УДК 004.056

Обеспечение информационной безопасности 4G-сетей

А.И. Сухотерин, к.в.н., доцент,
К.А. Руденко, студент 4 курса кафедры Информационная безопасность,
О.В. Якушев, студент 4 курса кафедры Информационная безопасность,
Государственное бюджетное образовательное учреждение
высшего образования Московской области
«Технологический университет», г. Королев, Московская область

Мобильные операторы активно рекламируют и распространяют дешёвую и быструю 4G-связь, однако о её защищённости известно мало. Раньше считалось, что переход на сети 4G повышает устойчивость телефона к атакам. Каждое поколение мобильной связи предполагало повышение безопасности. В 4G сетях, например, безопасность была усилена за счёт аутентификации и защиты ряда сигнатурных протоколов. На основе анализа материалов по исследованиям защищённости 4G-сетей в данной работе были выделены основные угрозы и предложения по их устранению.

Мобильные системы связи, мобильные сети, мобильные услуги, LTE, информационная безопасность.

Ensuring information security 4G-networks

A.I. Sukhoterin, Associate Professor candidate of military Sciences,
K.A. Rudenko, 4rd year students, Department of information security,
O.V. Yakushev, 4rd year students, Department of information security,
State Educational Institution of Higher Education
Moscow Region «University of technology», Korolev, Moscow region

Mobile operators are actively advertise and distribute cheap and fast 4G-communication, but on the security of its little known. Previously it was thought that the transition to 4G network increases the stability of the phone to the attacks. Each generation mobile communications expected to increase security. In 4G networks, for example, security has been strengthened at the expense of a number of authentication and security protocols signature. Based on the analysis of research materials security of 4G-networks in this study were identified the main threats and suggested remedies.

Mobile communication systems, mobile networks, mobile services, LTE, information security.

Оказывается, что LTE-сети выдают информацию о местоположении устройства, хотя даже во времена 2G приватность пользователя была в приоритете. Когда устройство подключается к сети, ему присваивается временный идентификатор (TMSI – Temporary Mobile Subscriber Identity). При обмене сигналами между сетью и устройством учитывается только TMSI, а не IMSI

(International Mobile Subscriber Identity) или телефонный номер абонента. Таким образом, потенциальному атакующему будет труднее отследить конкретного пользователя, так как TMSI постоянно меняется при переподключении телефона к новой базовой станции [2].

Несколько лет назад корейские исследователи смогли отследить пользователя в сети 2G путем запросов page request – отправления пустых сообщений или совершения коротких звонков на номер абонента, но такая атака была маловероятна в реальных условиях [1].

Теперь же исследователи обнаружили подобный метод отсылки запросов через мессенджеры соц. сетей. Например, если пользователь Facebook вне списка друзей конкретного человека посылает ему сообщение, Facebook помещает сообщение в папку «Другие», дабы защитить пользователя от спама. Если на LTE-смартфоне установлен мессенджер Facebook, то потенциальный злоумышленник имеет возможность связать идентификатор TMSI с профилем в соц. сети через запрос page request.

Несмотря на «временную» природу идентификатора, TSMI меняется не так часто – например, в городах с большой плотностью населения идентификатор оставался неизменным до трех дней, и для многих хакеров этого будет более чем достаточно, особенно если они используют «подставные» БС.

Протоколы доступа в сетях LTE используют некоторые алгоритмы отчетности, абсолютно необходимые для функционирования LTE, – например, для обеспечения устранения неисправностей при подключении к сети и переподключении абонента между сетями. Если атакующий получит доступ к одному из таких отчетов, которыми устройство обменивается с сетью, то потенциально сможет выявить местоположение смартфона – в некоторых случаях с точностью GPS-координат.

Также, эксперты обнаружили возможность проведения DDoS-атак по LTE. Например, в ситуации, когда абонент находится в роуминговой зоне, а тарифный план не позволяет пользоваться услугами в роуминге, при попытке подключения к сети смартфон получит сообщение вроде «ROAMING NOT ALLOWED». После этого следующий запрос к сети произойдет при перезагрузке устройства. Этот механизм разработан для того, чтобы сократить количество обращений к сети и сэкономить расход батареи. Таким образом, данная особенность LTE позволяет атакующему обеспечить «отказ в обслуживании» при подключении к 3G или 4G, вынудив устройство подключиться к менее защищенным сетям 2G, открытым для уже известных атак [2,7,8,9,10,11].

Оборудование, необходимое для осуществления этих атак, состоит из платы USRP и нескольких антенн, снабженных открытым ПО openLTE. Весь пакет обойдется хакеру всего в тысячу евро.

Для устранения выявленных уязвимостей необходим пересмотр сигнатурных протоколов, а также программируемых сетей (SDN). Ряд производителей уже разрабатывают патчи, а также изменения существующих спецификаций LTE (4G-сетей) [5].

Цифровая мобильная связь стандарта GSM используется сейчас во многих критических инфраструктурах, включая промышленные системы управления (SCADA). Другой пример из повседневной жизни, с которым никому не хотелось бы встретиться – это кража денег с банковских счетов. Многие наверняка видели

такие маленькие антенны у банкоматов (рис. 1) – здесь тоже GSM [1].

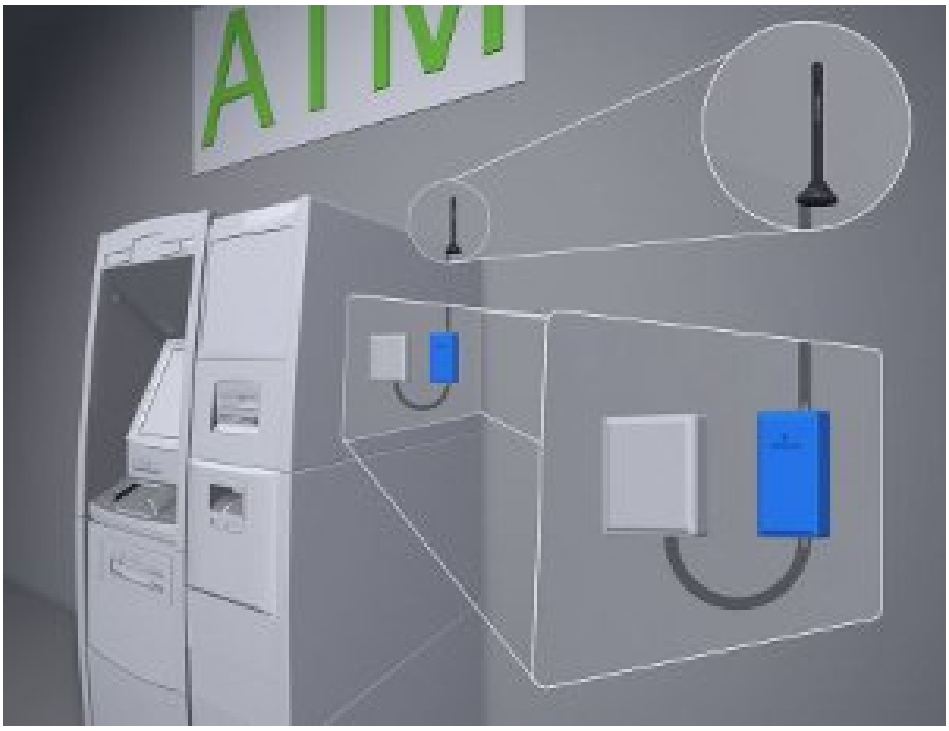

Рисунок 1 – Банковский автомат

Современный модем для беспроводной связи – это компьютер, на который установлена известная операционная система (обычно Linux или Android) и ряд специальных приложений с достаточно широким и возможностями. В этом программном обеспечении и протоколах передачи данных есть уязвимости, которые уже эксплуатировались в последние годы – например, чтобы разлочить модем и отвязать от оператора. Одним из средств защиты от таких взломов стал перенос многих сервисов на Web – однако это дало лишь новые возможности для атак [2].

Для идентификации оборудования нам необходимы документация и поисковая система. В некоторых случаях Google помогает даже больше – можно сразу найти пароль для telnet-доступа (рис. 2).

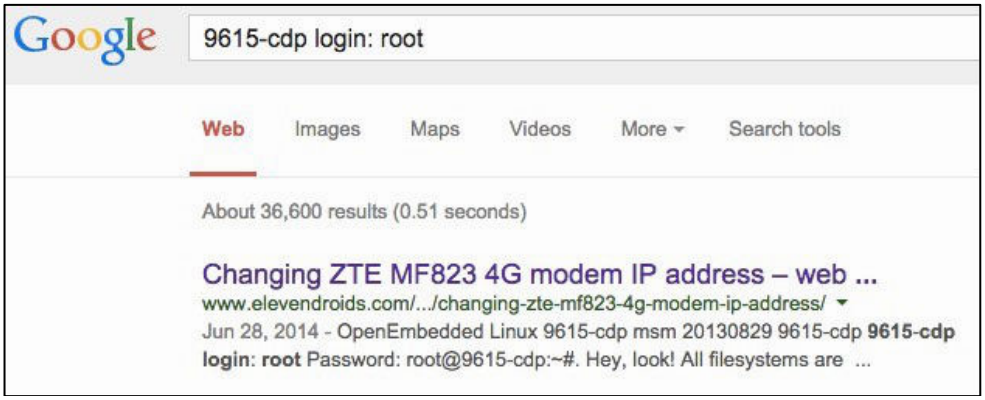

Рисунок 2 – Поиск информации

Однако для внешних коммуникаций нам нужен не telnet, а http. Подключаем модем к компьютеру и изучаем его, как отдельный сетевой узел с веб-приложениями. Находим возможность атаки через браузер (CSRF, XSS, RCE). Таким способом заставляем модем рассказать о себе разные полезные данные (рис. 3) и (рис. 4) [4].

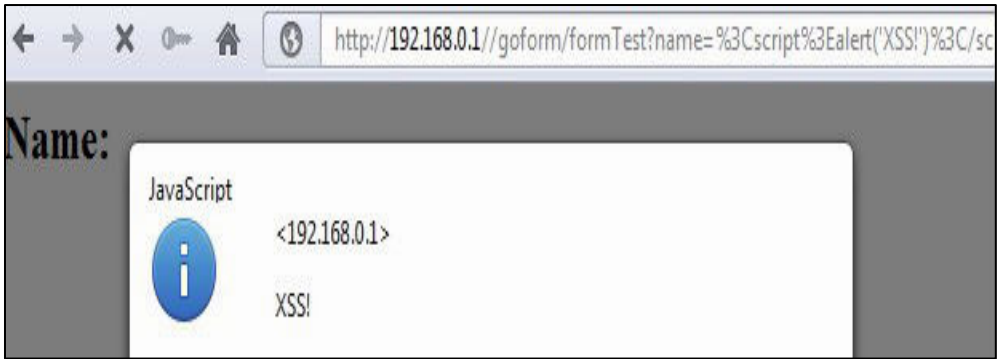

Рисунок 3 – Полученные данные

Помимо раскрытия данных, на атакованном модеме можно выделить следующие уязвимости:

- Смена настойки DNS (что позволяет перехватывать трафик);
- Смена настройки SMS-центра (перехват SMS или манипулирование ими);
- Смена пароля на портале самообслуживания через SMS (что позволяет увести деньги со счета, подписавшись на сторонний сервис);
- Блокировка модема путём набора неверных PIN- и PUK-кодов;
- Удаленно «обновить» прошивку модема.

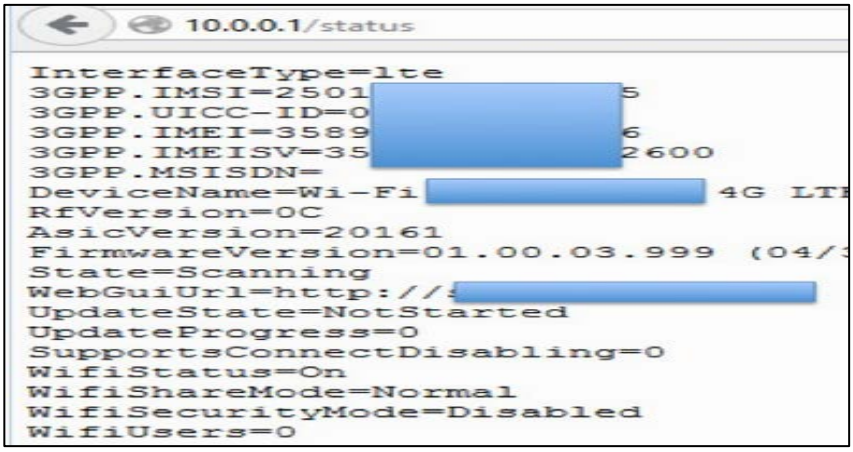

Рисунок 4 – Данные оборудования

Можно развить атаку и дальше – добраться до компьютера, к которому подключён USB-модем. Один из вариантов такой атаки: на захваченный модем устанавливается драйвер USB-клавиатуры, после чего компьютер воспринимает модем как устройство ввода. С этой «мнимой клавиатуры» на компьютер передаётся команда перезагрузки с внешнего диска, роль которого играет всё тот же модем. Таким образом, на «материнский» компьютер можно установить bootkit, позволяющий дистанционно управлять компьютером.

Лучшее, что может сделать пользователь для защиты от подобных атак – не засовывать что попало в свои USB-порты. Понимая при этом, что к выражению «что попало» относятся даже USB-модемы, которые снаружи кажутся всего лишь маленьким и безобидным устройством связи.

Разработчики мобильной технологии LTE все же позаботились о ее защите несколько больше, чем разработчики Интернета. Поэтому можно надеяться, что мобильная сеть будет более надежна и безопасна, чем Всемирная сеть. В LTE используется почти такая же модель безопасности, как и в ранних версиях мобильной связи. Хотя архитектура сети несколько изменилась, общие принципы защиты остались прежними. Если в предыдущих версиях мобильной сети за безопасность отвечал RNC, то теперь его нет, а защита возложена на базовые станции, которые стали более интеллектуальными. Как сообщил Дмитрий Костров, главный эксперт МТС, все функции защиты в LTE объединены стандартом и подразумевают защиту на нескольких уровнях. Предусмотрена защита на уровне доступа к сети, на уровнях сетевого и пользовательского доменов, на уровне приложений и уровне отображения и конфигураций [3].

Каждый из этих уровней предполагает аутентификацию и авторизацию всех устройств, чего нет в Интернете. Хотя каждое устройство в IP-сети имеет свой адрес, а часто еще и уникальный идентификатор MAC, его достаточно легко изменить и подделать. Однако технология LTE предусматривает использование не только IP-адреса, но и системы распространения ключей шифрования для всех устройств, подключенных к сети. В результате для всех взаимодействий в мобильной сети есть возможность безопасного обмена ключевой информацией и установления шифрованного канала связи между ними.

В LTE сохраняются и методы аутентификации пользователей по привязке к карте USIM, как в традиционной мобильной связи: пользователь может заблокировать доступ к телефону по PIN-коду. Василий Сахаров, руководитель отдела информационной безопасности компании «Демос», отмечает, что в LTE от GSM и UMTS наследуются схемы протокола аутентификаиции EAP, в которые добавлены новые алгоритмы, более длинные ключи и расширенная иерархия PKI. Предусмотрены и новые функциональные возможности для новых сценариев, включающих межмашинное взаимодействие (M2M) и однократную аутентификацию (SSO). Кроме того, предусмотрена защита от несанкционированных соединений поверх мультимедийной IP-сети IMS. Вполне возможно, что используемая в мобильной связи более жесткая система аутентификации позволит навести порядок и в Интернете [5].

Таким образом, для решения проблемы эффективного обеспечения информационной безопасности 4G-сетей, в рамках проведённого исследования, были предложены следующие рекомендации:

- совершенствование протоколов и методов аутентификации пользователей по привязке к карте USIM (получение доступа по PIN-коду);
- использование жесткой системы аутентификации;
- добавление новых алгоритмов в протокол аутентификации и использование расширенной иерархии PKI;
- ограничение доступа к оборудованию передачи данных, скрытие его технических характеристик и установленного программного обеспечения;
- пересмотр, дополнение и модификация сигнатурных протоколов, а также программируемых сетей (SDN);
- использование только проверенных (безопасных) устройств и специального защитного программного обеспечения.

Комплексная реализация данных рекомендаций позволит уменьшить возможную величину, возможного как для рядовых пользователей, так и для корпоративных сетей.

Литература

1. Статистика уязвимостей корпоративных информационных систем в 2013 г. Positive technologies, 2014.
2. Уязвимости сетей мобильной связи на основе SS7. Positive technologies, 2014.
3. Статистика уязвимостей мобильной связи на основе SS7. Positive technologies, 2014.
4. Мобильные телефоны и тотальная слежка АНБ: как это работает. Positive technologies, 2014.
5. Безопасность мобильного интернета изнутри и снаружи. Positive technologies, 2013.
6. 4G ‘inherently less secure’ than 3G. The Telegraph, 2014.
7. Соляной, В. Н., Сухотерин, А. И., Воронов, А. Н. Развитие сотрудничества российских и зарубежных ВУЗОВ по защите информационного ресурса. Научная статья. «Перспективы организационные формы и эффективность развития сотрудничества Российских и зарубежных ВУзов» При поддержке Посольства Туркменистана в Российской Федерации. Сборник материалов III Ежегодная международной научно-практическая конференция 6-7 апреля 2015 г.: Королев МО: ФТА // Издательство «Канцлер». – 2015-52 с.

8. Соляной, В. Н., Сухотерин, А. И, Шихнабиева, Т. Ш., Сиротский, А. А. Некоторые элементы ассоциативности в методиках преподавания дисциплин технической направленности. Организация менеджмента информационной безопасности в финансово-кредитных учреждениях. Информационная безопасность бизнеса и общества. Сборник статей научно-преподавательского состава кафедры информационных систем, сетей и безопасности / Российский Государственный Социальный Университет // М.: Издательство «Перо». – 2016. – 111 с. ISBN 978-5-906851-15-4.
9. Соляной, В. Н., Сухотерин, А. И Выработка коммуникативной компетенции при подготовке профессионалов по информационной безопасности с использованием технологии модерации «Инновационные технологии в современном образовании» // Сборник трудов по материалам III Международной научно-практической Интернет-конференции 18 декабря 2015 г. // М.: Издательство «Научный консультант». – 2016. – 784 с. ISBN: 978-5-9907976-9-7.
10. Соляной, В. Н., Сухотерин, А. И, Антоненко, В. И. Проблемно- ориентированная подготовка специалистов по информационной безопасности с использованием имитационного метода (мозговой штурм). «Инновационные технологии в современном образовании» // Сборник трудов по материалам III Международной научно-практической Интернет-конференции 18 декабря 2015 г. // М. Издательство «Научный консультант». – 2016. – 784 с. ISBN: 978-5-9907976-9-7.