Уязвимости систем дистанционного банковского обслуживания

Гилязов Руслан Раджабович
Смышляев Станислав Витальевич

Содержание

- Описание проблематики
- Существующие решения
- Теоретическая модель
- Методы реализации модели

Описание проблематики

- Кража пользовательских аутентифицирующих данных
- Сокрытие от пользователя проводимых от его лица операций

Технологии:

- Фишинг
- Фарминг
- Межсайтовый скриптинг
- Перехват вводимой с клавиатуры аутентифицирующей информации
- Скрытое копирование файлов с аутентифицирующей информацией с жесткого диска клиентской машины.
- Скрытый доступ к отделяемым аппаратным носителям ключей.
- Подлог подписываемых пользователем платежных документов.
- …

Существующие решения

Использование отделяемых аппаратных модулей для работы с ключами (токенов).

• Использование токенов делает недостаточным для нарушителя получение парольной информации и образа жесткого диска

• Данная мера непосредственным образом не предотвращает атаки, связанные со скрытым от пользователя использованием токена в те промежутки времени, когда он подключен к системе.
• Для этого нарушителю достаточно получить парольную информацию и возможность вызовов функций, с помощью которых интерфейсные элементы клиентской части системы ДБО получают доступ к токену.

Описание проблематики

Угрозы:

- Получение противником парольной информации.

- Подлог передаваемой для подписи информации (нарушение требований N63-ФЗ, ст.12, п.2)

- Несанкционированный доступ к криптографическим функциям токена (пример: USB-over-IP)

Существующие решения

Меры противодействия некоторым из атак:

Использование виртуальных клавиатур вместо физических

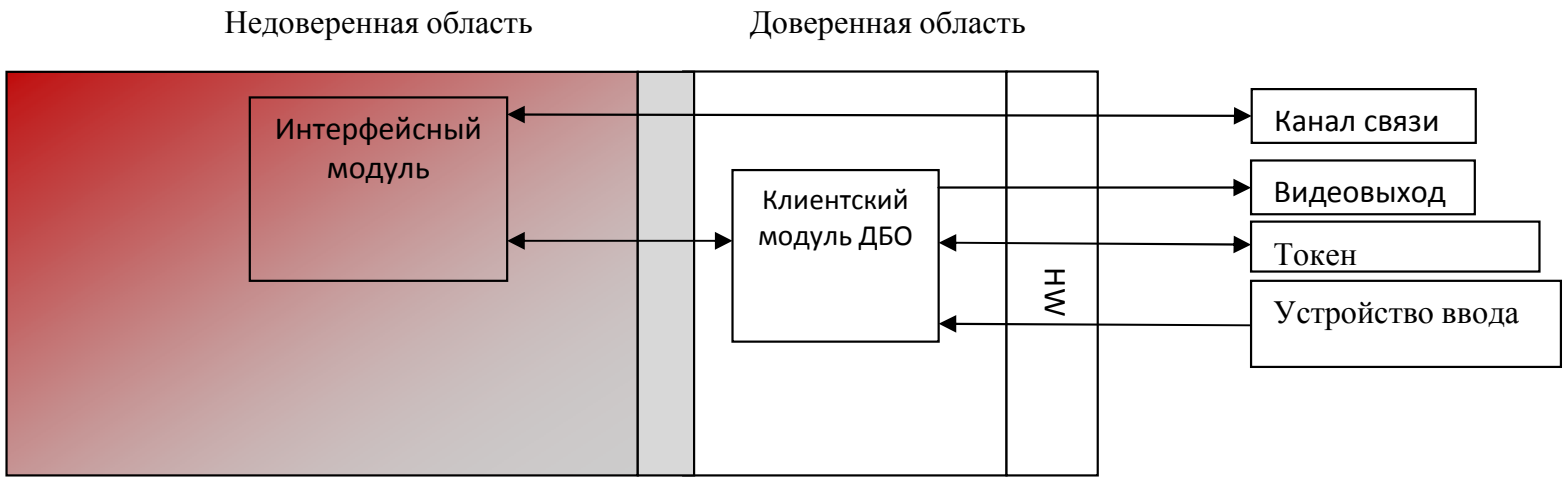
Данная мера предназначена для противодействия кейлоггерам. Но в случае, если не используются специализированные виртуальные клавиатуры, данная мера является бессмысленной: нарушитель, способный отследить нажатия клавиш физической клавиатуры, сможет также отследить и позиции нажимаемых клавиш виртуальной клавиатуры.

Теоретическая модель

Рассмотрим модель, при которой в клиентской системе существует доверенная область, из которой возможен неперехватываемый доступ к устройству ввода, устройству вывода и криптографическому токену.

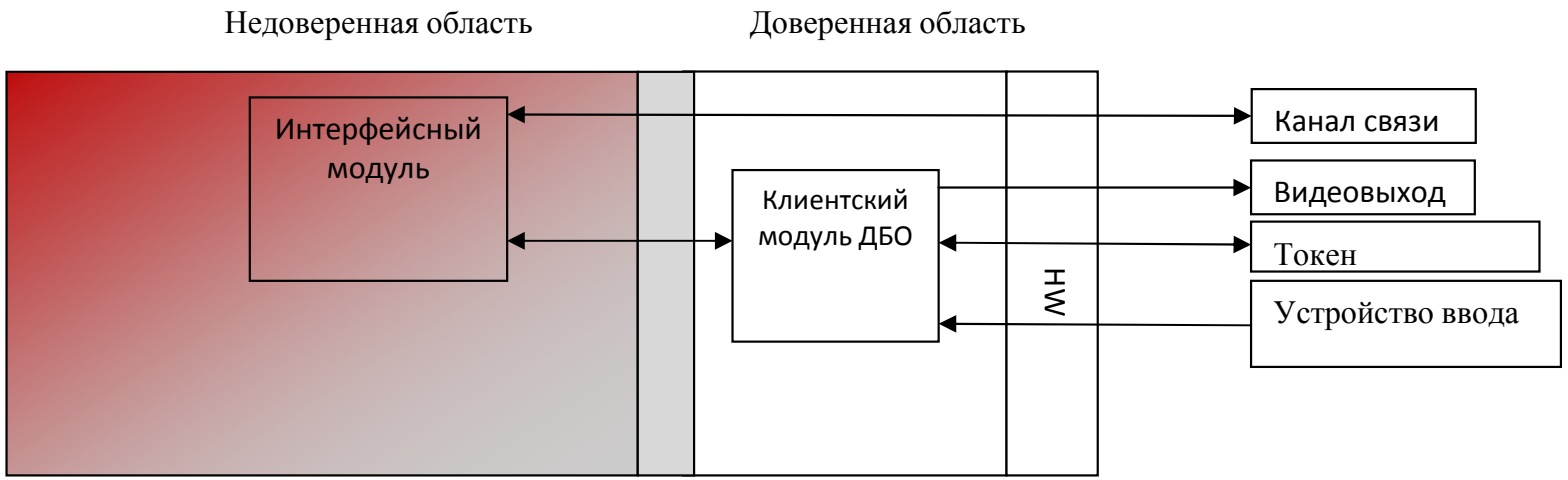
Теоретическая модель

Рассмотрим модель, при которой в клиентской системе существует доверенная область, из которой возможен неперехватываемый доступ к устройству ввода, устройству вывода и криптографическому токену.



Теоретическая модель

Существование в клиентской системе данной доверенной области необходимо и достаточно для защиты от описанных угроз.



Теоретическая модель

- Все критические транзакции происходят исключительно в защищенном режиме.
- Вход в защищенный режим происходит с гарантированным уведомлением пользователя.
- При осуществлении транзакций клиент имеет возможность полного визуального контроля платежной информации перед осуществлением подписи.
- Транзакции подтверждаются вводом PIN-кода в защищенном режиме работы.

Изменения инфраструктуры

Строгие требования к формату подписываемых платежных документов, для обеспечения возможности эквивалентности отображаемого представления байтовому.

- Недопустимость непечатаемых символов.
- Ограничения по объему документов (зависит от аппарата защищенного режима работы с экраном).
- Недопустимость неявных представлений данных и интерпретируемых форматов (ex: .djvu, .pdf, etc).
- Однозначное соответствие выводимого на экран для подтверждения и байтового представлений документов.

Методы реализации модели

Модель потенциально реализуется на практике рядом методов, отличающихся требованиями к наличию дополнительных устройств и предположениями о противнике.

В качестве доверенной области могут выступать следующие элементы:

• Внешнее устройство с портом для доступа к токену, экраном и устройством ввода.

• Уровень ядра ОС.

• Гипервизор.

Методы реализации модели

Внешнее устройство

Уровень ядра

Предположения о противнике:
Отсутствие аппаратных закладок и исполняемого в кольце 0 программного кода нарушителя в произвольный момент времени

Компоненты системы:
• Система обеспечения безопасного доступа к парольной информации, состоящая из драйвера-фильтра, осуществляющего маскирование вводимой парольной информации и защищенную передачу в работающий на уровне ядра модуль СКЗИ.
• Система охраны дверей, поддерживающая целостность используемых модулей в случае и контролирующая исполнение кода в кольцо 0.
• Система управления установкой/деинсталляцией комплекса, требующая для отключения/деинсталляции комплекса ввода корректного пароля.

Уровень ядра

Предположения о противнике:
Отсутствие аппаратных закладок и исполняемого в кольце 0 программного кода нарушителя в произвольный момент времени

Компоненты системы:
• Модуль СКЗИ и взаимодействия с токеном, работающий на уровне ядра.
• Система пользовательских интерфейсов, отображающая информацию о статусе производимых действий (например, о числе введенных символов пароля), но не о самих действиях.
• Модифицированный видеодрайвер, позволяющий защитному модулю осуществлять непосредственный доступ к видеобуферу

Уровень ядра

Особенности реализации:

- Защищенный режим ввода пароля начинает работать строго после нажатия некоторой жестко зафиксированной специальной комбинации клавиш.
- После установки комплекса ввод пароля в защищенном режиме производится тогда и только тогда, когда была нажата комбинация СКК.
- Навязывание противником пользователю ситуации с небезопасным вводом пароля невозможно.
- Для обеспечения неперехватываемого вывода на экран реализовывается соответствующий драйвер-фильтр для видеокарты.
- Механизмы защиты от выгрузки модуля.

Гипервизор

Гипервизор – совокупность программно-аппаратных средств, позволяющая обеспечить одновременное функционирование нескольких операционных систем на одной аппаратной платформе.

КРИПТО ПРО

СПАСИБО ЗА ВНИМАНИЕ!

КРИПТО-ПРО – ключевое слово в защите информации

http://www.cryptopro.ru
svs@cryptopro.ru
rubin@cryptopro.ru

Тел./факс:
+7 (495) 780-48-20
+7 (495) 660-23-30