УДК 681.322;003.26

Скалозуб В. В.,
бакалавр,
ovstreltsov@gmail.com
Ситников В. С.,
д-р техн. наук, профессор,
sitnvs@mail.ru
Яковлев Д. П.,
канд. техн. наук, профессор,
Одесский национальный
политехнический университет,
г. Одесса, Украина,
e-mail ----------

ЦИФРОВЫЕ СЕРТИФИКАТЫ ДЛЯ ВЛАДЕЛЬЦЕВ МОБИЛЬНЫХ ТЕЛЕФОНОВ

У каждого владельца мобильного телефона записано некоторое количество важной информации на нем, которую тяжело восстановить. Важной задачей является нахождение утерянных аппаратов. В данной статье рассматриваются мобильные устройства с операционной системой Android – смартфоны и др. У всех подобных аппаратов имеются различные идентификационные номера, которые могут быть использованы для нахождения.

Ключевые слова: *IMEI; MEID; ESN; IMSI; MAC-Address; Serial Number; Android ID.*

Постановка проблемы. Система мобильной связи, как и Интернет, являются открытыми (не безопасными) системами, в том смысле, что перехват, модификация сообщений или создание ложных сообщений и т.д. доступны среднему хакеру, не говоря уже о полной доступности информации со стороны провайдеров Интернет или мобильной связи.

Анализ последних исследований и публикаций. Среди авторов, чьи исследования послужили основой написания данной статьи, можно выделить А. Колосову и Д. Намиот. В их статье «Цифровые сертификаты для владельцев мобильных телефонов» в журнале International Journal of Open Information Technologies за 2013 год рассматривается задача подтверждения факта владения мобильным телефоном [3]. Ими 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).

Постановка задачи. Постановка задачи данной статьи является рассмотрение мобильных устройств с операционной системой Android – смартфонов и др. Анализ модели цифровых сертификатов для мобильных телефонов, предложенной А. Колесовой и Д. Намиот. Изучение введения возможности проверки владельца в момент использования телефона.

Изложение основного материала. В настоящее время все более востребованными являются услуги Мобильного банкинга (М-банкинг, mBanking). Эта система предназначена для: контроля за движением средств по банковскому счету с помощью SMS-сообщений на мобильный телефон или через WAP-протокол; управления банковскими счетами.

Услуги мобильного банкинга широко распространены. Сегодня пользователи М-банкинга в ряде банков могут [2]:

– в любое время суток без посещения банка, отправив SMS-запрос с мобильного телефона, получать информацию о состоянии карточного счета (об остатке денежных средств и последних N транзакциях), о номерах своих счетов, а также о номерах платежных карт к счетам, подключенным к М-банкингу;

– автоматически получать на дисплей мобильного телефона информацию о поступлении и списании средств со счета, обо всех операциях с платежной карточкой, о каждой проведенной операции или авторизации по счету;

– в случае необходимости блокировать карточку, отправив соответствующее SMS-сообщение;

– получать информацию о статусе карточек, подключенных к системе М-банкинг и временно блокировать/разблокировать услуги М-банкинга по этим карточкам.

Исходя из этого перечня, очевидно, что сообщения мобильной связи требуют защиты конфиденциальности (шифрованием) и дополнительно защиты авторства и целостности сообщений (цифровой подписью для того, чтобы сообщения имели юридический статус электронного документа).

Существует несколько различных типов идентификационных номеров для аппаратов с операционной

системой Android. В недавнем прошлом все Android-аппараты обладали сервисами телефонии, поэтому всегда можно было определить уникальный номер IMEI, MEID или ESN. Но сейчас уже существуют Wifi-only аппараты, музыкальные плееры и др. устройства с операционной системой Android, не обладающие сервисами телефонии. У таких устройств тоже можно определить идентификационные номера. Ниже указаны все имеющиеся на данный момент типы идентификационных номеров Android-аппаратов.

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, 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. Опорная сеть GSM хранит IMEI в EIR.

EIR (Equipment Identity Register) – регистр идентификации абонентского оборудования. Он относится к NSS (Система коммутации) сетей стандартов GSM и UMTS. Представляет собой базу данных с информацией об оборудовании абонентов с указанием: можно ли данному оборудованию зарегистрироваться в сети или нет (рис. 1).

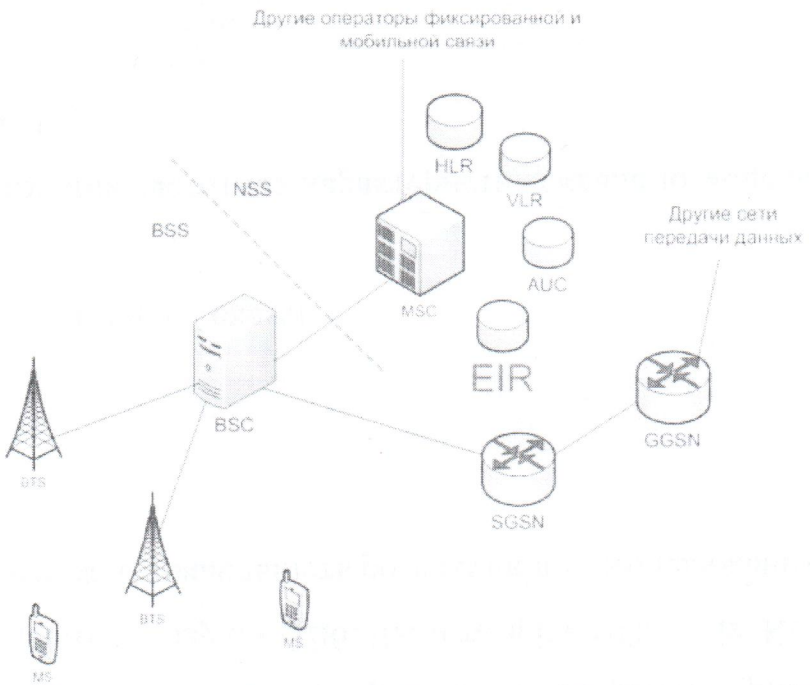

Рис. 1. Идентификация абонентского оборудования (EIR) в составе сети GSM

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.

В EIR хранятся три списка (белый, серый и черный) с IMEI (international mobile equipment identity) – идентификаторами оборудования абонентов. Наличие IMEI в белом списке разрешает доступ в сеть безоговорочно. Оборудование из серого списка будет допущено в сеть, но будет непрерывно отслеживаться во время его нахождения в сети. Черный список предназначен для хранения IMEI аппаратов, которым в сеть доступ запрещен. Исходя из этого, назначение EIR очевидно: оказать помощь правоохранительным органам в поиске и отслеживании абонентов и украденного оборудования [6].

Согласно СТБ 1356-2002 «Система сухопутной подвижной цифровой сотовой связи общего пользования GSM 900» система сотовой связи состоит из [4]:

1. Подсистемы коммутации, которая включает:

– центр коммутации подвижных служб, выполняющий функции коммутации вызовов абонентов системы и стационарной сети;

– регистр пользователя – централизованную сетевую базу данных, хранящую информацию обо всех зарегистрированных абонентах сети данного оператора и видах услуг, которые могут быть им оказаны;

– регистр регистрации посетителя – базу данных, хранящую информацию обо всех абонентах, находящихся в данное время в зоне обслуживания центра коммутации подвижных служб;

– центр аутентификации – базу данных, взаимодействующую с регистром пользователя с целью

определения подлинности абонента и недопущения несанкционированного использования сети;

– регистр идентификации оборудования – базу данных, содержащую информацию об оборудовании подвижных станций.

2. Подсистемы базовых станций, которая включает:

– контроллер базовых станций;

– базовые станции, состоящие из приемопередающего оборудования и антенных систем. Базовые станции обеспечивают информационный обмен с подвижными станциями.

3. Подвижных станций, которые состоят из абонентского терминала (именуемого в быту как сотовый телефон) и модуля подлинности абонента (SIM).

4. Подсистемы эксплуатации и обслуживания сети GSM, которая, как правило, включает центр эксплуатации и технического обслуживания – компьютерный центр управления функциями эксплуатации и обслуживания центра коммутации подвижных служб.

Исходя из содержания указанного стандарта IMEI идентифицирует конкретный сотовый телефон в системе сотовой связи аналогично тому, как, например, номер кузова автомобиля идентифицирует автомобиль в системе регистрации автотранспортных средств (при указанной аналогии государственный регистрационный номер автотранспортного средства можно сравнить с SIM-картой) [4].

MEID (Mobile Equipment IDentifier) – глобальный уникальный идентификатор подвижного оборудования, работающий в сетях CDMA, использует тот же базовый формат, что и IMEI [13][5]. MEID был создан на смену ESN [5].

ESN (Electronic Serial Number) – уникальный номер для идентификации CDMA мобильных телефонов [13].

IMSI (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 [8]. 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) [8].

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) [2].

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].

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) [2]. 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 [2]. 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. Возможно 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 есть он должен быть обязательно включен, иначе MAC-адрес не определится. Кроме того MAC-адрес устройства можно изменить программным путем [2].

Серийный номер можно определить у устройств, не обладающих сервисом телефонии начиная с операционной системы Android 2.3 («Gingerbread») и у некоторых телефонов [13].

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 [13].

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 контак-

ты владельца. А если он честно подарен, продан и так далее – то можно посмотреть историю владения.

Можно согласиться с мнением Д. Е. Намиот [3], что 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 профиль 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. Вся персональная информация остается в социальной сети.

В базе данных сертификатов хранится только открытая ссылка на соответствующий профиль. 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. Важный момент, что такой интерфейс должен включать в себя и программный API.

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.

Модель 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 [3].

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.

Таким образом, общая идея данной модели состоит не в отслеживании потерянного (похищенного) телефона, а во введении возможности проверки владельца телефона в момент использования телефона. При этом, в первую очередь, имеется в виду использование смартфонов в сети Интернет. Самая простая модель использования: приложение во время авторизации пользователя в социальной сети может проверить, кому принадлежит данный телефон.

Естественно, что ничто не препятствует и операторам связи использовать ту же самую открытую базу данных для проверки владельцев в момент совершения звонков и отправки SMS.

К примеру, Orange Moldova предоставляет возможность для всех клиентов PrePay и Абонемент, с активированной услугой Мобильной Подписи, обновлять цифровой сертификат, дистанционно: с мобильного телефона, через SMS или по интернету, зайдя на semnatura.orange.md. Сертификат может быть обновлен дистанционно, только в течении последних 30 дней действительности текущего сертификата.

Мобильная Подпись работает на основе цифрового сертификата: «Сертификат публичного ключа». Этот сертификат включает в себя ваши идентификационные данные и гарантирует ваш статус владельца Мобильной Подписи, при использовании услуги. В соответствии с законодательством, срок действия сертификата публичного ключа составляет 1 год с даты выпуска.

Формально говоря, цифровой сертификат – это всего лишь открытый ключ, подписанный центром сертификации. Существует еще закрытый ключ, который должен хранится у владельца сертификата. То, что зашифровано с помощью открытого ключа, можно расшифровать исключительно закрытым ключом, и наоборот. Подразумевается, что открытый ключ известен всем, поэтому он так и называется.

Информация, зашифрованная закрытым ключом, может быть расшифрована кем угодно, так как открытый ключ ни от кого не прячется. Однако можно однозначно сказать, что расшифрованная информация исходила только от того, у кого есть закрытый ключ. Это и есть цифровая подпись.

Информация, зашифрованная открытым ключом, может быть расшифрована закрытым ключом, это значит, что прочитает ее только владелец сертификата. А шифровать открытым ключом может кто угодно, так как открытый ключ доступен всем. Это и есть шифрование сообщений.

Цифровые сертификаты выпускает издающий центр сертификации. Если сертификат был скомпрометирован (например владелец сертификата не сберег свой закрытый ключ), то сертификат отзывается. Центр сертификации выпускает и подписывает список отозванных сертификатов CRL (Certificate Revocation List), который потом публикуется на сервере. Ссылка на этот ресурс содержится в каждом выпущенном сертификате, поэтому приложение, использующее сертификаты (например VPN сервер) может загрузить CRL и проверить действительность сертификата.

Для большей защищенности, пара ключей может храниться на специальных смарт-картах (smart card) или USB-ключах (cryptographic token). Из большинства подобных изделий физически невозможно извлечь закрытый ключ, что делает компрометацию закрытого ключа крайне маловероятной.

Заключение. *Основная идея исследуемой модели* состоит не в отслеживании потерянного (похищенно-

го) телефона, а во введении возможности проверки владельца телефона в момент использования телефона. При этом, в первую очередь, имеется в виду использование смартфонов в сети Интернет. Самый простой способ применения: приложение во время авторизации пользователя в социальной сети может проверить, кому именно принадлежит данный телефон. Дальнейшие исследования могут быть направлены на изучение и анализ электронной цифровой подписи для защиты мобильных приложений.

ЛИТЕРАТУРА

1. Namiot D. Geo messages, In Ultra Modern Telecommunications and Control Systems and Workshops (ICUMT) / D. Namiot. // International Congress. – 2010. – №2. – P. 14–19.
2. Namiot D. Network Proximity on Practice: Context-aware Applications and Wi-Fi Proximity / D. Namiot. // International Journal of Open Information Technologies. – 2013. – №1. – P. 1–4.
3. Колесова А., Намиот Д. Цифровые сертификаты для владельцев мобильных телефонов / А. Колесова, Д. Намиот // International Journal of Open Information Technologies. – 2013. – №4. – С. 1–5.
4. Шалькевич В., Макаревич А. Противодействие теневому обороту мобильных телефонов уголовно правовыми мерами / В. Шалькевич, А. Макаревич // Законность и правопорядок. – 2008. – № 3(7). – С. 36–40.
5. 3G Mobile Equipment Identifier (MEID) (3GPP2 S.R0048-A Version 4.0 Date: 23 June 2005) [Электронный ресурс]. – Режим доступа : http://www.3gpp2.org/public_html/specs/S.R0048-A_v4.0_050630.pdf.
6. Equipment Identity Register (EIR) [Электронный ресурс]. – Режим доступа : http://celnet.ru/EIR.php.
7. FAQs on mobile security [Электронный ресурс]. – Режим доступа : http://www.amta.org.au/pages/amta/FAQs.on.mobile.security.
8. Gaechter F. Chairman of IMSI Oversight Committee [Электронный ресурс] / Fred Gaechter. – 2002. – Режим доступа : http://www.ifast.org/files/IFAST22_015_GSMNALetter.pdf.
9. GSM Association Non Confidential Official Document IMEI Allocation and Approval Guidelines Version 6.0 (27th July 2011) [Электронный ресурс]. – Режим доступа : http://www.gsma.com/newsroom/wpcontent/uploads/2012/03/ts0660tacallo cationprocessapproved.pdf
10. GSME proposals regarding mobile theft and IMEI security [Электронный ресурс]. – Режим доступа : https://docs.google.com/viewer?a=v&q=cache:0mXtXE_yM3EJ:www.gsmeurope.org/documents/positions/.
11. IEEE Standard for Local and Metropolitan Area Networks: Overview and Architecture // [Электронный ресурс]. – Режим доступа : https://standards.ieee.org/findstds/standard/802-2014.html.
12. Re-programming mobile telephone [Электронный ресурс]. – Режим доступа : http://www.legislation.gov.uk/ ukpga/2002/31/section/1.
13. Техническая документация к устройствам Android Samsung [Электронный ресурс]. – Режим доступа : http://developer.samsung.com/android/technical-docs/How-toretrieve-the-Device-Unique-ID-from-android-device.

В. В. Скалозуб,
В. С. Ситніков,
Д. П. Яковлев,
Одеський національний політехнічний університет,
м. Одеса, Україна

ЦИФРОВІ СЕРТИФІКАТИ ДЛЯ ВЛАСНИКІВ МОБІЛЬНИХ ТЕЛЕФОНІВ

У кожного власника мобільного телефону записано кілька важливої інформації на ньому, яку важко відновити. Важливим завданням є знаходження загублених апаратів. У статті розглядаються мобільні пристрої з операційною системою Android – смартфони і ін. У всіх подібних апаратів є різні ідентифікаційні номери, які можуть бути використані для знаходження.

Ключові слова: *IMEI; MEID; ESN; IMSI; MAC-Address; Serial Number; Android ID.*

V. V. Skalozub,
V. S. Sytnikov,
D. P. Yakovlev,
Odessa National Polytechnic University,
Odessa, Ukraine

DIGITAL CERTIFICATES FOR MOBILE PHONE OWNERS

Every cell phone owner's written a number of important information on it that is hard to restore. An important task is to find the lost phones. This article discusses the mobile devices with the Android oper-

ating system – smart phones and other. All of these devices have different identification numbers that can be used to find.

Key words: *IMEI; MEID; ESN; IMSI; MAC-Address; Serial Number; Android ID.*

Рецензенти: д. т. н., проф. ***М. П. Мусієнко;***
к. т. н., доц. ***І. М. Журавська.***

Дата надходження статті до редколегії 03.10.16