СРАВНИТЕЛЬНЫЙ АНАЛИЗ АЛГОРИТМОВ ШИФРОВАНИЯ MPEG ВИДЕОДАННЫХ

А.А. БОРИСКЕВИЧ, И Ю. Г.КОЧУБЕЕВ

Сетевые приложения мультимедиа, такие, как Видео-По-Требованию, широковещательная передача видео и видеоконференции требуют проведения исследований в области безопасности мультимедиа. Из-за особенностей мультимедийных данных возникает необходимость в разработке специальных алгоритмов шифрования *MPEG* видеоданных, которые должны быть одновременно высокозащищенными, высокоскоростными и не ухудшать уровень сжатия.

Стандарт *MPEG* является одним из наиболее универсальных принятых международных стандартов для кодирования и передачи динамических видеоизображений. Предлагается следующая классификация современных методов шифрования *MPEG* данных:

1) методы, использующие особенности формата *MPEG*;

2) методы, основанные на статистических особенностях потока *MPEG*;

3) методы, использующие возможности кодирования при шифровании *MPEG* видеоданных.

Рассмотрен селективный алгоритм шифрования наиболее важных частей потока *MPEG* (*I*-кадров), относящийся к первой группе. Он обеспечивает четыре уровня защиты с разным объемом шифруемой информации. Представителем второй группы является алгоритм видео шифрования (*VEA*), использующий шифры с разной вычислительной сложностью и обеспечивающий высокое быстродействие (на 48 % быстрее прямого шифрования), высокую защищенность. К третьей группе относится алгоритм с изменяемой моделью адаптивного кодека (*ИМАК*), обеспечивающий высокую скорость, защищенность и не увеличивающий исходный поток данных. Он основан на применении для каждого байта не сжатой информации своей таблицы Хаффмана.

Из сравнительного анализа следует, что более предпочтительными по всем критериям являются алгоритмы *VEA* и *ИМАК*. Они обеспечивают высокую защищенность наряду с высоким быстродействием и малым размером зашифрованного потока *MPEG*.

МАГНИТНАЯ ЗАЩИТА НОСИТЕЛЯ ИНФОРМАЦИИ НА ОСНОВЕ ИМПУЛЬСНОГО МАГНИТНОГО МАРКЕРА

А.А. БОРИСКЕВИЧ, В.Я. КУЛИК

Метод защиты основан на имплантировании в материальный носитель информации маркера со специфической магнитной структурой, обеспечивающей эффект быстропротекающего перемагничивания вещества маркера. Данный эффект наблюдается в виде скачкообразного изменения намагниченности при помещении маркера в переменное магнитное поле. Магнитная структура маркера, представляющая собой два или больше доменов, намагниченных встречно, идентифицирует носитель. Под воздействием внешнего возбуждающего магнитного поля в направлении намагниченности одного из доменов при пороговом значении поля происходит спонтанное перемагничивание домена с противоположным полю исходным направлением намагниченности. Такой процесс повторяется при циклическом перемагничивании маркера.

При помещении считывающей обмотки вблизи маркера в момент его скачкообразного перемагничивания поместить в ней возбуждается импульс напряжения. Форма и другие характеристики импульса существенно зависят от материала маркера, его геометрии, способа и режимов его получения, обработки сигнала с выхода приемной катушки.

К достоинствам магнитной защитной маркировки на основе импульсного магнитного маркера следует отнести стабильность параметров регистрируемого импульса напряжения, технологичность получения и встраивания маркера в корпус носителя, высокую надежность, объективность и бесконтактность контроля подлинности.

ОБЕСПЕЧЕНИЕ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ НА АТС

Д.В. ШИПОВАЛОВ

В докладе рассматривается некоторые аспекты обеспечения информационной безопасности *АТС*, которая должна достигаться с помощью системы комплексной защиты информации (*КЗИ*) от перехвата информации в каналах связи, несанкционированного доступа к информации, утечки информации по побочным каналам, внедрения специальных технических устройств перехвата информации, программно-технических воздействий и программ-вирусов. Исследуются вопросы защиты от наличия в составе программного обеспечения (*ПО*) возможных программных закладок (*ПЗ*), активация которых может дезорганизовать работу как отдельной станции, так и всей сети.

Рассматривается необходимость реализации на *АТС* ряда эксплуатационных правил, регламентирующих периодическое выполнение копирования на специально выделенный внешний носитель (*ВНН*) рабочих областей оперативного запоминающего устройства (*ОЗУ*), станционных управляющих устройств, а также областей *ОЗУ*, хранящих программы, текущие переменные и постоянные данные о ресурсах станции и системы.

В докладе предлагаются методы действия персонала при обнаружении признаков активации *ПЗ*.

Исследуется необходимость разработки, и внедрения технических средств познакового документирования всей вводимой с пультов информации с жестким непрерывным административным контролем регламента пультового времени.

Также в докладе рассматриваются аспекты защиты информации исключением передачи по *ОКС* № 7 от международного центра коммутации к станциям *АМТС* сообщений с нетелефонными функциями (для предотвращения активации *ПЗ*, форматов *TCAP* и *OMAP*). В докладе предлагается разработка и установка на международном участке специальных тестирующих устройств, обеспечивающих обнаружение и фиксацию всех случаев передачи нетелефонных сообщений четвертого уровня.

Рассматривается обеспечение защиты от несанкционированного доступа к передаваемой информации, которое может быть достигнуто обнаружением искажений в передаваемой информации, реализуемое, например, методом контрольных сумм.

Литература

1. Технические аспекты защиты информации в АТСЦ-90 // http://kiev-security.org.ua
2. Бобов М.Н., Конопелько В.К. Обеспечение безопасности информации в телекоммуникационных системах. Мн.: БГУИР, 2002, 164 с.

ВЫБОР СТРУКТУРЫ АППАРАТНЫХ СРЕДСТВ ЗАЩИТЫ ИНФОРМАЦИИ В СИСТЕМАХ ВИДЕОКОНФЕРЕНЦИЙ

В.Е. САМСОНОВ, В.С. ШАРАК

В связи с широким распространением систем видеоконференций актуальной задачей является обеспечение защиты сетевого трафика в этих системах. Повышенные требования к пропускной способности сетевой инфраструктуры видеоконференций требуют аппаратной реализации криптографической защиты сетевого трафика.

В докладе изложены результаты экспериментальных работ по аппаратной реализации криптографической защиты информации на сетевом уровне стека протоколов TCP/IP для использования в системах видеоконференций.

Экспериментальный образец устройства выполняет все функции интерфейса PCI шины и управляется драйвером ядра ОС Windows NT, 2000.

Были исследованы такие параметры как скорость аппаратного шифрования одного, скорость преобразования одного IP-пакета, время выполнения передачи пакета в память ЭВМ в режиме DMA, время реакции на прерывания устройства в т.ч. по завершению DMA, а также различные варианты построения драйвера устройства в операционных системах Windows NT, 2000. На основании проведенных оценок выбрана оптимальная структура устройства и метод построения драйвера, позволяющих эффективно производить криптографическое закрытие информации в системах видеоконференций.

ВНЕДРЕНИЕ ВОДЯНОГО ЗНАКА В ПО НА ОСНОВЕ ИСПОЛЬЗОВАНИЯ СТАТИСТИЧЕСКИХ СВОЙСТВ ИСПОЛНЯЕМОГО КОДА

С.С. ПОРТЯНКО

Уже на протяжении многих лет компании, разрабатывающие ПО с целью его продажи, теряют значительную часть доходов из-за компьютерного пиратства. Для того, чтобы препятствовать незаконному тиражированию ПО и для идентификации своих продуктов с целью обеспечения возможности доказательства принадлежности ПО разработчику, чьей интеллектуальной собственностью оно является, используется ряд методик. К их числу относится использование программно-аппаратных ключей (Software Dongles), стеганографические методы, такие как внедрение водяных знаков (watermarks) и "отпечатков пальцев" (fingerprints).

Предлагаемый метод идентификации исполняемого кода приложения является адаптацией основной идеи метода Patchwork, предложенного в [1] применительно к графическим изображениям, к использованию её для внедрения в код программы некоторого признака, характеризующего её принадлежность тому или иному разработчику. Метод основан на использовании статистических свойств исполняемого кода программы, определяющихся частотами встречаемости той или иной команды при осуществлении их случайной выборки.

Проведённые экспериментальные исследования показали, что для конкретной программно-аппаратной платформы распределение инструкций в исполняемых файлах имеет определённый вид, незначительно меняющийся от приложения к приложению.

Непосредственно внедрение водяного знака в программу заключается в модификации вида распределения индексов команд для некоторого подмножества команд программы, полученного в результате случайной выборки, таким образом, что бы оно существенно отличалось от типичного распределения команд для исполняемых файлов для данной программно-аппаратной платформы.

Для того, что бы при статистическом анализе исполняемого кода перейти от символик либо кодов инструкций к числам, производится назначение каждому типу команды индекса.