Цифровые сертификаты для владельцев мобильных телефонов.

Колосова А.И., Намиот Д.Е.

***Аннотация*—В работе рассматривается задача подтверждения факта владения мобильным телефоном. Предложена модель цифровых сертификатов для мобильных телефонов. В этой модели каждый мобильный пользователь может создать некоторую цифровую метку для своего телефона и подписать ее с помощью ссылки на свой профайл в социальной сети. Далее возможен поиск по базе цифровых сертификатов. Поиск может осуществляться как по идентификации мобильного телефона, так и по профайлам социальной сети (сетей).**

***Ключевые слова*—IMEI, Android, мобильные цифровые сертификаты.**

I. Введение

Проблема хищений мобильных телефонов остро стоит во всем мире. Как правило, у каждого владельца мобильного телефона записано некоторое количество важной информации на нем, которую тяжело восстановить. Как-то – список контактов, TODO лист и др., в зависимости от сложности устройства. Поэтому важной задачей является нахождение утерянных аппаратов.

В данной работе рассматриваются мобильные устройства с операционной системой Android – смартфоны и др. У всех подобных аппаратов имеются различные идентификационные номера. Которые могут быть использованы для нахождения утерянных телефонов, мониторинга установок некоего приложения, генерации технических средств защиты авторских прав (ТСЗАП, DRM – digital rights management). Например, мобильные операторы, при наличии определенного оборудования могут полностью или частично прекратить обслуживать украденный телефон, перенаправлять SMS-сообщения с него на другой телефон. Или отследить его место нахождения по GPS. В России подобная практика не так распространена, как в некоторых других странах, однако и у нас есть случаи нахождения украденных телефонов по IMEI номеру.

Статья получена 10 июня 2013. В статье изложены результаты дипломной работы, выполненной на факультете ВМК МГУ им. М.В. Ломоносова

Колосова Алена Игоревна – студентка третьего курса второго высшего образования факультета Вычислительной Математики и Кибернетики Московского государственного университета им. Ломоносова.

Намиот Дмитрий Евгеньевич – кандидат физико-математических наук, старший научный сотрудник лаборатории Открытых Информационных Технологий факультета Вычислительной Математики и Кибернетики Московского государственного университета им. Ломоносова.

Задачи этой работы:

-разработка методики определения идентификационных номеров мобильных аппаратов;

-разработка системы регистрации идентификационных номеров мобильных аппаратов и их владельцев в общей базе данных.

-разработка сайта с системой взаимодействия с получившейся базой данных.

II. Основные существующие методы идентификации мобильных телефонов

A. IMEI

IMEI (International Mobile Equipment Identity) - число (обычно 15-разрядное в десятичном представлении), уникальное для каждого использующего его аппарата. Применяется в сотовых телефонах сетей GSM, WCDMA и IDEN а также в некоторых спутниковых телефонах [7].

IMEI присваивается телефону во время изготовления на заводе. Он служит для идентификации устройства в сети и хранится в прошивке аппарата. Как правило, IMEI указывается в четырёх местах: в самом аппарате (в большинстве случаев его можно вывести на экран набором *#06# на клавиатуре), под аккумуляторной батареей, на упаковке и в гарантийном талоне. IMEI играет роль серийного номера аппарата и передаётся в эфир при авторизации в сети. Также IMEI используется для слежения за аппаратами и блокирования краденых телефонов на уровне оператора сотовой связи, что не позволяет в дальнейшем использовать такой аппарат в сети этого оператора, однако не мешает его использованию в других сетях.

В отличие от ESN и MEID, используемых в CDMA и прочих сетях, IMEI используется только для идентификации устройства и не имеет постоянного отношения к абоненту. Вместо него используется номер IMSI, хранящийся на SIM-карте, которую можно вставить в практически любой другой аппарат. Однако существуют специальные системы, позволяющие одному телефону использовать только одну определённую SIM-карту.

Модель и происхождение телефона описываются первыми 8 цифрами IMEI (так называемый TAC). Оставшаяся часть — серийный номер с контрольным числом в конце. Телефонам, поддерживающим одновременную работу с двумя SIM-картами, присваивается два номера IMEI [5].

Производители постоянно совершенствуют методы

защиты программного обеспечения аппарата от изменения IMEI. В современных аппаратах IMEI хранится в однократно программируемой зоне памяти и не может быть изменен программными средствами [4].

В некоторых странах, например в Латвии, Великобритании, Республике Беларусь изменение IMEI является уголовно наказуемым деянием. Имеется также прецедент попытки уголовного преследования за изменение IMEI в России [1][6].

B. MEID

MEID (Mobile Equipment IDentifier) – глобальный уникальный идентификатор подвижного оборудования, работающий в сетях CDMA, использует тот же базовый формат, что и IMEI [3][8].

C. IMSI

MSI (International Mobile Subscriber Identity) - международный идентификатор мобильного абонента (индивидуальный номер абонента), ассоциированный с каждым пользователем мобильной связи стандарта GSM, UMTS или CDMA. При регистрации в сети аппарат абонента передаёт IMSI, по которому происходит его идентификация. Во избежание перехвата, этот номер посылается через сеть настолько редко, насколько это возможно — в тех случаях, когда это возможно, вместо него посылается случайно сгенерированный TMSI [9].

В системе GSM идентификатор содержится на SIM-карте в элементарном файле (EF), имеющем идентификатор 6F07. Формат хранения IMSI на SIM-карте описан ETSI в спецификации GSM 11.11. Кроме того, IMSI используется любой мобильной сетью, соединенной с другими сетями (в частности с CDMA или EVDO) таким же образом, как и в GSM сетях. Этот номер связан либо непосредственно с телефоном, либо с R-UIM картой (аналогом SIM карты GSM в системе CDMA) [9].

Длина IMSI, как правило, составляет 15 цифр, но может быть короче. Например: 250-07-XXXXXXXXXX. Первые три цифры это MCC (Mobile Country Code, мобильный код страны). В примере 250 - Россия. За ним следует MNC (Mobile Network Code, код мобильной сети). 07 из примера - СМАРТС. Код мобильной сети может содержать две цифры по европейскому стандарту или три по североамериканскому. Все последующие цифры — непосредственно идентификатор пользователя MSIN (Mobile Subscriber Identification Number) [9].

D. Serial number

Серийный номер можно определить у устройств, не обладающих сервисом телефонии начиная с операционной системы Android 2.3 (“Gingerbread”) и у некоторых телефонов [3].

E. Android Id

Это 64 битный номер, который случайным образом генерируется при первом запуске устройства и остается неизменным далее. У устройств с операционной системой более ранних версий чем 2.2 (“Froyo”) он может не определяться [3].

F. Mac-Address

MAC-адрес (от англ. Media Access Control — управление доступом к среде, также Hardware Address) — это уникальный идентификатор, присваиваемый каждой единице оборудования компьютерных сетей. Большинство сетевых протоколов канального уровня используют одно из трёх пространств MAC-адресов, управляемых IEEE: MAC-48, EUI-48 и EUI-64. Адреса в каждом из пространств теоретически должны быть глобально уникальными. Не все протоколы используют MAC-адреса, и не все протоколы, использующие MAC-адреса, нуждаются в подобной уникальности этих адресов [2][10].

В широковещательных сетях (таких, как сети на основе Ethernet) MAC-адрес позволяет уникально идентифицировать каждый узел сети и доставлять данные только этому узлу. Таким образом, MAC-адреса формируют основу сетей на канальном уровне, которую используют протоколы более высокого (сетевого) уровня. Для преобразования MAC-адресов в адреса сетевого уровня и обратно применяются специальные протоколы (например, ARP и RARP в сетях IPv4 и NDP в сетях на основе IPv6) [10].

Адреса вроде MAC-48 наиболее распространены; они используются в таких технологиях, как Ethernet, Token ring, FDDI, WiMAX и др. Они состоят из 48 бит, таким образом, адресное пространство MAC-48 насчитывает 248 (или 281 474 976 710 656) адресов. Согласно подсчётам IEEE, этого запаса адресов хватит по меньшей мере до 2100 года [10].

EUI-48 от MAC-48 отличается лишь семантически: в то время как MAC-48 используется для сетевого оборудования, EUI-48 применяется для других типов аппаратного и программного обеспечения.

Идентификаторы EUI-64 состоят из 64 бит и используются в FireWire, а также в IPv6 в качестве младших 64 бит сетевого адреса узла.

Можно также получить MAC-адрес Wi-Fi или Bluetooth оборудования устройства, однако не рекомендуется использовать его в качестве уникального идентификационного номера, так как не все мобильные устройства имеют Wi-Fi. Если Wi-Fi модуль есть, он должен быть обязательно включен, иначе MAC-адрес не определится. Кроме того, MAC-адрес устройства можно изменить программным путем [10].

III. Модель цифровых сертификатов задачи

Идея цифровых сертификатов состоит в создании открытой базы данных, где каждый владелец мобильного телефона мог бы сохранить идентифицирующие признаки своего аппарата, заверив (подписав) их ссылкой на собственный профайл в социальной сети. Идея использования ссылки на профайл состоит в том, что в этом случае база данных избегает проблем, связанных с хранением персональной информации. В таком случае ее просто нет. Она вся остается в социальной сети.

Соответственно этому, реализация такой модели

должна включать в себя мобильное приложение для создания сертификата, базу данных для хранения сертификатов и интерфейс к базе данных для поиска.

Владелец телефонного аппарата может бесплатно, по собственной инициативе, добавить сертификат для своего телефона в общую базу. База сертификатов публично доступна. Следовательно, сильно упрощается процесс проверки владельца телефона. А это, в свою очередь, сможет остановить какой-то значимый процент мобильных абонентов от пользования телефоном, который попал к ним не совсем законным способом. Кроме того, такая база может оказаться подспорьем для официального следствия.

В данной работе решено было использовать IMEI номер и Android ID, чтобы увеличить надежность идентификация Android аппарата. На практике, не у всех устройств определяются оба эти номера, но хотя бы один из них определяется практически всегда. Мобильные операторы для взаимодействия с телефоном используют IMEI номер.

Мобильное приложение разработано на *Java*, в среде *Eclipse*. Так как именно для этой среды существует официальный плагин *Android Developer Tools* (ADT), который предоставляет профессиональную среду разработки Android-приложений. Для определения IMEI номера и Android ID воспользовались классами *TelephonyManager* и *Settings*. Для определения ссылки на страницу пользователя в Facebook воспользовались некоторыми функциями Facebook SDK. В результате, при нажатии на кнопку регистрации, пользователь перенаправляется в окно авторизации в Facebook. Иными словами, используется стандартная схема авторизации с помощью Facebook в сторонних приложениях.

Взаимодействие с удаленной базой данных осуществлено на PHP с использованием JSON, в отдельном классе *JSONParser*, с помощью функций из класса *org.apache.http*.

JSON (англ. JavaScript Object Notation) это текстовый формат обмена данными, основанный на JavaScript и обычно используемый именно с этим языком. Несмотря на происхождение от JavaScript, формат считается языко-независимым и может использоваться практически с любым языком программирования. Для Java и PHP существуют функции для создания и обработки данных в формате JSON.

В качестве удаленной базы данных используется MySQL. Основная таблица содержит 4 столбца: ID, IMEI, AndroidID и Link. Взаимодействие с ней сделано таким образом, чтобы было невозможно добавить строку с каким-то определенным IMEI-номером или Android ID более одного раза.

Для того, чтобы информировать пользователя об успешной отправке запроса с телефона в базу данных, и успешной авторизации в Facebook, добавлено соответствующее всплывающее сообщение (*Toast*) и функция добавления фото из профайла пользователя с его личной страницы. На рисунке 1 представлен общий вид после авторизации, получившегося в итоге приложения на Android-эмуляторе. А на рисунке 2 – вид окна авторизации в Facebook.

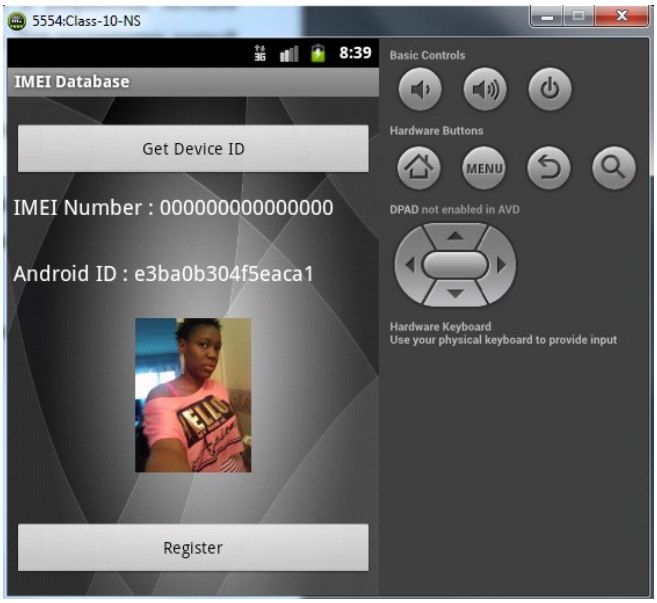

Рис. 1. Приложение после авторизации.

Для того чтобы просматривать удаленную базу данных приложения авторами был сделан сайт *http://fr30706.tw1.ru/*.

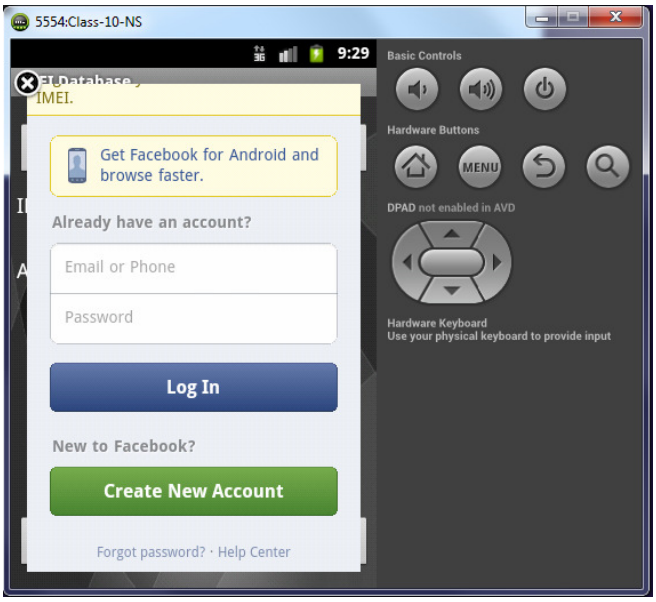

Рис. 2. Окно авторизации в Facebook.

На рисунке 3 представлен вид главной страницы сайта. На этом сайте по вкладке «Search» можно перейти на страницу с функциональностью поиска по получившейся IMEI-базе данных. Взаимодействие сайта с базой данных реализовано на PHP. Искать записи в базе данных можно по любому из трех полей: по IMEI номеру, по Android ID, или же по ссылке на личную страницу в Facebook. На рисунке 4 представлен вид страницы поиска.

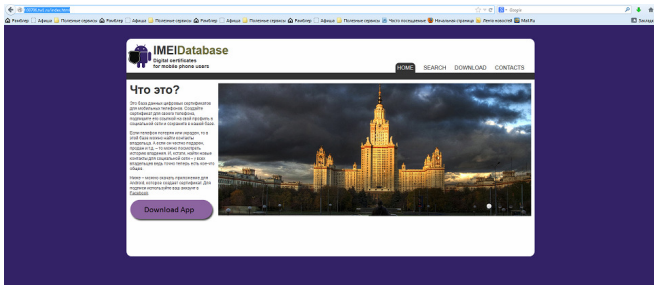

Рис. 3. Главная страница сайта проекта.

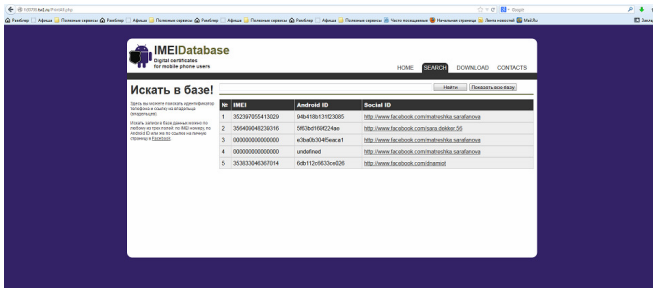

Рис. 4. Страница поиска по базе данных.

Также на этом сайте можно скачать последнюю версию приложения для аппаратов с операционной системой Android.

Дизайн сайта разработан с поддержкой технологии Responsive Design, чтобы сайт хорошо отображался, и с ним было удобно работать как на стандартных компьютерных мониторах, так и на маленьких экранах смартфонов. Таким образом, у сайта реализованы 2 разные разметки.

На рисунке 5 представлен вид страницы поиска на экране смартфона. А на рисунке 6 – сравнительный вид страницы «DOWNLOAD» на экране монитора и на Android-эмуляторе.

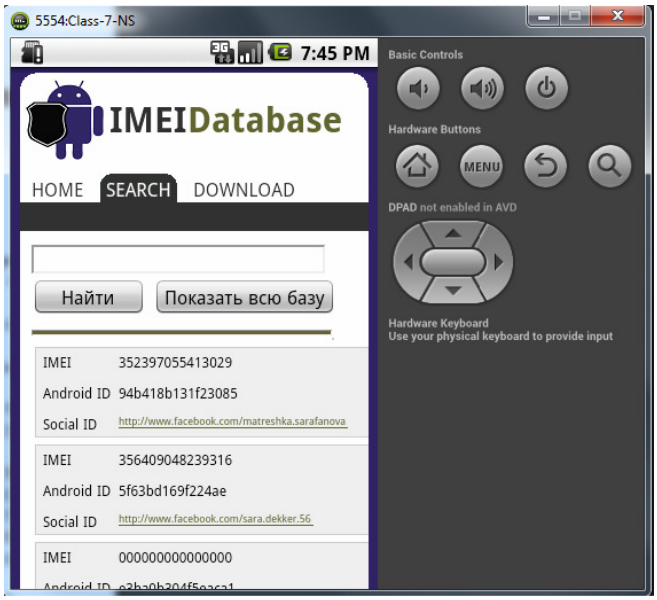

Рис. 5. Страница поиска на экране смартфона.

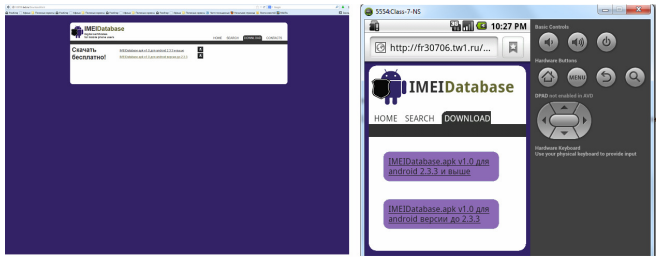

Рис. 6. Страница «DOWNLOAD» на разных экранах.

IV. Дальнейшие разработки

Можно указать следующие направления развития проекта. Во-первых, можно предложить пользователям физическое изготовление сертификатов. Это может быть реализовано в виде печати наклейки с QR-кодом, которая содержит URL для страницы с результатами поиска данного сертификата в базе данных. Получается некоторая аналогия контекстно-зависимого QR-кода [11].

Другим возможным направлением работы является добавление открытого API к базе данных. В этом случае, искать подтверждения владения можно будет программно. Например, приложения типа Geo Messages [12] смогут еще и проверять законность владения телефоном отправителя сообщений.

V. Заключение

Разработана и реализована модель цифровых сертификатов для владельцев мобильных устройств. Реализованы клиентские компоненты – мобильное приложение, веб-сайт для поиска по базе данных. И серверный компонент – база данных с интерфейсом для записи и поиска.

С помощью этой системы пользователь может создать сертификат для своего мобильного телефона, подписать его ссылкой на свой профиль в социальной сети и сохранить в базе данных.

Если телефон потерян или украден, то в этой базе можно найти контакты владельца. А если он честно подарен, продан и так далее – то можно посмотреть историю владения.

Библиография

[1] В. Шалькевич, А. Макаревич «Противодействие теневому обороту мобильных телефонов уголовно правовыми мерами», Журнал «Законность и правопорядок», No 3(7)/2008, стр. 36-40.

[2] http://ru.wikipedia.org/

[3] http://developer.samsung.com/android/technical-docs/How-to-retrieve-the-Device-Unique-ID-from-android-deviceJ.

[4] GSME proposals regarding mobile theft and IMEI security (https://docs.google.com/viewer?a=v&q=cache:0mXtXE_yM3EJ:www.gsmeurope.org/documents/positions/gsme_proposals_mobile_thefts_imei_security.pdf+imei+standard&hl=en&gl=au&pid=bl&srcid=ADGEESgutC2Wv66x8SweH6Tb3AIpZ_e0FtPSpsHeFrswQiPqnm5TgPV440ooDWS_ElQc8aPkeimqNLbd969ngHkpbIbtCcVHQzi_PyYDa0LTFY1m7Pf0Fuh40RUMIpUq4Hf0cAl8ZND4&sig=AHIEtbStnM1cqejWPnMi2PpVLCDSSfJgJQ).

[5] GSM Association Non Confidential Official Document IMEI Allocation and Approval Guidelines Version 6.0 (27th July 2011) (http://www.gsma.com/newsroom/wp-content/uploads/2012/03/ts0660tacallocationprocessapproved.pdf).

[6] http://www.legislation.gov.uk/ukpga/2002/31/section/1.

[7] http://www.amta.org.au/pages/amta/FAQs.on.mobile.security.

[8] 3G Mobile Equipment Identifier (MEID) (3GPP2 S.R0048-A Version 4.0 Date: 23 June 2005).
[9] Fred Gaechter "Chairman of IMSI Oversight Committee" (IOC)(GSMNA Doc 036/02) (http://www.ifast.org/files/IFAST22_015_GSMNALetter.pdf).
[10] IEEE Standard for Local and Metropolitan Area Networks: Overview and Architecture (IEEE Std 802®-2001 (R2007)(Revision of IEEE Std 802-1990)).
[11] D. Namiot. Network Proximity on Practice: Context-aware Applications and Wi-Fi Proximity. International Journal of Open Information Technologies, 1(3), 2013, pp. 1-4.
[12] Namiot, D. “Geo messages”, In Ultra Modern Telecommunications and Control Systems and Workshops (ICUMT), 2010 International Congress on (pp. 14-19). IEEE. DOI: 10.1109/ICUMT.2010.5676665