ИСПОЛЬЗОВАНИЕ ОДНОРАЗОВОГО SMS-КОДА ДЛЯ АУТЕНТИФИКАЦИИ ПОЛЬЗОВАТЕЛЯ НА ПЛАТФОРМЕ ANDROID

Новик А.М.
Белорусский государственный университет информатики и радиоэлектроники
г. Минск, Республика Беларусь
Пискун Г.А. – канд. техн. наук, доцент

Одним из наиболее надёжных способов защиты пользовательских данных в мобильном приложении является использование одноразового SMS-кода. Актуален этот способ для приложений, которые хранят важную информацию пользователя, такую как номера банковских карт, сообщения, фотографии, которые имеют доступ к финансовым операциям пользователя.

Преимущества такого способа: каждая операция подтверждается новым, автоматически сгенерированным кодом. Таким образом, если кто-то подсмотрит или перехватит код – второй раз его не получится использовать, те же трудности возникнут, если его подобрать или угадать.

Реализация автоматической подстановки SMS-кода в поле ввода – это выгодное решение для разработчика, так как такой функционал является очень удобным для пользователя: исключены лишние действия по прочтению сообщения из другого приложения, исключён ручной ввод и подтверждение введённой информации, исключена ошибка ввода неправильного кода.

Проблема реализации такого функционала заключается в доступе к сообщениям пользователя. Не каждый пользователь желает давать доступ к своим сообщениям, что может повлиять на количество пользователей. Однако не всегда пользователи обращают внимание на требования при скачивании приложения с playMarket и могут столкнуться с тем, что приложение будет иметь доступ к личным сообщениям без их ведома, что в свою очередь может плохо сказаться для пользователя: он может столкнуться с киберпреступностью.

Для повышения уровня защиты пользовательских данных компания Google запретила выкладывать в playMarket приложения, запрашивающие доступ к SMS пользователя.

Одновременно с этим разработчики из компании Google предложили следующие способы решения возникшей проблемы:

- автоматическая подстановка кода, но при этом сообщение должно иметь специальный хэш-код, генерируемый приложением;
- подстановка смс кода в одно касание – при старте операции верификации пользователя приложение делает запрос на разрешение к прочтению сообщений от определенного номера телефона, появляется диалоговое окно, в котором пользователь выбирает «разрешить/запретить», после разрешения происходит автоматическая подстановка кода в соответствующее поле ввода.

Анализ второго способа привёл к тому, что данный способ не является гибким для пользователя, так как предусматривает чтение сообщения и выполнение лишних действий. В случае если пользователь случайно или по незнанию запретит доступ к прочтению сообщения, то у него возникнут трудности с аутентификацией в приложении. Это может повлиять на лояльность пользователя к компании и приложению, отчего в свою очередь зависит коммерческая составляющая бизнеса.

Особенность первого способа в том, что хэш-код выступает в роли сигнала приложению, который означает, что именно это сообщение можно прочитать. Таким образом, этот способ не нарушает границы конфиденциальности пользователя, является удобным в использовании и наиболее актуальным на сегодняшний день.

Список использованных источников:

1. SMS Verifiction [Электронный ресурс]. – Режим доступа: https://developers.google.com/identity/sms-retriever/overview. – Дата доступа: 07.03.2020.