УДК 621.391

СРАВНИТЕЛЬНЫЙ АНАЛИЗ УГРОЗБЕЗОПАСНОСТИ СЕТЯMUMTS

Пудалев Т.О.,Феоктистов Д.С.

Научный руководитель: ***Черников Дмитрий Юрьевич***

Институт инженерной физики и радиоэлектроники СФУ

Россия, Красноярск

В данной статье рассматриваются основные аспекты безопасности на уровне системы и сети UMTS. Приведены самые общие способы атак на безопасность, а также перечислены возможные способы защиты от них.

Ключевые слова: мобильные сети, UMTS, безопасность, потенциальная угроза, DoS-атака.

This article discusses the main aspects of security at the system level and network UMTS. There are the most common methods of attacks on security, and lists of possible ways to protect against them.

Keywords: mobile network, UMTS, security, potential threat, DoS-attack.

Развитие мобильных сетей всегда было тесно связано с вопросами безопасности в силу самого характера радиосвязи, которая легко доступна не только пользователям мобильных телефонов, но и потенциальным перехватчикам. Однако безопасность– это более широкое понятие, при рассмотрении которого нужно учитывать всех игроков рынка мобильной связи. В данной статье мы рассмотрим безопасность как с точки зрения услуг для конечного пользователя.

В глобальной системе мобильной связи GSMаспекты безопасности со-средоточены на защите радиоканала. В сетях универсальной мобильной телекоммуникационной системы UMTSбезопасность представляет более широкое понятие. Естественно, соединения в сети доступа должны быть

защищены, но кроме того, безопасность должна учитывать и многие другие аспекты. Различные сценарии предоставления услуг на рынке связи приводят к тому, что иногда даже конфиденциальная информация передается между разными пользователями и сетями. Очевидно, что в такой ситуации существуют очень серьезные риски. Кроме того, местные и международные органы власти издают директивы по этому вопросу. Система UMTS интегрирует связь и передачу данных, а это, в свою очередь, создает угрозу безопасности. Безопасность в среде протокола IP была предметом обсуждения в течение многих лет, и за эти годы были идентифицированы многочисленные угрозы безопасности и разработаны механизмы защиты.

Кратко рассмотрим потенциальные угрозы безопасности на сетевом уровне и защиту от них. Цель состоит в том, чтобы обеспечить конфиденциальность и защиту целостности связи между различными сетевыми элементами. Эти элементы могут принадлежать либо одной и той же сети, либо двум различным сетям. В последнем случае для обеспечения возможности взаимодействия требуются полностью стандартизованные решения в области защиты.

В цепочке услуг 3Gучаствуют четыре стороны: «абонент», «поставщик сетевых ресурсов», «поставщик услуг» и «поставщик информации» (рис. 1).

Рисунок 1 – Угроза безопасности в цепочке услуг

При рассмотрении услуги, которую использует и оплачивает абонент, мы видим, что здесь участвует каждая часть данной цепочки: поставщик сетевых ресурсов обеспечивает платформу, на которой устанавливается соединение. Поставщик услуг работает с USIM, уточняет идентифицирующую информацию и предоставляет саму услугу; а поставщик информации отвечает за информацию, которую обычно требует услуга. Физически поставщиком сетевых ресурсов, услуг и информации может быть одна и та же компания, но на самом деле это необязательно так. На практике в среде GSMсуществуют все виды комбинаций этих трех сторон. Ясно, что абонент платит за услугу и использует ее, в то время как другие стороны цепочки услуг делят доходы. Система, контролирующая денежные потоки между поставщиками сетевых ресурсов, услуг и информации, представляет потенциальную угрозу безопасности, поскольку между этими участниками передается конфиденциальная информация.

Многие угрозы для связи между сетевыми элементами UMTSаналогичны тем, которые имеют место на прикладном уровне. Ясно, что между приложениями уже существуют большие различия, но примеры атак, представленные ниже, должны учитываться во всех случаях.

Существует множество способов совершать атаки, которые могут быть предотвращены только изобретательностью и эффективной защитой. Ниже представлен перечень некоторых примеров:

- социотехника;
- пассивное прослушивание;
- спуфинг;
- перехват сеанса связи;
- DoS-атака.

Социотехника обычно не рассматривается пользователем как угроза безопасности, хотя она играет основную роль во многих атаках. Если говорить об абонентах, социотехника может означать способы получения доступа к их терминалам с помощьюPIN-кода. Абоненты могут защитить себя от социотехники, поддерживая активность запроса PIN-кода в терминале и запоминая свои номера PIN-кодов. На удивление социотехника распространена и на стороне сети. Нередко люди, работающие с сетевыми элементами на операторских станциях, принимают странные вызовы, когда говорящий объясняет, что ему нужен идентификатор пользователя и пароль к определенному оборудованию, а человек, ответственный за это оборудование находится в отпуске или по каким-то причинам недоступен. Часто эти вызовы не что иное, как социотехника, когда конфиденциальная информация может попасть в чужие руки. Фактически хакеры обычно делают такую попытку как первый шаг. В результате социотехника может использоваться, чтобы дать хакеру доступ как к жизненно важным, так и к не столь важным элементам сети. В среде IPсоциотехника представляет относительно распространенное явление, но в области связи она используется не так часто; оборудование не является предметом общественного доступа и персонал, который его обслуживает, очень хорошо знает свои обязанности.

Пассивное прослушивание – это еще один распространенный метод атаки, его очень трудно обнаружить и физически предотвратить. С помощью

пассивного прослушивания хакер стремится собрать идентификаторы пользователейи информацию о паролях. К сожалению, программы пассивного прослушиванияшироко доступны для всех в Интернете. Сама по себе программа пассивного прослушивания – это только инструмент, и в хороших руках она используется для мониторинга и определения возможных отказов. В чужих руках это мощное средство, позволяющее хакеру незаметно отслеживать большое количество соединений в Интернете.

Информация, собранная с помощью пассивного прослушивания, может использоваться на следующем этапе: речь идет о методе неавторизованного доступа, который называется спуфинг. Спуфинг позволяет хакеру использовать чужой IP-адрес и принимать пакеты от других пользователей. Другими словами, хакер занимает в соединении место правильного приемника. Вооруженный этой информацией, хакер может свободно использовать чей-то IP-адрес. К счастью, это более сложно. Однако прием «одностороннего трафика» часто и есть все, что нужно хакеру. Сегодня, когда люди проводят очень много времени, работая дистанционно на дому, это может быть одним из способов получения доступа к информации компании.

Следующий шаг, который может предпринять хакер, называется «перехватом сеанса связи», когда он делает попытки перехватить существующее соединение. Как уже упоминалось ранее, даже сильный механизм аутентификации в начале соединения не гарантирует того, что оно не будет перехвачено позднее. Необходима защита целостности для всего сеанса связи.

При атаке DoSхакер стремится не собрать информацию, а скорее причинить вред и неудобство другим пользователям и поставщикам услуг. При обычной атаке DoSхакер генерирует «разрушающий» трафик, который в худшем случае загромождает сервер назначения так, что он больше не может выполнять свои функции. Здесь идея в том, чтобы блокировать очередь запросов с требованием услуг сервера, а затем игнорировать все подтверждения, которые посылает сервер. Следовательно, сервер расходует

свои ресурсы на установление входящего соединения, которое никогда не устанавливается. Когда время соединения иссякает, ресурсы освобождаются для обслуживания другого соединения. Когда буфер, содержащий запросы на соединения, непрерывно заполняется новыми запросами, сервер загромождается этими запросами и, следовательно, не может предоставлять «реальное» обслуживание.

К сожалению, существуют и более изощренные атаки DoSи, что поразительно, в Интернете имеется множество инструментов, которые может использовать хакер для атаки DoS. В общем, обеспечить защиту от DoSочень трудно. На рисунке 2 представлена статистика DoS-атак за последнее десятилетие.

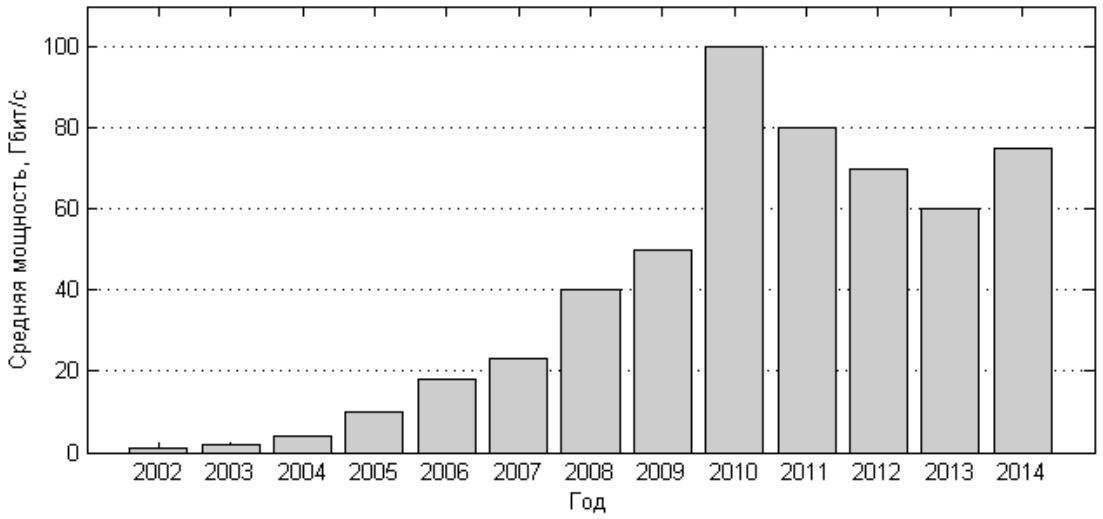

Рисунок 2 – Изменение мощности DoS-атак в периоде с 2002 по 2014 года

Современная атака DoSможет быть объединена с другими методами, описанными выше. Например,DoSможет инициироваться с «украденных»IP-адресов и, если она используется в режиме распространения, в атаке DoSмогут принимать участие сотни компьютеров. DoS— это очень опасная и мощная атака, которая может легко привести к серьезным финансовым потерям.

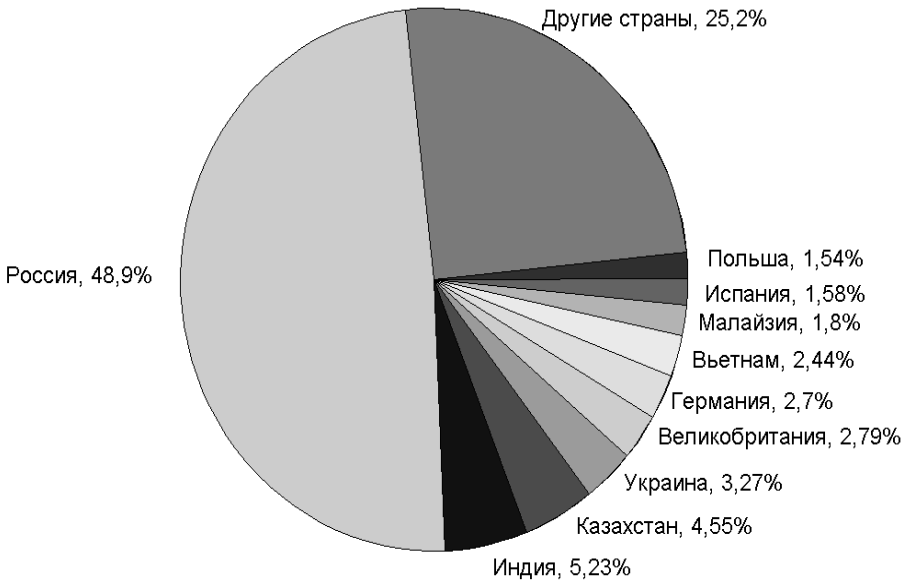

Рисунок 3 – Диаграмма географии DoS-атак за 2013 год

Основное средство защиты трафика в сетевом домене представляет набор протоколов IP-безопасности IPSec. Взаимодействующие стороны могут аутентифицировать друг друга с помощью IPSec. Серьезную проблему представляет управление ключами: как генерировать, передавать и распределять различные ключи, необходимые в алгоритмах, которые используются для обеспечения конфиденциальности и защиты целостности.

В дополнение к защите сетей, построенных на базе IP, в системе UMTSверсии 4 расширены возможности защиты сетей, работающих только на базе SS7. В частности, для протокола мобильных приложений MAP был разработан специальный механизм защиты. Он называется MAPSeci обеспечивает конфиденциальность и защиту целостности.

В заключение хотелось бы отметить, что в статье приведены лишь самые общие способы атак на безопасность, которые могут произойти.Все эти угрозы нельзя игнорировать, поскольку средства их реализации могут быть легко найденыв Интернете совершенно бесплатно. Ключевой слабостьюархитектуры безопасности сетей UMTSявляется отсутствие шифрования данных при аутентификации.В действительности безопасность должнарассматриваться как цепь, в которой вся система: безопасность связи, безопасность данных и

безопасность сигнализации – имеет такую же прочность, как ее самое слабое звено. Другими словами, все должно быть защищено, включая алгоритмы, протоколы, каналы, сквозные тракты, приложения и т. д.

Согласно приведенной статистике, для нашей страны данный вопрос стоит особенно остро, поэтому исследование и разработка новых алгоритмов и методов защиты систем и сетей передачи как никогда актуально.

Библиографический список

1 Гельгор А.Л. Сотовые сети мобильной связи стандарта UMTS: учеб. пособие / Гельгор А.Л., Попов Е.А. –СПб.: Изд-во Политехн. ун-та, 2010. – 227 с.

2NiemiV., NybergK. UMTSSecurity. Chichester, UK: John Wiley & Sons, 2003, – 273 pp.

3Hillebrand F. GSM and UMTS: The creation of global mobile communication. Chichester, UK: John Wiley & Sons, 2002, –580 pp.