Обеспечение безопасного доступа к ключам в слабозащищенных системах

Гилязов Руслан Раджабович

Смышляев Станислав Витальевич

Содержание

- Описание проблематики
- Постановка задачи
- Модель функционирования
- Используемые понятия
- Рассматриваемая модель
- Модель нарушителя
- Рассматриваемые атаки
- Существующие решения
- Предлагаемое решение: концепция
- Предлагаемое решение: реализация

Описание проблематики

•На текущий момент существует большое количество разработок вирусного характера, нацеленных на получение доступа к пользовательской ключевой информации.

• Наиболее явная уязвимость: путь доставки пароля для получения доступа к хранящемуся в контейнере ключу.

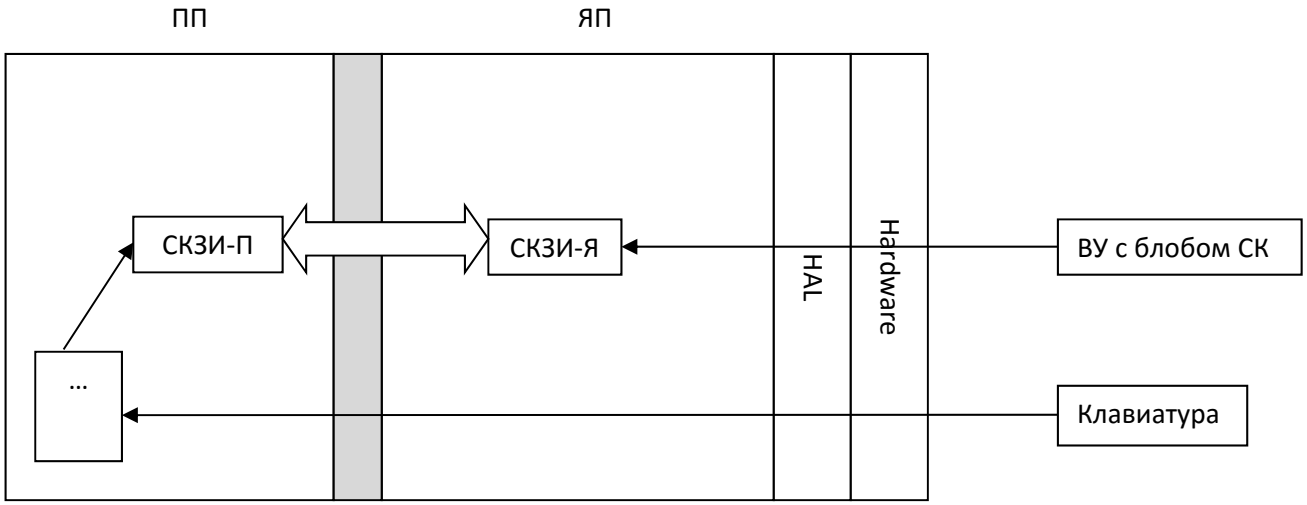
• ИСО/МЭК 15408-2002: важность задачи защиты паролей.

• Введение в РФ электронных карт гражданина: необходимость защищать парольную информацию в минимально обеспеченных средствами защиты компьютерных системах.

Постановка задачи

Требуется в предположениях о невозможности присутствия в системе программного кода противника, работающего в кольце 0, обеспечить возможность безопасного доступа к ключам, находящимся на внешнем устройстве (жесткий диск ПК, отделяемый носитель).

Рассматриваемая модель



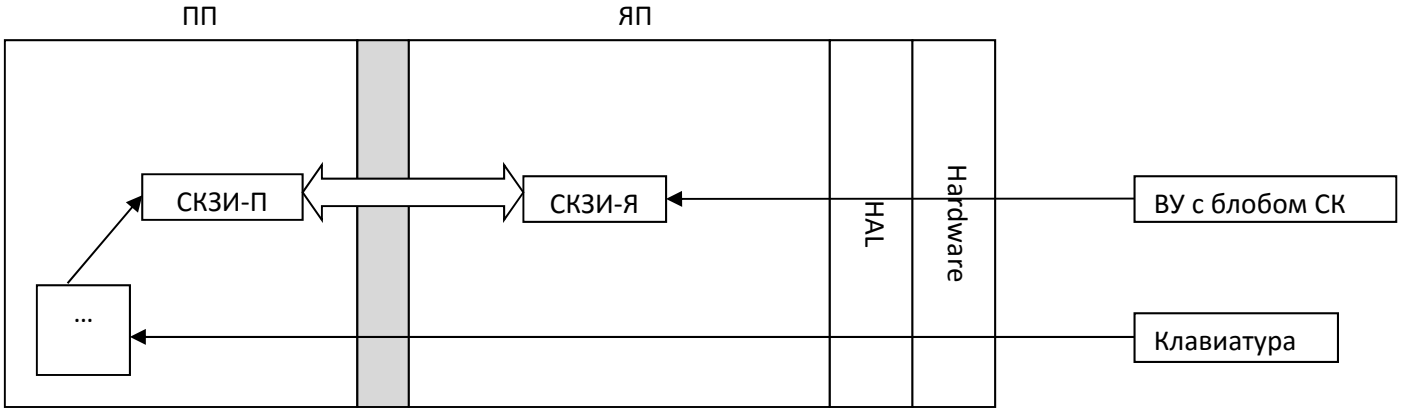
Рассматриваемая модель

Предположения:

• СК находится на внешнем устройстве (отделяемый ключевой носитель, жесткий диск компьютера, …) в блобе, зашифрованном на диверсифицированном из пароля ключе шифрования ключа.

• Первичная загрузка СК в СКЗИ происходит с внешнего устройства.

• После загрузки СК в СКЗИ все операции с данным ключом производятся без выхода ключевой информации из области памяти, доступ к которой возможен исключительно для кода, работающего в кольце 0.

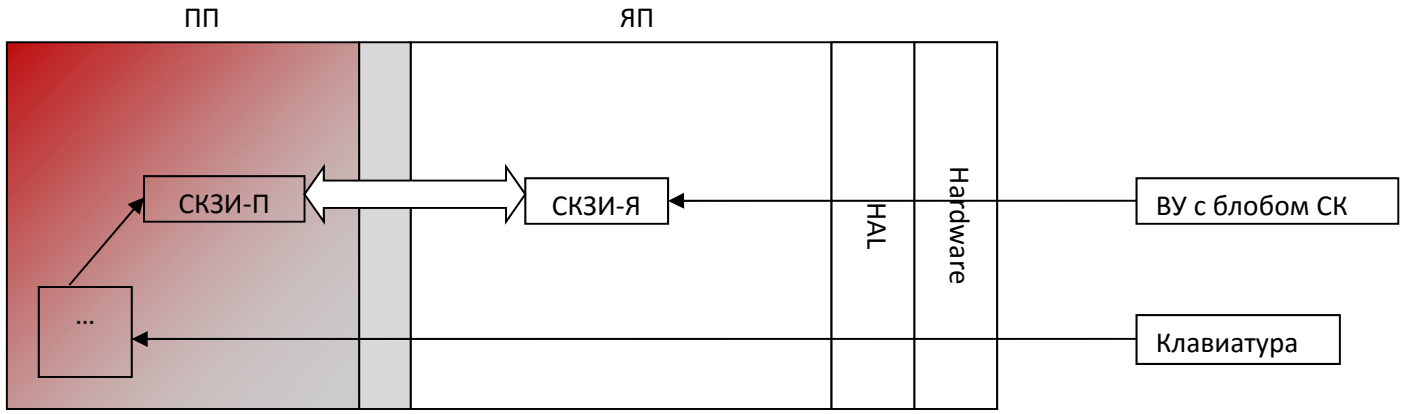


Модель нарушителя

• Угроза: получение противником информации об СК.

• Предположения о противнике: программного кода противника, работающего в кольце 0, в системе ни в один момент времени нет.

• Возможны модули противника, работающие в кольце 3 и имеющие доступ к соответствующему пользовательскому пространству памяти.



Модель нарушителя

• В случае отсутствия дополнительных программных средств защиты: пароль поступает по стандартным каналам, по которым идет поток ввода с клавиатуры, что позволяет противнику перехватить его на пользовательском уровне.

• Перехват возможен либо с помощью построенных по различным технологиям программ перехвата вводимой с клавиатуры/мыши информации (кейлоггеров), либо с помощью целевых атак, направленных на используемые во время пересылки пароля области памяти, находящиеся в рамках ПП.

Рассматриваемые атаки

- Противник в данных предположениях может отобразить на экране фальшивое окно ввода пароля на СК в произвольный момент времени.

- Будем рассматривать как класс атак, ограниченный кейлоггерами, так и наиболее широкий возможный в данных предположениях о противнике класс атак, включающий также и произвольные целевые атаки.

Существующие решения

Hanno Langweg
«Building a Trusted Path for Applications Using COTS Components»

Технологии противодействия подмены противником окна ввода, основанные на эксклюзивном (в определенных предположениях) выводе на экран средствами DirectX специальных изображений, распознаваемых пользователем (и заранее им выбранных из ограниченного набора изображений) и являющихся подтверждением аутентичности окна ввода пароля.

Существующие решения

Hanno Langweg
«Building a Trusted Path for Applications Using COTS Components»

Критика:

• Слишком малое (в сравнении с энтропией вводимого пароля) число легко отличимых пользователем друг от друга заложенных в приложение изображений.

• Избыточная жесткость предположений о противнике, требуемых для работоспособности данной технологии (по причине необходимости эксклюзивности и неперехватываемости изображения во время аутентичного ввода).

Предлагаемое решение: концепция

- Защищенный режим ввода пароля начинает работать строго после нажатия некоторой жестко зафиксированной специальной комбинации клавиш (СКК).

- Таким образом, после установки комплекса ввод пароля в защищенном режиме производится тогда и только тогда, когда была нажата комбинация СКК.

- Обман противником пользователя, каждый раз перед вводом пароля вводящего СКК, невозможен.

Предлагаемое решение: концепция

Случай 1: Противник использует для перехвата пароля работающие на пользовательском уровне кейлоггеры, построенные по одной из ранее описанных технологий.

• После включения защитный модуль начинает вместо введенных символов выдавать один и тот же символ, сохраняя в находящейся в ЯП области памяти все введенные символы, пропуская только служебные символы, такие, как Backspace, Tab и Enter.

• После сеанса ввода СКЗИ-П запрашивает у защитного модуля введенный пароль (с обязательной аутентификацией защитным модулем СКЗИ-П), после этого передавая его по стандартным каналам в СКЗИ-Я.

Предлагаемое решение: концепция

Случай 2: Противник присутствует на пользовательском уровне, возможны целевые атаки.

• На уровне ядра реализуется кэш паролей; пароли вовсе не попадают в СКЗИ-П, их из кэша запрашивает непосредственно СКЗИ-Я.

Предлагаемое решение: концепция

Случай 3: Противник присутствует на пользовательском уровне, возможны целевые атаки, противник с помощью средств видеофиксации или аппаратных закладок в клавиатуре отслеживает все нажатия клавиш.

• На экран перед вводом каждого символа выводится новая перестановка клавиш клавиатуры, сгенерированная в защитном модуле и передаваемая в СКЗИ-Я.

• Пароль вводится пользователем строго в том виде, как это предполагается перестановкой клавиш клавиатуры, в этом виде он и поступает в СКЗИ-П или СКЗИ-Я вышеописанным образом; обратная перестановка символов производится позже в СКЗИ-Я.

Предлагаемое решение: реализация

Рассматриваются операционные системы типа Windows NT. В качестве испытуемого стенда использовались Windows 7 (без SP) и Windows XP SP3. В качестве испытуемых кейлоггеров использовались общедоступные разработки.

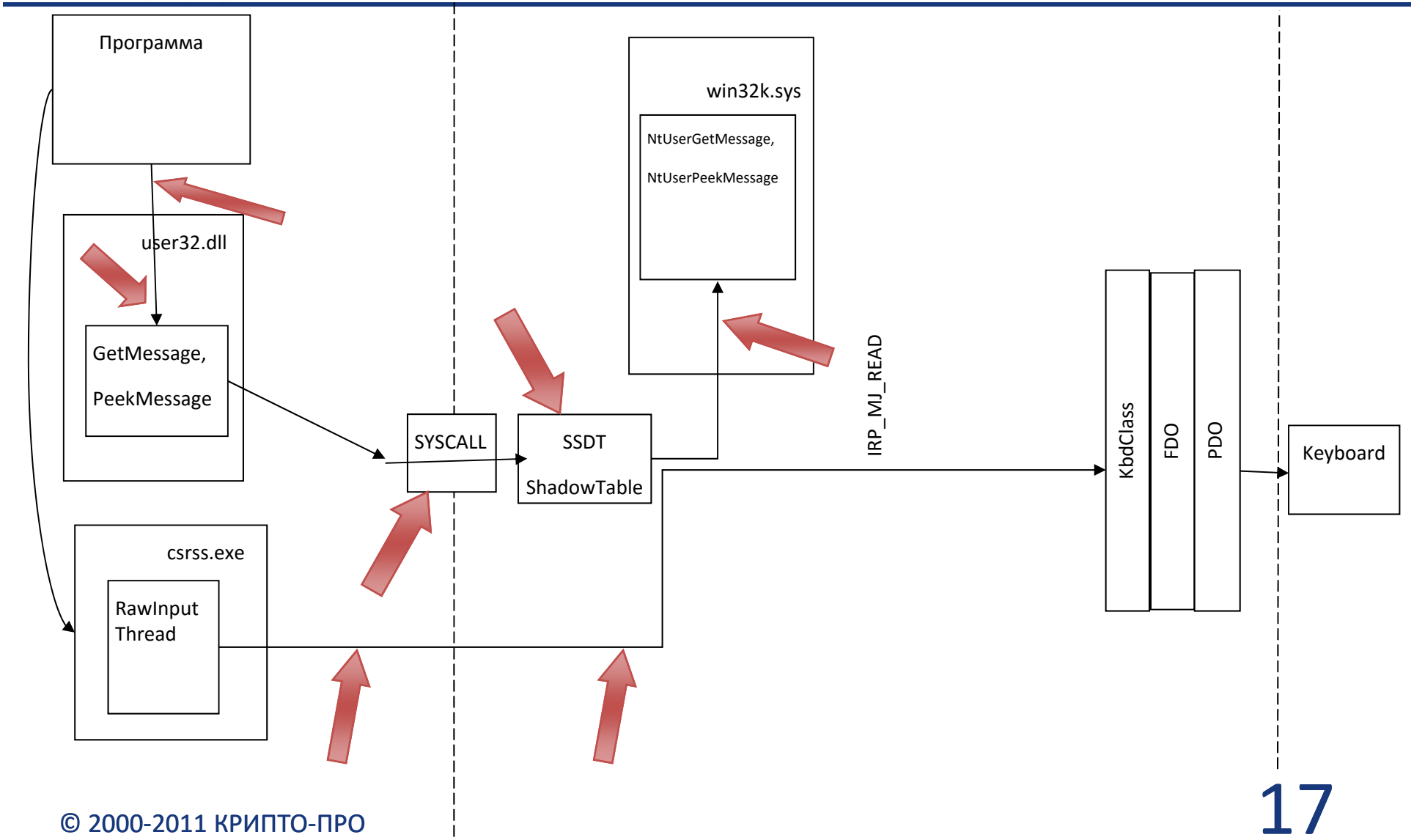
• В стек драйверов клавиатуры ставится драйвер-фильтр, осуществляющий просмотр и модификацию всех вводимых с клавиатуры символов в соответствии с одной из описанных ниже схем.

• Драйвер-фильтр начинает работать строго после нажатия некоторой жестко зафиксированной специальной комбинации клавиш (СКК).

• Таким образом, после установки комплекса ввод пароля в защищенном режиме производится тогда и только тогда, когда была нажата комбинация СКК.

• Обман противником пользователя, каждый раз перед вводом пароля вводящего СКК, невозможен.

Технологии кейлоггеров



Предлагаемое решение: реализация

Случай 1: Противник использует для перехвата пароля работающие на пользовательском уровне кейлоггеры, построенные по одной из ранее описанных технологий.

• После включения драйвер-фильтр начинает вместо введенных символов выдавать один и тот же символ, сохраняя в находящейся в ЯП области памяти все введенные символы, пропуская только служебные символы, такие, как Backspace, Tab и Enter.

• После сеанса ввода СКЗИ-П запрашивает у драйвера-фильтра введенный пароль (в процессе чего происходит идентификация драйвер-фильтром СКЗИ-П), после этого передавая его по стандартным каналам в СКЗИ-Я.

Предлагаемое решение: реализация

Случай 2: Противник присутствует на пользовательском уровне, возможны целевые атаки.

• На уровне ядра реализуется кэш паролей; пароли вовсе не попадают в СКЗИ-П, их из кэша запрашивает непосредственно СКЗИ-Я.

Предлагаемое решение: реализация

Случай 3: Противник присутствует на пользовательском уровне, возможны целевые атаки, противник с помощью средств видеофиксации или аппаратных закладок в клавиатуре отслеживает все нажатия клавиш.

• На экран перед вводом каждого символа выводится новая перестановка клавиш клавиатуры, сгенерированная в драйвере-фильтре и передаваемая в СКЗИ-Я.

• Пароль вводится пользователем строго в том виде, как это предполагается перестановкой клавиш клавиатуры, в этом виде он и поступает в СКЗИ-П или СКЗИ-Я вышеописанным образом; обратная перестановка символов производится позже в СКЗИ-Я.

Предлагаемое решение

• Одновременно с установкой утилиты устанавливается драйвер, работающий с этого момента в системе непрерывно (загружающийся до WinLogon для потенциальной возможности обеспечить защищенный ввод пароля на этапе загрузки системы). Невозможность выгрузки драйвера с пользовательского уровня необходима для противодействия попыткам нарушителя незаметно для пользователя отключить систему защиты.

• Хранилище паролей реализовано в ядре. Память, выделанная под них, не свопируемая. Поддерживается одновременное хранение нескольких паролей с различными значениями их времени жизни. Присутствует операция гарантированного очищения.

• Присутствует система разграничения доступа приложений пользовательского уровня к драйвер-фильтру.

Результаты

Проведен ряд экспериментов с использованием общедоступных кейлоггеров, показавших эффективность предложенного подхода на практике.

СПАСИБО ЗА ВНИМАНИЕ!

КРИПТО-ПРО – ключевое слово в защите информации

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

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