Vojnotehnicki glasnik/Military Technical Courier
ISSN: 0042-8469
ISSN: 2217-4753
vojnotehnicki.glasnik@mod.gov.rs
University of Defence
Serbia

Data security in mobile healthcare

Zajeganović, Marija B.
Vugdelija, Natalija J.
Stefanović, Radiša R.
Kostić, Silva M.
Miljković, Uroš D.
Mach, Georg G.

Data security in mobile healthcare
Vojnotehnicki glasnik/Military Technical Courier, vol. 71, no. 3, pp. 748-768, 2023
University of Defence
Available in: https://www.redalyc.org/articulo.oa?id=661775012013
DOI: https://doi.org/10.5937/vojtehg71-44245
http://www.vtg.mod.gov.rs/copyright-notice-and-self-archiving-policy.html

This work is licensed under Creative Commons Attribution 4.0 International.

PDF generated from XML JATS4R by Redalyc
Project academic non-profit, developed under the open access initiative

Review papers

Data security in mobile healthcare

Безопасность данных в мобильном здравоохранении

Безбедност података у мобилном здравству

Marija B. Zajeganović a
Academy of Technical and Art Applied Studies Belgrade, Serbia
marija.zajeganovic@ict.edu.rs
https://orcid.org/0000-0002-6525-1949
Natalija J. Vugdelija b
Academy of Technical and Art Applied Studies Belgrade, Serbia
natalija.vugdelija@ict.edu.rs
https://orcid.org/0000-0002-4051-3148
Radiša R. Stefanović c
The Academy of Applied Technical Studies Belgrade, Serbia
rstefanovic@atssb.edu.rs
https://orcid.org/0000-0001-5497-3826
Silva M. Kostić d
Academy of Technical and Art Applied Studies Belgrade, Serbia
silva.kostic@ict.edu.rs
https://orcid.org/0000-0002-7766-6391
Uroš D. Miljković e
H Campus Wien - University of Applied Sciences, Austria
uros.miljkovic@fh-campuswien.ac.at
https://orcid.org/0009-0007-2416-0649
Georg G. Mach f
FH Campus Wien - University of Applied Sciences, Austria
georg.mach@fh-campuswien.ac.at
https://orcid.org/0009-0001-3538-6228

DOI: https://doi.org/10.5937/vojtehg71-44245

Received: 22 April 2023

Author notes

a Academy of Technical and Art Applied Studies Belgrade, Department School of Information and Communication Technologies, Belgrade, Republic of Serbia

b Academy of Technical and Art Applied Studies Belgrade, Department School of Information and Communication Technologies, Belgrade, Republic of Serbia

c The Academy of Applied Technical Studies Belgrade, Department of Applied Engineering Sciences, Požarevac, Republic of Serbia

d Academy of Technical and Art Applied Studies Belgrade, Department School of Information and Communication Technologies, Belgrade, Republic of Serbia

e FH Campus Wien - University of Applied Sciences, Vienna, Republic of Austria

f FH Campus Wien - University of Applied Sciences, Vienna, Republic of Austria

marija.zajeganovic@ict.edu.rs

PDF generated from XML JATS4R by Redalyc
Project academic non-profit, developed under the open access initiative

Revised document received: 14 June 2023
Accepted: 16 June 2023

Acceso abierto diamante

Abstract

Introduction/purpose: The digitization of healthcare has gained particular importance in the years since the emergence of COVID-19 and also has become one of the primary goals of the Government of the Republic of Serbia. Telemedicine is a good solution when the patient cannot come to a healthcare facility. Mobile healthcare applications are already widely used, but in both fields the important challenge is data security. The aim of this paper is to review solutions for data security in mobile healthcare from the technical side and possible challenges in the process of digitization of the healthcare system in Serbia.
Methods: This review is based on current papers in this area, on the available relevant literature and the authors' many years of experience in this field. Experiences in the process of digitization of healthcare in Serbia are based on available articles and regulations. Finally, possible challenges are presented from the authors' perspective based on everything presented in the field of data security in mobile healthcare.
Results: The analysis of the papers reviewed from the point of view of data security showed that users are often ready to sacrifice their privacy for the sake of convenience provided by mobile applications.
Conclusion: Based on the review of the papers and clear data security requirements that include the presented safeguards, one of the main tasks of the entire community is to raise awareness of information security and awareness of the need for cyber hygiene of each individual, which is the basis for the safe use of e-health services.
Keywords: information security, e-health, telemedicine, mobile healthcare, attacks, attack prevention.

Резюме

Введение/цель: Цифровизация здравоохранения приобрела особое значение с момента начала пандемии COVID-19. С тех пор ее совершенствование является одной из основных целей правительства Республики Сербия. Телемедицина – отличное решение особенно для пациентов, которые не могут посещать медицинские учреждения. Мобильные медицинские приложения уже широко используются, однако в обеих областях важной проблемой является безопасность данных. Целью данной статьи является обзор технических решений для обеспечения безопасности данных в мобильном здравоохранении, а также выявление возможных проблем в процессе цифровизации системы здравоохранения в Сербии.
Методы: Данный обзор основан на современных исследованиях в этой области, на имеющейся релевантной литературе и многолетнем опыте авторов в этой области. Опыт процесса цифровизации здравоохранения в Сербии основан на имеющихся статьях и регламентах. В заключении статьи авторы обсуждают возможные вызовы на основании всех перечисленных факторов в области безопасности данных в мобильном здравоохранении.
Результаты: Анализ доступных работ с точки зрения безопасности данных показал, что пользователи часто готовы пожертвовать своей конфиденциальностью ради удобства, предоставляемого мобильными приложениями.
Выводы: На основании обзора исследований и четких требований к безопасности данных, включающих представленные меры предосторожности можно сделать вывод, что одной из основных задач всего сообщества является повышение осведомленности об информационной безопасности и понимания того, насколько кибергигиена важна для каждого человека, так как она является фундаментом безопасного использования услуг электронного здравоохранения.
Ключевые слова: информационная безопасность, электронное здравоохранение, телемедицина, мобильное здравоохранение, атаки, предотвращение атак.

Abstract

Увод/циљ: Дигитализација здравства добила је посебан значај у време појаве корона вируса COVID-19, и постала један од примарних циљева Владе Републике Србије. Телемедицина је добро решење у случају када пацијент није у могућности да дође у здравствену установу. Мобилне апликације које се односе на здравство су увелико у употреби, али у оба случаја важан изазов је безбедност података. У раду су сагледана техничка решења која се односе на безбедност података у мобилном здравству и представљени су могући изазови у процесу дигитализације здравственог система у Србији.
Методе: Овај рад заснива се на актуелним радовима , на доступној релевантној литератури и вишегодишњем искуству аутора у овој области. Предочена су и искуства у процесу дигитализације здравства у Србији, као и могући изазови у области безбедности података у мобилном здравству.

PDF generated from XML JATS4R by Redalyc
Project academic non-profit, developed under the open access initiative

Резултати: Анализом прегледаних радова са становишта безбедности података показано је да су корисници често спремни да жртвују своју приватност ради погодности које им пружају мобилне апликације.
Закључак: На основу прегледа радова и јасних захтева у погледу безбедности података који укључују представљене заштитне мере, један од главних задатака целокупне заједнице јесте подизање свести о безбедности информација и о потреби сајбер хигијене сваког појединца, што представља основ за безбедно коришћење услуга е-здравства.
Keywords: безбедност информација, е-здравство, телемедицина, мобилно здравство, напади, спречавање напада.

PDF generated from XML JATS4R by Redalyc
Project academic non-profit, developed under the open access initiative

Introduction

Mobile healthcare (mHealth) refers to the application of mobile technologies in healthcare, including mobile applications, wearable devices, telemedicine, and other technologies that enable quick and easy exchange of medical data and information.

Information security in mHealth is of particular importance to ensure that medical data is stored securely and to maintain the patient's privacy. It is important to implement all security measures to ensure the data is protected from unauthorized access or misuse.

When it comes to information security in mobile healthcare, there are several key factors to consider: data transfer security, user authentication, device security, regulatory compliance, and software security.

Healthcare mobile applications use data encryption, which means that all data transmitted is encrypted and protected from unauthorized access. Encryption means that data is converted into an encrypted form before it is transmitted via the Internet, and only authorized persons with the right key can decrypt the data. Applications may implement other security measures, such as user authentication by using passwords, biometrics, or two-factor authentication, access control, and regular software updates to ensure data security.

Apps often provide privacy settings, allowing users to decide what data is shared with others and how. This includes sensitive medical data, such as data on health and medical conditions, as well as other types of data may be collected, such as data on physical activity, diet, sleep and other factors that may affect health, which can help users maintain a healthy lifestyle and improve their health. Depending on the type and sensitivity of the data, some is stored on servers in accordance with the law on the protection of personal data, which prescribes obligations and responsibilities related to the processing of personal data, while some is stored on mobile devices themselves, so users of these applications should be aware that they should apply security measures themselves, such as locking the device's screen, not using unsecured Wi-Fi networks, and not installing suspicious applications. Therefore, it is important to emphasize that in the case of mobile healthcare, when it comes to sensitive medical data, data security does not only refer to data storage on servers, but also on users' mobile devices. In any case, the data must be stored securely. This can be achieved by applying encryption or remotely erasing the data in case the device is lost or stolen. It is also necessary to comply with laws and regulations to ensure the legality and security of medical data processing.

Software used in mobile healthcare must be safe and secure. When developing and testing applications, security standards should be applied to ensure protection against hacker attacks or other types of cyberattacks. When creating a database, designers should adhere to the best practices and security standards, such as the GDPR (General Data Protection Regulation) and the HIPAA (Health Insurance Portability and Accountability Act), to ensure user privacy protection and regulatory compliance in the field of personal and health data protection.

Security of information systems

The term cybersecurity implies the protection of digital information, devices and resources. John McCumber (McCumber, 2004, pp.99-107) developed a network security management tool that he named the Cybersecurity Cube (Figure 1).

PDF generated from XML JATS4R by Redalyc
Project academic non-profit, developed under the open access initiative

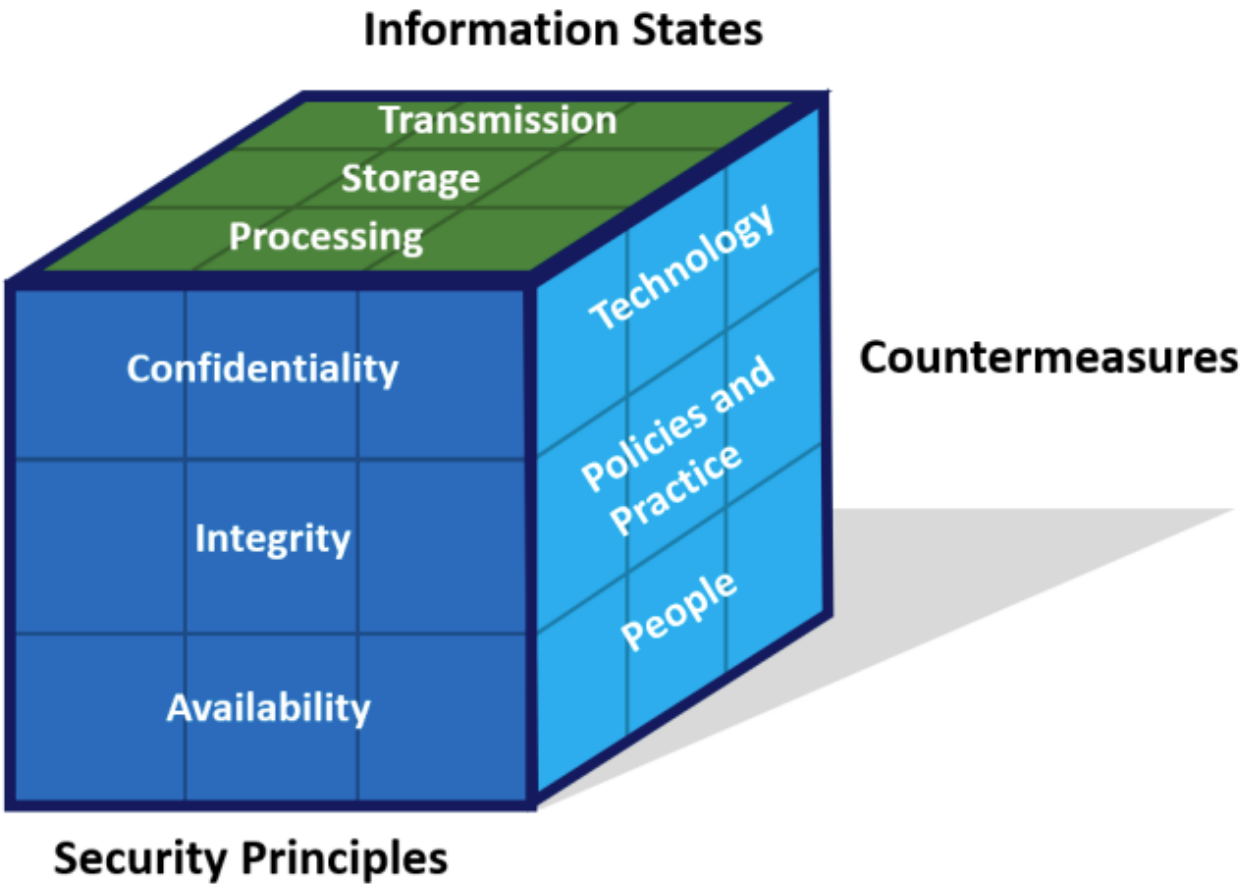

Figure 1
Cybersecurity Cube
Рис. 1 – Куб кибербезопасности
Слика 1 – Коцка сајбер безбедности

Like any cube, it has three dimensions that represent one of the tools for a comprehensive approach to information systems security. The first dimension of the cube includes the three principles of information security (CIA triad). The second dimension identifies three data states. The third dimension of the cube represents protective measures.

Principles of information security

In telecommunications, i.e., computer systems that enable data transmission, it is necessary to consider three key principles that form the core of security and represent desired goals when it comes to information security: confidentiality, integrity and availability, i.e., the so-called CIA triad (Stallings, 2014).

Confidentiality is assurance that information is neither intentionally nor accidentally disclosed to unauthorized persons. Confidentiality encompasses two related concepts: data confidentiality and privacy. Data confidentiality ensures that information is not disclosed to or made available to unauthorized individuals. Privacy means that individuals control and influence what personal information may be collected and stored, who may do so, and to whom that information may be disclosed.

Integrity is a guarantee that the information has not been modified either accidentally or intentionally, thereby guaranteeing its credibility. In this sense, data integrity and system integrity should be taken into account. Data integrity guarantees that information and programs are not changed, that is, that they are changed only in a specific and authorized way. System integrity guarantees that the system performs the functions for which it is intended in an uninterrupted manner, protected from intentional, unintentional, and unauthorized manipulation of the system.

PDF generated from XML JATS4R by Redalyc
Project academic non-profit, developed under the open access initiative

Availability ensures that the systems work quickly, that is, without delay, and that the service is not denied to authorized users who should have timely and secure access to data and other resources.

The use of the CIA triad to define security goals is often supplemented with two more concepts: authenticity and accountability. Authenticity is the property of being able to trust the validity of the transmission of messages, the validity of the message itself, and the validity of the source of the message. Accountability is a security goal that supports non-repudiation and allows for the traceability of possible security breaches as truly secure systems are not yet achievable, so systems must keep activity logs to enable forensic analysis in the event of a security breach.

Data states

Cyberspace is a domain that contains a significant amount of sensitive information, and therefore the second dimension of the Cybersecurity Cube is the state of the data, because it is important to protect the data in each of the possible states.

Data at rest (storage) is the data which is stored while no user or process is using it. It can be stored locally on a device or centrally in a network. Data storage can be directly attached storage (DAS, Direct-Attached Storage) such as hard disks, USB flashes and similar, as well as RAID (Redundant Array of Independent Disks) which provide improved performance and fault tolerance. There are also network storage devices such as NAS (Network Attached Storage), and storage networks, SAN (Storage Area Network). A remote data storage option is cloud data. Each of the mentioned warehouses has specific challenges when it comes to their protection. Direct-attached storage is the most difficult type to manage and control, while network systems are a more secure option due to better performance and redundancy. On the other hand, network storage systems are more complicated to configure, so proper configuration, testing, and monitoring of such a system are extremely important.

Data in transmission is data transferred from one device to another. This can be done by using removable media to physically move data from one device to another (sneaker net) and over a wired or wireless computer network. Through computer networks, data is transmitted in accordance with standard protocols that are available to the public. Protecting the confidentiality, integrity and availability of transmitted data is one of the most important responsibilities of a cyber security professional. Protection of data in transmission is implemented through various technologies and protocols such as VPN (Virtual Private Network), SSL/TSL, IPsec, etc.

Data in processing is the third state of data that refers to data during initial input, modification, calculation, or during output. Data integrity protection begins with the initial data entry. Errors during input, data reading, faulty sensors or mismatched data formats are examples of data corruption during input. Data modification during encoding/decoding, compression/expansion, encryption/decryption is a stage where integrity can be damaged by a malicious code. Data protection during processing requires well-designed systems. Cybersecurity professionals create policies and procedures that require testing, maintaining, and updating systems to keep them functioning with the least amount of errors.

Protective measures

The third dimension of the Cybersecurity Cube defines the skills and disciplines that can be used to protect cyberspace. These include technologies, human factors, and security policies.

Technologies for the protection of information systems can be based on software, hardware, network, or cloud. Software protections include programs and services that protect operating systems, databases, servers and end devices. Software firewalls protect remote access to the system. Hardware protection includes firewall devices that block unwanted traffic. Protection at the level of network technologies provides protected transmission such as VPN (Virtual Private Network), protected access to network devices (NAC Network access control) and authentication and encryption for wireless access. Cloud service providers use virtual security appliances that run in a virtual environment with a security-enhanced operating system running on virtualized hardware.

PDF generated from XML JATS4R by Redalyc
Project academic non-profit, developed under the open access initiative

The human factor is often the weakest link in cyber security. Protective measures primarily include security awareness programs, which should be a constant process because new techniques and new threats are always present. People may not be intentionally malicious, but simply unaware of the consequences of not following security procedures. Establishing a culture of cyber security awareness should be implemented through formal education from early childhood to active security awareness programs in work organizations. Cyber security experts are also included in the protective measures. This is a particular challenge for education in the IT sector. A cyber security expert must master all techniques mastered by an attacker and must stay one step ahead of the attacker. Ethical hacking is a significant process in educating and creating cyber security professionals.

A security policy is a set of security goals that include rules of conduct for users and administrators. A comprehensive security policy must be clearly defined. Security policy usually includes identification and authentication policy, password policy, network resource usage policy, remote access policy, computer network maintenance policy, incident handling policy, etc. Standards help IT staff maintain consistency in network operation. Guidelines define how standards are developed and guarantee compliance with general security policies. Some of the most useful guidelines are good practices from organizations. Procedures are documents that are more detailed than standards and guidelines and include details of security policy implementation that usually contain step-by-step instructions and diagrams.

E-health

E-health is a branch of medical informatics that refers to the application of information and communication technologies for the provision of health services and health information. Thus, e-health promotes the sharing of health information, provides effective health care, and enables patients to manage their own health. The goal of e-health is to transform the healthcare system into a patient-centered model.

The COVID-19 pandemic has contributed to the increase in the research and development of e-health systems. Although there are many aspects, three areas can be singled out as key areas: the architecture of e-health, the development of mobile healthcare technologies, and the field of security of e-health systems (Alenoghena et al, 2022). E-health includes health informatics, electronic health record, electronic entry of medical orders, electronic prescriptions, telemedicine, and mobile healthcare.

Telemedicine

Telemedicine involves the use of information and communication technologies in order to provide health services to remote patients and to facilitate the exchange of information between the primary service of a doctor or medical staff and a specialist, or an expert in a subspecialty. Distance is the motive for the development of this area, which arose from the need to facilitate the treatment of patients in rural areas, that is, to provide adequate first aid in emergency cases (Reljin & Gavrovska, 2013). Telemedicine is a multidisciplinary field that includes processing, transmission, storing and searching of data that often include multimedia and have high requirements related to quality, flow, reliability, and protection.

There are three basic types of telemedicine: store and forward, remote monitoring, and real-time interactive services. Store and forward is a method where the sender has all information, and forwards to the recipient when it suits them. Remote monitoring implies that the patient's health is checked using various technical means and thus clinical indicators about them are obtained remotely. In the case of an interactive service, the doctor and the patient are online and the transfer of information is live and two-way between them. Within telemedicine, there are branches such as telecardiology, teleradiology, telepsychiatry, telesurgery, etc.

Mobile healthcare

Mobile healthcare is a technology that enables the application of e-health anytime and anywhere, which implies the use of mobile telecommunications and new network technologies. The term digital health, in

PDF generated from XML JATS4R by Redalyc
Project academic non-profit, developed under the open access initiative

addition to the already mentioned e-health, also includes the use of sophisticated computer sciences such as "big data" and artificial intelligence. The components of mobile health are wireless sensors, mobile devices, and communication technologies. Wireless sensors are used in the medical field to collect data on the condition of patients. Mobile devices enable the transmission of data, sound and images via a wireless connection, regardless of where they are. Communication technologies used in mobile healthcare are primarily short range systems (Bluetooth, Zigbee), WiFi, mobile cellular systems (2G, 3G, 4G, 5G), and satellite systems.

Mobile healthcare (mHealth) is defined by the World Health Organization (WHO) as mobile applications and wearable devices that are used for health care. Mobile apps are software programs used by mobile phones and tablets, while mHealth App are mobile applications used for health care.

The growing number of mobile applications including mHealth applications leads to increased access to health data. Research shows that many of the most popular mHealth apps for women on the market have poor data protection and security standards (Alfawzan et al, 2022). Although there are regulation, such as the EU GDPR (European Union General Data Protection Regulation), research shows that the regulations are not always followed in practice. A large number of medical, health and fitness applications can collect and potentially share data with third parties without always being transparently presented (Tangari et al, 2021). Mobile applications are rapidly becoming a source of information and decision support tools for both clinicians and patients. Such privacy risks should be presented to patients and may be part of consent when using a mobile application. Primarily, mHealth applications help users manage their health and receive health services. Research shows that people take responsibility for the risks while evaluating benefits when faced with a choice (Zhou et al, 2019). The advantages provided by mHealth applications, such as convenience, real-time health care, time saving and often free use, may outweigh the security and privacy risks, so users are willing to sacrifice privacy for the convenience that mHealth applications provide.

Data security in e-health

The CIA (Confidentiality, Integrity, Availability) triad represents the basic principle of information security, and it also applies to data security in e-health. Confidentiality guarantees that data will not be disclosed by unauthorized persons. This becomes even more important in mobile healthcare. First of all, information itself is sensitive, i.e., patient privacy must be protected. Second, wireless transmission and the very architecture of the network makes that data available to a large number of users, so there is a risk of its being compromised. That is why data encryption is necessary. Different types of encryption provide different levels of protection (Zajeganović et al, 2019). Integrity refers to the fact that the data has not been altered, which is of great importance when it comes to the data sent and recorded within e-health. This is accomplished using hashes or checksums. If the integrity check fails, the application must report an error and close without any data processing. And finally, the availability that allows the data to be always available when needed, is an extremely important condition because the patient's life can be threatened if they are denied medical services. The HIPAA (Health Insurance Portability and Accountability Act) security rule requires the protection of sensitive health information about a patient, which means that that information will not be disclosed without the consent or knowledge of the patient. Authentication processes are varied and standards are constantly evolving. Biometric methods are involved in that process to a great extent (Tot et al, 2021a). The field of development and standardization of methods for biometric authentication is certainly one of the most important ones, and there is a large space for research in this area (Tot et al, 2021b).

In order for the data to be safe, it is necessary to have a secure computer network. The security of computer networks is a prerequisite for secure data transmission.

Threats and attacks in the computer network

PDF generated from XML JATS4R by Redalyc
Project academic non-profit, developed under the open access initiative

Threats and attacks in a computer network are very diverse and difficult to classify. The list of possible attacks is constantly increasing because different techniques for exploiting system vulnerabilities are continuously being developed. The specificity of the attack can also be related to the type of network infrastructure. In case of wireless communications, there are very specific attack techniques (Stefanović & Pavlović, 2013). Attacks can be divided into those that come from outside, from the Internet, and those that come from inside the network. Cyber attacks in a broader sense can also be divided depending on which layer of the OSI model they attack (Mitić et al, 2020) so we can classify them into:

- Attacks on the second layer (Layer 2 attacks) - attacks in the LAN network on one broadcast domain,
- Attacks by protocols (Protocols Attack) - attacks on routing protocols (RIP, OSPF, EIGRP, BGP), attacks on DHCP (Dynamic Host Configuration Protocol), HSRP (Hot Standby Routing Protocol), CDP (Cisco Discovery Protocol), ICMP (Internet Control Message Protocol),
- Quantitative attacks - attacks where attackers send a large amount of traffic over the botnet that exceeds the available flow capacity of the victim, and
- Application attacks - attacks that use vulnerabilities in applications and operating systems.

The list of frequent attacks on the computer network consists of:

- eavesdropping,
- data modification,
- IP address spoofing attack,
- password-based attacks,
- Denial of Service (DoS) attack,
- Man-in-the-Middle attack,
- compromised key attack, and
- sniffer.

The above list only represents some of the common computer network attacks. The tools used by attackers are also diverse and their sophistication is constantly increasing. The decryption process is definitely being accelerated by the development of computer technology, but it is unlikely that it will completely replace the role of humans (Stefanović & Srdanov, 2014). In the past, the tools were not so sophisticated and the attackers had to have a lot of knowledge about networks, while today the situation is completely different . The user of the attack tools does not need to have any technical knowledge. Today, even cybercrime is offered as a service and cybercriminals, malware developers and other participants in the cybercrime infrastructure sell their services to potential clients. However, in contrast to cybercriminals (black hat hackers) there are also benevolent hackers (white hat hackers) who use the same tools, but with the aim of finding system vulnerabilities in order to improve their protection. The list of attack tools is not exhaustive and is constantly growing. However, the following are some of the commonly used cyber attack tools:

- password cracking tools,
- tools for hacking wireless networks,
- network scanning and hacking tools,
- tools for creating fake packages,
- packet capture and analysis tools,
- Rootkit detectors,
- tools for detecting, scanning and exploiting vulnerabilities,
- forensic tools,
- operating systems with hacking tools, and
- encryption tools.

In order for hackers to access the system and apply any of the tools mentioned above, they need to compromise the respective device, which is done by some of the malicious software such as:

- different types of viruses,
- different types of Trojans,
- worms,

PDF generated from XML JATS4R by Redalyc
Project academic non-profit, developed under the open access initiative

- adware,
- ransomware,
- spyware, and
- rootkit.

Finally, in order to develop a new attack technique, a good knowledge of the functioning of the system as well as the vulnerabilities that the system has in order to exploit these vulnerabilities is necessary. The overview of cyber attacks, protection techniques and their recognition is inexhaustible because with the development of new technologies, new types of attacks appear as well as techniques for detecting and preventing cyberattacks. Since there is no perfect protection, it is necessary to combine different protection techniques and educate users on how to protect their accounts (Vugdelija et al, 2021). Vulnerability detection is primarily the task of well-intentioned attackers whose goal is to improve system security. Ethical hacking is precisely the field of cyber security that deals with this.

Cyberattack protection techniques

As cyberattack techniques advance, so does the defense, that is, the response to the attack. To defend a larger network, dedicated protection devices are used at the Internet exit. Different software solutions such as antivirus, antimalware and firewall are used for individual defense. Restrictions are set on routers in the form of access lists. More sophisticated devices such as dedicated firewalls can filter traffic by checking the header at higher layers of the OSI model such as Intrusion Prevention System (IPS) and Intrusion Detection System (IDS) firewalls such as ASA (Adaptive Security Appliance) devices and ISR (Integrated Services) Routers), then ESA/WSA (Email Security Appliance/Web Security Appliance) that filter spam emails and prevent access to suspicious sites that have malicious software, as well as AAA servers (Authentication, Authorization and Accounting) that allow access only to authorized users. As stated earlier, cryptography is one of the basic methods of data protection and the trend is to encrypt all data. Secure communication has the following four elements: data integrity, provenance, data confidentiality, and data non-repudiation. This is achieved by appropriate techniques such as: symmetric and asymmetric encryption, hash functions, digital signature, and digital certificates (Zajeganović et al, 2019).

Complete protection against cyberattacks is difficult to achieve because there are many links in that defense chain, of which the human being is one of the weakest, so the way to improve security is the so-called zero-trust architecture (Zero-Trust Security Model).

Digitization of healthcare in Serbia

Digitalization program in the healthcare system of the Republic of Serbia for the period 2022 - 2026 adopted by the Government of the Republic of Serbia provides recommendations, i.e., measures that should be taken in order to digitize and comprehensively modernize healthcare, so as to obtain connected, efficient, and better quality healthcare.

One of the special goals is the establishment of a secure and integrated information and communication infrastructure and electronic services. In order to achieve this goal, among other things, legal frameworks related to the security of sensitive health information that is used, exchanged and stored, as well as the rights of access to that data, are necessary. New technologies are introducing solutions that allow healthcare professionals to communicate with patients remotely and opening the door to the use of telemedicine devices for remote monitoring of the patient's condition. The Government of the Republic of Serbia has foreseen that eHealth provides other possibilities in terms of electronic regulation of sick leave, renewal of electronic prescriptions, requests for issuance and renewal of health insurance cards, insight into the costs of health services provided, participation in the selection of options for locations for the provision of health services, receiving advice from health workers about the prescribed therapy and treatment. Certainly, in order to achieve this, a coordinated activity of adapting already existing software programs and developing new ones is needed. In Serbia, there is an IZIS (integrated Health Information System) and all data exchanged must comply with the existing standards, including data security.

PDF generated from XML JATS4R by Redalyc
Project academic non-profit, developed under the open access initiative

A special challenge in terms of data security and privacy is the establishment of a system for collecting depersonalized data periodically or in real time for the purposes of analytics and reporting, as well as operational data on the use of resources in the health system. This would enable the improvement of a decision-making system based on machine-readable data, analysis, and reports.

Above all, the basis on which everything rests is the computer network, technologies for remote data transmission as well as the availability of network devices and servers. In this sense, all system should have resources and procedures for back-up so that all data would be saved in case of failure for any reason, including cyberattacks.

In the Republic of Serbia, the process of digitizing the healthcare system began several years ago but the COVID-19 pandemic made people more aware of the need and importance of remote treatment and the use of mobile applications in healthcare, and accelerated this process by placing it among the priority tasks on the way to the e-society.

Telemedicine in Serbia

The modern telemedicine program started in Europe in 1988 (Reljin & Ćućuz, 2007), and Serbia did not lag behind. Although in the 90s there was a difficult situation in the country due to sanctions, hyperinflation and war actions, 1995 saw the beginning of the digitization of the large library of classic glass slides at the Military Medical Academy (VMA) at the Institute of Pathology and Forensic Medicine, and in 1997 Telemedicine Center was established at the VMA and a permanent telepathological connection was established between the VMA in Belgrade and the Military Hospital and Institute of Pathology of the Faculty of Medicine in Niš. The VMA had several experimental connections with other medical centers: in Podgorica, Sremska Kamenica, and with KBC Bežanijska Kosa.

Medical institutions in Serbia have been faced with a lack of professional staff for decades, and for this reason, in 2012, the Project "Introduction of Telemedicine in Eastern Serbia" was launched. The Project was implemented by the National Alliance for Local Economic Development (NALED) and the "Merck Sharp & Dohme" (MSD) foundation, and within a year, the idea came to fruition. The health center in Boljevac is connected with the Zaječar Health Center and the Clinical Center in Niš by means of telecommunication equipment. The biggest challenge for the implementation of telemedicine is providing good equipment and support to patients and doctors.

After these pioneering efforts, subsequent projects in the field of e-health were supported by the Government of the Republic of Serbia, so that today, for more than a year, patients can be examined through the Heliant Telemedicine platform at KBC Zvazdara, in which the service is intended for patients suffering from inflammatory bowel disease. This kind of service should take root in other areas of medicine as well.

Mobile healthcare in Serbia

As mentioned earlier, mobile healthcare includes mobile applications and wearable devices used for health care. The importance of mobile healthcare is also shown by the fact that since the Apple smart watch was registered as a medical device, more and more people appeared who did not know they had cardiac arrhythmias, and received a warning from such a watch. Of course, there are far more specialized devices used in mobile healthcare to monitor the health of patients, such as smart pressure gauges that, in addition to analyzing blood pressure and heart rate, monitor ECG and heart sounds, and all these results can be made available to the doctor for further analysis. In addition to specialized devices, there are also mobile applications that allow monitoring and saving of recorded health data that can be used for further analysis. The fact that devices like smart watches and mobile phones can be made into medical devices with the right mobile apps makes it easier for people to get involved in the process of taking care of their health.

Various mobile applications for health care are available in Serbia. In cooperation with the Multiple Sclerosis Society of Serbia, the Heliant company developed the mobile application My MS World. The application is conceptually divided into three units. The first part consists of educational content, the

PDF generated from XML JATS4R by Redalyc
Project academic non-profit, developed under the open access initiative

second part represents support for patients in fulfilling their daily activities, and the third part contains information about therapeutic methods, and questionnaires and tests that help self-assessment of patients' health status. There are a number of mobile applications whose development was initiated by the corresponding association, so the MyMelanoma application was prepared by the Association of Melanoma Patients, while the MojRA application was prepared by the Association of Rheumatic Diseases of Serbia, and the HemApp application was prepared by the Association of Hemophiliacs of Serbia. After successful implementations in Serbia, the same applications were implemented in Montenegro (MojRA ME, HemApp ME). The ONKO application was created as part of the "Knowledge Against Cancer" project of the Institute of Oncology and Radiology of Serbia and is motivated by the idea of making it easier for patients to access the Institute of Oncology and Radiology of Serbia and to enable them to have the right information when it comes to the treatment of malignant diseases. The Open the Blue Circle (OPK) mobile application, which is part of the Cities Change Diabetes project, was developed to promote healthy lifestyles and thereby influence the prevention of diabetes. UNICEF in Serbia and the City Public Health Institute of Belgrade have developed a Bebbo mobile application to support parenting and monitor children's development from birth until they start school, and in addition to reminders for preventive pediatric examinations and immunisation schedule, it also suggested how to enrich family routines through games or how to set healthy boundaries for your child when it comes to behavior. Therefore, mobile applications used in mobile healthcare, in addition to health data and information, often have recommendations and activities that are generally related to a healthy lifestyle, both physical and mental, in order to prevent various diseases.

In mobile applications used for health care, general information is stored on servers, and personal data is stored on the mobile phone itself and cannot be accessed by anyone other than that user. For any other data processing and storage of personal information in a place other than the phone, it is necessary to give the appropriate consent. Privacy rights and data security should be respected in all applications.

Data security

Since the beginning of remote treatment, the security of communication itself and the security of data are topics that must not be bypassed. This must be looked at from both technical and legal aspects. Legal acts related to the security of e-health and e-government in Serbia have been adopted. There is also the ConsentID application that can be used when signing up for eHealth and other e-services available to citizens of Serbia. The ConsentID application enables authentication when accessing the e-service, which is connected to the citizen's qualified electronic certificate. The portal for electronic identification, eid.gov.rs, enables access with different degrees of privileges, as well as the possibility of having a qualified electronic certificate in the cloud and a signature in the cloud.

Communication via the Heliant Telemedicine platform takes place via a video link generated through the Hedex (Heliant Data Exchange) service. Data servers are e-government servers. The mobile application "My MS World" stores data on the servers in Kragujevac, and for now there is much more informative content there than personal data, and work is being done, in cooperation with Heliant, to improve the application.

Finally, when it comes to data security in e-health, whether it is about telemedicine services or mobile applications used in healthcare, the biggest challenge is to design the system well enough from the point of view of security and privacy of sensitive personal data. Software designers need precise information about who can or must access which data in order to keep data systems connected, to properly create roles and access rights for different types of data. In this sense, in addition to technical, legal regulation is also necessary based on which requirements would be clearly defined. The topic of data security, especially when it comes to healthcare data, must be approached both from a technical and legal perspective.

Conclusion

PDF generated from XML JATS4R by Redalyc
Project academic non-profit, developed under the open access initiative

The aim of this review paper is to present the basic principles of information security as well as their application in technologies used in mobile healthcare, given that information security is of great importance in healthcare in general, and especially in the field of electronic healthcare due to the challenges that inevitably arise in that process.

Human error is the biggest problem for information security. Although many companies invest heavily in vulnerability scanning, antivirus programs, software updates, and more, the problem of undertrained employees remains. That is why it is of great importance that both employees and users are regularly trained in this area and that the awareness of information security is raised among all individuals. One of the main tasks of the entire community, above all the state, which has set the digitalization of society as its strategic goal, should be to raise awareness of information security and awareness of the need for cyber hygiene of every individual, either as an employee at the workplace or as a user of e-services. This is the only way to build an e-society that will safely use the services of e-government, e-health, etc.

PDF generated from XML JATS4R by Redalyc
Project academic non-profit, developed under the open access initiative

Acknowledgments

The authors would like to thank the Heliant company for providing information about the applied technologies in the health information system and the implemented projects in Serbia in the field of e-health.

References

Alenoghena, C.O., Onumanyi, A.J., Ohize, H.O., Adejo, A.O., Oligbi, M., Ali, S.I. & Okoh, S.A. 2022. eHealth: A survey of architectures, developments in mHealth, security concerns and solutions. *International Journal of Environmental Research and Public Health*, 19(20), art.number:13071. Available at: https://doi.org/10.3390/ijerph192013071.

Alfawzan, N., Christen, M., Spitale, G. & Biller-Andorno, N. 2022. Privacy, Data Sharing, and Data Security Policies of Women's mHealth Apps: Scoping Review and Content Analysis. *JMIR mHealth and uHealth*, 10(5), e33735. Available at: https://doi.org/10.2196/33735.

McCumber, J. 2004. *Assessing and managing security risk in IT systems: A structured methodology, 1st edition*. New York: Auerbach Publications. ISBN: 9780429208409.

Mitić, M., Zajeganović, M., Kurbalija, N., Čabarkapa, S. & Pavlović, M. 2020. Web server security. In: *15th International conference on Risk and safety engineering*, Kopaonik, Serbia, pp.250-256, January 16-18 [online]. Available at: http://www.rizik.vtsns.edu.rs/RSE_2020/radovi/05/RIZIK_05_3.pdf (in Serbian) [Accessed: 20 April 2023]. ISBN: 978-86-6211-124-1.

Reljin, B. & Ćućuz, V. 2007. Project telepathology network. In: *XXV Simpozijum o novim tehnologijama u poštanskom i telekomunikacionom saobraćaju - PosTel 2007*, Belgrade, pp.101-108, Decembar 11-12 [online]. Available at: https://postel.sf.bg.ac.rs/simpozijumi/POSTEL2007/RADOVI%20PDF/(3)%20-%20MULTIMEDIJA/03-Reljin%20Cucuz.pdf (in Serbian) [Accessed: 20 April 2023]. ISBN: 978-86-7395-243-7.

Reljin, I. & Gavrovska, A. 2013. *Telemedicina*. Belgrade: Akademska misao (in Serbian). ISBN: 978-86-7466-458-2.

Stallings, W. 2014. *Osnove bezbednosti mreža: aplikacije i standardi*. Belgrade: School of Computing & CET (in Serbian). ISBN: 978-86-7991-376-0.

Stefanović, R.R. & Pavlović, B.Z. 2013. Safety of routing protocols in ad hoc networks and possible attacks in the network. *Vojnotehnički glasnik/Military Technical Courier*, 61(2), pp.200-217 (in Serbian). Available at: https://doi.org/10.5937/vojtehg61-1826.

Stefanović, R.R. & Srdanov, A.S. 2014. Use of computers for decrypting messages. *Vojnotehnički glasnik/Military Technical Courier*, 62(2), pp.96-108 (in Serbian). Available at: https://doi.org/10.5937/vojtehg62-3831.

Tangari, G., Ikram, M., Ijaz, K., Kaafar, M.A. & Berkovsky, S. 2021a. Mobile health and privacy: cross sectional study. *BMJ*, 373, art.number: 1248. Available at: https://doi.org/10.1136/bmj.n1248.

Tot, I.A., Bajčetić, J.B., Jovanović, B.Ž., Trikoš, M.B., Bogićević, D.Lj. & Gajić, T.M., 2021. Biometric standards and methods. *Vojnotehnički glasnik/Military Technical Courier*, 69(4), pp.963-977. Available at: https://doi.org/10.5937/vojtehg69-32296.

Tot, I., Trikoš, M., Bajčetić, J., Lalović, K. & Bogićević, D. 2021b. Software platform for learning about brain wave acquisition and analysis. *Acta Polytechnica Hungarica*, 18(3), pp.147-162. Available at: https://doi.org/10.12700/APH.18.3.2021.3.8.

Vugdelija, N., Nedeljković, N., Kojić, N., Lukić, L. & Vesić, M. 2021. Review of brute-force attack and protection techniques. In: *13th International Conference, ICT Innovations 2021*, Skopje, North Macedonia, (18), pp.220-230, September 27–29 [online]. Available at: https://

PDF generated from XML JATS4R by Redalyc
Project academic non-profit, developed under the open access initiative

proceedings.ictinnovations.org/2021/paper/554/review-of-brute-force-attack-and-protection-techniques [Accessed: 20 April 2023].

Zajeganović, M., Zajić, G., Kurbalija, N., Pavlović, M. & Čabarkapa, S. 2019. Encryption types overview. In: *14th International conference on Risk and safety engineering*, Kopaonik, Serbia, pp.145-150, January 11-13 [online]. Available at: http://www.rizik.vtsns.edu.rs/wp-content/uploads/2019/03/Zbornik-RIZIK-2019.pdf (in Serbian) [Accessed: 20 April 2023]. ISBN: 978-86-6211-116-6.

Zhou, L., Bao, J., Watzlaf, V. & Parmanto, B. 2019. Barriers to and Facilitators of the Use of Mobile Health Apps From a Security Perspective: Mixed-Methods Study. *JMIR mHealth and uHealth*, 7(4), e11223. Available at: https://doi.org/10.2196/11223.

Additional information

FIELD: telecommunications, IT
ARTICLE TYPE: review paper

Alternative link

https://scindeks.ceon.rs/article.aspx?artid=0042-84692303748Z (html)
https://aseestant.ceon.rs/index.php/vtg/article/view/44245 (pdf)
https://doaj.org/article/bf8f4734eb424a018b8435b9d56a1227 (pdf)
https://www.elibrary.ru/item.asp?id=53973019 (pdf)
http://www.vtg.mod.gov.rs/archive/2023/military-technical-courier-3-2023.pdf (pdf)

PDF generated from XML JATS4R by Redalyc
Project academic non-profit, developed under the open access initiative