Модель динамической системы обеспечения комплексной защиты информации при передаче голосовых сообщений

Московский авиационный институт (национальный исследовательский университет)

К. А. Коновалов

Н. Е. Балакирев

Общая проблема систем защиты

- **Любая система защиты информации подвержена вскрытию.**
- **Ограничения для вскрытия**:

1) временные интервалы (T),
2) ресурсы злоумышленника (R),
3) квалификация злоумышленника (IQ),
4) точки вскрытия (прием и передача),
5) преобладающая бесконтрольность использования программных средств в информационной сфере.

Действия злоумышленника, нацеленные на получение конфиденциальной информации

- Различные способы вскрытия, например анализ передаваемых потоков информации, либо анализ кода программного продукта. Например используются:
- Средства дизассемблирования (например такие, как IDA).*
- Инструментарий перехвата передаваемых данных (через утилиты прослушивания трафика и/или воздействия на сетевое оборудование).*
- * с последующим анализом полученных сведений о программе или передаваемых данных, используя T, R, IQ.

Метод противодействия злоумышленникам

- **Задача**: предложить методы и алгоритмы по нейтрализации основных методов по несанкционированному получению конфиденциальной информации.
- **Предлагается**: механизмы и методы противодействия вышеуказанным возможностям по вскрытию. Реализовать программный комплекс, использующий данные механизмы и методы.

Противодействие злоумышленнику для защиты конфиденциальной информации

- С целью усложнения анализа кода программного продукта используется ассемблер при написании ключевых частей для минимизации повторяющихся участков кода.
- Создаются экземпляры (индивидуальные версии) программного продукта меняя части кода (не влияя на функционал).
- Вводится контроль использования индивидуальных версий программного продукта (назвали «индивидуализация программного продукта»).
- «Разрывается» цепочка приема и передачи данных, реализуя программы только на прием и только на передачу для минимизации возможных воздействий на серверно-коммутационную среду.

Модель динамической системы

- **Модель динамической системы** подразумевает механизм взаимодействия участников обмена информации используя комплекс защитных мер при передаче информации.
- Предлагаемый комплекс мер реализует:

1) вариабельность кода программного продукта через индивидуализацию кода,
2) индивидуализацию структур пакета передачи без изменения функциональности,
3) возможность периодического изменения (кода и структур).

Цели и задачи модели динамической системы

- **Достигаемые цели**: бесполезность использования результатов вскрытия алгоритмов программного продукта, так как к завершению вскрытия код программного продукта уже может быть изменен.
- Периодичность изменения индивидуальных экземпляров программного продукта предлагается отработать имитируя действия злоумышленника, осуществляя сменяемость продукта в рамках правил выбранной политики.

Индивидуализация программного продукта

- Возникает необходимость в реализации службы, закрепляющей за каждым пользователем свой индивидуальный экземпляр (индивидуализация) программного продукта.
- Данная служба по мере необходимости регулярно перерегистрирует и обновляет программный продукт в соответствии с установленной политикой.

Получаемые возможности от индивидуализации программного продукта

- **Установление источника утечки** и обеспечение доказательной базы нарушения прав пользования программным продуктом: с индивидуализацией добавляется набор возможностей, облегчающий выявление злоумышленника через маркировку передаваемой информации изменяемыми элементами **«водяных знаков»**.
- *Предлагается закреплять за участниками общения определенные метаданные, реализуемые «водяными знаками», по которым однозначно можно идентифицировать экземпляр конкретного владельца программного продукта и сеанс передачи, привязанный к дате и времени.*

Учет и контроль

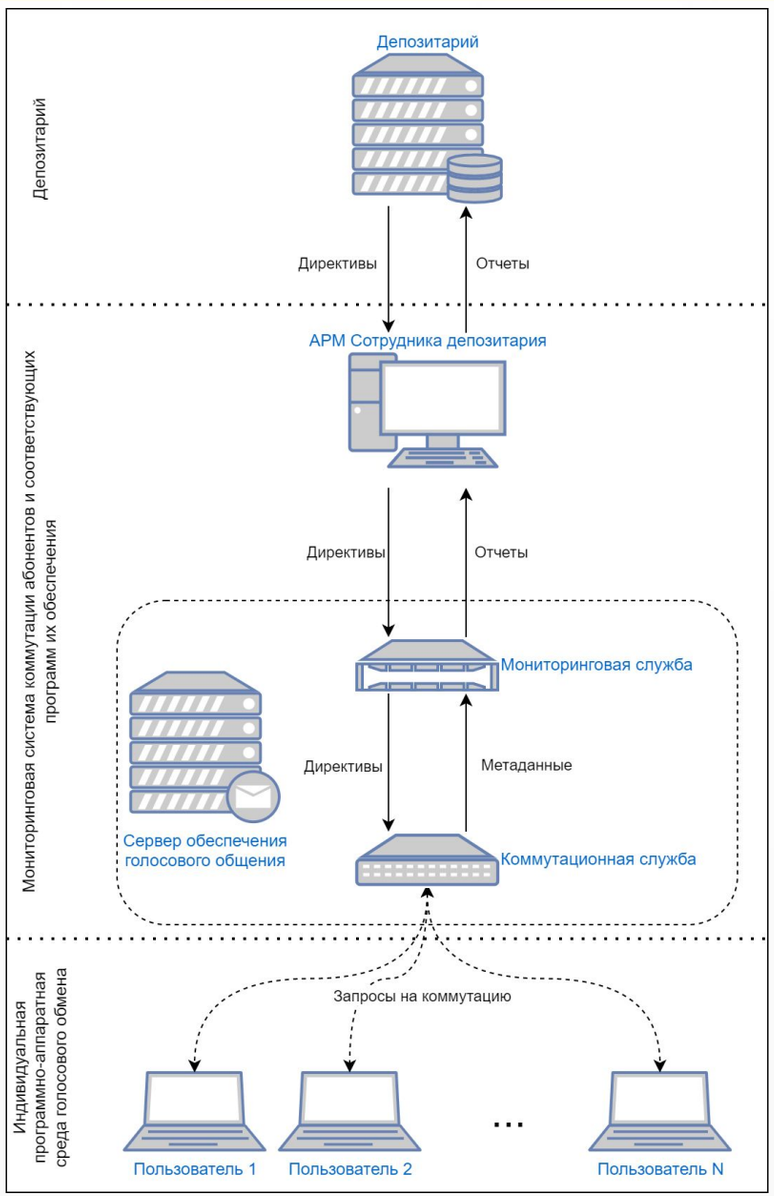
- Для обеспечения учета и контроля за правомочностью и корректностью использования экземпляров программных продуктов было решено реализовать **централизованную систему учета и контроля** использования выдаваемых пользователю индивидуальных экземпляров программ.

Реализация на примере программной системы "Голосовая почта"

- Для реализации модели динамической системы обеспечения комплексной защиты информации необходимо, чтобы были реализованы следующие механизмы:

1) Механизм Идентификации (информация однозначно идентифицирует источник — экземпляр программного продукта через «водяные знаки»).
2) Механизм Защиты (структуризация передаваемого потока амплитуд на базе качественного подхода к анализу данных для защиты от просмотра при перехвате).
3) Механизм Уникальности (каждому пользователю создается персональный экземпляр программного продукта).
4) Механизм Функциональности (каждый экземпляр соотносится только с одним пользователем).
5) Механизм Учета и контроля (индивидуализация обеспечивает систему учета и контроля предоставления программного продукта).
6) Механизм Мониторинга (на основе интегральной информации производится регулярный мониторинг использования программного кода и контроль процесса приема-передачи).

Концептуальная модель



Компоненты комплекса

- В комплексе выделено три компонента:
- **Депозитарий** - агрегирование и последующее хранение сведений участников общения с проверкой (согласно протоколу взаимодействия) участников мониторинговой системой коммутации),
- **Мониторинговая система коммутации** абонентов и соответствующих программ их обеспечения через механизм взаимодействия участников общения (не допустить подключение злоумышленника под видом легитимного пользователя),
- **Индивидуальная программно-аппаратная среда голосового обмена**, реализующая несколько стратегий общения (симплексное, дуплексное, а также один к одному или один ко многим с их комбинациями), например: отправитель к только слушающему получателю (получателям) или равноправные участники (с точки зрения возможности отправки и получения).

Результат и дальнейшие планы

- Предложенная модель динамической системы комплексной защиты информации должна обеспечить высокую степень надежности, а индивидуализация экземпляров программного обеспечения дает документальную основу для выявления злоумышленников.
- Дальнейшие шаги: Моделирование и имитация возможных действий злоумышленника для отработки механизма периодического изменения индивидуальных экземпляров программного продукта.

Используемые материалы

1) Коновалов К. А., Балакирев Н. Е.. Создание системы обеспечения учета и контроля защиты информации при передаче голосовой информации. 20-я Международная конференция «Авиация и космонавтика». 22-26 ноября 2021 года. Москва. Тезисы. Сс. 231-232. ISBN 978-5-00189-750-7.

2) Думанский А. И., Семенова Т. Б., Бабуджи С. Ю., Балакирев Н. Е.. Обеспечение конфиденциальной передачи информации через интернет. Гагаринские чтения — 2019. Сборник тезисов докладов. 2019. С. 337.

3) Думанский А. И., Федюк Ю. О., Балакирев Н. Е.. Защита программного продукта через его индивидуализацию на примере модели голосовой почты. Гагаринские чтения - 2020. Сборник тезисов докладов. 2020. С. 294-295.

4) Федюк Ю. О., Балакирев Н. Е.. Разработка различных стратегий использования голосовой почты с целью обеспечения дополнительных видов конфиденциальности. Гагаринские чтения - 2020. Сборник тезисов докладов. 2020. С. 523-524.

5) Селиванов Д. А., Думанский А. И., Балакирев Н. Е.. Индивидуализация кода программ, учитываемых в депозитарии. XLVII Гагаринские чтения 2021. Сборник тезисов работ. 2021. С. 451-452.

6) Думанский А. И., Балакирев Н. Е., Зеленова М. В., Лазунин К. А., Фадеев М. М.. Распределенная система защитных механизмов программного комплекса «Голосовая почта» на базе структуризации звукового потока волн. Информатика: проблемы, методы, технологии. Материалы XXI Международной научно-методической конференции. Воронеж, 2021. С. 709-716.