

Биометрическая идентификация в мобильных устройствах



Intro



Android developer,
Lamantine Software a.s.

Co-founder,
Google Developers Group Kremenchuk



Достоинства и недостатки

- «Классический» подход получил широкое распространение из-за простоты реализации и использования. Интуитивно понятное использование — ввел пароль или активировал устройство и ты авторизован.

Пароли, PIN-коды, графические пароли поддаются подбору (брутфорс, социальная инженерия, кейлогеры и т. п.), возможна утеря/кража физического носителя с данными авторизации (да, есть пользователи записывающие пароли в записную книжку или на стикеры)

RFID/Bluetooth/USB — возможна кража или создание дубликата устройства.

Пароли и PIN-коды распространены повсеместно — ПК, веб, мобильные устройства. Аутентификация по RFID/NFC/USB получила большее распространение в стационарных системах авторизации и на ПК.

- Биометрический подход: более надежный способ аутентификации пользователя. Уникальные для каждого человека токены авторизации. Сложнее поддается обходу.

К сожалению, подвержены взлому с использованием дубликатов или имитаторов. Могут изменяться под действием внешней среды (болезнь, травмы и тому подобное), таким образом блокируя аутентификацию владельца.

Биометрическая аутентификация используется давно (дактилоскопические сканеры на ноутбуках или в банках), но до последнего времени не имела большого распространения. С началом бума биометрических датчиков в мобильных устройствах, технология начала более широко применяться (Samsung Fingerprint, Apple TouchID)

«Классическая» аутентификации

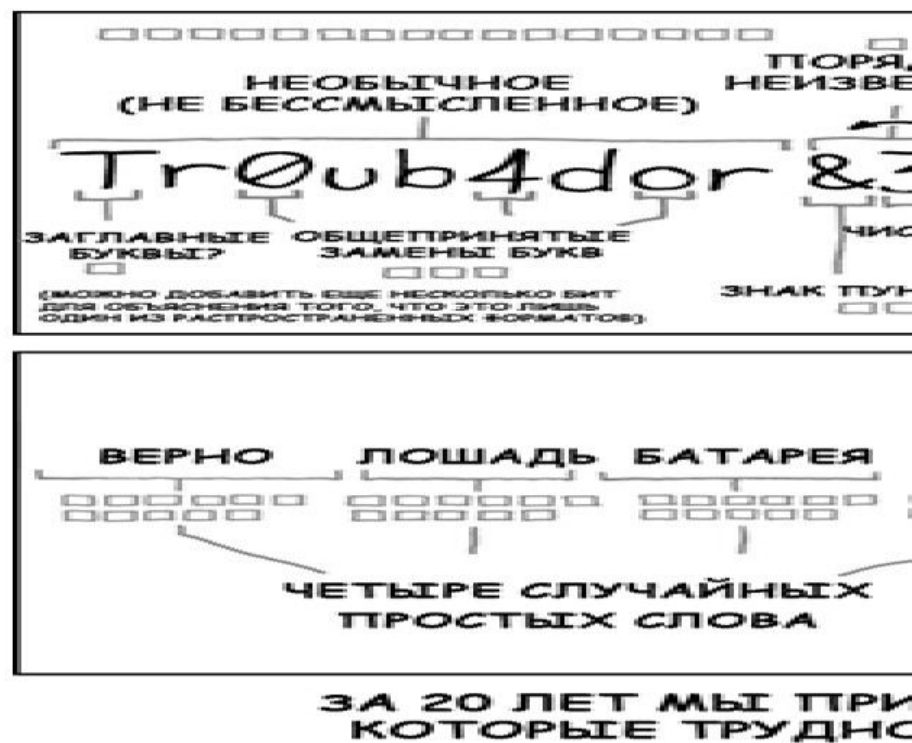
Пароли (мастер-пароли)

В настоящее время парольная аутентификация является наиболее распространенной, прежде всего, благодаря своему единственному достоинству – простоте использования.

Пользователи обычно не хотят создавать сложные и длинные пароли, чем значительно упрощают работу хакерам.

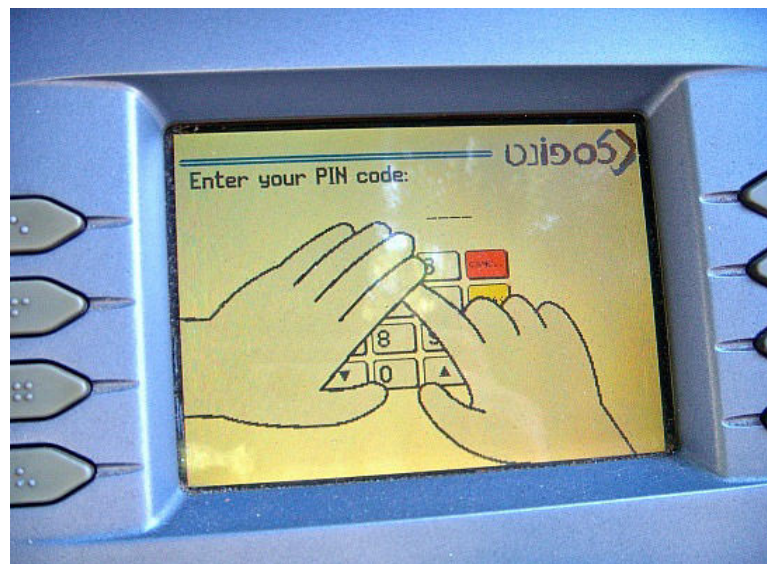
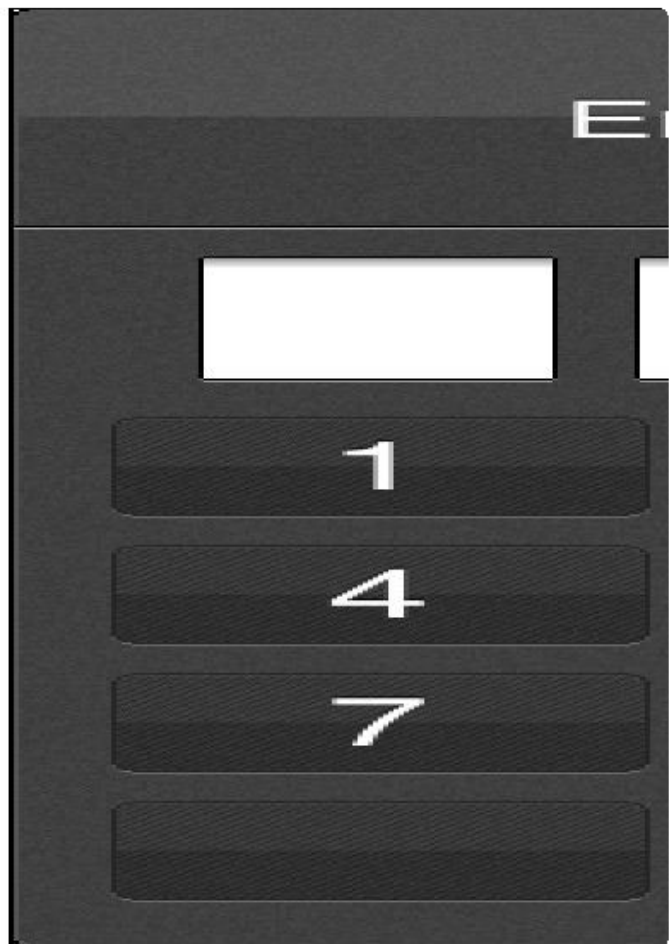
Для взлома пароля состоящего из одних только символов хакеру потребуется меньше часа, даже если пароль состоит из 8 символов. Больше времени потребуется ему на то, чтобы взломать пароль из больших и маленьких букв, цифр и знаков, но все же он это сделает.

- | | |
|--------------|---------------|
| 1. password | 14. sunshine |
| 2. 123456 | 15. master |
| 3. 12345678 | 16. 123123 |
| 4. abc123 | 17. welcome |
| 5. qwerty | 18. shadow |
| 6. monkey | 19. ashley |
| 7. letmein | 20. football |
| 8. dragon | 21. jesus |
| 9. 111111 | 22. michael |
| 10. baseball | 23. ninja |
| 11. iloveyou | 24. mustang |
| 12. trustno1 | 25. password1 |
| 13. 1234567 | |



PIN-коды

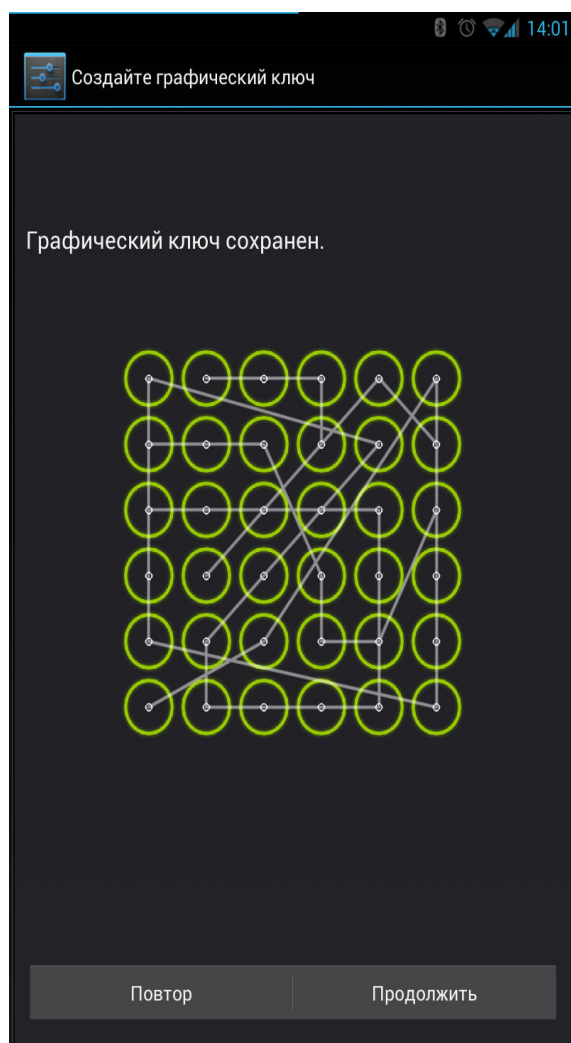
Один из самых простых видов идентификации. Обычная длина PIN-кода колеблется в пределах 4-5 символов, и обычно это цифры. К тому же большая часть пользователей использует комбинации вида 1111, 1234, 0000 или 1986. Данный тип является самым уязвимым и небезопасным способом идентифицировать пользователя.



Графические ключи

Один из самых простых, быстрых, но эффективных способов аутентификации. Регистрируем последовательность точек или местоположение контрольной точки, и затем повторяем их для авторизации.

При небольшом количестве точек может быть достаточно просто взломан. Но к примеру Blackberry усилили его использованием генерацией случайным образом цифровой сетки, таким образом добились уникальности пути от контрольной цифры до контрольной точки.



Бессознательная и социальная аутентификация

- Бессознательная аутентификация: в наборе графических объектов необходимо выбрать схожее с эталоном изображения (среди 10 изображений выбрать только логотип Android к примеру). Мало распространенная технология, поддается взлому через соц.инженеринг.
- Facebook применяет(-ял) социальную аутентификацию пользователей, используя фото друзей. Поддается взлому через соц.инженеринг, так же имеются правовые проблемы с используемым контентом (личные фото). Сейчас функция отключена.

Identify This Friend

0 of 5 Friends Identified



This appears to be:

☐ Mike Steding

☒ Dan Muriello

☐ Ross Johnson

☐ Adam Ringel

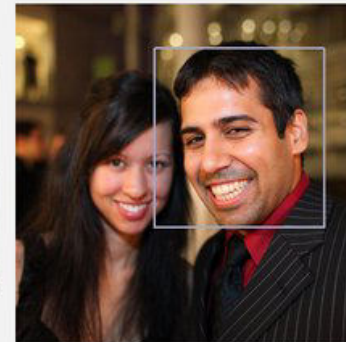
☐ Matt Jones

☐ Ivan Lucuk

Refresh Photos

Submit

Photo 2 of 5



This appears to be:

☐ Naitik Shah

☐ Tim Kuper

☐ Alok Menghrajani

☐ Nick Wilkerson

☐ David Starling

☐ Alessio Riso

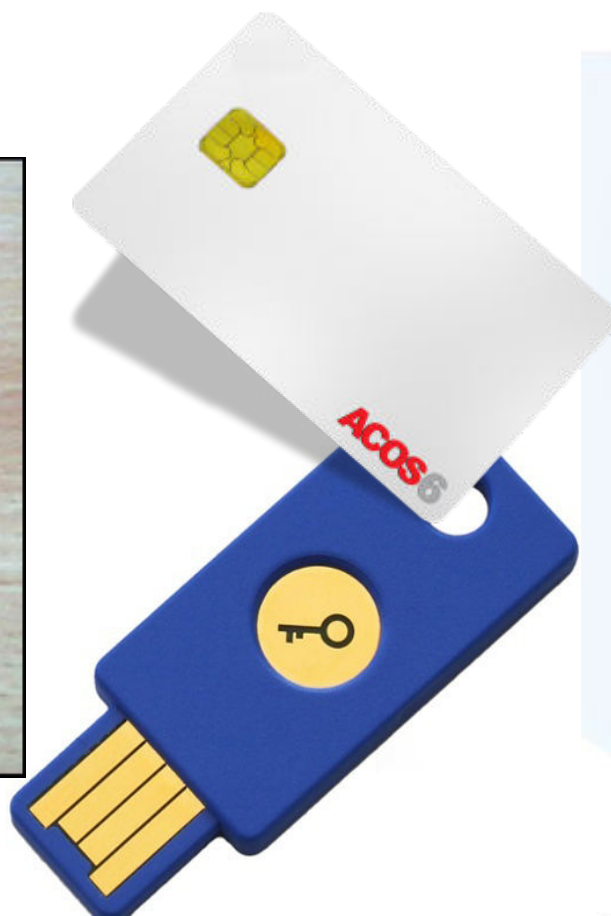
Submit

Skip (2 skips left)

RFID/Bluetooth/USB/NFC

Распространенный способ авторизовать владельца, особо популярен в корпоративном сегменте (RFID). Прост и удобен в использовании.

Опасность в возможности клонировать или эмулировать устройство. Подвержен утере или краже.

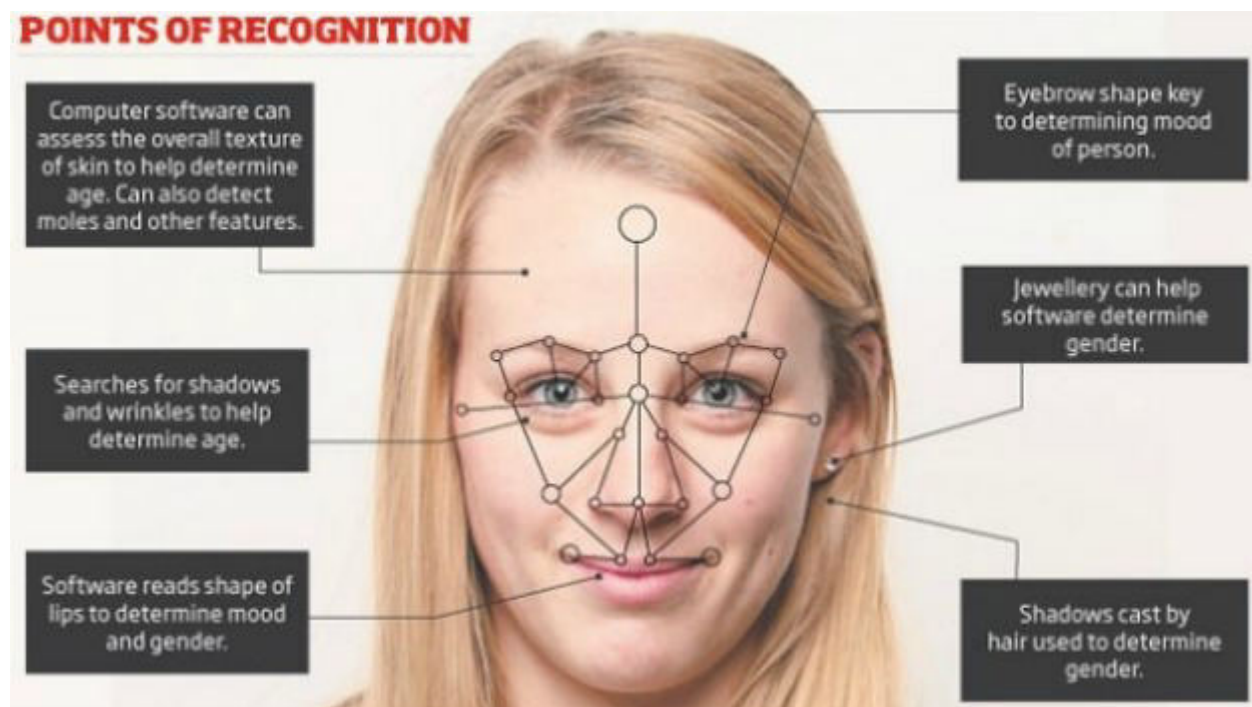


Biometric

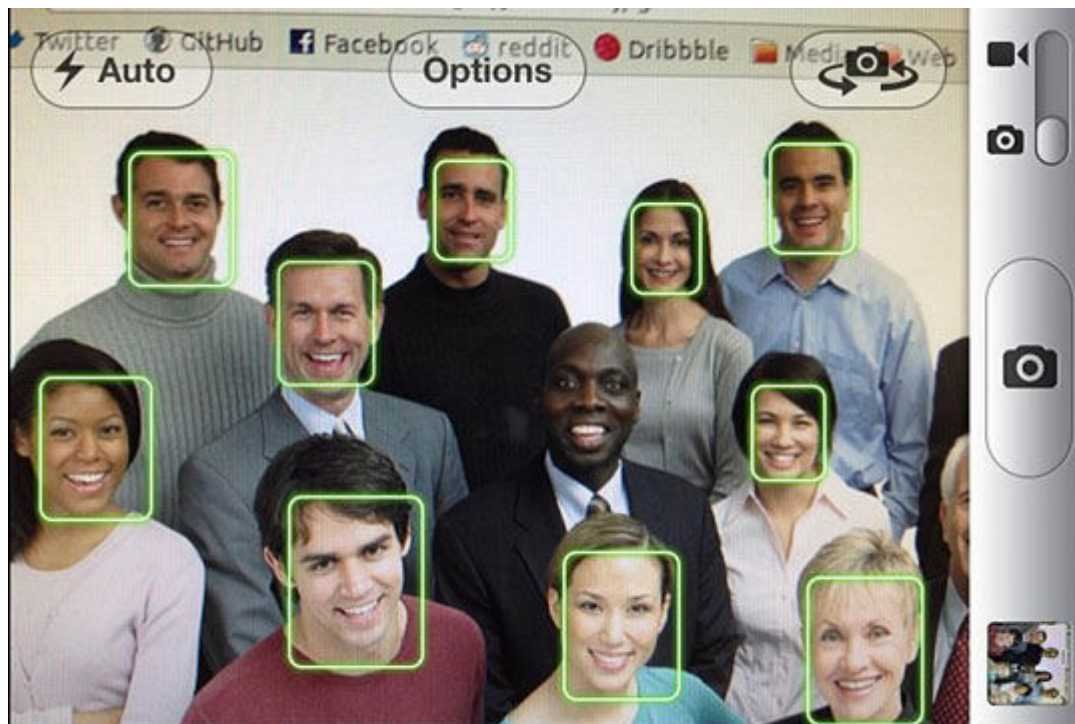
Распознавание по чертам лица

Старая теплая ламповая технология распознавания черт лица на спутниковых снимках из шпионских фильмов.

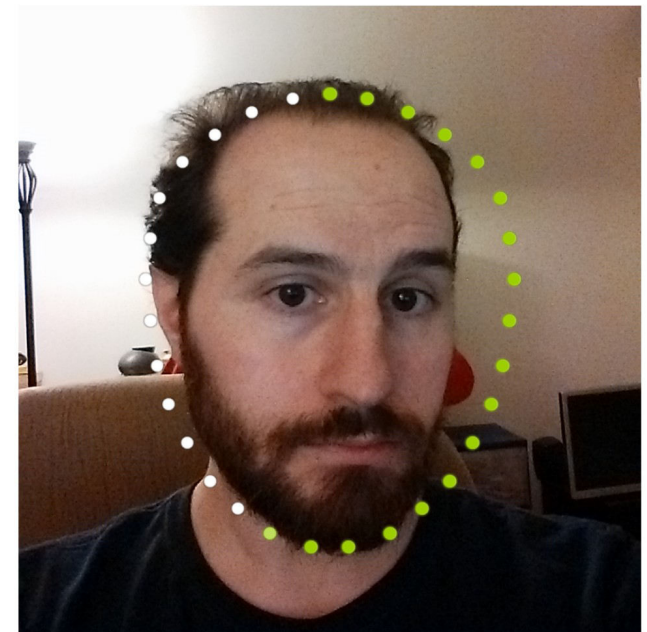
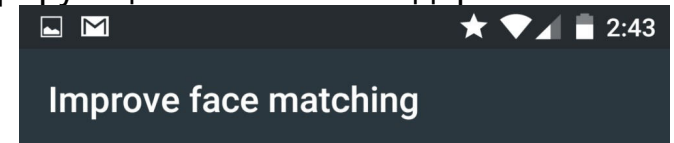
Используя овал лица для фокусировки, находит контрольные точки — глаза, нос, уши, губы, лоб и по уникальным маркерам авторизует владельца.



- Несовершенные алгоритмы компьютерного зрения (CV), из этого вытекает...
- Главным недостатком является очень грубая точность. Подсунь фото (или брата-близнеца) — и ты авторизован.
- В свое время в Android была реализована проприетарная функция FaceLock, но она не получила широкой популярности среди пользователей. В Android 5.0 Lollipop функция значительно доработана.



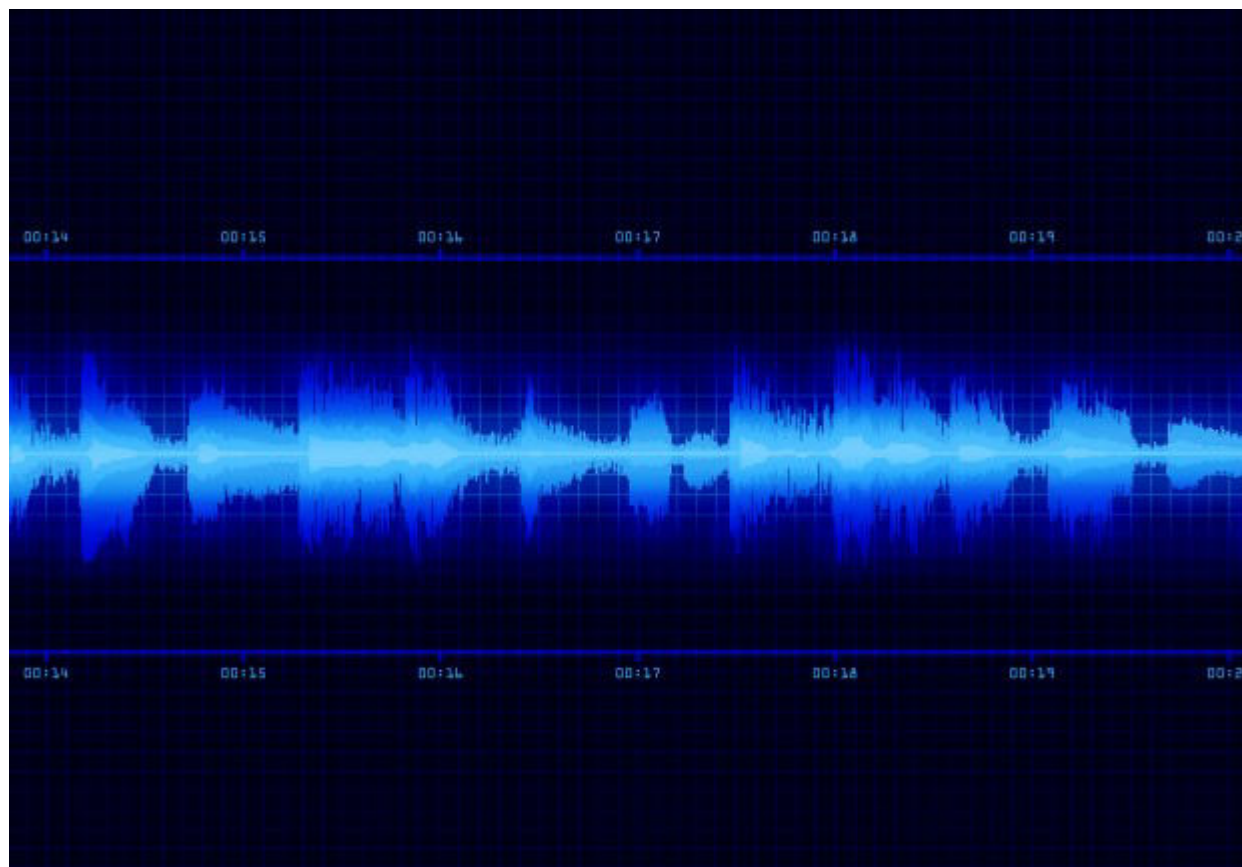
more awesome pictures at THEMETAPICTURE.COM



Распознавание голоса

Выделяет из аудиопотока речь, генерирует маску голоса конкретного человека. Имеет неплохую чувствительность, но из-за этого страдает при постороннем шуме. При простуде горла вы уже не сможете пройти проверку. Но ваша диктофонная запись — да. Если записать секретную фразу ;)

Применяется в встроенных системах, ПК, значительно реже в мобильных устройствах



Дактилоскопическая авторизация

Одна из самых старых технологий, имеющих беспрецедентную точность (про уникальность отпечатков пальцев помним?) Используется пожалуй чаще остальных реализаций. В встроенных системах (банки и прочие хранилища), в ноутбуках, мобильных устройствах (помнит кто раскладушку Pantech с дактилоскопическим датчиком?) Получила второе дыхание после начала применения в смартфонах и планшетах Apple, Samsung и с недавних пор Meizu (MX5). По слухам LG и Huawei так же планируют использование сканеров.



Как и другие технологии, не лишена недостатков. Взлом Apple TouchID не обсуждал только ленивый. К сожалению Яблоки не одиноки, Samsung Fingerprint ушел не намного дальше.

Каждый человек в повседневной жизни оставляет массу своих отпечатков, которые при определенной подготовке достаточно просто восстановить.

Ну проще получить физический доступ к пальцу, во время сна, алкогольного опьянения или с помощью пилы ;)

Так же не стоит забывать что в случае повреждения эпителия (порез или ожог пальца) провести идентификацию будет невозможно.



Сканер радужки глаза

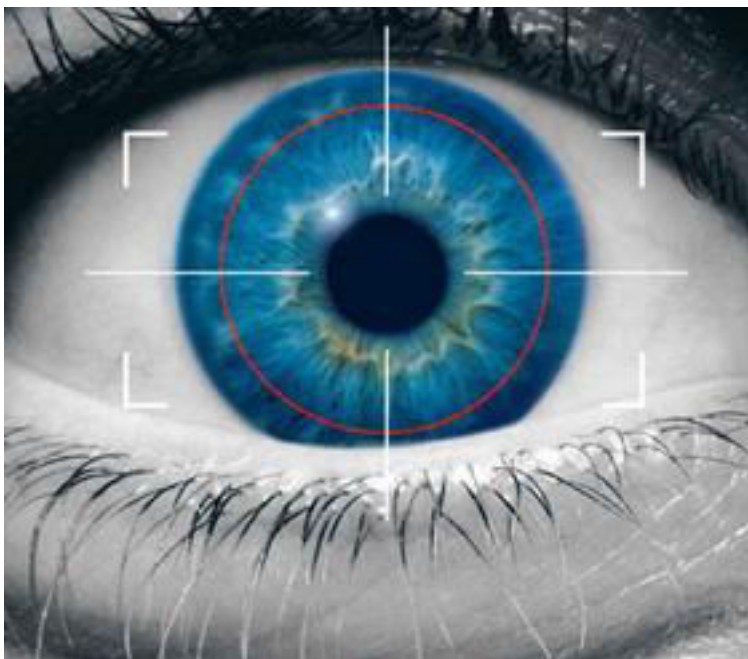
Без вариантов, самый джеймсбондовский и крутейший способ идентифицировать пользователя.

Рисунок радужки глаза не менее уникален чем отпечаток пальца. Технология имеет очень высокую точность и с большим трудом поддается взлому или обходу.

Из личного опыта работы с подобным устройством, ни фото, ни даже зеркало не позволяет пройти верификацию пользователя. Только живой глаз.

Используется в встроенных системах, ПК.

Не работает или работает плохо через очки, линзы, а так же с людьми азиатской внешности :)



Была информация что LG в следующем смартфоне-флагмане добавит такую возможность.
Неожиданно для всех компания ViewSonic представила смартфон V55



Сердечный ритм

Достаточно необычный вариант идентификации, но тем не менее ведутся активные разработки в его совершенствовании. Сердцебиение достаточно уникально чтобы идентифицировать по нему человека.

С ростом количества различных фитнес-трекеров данный способ не кажется таким уж фантастическим.

Как мне кажется, имея достаточно высокую погрешность будет иметь низкую надежность.

Известно что некоторые компании (браслет-кардиомонитор Numi) ведут разработку браслетов, совместимых с мобильными и ПК.



Почерк и скорость набора текста

Как известно, графология достаточно точная наука, ее очень часто используют правоохранительные органы для идентификации человека написавшего некий текст. Поэтому идентифицировать пользователя по написанному на экране тексту достаточно тривиальная задача.

То же относится к таймингу набора текста. Каждый человек набирает определенный текст обычно с определенным ритмом, по которому можно идентифицировать его.

Эти варианты достаточно просты, но малоудобные для повседневного использования и имеют низкую точность, благодаря чему достаточно легко подделав почерк получить доступ к данным.



Biometric v2.0

Активность и поведение

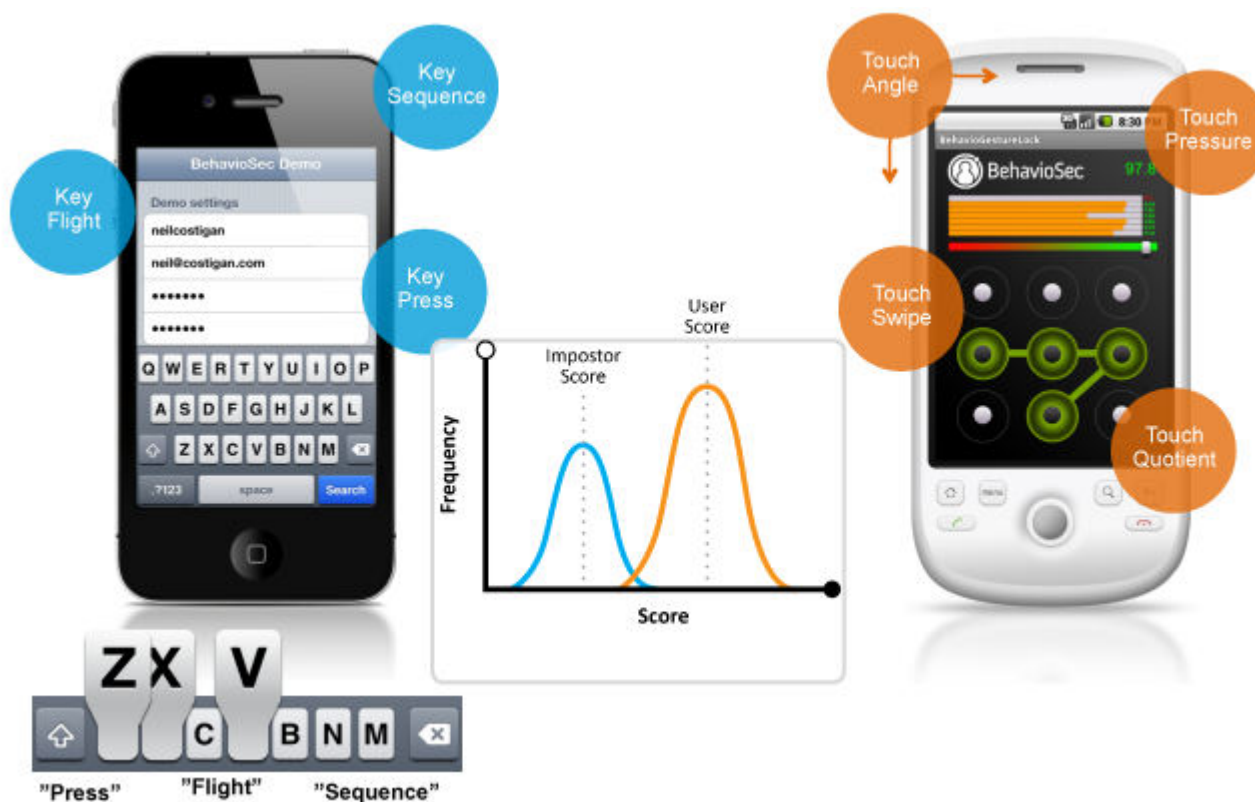
Носимые устройства — смартфоны, смарт-часы, фитнес-трекеры, - постоянно рядом. Они собирают информацию о Вас
Ваша активность, где бываете, чем коротаете время

What is a Wearable Device?

Health & Fitness Monitors	Wearable Camera	Smart Watch Devices	Wearable Computer	
FitBit 	Looxie 	Pebble 	Sony 	Google Glass 
Sensoria 	Zeal 	Motorola 	Qualcomm 	Motorola Industrial solutions 
Wearable pancreas (Medtronic) 	Go Pro 			

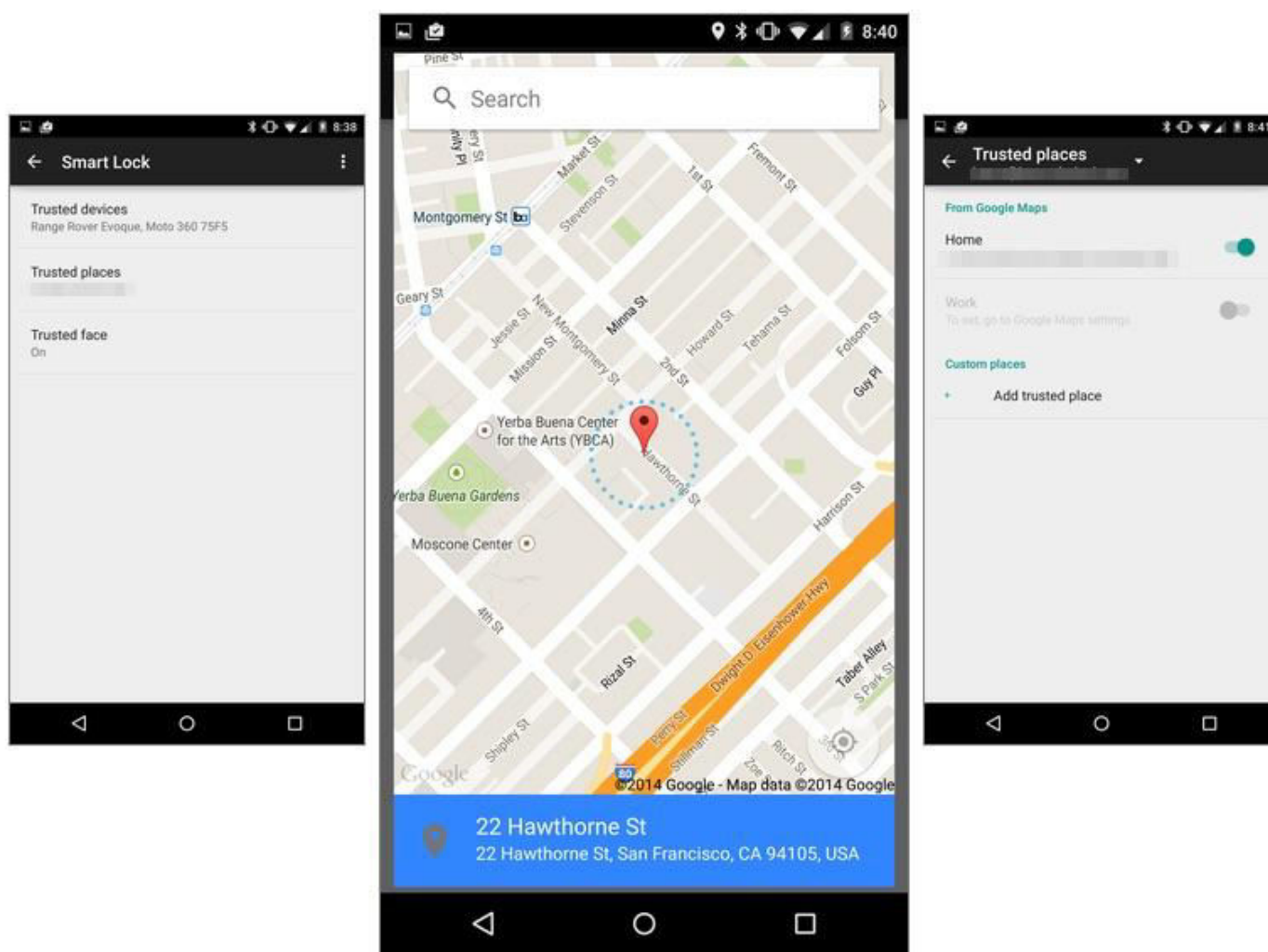
BehavioSec/BehavioMobile

- Ваша манера набора текста или рисования, манера управления устройством



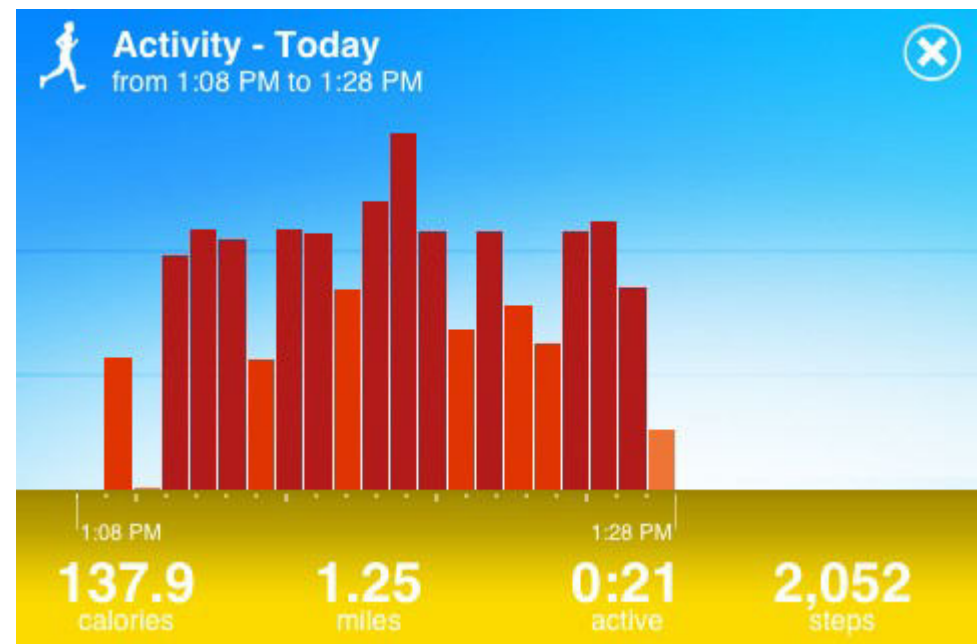
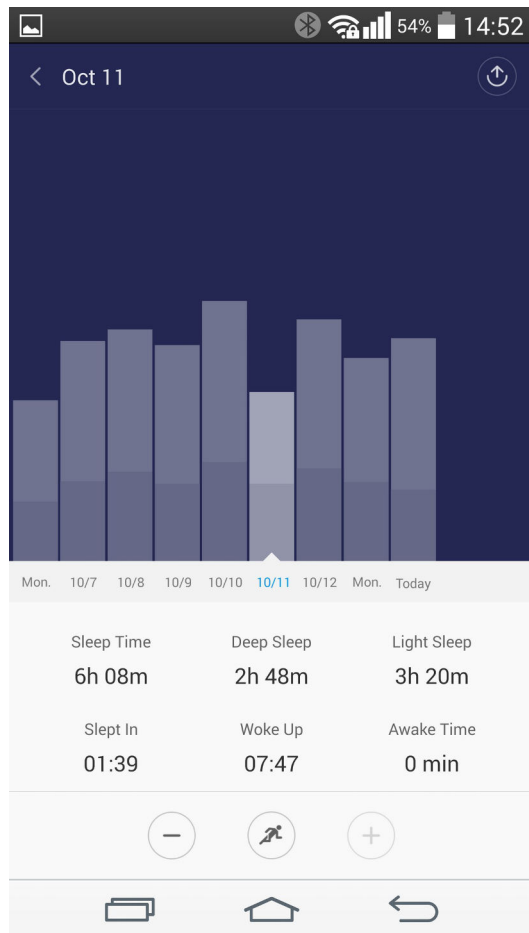
Geo-behavior /Trusted places

- Дом, работа — где, когда и сколько времени



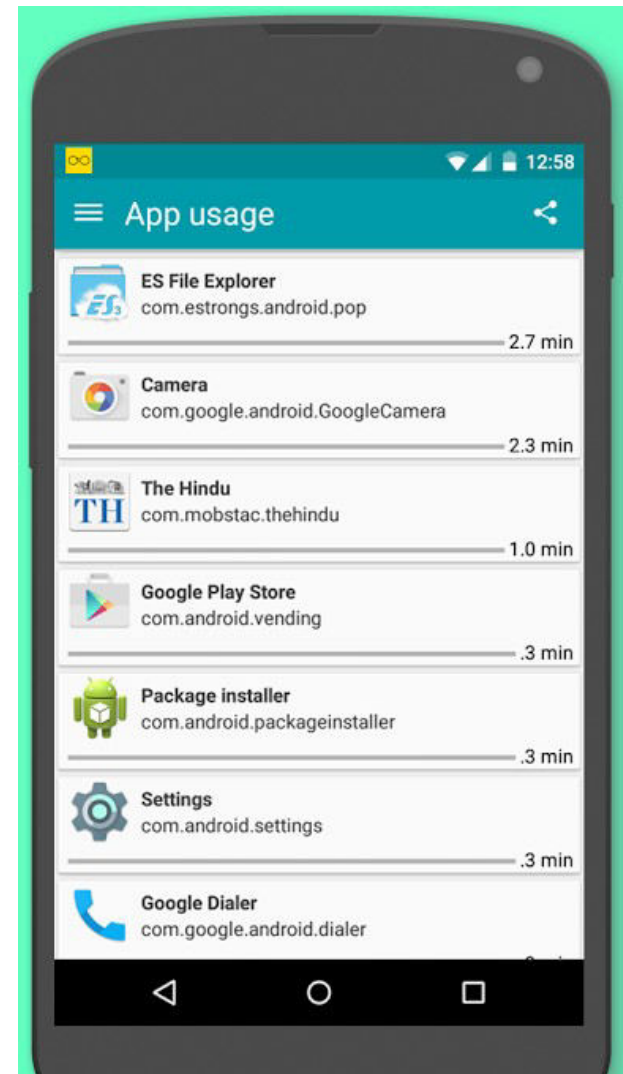
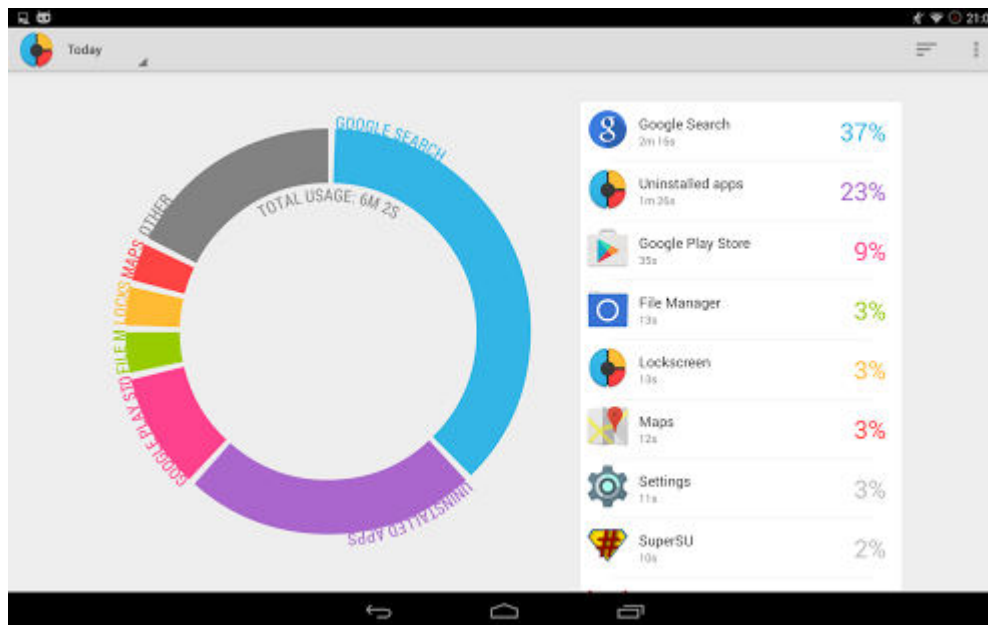
ActivityTracking

- Физическая активность



Habits

- Ваши привычки и предпочтения



Знает где, когда и как долго вы бываете

+

Знает сколько и когда вы активны

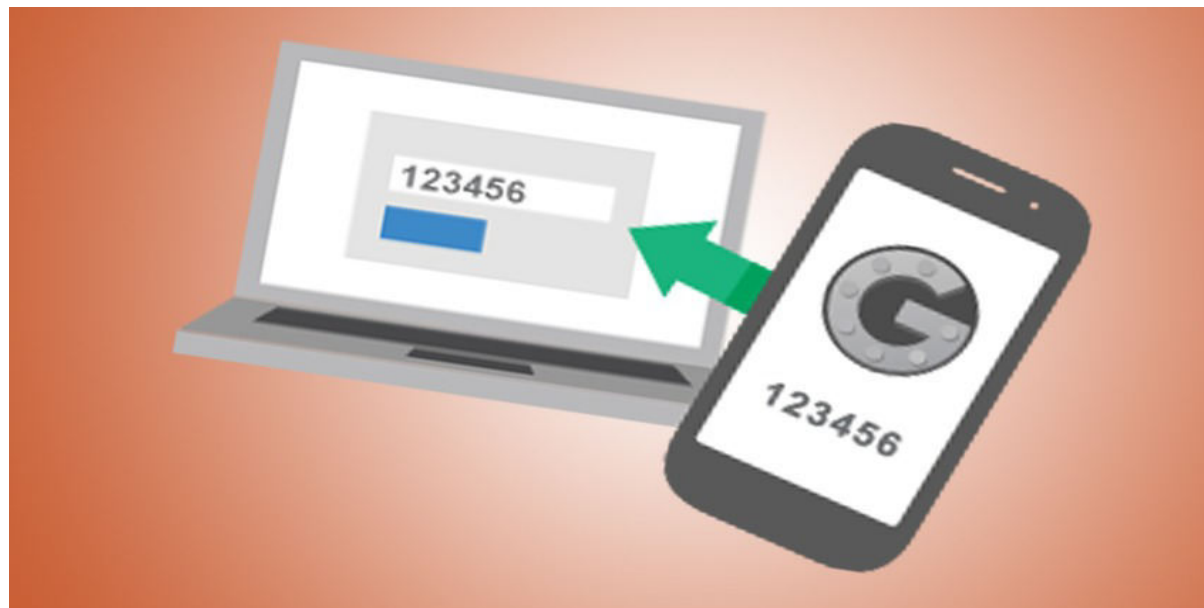
+

Знает чем и когда вы коротаете время

=

Может сделать вывод Вы сейчас пользуетесь
устройством или нет

- «Серебрянной пули» не существует. Идентификация пользователя может быть:
 - ИЛИ надежной, но продолжительной и неудобной
 - ИЛИ простой и быстрой, но ненадежной
- Лучше всего использовать комбинацию вариантов: двухфакторная авторизация, отпечаток пальца и пароль (к примеру)
- В зависимости от нужд, можно использовать параллельно (ввод или пароля или отпечатка) либо последовательно (ввод пароля и подтверждение отпечатком)
- При использовании биометрической авторизации предпочтительней использовать offline решения, дабы не передавать личные данные третьим лицам (в случае с REST API)
- Biometric v2.0 можно использовать к примеру для определения необходимости принудительного усиления защиты





Sticky Password

securing your personal data

Сергей Комлач

sergey.komlach@stickypassword.com

Skype: s.komlach

