УДК 004.004

Студ. А.В. Кизино, Е.В. Обухова
Науч. рук. ст. преп. Н.В. Ржеутская
(Кафедра информационных систем и технологий, БГТУ)

ИСПОЛЬЗОВАНИЕ NFC ТЕХНОЛОГИЙ ДЛЯ ПОМОЩИ МАЛО ЗАЩИЩЕННЫМ СЛОЯМ НАСЕЛЕНИЯ

В настоящее время технология NFC (Near Field Communication) широко используется для бесконтактных платежей, обмена данными и других целей. Однако потенциал этой технологии не ограничивается этими сферами. В этой статье мы рассмотрим, как технология NFC может быть использована для помощи мало защищенным слоям населения, таким как пожилые люди, люди с инвалидностью или хроническими заболеваниями, дети и другие группы, нуждающиеся в социальной поддержке.

Использование NFC в здравоохранении. Достаточно обширная группа людей, которым может помочь NFC технологии – люди с заболеваниями различной стадии. Многие заболевания сопровождаются периодами обострения, которые могут начаться в самый неожиданный момент: на улице, в общественном месте, на работе. В эти моменты важно грамотно оказать медицинскую помощь. Зачастую фельдшерам достаточно сложно сразу определить причину ухудшения состояния здоровья пациента, что приводит трате драгоценного времени. Поэтому возможно использовать NFC чипы, встроенные в смартфоны, в качестве портативной медицинской карты, на которой будет записано заболевание пациента, его лечащий врач, контакты родственников, аллергии и другой. Концепция такова: приложение имеет три ключевые роли - пациент, лечащий врач и фельдшер. Пациент скачивает приложение и заходит в свой аккаунт, с этого момента система начинает работать в фоновом режиме. Лечащий врач имеет список своих пациентов и имеет возможность заполнять данные о пользователе, тем самым можно гарантировать корректность и достоверность данных. Фельдшеру же достаточно просто приложить свой мобильный телефон к телефону пациента и получить всю необходимую информацию и незамедлительно приступить к оказанию медицинской помощи. Однако, в этой системе есть некоторые преграды, например, как фельдшер сможет понять, что приложение работает и пациент подключен к нему? Эту проблему возможно решить, например, при помощи специальных наклеек, которые будут клеятся на заднюю поверхность телефона, тем самым показывая, что человек имеет данное приложение. Следующая преграда заключается в том, что на телефоне пациента всегда должен быть включен NFC-модуль, что существенно влияет на

производительность устройство и на время его работы. В качестве альтернативы, можно предложить использовать магнитный чип, подобный тому, что установлен в пластиковых картах и проездных, выступающий в качестве посредника. NFC-модуль пациента записывает на чип номер пациента, по которому можно получить информацию. Затем модуль NFC на устройстве пациента можно отключить, т.к. теперь необходимые данные есть на чипе. После этого, при необходимости фельдшер сможет получить данные с чипа вне зависимости от состояния телефона.

УДК 004.056.55

Студ. П.П. Позняк
Науч. рук. проф. П.П. Урбанович
(Кафедра информационных систем и технологий, БГТУ)

СКВОЗНОЕ ШИФРОВАНИЕ ИЛИ END-TO-END ENCRYPTION (E2EE) В МЕССЕНДЖЕРАХ

Современные технологии связи позволяют людям общаться мгновенно, независимо от расстояния и времени. Однако, при этом, возникает вопрос безопасности передачи информации [1, 2]. Одним из методов защиты данных является сквозное шифрование (СШ), которое позволяет защитить сообщения, передаваемые через мессенджер, от доступа третьих сторон. В данном исследовании мы рассмотрим, почему мессенджеры, использующие СШ, являются более защищенными, чем те, что не используют его.

Для понимания того, как работает данный метод, необходимо прояснить, что он из себя представляет. СШ, или end-to-endencryption – это технология шифрования, которая позволяет зашифровать сообщения перед отправкой, таким образом, что только отправитель и получатель могут их прочитать [3].

Как работает СШ на примере двух пользователей А и Б? Пользователь Б хочет поздороваться с А конфиденциальным сообщением. Расшифровать его может только закрытый ключ А. Открытый ключ может быть передан кому угодно, но закрытый ключ предназначен только для А.

Сначала Б использует открытый ключ А для шифрования сообщения и преобразует сообщение «Привет А от Б!» в закодированный текст, буквы которого кажутся бессмысленными и случайными. Б отправляет это зашифрованное сообщение через общедоступный Интернет. Это сообщение может проходить через несколько серверов, включая серверы почтовых провайдеров и серверы интернет-провайдеров.