УДК 004.056.5

ПОСТРОЕНИЕ МОДЕЛИ НАРУШИТЕЛЯ В СИСТЕМЕ МОБИЛЬНОЙ СВЯЗИ

Е. М. Галка

Донской государственный технический университет, Ростов-на-Дону, Российская Федерация
galka.skakalka94@gmail.com

Повсеместное использование мобильных систем связи, разнообразных по используемым информационным технологиям, принципам организации и способам физического представления информации, а также применение множества сервисов мобильных приложений обуславливают сложность обеспечения в них защиты персональных данных пользователей. Для решения этой актуальной задачи автором было проведено построение модели нарушителя в системе мобильной связи. Сформированная модель нарушителя позволяет более узко классифицировать злоумышленника в рассматриваемой системе в соответствии с уровнем его воздействия.

Ключевые слова: система мобильной связи, персональные данные, мобильное приложение.

УДК 004.056.5

DEVELOPMENT OF THE ATTACKER MODEL IN MOBILE COMMUNICATION SYSTEM

E. M. Galka

Don State Technical University, Rostov-on-Don, Russian Federation
galka.skakalka94@gmail.com

The widespread use of mobile communications systems which differs in the used information technology, principles of organization and methods of physical information presentation as well as the use of multiple services for mobile applications are the reasons why there exists the difficulty in providing users' personal data protection. To address this challenge the author has carried out the construction of the model of the attacker in the mobile communication system. The proposed model of the attacker allows us to better classify an attacker in the system in accordance with the level of its impact

Keywords: mobile communication system, personal data, mobile application.

Введение. В настоящее время среди современных информационных телекоммуникационных систем особое место занимают мобильные системы связи (МСС), предназначенные для обеспечения пользователя связью, предоставления ему доступа к различным информационным ресурсам, осуществления передачи данных и речевой информации.

Повсеместное применение МСС, разнообразных по используемым информационным технологиям, принципам организации и способам физического представления информации, обуславливает сложность обеспечения в них конфиденциальности данных. Особое внимание заслуживает использование клиентами множества популярных сервисов мобильных приложений, позволяющих пользователю осуществлять банковские переводы, пополнение счетов мобильной связи, синхронизацию фотографий с мобильных устройств на облачное хранилище, реализовать режим онлайн с другими пользователями через сеть Интернет, предоставляя тем самым собственные геоданные, и многое другое. Принимая на этапе авторизации соглашение о доступе мобильных приложений ко всем личным данным, пользователь предоставляет данным сервисам доступ к своим персональным данным, подвергая их риску хищения сторонним лицом (нарушителем).

Для определения и организации системы защиты МСС первоочередной задачей является определение видов защищаемой информации, возможных каналов её утечки, а также формирова-

ние обобщенной модели вероятного нарушителя, позволяющей оценить возможности, мотивы, каналы и средства проведения атаки.

На сегодняшний день в научно-технической литературе и в нормативно-методических документах отсутствует единый подход к построению модели нарушителя. В общем случае модель нарушителя носит неформальный характер и может быть представлена как описание потенциальных возможностей и действий злоумышленника.

Одним из наиболее полных подходов к построению моделей нарушителей является описанная типовая модель нарушителя, предложенная в работе [1]. В данной работе предлагается рассматривать такие классификационные признаки нарушителя, как место его воздействия, цели и мотивы действий, каналы и средства для проведения атак и т. д. Предложенный в работе [1] подход является наиболее целесообразным при построении моделей нарушителя для широкого спектра автоматизированных систем и, в частности, может быть применим к системам мобильной связи.

В МСС существует множество различных каналов утечки информации, что обусловлено разнообразием способов ее физического представления [2–3]. Перехват данных, передаваемых по каналам связи, может осуществляться как беспроводным путем, по линиям, использующим излучающие средства радиосвязи, так и по проводным линиям связи.

При оценке возможностей нарушителя необходимо исходить из его максимально допустимых возможностей. В техническом плане предполагается, что нарушитель обладает любыми аппаратными и программными средствами для осуществления несанкционированного доступа (НСД) к защищаемой информации. Оперативно-тактические возможности нарушителя определяются источниками угроз для конкретной МСС, при отсутствии данных о которых предполагается, что нарушитель обладает потенциально достижимыми возможностями для атаки. Аналитические возможности нарушителя предполагают наличие у него специальных знаний в области техники и алгоритмов обработки сигналов, позволяющих осуществлять перехват и восстановление информации по техническим каналам.

При построении модели информационной безопасности автоматизированных систем выделяют непреднамеренные действия нарушителя, отражающие ошибки персонала или характеризуемые недостаточной надежностью системы, и преднамеренные действия нарушителя, подразделяющиеся на активные, пассивные и не преследующие целей [4]. Поскольку в аспекте МСС под нарушителем понимается стороннее лицо, осуществляющее несанкционированный доступ к информации, то в формировании модели вероятного нарушителя его действия рассматриваются как преднамеренные, предназначенные для хищения персональных данных пользователя с применением дополнительных программно-аппаратных средств.

К основным каналам проведения атаки нарушителем относят технические каналы и каналы НСД [2]. При построении модели нарушителя в МСС необходимо комплексно учитывать оба канала проведения атаки. По техническим каналам нарушитель может получить информацию об учетных данных пользователя, и удаленно зайти в приложение, пройдя процедуру идентификации, а через канал НСД спровоцировать пользователя к предоставлению дополнительной информации под видом запроса данных со стороны приложения [5].

Среди средств проведения атак [2] выделяют:

- применение пассивных технических средств;
- применение активных технических средств;
- применение штатных средств и использование недостатков системы защиты для ее обхода.

Для рассматриваемой предметной области модель нарушителя предполагает применение всех вышеприведенных средств атак, с целью получения частичной или полной информации о персональных данных пользователя.

Наличие доступа для нарушителя существенным образом зависит от его функциональных обязанностей в отношении разработки рассматриваемого приложения. Согласно федеральным нормативным актам, имеется шесть категорий потенциальных злоумышленников. Исходя из предположения, что потенциальные нарушители обладают всей информацией, необходимой для проведения атаки, за исключением информации, доступ к которой исключается системой защиты информации, а также учитывая масштаб и широту использования мобильных приложений, можно исключить вероятность того, что потенциальный нарушитель будет относиться к персоналу, обслуживающему приложение. Более вероятно, что таковым будет являться зарегистрированный пользователь, осуществляющий удаленный доступ по распределенным каналам передачи данных.

Следовательно, потенциальный злоумышленник в модели нарушителя в МСС в соответствии с его функциональными обязанностями будет относиться к третьей категории, к которой относятся зарегистрированные пользователи, осуществляющие удаленный доступ по локальным каналам передачи данных.

За счет разнообразия штатных средств, с использованием которых возможен НСД, необходимо классифицировать уровень НСД к защищаемой информации. Классификация уровней НСД [1] может быть представлена в виде уровней стека протоколов *TCP/IP* или в виде иных моделей, отражающих сетевые принципы правил обмена данными между субъектами, а также в виде уровней с применением криптографических и некриптографических средств защиты информации.

Согласно [1], уровни воздействия нарушителей и категорий нарушителей могут быть связаны между собой через наличие угроз информационной безопасности, которые могут быть осуществлены нарушителем на определенном уровне воздействия. При этом уровни воздействия нарушителей в автоматизированной системе могут быть определены как: уровень закладных устройств; уровень системы защиты информации с применением криптографических средств; уровень системы защиты информации с применением некриптографических средств; уровень технических каналов; прикладной уровень стека протоколов *TCP/IP*; транспортный уровень стека протоколов *TCP/IP*; сетевой уровень стека протоколов *TCP/IP*; канальный уровень стека протоколов *TCP/IP*; физический уровень стека протоколов *TCP/IP*; уровень вредоносного воздействия.

По результатам анализа предметной области можно сделать вывод, что наибольшими возможностями к НСД, подразумевающими наличие угроз на всех уровнях воздействия, обладают штатные сотрудники, к которым могут быть отнесены: пользователи с полномочиями администратора информационной безопасности; разработчики прикладного программного обеспечения и технических средств; лица, обеспечивающие их поставку и сопровождение и т. д. Однако, исключив вероятность злоумышленных действий со стороны штатных сотрудников организации, в силу их профессиональной компетенции и осведомленностью об уголовной ответственности и, как следствие, меньшей вероятностью сговора с нарушителем, в соответствии с ранее определенной третьей категорией злоумышленника, к потенциальным нарушителям в МСС могут быть отнесены пользователи, не имеющие отношение к персоналу, обслуживающему приложение, но обладающие возможностями и программно-аппаратными средствами для НСД по локальным и (или) распределенным каналам передачи данных. Такие пользователи могут воздействовать на физический, канальный, сетевой, транспортный и прикладной уровни стека протоколов *TCP/IP*, на уровни вредоносного воздействия и закладных устройств с целью хищения информации.

Заключение. В результате проведенных аналитических исследований сформирована модель нарушителя для мобильных приложений и сервисов массового использования. Учет особенностей данной модели позволяет в дальнейшем выполнить построение системы защиты для персональных данных пользователя. В связи с масштабностью использования мобильных сервисов, в дальнейшем представляется целесообразным проектирование системы или мобильного приложения с применением технологий искусственного интеллекта, способного определить степень угрозы для пользователя, устанавливающего на свое мобильное устройство какое-либо приложение.

Библиографический список

1. Стефаров, А. П. Формирование типовой модели нарушителя правил разграничения доступа в автоматизированных системах / А. П. Стефаров, В. Г. Жуков // Известия ЮФУ. Технические науки. — 2012. — № 12 (137), Т. 137. — С. 45–54.

2. Базовая модель угроз безопасности персональных данных при их обработке в информационных системах персональных данных : [утв. Федеральной службой по техническому и экспортному контролю 15.02.2008 г.] – 2008. — 69 с.

3. Меры защиты информации в государственных информационных системах [Электронный ресурс] — Режим доступа: http://fstec.ru/component/attachments/download/675 (дата обращения: 08.05.2016).

4. Концепция защиты средств вычислительной техники и автоматизированных систем от несанкционированного доступа к информации : [руководящий документ: утв. решением гос. техн. комиссии при президенте Рос. Федерации от 30 марта 1992 г.] — Москва : ГТК РФ, 1992. — 12 с.

5. Чекалин, А. А. Защита информации в системах мобильной связи / А. А. Чекалин, А. В. Заряев, С. В. Скрыль, В. А. Вохминцев. — Москва : Горячая линия — Телеком, 2005. — 171 с.