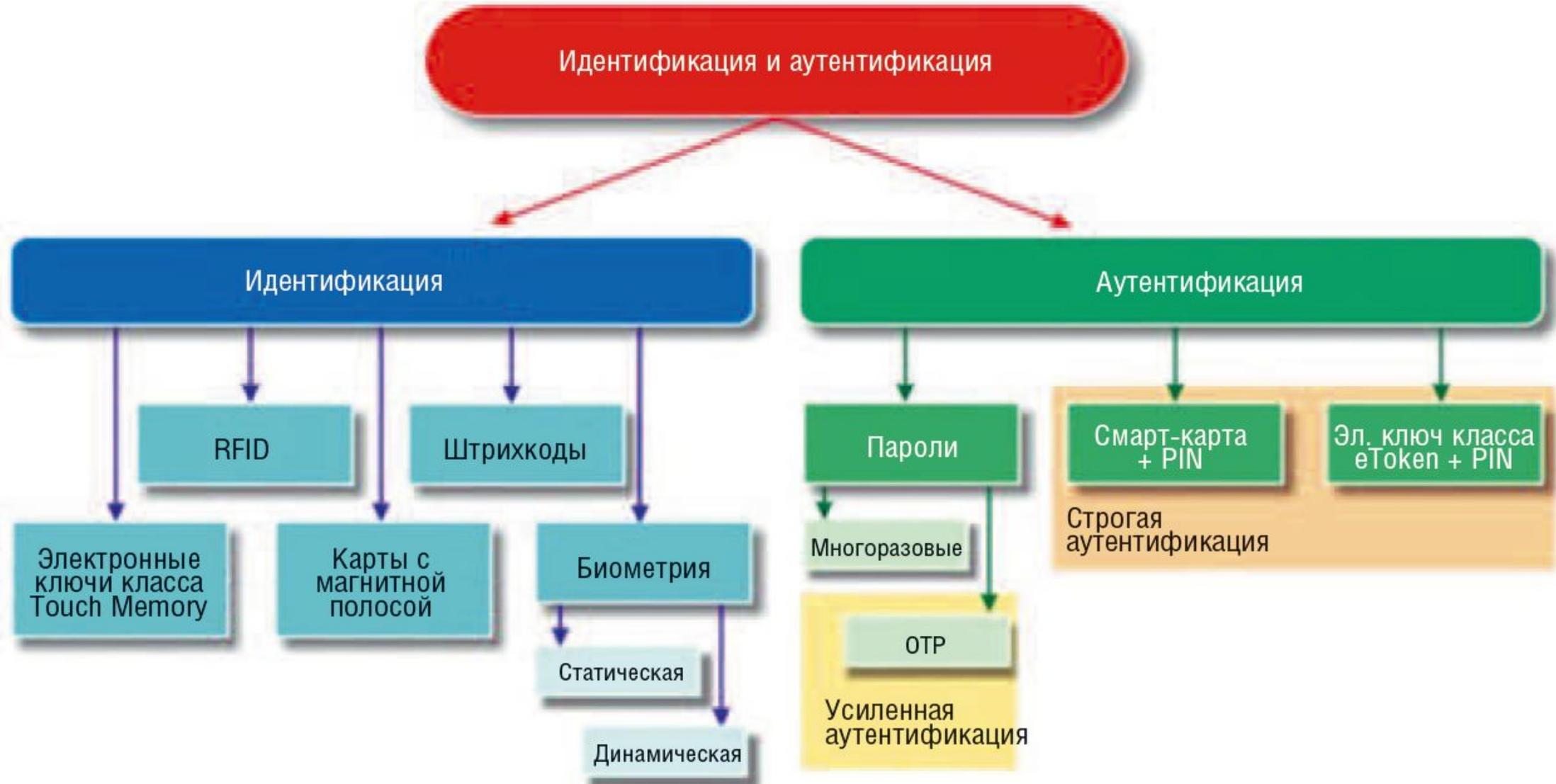


Методы идентификации и аутентификации на мобильных устройствах

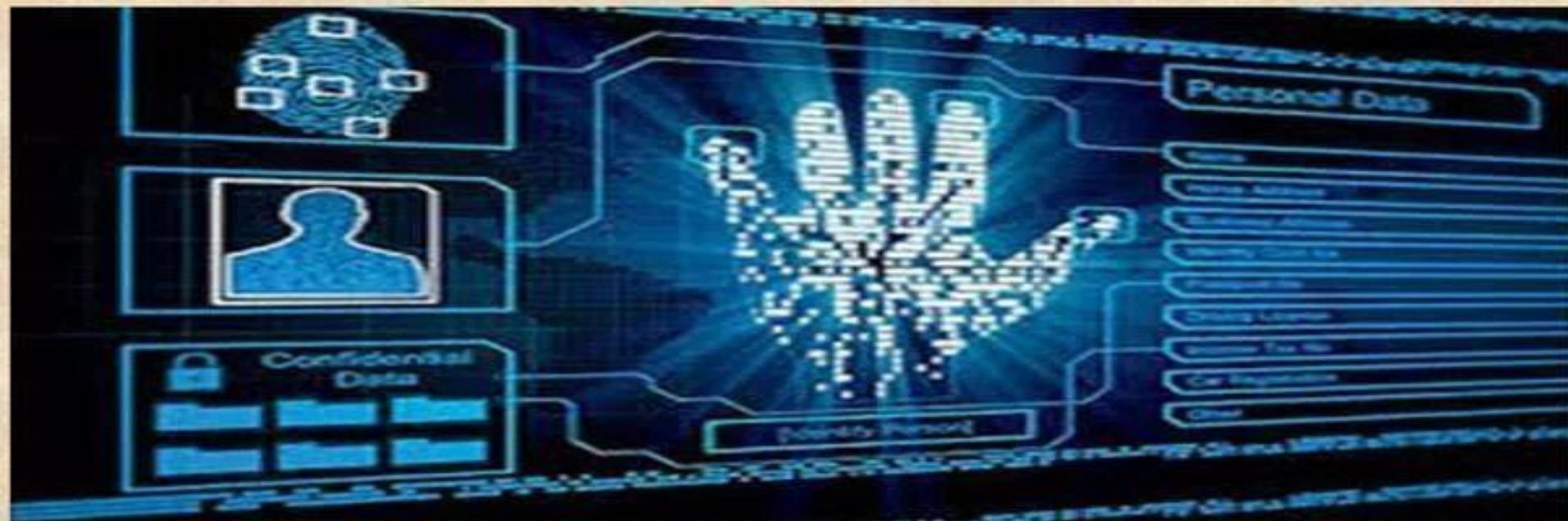
Выполнил: студент БКС 1901
Ахмедов Вадим

Введение



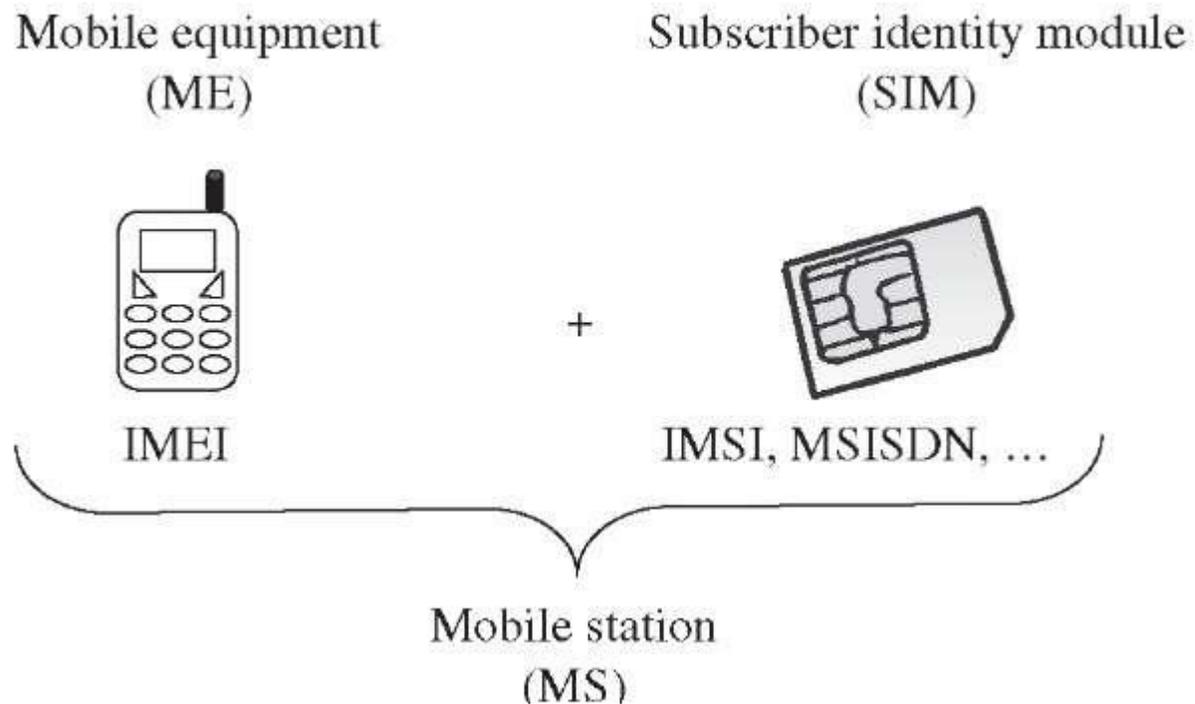
Идентификация

Indentifico [лат] – отождествляю



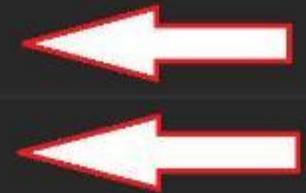
Идентифицировать объект – означает установить его тождество в разные периоды времени в разных состояниях путем проведения сравнительного исследования этого объекта с его отображениями (в виде следов) или его фрагментами.

Устаревшие аппаратные идентификаторы



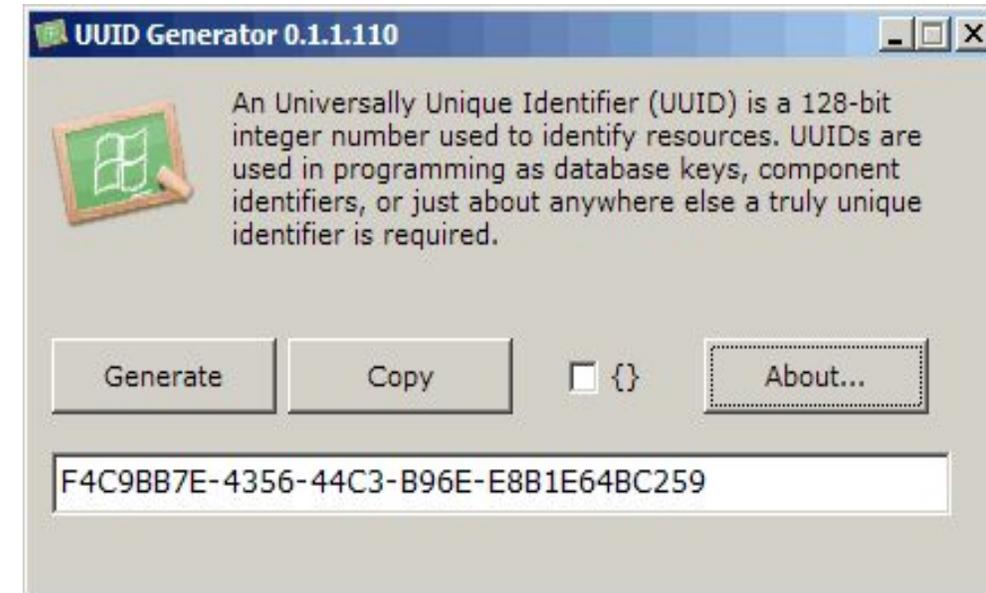
Общая информация

Состояние батареи	Не заряжается
Уровень заряда батареи	79%
IP-адрес	192.168.1.8 fe80::ad4:2bff:fe17:ac46
MAC-адрес Wi-Fi	08:d4:2b:17:ac:46
Адрес Bluetooth	08:D4:2B:17:AC:45
Серийный номер	R32D102DW6X
Время с момента включения	15:47:15



Генерация UUID с первым запуском

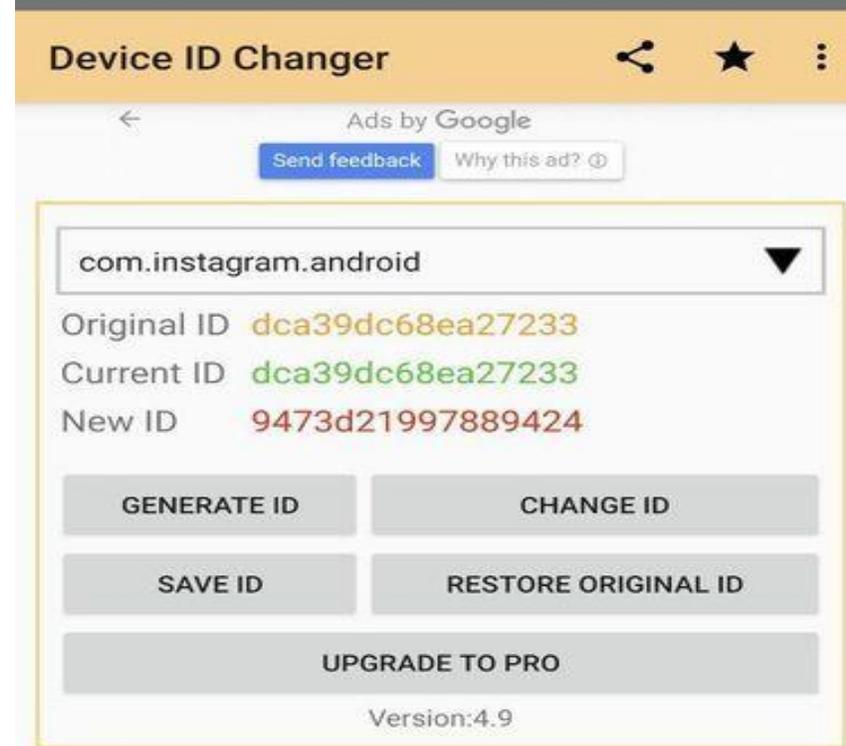
Данный способ схож с использованием cookie: создаем файл со сгенерированной строкой, сохраняем его в песочнице нашего приложения, и используем как идентификатор. Недостаток тот же, что и у cookie — вся песочница удаляется вместе с приложением. Еще она может быть очищена пользователем явно из настроек. При наличии у приложения доступа к хранилищу вне песочницы можно сохранить идентификатор где-то на устройстве и постараться поискать его после переустановки. Будет ли в тот момент нужное разрешение у приложения — неизвестно. Этот идентификатор можно использовать как идентификатор установки приложения (app instance ID).



Использование идентификаторов, предоставляемых системой

В документации для разработчиков представлен идентификатор `ANDROID_ID`. Он уникален для каждой комбинации устройства, пользователя, и ключа, которым подписано приложение. До Android 8.0 идентификатор был общим для всех приложений, после — уникален только в рамках ключа подписи. Этот вариант в целом годится для идентификации пользователей в своих приложениях (которые подписаны вашим сертификатом).

Существует и менее известный способ получить идентификатор общий для всех приложений, независимо от сертификата подписи. При первичной настройке устройства (или после сброса к заводским) сервисы Google генерируют идентификатор. Но это не самое плохое. Самый большой недостаток в том, что такие фреймворки, как Xposed, позволяют с помощью расширений в пару кликов подменить как `ANDROID_ID`, так и `GSF_ID`. Приложение Device ID Changer в связке с Xposed позволяет подменять практически любой идентификатор. В бесплатной версии — только `ANDROID_ID`



Создание цифрового отпечатка (fingerprint) устройства

- Идея device-fingerprinting не новая, и активно используется в самой популярной библиотеке для создания отпечатка — FingerprintJS — 13 тысяч звезд на GitHub. Она позволяет идентифицировать пользователя без использования cookie.

Рассмотрим идею на примере.

- Возьмем ежедневную аудиторию какого-нибудь Android-приложения. Допустим она составляет 4 миллиона. Сколько среди них устройств марки Samsung? Гораздо меньше, примерно 600 тысяч. А сколько среди устройств Samsung таких, что находятся под управлением Android 9? Уже около 150 тысяч. Выделим среди последних такие, что используют сканер отпечатков пальцев? Это множество устройств еще меньше, ведь у многих планшетов нет сканера отпечатков пальцев, а современные модели опираются на распознавание лица. Получим 25000 устройств. Добавляя больше условий и получая больше информации, можно добиться множеств малых размеров. В идеальном случае — с единственным элементом внутри, что и позволит идентифицировать пользователя.

Аутентификация - это процедура, проверяющая, имеет ли пользователь с предъявленным идентификатором право на доступ к ресурсу.



Реализация аутентификации

Субъект может подтвердить свою подлинность, предъявив, по крайней мере, одну из следующих сущностей:

- 1. Что-то, что он знает -- пароль. Это секретная информация, которой должен обладать только авторизованный субъект. Паролем может быть речевое слово, текстовое слово, комбинация для замка или персональный идентификационный номер (PIN).
- 2. Что-то, что он имеет -- устройство аутентификации. Здесь важен факт обладания субъектом каким-то уникальным предметом. Это может быть личная печать, ключ от замка, для компьютера это файл данных, содержащих характеристику. Характеристика часто встраивается в специальное устройство аутентификации, например, пластиковая карта, смарт-карта.
- 3. Что-то, что является частью его самого -- биометрика. Характеристикой является физическая особенность субъекта.

Пароли



Пароль

adme@почта.ru



Пароль

qwerty



Пароль

Sk0ro_budet_sUmmEr3529



Пароль

95nEn@dOpEchAlitsY@12



Токены



Биометрическая аутентификация

Биометрия - совокупность автоматизированных методов аутентификации людей на основе их физиологических и поведенческих характеристик.



Выводы

- Современные средства идентификации/аутентификации должны поддерживать концепцию единого входа в сеть. Единый вход в сеть - это, в первую очередь, требование удобства для пользователей. Если в корпоративной сети много информационных сервисов, допускающих независимое обращение, то многократная идентификация/аутентификация становится слишком обременительной. К сожалению, пока нельзя сказать, что единый вход в сеть стал нормой, доминирующие решения пока не сформировались.
- Любопытно отметить, что сервис идентификации / аутентификации может стать объектом атак на доступность. Если система сконфигурирована так, что после определенного числа неудачных попыток устройство ввода идентификационной информации (такое, например, как терминал) блокируется, то злоумышленник может остановить работу легального пользователя буквально несколькими нажатиями клавиш.
- Таким образом, необходимо искать компромисс между надежностью, доступностью по цене и удобством использования и администрирования средств идентификации и аутентификации.

Спасибо за внимание!