Заблуждения банковской безопасности

Алексей Лукацкий

Бизнес-консультант по безопасности

Несколько предпосылок

- Безопасность системы равна безопасности самого слабого звена
- Построение системы безопасности должности начинаться с моделирования угроз
- Угрозы могут быть совершены не только на технологическом, но и на организационном или «человеческом» уровнях
- Нельзя анализировать безопасность в отрыве от защищаемой системы

Рассматриваемые заблуждения

- Виртуальная клавиатура спасает от троянов
- Одноразовые коды предотвращают несанкционированное списание средств со счета
- SMS-аутентификация делает невозможной действия злоумышленников
- USB-токены с неизвлекаемыми ключами спасают от кражи ключей ЭЦП
- SSL обеспечивает защиту транзакций в Интернет

Виртуальная клавиатура и keylogger’ы

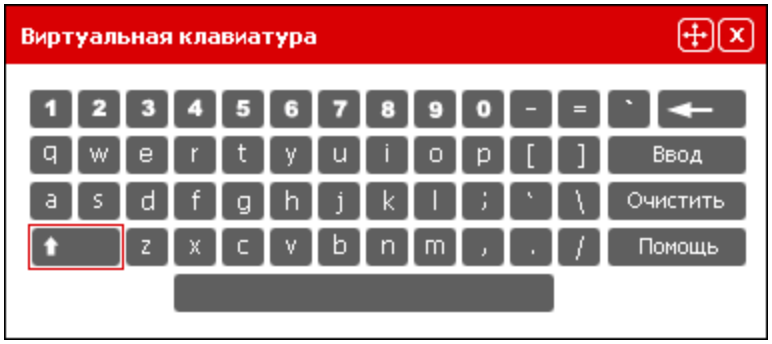
Что делает виртуальная клавиатура

- Защита от перехватчиков ввода с клавиатуры
- Защита от специальных механизмов в троянах

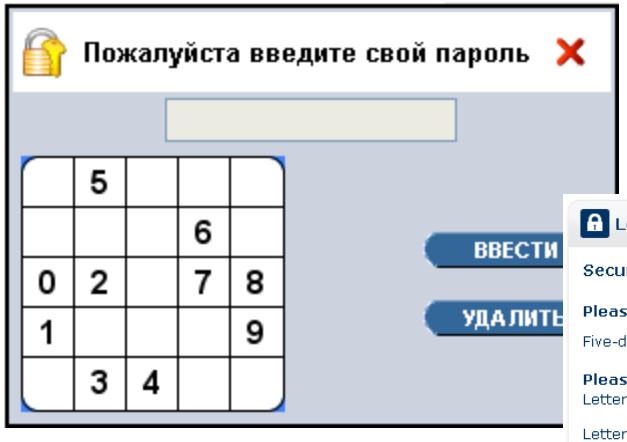
  Bancos, Ldpinch, Refest, Finero, Bankerash, Bancodor и т.п.
- Исключение перехвата ввода логина, пароля, ключевого слова, PIN-кода с обычной клавиатуры

Виртуальные клавиатуры

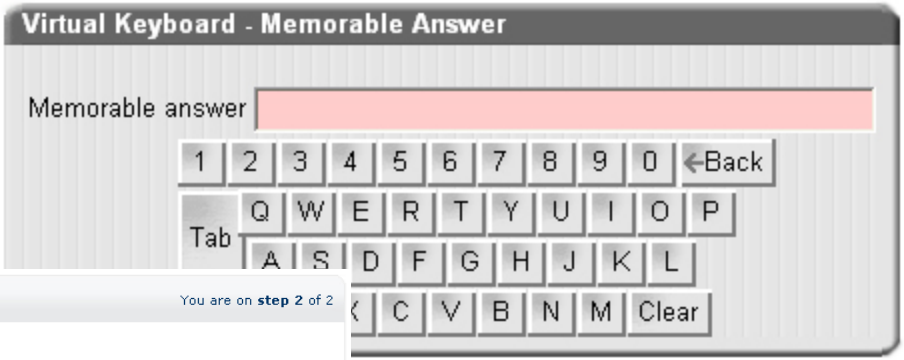
- Различные реализации
  - Обычная клавиатура
  - Случайное расположение клавиш
  - Выбор случайных символов ключевого слова



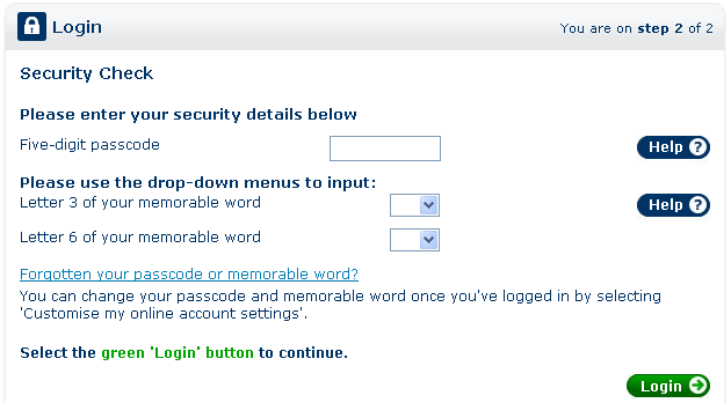
Альфа-банк



BSGV



HSBC



Barclays Bank

Что на самом деле?!

- Перехват координат мышки в момент «кликанья»
  - Многие виртуальные клавиатуры располагаются в одном и том же месте экрана
- Снятие копий экрана и пересылка на e-mail
  - Трояны Bancos и Zeus
  - Уже не важно динамически ли меняется место клавиатуры на экране
- Снятие копии экрана вблизи места клика
  - Снижает объем передаваемой информации
- Контроль буфера обмена
  - Троян Nibu

Что делать?

- Четко понять достоинства и недостатки виртуальных клавиатур
- Повышение осведомленности клиентов

  Если злоумышленник может установить перехватчика ввода с обычной клавиатуры, что мешает ему поставить перехватчика ввода с виртуальной клавиатуры
- Традиционная безопасность клиентов

  Антивирусы, обновление ПО и т.п.
- Статические идентификационные параметры не способны сегодня защитить пользователя банка

  Динамическая смена паролей

  Одноразовые пароли

USB-токен спасает от кражи секретных ключей ЭЦП

Какие бывают USB-токены?

- Обычная USB-флешка
  - По уровню защищенности приравнивается к дискете
- USB-флешки с защищенным хранилищем
  - Например, Verbatim Store ‘n’ Go USB Executive Secure, Kingston DataTraveler или Buffalo RUF2-HSCL-U
  - Ключ ЭЦП только хранится на флешке, а для подписи передается в программу, где и может быть перехвачен, модифицирован и помещен обратно на флешку
- USB-токен с встроенным криптопроцессором
  - Например, VeriSign USB Token, eToken PRO или Rutoken
  - Предыдущий вариант с ярко выраженной функцией идентификации пользователя + 2 области хранения (RW/RO)
  - Кража ключей в момент передачи в программу

USB-токен с генерацией ЭЦП

- Не только хранение ключей ЭЦП, но и их генерация и проверка
  - За счет встроенного специализированного криптопроцессора
  - Например, iBank 2 Key, eToken ГОСТ и Rutoken ЭЦП
- На вход токена подается документ (платежка)
  - На выходе подписанный документ или результат проверки ЭЦП
- Секретный ключ никогда не покидает токен

Но защищает ли это банк и пользователя?

Немного маркетинга

- Как банки и производители продвигают такие токены

  Радикальной мерой борьбы с выявленным трояном, является использование носителя ключевой информации - USB-токен, который делает невозможным копирование ключей ЭЦП

  Это радикальная мера защиты для противодействия хищению ключей ЭЦП Клиента. Основное достоинство заключается в том, что ключи, созданные на USB-токен, невозможно скопировать. Так, физическое нахождение у Вас токена, дает гарантию того, что никто другой им не воспользуется, и Вы смело можете использовать открытые точки доступа в Интернет

В чем угроза?

- Угроза заключается не в копировании ключей ЭЦП
  - Для клиента – несанкционированный перевод его средств
  - Для банка – возврат/потеря средств или удар по репутации
- Угроза может быть реализована не только за счет кражи ключей ЭЦП
- Что если на вход такого токена подать уже поддельное платежное поручение?
  - Безопасность системы равна защищенности самого слабого звена. Защитив токен, мы оставили незащищенным ПО и канал его взаимодействия с защищенным токеном
  - Сложность реализации равна сложности перехвата PIN-кода на доступ к токену

Варианты реализации угрозы

- Подменить платежные реквизиты в банковской программе
- Подменить платежные реквизиты в созданной платежке в процессе передачи ее в токен
- Отдавать в токен две платежки – оригинальную и фальшивую

Усилия по внедрению троянца, крадущего пароли с обычного токена, и троянца, подменяющего платежки, идентичны

Оправдания разработчиков

- Угроза реализуема только в момент физического подключения токена к ПК
  - Достаточно фальсификации всего одной платежки
  - Схема с подменой платежки и рассчитана на подключение токена

Если токен не подключать к ПК, то зачем он нужен?

Что делать?

- Частичное решение – хранение всех подписанных документов в энергонезависимой памяти токена
  - Для разбора конфликтов
  - eToken ГОСТ/Flash – 4 Гб, Rutoken ЭЦП – 64 Кб, iBank 2 Key - ??? (тоже не предусмотрено хранение)
- Необходимо комплексное решение
  - Повышение осведомленности клиента
  - Традиционная защита клиента (антивирус, обновление ПО и т.п.)

А есть еще и side channel attacks

- Side channel attack (атака по сторонним каналам) опирается на сведения, полученные в результате наблюдения за физическим процессом работы USB-токена

  http://www.sidechannelattacks.com/

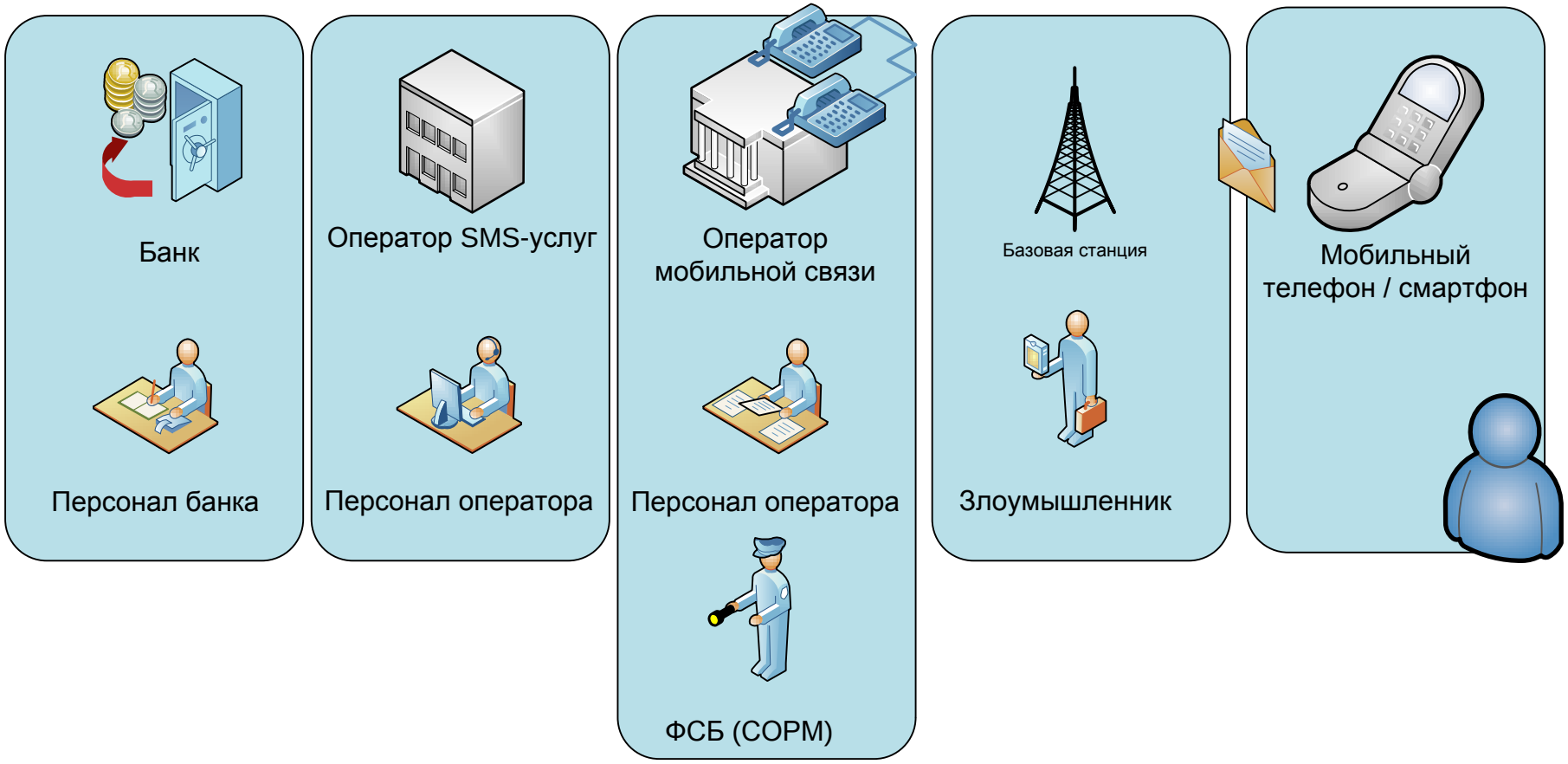
- Атаки данного типа известны с 80-х годов
- Примеры успешных атак на смарт-карты и токены безопасности

Одноразовые коды по SMS спасают от несакционирован-ного перевода средств со счета

SMS как канал взаимодействия

- *Одноразовый пароль необходим для осуществления операций в интернет-банке «Альфа-Клик». Для получения одноразового пароля необходим мобильный телефон, номер которого был указан Вами при подключении услуги «Альфа-Клик». После ввода всех необходимых платежных данных, система предложит ввести одноразовый пароль для совершения операции. Для получения одноразового пароля нужно нажать на кнопку «Получить пароль», пароль будет доставлен SMS-сообщением на Ваш мобильный телефон. После получения SMS проверьте правильность реквизитов платежа, указанных в тексте сообщения, введите пароль и нажмите кнопку «Отправить»*

Рассмотрим систему целиком



Звено «Банк»: угрозы

- Персонал банка

  Прецеденты в российской практике есть

- Вредоносное ПО, интегрированное в банковское приложение

  Банковское приложение отправляет SMS-ки (как обычный мобильный телефон)

  Банковское приложение отправляет специально сформированный XML-запрос по протоколу HTTP(S), который на стороне оператора SMS-услуг транслируется в короткое сообщение клиенту банка

  Банковское приложение передает информацию через шлюз к СУБД, предоставленный оператором SMS-услуг, через стандартный API. Данный шлюз передает информацию оператору, который и транслирует ее в SMS

  Банковское приложение отправляет информацию через SMPP

Звено «SMS-центр/оператор»: угрозы

- Персонал

  SMSки хранятся недолго (3-7 дней максимум), но в открытом виде

  Зарплата персонала SMS-центра низка, а ротация велика

  Примеры передачи за вознаграждение SMS третьим лицам также есть

- SMS-перехват

SMS-перехват

- Три варианта
  - Троянцы, маскирующиеся под перехватчиков
  - Мошенничество
  - Специализированные скрытно работающие программы, устанавливаемые на телефон/смартфон
  - Специализированное оборудование для радиоперехвата
- Специальные программы
  - Пересылают всю информацию по GPRS на указанный e-mail или телефон
  - Поддержка широкого спектра мобильных платформ
  - Например, IntelSpy или Mobcontrol

Радиоперехват

- Разве канал мобильной связи не шифруется?
  - Это не всегда спасает!
- Во время массовым мероприятий с целью снижения нагрузки шифрование часто отключается
  - Празднование 300-летия Санкт-Петербурга
- Шифрование может быть отключено по требованию спецслужб (если не упоминать про СОРМ)
  - Норд-Ост
- Взлом алгоритма A5/1
  - Сейчас взлом занимает несколько часов (Карстен Нол)
  - Группа CCC реализует взлом в реальном времени
  - Привлечение ботнета к взлому

Звено «мобильный телефон»: угрозы

- Кража телефона

  Имеет смысл при длительной недоступности абонента (самолет и т.п.)

- Клонирование телефона

  Только для старых SIM-карт

  Как получить доступ к SIM на время клонирования?

- «Легальное» клонирование

  Доверенность на перевыпуск SIM-карты

Звено «мобильный телефон»: угрозы

- Совет от банка

  В случае возникновения трудностей с получением одноразового пароля, Вам потребуется проверить номер мобильного телефона, указанный в системе Банка. Для этого нужно позвонить в Телефонный центр «Альфа-Консультант» по телефону в Москве +7 (495) 78-888-78 или 8 (800) 2-000-000 (для бесплатного звонка из регионов России). Если указанный Вами номер окажется неверным, необходимо изменить его самостоятельно при помощи любого банкомата в отделениях Альфа-Банка или через сотрудника Альфа-Банка

- При «легальном» клонировании совет не работает

  Телефон не работает

  В офис клиент пойдет не сразу

Парафраз об одноразовых кодах

Еще одна проблема с одноразовыми кодами

- Подмена платежных реквизитов в момент нажатия кнопки «Оплатить» или «Перевести»

  Так действует троян URLzone

SSL обеспечивает защиту транзакций в Интернет

SSL обеспечивает защиту?

- Классическая рекомендация

  Проверяйте, что соединение действительно происходит в защищенном режиме SSL, в правом нижнем углу Вашего вэб-браузера должен быть виден значок закрытого замка

  Защищает нас от атаки «человек посередине»

- 4 сценария атаки

  SSLstrip

  SideJacking

  PhoneFactor

  Фальшивый сертификат

Вопросы?

Дополнительные вопросы Вы можете задать по электронной почте security-request@cisco.com
или по телефону: +7 495 961-1410