POSITIVE TECHNOLOGIES

Актуальные проблемы двухфакторной аутентификации в финансовых сервисах для физических лиц

Юнусов Тимур

Positive Technologies

Старший эксперт,
руководитель отдела безопасности банковских систем

Кто

О нас:

— Десятки аудитов и работ по анализу защищенности банковских продуктов ежегодно

— Постоянное желание увеличивать свою компетенцию

— Ежегодная статистика

Обо мне:

— Почти 6 лет в Application Security

Почему

— Одноразовый код в СМС - стандарт де-факто, но так ли он хорош?

— Используется не только в финансовых продуктах

Почему

— Потери от мошенничества в банках растут ежегодно (26% в 2015г)
  - Атаки на пользователей
  - Атаки на банки

Почему

— Потери от мошенничества в банках растут ежегодно (26% в 2015г)

- Атаки на пользователей
- Атаки на банки
- **Атаки на пользователей через проблемы банков**

Двухфакторная аутентификация

Знаю (пароль), обладаю (устройство):

- Одноразовые пароли (СМС, генераторы OTP, чеки)
- Криптоподпись операций (токены, клиентские сертификаты)
- Остальное (голосовая аутентификация, кодовое слово и т.д.)

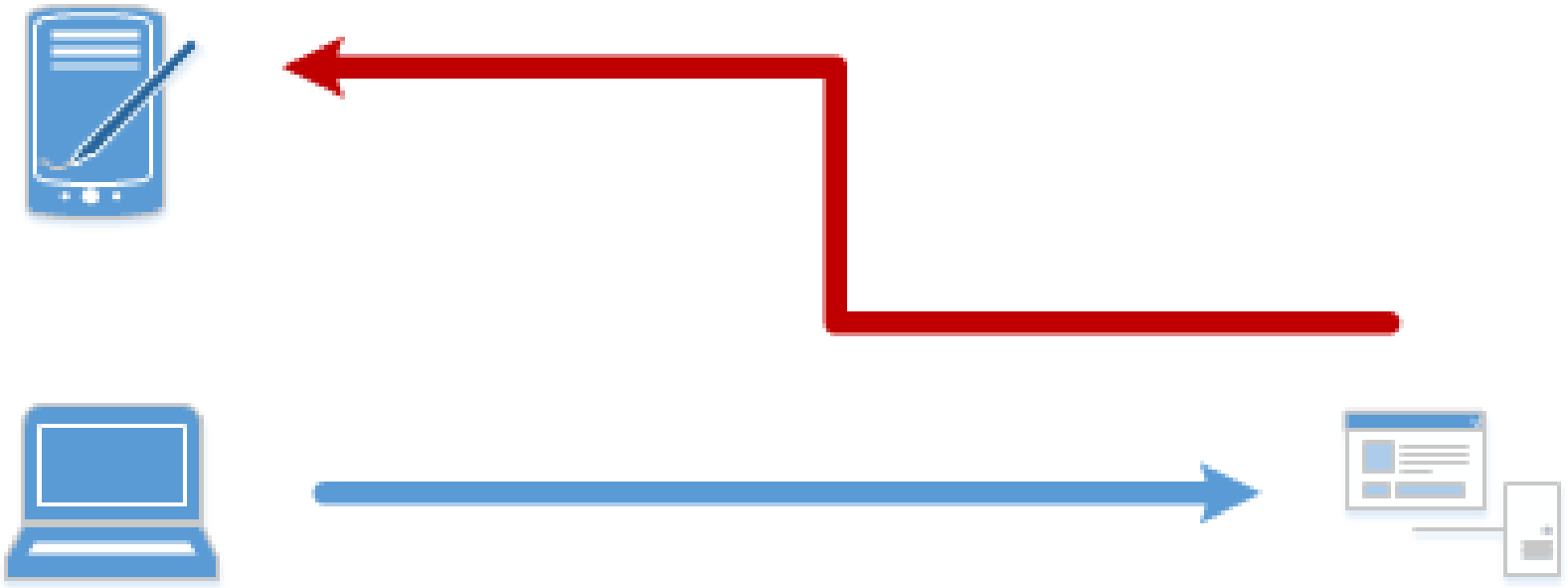
ДА в банковских продуктах для физлиц

— **Одноразовые пароли в СМС**

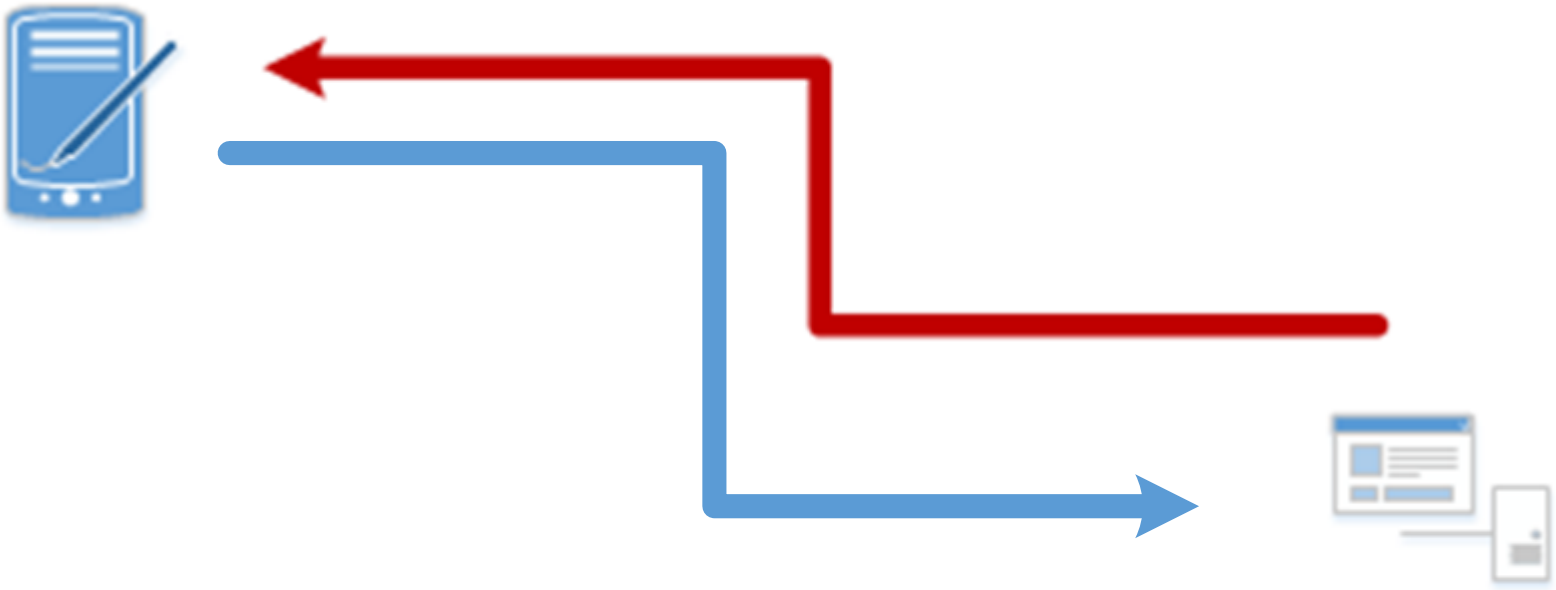
- Вход в систему
- Критичные операции
- Финансовые операции

Двухфакторная аутентификация

Двухфакторная аутентификация



Мобильный банк?



Требования к одноразовому паролю

—Уникальность

—Атомарность

—3 попытки на пароль

—Временное блокирование

—Длина – тоже мера!

Что может пойти не так?

Проблемы

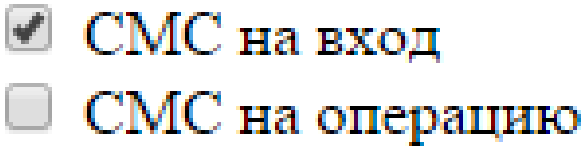
- Проблемы на стороне банка
- Проблемы на устройстве
- Проблемы в канале
- **Проблемы на стороне клиента в банке**

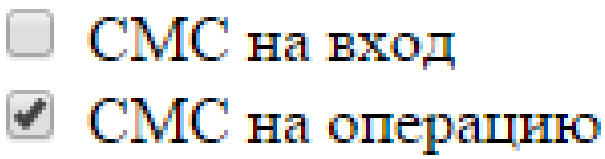
Проблемы на стороне банка

- Бизнес-логика / Логика?
- Атаки на ГПСЧ
- Другие методы

Бизнес-логика

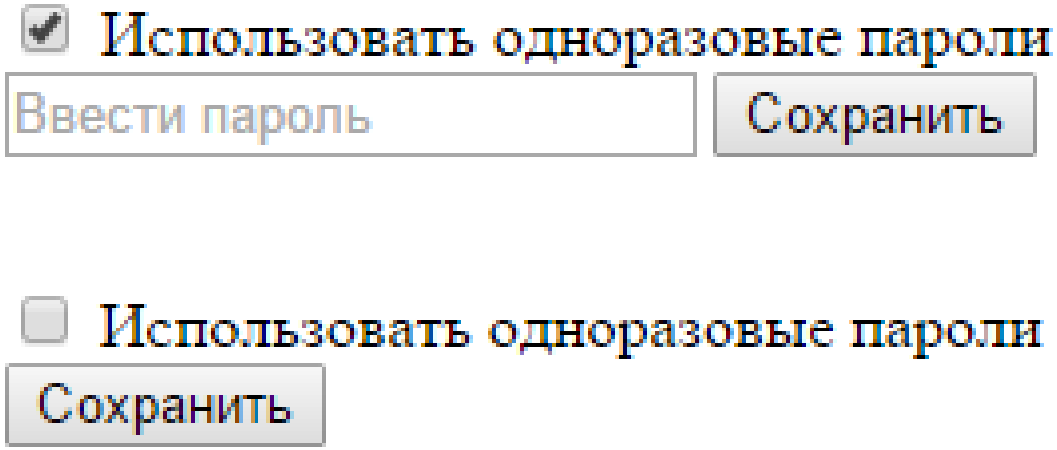
—Пример 1





Бизнес-логика

—Пример 2



Бизнес-логика

—Пример 3

```
POST /templates/ HTTP/1.1
Host: mobilehost

fields_object={
  "account_" : "34909312",
  "amount" : "150.00",
  "debitid" : "2476178"
}
```

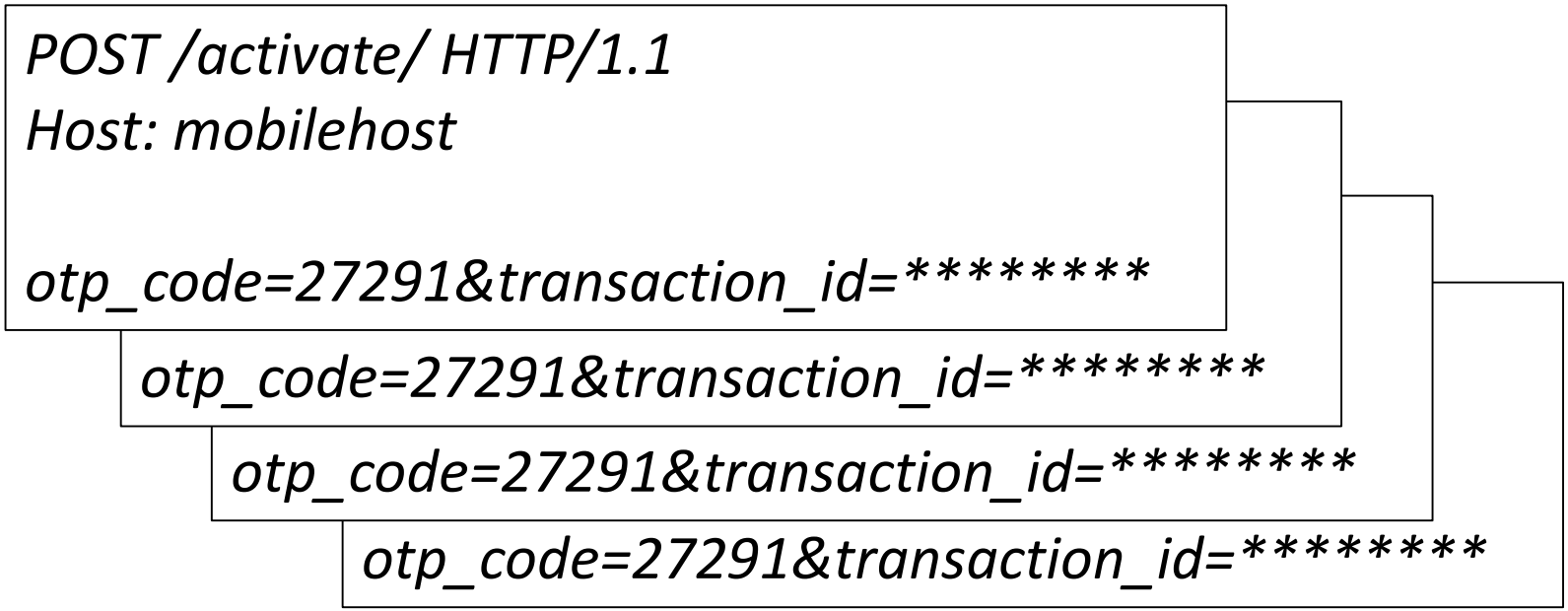
Бизнес-логика

—Пример 3

```
fields_object={
  "account_" : "34909312",
  "amount" : "150.00",
  "debitid" : "2476178"
}
```

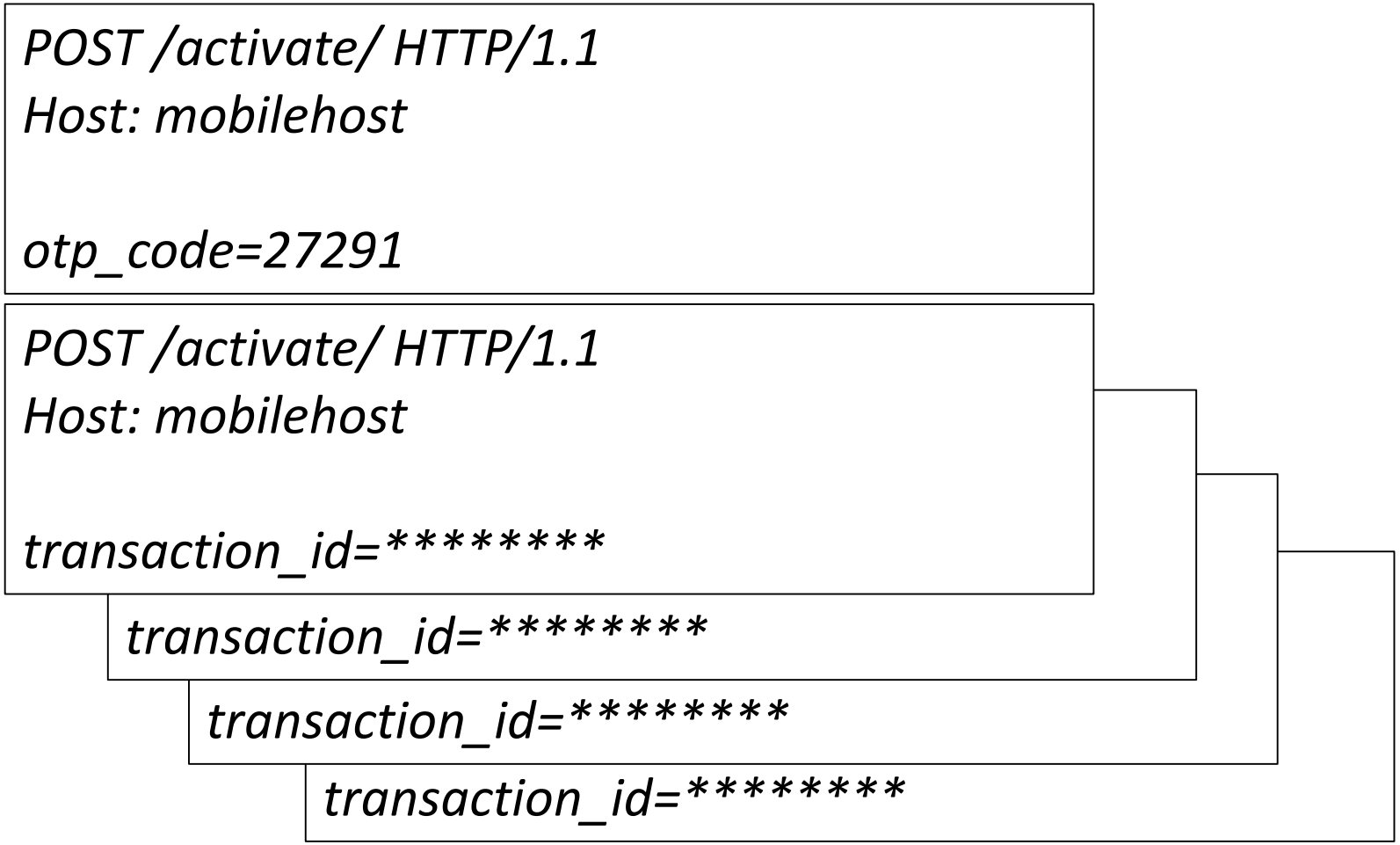
Бизнес-логика

—Пример 4



Бизнес-логика

—Пример 5



Бизнес-логика

—Пример 6

POST /activate/ HTTP/1.1

Cookie: {EMPTY}

Host: otherhost.bankhost

otp_code=27291

HTTP/1.0 301 Moved Permanently

*Location: https://bankhost/auth/?login=**ivanov***

Бизнес-логика

—Пример 7

- 3 попытки на пароль
- ~~Временное блокирование~~

12345; 12346; 12347

ГПСЧ

- **Java:** Java.util.Random(), Math.random(), java.security.SecureRandom();
- **Windows:** LCG

Другие методы

- SQLi
- XXE/SSRF
  - XXE+WebLogic admin
- Remote Code Injection/Execution

Проблемы на стороне клиента в банке

—Атаки на клиентов:

- Clickjacking/UI redress
  - —X-Frame-Options (27%-33%, исследование DSec)
- XSS (36%)

(Бес)Полезные смс

Dlya perevoda s karti na kartu na summu 0.10 RUB vash odnorazoviy parol:104659. Ne soobshayte etot parol nikomu,v tom chisle sotrudnikam bankov.

Ваш код 6573. Не сообщайте никому, включая сотрудника Банка

10:30 26.06.14
Vash odnorazovyj parol dlja sovershenija operacii v Internet: 182365

27 Jun 2014 13:56

Проблемы в канале

— Интернет
  - Заголовок HSTS (36%-38%, исследование DSec)
— 2G/3G/LTE

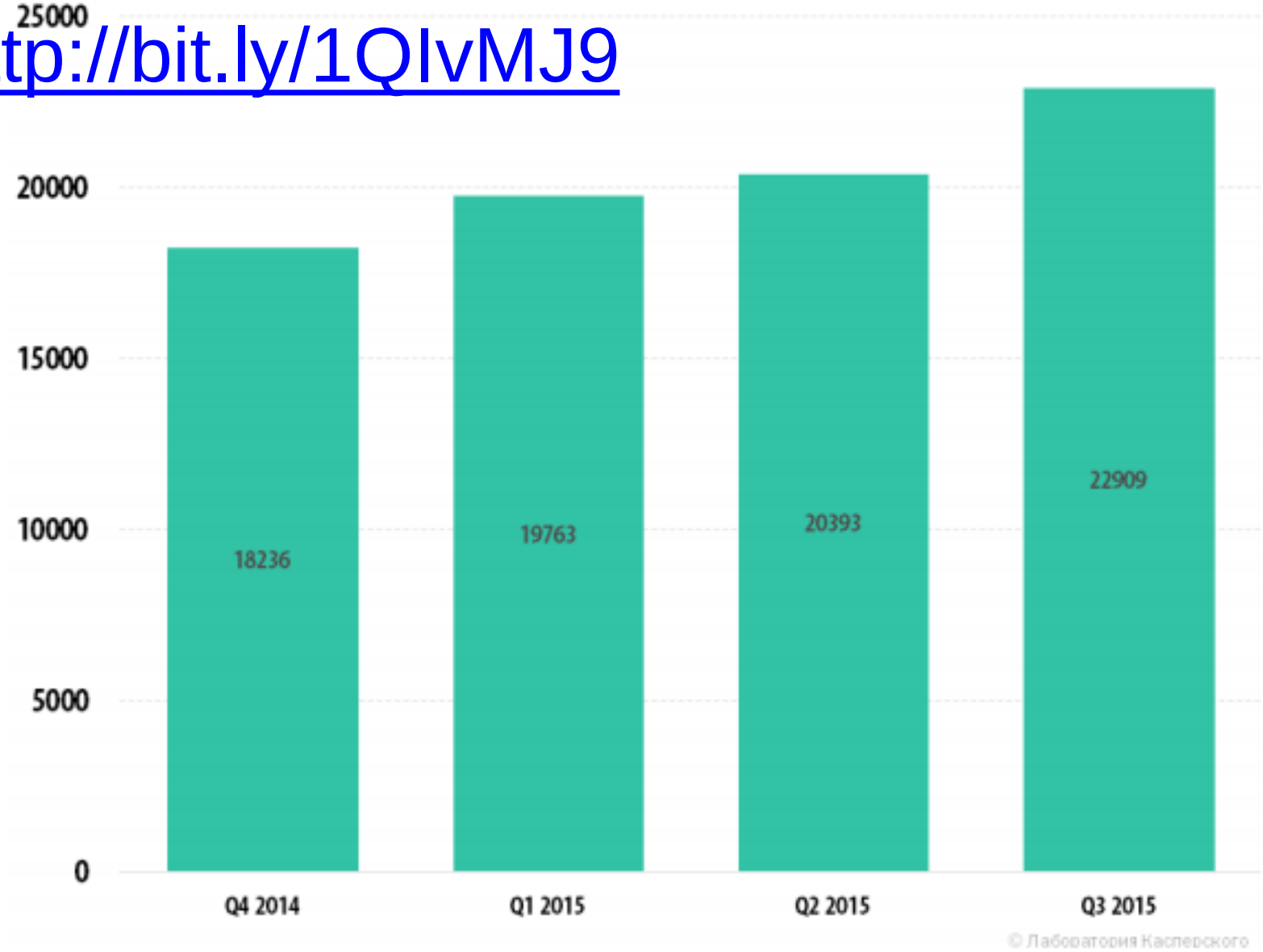
Мобильный интернет

- Недостатки СМС/USSD
- Перевыпуск SIM
- Клонирование SIM
- Перехват радиосигнала+Kraken
- FakeBTS
- Атаки на SS7 http://bit.ly/1mHgZ9j

Проблемы на устройстве

- Банковская мобильная малварь
  - Q3/2015 = 4 * Q2/2015
- Jailbreak detection
- Недостатки мобильных приложений

http://bit.ly/1QIvMJ9



Количество мобильных банковских троянцев в коллекции «Лаборатории Касперского» (Q4 2014 – Q3 2015)

Проблемы на устройстве

- Банковская мобильная малварь
  - Q3/2015 = 4 * Q2/2015
- ~~Jailbreak detection~~
- Недостатки мобильных приложений

Проблемы на устройстве

— Пример 1

- BroadcastReceiver

Проблемы на устройстве

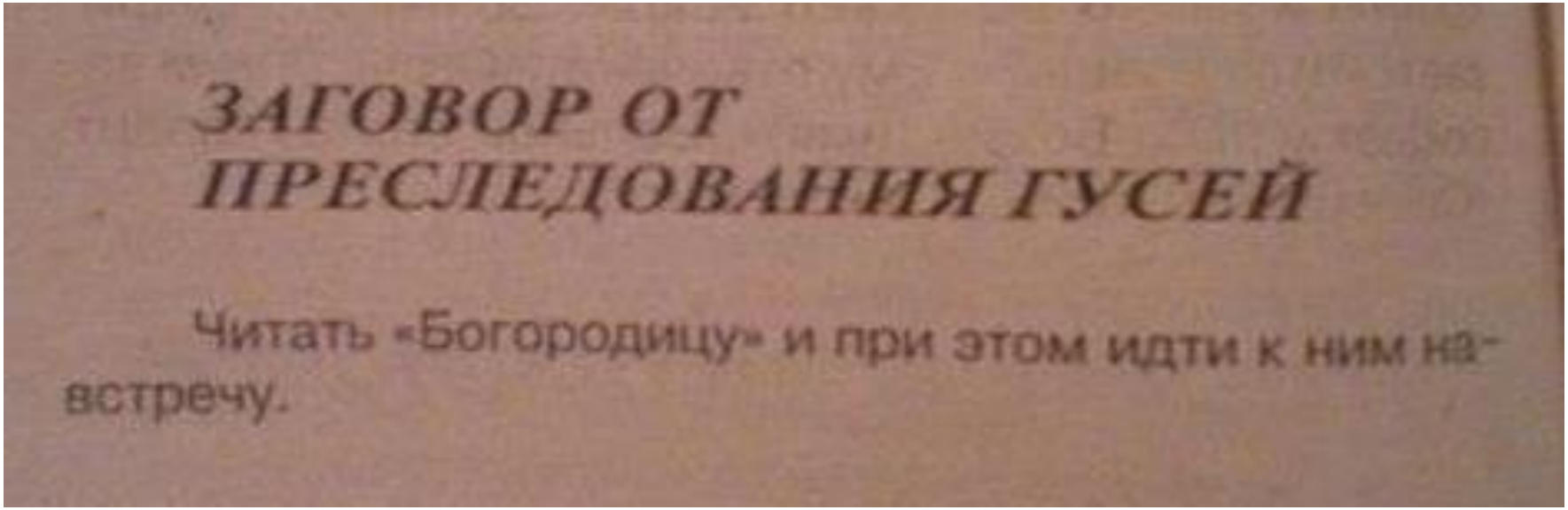
— Пример 2

- SIM Applications spoofing/intercepting

Статистика 2015

- 27% проектов не содержали уязвимостей
- 36% содержали XSS, которые помогали злоумышленникам в фишинговых атаках и обходе механизмов ДА
- 54% проектов некорректно реализовывали механизмы ДА, что позволяло их обходить тем или иным способом.

Как перестать быть самым слабым звеном



ЗАГОВОР ОТ
ПРЕСЛЕДОВАНИЯ ГУСЕЙ

Читать «Богородицу» и при этом идти к ним на-
встречу.

Как перестать быть самым слабым звеном

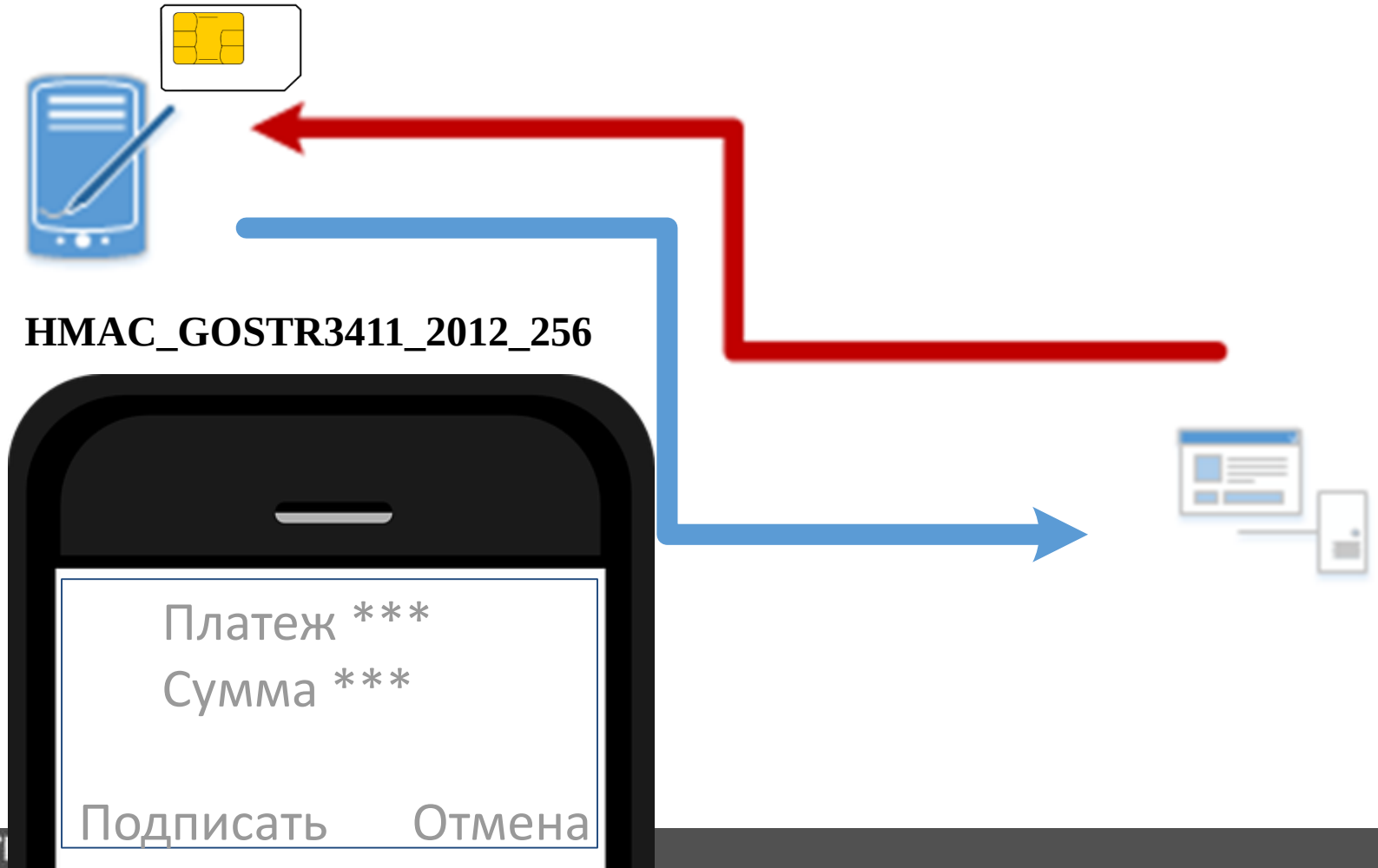
- Взаимодействие с операторами
  - IMSI
- Корректная реализация алгоритма на сервере и мобильном клиенте
- Защита периметра
- Обучение клиентов и сотрудников
- Антифрод

Что, если не СМС

- Мобильное приложение с криптографическим ключом
  - Извлекаемость ключей
  - Требования к аппаратной части
- Мобильное приложение для генерации ОТП
- DCV от Gemalto
  - Только карточный фрод
  - Технические ограничения (перевыпуск карт)

Что, если не СМС

—Решение от КРИПТО-ПРО



Плюсы

- Появление «второго фактора»
- Никакого «тупого» перебора
- Атаки на атомарность по GSM
- Пример 6
- ГПСЧ
- Атаки на GSM, перевыпуск SIM
- Больные вопросы с CMC/USSD

Минусы

— Атака на сервер и извлечение симметричного ключа (если ты в АБС, то можно просто создать платеж)

— Заражение 2 устройств из 3

- Банк-клиент
- Сервер
- Смартфон

Спасибо!

Вопросы?

@a66at

https://uk.linkedin.com/in/tyunusov

tyunusov@ptsecurity.com