCrypt, который имеет возможность передачи на многих языках и имеет утилизированное многоязыковое понятное меню.

Особенности и применение.

Smart-карта является главным ключом к системе Videocrypt. Smart-карта имеет большое множество вариантов применений: она специально кодируется (до реализации) для реализации всех потребностей определенного пользователя. Карта может быть впоследствии может быть улучшена станцией телевизионного вещания по мере необходимости.

Существует несколько режимов вещания станции, которые понимает и обрабатывает smart-карта:

- Простой режим (Clear mode);
- Режим посылки сигнала, различаемого декодерами и передача на экран без дальнейшей обработки;
- Режим передачи кадров вместе с ключом шифрования, которые впоследствии попадают на экран, расшифрованные декодером.

Контроль доступа.

Доступ к зашифрованным кадрам определяется соответствующим уровнем доступа smart-карты пользователя. Незашифрованный сигнал не может быть передан без предшествующей авторизации пользователя. Программы могут быть легко приспособлены к системе Videocrypt и система также очень гибка для операторов

платного телевидения. Несколько возможных уровней доступа предлагаются как стандартные:

* Single or multiple subscriptions with many tier levels in one channel

* Pay Per View (PPV) and impulse purchasing

* Thematic selection (enable all arts programming)

* Geographic limitation (restrict to a country/area)

* Single-event (throwaway cards)

* Parental Control (reception with card only)

* Pre-determined time period

Videocrypt позволяет предварительным программированием smart-карты разрешить специфические требования пользователей.

Smart-карта является ключом безопасности и доходов операторов. Соответствующая безопасность обеспечивается многими уровнями, которые использует smart-карта. Они включают:

- Chaining (стадии получения карты)
Потенциальный потребитель хотел бы получить новую карту, которая содержит часть нового кода. Но оставшийся код передается оператором только в момент, когда карта находится в декодере. Только потом пользователь компилирует код, имея инструкцию и элементы графики на дисплее.

- Over-the-air addressing (адресация)
Системные операторы могут обратиться к определенному пользователю, что является большим преимуществом перед другими системами скремблирования. Оператор может обеспечить пользователю дополнительные услуги, отсылать индивидуальные сообщения, «черные» и «белые» списки зрителей.

- Cloning (клонирование)
Несколько заметных продвижений для прекращения клонирования карт произошли за последнее время. Физическая защита (physical deterrent) является первым элементом защиты: интегральная микросхема, которую содержит карта, очень чувствительна к «исследованиям» взломщика, она может быть легко повреждена в подобном процессе зондирования.

Стоимость является вторым фактором, который защищает легальных производителей от хакеров, клонирующих карты. Много времени, проблем и финансов нужно затратить для клонирования карты.
Разработчики рекомендуют менять карту каждые полгода, и каждый такой раз секретный алгоритм (о котором упоминается позже) также меняется. Любые декодеры пиратов за эти полгода будут позже просто бесполезны. И любой пиратский декодер должен содержать уникальный код, который впоследствии, скорее всего, будет помещен в «черный список», в результате звонков недовольных пользователей!☺

Далее, перейдем к деталям данного формата шифрования!

Принцип шифрования

Videocrypt кодирует ТВ кадр путем «разрезания» каждой линии кадра на две подлинии в какой-то точке разреза, затем меняет их местами и так для каждой линии кадра.
Например, если линия сигнала выглядела до шифрования так:

0123456789

и пройдя через кодирование, выход может быть таким:

4567890123

где каждая цифра представляет собой пиксель кадра. Существует 256 таких точек разреза, и она должна быть на определенном расстоянии от границы линии кадра (минимальная дистанция от границы 12-15% ширины кадра). Это причина того, что иногда вы можете видеть вертикальные участки подобия оригинальной картинки.

Несколько раз в секунду, компьютер на удаленной станции генерирует 32 байтное сообщение, которое он шифрует и передает вместе с информацией корреляции ошибок в первых невидимых строках кадра ТВ сигнала подобно телетексту. Примерно каждые 2.5 секунды одно из таких 32 байтных сообщений обрабатывается в декодере секретным алгоритмом хеширования, который преобразует данные 32 байта в 60-битное значение. Эти 60 бит далее используются вторым алгоритмом для получения 8-битового значения точки разреза, которая согласуется со следующей линией каждые 2.5 секунд. Никаких деталей о втором алгоритме пока неизвестно, но будем полагать, что это 60-битный генератор псевдослучайных чисел, где 60-битное значение используется как зерно (стартовое значение) этого генератора.

Декодер получает сообщение 32 байта и другую информацию с ТВ сигналом, применяя некоторые алгоритмы коррекции ошибок, и передает все 32 байтные пакеты на smart-карту, находящуюся в определенном для этого слоте. Smart-карта реализует такой же алгоритм хеширования как и тот, который использовался на кодирующей стороне и получает такое же 60-битное значение. Используя это переданное smart-картой значение, декодер может генерировать с таким же генератором псевдослучайных

чисел точку разреза соответствующей строки кадра. Далее декодер перемещает две линии от этой точки разреза и восстанавливает исходный кадр. Секретная хеш-функция является криптостойким элементом данной системы. Функция сделана так, что почти невозможно догадаться об ее действии, анализируя множество пар 32байта/60бит значений.
Не говоря уже о источнике создания 60-битных значений, сообщения из 32 байт, присылаемые удаленным источником, содержат номера карт, для того, чтобы можно было адресоваться к индивидуальной карте, и также они содержат команды, такие как активация, деактивация и изменения номера аккаунта. В дополнении, 32-байтные пакеты содержат цифровую подпись (на данный момент 4 байта), которая позволяет карте определить, действительно ли данное сообщение пришло от удаленной стороны, а не сгенерировано кем-то, анализирующим карту. Опять же, цифровая подпись, как и хеш-функция, сконструирована так, что сложно симулировать такую подпись, посмотрев на некоторое количество ее вариантов. Это предотвращает систему от атак, когда кто-то хочет определить секретную хеш-функцию и генерировать новые команды активации для карты.

В начале 1993 года, кому-то удалось взломать систему и получит доступ к секретной хеш-функции для некоторых станций, которые использовали Videocrypt(British Sky Broadcasting, Adult Channel, JSTV, BOB, Red Hot TV). Большинство из этих систем использовали одни и те же алгоритмы хеш-функции и цифровой подписи, разница между станциями была только в разных таблицах 32-байтных секретных ключей. Неизвестно, как тот человек получил такую информацию. Или кто-то из компании, кто разрабатывал карты, распространил такую информацию, или кто-то прочитал содержимое EEPROM для процессора карты (очень сложно, но теоретически возможно). С такими данными было очень просто хакерам клонировать карты. Это были простые PCB с микроконтроллером, который вырабатывает секретную хеш-функцию, серийные процедуры ввода-вывода и 60-битное значение из 32-байтного сообщение, ну вообщем все то, что необходимо для работы такой карты. Для некоторых каналов, такие карты-клоны доступны до сих пор, но BSkyB выпустила новую серию 09 карт весной 1994 и изменила алгоритм хеш-функции и подписи на новые. Каждый раз, карты-клоны переставали работать и, вообще, это занимало много времени, чтобы получить доступ к новым секретным данным.

Карты-клоны не выполняли каких-нибудь процедур, интерпретирующих активацию, деактивацию и другие подобные функции, поэтому их программное обеспечение было значительно проще, чем на настоящих картах. Это привело к тому, что немного разные реакции возвращали настоящая карта и карта-клон на патологические 32-байтные сообщения. Этим конечно же пользовались владельцы каналов, и запрещали удаленно такие карты. Но было очень просто каждый раз находить такие баги в обеспечении карт-клонов и исправлять их.

Вся система Videocrypt очень безопасна по своей структуре, так как все секретные части для правильного расшифровывания находились на smart-карте и если секретные алгоритмы хеш-функции становятся, вдруг известны, то они могут очень динамично быть заменены другими, и тогда компании просто высылают пользователям новые карты. Такая замена также имеет смысл, когда детали о формате команд скрытых в 32-байтной последовательности становятся известными; это позволяет, зная алгорим цифровой подписи, создавать новые сообщения активации и фильтровать сообщения деактивации карты.

Однако существует по-крайней мере две недоработки в секретности данной системы, которые не могут быть исправлены путем замены карт:

1) Диалог между картой и декодером одинаково синхронизирован для всех Videcrypt декодеров, подключенных к какому-нибудь каналу. Это значит, что декодер не добавляет никакой специфической информации карты или своей в поток. Т.е. есть возможно записывать 32-байтные сообщения, пересылаемые удаленным источником в течение какого-нибудь вечера, затем отослать эти сообщения кому-нибудь с оригинальной картой и попросить его карту ответить 60-битными сообщениями на каждое записанное 32-байтное сообщение. Если потом отослать уже 60-битные сообщения назад, то вы уже сможете легко дескремблировать записанную прежде программу того вечера. Также есть возможность передавать такие 60-битные ответы в реальном времени по кабелю на многие декодеры в доме или радио-сигналом на еще большие расстояния.
2) Такой элемент в шифровании, как разрезание и перестановка и факт, что соседние линии кадра почти идентичны, делает возможным перебрать все 256 возможных точек разреза и выбрать такой вариант, где они больше всего совпадают. Такой метод уже реализован на быстрой машине с framegrabbers, которая загружает изображение в память и далее показывает уже скорректированное изображение на мониторе. На параллельных суперкомпьютерах можно добиться декодирования в реальном времени. Однако, в таком методе возможны некоторые потери качества.

Оба таких метода были реализованы, и пользуются популярностью на данный момент.

Используемая литература:

http://www.cl.cam.ac.uk/~mgk25/

http://www.cl.cam.ac.uk/~mgk25/nagra.pdf

Markus Kuhn –
Analysis of the Nagravision Video Scrambling Method discusses methods of how to decode in realtime without a regular decoder box the pay-TV conditional access system used for instance by the German broadcaster *Premiere*.

Attacks on Pay-TV Access Control Systems was a talk that was presented 1997-12-09 in the Cambridge Security Seminar

Darren Ingram – Videocrypt (An Overview)