Секция «Круглый стол для школьников «Постигая аудит»»

Уязвимость SMS-сообщений при двухфакторной аутентификации. Новые технологии

Научный руководитель – Тарасов Иван Владимирович

Киселев Фёдор Сергеевич
E-mail: tiwell26@rambler.ru

ГБОУ «Школа №556», Москва, Днепропетровская ул., 33А

Аннотация. С каждым годом появляется всё больше информации, а имеющаяся ранее — устаревает, становясь не актуальной. Мир интернета тесно связан с реальным миром.

Ключевые слова: информационная безопасность, аутентификация, виртуальный мир, игры, sms-сообщения.

Annotation. Every year more and more information appears, and the previously available information becomes outdated, becoming irrelevant. The world of the Internet is closely connected with the real world.

Keywords: information security, authentication, virtual world, games, sms messages.

Введение

В настоящее время мы живём в мире VUCA (Volatility, Uncertainty, Complexity, Ambiguity). С каждым годом появляется всё больше информации, а имеющаяся ранее — устаревает, становясь не актуальной. Мир Интернета тесно связан с реальным миром. В сфере информационной безопасности с каждым годом возникает всё больше проблем. Некоторые компании соревнуются между собой за первенство в обеспечении наиболее оптимального варианта для защиты данных своих пользователей, и самой главной проблемой является проблема авторизации, а если точнее — аутентификации: возможность контроля информации от проникновения со стороны, юридические ограничения системы.

Уязвимость SMS-сообщений при двухфакторной аутентификации

Простой идентификации с аутентификацией пользователя бывает недостаточно, тем более работники компании, ставшие инсайдерами (сотрудник, который своими действиями или бездействием, умышленно или неосознанно причиняет вред организации, в которой работает), становятся угрозой информационной безопасности. Одним из выходов из данной ситуации может стать авторизация не только с персонального компьютера, но и с мобильного телефона или с других гаджетов.

Учитывая повышенный интерес в наше время к видеоиграм, люди-геймеры (человек, играющий в видеоигры), уже не используют для установки игры физические носители: дискеты, картриджи, используют компьютер с доступом в Интернет. Благодаря Интернету в сети стали появляться различные сервисы цифрового распространения видеоигр и программ, таких как Steam, Origin, Epic Games, которые предоставляют возможность пользователю покупать и играть в игры. Но перед этим пользователю необходимо зарегистрироваться, тем самым защитить свой будущий аккаунт, чтобы нежелательный гость не смог воспользоваться купленными человеком играми. Размещая свои личные данные, необходимо их защитить от действий киберпреступников. Пользователю даётся право дополнительно защитить свой аккаунт, чтобы снизить процент взлома к нулю. Здесь мы сможем подключить двухфакторную аутентификацию на примере SMS-сообщений как вид защиты.

Исследуя практику использования данного вида защиты, выявляется ряд **противоречий**:

— если будет настроен фактор аутентификации через мобильное устройство путём SMS-сообщения, то при потере сигнала сети не получится войти в аккаунт.

— если кому-то очень нужно будет — есть вероятность клонирования SIM-карты и перехвата сообщений на уровне провайдера услуг мобильной связи

— vобильное устройство в самый неподходящий момент может разрядиться.

Выявленные противоречия определяют **проблему исследования**: необходимо проанализировать уязвимости двухфакторной аутентификации — SMS-сообщений как вида защиты.

Целью исследования является раскрытие понятия двухфакторной SMS-аутентификации и анализ эффективности использования данного вида защиты. Экспериментальная проверка данного вида защиты для выявления её недостатков.

Объект исследования — процесс повышения целостности SMS-аутентификации в безопасности личной информации.

Предмет исследования — возможность последствий при использовании SMS-аутентификации как слабого вида защиты.

Гипотеза исследования: SMS-аутентификация не будет являться эффективным и безопасным способом защиты, если:

— Заполучили телефон с SIM-картой внутри.

— Используется как самостоятельный вид защиты.

— Перехватят SMS-сообщение с помощью уязвимостей в самой SIM-карте или в телефоне.

— Перевыпустят SIM-карту по поддельным документам.

Для достижения цели исследования и проверки выдвинутой гипотезы был поставлены следующие **задачи**:

1) Раскрыть понятие двухфакторной аутентификации и выделить её виды.
2) Рассмотреть более подробно SMS-Сообщения как вид аутентификации.
3) Рассмотреть примерный алгоритм аутентификации через SMS.
4) Изучить уязвимости SMS-Сообщений при двухфакторной аутентификации.

Теоретико-методологические исследования уязвимости SMS-сообщений при двухфакторной аутентификации

Двухфакторная аутентификация и её виды

Аутентификация имеет особое значение в авторизации пользователя, ведь идентификация без аутентификации бесполезна. Войти в чужой аккаунт, используя логин, достаточно легко, если вы не имеете подтверждения того, что являетесь его владельцем. Дополнительной защитой личной информации - подтверждением того, что вы - это вы, является многофакторная аутентификация, а точнее, двухфакторная аутентификация.

Двухфакторная аутентификация — тип многофакторной аутентификации, требующий для доступа к чему-либо два различных «ключа», один из которых мы знаем (логин или же пароль), а другим владеем (телефон или другой гаджет) [1]. Дополнительный уровень защиты — так называемый второй фактор, подразумевает под собой множество видов, мы же рассмотрим SMS-сообщения как дополнительный уровень защиты [2].

SMS-аутентификация как вид двухфакторной аутентификации

SMS (Short Message Service — служба коротких сообщений) — технология, позволяющая осуществлять приём и передачу коротких текстовых сообщений сотовым телефоном.

SMS-аутентификация является одной из реализаций OTP (One Time Password - Одноразовый пароль), которая получила свою популярность, благодаря простоте использования. На данный момент у большинства людей имеются мобильные телефоны, из-за чего этот метод стал более удобным и популярным. Данный метод имеет большой потенциал для охвата потребителей при низких общих затратах на внедрение [3].

Для начала работы зарегистрировать номер телефона на сервере организации, к ресурсам которой мы хотим получить доступ. После чего при попытке аутентификации на зарегистрированный номер телефона придет SMS с одноразовым паролем для входа в систему.

Возможен и другой вариант. Помимо регистрации номера телефона необходимо знать специальный код. При успешном вводе этого когда на зарегистрированный номер телефона придет SMS с одноразовым паролем для входа в систему.

В качестве примера рассмотрим алгоритм аутентификации через CMC - RSA Mobile. Доставка атрибутов одноразового пароля через CMC на мобильный телефон основана на двух основных программных компонентах: сервер аутентификации и агент, устанавливаемый на защищаемый ресурс.

Для подключения к GSM-сети (Groupe Spécial Mobile — глобальный цифровой стандарт для мобильной сотовой связи) и передачи текстовых сообщений SMS по протоколу SMPP (Short message peer-to-peer protocol — протокол, описывающий взаимодействие конечного клиента с SMS-сервером) используется специальный plug-in (плагин). Никакого дополнительного аппаратного и программного обеспечения на рабочем месте конечных пользователей не требуется.

Схема предоставления доступа зарегистрированному пользователю весьма проста. При входе на Web-портал, защищенный средствами RSA Mobile, вводится имя и пароль, после этого система ищет номер телефона, соответствующий имени абонента, и пересылает на него одноразовый код доступа в виде сообщения SMS. Пользователь вводит код и получает доступ к требуемому ресурсу. Проведенные испытания показали, что код доступа доставляется по назначению менее чем за 6 секунд. Программное обеспечение RSA Mobile, прежде всего, ориентировано на корпоративных пользователей, которые могут применять его в интересах своих сотрудников и клиентов [4].

Уязвимости SMS-аутентификации при двухфакторной аутентификации

Со временем специалисты и обычные пользователи стали сомневаться в надёжности SMS-аутентификации как вида защиты при двухфакторной аутентификации и признали её небезопасной не только для оплаты, но и авторизации. Такое подтверждение всё чаще мы можем найти в публикациях СМИ. Рассмотрим основные уязвимости SMS-аутентификации.

Первая уязвимость SMS-аутентификации, которую мы рассмотрим — это уязвимость протокола SS7 (Signaling System 7 - Сигнальная Система №7). Вообще, сигнальную сеть SS7 разработали в 1975 году (для маршрутизации сообщений при роуминге) и в неё не были изначально заложены механизмы защиты от подобных атак. Подразумевалось, что эта система и так закрытая и защищена от подключения извне. На практике этой не так: к ней можно подключиться. Теоретически, к ней можно подключиться в каком-нибудь Конго или любой другой стране — и тогда вам будут доступны коммутаторы всех операторов в России, США, Европе и других странах. В том числе и перехват входящих SMS любого абонента осуществляется таким образом, как описали специалисты Positive Technologies. При этом атакующему не требуется сложное оборудование: достаточно компьютера под Linux с генератором пакетов SS7, какие можно найти в Интернете.

Если вкратце, то атака представляет собой процедуру регистрации абонента в зоне

действия «фальшивого» MSC/VLR. Исходными данными являются IMSI абонента и адрес текущего MSC/VLR, что можно получить с помощью соответствующего запроса в сети SS7. После проведения регистрации абонента на «фальшивом» адресе MSC/VLR все SMS-сообщения, предназначенные абоненту, будут приходить на узел атакующего. Атакующий может:

— отправить ответ о получении сообщения (у отправляющей стороны будет впечатление, что SMS доставлено получателю);

— не отправлять отчёт о получении и перерегистрировать абонента на прежний коммутатор (в этом случае через несколько минут сообщение будет отправлено получателю вторично);

— отправить отчёт о получении, перерегистрировать абонента на прежний коммутатор и отправить ему изменённое сообщение.

Атака используется для:

— перехвата одноразовых паролей мобильного банка;

— перехвата восстановленных паролей от интернет-сервисов (почты, социальных сетей и т. п.);

— получения паролей для личного кабинета на сайте мобильного оператора

Фактически, эту опцию раньше могли использовать только спецслужбы, ну а сейчас может использовать любой желающий, у которого есть компьютер под Linux. Газета Süddeutsche Zeitung (Южногерманская газета - крупнейшая ежедневная газета) пишет, что доступ к коммутатору SS7 кое-где можно купить за 1000 евро. С помощью взятки можно ещё добыть идентификатор https://en.wikipedia.org/wiki/Global_title мобильного оператора — это тоже возможно в некоторых бедных коррупционных странах, где чиновники иногда позволяют себе нарушать закон в целях личного обогащения.

Злоумышленники узнавали банковские реквизиты жертв с помощью фишинга или зловредов, а затем использовали уязвимость SS7, чтобы получить одноразовый код подтверждения транзакции (mTAN), который банк присылает по SMS [5].

Вторая уязвимость — Угон SIM-карты. Каждый мобильный телефон оснащен картой модуля идентификации абонента, она же SIM-карта. Она содержит всевозможную уникальную информацию о телефоне, пользователе и его операторе. Самым важным элементом является номер телефона.

Мошенники используют копирование номера телефона у оператора мобильной связи на свою SIM-карту. Таким образом они получают доступ к различным ресурсам, связанным с мобильным телефоном жертвы — SIM-свопинг.

Есть два основных метода сим-свопинга:

Первая уязвимость, социальная инженерия. Мошенник узнает данные жертвы, включая имя, номер паспорта и сам номер телефона. Затем он подкупает, заговаривает или обманывает сотрудника телекоммуникационной компании, чтобы получить новую SIM-карту взамен старой. Например, показывает копию паспорта и доверенность на лицо жертвы. Естественно, потерпевший ничего не знает и в один момент просто получает неработающую сим-карту.

Вторая уязвимость, быть сотрудником поддержки оператора, сотрудником сервисного центра и любой другой компании, которая может получить доступ к вашей карте. Есть несколько программ для клонирования сим-карт без обращения к оператору [6]. Если телефон потерян или украден, то SIM-карта так же может оказаться в руках злоумышленника.

Третья уязвимость, отсутствие шифрования. SMS-сообщения, которые отправляются вам, не шифруются. Так, если сообщение с кодом перехватят той же уязвимостью SS7, то злоумышленник сможет спокойной просмотреть содержимое сообщения без ка-

ких-либо дополнительных манипуляций. Никто не отменял, что и ваш оператор может сделать так же. Операторы сотовой связи хранят содержимое этих сообщений разный период времени. Сообщения часто хранятся только в течение нескольких дней, но они хранят метаданные (какой номер отправил сообщение, на какой номер и в какое время) еще дольше. Эти записи могут быть предметом повестки в суд в ходе судебного разбирательства [7].

Четвёртая уязвимость, относится больше к недостатку, но всё же её стоит отнести. В случае отсутствия покрытия сотовой связи (на отдаленных территориях или за рубежом) или если телефон внезапно разрядился, то нам не придёт SMS-код. Так же особенно важно для компаний, защищающие своих пользователей, оплатить комиссию за отправку SMS [8].

Пятая уязвимость, довольно редкий, но простой случай - отсутствие Rate Limit (ограничение по скорости на отправку кодов). Как правило, код подтверждения состоит из 4-6 цифр, так что максимальное количество запросов, необходимых для перебора, — 1 миллион, что совсем не много для современного веба (распределенная система информационных ресурсов — веб-сайтов). В данном случае оставалось просто найти номер, который зарегистрирован в сервисе, отправить на него код и перебрать его, без каких-либо ограничений. В большинстве случаев есть лимиты на перебор полученного кода и нужно искать обход [9], но есть уже более интересный случай - одинаковый код для разных эндпоинтов (конечная точка, шлюз, который соединяет серверные процессы приложения с внешним интерфейсом). В данном случае было два эндпоинта, где можно было получать код на номер. При регистрации лимита не было. И вот этим удалось воспользоваться из-за ошибки разработчиков, так как они генерировали для эндпоинта авторизации и регистрации один и тот же код. Использовать это можно было следующим образом, авторизация с помощью номера, получал код и начинал перебирать этот код не на эндпоинте авторизации, а на эндпоинте регистрации, тем самым получали ответ «Что такой номер уже зарегистрирован», код теперь знаем, идем с эти кодом к эндпоинту авторизации, где запросили код и вводим код, тем самым захватываем аккаунт.

Вывод. Более частый случай - привязка Rate Limit к Cookie. Cookie, что в прямом смысле переводится как «печенье», - небольшой фрагмент данных, который отправляется веб-сервером и хранимый на компьютере пользователя.

Пользователь должен уметь пользоваться:

- аутентификации;
- хранением своих персональных;
- отслеживания состояния сеанса доступа;

Разработчики привязывают Rate Limit к Cookie и как мы уже могли понять обход такого лимита - удалить Cookie и перебрать код.

Источники и литература

1) Багров Е. В. Мониторинг и аудит информационной безопасности на предприятии. Вестник волгоградского государственного университета. Волгоград.: 2011, с.54.

2) ГОСТ Р ИСО/МЭК 9594–8-98. Информационная технология. Взаимосвязь открытых систем. Справочник. Часть 8. Основы аутентификации.

3) Никишова А. В., Чурилина А. Е. Программный комплекс обнаружения атак на основе анализа данных реестра// Вестник ВолГУ. Серия 10. Инновационная деятельность. Выпуск 6. 2012 г. В.: Изд-во ВолГУ, 2012, стр. 152–155

4) Мартынова, Л. Е. Исследование и сравнительный анализ методов аутентификации / Л. Е. Мартынова, М. Ю. Умницын, К. Е. Назарова, И. П. Пересыпкин. — Текст:

непосредственный // Молодой ученый. — 2016. — № 19 (123). — С. 90-93. — URL: https://moluch.ru/archive/123/34077/ (дата обращения: 15.11.2022).