ThreatMetrix®
The Digital Identity Company™

Ценность доверия

Андрей Ковалев
ThreatMetrix

IX Уральский Форум «Информационная безопасность финансовой сферы»

Пользователь или мошенник?

"On the Internet, nobody knows you're a dog."

А кому это важно?

Интернет-банк?

Платежная система?

МФО?

Вы взаимодействуете с пользователями через интернет?

Ключевые точки взаимодействия

Регистрация

- Новый пользователь?
- Бот?
- Массовая регистрация?

Логин

- Владелец аккаунта?
- Украденые реквизиты?
- Подбор паролей?

Операция

- Нормальная операция?
- Социальная инженерия?
- Подмена данных транзакции?

Доверие

- Незнакомец?
- Мошенник?
- Ваш доверенный пользователь?
- Ваш доверенный пользователь – но с ним что-то произошло?

Как определить, можно ли доверять?

Классический способ – аутентификация.

Пароли – закопайте их уже!

Password	Length
pussy.passwordLimitExceeded:07/1	32
gladiatoreetjaimelesexetjaimefum	32
antidisestablishmentarianism	28
pussypussymoneymoneyweedweed	28
1234tellmethatyoulovememore	27
ifyourreadingthisitstoolate	27
12bucklemyshoe34shutthedoor	27
iloveyousomuchdarling123456	27
fuck her right in the pussy	27
killerklownzfromouterspace	26
sexisthesecretofmyenergy	24
thingsyouseeinagraveyard	24
schrodingersfavouritecat	24

Трение – сложно пользователям, легко врагам

Слишком простой пароль
Вы ввели пароль, который легко подобрать. Из соображений безопасности Вам нужно задать более сложный пароль.

Текущий пароль ●●●●●●●●●●●●●●●●●●●●●●●●

Новый пароль ●●●●●●●●●●●●●●●●●●●●●●●●●●●●●●●●

Повтор нового пароля ●●●●●●●●●●●●●●●●●●●●●●●●●●●●●●●●

Имя

Фамилия

День рождения день ▾ месяц ▾ год ▾

Город

Пол ○ Мужской ○ Женский

Почтовый ящик

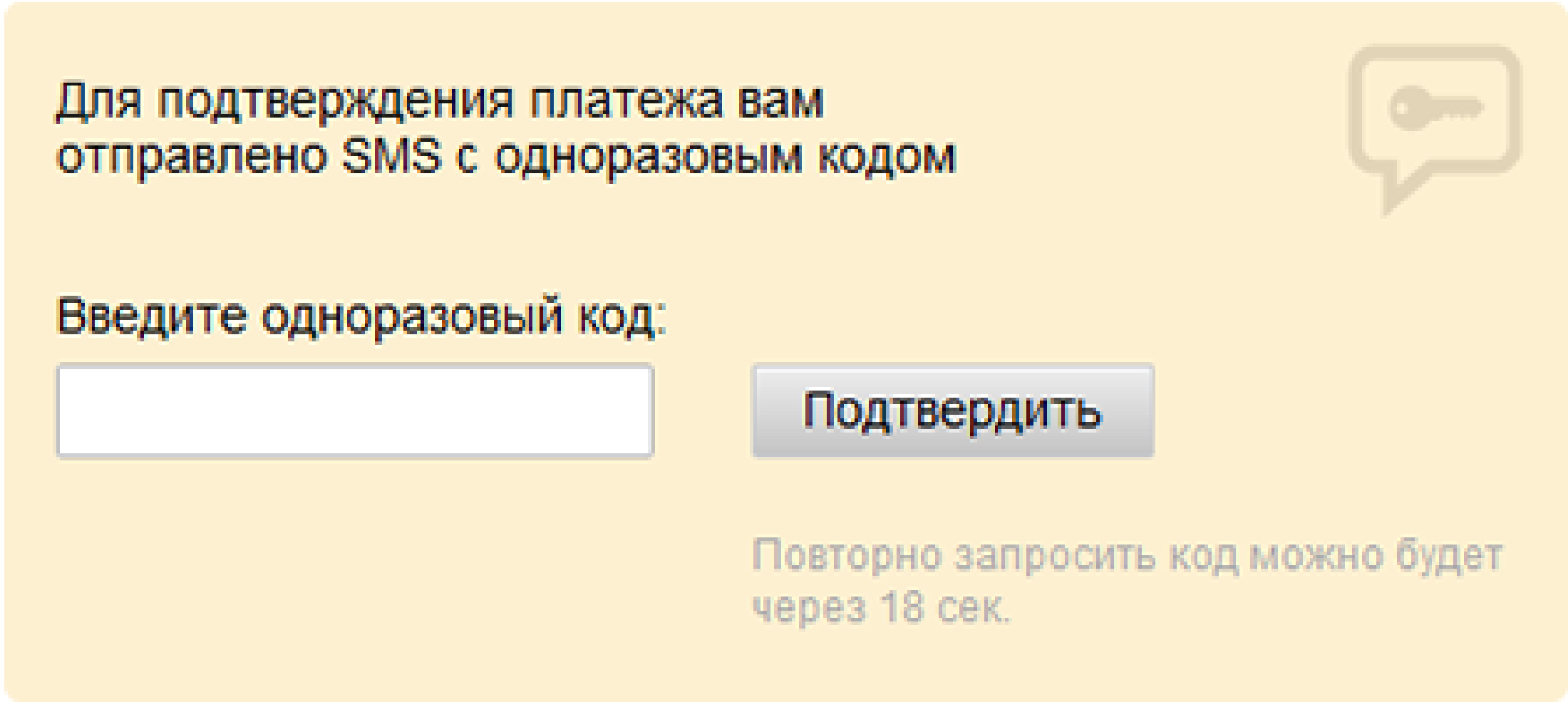
Пароль

Повторите пароль

Мобильный телефон Россия ▾ +7

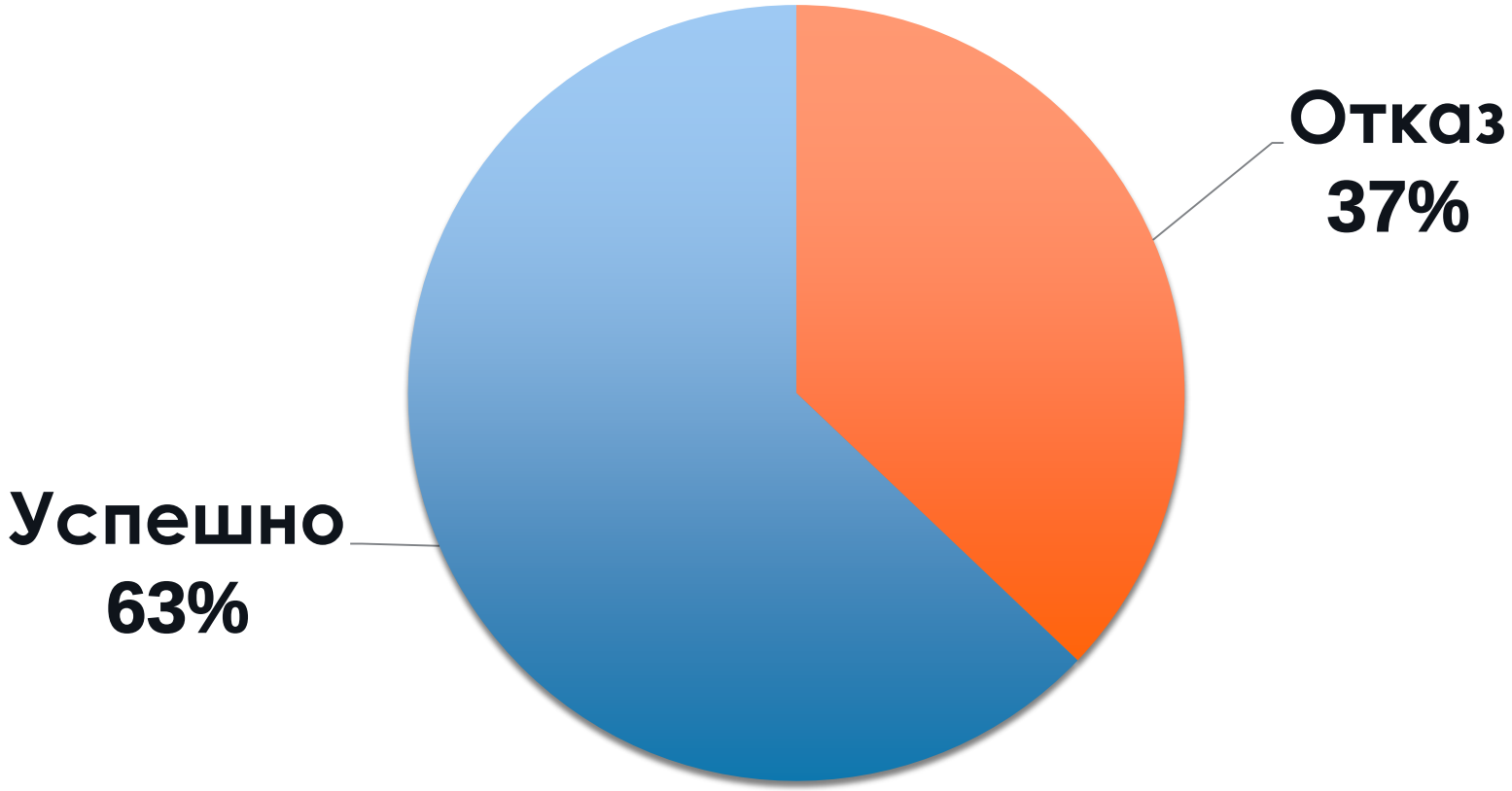
ThreatMetrix®

Давайте улучшим аутентификацию



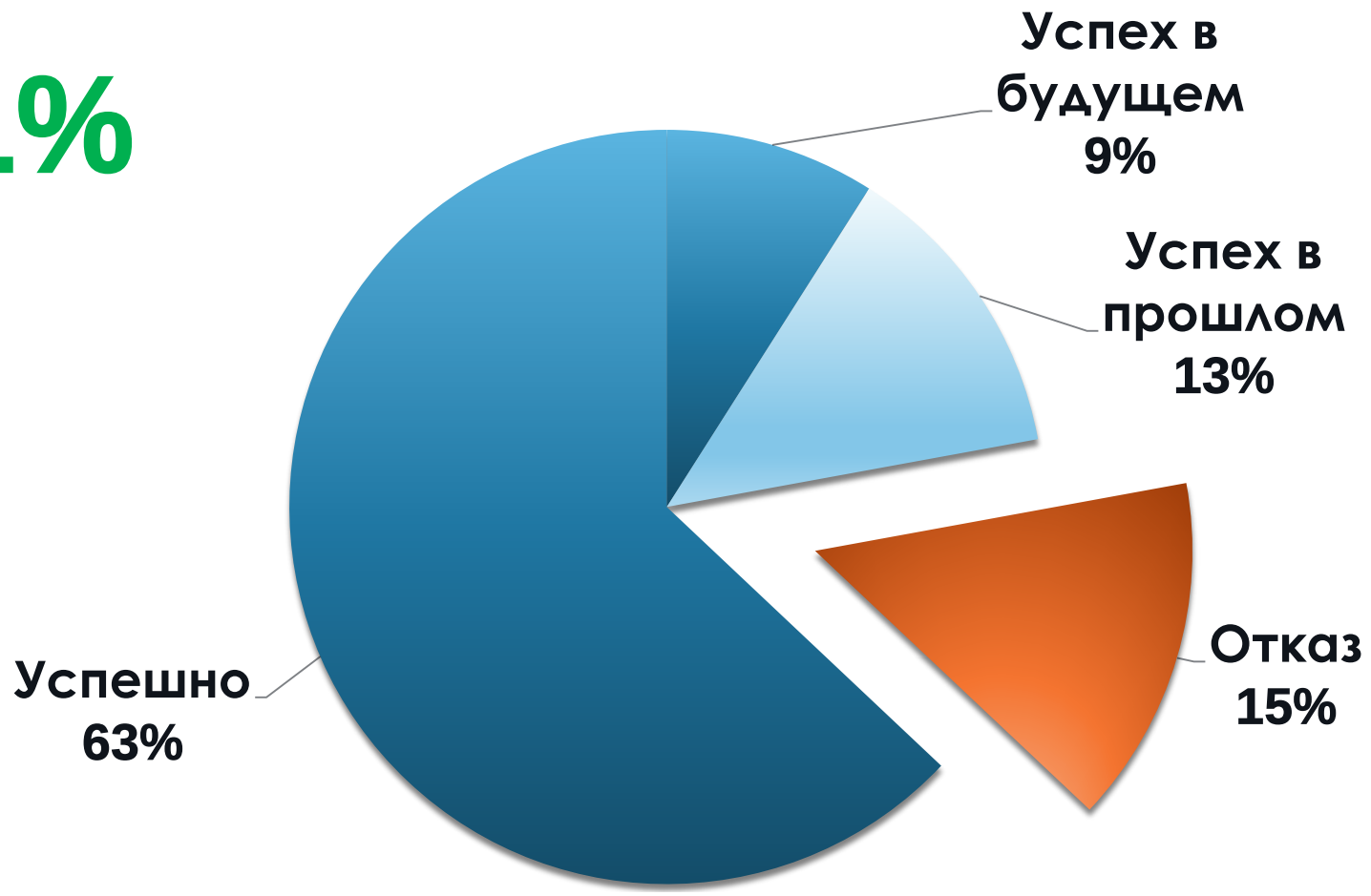
ThreatMetrix®

Одноразовые пароли по SMS спасают от мошенников



Одноразовые пароли спасают от пользователей

21%



И не всегда спасают от мошенников

4.4. Intercepting incoming SMS messages

Goal: Intercept a subscriber's incoming SMS messages.

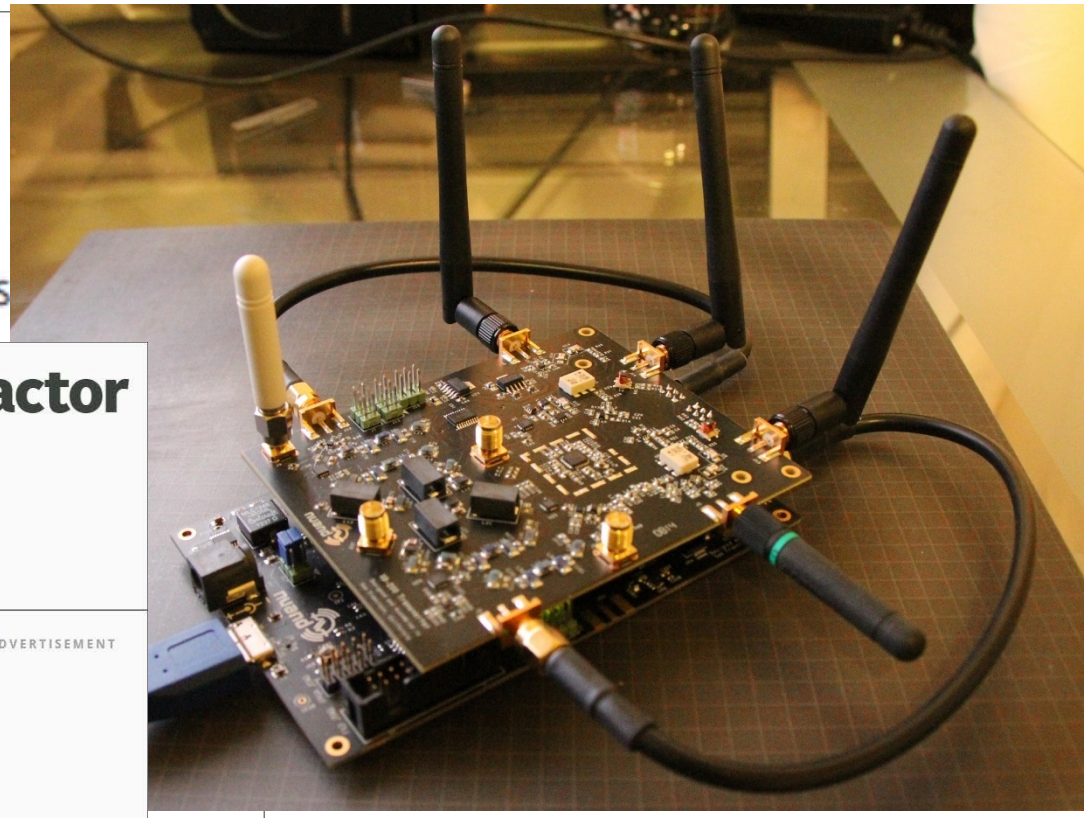
Description: This attack is an extension of Attack 4.3 and does

addition

NIST declares the age of SMS-based 2-factor authentication over

Posted Jul 25, 2016 by Devin Coldewey, Contributor

ADVERTISEMENT



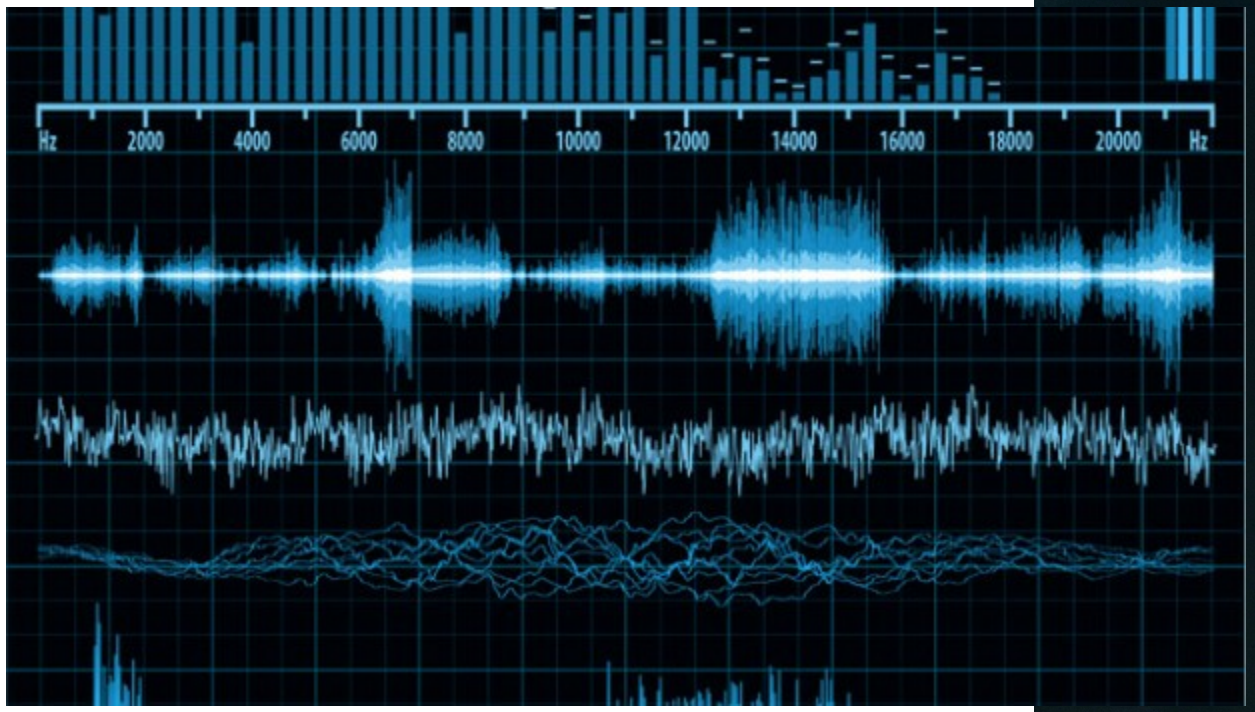
ThreatMetrix®

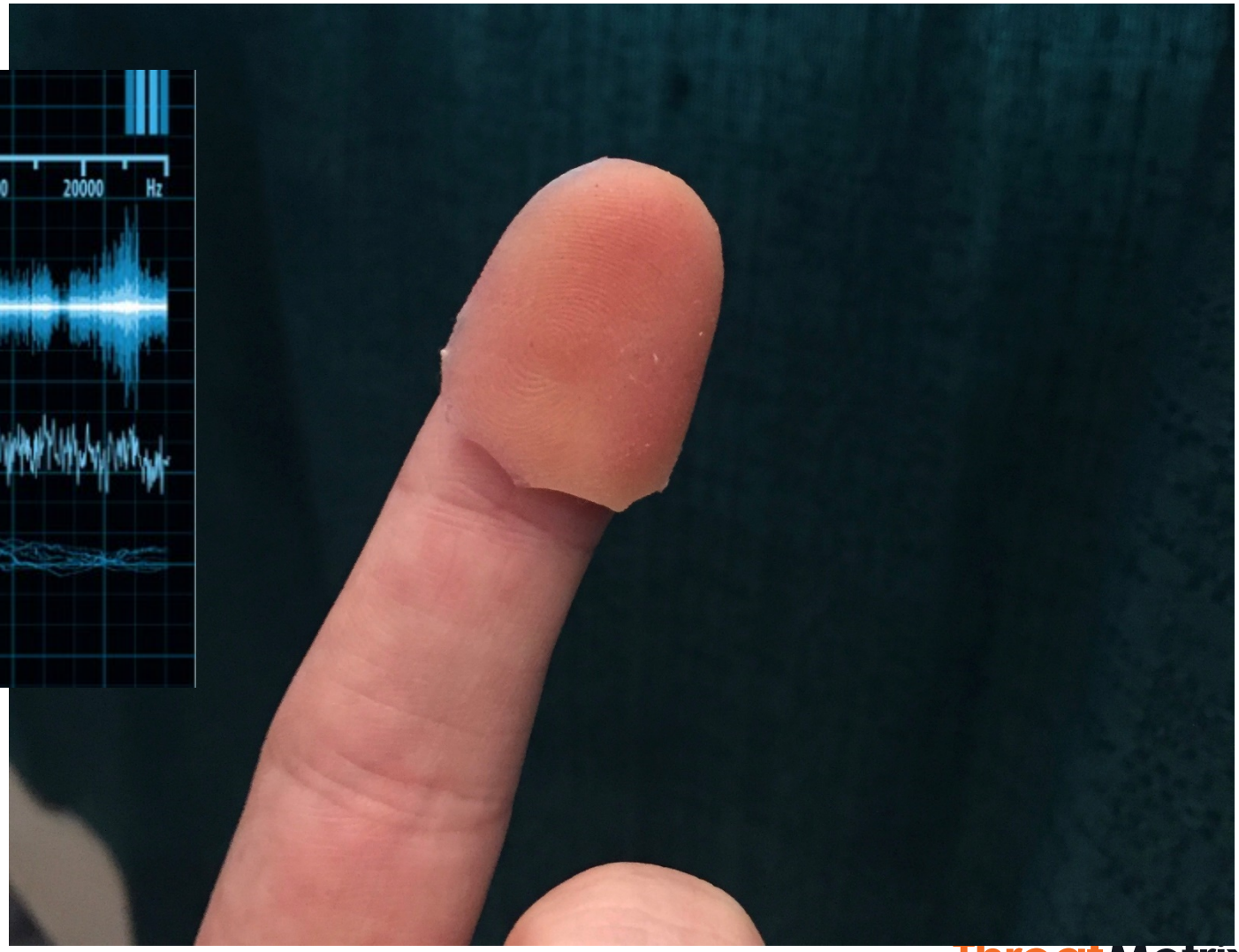
К чему мы пришли?

- Пользователям – все сложнее. Они пугаются и убегают.
- Мошенникам – все равно. Они не пугаются. Они воруют.

- Давайте еще улучшим аутентификацию! Добавим третий фактор!

Биометрия на помощь!





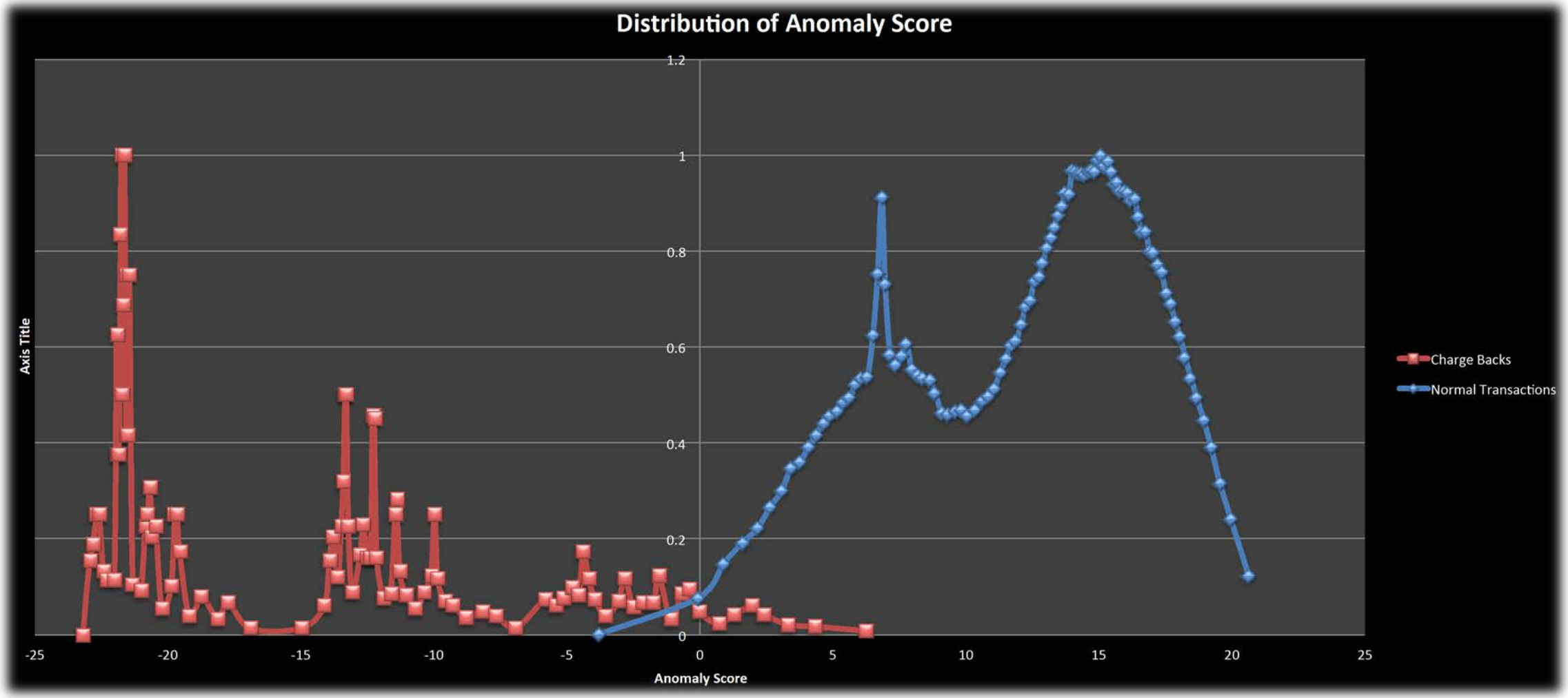
Но есть проблемы...

- Дорого
- Неудобно
- Не всегда доступно
- Не очень точно
- А попробуйте поменять скомпрометированный палец. Или глаз.

Нужно что-то новое

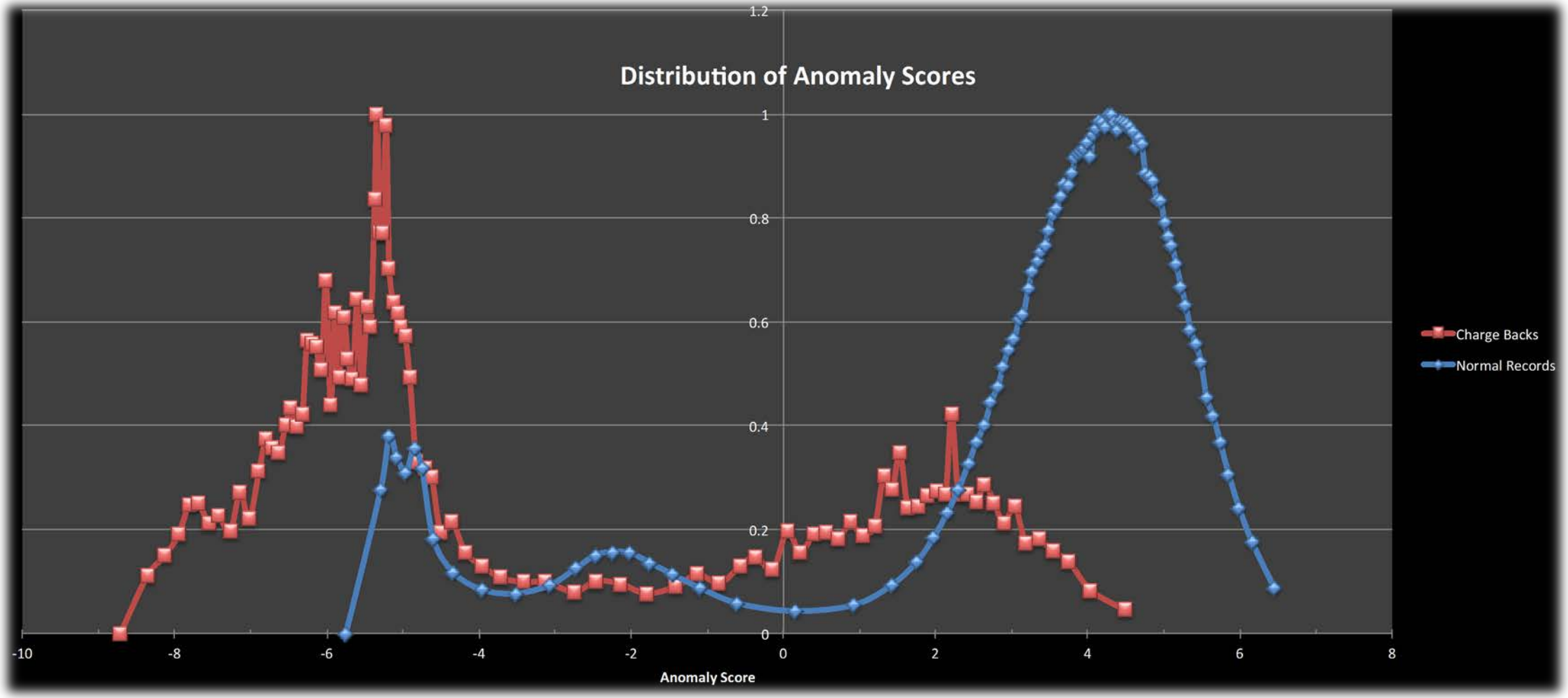
- Не только аутентификация:
  - Поведенческий анализ?
  - Машинное обучение?
  - Пользователи – направо, мошенники – налево!

Так должно быть



ThreatMetrix®

Но чаще получается так



ThreatMetrix®

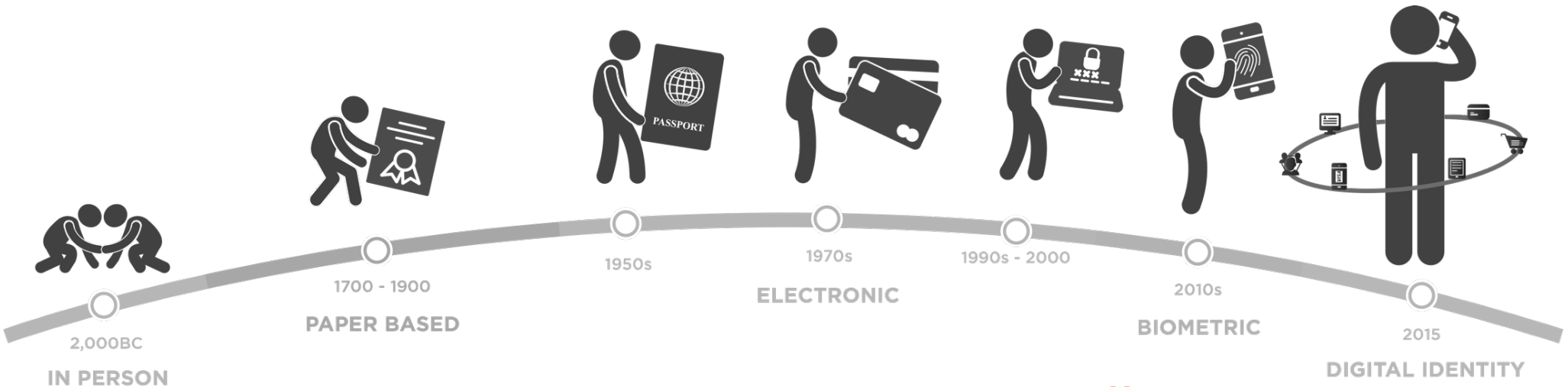
Машинное обучение – не панацея

- Мир становится все мобильней и разнообразней
- Пользователи – не (только) статистика, они не хотят в прокрустово ложе
- Аномалии становятся нормой

Посмотрим шире

ThreatMetrix®

Эволюция аутентификации



Традиционная модель

Активное участие пользователя

- Что знает
- Чем владеет
- Что говорит

Новая модель

Пассивная аутентификация

- Кто он
- Где он
- Что он делает

ThreatMetrix®

Как же эволюционировать?

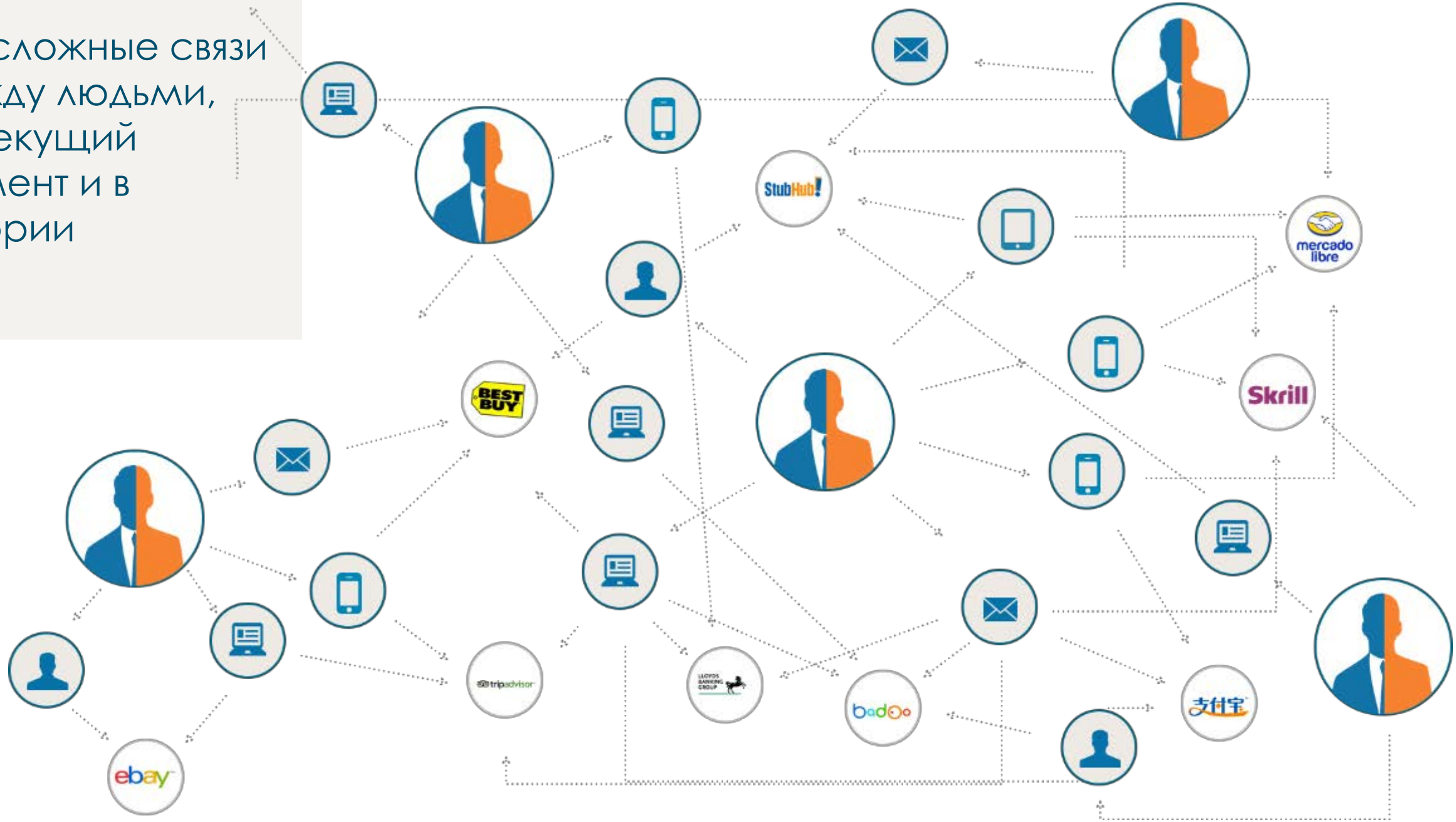
- Нужны хорошие данные – в идеале вся картина
- Из них нужно извлечь знания
- Подробно, о каждом пользователе
- Заплатить американской картой в российском магазине, находясь в Африке – вполне реальный кейс.

Глобальный профиль

Глобальный профиль – устройства, идентификаторы, реквизиты доступа, средства платежей, география, привычки...

ThreatMetrix®

…и сложные связи между людьми, на текущий момент и в истории



ThreatMetrix®

Большие данные – умные правила

Классические правила

Переместился больше, чем на 1000 км в день – стой!

Умные правила

Переместился больше, чем обычно – подтверди, что это ты.

Большие данные – умные правила

Классические правила

Заплатил в день больше, чем 100 000 рублей – подтверди, что все в порядке

Умные правила

Заплатил в два раза больше, чем за всю прошлую неделю – подтверди, что все в порядке.

Большие данные – умные правила

Классические правила

Больше 4 устройств в неделю – украли пароль!

2.5% логинов, 2% украденных аккаунтов

Умные правила

Больше устройств, чем на прошлой неделе плюс два – украли пароль!

0.2% логинов, 12% украденных аккаунтов

Что в результате

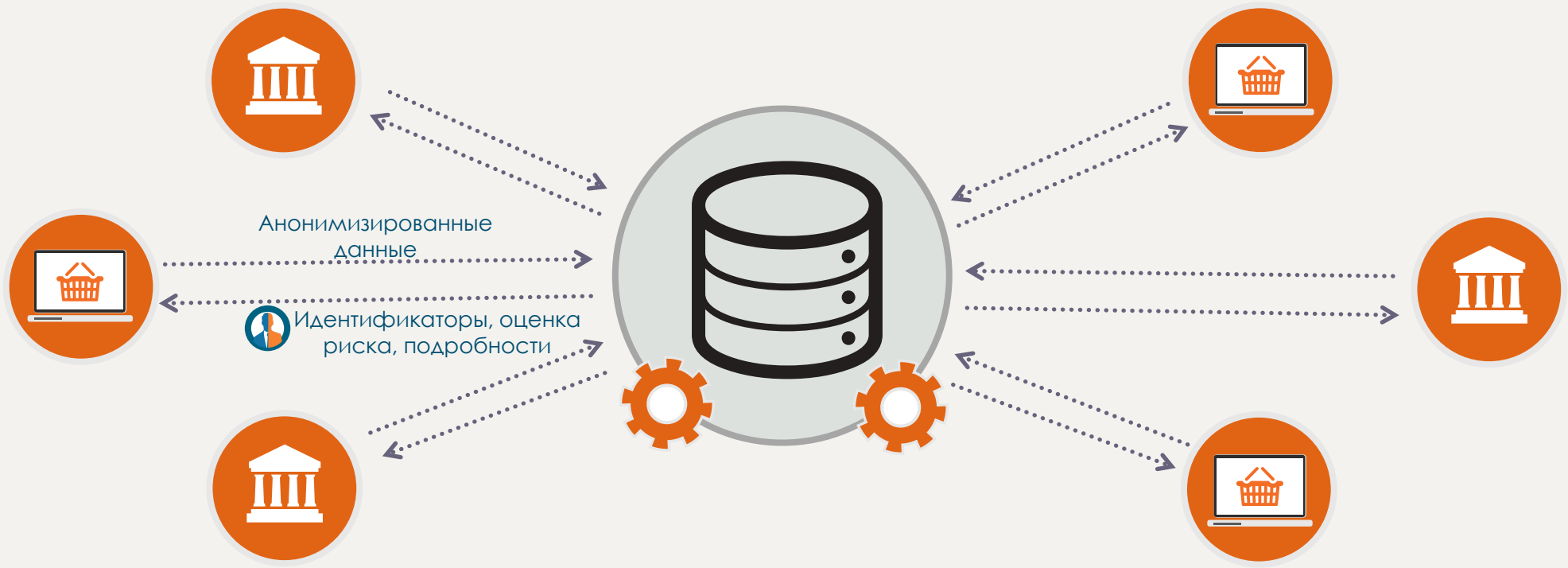
- Мы не заставляем пользователя доказывать, что он не верблюд
- Повышается конверсия и лояльность
- Снижаются затраты на ручной разбор, колл-центр и тд
- **Снижается фрод**

Как это работает

- Код на странице – анализирует устройство, ищет аномалии
- API-запрос – возвращает данные в реальном времени

Проверка каждой операции порождает данные

Краудсорсинг цифровых профилей



ThreatMetrix®

ThreatMetrix

На 70% меньше ложных срабатываний
На 90% меньше мошенничества

ThreatMetrix®
The Digital Identity Company™

Спасибо!

ThreatMetrix.com | sales@threatmetrix.com | partners@threatmetrix.com

1.408.200.5700 (Americas) | +61 2 9411 4499 (Asia Pacific) | +31 (0)20 800 0638 (EMEA)

ThreatMetrix®

https://digitalidentitysummit.com/
Лондон 12-13 июня

akovalev@threatmetrix.com
www.threatmetrix.com