МЕТОДЫ И СПОСОБЫ ЗАШИТЫ МОБИЛЬНОГО СЕРВИСА КОРОТКИХ СООБЩЕНИЙ

[1]Нигматов Хикматулла[2]Умаров Улугбек Агзамович
[1]доктор технических наук, профессор Международная Исламская академия Узбекистана, E-mail: khikmatulla@mail.ru
[2]старший преподаватель, ТУИТ имени Махаммада ал-Хоразмий, E-mail: umarov_u.a@inbox.ru

https://doi.org/10.5281/zenodo.7856755

Аннотация. *В этой статье обсуждается важность безопасности в службе коротких сообщений (SMS), которая стала важным аспектом различных отраслей, таких как мобильная коммерция, мобильный банкинг, электронное правительство и повседневное общение. В статье освещаются уязвимости и угрозы безопасности SMS, такие как перехват сообщений, подделка сообщений и изменение содержимого. В статье также представлен обзор двух путей передачи SMS, а именно локального и роумингового, и описаны различные этапы доставки SMS-сообщений.*

Ключевые слова: *мобильные устройства, SMS сообщения, безопасность, шифрование, аутентификация.*

Использование мобильных устройств стремительно возросло в течение многих лет, особенно в последнее десятилетие. Начальная цель этих беспроводных устройств была связана с обменом личной информации. Однако, служба коротких сообщений (SMS) становится ключевой в различных сферах бизнеса, таких как мобильная коммерция, мобильный банкинг, электронном правительстве и повседневное общение. Кроме того, SMS является популярной услугой беспроводной связи по всему миру, так как она позволяет пользователям мгновенно и без труда поддерживать связь с абонентами мобильных телефонов в любой точке мира.

Действительно, безопасность SMS является важной проблемой, которую необходимо решить для обеспечения конфиденциальности и целостности передаваемых данных. Существуют различные уязвимости и угрозы для безопасности SMS, такие как перехват сообщений, подделка сообщений, изменение содержимого сообщений и другие. Поэтому, для того чтобы обеспечить безопасность SMS, необходимо использовать надежные методы шифрования и аутентификации, которые гарантируют конфиденциальность, целостность и подлинность передаваемых данных. Кроме того, важно, чтобы как разработчики мобильных приложений, так и поставщики услуг мобильной связи обеспечивали правильную идентификацию общающихся сторон и обеспечивали конфиденциальность и целостность содержимого SMS во время передачи данных, чтобы избежать угроз безопасности. В целом, улучшение безопасности SMS является важной задачей, которую нужно решить для обеспечения безопасности и защиты конфиденциальности данных.

Первый путь для передачи SMS называется "локальный путь" и используется в случае, когда отправитель и получатель находятся в одной и той же сети связи. В этом случае SMS-сообщение передается напрямую от отправителя к получателю внутри сети связи. На рисунке 1 приведено локальный путь коротких сообщения.

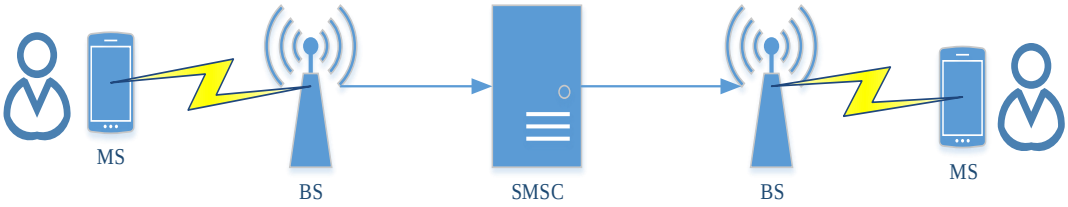

Рис. 1. Локальный путь SMS сообщения

Второй путь для передачи SMS называется "роуминговый путь" и применяется в случае, когда отправитель и получатель находятся в разных сетях связи, например, когда отправитель находится в одной стране, а получатель - в другой. В этом случае SMS-сообщение проходит через несколько сетей связи, прежде чем будет доставлено адресату. На рисунке 2 приведено локальный путь коротких сообщения.

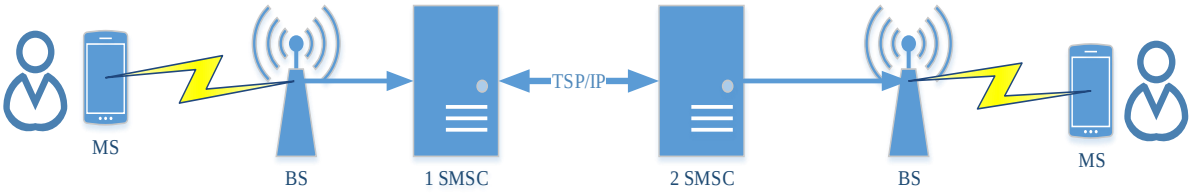

Рис. 2. Роуминговый путь SMS сообщения

Передача SMS-сообщения проходит через несколько этапов, включая регистрацию в сети, отправку запроса на доставку, маршрутизацию, передачу и доставку. Каждый из этих этапов имеет свои протоколы и механизмы для обеспечения надежности и безопасности передачи.

Одной из основных проблем безопасности при передаче SMS является возможность перехвата сообщения третьей стороной. SMS-сообщения могут быть перехвачены на разных этапах передачи, например, во время передачи через сеть связи или во время хранения на мобильном устройстве. Для обеспечения безопасности передачи SMS используются различные методы шифрования и аутентификации, такие как A5/1, A5/2, A5/3 и SHA-1.

Также следует учитывать, что SMS-сообщения могут быть подвержены спаму или фишинговым атакам. Некоторые злоумышленники могут отправлять SMS-сообщения с ложным именем отправителя или содержащие ссылки на вредоносные сайты. Для борьбы со спамом и фишингом существуют различные методы фильтрации, такие как блокирование сообщений от определенных отправителей или использование системы фильтрации на стороне сетевого оператора.

В целом, передача SMS-сообщений включает множество шагов и протоколов, и обеспечение безопасности и надежности этой передачи - сложная задача.

Иногда мы передаем конфиденциальную информацию, такую как пароли, коды доступа, банковские реквизиты и личную информацию через SMS нашим друзьям, членам семьи и поставщикам услуг. Однако, традиционная услуга SMS, предоставляемая различными операторами мобильной связи, не обеспечивает достаточной информационной безопасности сообщений, отправляемых по сети. Для защиты такой конфиденциальной информации крайне необходимо обеспечить сквозную безопасную связь между конечными пользователями. Использование SMS связано с проблемами безопасности, такими как

раскрытие SMS, атака "человек посередине", атака с повторным воспроизведением и атака с имитацией личности. Кроме того, функциональность SMS открыта для атак, которые могут привести к сбою всех голосовых коммуникаций в мегаполисе, и могут уязвимым абонентам на основе SMS, таким как абонентам Android. SMS-сообщения передаются в виде открытого текста между мобильным пользователем (MS) и SMS-центром (SMSC) через беспроводную сеть. Содержание SMS хранится в системах сетевых операторов и может быть прочитано их персоналом.

Небезопасные каналы связи представляют значительные уязвимости для системы безопасности. Поэтому важно, чтобы как мобильные приложения, так и операторы мобильной связи использовали надежные методы защиты для предотвращения таких уязвимостей. Эти методы используются для защиты мобильных абонентов от возможных коммуникационных атак во время передачи SMS. Они могут быть реализованы на уровне сети (транспортный уровень) или на уровне приложений (мобильные приложения). В данном случи рассмотрены и описаны механизмы безопасности, применяемые для защиты передачи SMS, а также будет произведен анализ этих механизмов в соответствии с требованиями безопасности в сравнении с возможностями мобильной связи. Кроме того, будет описано, как можно использовать эти механизмы для предотвращения проблем с безопасностью.

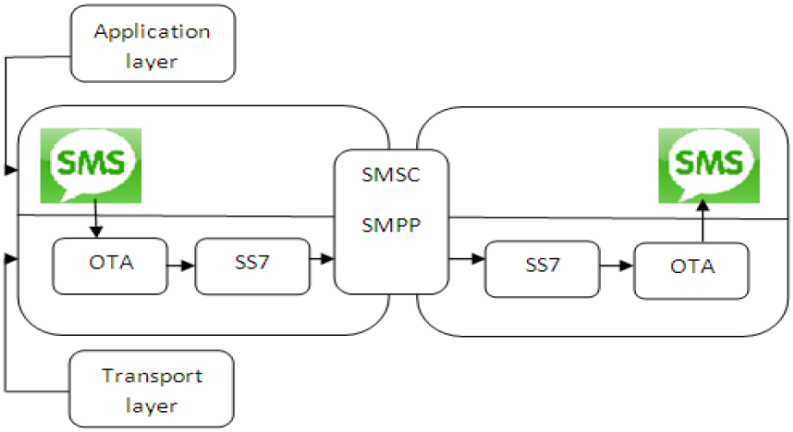

Рис. 3. Слои передачи SMS сообщения

Содержание SMS передается через различные протоколы и интерфейсы, но несмотря на принимаемые меры безопасности, сеть GSM страдает от ограничений безопасности, что приводит к небезопасной сквозной передаче SMS. Из-за отсутствия достаточной защиты транспортного пути передачи SMS (от отправителя до получателя), нет доказательств его безопасности. Анализ транспортного пути сообщения выявил несколько проблем безопасности SMS на различных этапах (компонентах GSM), которые могут негативно сказаться на безопасности SMS-сообщений на транспортном уровне. Кроме того, криптографически незащищенные сообщения уязвимы на всех узлах транспортного уровня.

Прикладная база в данном контексте относится к проектированию и разработке мобильного приложения, которое обеспечивает безопасность передачи SMS-контента. Один из способов защиты конфиденциальности SMS состоит в шифровании сообщения на отправителе и последующей расшифровке на приемнике, что обеспечивает сквозную безопасную передачу сообщения. В случае необходимости защиты коммуникационной

среды, возникает потребность в разработке механизмов безопасности, включающих целостность, конфиденциальность, аутентификацию и недоказуемость, для служб SMS. Это дает возможность разработчикам проектировать и разрабатывать механизмы безопасности в мобильных устройствах, которые могут снять с оператора мобильной связи ответственность за безопасность передачи SMS-контента.

Защита информации в процессе передачи является критически важным аспектом разработки программного обеспечения на рынке SMS. Исследования показывают, что мобильные приложения становятся все более ценными и содержат конфиденциальную информацию, что повышает риски связанные с безопасностью. В связи с этим, существует неотложная потребность в защите электронной передачи данных, и разработка приложений безопасности на рынке SMS является критически важной задачей для разработчиков программного обеспечения. Преимущество заключается в том, что эти методы применения не зависят от сферы деятельности оператора мобильной связи и могут существенно снизить издержки безопасности.

В заключении можно сказать, что безопасность передачи SMS-сообщений является важной задачей для обеспечения конфиденциальности и защиты информации. Небезопасные каналы связи могут привести к возможным коммуникационным атакам и уязвимостям в системе безопасности. Поэтому, как мобильные приложения, так и операторы мобильной связи должны использовать надежные методы защиты для предотвращения таких уязвимостей.

Для защиты конфиденциальности SMS-контента, могут быть применены методы шифрования на отправителе и расшифровки на приемнике, обеспечивающие безопасную передачу сообщения. Кроме того, разработка механизмов безопасности, включающих целостность, конфиденциальность, аутентификацию и недоказуемость, для служб SMS, может снять с оператора мобильной связи ответственность за безопасность передачи SMS-контента.

Мобильные приложения становятся все более ценными и содержат конфиденциальную информацию, поэтому существует неотложная потребность в защите электронной передачи данных и разработке приложений безопасности на рынке SMS. Применение этих методов может снизить издержки безопасности и обеспечить более безопасную передачу SMS-сообщений.

REFERENCES

1. Nigmatov X., Umarov U.A. Exchange of messages in the telecommunication network with different types of communication channels. 2021 International Conference on Information Science and Communications Technologies (ICISCT) 4-5 November 2021. DOI:10.1109/ICISCT52966.2021.9670173
2. Nigmatov X., Umarov U.A. Analytical simulation methods determining the basic characteristics of a telecommunication network with different communication channels and a changing structure. Bulletin of TUIT Bulletin of TUIT: Management and Communication Technologies is science-technical journal DOI:10.51348/tuitmct433.
3. Нигматов Х., Умаров У.А. «Определение основных характеристик телекоммуникационной сети с разнотипными каналами связи и изменяющееся

структурой». Муҳаммад ал-Хоразмий авлодлари илмий-амалий ва ахборот-таҳлилий журнали 2(12)/2020.

4. Nigmatov X., Umarov U.A. “Zamonaviy axborot-kommunikatsiya texnologiyalarining aloqa kanallarida axborotlarni himoyalash”. Monografiya. “Innovatsion rivojlanish nashriyot-matbaa uyi”. Toshkent sh. 2020.
5. A. Medani, A. Gani, O. Zakaria, A. A. Zaidan, B. B. Zaidan. Review of mobile short message service security issues and techniques towards the solution. Scientific Research and Essays Vol. 6(6), pp. 1147-1165, 18 March, 2011. DOI: 10.5897/SRE11.107
6. Sharma, S. K., & Sharma, S. (2020). Information security in mobile communication networks. International Journal of Computer Applications, 180(45), 15-18.
7. Adhikari, N., & Chauhan, N. (2019). Secure communication in mobile networks: A survey. Journal of King Saud University-Computer and Information Sciences, 31(4), 540-551.
8. Wang, H., Zhang, Y., Wang, F., & Liu, C. (2019). A secure data transmission scheme based on chaotic map and ciphertext-policy attribute-based encryption in mobile networks. Wireless Personal Communications, 106(3), 1233-1252.
9. Wang, W., Wang, Y., & Zhang, Y. (2019). A novel secure and efficient authentication scheme based on elliptic curve cryptography for mobile networks. International Journal of Network Security, 21(1), 1-10.
10. Chen, W., Huang, J., & Guan, X. (2020). A novel secure authentication scheme for mobile networks based on biometrics and blockchain. International Journal of Communication Systems, 33(9), e4322.
11. Abdallah, S., Moubayed, N., & Issa, Y. (2020). Enhancing security in mobile communication networks through biometric authentication and elliptic curve cryptography. Future Generation Computer Systems, 107, 977-987.