V Юбилейный Уральский форум
«Информационная безопасность банков»

Башкортостан, 14 февраля 2013 г.

Доверенная визуализация подписываемых платежей в системах ДБО без применения дополнительных аппаратных устройств

Андрей Степаненко
Директор по маркетингу

Код Безопасности
ГК «Информзащита»

Глобальная проблема

- Применение электронной подписи для заверения документов породило желание подделывать такие документы с сохранением значимости подписи
- Способы подделки электронных документов эволюционируют быстрее, чем способы противодействия им
- Пользователи мало озабочены «здоровьем» своих компьютеров
- Carberp, Zeus, SpyEye и др. – реальная угроза для систем дистанционного банковского обслуживания

Типовые сценарии

- Кража секретного ключа пользователя с незащищенного носителя при помощи вредоносной программы и выполнение действий от имени пользователя на другом компьютере
- Кража секретного ключа пользователя из оперативной памяти (при использовании защищенного носителя) и выполнение действий от имени пользователя на его компьютере (удаленное управление или автоматическое создание документов)
- Подмена реквизитов документа непосредственно перед подписанием

Код Безопасности
ГК «Информзащита»

Масштабы бедствия

ТРЕНД	ДОЛЯ ОТ ОБЩЕГО ОБЪЕМА РЫНКА	СУММА
ИНТЕРНЕТ-МОШЕННИЧЕСТВО		
Мошенничество в системах интернет-банкинга	21.3 %	490 млн. $
Обналичивание денежных средств	16 %	367 млн. $
Фишинг	2.4 %	55 млн. $
Хищение электронных денег	1.3 %	30 млн. $
Итого:	41 %	942 млн. $

Код Безопасности
ГК «Информзащита»

Источник: отчет Group-IB «Рынок киберпреступности в России–2011»

Варианты противодействия

Единственная технология, которая сейчас успешно противостоит новым типам атак – **Trusted Screen со встроенной криптографией**:

- Доверенное отображение документа перед подписанием
- Обязательное ручное подтверждение подписи
- Реализация функции подписи вне потенциально зараженной среды

Код Безопасности
ГК «Информзащита»

Преимущества и недостатки

Преимущества:

- Пока нет способов обхода

Недостатки:

- Дополнительное аппаратное устройство
- Использование дорогих токенов/смарткарт с криптографией на борту
- Небольшой размер экрана для доверенного отображения

Код Безопасности
ГК «Информзащита»

Альтернативное решение

Новое решение компании «Код Безопасности» Jinn – технология доверенной визуализации и подписи электронных документов:

- Реализация доверенной среды даже на зараженных компьютерах (защита от кражи ключей с носителей или из оперативной памяти, защита от перехвата паролей доступа к ключевым контейнерам и т.п.)
- Невозможность подписания платежного документа без участия легального пользователя
- Выявление подмены содержимого документа перед подписанием и отказ от подписи подложного документа

Код Безопасности
ГК «Информзащита»

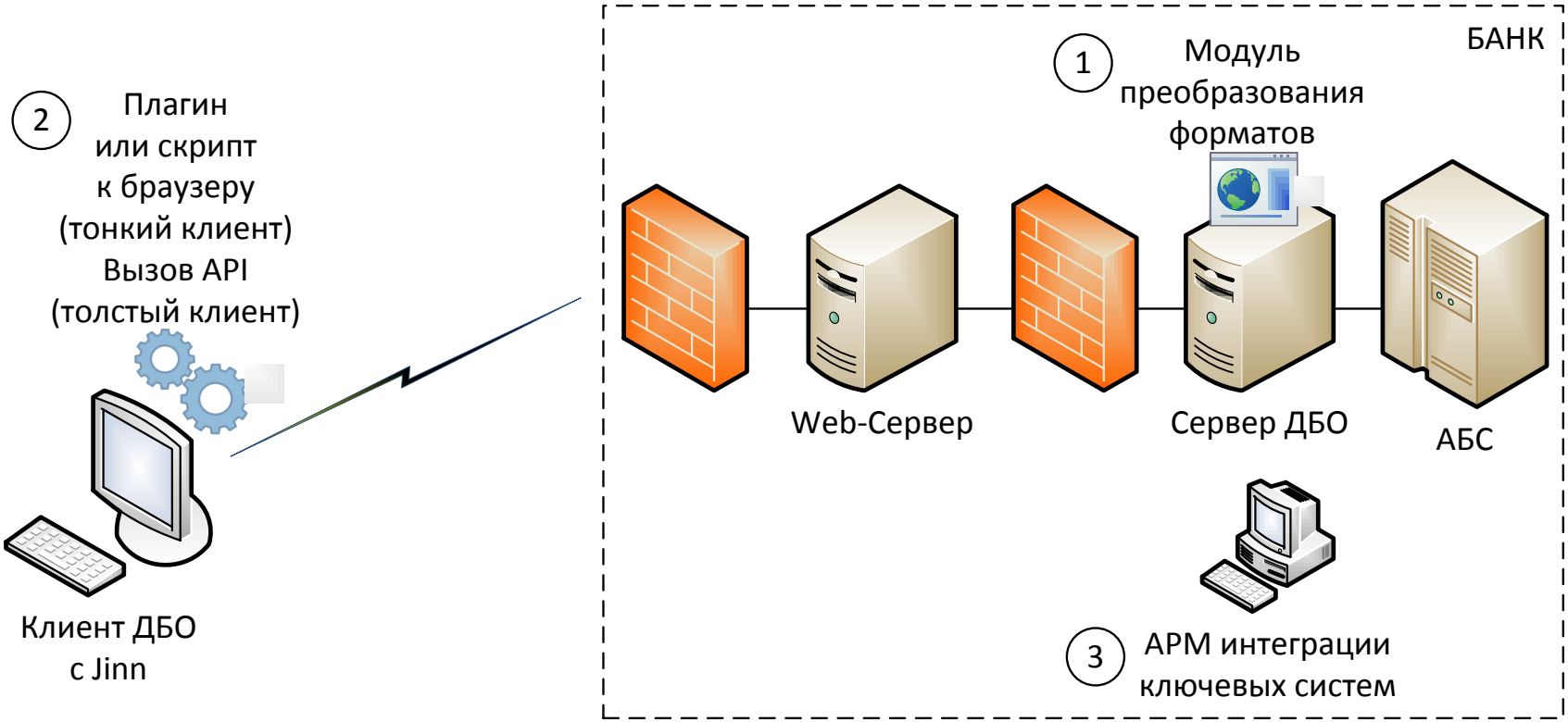
Принципиальные отличия Jinn

Доверенная среда для отображения документа и выполнения криптографических функций создается **непосредственно на компьютере пользователя** без применения дополнительных устройств

- Все вычисления производятся на изолированных ядрах процессора, недоступных операционной системе
- Микрокод доверенной среды и ключи пользователей хранятся непосредственно в памяти выделенных ядер процессора
- Для отображения документов используется монитор компьютера

Код Безопасности
ГК «Информзащита»

Схема встраивания в систему ДБО



В состав решения входят все необходимые для интеграции в систему ДБО компоненты

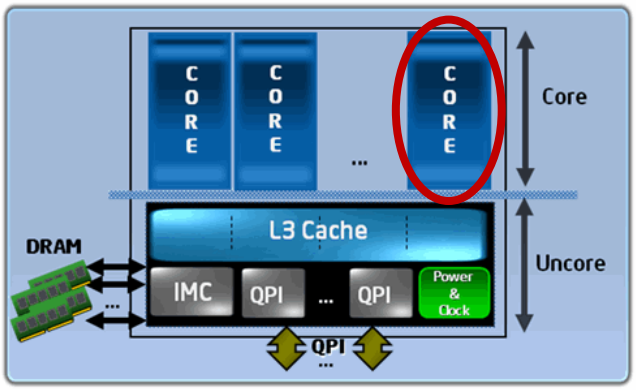
Код Безопасности
ГК «Информзащита»

Как Jinn защищает АРМ ДБО

Пользователь загружает АРМ ДБО с флэш-диска:

- Одно из ядер процессора изолируется от остальной системы и используется для реализации функций защиты
- непосредственно в память ядра загружаются микрокод доверенной среды и ключи пользователя

После удаления флэш-диска загружается операционная система, которая «не видит» выделенное ядро



Код Безопасности
ГК «Информзащита»

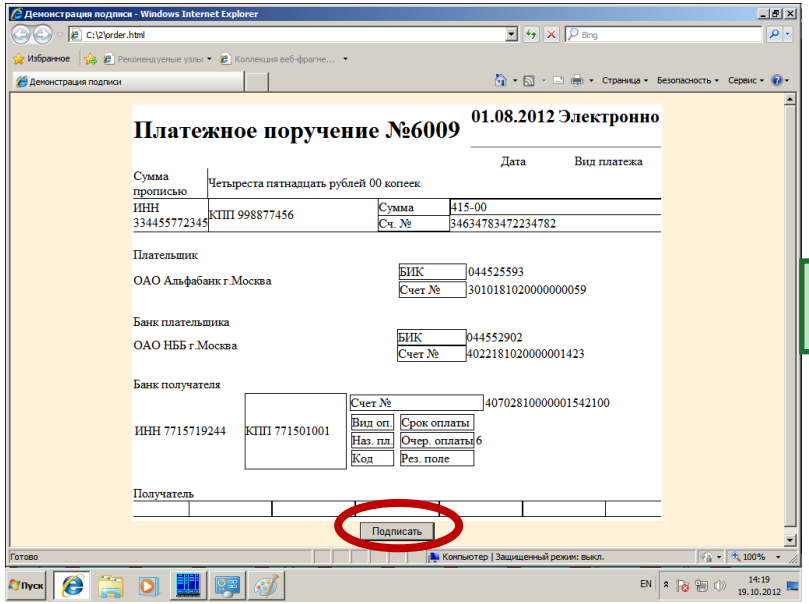
Как работает Jinn

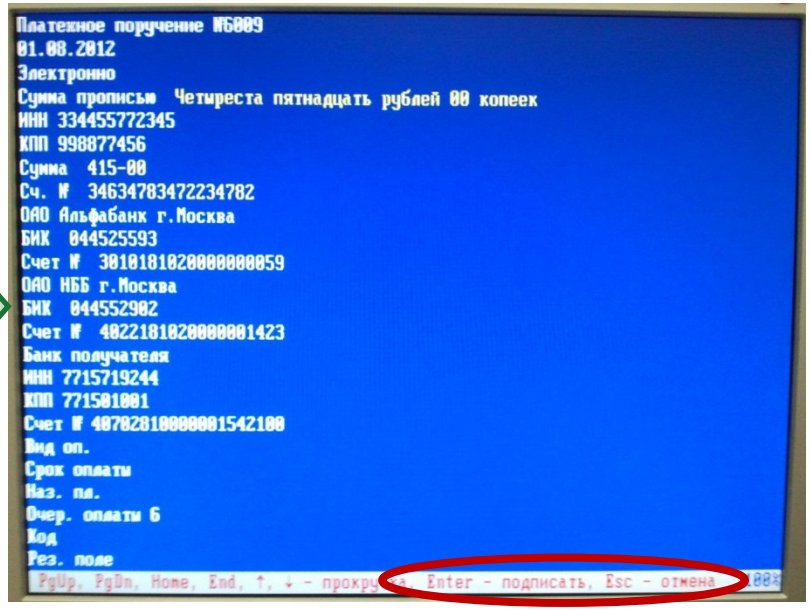
После формирования в системе ДБО платежного поручения пользователь нажимает «Подписать»:

- Jinn переключает компьютер в доверенную среду и отображает документ на экране компьютера
- Пользователь контролирует неизменность документа и подтверждает разрешение на подписание
- Jinn формирует электронную подпись и возвращает управление операционной системе
- Клиент ДБО принимает подписанный платежный документ и отправляет его в обработку

Код Безопасности
ГК «Информзащита»

Как работает Jinn





Код Безопасности
ГК «Информзащита»

Совместимость

- Доверенная среда технологии Jinn работает на процессорах Intel и AMD, имеющих 2 и более ядер процессора (выпускаются с 2006 г.)
- Обеспечивается возможность использования существующих сертификатов пользователей, выданных удостоверяющими центрами, реализующими ГОСТ Р 34.10-2001 и ГОСТ Р 34.11-94
- Поддерживаемые форматы электронной подписи:
  - CMS
  - XML-Dsig

Код Безопасности
ГК «Информзащита»

Преимущества технологии Jinn

- Реализация Trusted Screen со встроенной криптографией без дополнительных аппаратных устройств
- Использование монитора компьютера пользователя для удобного просмотра всего подписываемого документа
- Возможность применения обычных незащищенных носителей без ущерба для безопасности
- Простота встраивания в уже функционирующие системы

Код Безопасности
ГК «Информзащита»

Возможности для сотрудничества

- Для разработчиков систем ДБО и банков – дополнительные выгоды для клиентов и снижение уровня мошенничества, совершаемого при помощи вредоносных программ, за счет повышение защищенности систем ДБО
- Для производителей систем ЭДО и интеграторов – предоставление клиентам решений, обеспечивающих юридическую значимость электронных документов

Код Безопасности
ГК «Информзащита»

Спасибо!

Андрей Степаненко
Директор по маркетингу

ООО «Код Безопасности»
Тел.: +7(495) 980-2345
info@securitycode.ru

Код Безопасности
ГК «Информзащита»