С.А. Таратунин, М.В. Дикинштейн, Д.С. Лобунцов,
С.А. Писарев, Е.А. Оленников
Тюменский государственный университет, г. Тюмень

УДК 004.4

РАЗРАБОТКА ЗАЩИЩЕННОЙ СИСТЕМЫ ДОМАШНЕГО МОНИТОРИНГА ЭКГ

Аннотация. В статье рассматривается концепция защищенной системы домашнего мониторинга ЭКГ и актуальность введения ее в эксплуатацию. Кроме того, описывается взаимодействие компонентов системы и обеспечение защиты циркулирующей в ней информации.

Ключевые слова: Телемедицина, безопасность веб-приложений, безопасность мобильных приложений, информационные технологии.

Высокая смертность от болезней системы кровообращения – одна из основных причин отставания России от развитых стран по продолжительности жизни[1].

Люди, имеющие такие заболевания или предрасположенные к ним, нуждаются в постоянном наблюдении врача. Однако существует ряд причин, по которым оказание квалифицированной помощи не всегда возможно.

Основная причина заключается в том, что в последнее время сокращается количество медицинский учреждений разных масштабов[2], особенно это касается удаленных от крупных городов населенных пунктов, в которых у людей нет доступа к медицинским специалистам, способным провести необходимые обследования и поставить точный диагноз[3].

Кроме того, по стране наблюдается нехватка медицинский кадров, несмотря на стабильный приток молодых специалистов из учебных заведений[4].

К тому же значимая часть умерших от заболеваний сердечно-сосудистой системы - это пациенты, перенесшие операцию на сердце с недостаточным послеоперационным наблюдением и уходом во время восстановительного периода.

В связи с вышеперечисленными причинами возникает задача обеспечения удаленной связи между пациентом и врачом, с целью повышения эффективности оказания медицинских услуг пациентам различных населенных пунктов.

На данный момент существует система, в которой врач может удаленно проконсультировать пациента с помощью средств интернет-видеосвязи (например, Skype). Однако, данный подход не совсем эффективен, потому что данная система предполагает связь пациента и врача, но не передачу объективных показателей состояния пациента. Регистрация необходимых для точного диагноза данных возможна с помощью устройств мониторинга параметров организма человека[5].

В качестве решения данной проблемы могут использоваться портативные устройства, например, кардиорегистраторы, способные собирать данные о состоянии пациента.

Для передачи данных и связи между пациентом и экспертом предлагается реализовать систему следующим образом:

Система состоит из устройства регистрации необходимых данных (кардиорегистратора), мобильного приложения под ОС Android или веб-приложения, через которые осуществляется взаимодействие между пациентом и медицинским экспертом, а также сервер, осуществляющий сбор и хранений данных.

Рис. 1. Схема взаимодействия.

Однако, с появлением возможности передавать данные пациента удаленно к врачу, остро встает вопрос безопасности передаваемых данных.

В системе циркулируют конфиденциальные данные представляемые персональными данными и врачебной тайной (диагнозы и показатели состояния сердечно-сосудистой системы), а также коммерческая тайна (платежи за оказание услуг).

Доступ к вышеперечисленным данным имеется на сервере телемедицины, а также в мобильном и веб-приложении. Следовательно, утечка данных может произойти в любой из точек системы, и в каналах связи между ними. Поэтому необходимо использование защитных методов и средств для обеспечения безопасности данных обрабатываемых в системе.

При обеспечении безопасности необходимо учитывать требования законодательства Российской Федерации, а именно: 152 ФЗ (о персональных данных), 323 ФЗ (об основах охраны здоровья граждан в Российской федерации) и 98 ФЗ (о коммерческой тайне) [6-8].

Для удобной связи с врачом и передачи данных будет разработано мобильное приложение для операционной системы Android, взаимодействующее с персональным электрокардиографом. Однако, мобильные приложения подвержены определенным атакам, поэтому вопрос безопасности при работе с данными пациентов через мобильное приложение является приоритетным.

Рассмотрим основные виды атак на мобильное приложение:

Так как приложение устанавливается на мобильное устройство, то злоумышленник имеет возможность декомпилировать исполняемый файл, а также разобрать локально сохраненные данные с целью получения информации о принципах работы приложения.

В настоящее время нет никакого способа для полного избежания обратной инженерии, однако можно значительно усложнить декомпиляцию с помощью утилит для сокращения, оптимизации и обфускации кода. На

выходе получается .apk-файл меньшего размера, к которому намного сложнее применять методы обратной инженерии.

Поскольку наше приложение работает через сеть Internet, то оно подвержено угрозам утечки данных при передаче по сети, например, сниффингу или MITM-атакам.

В качестве защиты можно использовать сессионный механизм с ограничением времени жизни сессии. Это позволит уменьшить количество времени незащищенного пользования приложением.

Помимо этого, для защиты от атак используется криптографические алгоритмы и протоколы, которые позволяют предотвратить раскрытие и подмену передаваемой по сети информации. Пример такого протокола - HTTPS, работающий через шифрованные транспортные механизмы SSL и TLS.

Также стоит обратить внимание на проблему, свойственную самой мобильной платформе: получение прав суперпользователя и атака на приложение через внешние отладочные инструменты и вредоносное ПО.

Получение прав выполняется пользователем на своем устройстве самостоятельно, и не обязательно добровольно (пользователь может не подозревать, что устройство взломано), при этом все штатные средства защиты операционной системы не работают.

Для защиты необходимо предусмотреть механизм невозможности запуска защищаемого приложения при обнаружении прав суперпользователя (если существует такая техническая возможность на данной операционной системе).

Необходимо хранить важные данные приложения в защищенных хранилищах в зашифрованном виде, т.к. злоумышленник, имеющий права суперпользователя на устройстве, получает полный доступ к файлам во всех системных хранилищах.

Для возможности использования ПК при работе с системой домашнего мониторинга ЭКГ планируется разработать веб-приложение, реализующее

интерфейс доступа к серверу телемедицины для пациента и врача. При разработке веб части основное внимание будет уделено защите от актуальных на данный момент векторов атак на веб-приложения, таких как:

Инъекции кода, обрабатываемого базой данных - для веб-приложения особенно актуальны атаки инъекций кода исполняемого внутри систем управления базами данных. Такая атака позволяет злоумышленнику получить сначала полный доступ к данным, обрабатываемым веб-приложением, а в некоторых случаях расширить свои привилегии до полного контроля над системой путем загрузки командной оболочки в систему. Так, основой защиты является обработка всех данных поступивших с клиента на веб-сервер, удаляющая или инкапсулирующая любой код, который может исполнить СУБД, перед отправкой их в систему управления базами данных[9].

Кроссайтовый скриптинг. Атака такого типа обычно осуществляется путем отправки вредоносного кода на сервер, который, не обработав входные данные включает этот код в отдаваемую веб-страницу, что влечет за собой исполнение кода в браузере конечного пользователя и компрометацию и/или подмену вводимых им данных. Защита от этого вектора атак осуществляется с использованием средств фильтрации, принимаемых сервером данных, на наличие javascript кода, особенно в тех случаях, когда введенные данные включаются в отправляемые клиенту веб-страницы или контент для одностраничных веб-приложений. Также возможно применение средств для автоматического контроля и тестирования веб-приложения на наличие уязвимостей данного типа.

Межсайтовая подделка запроса - Атака реализуема злоумышленником в любом веб-приложении, серверная часть которого не предусматривает использование уникальных токенов. В таком случае, злоумышленник копирует запрос и использует для его отправки javascript код на стороннем сайте из браузера пользователя. Такая атака хоть и не приводит к прямой утечке данных, но позволяет злоумышленнику осуществить действия в веб-

приложении, используя личность легитимного пользователя. Защита от таких атак осуществляется не только в обработчике запросов пользователя, но и в коде, генерирующем данные запросы.

Сервер является основополагающим компонентом данной системы, а потому требует особого внимания в аспекте безопасности. Во избежание получения непреднамеренного доступа в приложении введена ролевая модель доступа, которая выбрана по нескольким причинам:

- Пользователь может иметь несколько ролей.
- Расширяемость данной модели достаточно высока, что удобно при разработке и развитии системы.
- Простота настройки и обслуживания.

Система устроена таким образом, что при запросе пользователя проверяется его роль, и если она недостаточна для совершения действия, то пользователю будет отказано в доступе.

Реализация такой модели должна быть не только в приложении, но и в базе данных, иными словами, приложение не должно подключаться к базе данных с максимальными привилегиями. Хорошим выходом будет создание роли для приложения и ограничение излишних прав на ряд операций.

В серверной части системы лучше использовать обратный прокси-сервер. Он может служить балансировщиком нагрузки, распределяя ее между серверами приложения. Кроме этого, обратный прокси выполняет защитную функцию - скрывает архитектуру серверной части. При атаке на серверную часть системы, обратный прокси-сервер примет на себя основной удар, при этом серверы приложений практически не пострадают.

В серверной части обеспечить защиту данных можно двумя способами: шифрованием данных и обезличиванием. Шифрование данных можно реализовать на стороне базы данных или как отдельный модуль приложения, который перед сохранением шифрует данные, а при обращении к этим данным выполняет обратные операции. Альтернатива шифрованию - обезличивание, то есть замена информации, которая дает возможность

определить принадлежность к конкретному субъекту. Оно может быть реализовано на стороне базы данных путем добавления “маскировочной” таблицы.

Таким образом, была разработана концепция защищенной системы домашнего мониторинга ЭКГ для использования на различных устройствах, которая позволит решить проблему удаленной коммуникации между наблюдаемым пациентом и лечащим врачом. Была разработана схема взаимодействия, основываясь на которой возможно создать современную телемедецинскую систему, соответствующую поставленной задаче. Помимо этого, были рассмотрены основные векторы атак на систему и методы защиты конфиденциальной информации, обрабатываемой в ней.

СПИСОК ЛИТЕРАТУРЫ

1. Вишневский, А. СМЕРТНОСТЬ ОТ БОЛЕЗНЕЙ СИСТЕМЫ КРОВООБРАЩЕНИЯ И ПРОДОЛЖИТЕЛЬНОСТЬ ЖИЗНИ В РОССИИ / А. Вишневский, Е. Андреев, С. Тимонин. // Демографическое обозрение. – 2016. – Том 3, №1. – С. 6-34.

2. Здравоохранение в России. 2017: Статистический сборник / Ред. колл.: Г. К. Оксенойт, С. Ю. Никитина и др. - М.: Росстат, 2017. - 172 с.

3. Ермакович, И. И. Возможности телемедицины в диагностике неотложных кардиологических состояний: опыт Харьковской области / И. И. Ермакович. и др. // Кардиология: от науки к практике. – 2014. – №2 (09). – С. 133-141.

4. Разработка защищенной телемедицинской системы / Н. О. Казанцев, И.И. Олейник, Д.В. Панфиленко и др. // Математическое и информационное моделирование: Сборник научных трудов. Т. Вып. 15 /Тюменский государственный университет. - Тюмень, 2017. - С. 186-193.

5. Телемедицина в России: реальность, проекты, законы, технологии [Электронный ресурс]. – Режим доступа :

https://teleradiologia.ru/телемедицина-в-россии-реальность-про/, свободный. – Загл. с экрана. – (Дата обращения: 13.04.2018).

6. Федеральный закон "О персональных данных" от 27.07.2006 N 152-ФЗ [Электронный ресурс]. – Режим доступа: http://www.consultant.ru/document/cons_doc_LAW_61801/, свободный. – Загл. с экрана. – (Дата обращения: 13.04.2018).

7. Федеральный закон "Об основах охраны здоровья граждан в Российской Федерации" от 21.11.2011 N 323-ФЗ [Электронный ресурс]. – Режим доступа : http://www.consultant.ru/document/cons_doc_LAW_121895/, свободный. – Загл. с экрана. – (Дата обращения: 13.04.2018).

8. Федеральный закон "О коммерческой тайне" от 29.07.2004 N 98-ФЗ [Электронный ресурс]. – Режим доступа: http://www.consultant.ru/document/cons_doc_LAW_48699/, свободный. – Загл. с экрана. – (Дата обращения: 13.04.2018).

9. OWASP Top 10 [Электронный ресурс]. – Режим доступа: https://www.owasp.org/index.php/Top_10-2017_Top_10, свободный. – Загл. с экрана.