Распределенная система защитных механизмов программного комплекса «Голосовая почта» на базе структуризации звукового потока волн

А. И. Думанский, email: dum_a_i@inbox.ru
Н. Е. Балакирев, email: balakirev1949@yandex.ru
М. В. Зеленова, email: businkakatilas@mail.ru
К. А. Лазунин, email: 07121917@mail.ru
М. М. Фадеев, email: fadeev_mix@bk.ru

Московский авиационный институт
(национальный исследовательский университет)

Аннотация. *На сегодняшний день в мире функционирует большое количество программных средств для обеспечения голосового общения пользователей через Интернет. Они обеспечивают высокий уровень качества, доступности и беспрерывности связи. Однако остается главный вопрос защищенности передаваемой личной информации пользователей от злоумышленников, которые имеют широкий перечень программных средств, инструментов, знаний и навыков в вопросах возможных уязвимостей аппаратно-программных средств. Они перехватывают, удаляют, изменяют и используют в корыстных целях конфиденциальную информацию пользователей. Задавшись вопросом о первопричине такой ситуации, был проанализирован весь путь перемещения информации и были определены возможные точки уязвимостей при приеме и передаче информации. Было констатировано, что необходимо защищать не только саму передаваемую информацию, но и программные средства. Кроме этого, необходимо рассредоточить зоны ответственности при передаче информации между участвующими сторонами, что возможно только при индивидуализации программных продуктов. Речь идет о единственности существования экземпляра программы, предоставляемой пользователю при сохранении общей сущности выполняемого алгоритма. Безусловно, предполагается соблюдение определенных условий внешнего характера, включая юридическую и организационную поддержку, выходящую за рамки компетенции специалистов программной отрасли. Для отработки предложенных моделей функционирования, методов защиты и других решений был реализован модельный программный комплекс «Голосовая почта».*

Ключевые слова: *голосовая почта, конфиденциальная информация, голосовое общение, методы защиты, индивидуализация программы.*

Введение

Массовый переход к использованию программных средств требует от производителей всё более пристального внимания к выявлению уязвимостей с целью выработки защиты от несанкционированных угроз и различных утечек. Можно привести множество примеров утечек конфиденциальной информации, и с каждым годом их количество и величина наносимого пользователю ущерба растут.

Наиболее критичными с точки зрения защиты информации являются системы, которые обеспечивают коммуникацию между отдельными пользователями либо группами пользователей. Утечка конфиденциальной информации может произойти в момент отправки сообщения («прослушка»), в момент передачи по линии связи к серверу (присоединение к линии), перехват на поле сервера, при передаче по линии связи к получателю (присоединение). Кроме этого, её могут передать злоумышленникам сами участниками общения или программы-«жучки», находящиеся на их компьютерах. Таким образом, в случае попытки найти точку утечки информации, если не касаться чисто технической стороны, источником расследования может быть сам файл (протокол передачи информации) и программный продукт, который является одной из копий, возможно, миллиона экземпляров одной программы. Отдельным вопросом является вмешательство в коммуникацию «пранкеров» (телефонных хулиганов), выступающих в качестве подставных лиц на принимающей или передающей стороне, что также находится в контексте выше обозначенных проблем. Отсутствие четко определенных мер ответственности за неправомерные действия в отношении к конфиденциальной информации усложняет применение наказания к злоумышленникам.

Для обеспечения всесторонней защиты конфиденциальной информации пользователя необходимо выполнить следующие действия:

1. Обеспечить два вида защиты информации (в нашем случае голосовой): защиту в виде кодирования и защиту в виде маркировки самой информации (нанесения водяного знака).
2. Обеспечить два вида защиты программ: защитить ее от анализа и индивидуализировать для привязки экземпляра программы к конкретному пользователю.
3. Обеспечить одновременную взаимозависимость участвующих сторон (отсутствие одной из сторон блокирует весь процесс) и

распределение ответственности в случае утечки информации при наличии подтверждающей документальной информации.

4. Описать и сертифицировать способы идентификации утечки в каждой функциональной точке передачи информации.

В качестве модели для отработки предлагаемых действий был реализован модельный программный комплекс (МПК) «Голосовая почта», в который по мере осмысления проблемы включались необходимые механизмы защиты. Система изначально проектировалась с учетом модели уязвимостей, полученной после глубокого анализа фактов утечки информации. Традиционная схема построения приема передачи уже всего комплекса МПК формировалась на выше указанных требованиях, но была расширена отдельной подсистемой Депозитария, которая должна, как мы понимаем, юридическо-организационными решениями легализована в жизнь.

1. Обеспечение защиты информации

Общая структура МПК «Голосовая почта» представлена на рисунке.

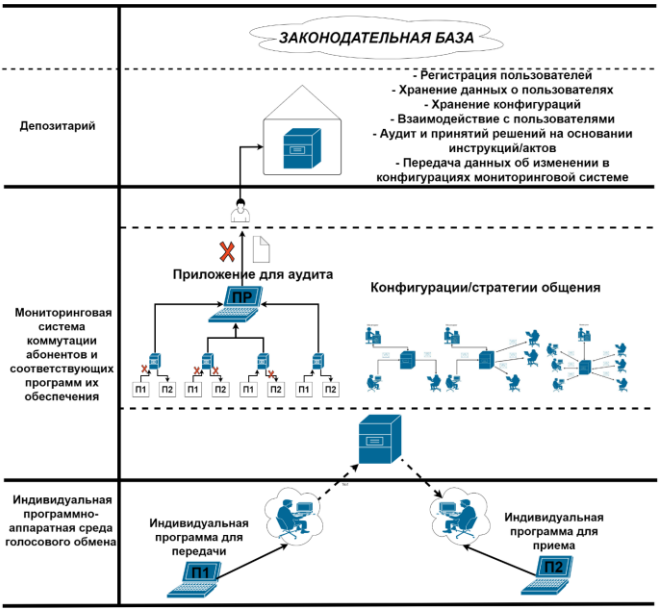

Рисунок. Модель конфиденциального речевого общения программной системы «Голосовая почта»

Защита передаваемой информации основывается на структуризации последовательности амплитуд в рамках логико-лингвистического подхода, которая фактически сжимает информацию и соответствует кодированию с потерями. Обратная операция восстановления практически не заметна относительно воспроизведения и имеет менее 10% отличающихся значений амплитуд. Объем передаваемой информации уменьшается в 2,5-10 раз, и таким образом экономится трафик. При передаче информации структура имеет персональное наполнение, которое относится к программе, которая структурирует входную информацию. Таким образом, имеем индивидуализацию передаваемых данных, которые восстанавливаются только той программой, которая создана под такие данные. Отсюда становится понятным, что прием и передача связаны в единую цепочку: должна быть программа, которая формирует структурные данные, эти данные имеют уникальное содержание, которое может быть раскрыто только уникальной программой. Одна программа на передающей стороне, другая на принимающей стороне, а по линии связи потоки каждый раз разных уникальных данных.

Для определения принадлежности передаваемой информации используется механизм нанесения «водяных знаков». Здесь снова используются получаемые структуры, которые позволяют логично и целенаправленно вносить маркеры и не нарушать качество воспроизведения ввиду внесения ничтожно малых изменений. Стоит заметить, что запись, сделанная сторонними устройствами, будет отличаться от той, которая будет передаваться по линии связи. Таким образом, сравнивая эти две записи, можно говорить о внешней «прослушке». Здесь также возможно варьировать маркеры и даже идентифицировать владельца информации.

Восстановленная информация может терять маркировку или же наоборот иметь другой вид маркирования. Таким образом, можно обеспечить отдельный вид маркировки при передаче и при приеме. На стороне сервера никаких действий не требуется, так он выступает в качестве коммутатора и непосредственного доступа данным не имеет. Всё это дает возможность документального подтверждения утечки информации и может служить доказательной базой факта утечки и установления «места» утечки.

2. Первопричина уязвимости при использовании программных продуктов и данных

Акцентируя внимание на информационной безопасности, подавляющее большинство специалистов области сосредотачивают внимание на конкретике противодействия возникающим угрозам, не

пытаясь взглянуть в суть или корень порождения таких угроз. Поняв это, можно найти более эффективные способы решения и преодоления этой проблемы исходя из более глубокого понимания сущности информационной отрасли, как специфической отрасли хозяйствования.

При акцентировании внимания на особенностях продукта в рассматриваемой информационной отрасли, следует сопоставить его с производством технических средств. Оба вида деятельности связаны с производством продукта, предназначенного для использования потребителем, но между ними громадная пропасть. Сравнение характеристик приведено в таблице.

Таблица

Сравнение характеристик технических средств и программных продуктов

№	Техническое средство	Программный продукт
1	Материальность	Виртуальность
2	Автономность	Общеплатформенность и сетевая общесвязанность
3	Уникальность производства и проектирования (но с типовыми решениями)	Единые технологичные решения
4	Различимость отдельного продукта	Неотличимость и клонируемость продуктов
5	Проблема тиражирования, требующая времени и мат. ресурсов	Быстрая скорость тиражирования
6	Реальность владения	Виртуальность владения (размытость границ)
7	Зависимость от условий	Независимость от условий
8	Требование квалификации при производстве и эксплуатации	Тиражирование и использование любым грамотным пользователем

Различия между двумя видами деятельности очевидны. Соответственно, совсем другой взгляд должен быть на характер владения, эксплуатации и защищенности. Виртуальность продукта и его обобщенность (один и тот же тиражируемый экземпляр) не позволяет в полной мере говорить о персональном владении, о путях утечки продукта, о претензиях на несоответствие заявленному качеству и многое другое.

Особая сущность информационной обработки и **создания продукта** лежит в основе всех рассмотренных аспектов. Вряд ли можно

переориентировать информационную отрасль, чтобы она повторила техническое производство. Но, рассматривая более внимательно пункты 4 и 6 таблицы, можно заметить, что они взаимозависимы. Если предположить, что для каждого пользователя создается программа, которая индивидуальна по своему внутреннему коду, то её как штрих-код можно было ассоциировать с владельцем.

Именно индивидуализация программы стала основой для создания всего МПК, и через программу реализуется механизм индивидуального наполнения структур. Указанная индивидуализации реализуется через механизм перемешивания независимых блоков с помощью операторов, реализованных макросредствами.

3. Защита программ от анализа и взлома

В ходе реализации программного комплекса наиболее важные функции системы реализовывались на языке ассемблера с использованием макросредств в виде процедур DLL. Это существенно затрудняет вскрытие логики работы программы.

Кроме этого, была опробовано расширение системы команд архитектуры Intel, в которой был введен механизм анклавов [7, 8]. Наиболее важные процедуры и данные были помещены в анклав. Но существенным моментом является то, что данное дополнение не имеет пока широкого распространения, и такие программы будут функционировать только на ограниченном множестве установок.

Отдельный вопрос касается **индивидуализации программ**. Вполне понятно, что программу, написанную на языке высокого уровня, трудно модифицировать при сложившихся технологиях.

4. Распределение ответственности между участвующими сторонами и их взаимозависимость

Вышеуказанные возможности дают гарантию защиты от любого вмешательства в процесс приема-передачи и гарантии обнаружения возможных утечек. Для увеличения степени надежности на передающей стороне хранится полный комплект программных средств и программа восстановления, которая поступает к принимающей стороне вместе с информацией. Происходит восстановление звукового потока и воспроизведение. Затем вся информация может быть уничтожена. Принимающая сторона, желающая выступать в роли передающей, получает собственный индивидуальный комплект с собственным способом передачи. Сервер выступает в роли коммутирующей и мониторинговой подсистем, следит за правильностью обращения к услугам системы и имеет возможность дополнительной защиты через коммутацию с передающей программой. При обращении к серверу

открываются определенные идентифицирующие данные, в ответ на которые передается адрес, куда нужно передать управление для продолжения дальнейшей работы. Такая возможность существенно затрудняет анализ программы через отладочные средства.

Дополнительной службой, которая в первую очередь регистрирует и распространяет программные системы приема передачи, является депозитарий. В нем происходит документированная привязка программной системы к конкретному владельцу. Кроме этого, служба может сертифицировать рабочее место и указать возможные угрозы и пределы ответственности и гарантии. Сразу же после регистрации необходимая информация предоставляется коммутационной и мониторинговой системой для обеспечения связи. Данная служба блокирована от сети и обменивается информацией только с помощью специальных съемных носителей для обеспечения гарантированной защиты от интернет-проникновения.

Сертификация рабочего места и предоставление информации о возможных утечках и границах ответственности для каждой из сторон и о предпринимаемых мерах в случае утечки и риска возникновения такой ситуации фактически должна находиться в зоне действия депозитарной службы. Именно она является ключевой подсистемой, которая обеспечивает юридические и организационные мероприятия, разрешает конфликтные ситуации и обобщает мониторинговую информацию для внесения изменений в защитные механизмы с учетом выявленных точек утечки информации.

Заключение

На данный момент обеспечивается полный цикл приема передачи с соответствующей поддержкой индивидуальными программами. Работы по реализации работы депозитария находятся на начальной стадии. Ведутся дополнительные работы по усилению мер защиты. Предлагаемая концепция и модель системы для отработки предложенных решений и проверки надежности защиты при передаче голосовых сообщений может стать прототипом других систем и откроет новые возможности по защите передачи информации в сети Интернет, обеспечит документальную основу в вопросах защиты интеллектуальной собственности в юридических инстанциях.

Список литературы

2. Скляров Д. В. Искусство защиты и взлома информации: монография / Д. В. Скляров. – СПб. : БХВ-Петербург, 2009. – 288 с.

3. Щелкунов Д. А. Автоматическая защита программ от исследования и отладки / Д. А. Щелкунов // Сборник трудов VII

Международ. симпоз. Интеллектуальные системы (INTELS 2006). – Краснодар, 2009. – 221 с.

4. Думанский А. И. Защита программного продукта через его индивидуализацию на примере модели Голосовой почты / А. И. Думанский, Ю. О. Федюк // XLVI Международная молодежная научная конференция «Гагаринские чтения»: сборник тезисов докладов, 2020. – С. 294