УДК 004

Несостоятельность DLP-систем

А. Ю. Чадов
Московский физико-технический институт (государственный университет), Москва, Россия

Рассмотрены методы защиты, применяемые в DLP-системах, и показана их неспособность противостоять инсайдерам.

Ключевые слова: DLP-системы, инсайдеры, защита конфиденциальных данных.

DLP (*Data Loss Prevention*) системы — это системы, предназначенные для предотвращения утечек конфиденциальных данных из информационного пространства заказчика. Предполагается перекрытие любых утечек, будь то инсайдерские действия или просто халатность и неаккуратность сотрудников [1—3].

Основным способом защиты является анализ сетевого трафика и информации, циркулирующей внутри сети. Есть несколько различных подходов:

- *Сигнатуры*

Самый простой метод — поиск в потоке данных последовательности символов (слова). Чаще всего идет поиск нескольких слов, оценивается частота их появления в тексте. К достоинствам можно отнести простоту пополнения словаря. К недостаткам — усложнение применимости для русского языка за счет изменения формы слова в различных контекстах.

- *«Цифровые отпечатки»*

Из «стандартного» документа при помощи некой преобразующей функции создается «цифровой отпечаток». Затем в фильтрации документов указывается процентное соответствие шаблону, таким образом, отслеживаются все похожие документы. При таком подходе нет необходимости в работе с лингвистикой, но нужно постоянно обновлять базу шаблонов, в больших компаниях это становится проблемой.

- *«Метки»*

Суть метода в расстановке специальных меток внутри файлов. Из достоинств — высокое качество детектирования. Но для расстановки меток внутри файла придется значительно менять инфраструктуру внутренней сети.

- *Регулярные выражения*

Метод позволяет производить поиск по форме данных, а не по самим данным. Удобен для поиска номеров телефонов, паспортов, кредитных карт. Из минусов — узкая область применения.

Все эти методы действенны, если документ передается в открытом виде. Если же инсайдер имеет опыт и технические знания, то, очевидно, отправлять защищаемую *DLP*-системой информацию в открытом виде он не станет.

Элементарная программа перезапишет весь документ побуквенно в обратном порядке, вставит двойной пробел после каждого 3-го символа, заменит все буквы "а" на "о", и наоборот, и документ можно свободно отправлять, например, по почте. Даже достаточно простая обратимая корректировка текста позволит обойти сигнатурный анализ и анализ регулярных выражений. Если же изменять файл в байтовом представлении, то обходятся "метки" и "цифровые отпечатки". Можно применить любые методы шифрования и изменения файла, включая, к примеру, вложение в архив с паролем.

Но наиболее интересными являются методы достаточно развитой сейчас стеганографии. К примеру, достаточно легкий в реализации метод *LSB*. Обнаружить информацию, передаваемую таким способом, несложно, но лишь при целенаправленном поиске. В противном случае информация уйдет вовне незамеченной. При этом для обнаружения придется затрачивать дополнительные ресурсы на анализ трафика, к тому же, замедляется, скорость передачи. Существует множество других алгоритмов встраивания информации, под каждый из которых нужно изменять систему, усложняя ее раз за разом.

Важным моментом является то, что почти все перечисленные способы не представляют большой сложности для реализации. Любой, кто целенаправленно хочет вынести информацию и знает о наличии *DLP*-системы в компании, может позволить себе ими воспользоваться. Можно было бы

Чадов Антон Юрьевич, студент 4 курса, кафедра защиты информации.
E-mail: ar_igul@mail.ru

Статья поступила в редакцию 14 июня 2014 г.

внедрять такие системы секретно, но такое их использование в общем случае может противоречить некоторым законам, связанным с тайной связи, тайной частной жизни, и во избежание проблем фирме придётся дополнительно регламентировать отношения с сотрудниками, в результате чего о наличии системы станет известно.

Еще одной важной частью *DLP*-системы является архивация. Трафик полностью или частично дублируется на сервера архивации, где с ним может работать аналитик. Но, очевидно, что использовать это можно лишь для выявления источника утечки. Данная мера никак не поможет предотвратить уход информации из системы.

С другой стороны, нельзя сказать, что *DLP*-системы бесполезны. Есть множество ситуаций случайных утечек информации: сотрудник случайно отправил по почте защищаемый документ не на тот адрес, при сканировании большого объема бумаг случайно среди прочих попали документы, содержащие конфиденциальную информацию, сотрудник принес из дома вирус на съемном носителе. *DLP*-система отследит эти ошибки и заблокирует попадание охраняемых данных наружу, как и во множестве других случаев, где возможность утечки информации открылась не по злому умыслу, а из-за халатности и неосторожности людей.

DLP-системы сейчас достаточно сильно распространены, а компании, поставляющие их на рынок, имеют постоянный доход. Плохо то, что создатели *DLP*-систем почти всегда обещают защиту от инсайдеров и даже делают на этом упор в представлении своих продуктов, хотя очевидно, что такие продукты могут гарантировать защиту лишь от случайной утечки и не могут обеспечить защищенность от мотивированных злоумышленников, по крайней мере, имеющих минимальные знания и навыки.

Литература

1. Статья "Защита информации от инсайдеров с помощью программных средств". http://www.securitylab.ru/contest/289337.php

2. Статья "Находка для шпиона". http://rg.ru/2012/06/26/insayd.html

3. "DLP системы или «Сожалеем, но у вас уже все украли»" http://daily.sec.ru/2013/06/04/Vasiliy-Kravets-OKB-SAPR-DLP-sistemi-ili-Soshaleem-no-u-vas-ushe-vse-ukrali.html

Insolvency of DLP systems

A. Yu. Chadov
Moscow Institute of Physics and Technology (State University), Moscow, Russia

My article is a little reflection *on the topic of inconsistency of DLP systems. It considers defense methods applied in such systems and shows their inability to resist insiders.*

Keywords: DLP systems, insiders, protection of confidential data.

Bibliography —3 references. *Received June 14, 2014*