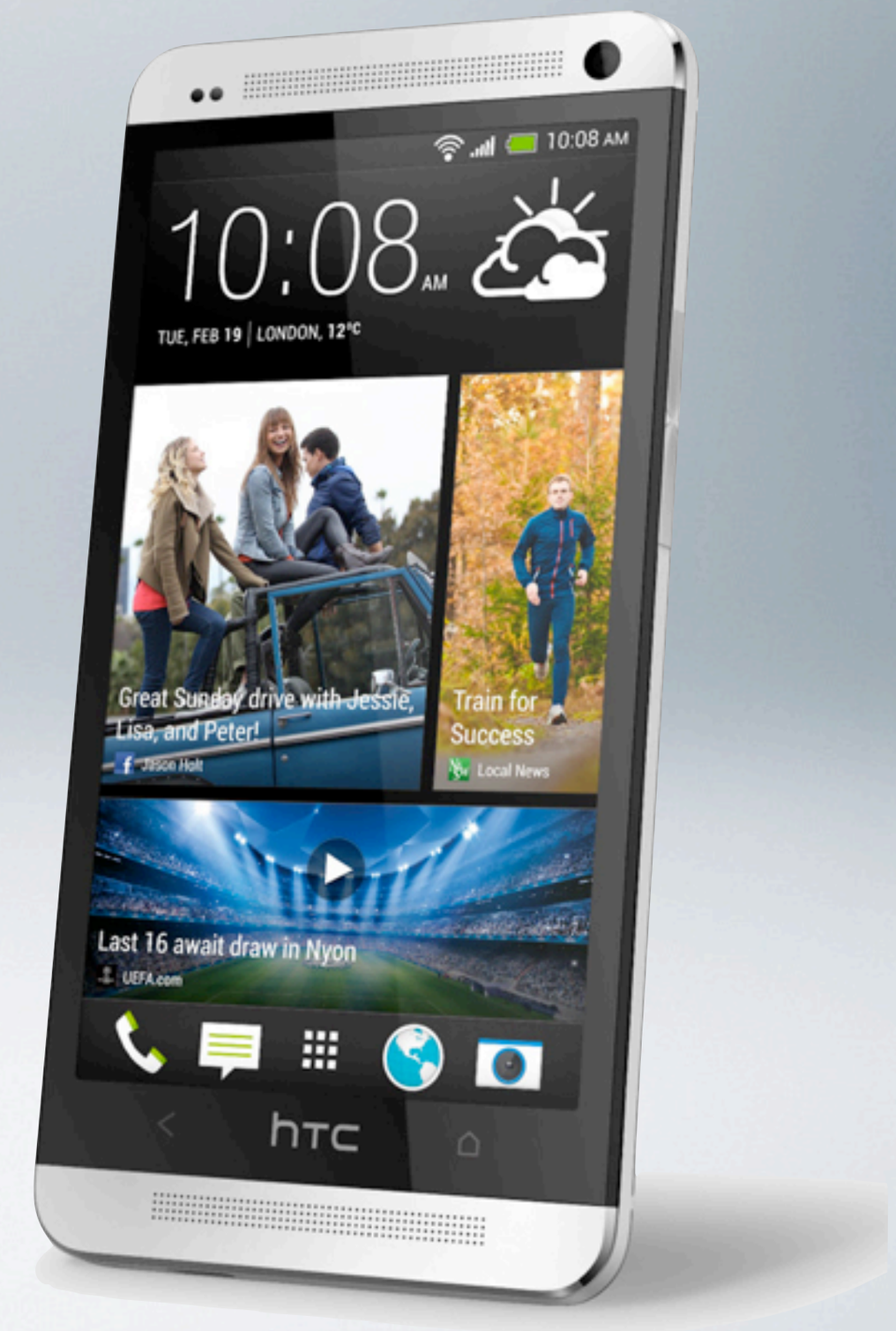
БЕЗОПАСНОСТЬ В МОБИЛЬНОМ БАНКИНГЕ

Максим Орловский
операционный и тех. директор
http://dev-iq.com
orlovsky@dev-iq.com

Основные типы угроз на стороне клиента

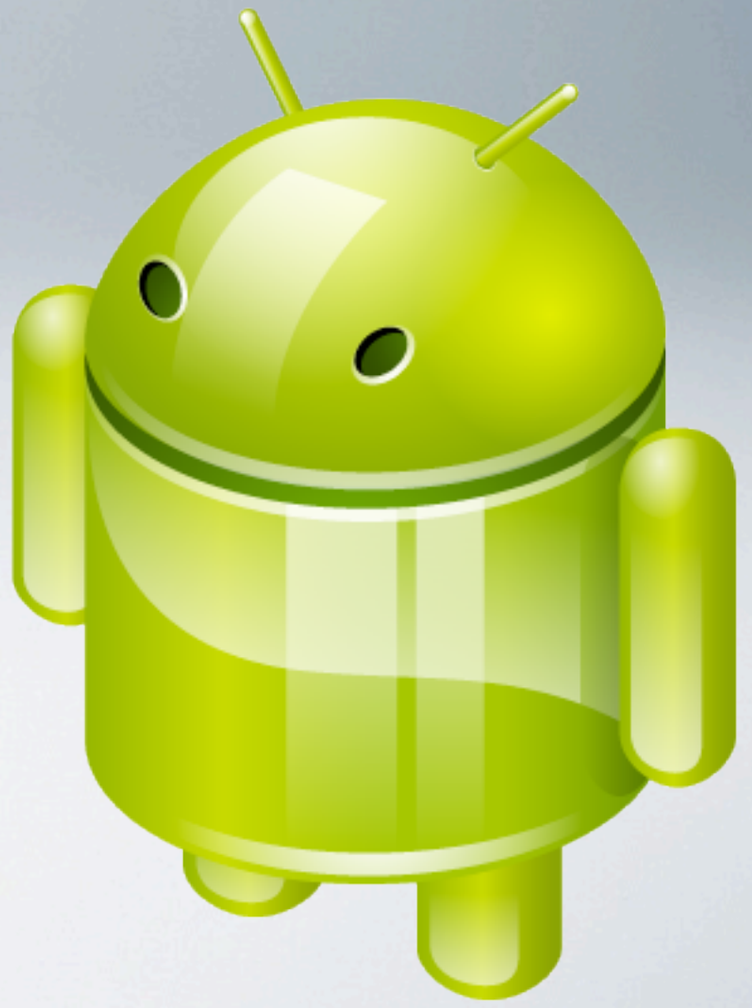
- Фишинг
- Троянские программы
- Перехват информации как внутри устройства, так и при передаче по сети
- Похищение и взлом



Dev iQ

Android: надо бдить

- Высокая уязвимость к фишингу
  - Единственная защита — информирование пользователей (малоэффективно)
- Троянские программы
  - Не хранить персонализированную информацию на телефоне
- Перехват информации
  - SSL
- Похищение и взлом
  - Не хранить персонализированную информацию на телефоне



iOS: защищенная закрытая платформа

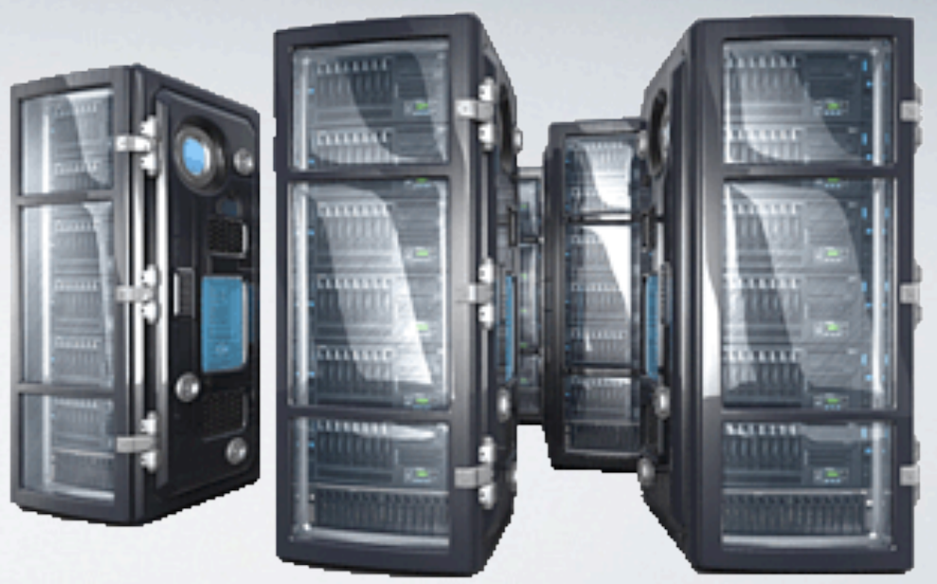
- Фишинг практически невозможен
- Троянские программы невозможны
- Перехват информации внутри ОС невозможен
- Похищение и взлом
  - Не хранить персонализированную информацию на телефоне

Внимание:

недопустимость Jailbreak

Угрозы на стороне банка

- DDoS от троянских коней и виджетов
- Прямое использование вызовов API
- Bruteforcing

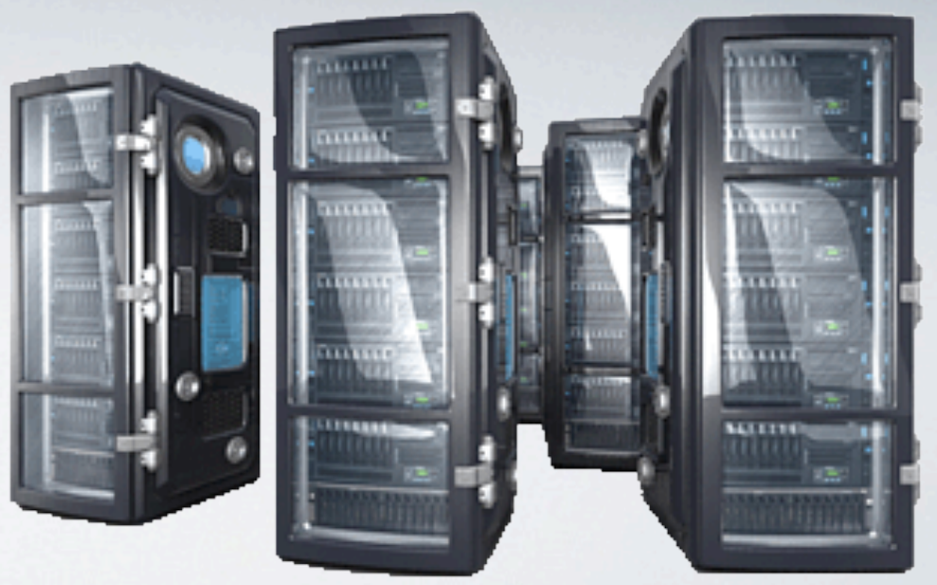


Dev iQ

Решения на стороне банка

Использование выделенного слоя бизнес-логики и системы безопасности для мобильного банкинга:

- интенсивное кэширование;
- лимиты на количество транзакций;
- лимиты на суммы операций;
- привязка операций к уникальным идентификаторам телефонов

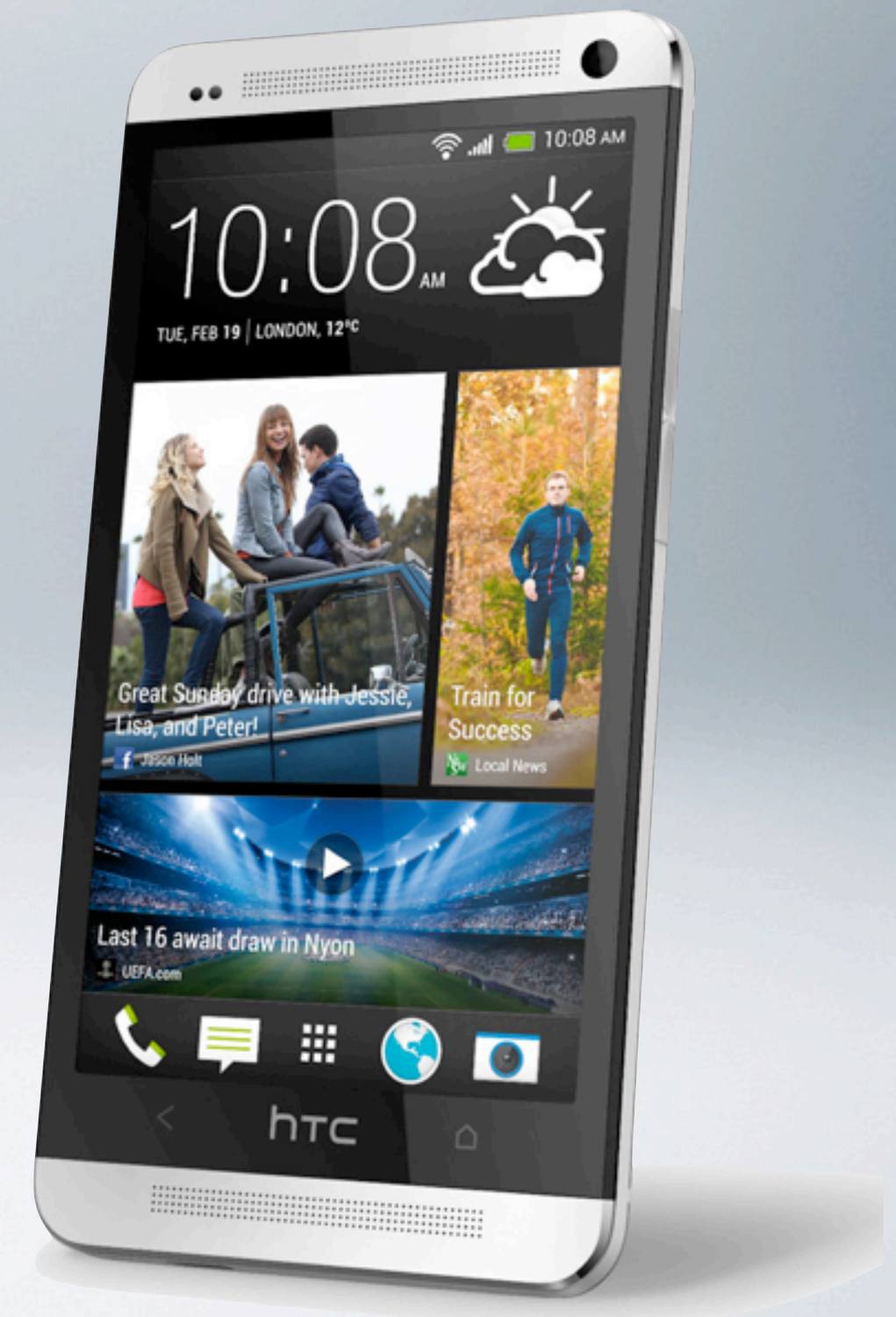


Dev iQ

Правильный подход к мобильному банкингу

Дайте пользователю совершать основные действия как со своим кошельком:

- платежи без пароля
- всегда видить баланс



Dev iQ

Как этого достичь?

- Устройство-специфическая функциональность (дифференциация телефонов и планшетов)
- Многоуровневые политики лимитов по операциям: похищение мобильного должно быть не дороже, чем похищение кошелька
- Возможность блокировки работы приложения на телефоне с сервера банка

Dev iQ

БЛАГОДАРЮ ЗА ВНИМАНИЕ!