УДК 004.056:004.89

ИССЛЕДОВАНИЕ РЕАЛИЗАЦИИ ПРИМЕНЕНИЯ СТЕНОГРАФИЧЕСКИХ МЕТОДОВ В DLP СИСТЕМЕ

Чуб В. С., Галушка В. В.
Донской государственный технический университет, Ростов-на-Дону, Российская Федерация
vadim-chub13@mail.ru
galushkavv@yandex.ru

Рассмотрены и проанализированы: строения функциональности DLP-системы, методы использования стенографии, уровни контроля DLP-системы

Ключевые слова: стенография конфиденциальность, алгоритм, системный анализ.

UDC 004.056:004.89

STUDY OF IMPLEMENTATION OF VERBATIM METHODS IN DLP-SYSTEM

Chub V. S., Galushka V. V.
Don State Technical University, Rostov-on-Don, Russian Federation

vadim-chub13@mail.ru
galushkavv@yandex.ru

The paper considers and analyzes the structure of DLP-system functionality, methods of verbatim usage, and control levels of DLP-system.

Keywords: verbatim , analysis, confidentiality, system analysis

Введение. Если анализировать все данные внутри информационной системы организации, возникает проблема избыточной нагрузки на IT-ресурсы и персонал. DLP-система должна уметь отличать конфиденциальную информацию от неконфиденциальной. DLP работает, в основном, «в связке» с ответственным специалистом, который не только «учит» систему корректно работать, вносит новые и удаляет неактуальные правила, но и проводит мониторинг текущих, заблокированных или подозрительных событий в информационной системе.

Функциональность DLP-системы строится вокруг «ядра» — программного алгоритма, который отвечает за обнаружение и категоризацию информации, нуждающейся в защите от утечек. В ядре большинства DLP-решений заложены две технологии — лингвистического анализа и технология, основанная на статистических методах. Также в ядре могут использоваться менее распространенные техники, например, применение меток или формальные методы анализа [3-1].

Разработчики систем противодействия утечкам дополняют уникальный программный алгоритм системными агентами, механизмами управления инцидентами, парсерами, анализаторами протоколов, перехватчиками и другими инструментами такими как стенографические инструменты.

Стенография — это наука, изучающая методы передачи скрытой цифровой информации [1-2]

Скрытая (стеганографическая) передача информации относится к процессам, которые реализуют методы передачи информации, в которых дополнительная информация может передаваться в структуре данных, представленной в цифровой форме и используемой в качестве контейнера, главным образом из-за их избыточности. Контейнер (охватывающий объект) — это цифровые данные, использование избыточности которых позволяет передавать дополнительную информацию без обнаружения факта передачи. Контейнер, который не содержит дополнительной информации, называется пустым, в противном случае он заполняется [1].

В целях использования цифровых и компьютерных методов стеганография обычно признается в трех областях:

– встраивание скрытых каналов передачи информации. Цель — встраивание скрывает наличие информационной передачи;

– встраивание цифровых (водяных) знаков (СЕН). Цель встраивания состоит в проверке подлинности передаваемых данных и предотвращении несанкционированного доступа к ним;

– встраивание уникальных идентифицирующих знаков. Цель состоит в скрытой аннотации и аутентификации передаваемой информации [1].

Исследования в области цифровой стеганографии посвящены встраиванию конфиденциальных сообщений и цифровых водяных знаков в статическую графику, например, в форматы, не использующие сжатие, хотя на данный момент встраивается большое количество информации алгоритмы и водяные знаки в файлы изображений форматов, использующих сжатие с потерями [1].

Один из методов, применяемых для скрытого текста, — метод LSB (наименьший значимый бит, наименьший значащий бит). Этот параметр заключается в замене последних значащих битов на контейнеры (изображения, аудио или заметки) на биты скрытого сообщения [2].

Младший бит. Известно, что человек в крайне редких случаях не способен заметить изменения в этом бите. На самом деле NSB является шумом, поэтому его можно использовать для встраивания информации, заменяя менее значимые биты изображениями на биты секретного сообщения. Количество встроенных данных может составлять 1/8 от общего объема контейнера.

DLP-системы с помощью стенографии отлавливают зашифрованную информацию различными методами.

– Метод лингвистики. Используется для стоповых словосочетаний, для блокировки исходящей электронной почты на почтовых серверах. Его можно считать прародителем современных систем DLP. Конечно, это не защищает от злоумышленников. Удаление стоповых словосочетаний, которые чаще всего переводятся в отдельный штамп документа, происходит легко и значение текста вовсе не изменяется.

– Метод статистики. Статистические технологии рассматривают тексты не как связную последовательность слов, а как произвольную последовательность символов, поэтому они одинаково хорошо работают с текстами на любых языках. Поскольку любой цифровой объект, даже изображение или программа, также являются последовательностью символов, одни и те же методы можно использовать для анализа не только текстовой информации, но и любых цифровых объектов.

Ранние DLP-системы базировались на одном методе в ядре — лингвистическом или статистическом анализе. На практике недостатки двух технологий компенсировались сильными сторонами друг друга, и эволюция DLP привела к созданию систем, универсальных в плане «ядра».

Определить какие технологии присутствуют в ядре можно по описанию возможностей конкретного DLP-комплекса [1].

Не меньшее значение, чем функциональность ядра, имеют уровни контроля, на которых работает DLP-система, приведены на рис. 1.

	• уровень сети, когда контролируется сетевой трафик в информационной системе;
	• уровень хоста, когда контролируется информация на рабочих станциях.

Рис. 1. Уровни контроля

Разработчики современных DLP-продуктов отказались от обособленной реализации защиты уровней, поскольку от утечки нужно защищать конечные устройства и сеть.

Сетевой уровень контроля при этом должен обеспечивать максимально возможный охват сетевых протоколов и сервисов. Речь идет не только о «традиционных» каналах (почтовые протоколы, FTP, HTTP-трафик), но и о более новых системах сетевого обмена (Instant Messengers, облачные хранилища). К сожалению, на сетевом уровне невозможно контролировать шифрованный трафик, но данная проблема в DLP-системах решена на уровне хоста.

Контроль на хостовом уровне позволяет решать больше задач по мониторингу и анализу. Фактически ИБ-служба получает инструмент полного контроля за действиями пользователя на рабочей станции. DLP с хостовой архитектурой позволяет отслеживать, что копируется на съемный носитель, какие документы отправляются на печать, что набирается на клавиатуре, записывать аудиоматериалы, делать снимки экрана. На уровне конечной рабочей станции перехватывается шифрованный трафик (например, Skype), а для проверки открыты данные, которые обрабатываются в текущий момент и которые длительное время хранятся на ПК пользователя.

Помимо решения обычных задач, DLP-системы с контролем на хостовом уровне обеспечивают дополнительные меры по обеспечению информационной безопасности: контроль установки и изменения ПО, блокировка портов ввода-вывода и т.п.

Минусы хостовой реализации в том, что системы с обширным набором функций сложнее администрировать, они более требовательны к ресурсам самой рабочей станции. Управляющий сервер регулярно обращается к модулю-«агенту» на конечном устройстве, чтобы проверить доступность и актуальность настроек. Кроме того, часть ресурсов пользовательской рабочей станции будет неизбежно «съедаться» модулем DLP. Поэтому еще на этапе подбора решения для предотвращения утечки важно обратить внимание на аппаратные требования.

Таким образом, принцип разделения технологий в DLP-системах остался в прошлом. Современные программные решения для предотвращения утечек задействуют методы, которые компенсируют недостатки друг друга. Благодаря комплексному подходу, конфиденциальные данные внутри периметра информационной безопасности становится более устойчивыми к угрозам.

Библиографический список

1. Абазина, Е. С. Цифровая стеганография: состояние и перспективы [Лектронный ресурс] / Е. С. Абазина, А. А. Ерунов. — Режим доступа : https://cyberleninka.ru/article/n/tsifrovaya-steganografiya-sostoyanie-i-perspektivy (дата обращения :25.03.2019).

2. Конахович, Г. Ф. Компьютерная стеганография. Теория и практика / Г. Ф. Конахович, А. Ю. Пузыренко. — Москва : МК-Пресс, 2006. — 288 с.

3. Грибунин, В. Г. Цифровая стеганография / В. Г. Грибунин, И. Н. Оков, И. В. Туринцев. — Москва : Солон-Пресс, 2002. — 272 с.