УДК 004.7.056 + 004.357.056 Вестник УрФО № 3(21) / 2016, с. 4–9

Захаров А. А., Несговоров Е. С., Оленников Е. А., Фучко М. М., Широких А. В.

АУДИОВЫХОД КАК СКРЫТЫЙ КАНАЛ УТЕЧКИ ДАННЫХ: ТЕХНОЛОГИИ СОЗДАНИЯ И МЕТОДЫ ЗАЩИТЫ

В статье исследуется возможность создания канала утечки информации через аудиовыход компьютера. Производится анализ существующих средств защиты информации на наличие контроля описанного канала. Предлагается технология, позволяющая преобразовывать данные в формат аудиофайла с их последующей скрытой передачей за пределы охраняемой зоны. Рассматриваются методы защиты от утечки через аудиовыход на всех этапах передачи данных: на уровне файловой системы, пользователей и процессов, звуковой подсистемы ОС. Предлагается методика контроля доступа обращений приложений к звуковой карте как расширение возможностей DLP систем.

Ключевые слова: *канал утечки информации, аудио выход, скрытая передача данных, DLP-система, контроль доступа к звуковой карте.*

Zakharov A. A., Nesgovorov E. S., Olennikov E. A., Fuchko M. M., Shirokih A. V.

AUDIO OUTPUT AS HIDDEN CHANNEL OF THE INFORMATION LEAKAGE: CREATION TECHNOLOGY AND SECURITY TECHNIQUES

In the article researched the opportunity of creation of a data leakage channel using an audio output of PC. Analyzed a possibility of existing means of protecting information to monitor the channel. Offered a technology which coding a data into an audio file and transfer it out of a secure area. Considered means of prevention data leakage using the audio output at all stages of the data transmission: at the file system level, in the context of users and processes, in the OS sound subsystem. Offered a sound card access control technique as expanding of available DLP-system features.

Keywords: *channel of the information leakage, audio output, secure communication, DLP system, sound card access control.*

Введение

Утечка конфиденциальных данных способна нанести существенный ущерб организации. Аналитики компании Zecurion Analytics отмечают [1], что в связи с кризисом участились случаи, когда сотрудники из опасения за собственное будущее копируют и уносят конфиденциальную информацию, реализуя достаточно сложные нетиповые схемы.

Для уменьшения рисков утечки данных компании применяют как организационные регламенты, так и программно-технические средства защиты, в частности, DLP (Data Leakage Protection – защита от утечки данных) системы. Например, программное обеспечение Cisco Security Agent (CSA) на уровне хоста составляет таблицы с информацией обо всем том, что происходит в системе с целью контроля заранее заданных правил доступа к файлам, приложениям, сетевыми транзакциями, доступом к реестру, использованием ядра, доступом к COM объектам, интерфейсам и т.п. Причем контролируются действия, совершаемые не только пользователем, но и злонамеренным кодом. Если обнаружено, что запрос не может быть разрешен в соответствии с локальной политикой безопасности, то действие блокируется и посылается сообщение о неверном поведении системы [2]. Аналогично работает DeviceLock DLP. Программа позволяет управлять доступом ко множеству интерфейсов, любым типам принтеров, к мобильным устройствам, к дисковым накопителям, устройствам Plug-and-Play и перенаправляемым терминальным устройствам [3].

Технологическая возможность использования аудиоканала в качестве сети передачи информации раскрывается в работах [4-7]. В частности, в работе [7] описывается механизм построения скрытых сетей на основе звуковых высокочастотных неслышимых каналов в обход существующей сетевой инфраструктуры, раскрывается опасность утечки данных через такие сети и приводятся методы возможного противодействия.

Вместе с тем, при отказе от использования "воздушного зазора" как среды передачи отпадает необходимость применять высокочастотный неслышимый звук, и предложенный в работе [7] в качестве защиты метод высокочастотной фильтрации просто не будет работать.

Постановка задачи

Целью данной работы является демонстрация схемы утечки данных через аудиовыход и анализ возможных механизмов защиты.

Пусть требуется скопировать файл с конфиденциальной информацией по аудиоканалу без использования "воздушного зазора", а программно-аппаратное обеспечение отвечает следующим требованиям:

Атака (кража конфиденциальной информации) исполняется на компьютере под управлением Microsoft Windows.

На жестком диске компьютера располагается текстовый файл с конфиденциальной информацией, которую необходимо скопировать, и злоумышленник имеет права на чтение данных из этого файла.

Отсутствует возможность отправить файл на принтер, скопировать на накопители, передать по сети или запустить стороннюю программу, например с флэш носителя.

На компьютере установлен браузер с поддержкой HTML-5 и текстовый редактор, с помощью которого злоумышленник может написать небольшой скрипт.

На компьютере имеется звуковая плата и разъем аудиовыхода.

У злоумышленника есть устройство аудиозаписи с возможностью прямого подключения через аудио кабель.

Отметим, что ситуация достаточная типичная, поскольку текстовый редактор присутствует в любой программной среде. На большинстве современных компьютеров имеется встроенная звуковая плата, а подключение аудио кабеля, как правило, не расценивается как угроза.

Возможный механизм реализации угрозы

Для реализации угрозы злоумышленник с помощью текстового редактора создает html-файл для копирования файла с конфиденциальной информацией, используя тот факт, что объект FileReader с помощью объектов File или Blob, позволяет веб-приложению асинхронно читать содержимое файлов, хранящихся на компьютере пользователя. Подробно этот небольшой скрипт описан, например, в [8]. Далее полученные данные кодируются в структуру формата Data-URL [9], содержащую WAV файл [10], который можно воспроизвести со страницы браузера. Размер создаваемого злоумышленником html-файла будет не более двух страниц.

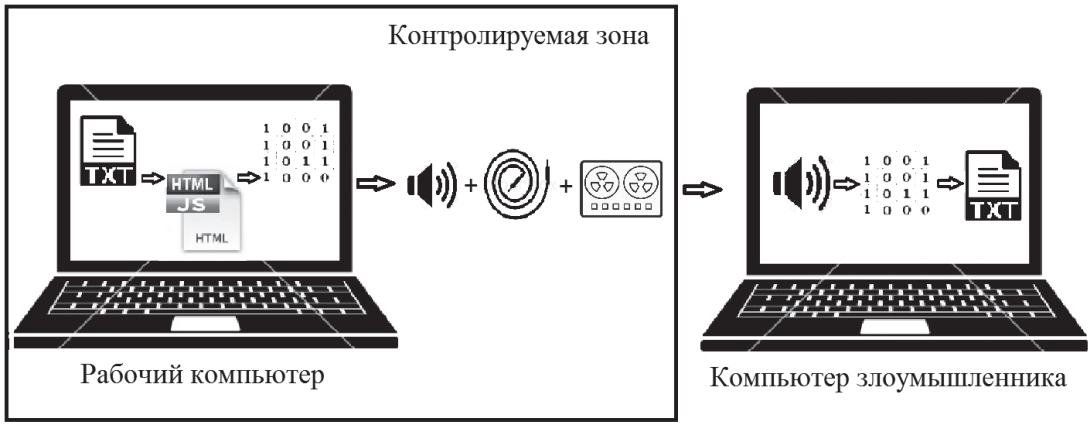

Рис. 1. Схема копирования файла

На Рис. 1 представлена схема копирования файла с конфиденциальной информацией. К компьютеру через аудио кабель подсоединяется цифровое звукозаписывающее устройство. Проигрываемая аудиозапись попадает на вход звукозаписывающего устройства, при этом поток данных не контролируется со стороны DLP систем. Устройство с записью выносится за пределы охраняемой зоны. Звуковой файл обрабатывается и декодируется в первоначальный вид.

На рис. 2 представлен результат работы тестового JS скрипта. Содержимое текстового файла кодируется в одноканальный аудио WAV файл с глубиной звучания 16 бит и частотой дискретизации 44100 Гц, путём преобразования набора битов в массив 16-битных чисел. Файл проигрывается JS скриптом и записывается на диктофон. Видно, что модуляция в записанном файле осталась неизменной. Изменилась амплитуда сигнала на отдельных отрезках, что является допустимым для декодирования полученной информации обратно в текстовый файл.

Реализация защиты от утечек данных через аудиовыход в модуле DLP

Главным недостатком использования DLP решений считается невозможность контроля всех каналов утечки данных, поскольку процесс реализации контроля над новыми каналами утечек осуществляется медленно. Количество возможных каналов утечек значительно превышает реализованный функционал защиты даже у самых продвинутых DLP систем [11]. Дополнительно возникает сложность централизованного администрирования настроек DLP на большом количестве хостов. У компаний, имеющих большое количество сотрудников и/или сложную структуру, появляются естественные трудности с администрированием правил на хостах. В любом случае нужны организационные меры для создания единых защищенных хранилищ конфиденциальных данных с последующей настройкой аудита. Если же хостов, обрабатывающих конфиденциальную информацию, немного, то при правильной настройке DLP можно добиться высокой степени защищенности.

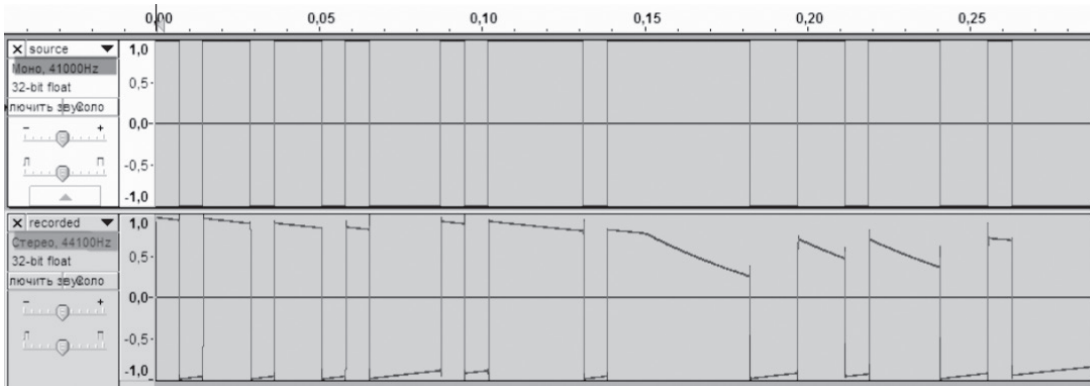

Рис. 2. Соответствие созданного и записанного аудиофайлов

Независимо от наличия мониторинга выбранного злоумышленником канала передачи, обеспечение безопасности на уровне обращений к контролируемым файлам позволяет перекрыть каналы потенциальных утечек и с большой вероятностью определить нарушителя в случае неправомерных инцидентов.

Стандартные средства Windows позволяют контролировать доступ к объектам файловой системы на уровне пользователей [12]. Современные DLP системы и программные средства защиты (например, Secret Net) расширяют возможности, предоставляя более удобную и гибкую настройку правил безопасности [13], обеспечивают возможность ограничения доступа процессов и потоков к защищаемым ресурсам на основании списка запрещённых и разрешенных приложений. Для звуковой платы будем руководствоваться правилом белого списка - "всё что не разрешено - запрещено".

Для предотвращения утечки на уровне звуковой подсистемы ОС нами предлагается два варианта расширения возможностей использования DLP систем: *белый список и помехи*.

Механизм "белый список", работающий в пространстве пользователя, можно реализовать следующим образом:

На основе политики безопасности определяем набор разрешенных приложений, например, можно только Webex, Skype или Viber.

В модуль анализа системных вызовов добавляется контроль функций, связанных со звуковой системой. Для этого создаётся динамическая библиотека, в которой реализуются копии методов работы со звуком, имеющие идентичную сигнатуру. Среди используемых функций можно выделить waveOutOpen (используется для получения устройства вывода) и waveOutWrite (отправляет аудио данные в устройство вывода) из мультимедиа библиотеки Winmm.dll.

В каждый процесс системы подгружается созданная библиотека, и стандартные функции подменяются копиями. Это можно сделать, используя только стандартные средства Windows, например, заменой в таблице импорта функций адресов вызовов оригинальных функций на адреса реализованных нами. Также вызов можно перенаправить с помощью модификации кода. Достаточно получить адрес функции, и непосредственно в памяти изменить первые несколько байт на конструкцию вида "JUMP addr", где addr - адрес вызова нашей функции, при этом сохранив начальное значение. С помощью начального значения, в последствии, можно будет вызывать оригинальную функцию [14].

Внутри наших функций выполним проверку идентификатора и/или имени вызывающего процесса или исполняемого файла со значениями, полученными из локальной базы данных, например, файла или реестра. Если процесс ограничен администратором, то через SetLastError выставляется код ERROR_ACCESS_DENIED и возвращается значение, обозначающее ошибку. Таким образом дальнейшая работа нарушается, а иначе происходит вызов оригинальной функции.

Для осуществления всех действий описанный процесс должен инициироваться с повышенными привилегиями, например, из службы Windows. Любой доступ к звуковому устройству в системе будет надёжно обрабатываться системой защиты.

Для реализации помех в аудио потоке предлагается использовать следующий подход:

На схеме внутреннего устройства аудио подсистемы Windows представленной в MSDN Microsoft [15], демонстрируются технологии пространства пользователя, используемые для работы со звуком, а также путь, который звуковые данные проходят от приложения до устройства вывода. Показано, что в ОС семейства Windows NT все аудио потоки приложений сначала попадают в общий буфер данных, где операционная система производит их микширование в общий выходной формат, и затем отправляются на звуковой драйвер и в устройство вывода.

Windows Audio Session API представляют собой низкоуровневые методы взаимодействия со звуковой системой. Объекты, реализующие интерфейс IAudioRenderClient, позволяют получать буфер данных, посылаемых на устройство воспроизведения [16]. Чтобы изменить звук, отправляемый на аудиовыход, необходимо создать приложение, которое в отдельном потоке, используя технологию WASAPI, получает и преобразовывает аудиоданные в системе следующим образом: постоянно, либо предварительно проводя анализ всех запущенных процессов, приложение получает звуковые данные и изменяет их, добавляя помеху в общий пул звуков, например, повторяя каждый n-й бит информации,

чтобы исказить попадающий на аудиовыход сигнал и усложнить процесс декодирования.

Поскольку для злоумышленника ключевым свойством передаваемых данных является целостность, то искажение исходящего из аудиовыхода сигнала с помощью создания помехи, в простейшем случае, когда злоумышленник записывает звук на диктофон, делает процесс декодирования невозможным.

Для борьбы с помехами злоумышленнику придётся добавлять дополнительные механизмы обеспечения целостности - создавая помехоустойчивый код, который практически невозможно набрать вручную.

Заключение

Рассмотренный канал утечки данных через аудиовыход не контролируется современными средствами защиты и может представлять потенциальную угрозу для информационной безопасности. Описаны технологии, позволяющие в качестве механизмов защиты от этой угрозы использовать белые списки, а также структура и алгоритм работы модуля для DLP приложения позволяющего за счет внесения помех значительно усложнить процесс декодирования информации, получаемой с аудиовыхода.

Примечания

1. См.: Утечки конфиденциальной информации в России и в мире. Итоги 2016 года. URL: http://www.zecurion.ru/upload/iblock/1e5/Zecurion_Data_Leaks_2016_full.pdf (дата обращения: 10.06.16).

2. См.: Cisco Security Agent Version 4.5 // Cisco. URL: http://www.cisco.com/c/en/us/products/collateral/security/security-agent/product_data_sheet09186a008033a40f.html (дата обращения 10.06.16).

3. См.: Основные функции и возможности DeviceLock Endpoint DLP Suite // DeviceLock DLP. URL: http://www.devicelock.com/ru/products/features.html (дата обращения: 10.06.16).

4. См.: A. Madhavapeddy, D. Scott, A. Tse, and R. Sharp. Audio Networking: The forgotten wireless technology // IEEE Pervasive Computing, vol. 4, no. 3, pp. 55–60, July 2005. doi:10.1109/MPRV.2005.50.

5. См.: H. Yan, S. Zhou, Z. J. Shi, and B. Li. A DSP implementation of OFDM acoustic modem // in Proc. Second Workshop on Underwater Networks, New York, USA: ACM, 2007, pp. 89–92. doi: 10.1145/1287812.1287831.

6. См.: C. V. Lopes and P. M. Aguiar. Acoustic modems for ubiquitous computing // IEEE Pervasive Computing, vol. 2, no. 3, pp. 62–71, 2003. doi:10.1109/MPRV.2003.1228528.

7. См.: Michael Hanspach and Michael Goetz, «On Covert Acoustical Mesh Networks in Air,» Journal of Communications, vol. 8, no. 11, pp. 758-767, 2013. doi: 10.12720/jcm.8.11.758-767.

8. См.: Robert Gravelle. Read Text Files Using the JavaScript FileReader // HTML Goodies: The Ultimate HTML Resource. URL: http://www.htmlgoodies.com/beyond/javascript/read-text-files-using-the-javascript-filereader.html#fbid=b2UHVUNmNZ1 (дата обращения: 10.06.16).

9. См.: RFC 2397. The «data» URL scheme // IETF Tools. URL:https://tools.ietf.org/html/rfc2397 (дата обращения: 10.06.16).

10. См.: Структура WAV файла // Audio Coding. URL: http://audiocoding.ru/article/2008/05/22/wav-file-structure.html (дата обращения: 10.06.16).

11. См.: Шемчук Е. В чем кризис DLP-технологий? // Журнал «Information Security/ Информационная безопасность». – 2015. – №3 – С. 26-27.

12. См. Windows Access Control Model // Microsoft Developer Network. URL: https://msdn.microsoft.com/en-us/library/windows/desktop/aa374876(v=vs.85).aspx (дата обращения 4.07.16).

13. См.: Средства разграничения доступа Secret Net // СЗИ Код безопасности. URL: http://www.securitycode.ru/products/secret_net/sredstva-razgranichenija-dostupa/ (дата обращения 4.07.16).

14. См.: Jeffrey Richter, Christophe Nasarre, Windows via C/C++, 5th ed., Redmond, WA: Microsoft Press, 2007. pp. 581-630.

15. См.:"User-Mode Audio Components" // Microsoft Developer Network. URL: https://msdn.microsoft.com/en-us/library/windows/desktop/dd316780(v=vs.85).aspx (дата обращения 4.07.16)

16. См.: Rendering a Stream // Microsoft Developer Network. URL:https://msdn.microsoft.com/en-us/library/windows/desktop/dd316756(v=vs.85).aspx (дата обращения 4.07.16).

Александр Анатольевич Захаров, доктор технических наук, профессор, заведующий кафедрой информационной безопасности ФГАОУ ВО «Тюменский государственный университет», 625003 Тюменская область, г.Тюмень, ул.Володарского, д. 6. E-mail: azaharov@utmn.ru.

Андрей Валерьевич Широких, кандидат технических наук, доцент кафедры информационной безопасности ФГАОУ ВО «Тюменский государственный университет», 625003 Тюменская область, г.Тюмень, ул.Володарского, д. 6. E-mail: maxwide@utmn.ru.

Евгений Фёдорович Попов, аспирант кафедры информационной безопасности ФГАОУ ВО «Тюменский государственный университет», 625003 Тюменская область, г.Тюмень, ул.Володарского, д. 6. E-mail: efpopov@gmail.com.

Михаил Михайлович Фучко, аспирант кафедры информационной безопасности ФГАОУ ВО «Тюменский государственный университет», 625003 Тюменская область, г.Тюмень, ул.Володарского, д. 6. E-mail: fuchkomm@gmail.com.

Несговоров Евгений Сергеевич, студент по направлению "Информационная безопасность" ФГАОУ ВО «Тюменский государственный университет», 625003 Тюменская область, г.Тюмень, ул.Володарского, д. 6. E-mail: evgeniyasheis@gmail.com.

Alexander Zakharov, doctor of Technical Sciences, Professor, Head. the Department of Information Security, Tyumen State University, 625003, Tyumen Region, Tyumen, Volodarskogo St., 6. E-mail: azaharov@utmn.ru.

Andrey Shirokih, candidate of Technical Sciences, Associate Professor, Tyumen State University, 625003, Tyumen Region, Tyumen, Volodarskogo St., 6. E-mail: maxwide@utmn.ru.

Mikhail Fuchko, postgraduate Student of the Department of Information Security, Tyumen State University, 625003, Tyumen Region, Tyumen, Volodarskogo St., 6. E-mail: fuchkomm@gmail.com.

Evgeniy Popov, postgraduate Student of the Department of Information Security, Tyumen State University, 625003, Tyumen Region, Tyumen, Volodarskogo St., 6. E-mail: efpopov@gmail.com.

Evgeniy Nesgovorov, student in the direction of «Information Security», Tyumen State University, 625003, Tyumen Region, Tyumen, Volodarskogo St., 6. E-mail: evgeniyasheis@gmail.com.