СОДЕРЖАНИЕ

Журнал входит в «Перечень российских рецензируемых научных журналов, в которых должны быть опубликованы основные научные результаты диссертаций на соискание учёных степеней доктора и кандидата наук» Высшей аттестационной комиссии Министерства образования и науки РФ.
Рукописи, принимаемые к публикации, проходят научное рецензирование.
Мнение редакции не всегда совпадает с точкой зрения автора.

Учредитель – Российский новый университет

РЕДАКЦИОННЫЙ СОВЕТ
Зернов В.А., д.т.н., профессор
Бугаев А.С., академик РАН
Гуляев Ю.В., академик РАН
Никитов С.А., чл.-корр. РАН
Андрюшин О.Ф., д.т.н., профессор
Волков В.Г., д.т.н.
Дворянкин С.В., д.т.н., профессор
Звежинский С.С., д.т.н., профессор
Крюковский А.С., д.ф.-м.н., профессор
Лукин Д.С., д.ф.-м.н., профессор
Минаев В.А., д.т.н., профессор
Палкин Е.А., к.ф.-м.н.
Филипповский В.В., к.т.н.
Черная Г.Г.

РЕДАКЦИОННАЯ КОЛЛЕГИЯ
Главный редактор – **Черная Г.Г.**
Научный редактор – **Дворянкин С.В.**
Научный консультант – **Растягаев Д.В.,** к.ф.-м.н.
Графика – **Абрамов К.Е.**
Распространение – **Михеев Б.Ю.**

ИЗДАТЕЛЬ
ООО «Спецтехника и связь»
Адрес редакции
111024 Москва,
ул. Авиамоторная, 55, кор. 31
Тел./факс: +7 (495) 544-4164,
тел.: +7(963) 636-8984
e-mail: rid@rosnou.ru
e-mail: galina_chernaya@bk.ru
http://www.st-s.su

ISSN 2075-7298
Индекс в каталоге Агентства «Роспечать» **80636**

Дизайн, верстка –
Фащевская И.А.

Тираж 2000 экз.

Отпечатано с готовых диапозитивов в ООО «Чебоксарская типография № 1» 428019, г. Чебоксары, пр. И. Яковлева, 15

Журнал зарегистрирован Федеральной службой по надзору в сфере связи и массовых коммуникаций.
Свидетельство о регистрации ПИ № ФС77-32855 от 15 августа 2008 г.

АРИСТОВ[1] Максим Сергеевич
ШИШИН[2] Олег Игоревич
РАПЕТОВ[3] Антон Максимович
КРЫМОВ[4] Антон Сергеевич
ЕГОРОВ[5] Алексей Дмитриевич

ОБЗОР И КРАТКИЙ АНАЛИЗ ТЕКУЩЕГО СОСТОЯНИЯ МОБИЛЬНОЙ СВЯЗИ НА ПРИМЕРЕ СЕТЕЙ GSM

Данная работа посвящена анализу текущего состояния мобильной связи на примере GSM-сетей. Рассмотрены различные уязвимости сетей и угрозы безопасности информации, передаваемой по сотовым сетям, а также модель атаки Man-in-the-Middle в беспроводных сетях связи. Приведен процесс моделирования и анализ способов защиты от атак Man-in-the-Middle.
Ключевые слова: GSM-сеть, мобильная связь, атаки Man-in-the-Middle, модель нарушителя и угроз.

This article deals with analytical statistics on mobile network state, by example of GSM. Different network vulnerabilities and threats to security of information transmitted over cellular networks, as well as a model of Man-in-the-Middle attack in wireless communication networks are considered. The paper covers modeling and analysis of the means of protection against Man-in-the-Middle attack.
Key words: GSM network, mobile communications, Man-in-the-Middle attack, intruder and threats model.

На сегодняшний момент GSM-сеть является самым распространенным и удобным средством связи. GSM-сеть получила большое распространение по всему миру благодаря своей относительно небольшой цене установки (по сравнению с другими технологиями мобильной связи), доступности и универсальности мобильных устройств, поддерживающих технологию, а также своей закрытости, что изначально делало систему неподдающейся атакам злоумышленников.

Сегодня GSM-технология считается устаревшей, многие отказываются от нее в пользу более современных сетей, таких как CDMA (Code Division Multiple Access — множественный доступ с кодовым разделением) и LTE (Long Term Evolution). Большинство уязвимостей этой сети известны и доступны общественности [1 — 3]. При этом многие из них лежат в основе концепции технологии и не могут быть устранены. Сеть третьего поколения (3G) решает многие проблемы GSM, но новая технология требует модернизации оборудования, чего некоторые операторы связи не могут себе позволить. Как и любая технология, сети третьего поколения также имеют уязвимости, которые также известны. Данные особенности поднимают проблему уязвимости конфиденциальной связи абонентов сети радиодоступа. Большинство уязвимостей можно устранить, не прибегая к большим затратам и модернизации оборудования.

Модель нарушителя и модель угроз в сетях сотовой связи

В качестве нарушителя информационной безопасности, рассматривается нарушитель, который не имеет непосредственного доступа к техническим средствам и ресурсам системы. Степень информированности нарушителя зависит от многих факторов, включая реализованные на объектах сети радиодоступа конкретные организационные меры и компетенцию нарушителей. Поэтому объективно оценить объем знаний вероятного нарушителя в общем случае практически невозможно.

В этой связи в целях создания определенного запаса прочности предполагается, что вероятные нарушители обладают всей информацией, необходимой для подготовки и проведения атак, за исключением информации, доступ к которой со стороны нарушителя исключается системой защиты информации. К такой информации, например, относится парольная (аутентифицирующая) информация.

Предполагается, что нарушитель имеет доступные в свободной продаже и специально разработанные технические средства и программное обеспечение.

[1-4] — НИЯУ МИФИ, аспиранты, [5] — НИ ЯУ МИФИ, студент.

А также все необходимые для проведения атак средства, возможности которых не превосходят возможности аналогичных средств атак на информацию.

К основным угрозам безопасности информации, передаваемой по каналу передачи сотовых сетей, относятся:

- осуществление пассивного прослушивания радиоканала злоумышленником;
- атака на оборудование абонентов сети;
- перехват информации по каналам связи операторов сети, изменение, искажение, перенаправление передаваемой информации;
- перегрузка оборудования оператора связи, вывод из строя связи;
- преднамеренная продажа конфиденциальной информации операторами связи сторонним лицам;
- преднамеренное предоставление ложной информации абоненту в целях обмана, ввода в заблуждение, саботажа;
- сбор данных посредством сторонних приложений, установленных пользователем;
- использование уязвимостей операционных систем оборудования абонента;
- использования уязвимостей интегрированных систем;
- использование конфиденциальных данных пользователей компаниями — разработчиками оборудования и программного обеспечения в сторонних целях.

Моделирование атаки Man-in-theMiddle в беспроводных сетях связи

Число пользователей сетей беспроводной мобильной связи постоянно увеличивается. Все более мощные мобильные устройства становятся доступны по более низкой стоимости. В связи с этим атака Man-in-the-Middle (MitM, «человек посередине») представляет реальную угрозу безопасности беспроводной сети [2]. Повсеместное распространение беспроводных сетей привело к ряду проблем в области безопасности между поставщиками услуг и конечными пользователями.

Радиоинтерфейс и доступ к беспроводной связи — это две области, где беспроводные сети не обеспечивают такой же уровень защиты, как проводные сети, если только не приняты дополнительные меры безопасности. Две основные угрозы представляют собой перехват данных по радиоинтерфейсу и незаконный доступ к беспроводной связи. Перехват пользовательских данных может привести к потере чувства защищенности и конфиденциальности у абонентов беспроводной сети. Защита от незаконного использования услуг должна прослеживаться не только по отношению к системам биллинга, но и к случаям представления злоумышленника оператором связи: представившись оператором связи в сети, злоумышленник имеет возможность перехвата всех пользовательских данных по радиоинтерфейсу.

Протоколы аутентификации, такие как WEP, EAP, GSM AKA, используются в различных беспроводных сетях для предотвращения незаконного использования беспроводных услуг. Но в этих протоколах безопасности механизм защиты основан только на односторонней аутентификации, где клиент проходит аутентификацию на сетевом сервере. Это открывает возможность злоумышленникам использовать атаки Man-In-The-Middle для выдачи себя за настоящего оператора связи.

Далее создана и рассмотрена математическая модель для анализа атак Man-In-The-Middle в разнообразных беспроводных сетях. Затем используются утверждения и логические операции для анализа отношений элементов в формальной модели. Модель и логические рассуждения, используемые в ней, помогают оценить, является ли данная система уязвимой для рассмотренного типа атак.

Атака Man-In-The-Middle в общем случае применима в любом протоколе связи, где отсутствует двусторонняя аутентификация. Для реализации MitM-атаки в беспроводной сети должны быть выполнены два условия. Во-первых, весь трафик между целевыми устройствами должен быть перехвачен и предоставлен злоумышленнику. Во-вторых, злоумышленник может выдавать свое оборудование за настоящее устройство сети.

Представленные условия легко осуществимы в сетях беспроводного доступа. Обычно мошенник использует в качестве оборудования сети мощные базовые станции (БС) или точки доступа (ТД). Когда мощность сигнала атакующего оборудования выше, чем настоящего, трафик абонентов автоматически проходит через оборудование злоумышленника. Для идентификации устройств злоумышленника используются необходимые сообщения для идентификации, стандартизированные в используемом типе беспроводной связи, в результате чего мошенник представляется в сети как настоящая БС или ТД оператора связи.

Наиболее распространенной моделью MitM-атаки в беспроводной сети является туннельная модель (Т-модель) [1]. Упрощенная схема отношений между участниками сети описана далее (**А** — абонент сети №1, **Б** — абонент сети № 2, **В** — злоумышленник). **В** перехватывает и блокирует начальное сообщение, которое является аутентификационным сообщением от абонента **А** абоненту **Б**. **В** изменяет сообщение, маскируется и отправляет его абоненту **Б**. Таким образом, **А** и **Б** договорились об используемом способе шифрования, который знает и понимает **В**. Тогда **В** может использовать свой способ шифрования, читать и передавать «конфиденциальные» сообщения между **А** и **Б**, выступая в роли своеобразного «туннеля».

В туннельной модели аутентификационное сообщение между клиентом и сервером, которое не видно абоненту беспроводной сети связи, определяется сервером. Таким образом, злоумышленник может легко подменить аутентификационное сообщение связи его собственными, что позволяет ему полностью контролировать и следить за общением абонентов **А** и **Б**.

Определим свойства безопасности абонента **А** и обозначим их в виде (Аутентификационная информация, RES); злоумышленник **В** имеет только одно свойство безопасности (Аутентификационная информация*); абонент **Б** имеет следующие свойства безопасности (Шифрование, XRES). Формальный анализ Т-модели изображен на *рис. 1*.

Путем логических рассуждений выведем правила, определяющие, соответствует ли данная система Т-модели.

Утверждение ***p***: аутентификационные сообщения не защищены, поэтому для злоумышленника **В** очень легко перехватить сообщения, заблокировать их,