

# Аутентификация в системах Интернет-банкинга

Анализ типичных ошибок

Сергей Гордейчик

Positive Technologies



**Аутентификация в системах Интернет-Банк**

**Актуальные векторы угроз**

**Уязвимости приложений**

**Системы одноразовых паролей**

**Цифровые сертификаты**

**Резюме**

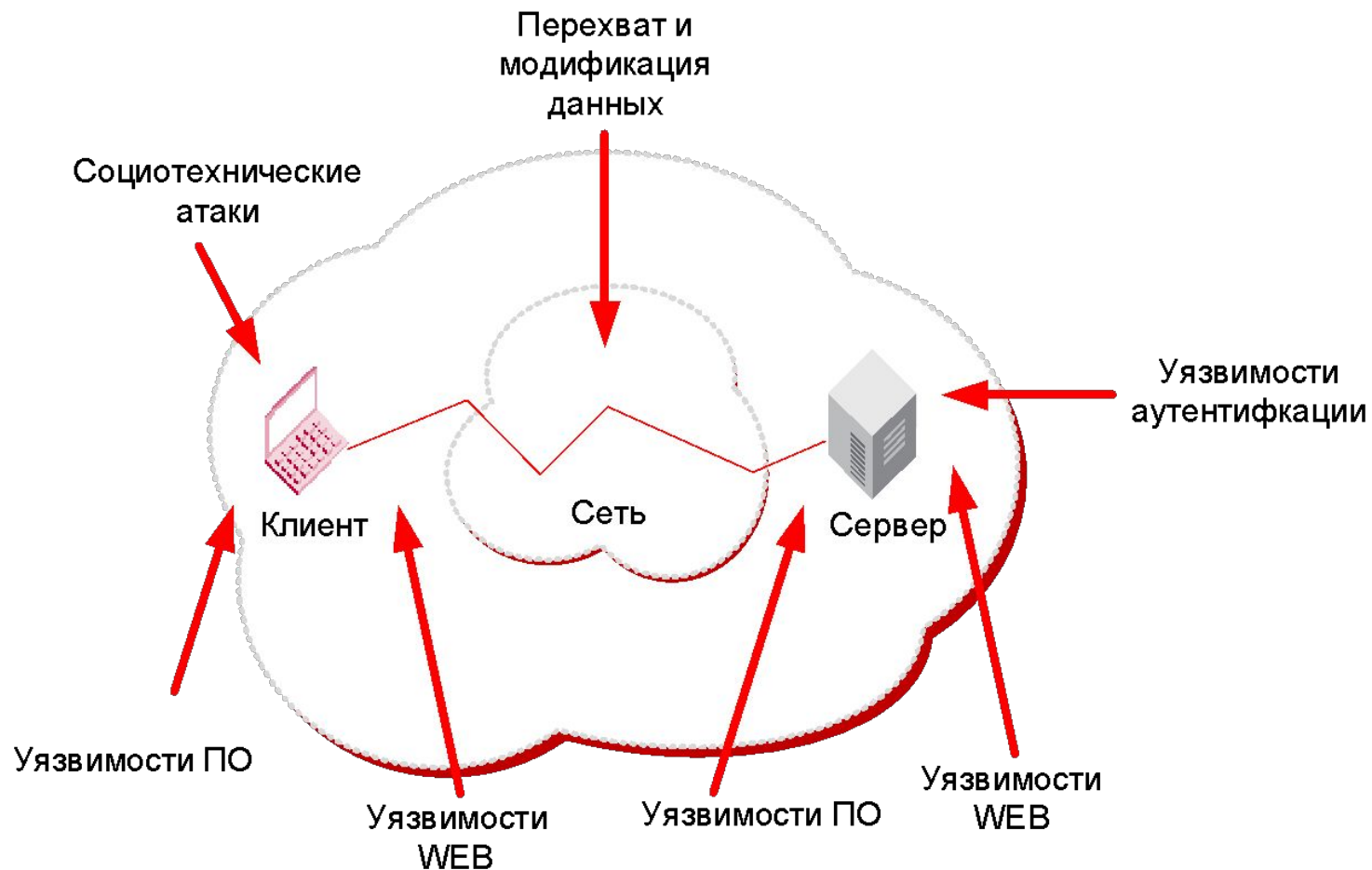


# Аутентификация в Интернет-Банках

- **Требуется обеспечить высокий уровень безопасности**
- **Широкое использование Интернет-технологий**
  - HTTP/HTTPS для передачи данных
  - Клиент - стандартный браузер и расширения (AJAX, ActiveX, Java)
  - Наследование уязвимостей Web-приложений
- **Низкое доверие к каналу связи и стандартным средствам криптографической защиты**
  - Высока опасность успешных атак типа «фишинг», «человек по середине»
- **Низкое доверие к рабочему месту клиента**
  - Вероятно отсутствие обновлений безопасности
  - Низкий уровень ИТ и ИБ грамотности
  - Возможно наличие вредоносных программ
  - Вероятна работа с недоверенного рабочего места



# Актуальные векторы угроз



- **Большинство транзакций производится из незащищенных сетей**
- **Как правило, применяется SSL/TLS (SSL+ГОСТ), что обеспечивает адекватный уровень защиты**
- **Комбинации технических и социотехнических атак**
- **SSL/TLS + аутентификация клиента по сертификатам**



- **Самая большая проблема**
- **Защита рабочих мест вне компетенции владельца ИС**
- **Рекомендательный характер мер**
- **Отсутствие обновлений, антивирусного ПО, пиратское ПО**
- **Широкое использование социотехник злоумышленниками**
- **Высокий уровень развития вредоносного ПО**



- **Менее популярны, но не менее эффективны**
- **Зачастую присутствуют уязвимости Web-приложений**
- **Уязвимости Web-сервера могут использоваться для атак на клиентов (XSS, CSRF)**
- **SSL – не защита от уязвимостей Web-приложений**



# Системы одноразовых паролей

- **Достаточно широко распространены**
  - Невысокая стоимость при потенциальной защищенности
- **Мало зависят от ОС/Браузера**
- **Возможны разные варианты реализации**
  - Заранее рассчитанные списки паролей
  - Генераторы паролей
  - SMS-сервис





- **Уязвимости Web-приложений**
  - Наличие уязвимости позволяет провести транзакцию без знания пароля
  - Необходимость контроля HTTP-сессии
- **Одноразовые пароли тоже пароли**
  - Возможен перехват
  - Небольшая энтропия – подбор значения
  - Большое «окно»



- **Наиболее мощный инструмент**
- **Позволяют компенсировать уязвимости Web-приложений**
  - Транзакция должна быть подписана
- **Зависят от ОС/Браузера**
- **Использование для защиты сети (SSL/TLS)**
- **Основные проблемы связаны с хранением закрытого ключа**



- **«Серверный» SSL/TLS недостаточно надежен**
  - Велика вероятность социотехнических атак
  - Аутентификация клиента по сертификатам
- **Уязвимости Web зачастую не учитываются**
  - Большинство Web-приложений содержит серьезные проблемы
  - Анализ защищенности/использование Web Application Firewall (PCI DSS)
- **Одноразовые пароли – тоже пароли**
  - К ним применимы стандартные парольные атаки
  - Стандартные контрмеры (защита от подбора и т.д.)
- **При использовании сертификатов требуется надежное хранилище**
  - Смарт-карты и токены



# Спасибо за внимание!

Сергей Гордейчик

[gordey@ptsecurity.ru](mailto:gordey@ptsecurity.ru)



POSITIVE TECHNOLOGIES