DESIGN OF A SYSTEM FOR THE PROTECTION OF CARDIAC DATA

Miroslav Dechev, Krasimir Cheshmedzhiev

Institute of Robotics at the Bulgarian Academy of Sciences, Bulgaria

miroslav.dechev@gmail.com; cheshmedzhiev@gmail.com

ДИЗАЙН НА СИСТЕМА ЗА ЗАЩИТА НА КАРДИОЛОГИЧНИ ДАННИ

Abstract: *The recording, processing, analysis and storage of cardiac data is an essential step in achieving better care for the cardiac health status of patients. An important aspect in the processing and access to this type of data is the ability to reliably protect it from unauthorized access. The article shows an automated system for registration and mathematical analysis of cardiac data and methods for their protection. Information protection is achieved by implementing two-factor authentication. The characteristic of two-factor authentication is that access to the system takes place in two stages: entering a password as the first step and a code/key as the second. In this way, for protection, unauthorized access to the patient #39 file, including personal information and results of cardiac tests, is prevented.*

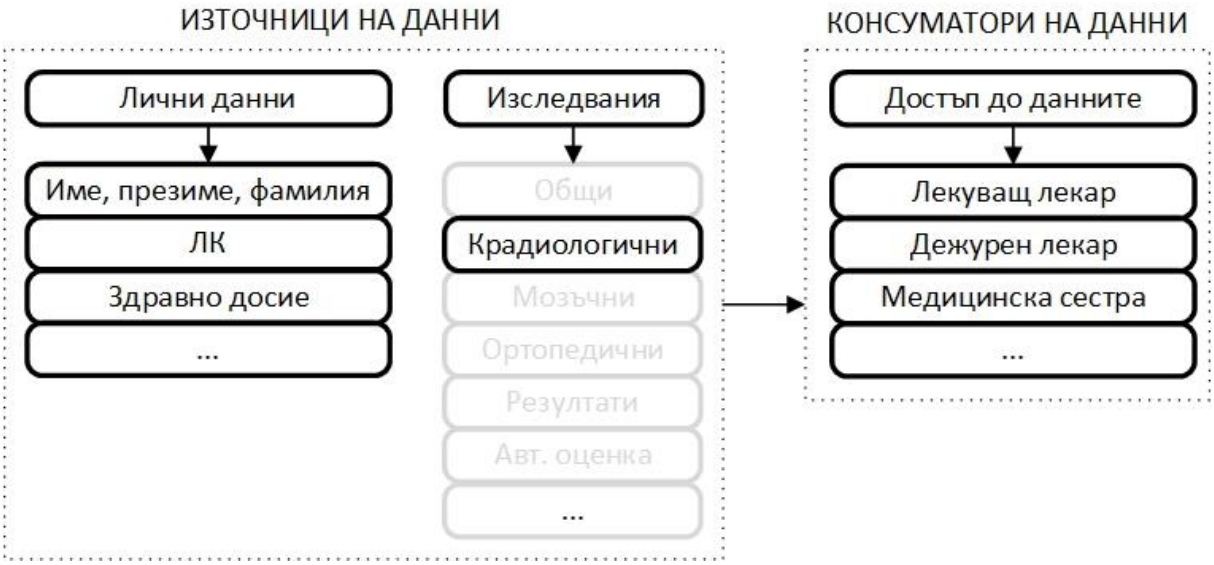
Keywords: *Cardiac Data; Electrocardiography, Photoplethysmography, Data Protection through Two-factor Authentication*

Въведение

Комуникационните и информационните технологии променят ежедневието ни, влияят на начина на живот и работа. Едно от най-важните им приложения е използването им в областите на здравеопазването и медицината. В резултат на използването на съвременни технологии за изследване и наблюдение на здравословното състояние на хората се създава голям обем от най-различни по своята същност данни в това число и кардиологични. В текущата статия е представен примерен дизайн на система за защита на кардиологични данни.

Изложение

На фиг. 1 е показана блокова схема на примерна система за регистриране и съхраняване на кардиологични сигнали и данни.



Фигура 1. Блокова схема на система за кардиологични данни

Представената система съдържа няколко основни относително самостоятелни градивни единици:

1. Източници на данни – тук се включват личните данни на пациента, здравното му досие, физически мерки като тегло, височина и т.н.
2. Консуматори на данни – лекуващ лекар, дежурен лекар и медицинска сестра.
3. Защита на кардиологични данни.

Осигуряването защитата на информацията започва още с проектирането и изграждането на бъдещата информационна система за защита на кардиологичните данни. Това става с конфигурирането на оборудването и програмното обезпечаване. Важен е анализът на информационните потоци и контрола на взаимната съвместимост. Когато този етап завърши се преминава към разработването на мерките за сигурност.

Защитата на данните се изразява в състоянието на дадена организация да осигури, поддържа и гарантира непрекъснатост на работните процеси, да минимизира рисковете. Най-важното е нейните системи да бъдат защитени от заплахи, компютърни измами, саботажи, шпионаж и природни катастрофи.

От първостепенно значение е гарантирането на сигурността и ефективното експлоатиране на информационните активи. Планирането на сигурността е сложен процес. На първо място при изграждането на системата за защита на кардиологичните данни е оценката на рисковете, при които се определят заплахите и уязвимостта. На второ място е дейността на организацията, която трябва да бъде съобразена с правните норми и законовите изисквания. И на трето – обособяването на специален набор от принципи, цели и функционални изисквания за обработка и

съхранение на информацията за пациента /име, ЕКГ, адрес, пол, възраст, тегло, височина, тел, e-mail/.

Развитието на информационните технологии и използването им във всички области на съвременния живот, в това число и в системите за сигурност и отбрана, поставя нови задачи и предизвикателства към защитата на тези системи и в частност към защитата на информацията в тях [7].

От изключително значение за информационната сигурност са стратегиите за управление на риска, тестването на системите за сигурност и оценката на информационната и мрежовата сигурност.

За да бъдат гарантирани тези защити се изисква изграждане на модел за сигурност в една организация. Системите за информационна сигурност трябва да осигурят изпълнението на определени изисквания, включени в държавни нормативни документи с цел защита на информацията от атаки, разкриване, неправомерно използване и унищожаване.

Мерките за сигурност се осъществяват чрез възможностите на техническите и програмните средства на компютърните системи и на специализирани средства. Технологиите за защита се модернизират постоянно, но заедно с тях напредък бележат и технологиите за атаки и неоторизиран достъп, като се развиват дори по-бързо. Онлайн средата става все по-рискова с нарастването на броя на потребителите, базата от данни, хилядите приложения, непрекъснатата свързаност към Интернет. Голяма част от системите са проблемни най-вече поради грешки в софтуера си и трудността си за разбиране. Повечето атаки са в резултат на това, че немалка част от потребителите, в случая пациентите срещат неразбиране при използване на сертификатите – пароли, автентификация, идентификатори за влизане, защита на акаунти и др.

Информационната защита представлява предотвратяването на загубата на данните при критични ситуации, като такива могат да бъдат, както природните бедствия, така и повредата на компютрите/сървърите, кражба или всеки друг риск от загуба на информацията. Сред заплахите се нареждат кражбите на устройства, софтуерните атаки, кражбите на интелектуална собственост и самоличности, саботажи и манипулации на информацията.

За целта трябва да бъдат опазени информационните инфраструктури и ресурси на организацията от всякакви опити с цел нарушаване на конфиденциалността, достъпността, целостта, достоверността, неприкосновеността, селективността и безотказността на информационните активи (сигнали, лични данни, знания, диагнози, ЕКГ, лечение, чувствителни данни), методи и средства за обработка, съхранение, потребление и обмен на данните. Най-общо групите от хора, които имат отношение към сигурността на информацията, свързана с пациента, включен в една система или мрежа, в случая трябва да бъдат лекаря на лицето, медицинските сестри, съпричастни към лечението, оторизирани медицински служители, системните администратори и самите потребители-пациенти.

Когато се осигурява за сигурността на една система за защита на кардиологични данни, се има предвид защита на информацията за пациента,

притежавана от вътрешните компоненти, а когато се осигурява сигурността в мрежата се обръща внимание на няколко основни елементи от модела на сигурност.

Това са идентичността, периметъра на сигурността, поверителността на данните, мониторинга на сигурността и управлението на политиката за защита на данните.

- Идентичност.

Това е способността да се идентифицира пациента и всички вътрешни компоненти на системата. Тук е необходимо да бъдат идентифицирани устройствата, хостовете, сървърите, услугите и приложенията, както и рутери, конектори и хъбове. Тези технологии включват мрежовите протоколи за автентикация (като Kerberos), старите инструменти за пароли, RADIUS и TACACS+. Съществуват и други методи за идентификация, като smart карти, цифрови сертификати и биометрични устройства [6].

- Периметър на сигурност.

Периметърът на сигурността налага условия за контрол на достъпа на базата на файлове с правила. Или накратко казано ресурсите в системата ще имат право да ползват само оторизирани потребители, като например лекуващия лекар, медицинския персонал, пациентите. Като периметър на сигурност могат да се определят защитните стени, тъй като те контролират външния достъп в системата.

- Поверителност на данните.

Това е умението информацията в системата да се предпази от неразрешен достъп или непозволени промени. За запазване поверителността на данните се използват двуслоен тунелинг, цифрово криптиране, виртуални частни мрежи и криптография.

- Мониторинг на сигурността.

Това е умението постоянно да се наблюдава системата.

- Управление на политиката.

Политиката на мрежовата сигурност определя очакванията на организацията за безпроблемно използване на мрежата и компютрите в нея и излага процедурите за предпазване от инциденти, свързани със сигурността.

Използваните методи и процеси в защитната архитектура на моделите за сигурност в една информационна система са: Криптографията, Автентикацията, Упълномощаването, Проверки, Инфраструктура на публичния ключ, Цифрови сертификати.

Криптографските алгоритми са много и разнообразни според криптографските преобразования. Те могат да бъдат симетрични, поточни, блокови, на публичните ключове, комбинирани, за еднопосочни хеш функции, за електронни подписи, за автентикация на съобщенията, за криптографски протоколи и др.

Автентикацията е процес, при който се използва име на акаунт и парола за идентифициране на потребител [6].

Типовете на автентикация са различни. Могат да се използват пароли и потребителски имена или биометрични данни. Упълномощаването представлява най-общо оторизирането на потребителите за достъп и дава определени права на

използване на системата. Проверките на потребителите изискват записването им в системата и тяхното проследяване.

Инфраструктура на публичния ключ е сбор от технологии и средства, чрез която се постига сигурна комуникация. Отговаря за проверка на поверителността и автентичността на информацията, обменяна между две точки. Инфраструктурата на публичния ключ използва следните три криптографски технологии за генериране на компонентите на сигурността: шифри на симетричните ключове, шифри на асиметричните ключове, еднопосочни хеш-функции [6].

Целта при използването на криптографските методи е след създаването на акаунта и паролата, хеш-функцията да ги криптира и запише. При всяко влизане в системата, хеш-функциите сравняват криптираната парола и ако е налице съвпадение се осигурява достъп в системата за потребителя.

Цифровите сертификати се базират на уникален цифров подпис. Автенчността на потребителя се установява след неговия електронен подпис /отпечатък/.

Защитата на правата на физическите лица при обработката на личните им данни е регламентирана от българското законодателство със Закон, според който физическите лица са защитени във връзка с обработването на личните им данни от институции в съответствие с Регламент (ЕО) 2016/679, както и по отношение на личните данни и тяхната обработка от компетентни органи.

Един от най-новите подходи в защитата на информацията включва използването на многофакторна аутентификация, геолокация, идентификация на устройства, анализ на потребителско поведение и други подобни способи [2].

Като специфична предпазна мярка при идентифициране в случаите на оторизиран достъп до данни, многофакторното удостоверяване е свързано с няколко важни стъпки.

С въвеждане на многоетапен процес за еднозначна идентификация на потребителя, в който извън стандартните потребителско име и парола се използват разнообразни технически способи и устройства, съчетани с предварително предоставена от пациента лична информация (напр. любим отбор, първа кола, домашен любимец и др.), спомагаща за неговото еднозначно разпознаване от автоматизираните информационни системи [2].

В многофакторната автентификация влизат още най-честото време на логване в системата, обичайните действия на потребителя, тяхната честота, вида устройства, които използват.

Съобразно тези действия се търсят сигнали, различни от познатите за системата, така наречените „червени флагове", подсказващи за неоторизиран достъп до информация и измама с фалшива самоличност.

На първо място потребителите на кардиологични информационни системи трябва да си изяснят контрола на достъп до тяхната информация. Поради критичния характер на кардиологичните данни, е важно те да бъдат достатъчно добре защитени, при експлоатиране в информационна система.

Поверителността включва правата на отделните лица да контролират събирането, използването и споделянето на техните лични данни и информация с

други. Поверителността е основно човешко право, което е крайъгълен камък на другите свободи в нашето общество. Той обхваща редица аспекти, включително физически, комуникационни, поведенчески и поверителността на информацията [1].

Всяка информация за едно физическо лице като име, дата на раждане, пол, адрес, образование, трудова история, медицински досиета и др., свързана с идентифициране на лицето е лична и като такава тя трябва да бъде защитена, на първо място, чрез Законите на всяка държава и на второ място, от разработчиците на информационната система и информационните бази от данни, в които е вписано физическото лице, в случая пациента. Нарушение на поверителността има тогава, когато се извършва неоторизирано събиране, използване или достъп до лични информация.

Данните могат да бъдат криптирани в компютъра на потребителя преди предаването, като се използва собствен софтуер на потребителя, или на доставчика. Дори ако потребителите възнамеряват да обработват данните си некриптирани в облака например, доставчикът може да избере дали да криптира всички или част от данните, които получава, преди да използва или продава анонимни или псевдонимизирани данни [5].

Като познат метод и предпочитан е прилагането на криптография към идентификатори, или така наречената двупосочна криптография, като при нея се кодират директни идентификатори необратимо. Потребителите могат да разчитат своята криптирана информация, като използват техния таен ключ за декриптиране. Понякога много малък фрагмет съдържа „лични данни". Дори ако само един фрагмент съдържа лични данни и те са разбираеми само за потребителя, вероятно става въпрос за „лични данни" за този потребител. Доставчиците имат различни системи за разделяне, т.е. по-сетнешния анализ е много труден без точни подробности.

Ефективността на ограниченията за контрол на достъпа и всякакви средства за достъп на доставчика до лични данни, съхранявани некриптирани, могат да повлияят на това дали данните са „лични данни" в ръцете на доставчика, дори ако доставчикът има само ограничен случаен достъп [5].

Все повече компании се обръщат към метода "Двуфакторна идентификация" с цел защита на данните и оторизиран достъп в сайтове, профили и акаунти. Това е метод, който използва два начина за влизане в профила на даден потребител. Методът е познат с няколко названия – автентикация, идентификация, верификация.

Двуфакторната автентикация засича опити за влизане във вашия акаунт от непознати устройства. При засичане на непознато устройство достъпът до профила ще завърши само след въвеждането на еднократен код, който се изпраща на смартфона ви. По този начин системата удостоверява, че човекът зад непознатото устройство е потребител с право на достъп [Киберсигурност на прост език, Над 50% от потребителите не използват двуфакторна автентикация, Темата е разработена от Customify, 2021, Questona, https://questona.com/potrebitelite-ne-izpolzvat-2fa/ (last view: 28-04-2023)].

Характерното за двуфакторната автентикация е, че влизането се осъществява посредством две стъпки /обикновено парола като първа стъпка и код или ключ като втора/.

Двуфакторната автентификация е предназначена да добави втори слой за удостоверяване в процеса на влизане, за да защити по-добре акаунтите на потребителите [https://bg.railstoolkit.com/odobreniya-za-vlizane-vv-facebook-nezadlzhitelnodvufaktorno (last view: 28-04-2023)].

Двуфакторната автентикация е обикновен метод за удостоверяване на потребителя, но създава достатъчно пречки. На практика това представляват две пароли за един профил, които обаче идват по различен път. Например след подаването на заявка за влизане или правилно въвеждане на първата парола, системата след това изпраща код по SMS или друг начин, който се въвежда в отделно поле. Има и вариант при който да се използва парола и пръстов отпечатък или друг метод за идентификация [Как да активираме двуфакторната автентикация за Google, Facebook и Twitter, 2018, Digital, https://www.digital.bg/kak-da-aktivirame-dvufaktornata-avtentikaciq-za-google-facebook--i-twitter-article670937.html (last view: 28-04-2023)].

Двуфакторната автентикация засича опити за влизане във вашия акаунт от непознати устройства. При засичане достъпът до профила ще завърши само след въвеждането на еднократен код, който се изпраща на смартфона на пациента текст на доклада.

Автентификацията и идентификацията са важна част от реализиране на сигурността на информационните системи [3]. За защитата на самите кардиологични данни има разработени различни криптографски алгоритми и комбинации от методи базирани на криптография, стеганография и математически трансформации [4], които постигат значително ниво на сигурност на потребителските данни.

Заключение

В създадения дизайн на система за защита на кардиологични данни са използвани два метода за защита на кардиологични данни: 1. прилагане на криптография към идентификатори, или така наречената двупосочна криптография, като при нея се кодират директни идентификатори необратимо и потребителите могат да разчитат своята криптирана информация, като използват таен ключ за декриптиране; 3. двуфакторната автентикация като метод за удостоверяване на потребителя, но създава достатъчно пречки; на практика това представляват две пароли за един профил, които обаче идват по различен път.

Благодарности

Научното изследване е проведено като част от проекта „Моделиране и създаване на сензорна система за изследване и анализ на здравословното състояние

на организма“ КП-06-М65/5 от 13.12.2022г., финансиран по Конкурс за финансиране на млади учени и постдокторанти 2022г. от Фонд „Научни Изследвания“.

References // Литература

[1] Alberta Government, (2016). “Cloud Computing and Privacy Toolkit Protecting Privacy Online”, Alberta Government https://www.alberta.ca/assets/documents/edc-cloud-computing-privacy-toolkit.pdf (last view: 28-04-2023)

[2] Bojinov, B. V. (2016). “Challenges for Ensuring the Information Security of Commercial Banks”, (2016). Available at SSRN: https://ssrn.com/abstract=2889351 (last view: 28-04-2023) or http://dx.doi.org/10.2139/ssrn.2889351

[3] Georgieva-Tsaneva, G. (2017). “Nature of Interactive System, Security and Accessibility”. Cultural and Historical Heritage: Preservation, Presentation, Digitalization (KIN Journal), 3(1), ISSN 2367-8038, Institute of Mathematics and Informatics – Bulgarian Academy of Sciences, pp. 138–147, 2017. http://www.math.bas.bg/vt/kin/book-3/10-KIN-2017.pdf (last view: 28-04-2023)

[4] Georgieva-Tsaneva, G.; Bogdanova, G.; Gospodinova, E. (2022). “Mathematically Based Assessment of the Accuracy of Protection of Cardiac Data Realized with the Help of Cryptography and Steganography”. Mathematics 2022, 10, 390. DOI: https://doi.org/10.3390/math10030390

[5] Hon, W. K.; Millard, C.; and Walden, I. (2011). “The Problem of 'Personal Data' in Cloud Computing - What Information is Regulated? The Cloud of Unknowing, Part 1” (March 10, 2011). International Data Privacy Law (2011) 1 (4): 211-228, Queen Mary School of Law Legal Studies Research Paper No. 75/2011, Available at SSRN: https://ssrn.com/abstract=1783577 (last view: 28-04-2023) or http://dx.doi.org/10.2139/ssrn.1783577

[6] Pritam, VV. NIIT. (2005). “Firewalls and Internet Security”, 2005.

[7] Stoyanov, N.; Ismailov, O.; Tselkov, V. (2016). “Risk management, testing and evaluation of network and information security”. Sofia, 2016.

Received: 15-05-2023 Accepted: 29-06-2023 Published: 24-07-2023
Cite as:
Dechev, M.; Cheshmedzhiev, K. (2023). “Design of a System for the Protection of Cardiac Data”, Science Series “Innovative STEM Education”, volume 05, ISSN: 2683-1333, pp. 45-52, 2023. DOI: https://doi.org/10.55630/STEM.2023.0506