Sağlık Akademisyenleri Dergisi
www.saglikakademisyenleridergisi.com

Derleme / Review Article

Kişiselleştirilmiş mobil sağlık uygulamaları bilgi güvenlik gereksinimleri

Information security requirements of customized mobile health applications

Mehmet Oguz

Southern University,
Institute of Management Business and Law Health Management , Ph.D. Program, Rostov-on-Don, Russia

Anahtar Kelimeler:
Bilgi güvenliği, Mobil sağlık, Ağ güvenliği

Key Words:
Information security, Mobile health, Network security

Yazışma Adresi/Address for correspondence:
Mehmet Oguz
Institute of Management Business and Law Health Management , Ph.D. Program, Rostov-on-Don, Russia.
mehmetoguz1964@live.com

Gönderme Tarihi/Received Date:
01.05.2017

Kabul Tarihi/Accepted Date:
22..05.2017

Yayımlanma Tarihi/Published Online:
15.06.2017

DOI:
10.5455/sad.13-1493676116

ÖZET

Bu çalışmanın amacı, kişiselleştirilmiş sağlık uygulamalarında bilgi güvenlik gereksinimleri ile ilgili farkındalığın geliştirilmesine katkı sağlamaktır. Çalışmada sağlık bilişimi alanındaki gelişmelere bağlı olarak, gelişen mobil uygulamalarının bilgi güvenliğini etkilemelerine atıf yapılarak, sağlık alanında kurulan sistemlerde ağ ve bilgi güvenliği boyutları ile birlikte saldırı ve türleri de değerlendirilmiştir. Günümüzde sağlık bilgi sistemleri uygulama, kontrol, izleme, uyarı sistemleri olarak birbirleriyle entegre sistemler olarak modellenmektedir. Bu sistemler bir tarafında hasta olduğu sürece, kişiselleştirilmiş özel bilgi biriktiren sistemler haline gelmektedir. Bu yaklaşımla hastadan dolayı mobilite kavramı sistemlerin olmazsa olmaz özellikleri arasına girmiştir. Hasta ile sistemler arasında günümüzde insan faktörü olmadan bilgi iletimi makinadan makinaya (M2M) yapılabilmektedir. Bu yaklaşım ile zamanında doğru verinin iletimi sağlamaktadır. Bu çalışmada sağlık sektör yöneticilerinin sağlıkta bilgi güvenliği farkındalığına, farklı bir bakış açısıyla katkıda bulunulmaktadır.

ABSTRACT

The purpose of this study is to contribute to creating awareness of information security requirements in customized health applications. The study refers to how developing mobile applications affect information security in accordance with the developments in health informatics and evaluates the aspects of network and information security in the health-related systems as well as attacks and types of attacks. Today, health information systems are modeled in integrated systems as application, control, tracking and warning systems. These systems have been turning into systems that collect private information as long as they have patients on one side. With this approach, the concept of mobility has become a must in systems because of the patient. Data communication can be performed from machine to machine (M2M) between the systems without the human factor. This ensures the communication of accurate and timely data. This study contributes to health administrators' awareness of information security in health with a different point of view.

INTRODUCTİON

In parallel with the advancements in Health Informatics, information system security is becoming more important for individuals, agencies and institutions. There are several different studies to achieve security in health information systems. It is aimed with these studies to provide information or computer systems with security. Security software utilized to this end is of great importance in the protection of systems.

This study addresses the network security in mobile health applications and the information security in health applications. It provides an overview of attacks and types of attacks on health systems from the perspective of personnel and administration

NETWORK SECURİTY İN MOBİLE HEALTH APPLİCATİONS

With the technological advancements in health, Body Area Networks (BANs) composed of medical devices interacting with human body have been developed. By this mean, devices that can automatically measure blood tension or insulin levels and transfer the values to hospital management systems have started to be used in daily life. While enhancing health management, these medical devices may also risk human health through unauthorized intervention with the devices and even cause deaths.

Wireless sensory networks are among highly important technologies that can be applied to different domains

in daily life. Using this technology along with medical technologies can provide solutions to several issues in health. Significant changes occurred in the operation of system with using wireless sensory networks in traditional patient tracking systems. Developing patient tracking systems are generally composed of transferring data of tracked patient to the medical server which involves hospital and/or doctor.

As the first layer of patient tracking systems and a widely-used technology, BAN draws attention with its applicability and cost. BAN is formed by smart sensors placed in human body or within tissue in general. If data acquired by sensors are transferred to a server using wireless connection for analysis or storage, this technology is called WBAN.

Even though WBAN has such advantages as tracking patient's medical data independently of time and space, security gaps of the technology can turn this into a disadvantage. Hence, customized mobile health applications come across as systems highly requiring security.

Today, rapid development of internet is increasing the demand for information and technology investments. Advancements in information technologies, especially database, internet and communication technologies, have brought health services in a transformation process. Portable devices, mobile phones and PDAs (Personal Digital Assistants), Universal Mobile Telecommunications System (UMTS), Digital Video Broadcasting (DVB) and developments in internet have become a routine channel of communication between health personnel and patients. These modern developments in information technologies have encouraged several countries about electronic health records and enabled them to interact with health informatic systems. These advancements directly affect and change the presentation of health services. (Bali & Dwivedi, 2007)

Security requirements of customized mobile health applications gain even more importance due to the increasing use of mobile devices. Whereas hardware and software security aspects necessary for the devices are developed, WBAN has also started to be included in the security efforts.

INFORMATİON SECURİTY İN CUSTOMİZED HEALTH APPLİCATİONS

Information security is explained as preventing unauthorized access, use, modification, disclosure, disruption, exchange or destruction of information as a type of asset. Even though technology-based solutions are provided in an effort by developing standards (ISO/IEC 2700xx) and software (antivirus software, firewalls, etc.) for achieving information security, those are humans that use these technologies. The idea that providing information security and solution to possible problems only with technology-based precautions cause the human factor, which may be the most important element in achieving information security in health, to be ignored. Yet, possible security vulnerabilities are increasingly reduced thanks to the technologies developed for information security over time. There is,

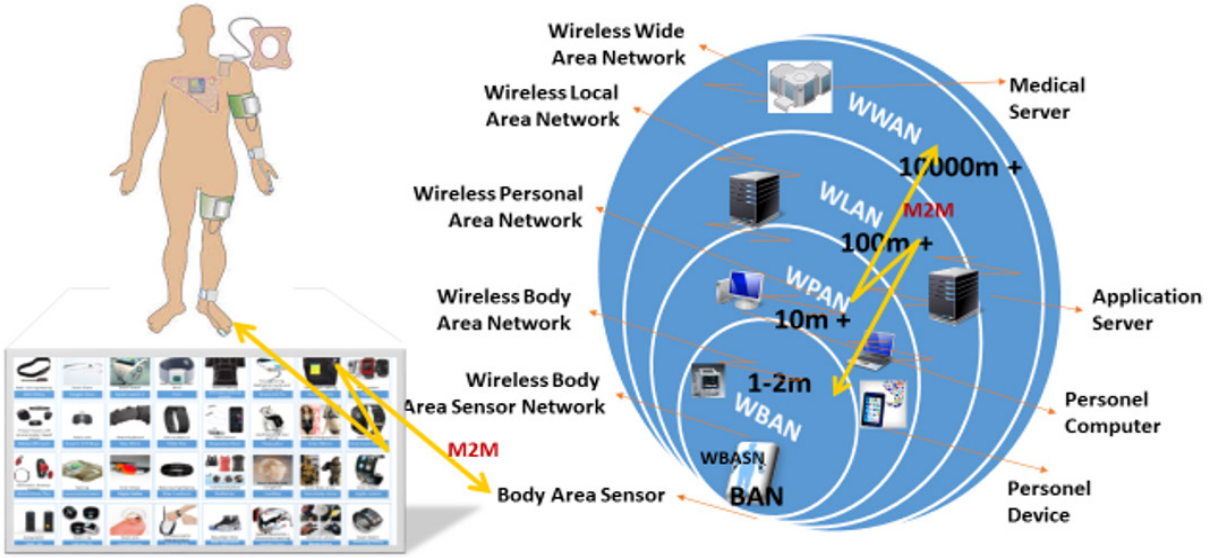

Figure 1. Network of Customized Mobile Health Applications

however, an effort to get the best of man-made errors and create security vulnerabilities. Hence, human factor is the weakest link of the personal and corporate information security. This indicates that the issue of information security cannot be solved by ignoring the human factor and only through technology-based methods. Therefore, it is quite important in minimizing the risks to take technology-based precautions in the information security of records in health as well as taking the human factor into consideration and creating awareness of information security to this end. Although it is not possible to eliminate the information security risks based on human factor entirely, a well-planned awareness activity may help lower security risks down to an acceptable level.

The information security standard was developed to be ISO 27799: 20xx on the grounds that information security management standards in health are different from those in normal enterprises. This standard presents directives for corporate information security standards and information security management applications including the selection, exercise and management of audits in consideration of the information security risk environment in health institutions. Similarly, ISO / IEC 27002 specifies directives to support interpretation and implementation in health informatics, accompanying the ISO 27799 international standards.

In today's practices, controls explained in ISO / IEC 27002 are used as guidelines to use and implement ISO 27799: 2016 health information security standard effectively. ISO 27799: 2016 is able to provide the minimum-security level for the confidentiality, integrity and availability of health institutions and other health units. (OBP, 2017)

Standard's main theme is how to protect health information (words, numbers, voice records, drawings, videos and medical images) via instruments (paper or electronically printing or writing in storage) used to store it no matter how as proper as possible all the time and it mentions about the information security in the process of communicating the information by hand and via fax, computer networks or by mail.

ATTACKS ON HEALTH SYSTEMS AND TYPES OF ATTACKS

In the security of health information and computer systems, individuals who are considered being malicious (hackers) and their attacks are defined as adverse parties. All attempts on computer systems for vicious purposes to breach or bypass and weaken an existing information and computer security system; damage individuals directly or indirectly; harm systems; impede, stop, bring down or collapse the operation of systems. Attackers perform attacks which include several different techniques to achieve their goal. Knowing the attack types and analyzing them properly to take necessary precaution is of great importance for information security. (Aslanbakan, 2016)

To understand the reason why the attacks are performed on computer systems contributes significantly to identifying the attacks and possible precautions.

Attack types primarily include code exploit, eavesdropping, denial of service (DoS), indirect attacks, backdoors, direct access attacks, social engineering and cryptographic attacks. (Canberk & Sağıroğlu, 2007)

Software defects such as buffer overflow, Common Gateway Interface (CGI) and scripting errors and encryption errors that may be present in all software used in information systems may cause the control of a computer system to be taken over or that computer to run in an unexpected way. Such attacks are called code exploit. As CGI programs are "executable" codes, others can execute a program on your system easily. Therefore, CGI codes are kept in private places on the system and under the control of the officials of that system.

Today's software firms have acknowledged the importance of security and started to increase their investments and efforts on the subject. How data communicated via a network or channel is intervened with and retrieved by malicious third parties is called eavesdropping. In this attack type, the data retrieved on its way from source to target can even be changed. Denial of service is an attack performed differently from those that try to have unauthorized access or seize the system control. The only goal of this attack is to render the system inoperable by bearing load on a computer, server or network more than it can take.

Indirect attacks include different types of attack started from a third-party computer which has been taken over remotely. Using another computer, also called zombie computer, in the attack makes it difficult to identify the actual source of attack. Methods that enable the person, who elude normal authentication processes in such a way that cannot be found with ordinary examinations on the computer or who is informed of this structure, to have remote access to that computer are called backdoor. A backdoor may be in the form of an installed program as well as may have been left in an existing legitimate program itself by the very person who wrote it. In these attacks, trojan horse programs are intensively used. (Dilek & Özdemir, 2014); (Bostancı, 2015)

Attacks performed by a person who has physical access to a computer system are defined as direct access attacks. The person who gain physical access to the computer may make alternations such as defining a user on the operating systems for himself which can be used in the future and install software worms, keystroke logging systems and hidden listening devices on the system. The attacker who has direct access can also copy large amount of data to his side by using backup units, memory cards, digital cameras, digital audio systems, mobile phones and wireless/infrared devices. (Aslanbakan, 2016); (Lewy, 2015)

Various events regarding the security which is encountered on computer systems occurs when human factor comes into play deliberately or knowingly. Social engineering in computer security is the general name attributed to the techniques of acquiring the necessary information to access the system by using psychological and social tricks on legitimate users who use or administrate the computer system. The typical example to this is acquiring user and password details via telephone. The hacker can obtain such information from system administrators like an ordinary company user. Several tactics can be thought of in this case and the most important thing to do to survive all those tactics without suffering is educating the users constantly and system administrators and all users applying the security policies without exception. (Singer & Friedman, 2015)

Attacks performed for breaking or decrypting password of encrypted information are called cryptographic attacks. These attacks are carried out with crypto-analysis methods. They include brute force attacks, dictionary attacks, man-in-the-middle attacks, and attacks of chiper text only, known plaintext, chosen plaintext, chiper text, adaptive chosen plaintext, and related key attack.

DİSCUSSİON

In the light of all these considerations, customized records and customized applications have become an integrated part of information security due to running in mobile environments. Medical devices to be designed or developed in compliance with security requirements would contribute to the protection of personal health data and enhance the quality of usage.

The fact that security is not neglected should be emphasized when integrating the latest technology with the system in mobile health. When setting strategic plans and processes and defining tactics, organization's system must be protected and secured. For example, the glasses as a wearable technology product used by a doctor attending to a patient in intensive care unit or in a critical treatment can broadcast the whole process to patient's relatives. Hence, the relatives can be satisfied via state-of-art technology whereas risks pf accessing several corporate or personal data emerge because general computer networks intermediate this communication. (Akbulut & Akan, 2015); (Carreiro, 2014)

When examining the studies on corporate information security, it is seen that rather technology-based elements are rather taken into account and research is made on information security management systems, information security problems, risk assessment and trainings for awareness of information security. In health enterprises or mobile health applications, one needs to go beyond this approach and personal data should be able to be shared by authorized personnel and all communication and measurement devices used meanwhile should be included in the scope of security.

In the light of all these approaches, researchers are to be more skeptical to go beyond the elements of information security management in health which are involved only within the standards. The whole structure starting from the sensors required by wearable technology to the networks on which health information systems run need to be included within the scope. Importance should be attached to the research on measuring administrators' awareness.

CONCLUSİONS

Consequently, it should be accepted that high-level information and computer system security is not a product but a process. One needs to determine in this process that security is not a technical issue but a human and management problem. This approach should be taken into account all the time. One should take notice of attacks on computer systems and methods used in those attacks, security elements targeted by attacks, characteristics of attacks, vulnerabilities and weaknesses targeted by attacks, attacker profile, and factors prompting attackers to attack and take preventive measures by applying the systematic approaches as addressed above.

As for the studies of information security in health, the primary objectives should be to set the legal legislation, prepare strategies, policies and plans, proliferate education and enhance awareness, train qualified personnel on information security, improve technological infrastructures, carry out research and development studies and ensure cooperation between governmental bodies and private sector.

REFERENCES

1. Akbulut, F. P., & Akan, A. (2015). Smart Wearable Patient Tracking Systems. Tıp Teknolojileri Ulusal Kongresi (pp. 440-443). Muğla: IEEE Xplore Digital Library.
2. Arslan, B., & Sağıroğlu, Ş. (2016). Mobil Cihazlarda Biyometrik Sistemler Üzerine Bir İnceleme [A Review on Biometric Systems Used in Mobile Devices]. Politeknik Dergisi [Journal of Polytechnic], 19(2), 101-114.
3. Aslanbakan, E. (2016). Bilgi Güvenliği ve Uygulamalı Hacking Yöntemleri (1. ed.). İstanbul: Pusula Yayıncılık ve İletişim.
4. Aydan, S., & Aydan, M. (2016). Sağlık Hizmetlerinde Bireysel Ölçüm ve Giyilebilir Teknoloji:Olası Katkıları, Güncel Durum ve Öneriler. Hacettepe Sağlık İdaresi Dergisi, 19(3), 325-342.
5. Bali, R. K., & Dwivedi, A. N. (Eds.). (2007). Healthcare Knowledge Management Issues, Advances and Successes. 10013 New York, USA: Springer Science + Business Media LLC.
6. Bostancı, E. (2015). Medical Wearable Technologies: Applications, Problems and Solutions. Tıp Teknolojileri Ulusal Kongresi (pp. 549-582). Muğla: IEEE Xplore Digital Library.
7. Canberk, G., & Sağıroğlu, Ş. (2007). Bilgisayar Sistemlerine Yapılan Saldırılar Ve Türleri: Bir İnceleme [Attacks Agaınst Computer Systems And Theır Types: A Revıew Study]. Erciyes Üniversitesi Fen Bilimleri Enstitüsü Dergisi(23), 1-12.
8. Carreiro, S. (2014, ekim). Real-Time Mobile Detection of Drug Use with Wearable Biosensors: A Pilot Study. Journal of Medical Toxicology.
9. Dilek, S., & Özdemir, S. (2014). Sağlık Hizmetleri Sektöründe Kablosuz Algılayıcı Ağlar. Bilişim Teknolojileri Dergisi, 7(2), 7-19. doi:10.12973/bid.2016
10. Graham, C. (2014, 09 30). Study: Wearable Technology & Preventative Healthcare. Retrieved 01 25, 2017, from http://technologyadvice.com/blog/healthcare/study-wearable-technology-preventative-healthcare/
11. Keser, H., & Güldüren, C. (2015). Bilgi Güvenliği Farkındalık Ölçeği (BGFÖ) Geliştirme Çalışması [Development Of Information Security Awareness Scale]. K. Ü. Kastamonu Eğitim Dergisi, 3(23), 1167-1184.
12. Laudon, K. C., & Laudon, J. P. (2014). Management Information Systems Managing the Digital Firm (13th ed.). Edinburgh Gate Harlow, England: Pearson Education Limited.
13. Lewy, H. (2015). Wearable technologies: future challenges for implementation in healthcare service. Healthcare Technology Letters, 2, 2-5.
14. OBP. (2017). Health informatics -- Information security management in health using ISO/IEC 27002. (T. C. informatics, Editor) Retrieved 04 21, 2017, from ISO - International Organization for Standardization - Online Browsing Platform: https://www.iso.org/standard/62777.html
15. Özgü Can, E. S. (2016). Nesnelerin İnterneti ve Güvenli Bir Sağlık Bilgi Modeli Önerisi. Alanya - Antalya: Published in 4th International Symposium on Innovative Technologies 2016.
16. PWC Health Research Institute. (2014). Health Wariables: Early Days. Retrieved 01 25, 2017, from www.pwc.com: http://www.pwc.com/en_US/us/health-industries/top-health-industry-issues/assets/pwc-hri-wearable-devices.pdf
17. Singer, P. W., & Friedman, A. (2015). Siber Güvenlik ve Siber Savaş. Etimesgut / ANKARA: Buzdağı Yayınevi.
18. Sözen, A. (2014, 11 17). Kendini Ölçüm Sağlık Sektörünü Değiştirecek. Retrieved 01 25, 2017, from www.tekdozdijital.com: http://www.tekdozdijital.com/kendini-olcum-saglik-sektorunu-degistirecek.html
19. Sultan, N. (2015). Reflective thoughts on the potential and challenges of wearable technology for healthcare provision and medical education. International Journal of Information Management, 35, 521-526.
20. Terkeş, N., & Bektaş, H. (2016). Yaşlı Sağlığı ve Teknoloji Kullanımı. Dokuz Eylül Üniversitesi Hemşirelik Fakültesi Elektronik Dergisi, 9(4), 153-159.