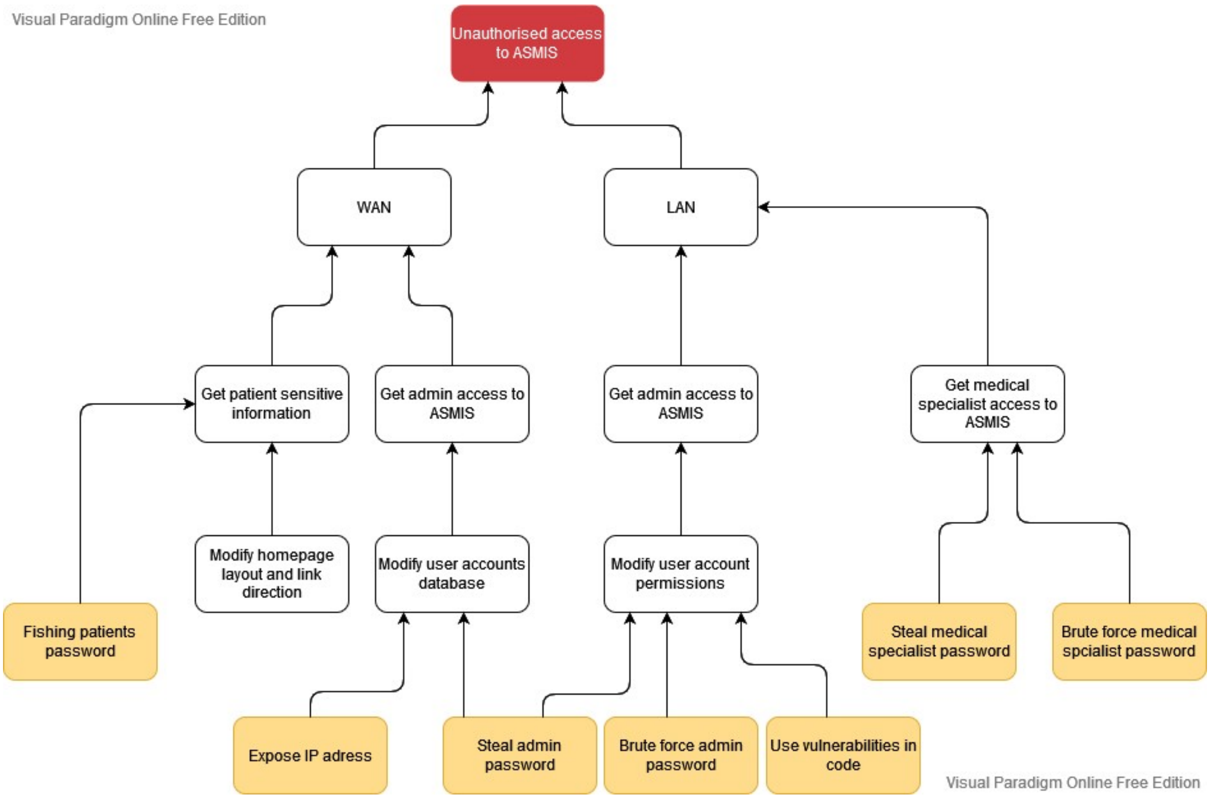
An essay on the advantages, potential problems and potential cyber threats of an ASMIS using the example of the Queens medical center

The appointment and scheduling management information system (ASMIS) is a web-based system that allows potential patients to schedule a doctor's appointment online. The ASMIS is intended to make appointments over the Internet, which relieves the burden of making appointments over the phone and in person. The advantages, potential problems and potential cyber threats for the system are analysed below.

The ASMIS enables a large number of simultaneous appointments to be made and changed over the Internet, which means that patients can contact the clinic in person and by telephone as an additional login option. By moving appointments to the Internet, the reception is relieved so that as many people as possible can get a doctor's appointment without having to increase the reception staff. Through the ASMIS, patients are automatically assigned to the responsible medical specialists related to their concerns and can choose an appointment based on availability. Studies suggest that choosing an appointment independently leads to fewer patients not showing up (Graham et al., 2020). It also creates a better bond with existing patients. The ASMIS also enables optimal coordination of the specialists, as the system selects the right and available specialist based on the patient's concerns and assigns them for the treatment. On the basis of the data collection, particularly frequent medical problems can be examined and, in combination with the volume of appointments, the future medical staff required can be determined. Since an internal medical record about the patient is stored in the system, doctors from other medical specialties can gain insight into the patient's treatment history, which enables better drug treatment of the people without having to physically request a medical record. This saves staff time and effort. Patients, on the other hand, can book an appointment regardless of time and place, which increases the attractiveness of the clinic. Deaf patients who are unable to make appointments by telephone are given the option of booking appointments without any problems, so that disabled-friendly access to medical treatments is made possible. Patients can be provided with a free appointment reminder service via email or SMS, so that they do not accidentally miss an appointment. In addition to the many advantages and optimization options mentioned, which an ASMIS enables, there are also potential risks and problems that must be taken into account.

First of all, it should be noted that despite increasing networking and availability of the Internet, not all potential patients have access to the Internet and therefore other contact options must be available to get in contact with the clinic. A potential lack of trust in the system must also be considered on the side of the patient. Due to increasing number of cyber attacks, especially in the medical field, concerns of patients regarding the security of the ASMIS are to be expected and also not completely unfounded (Davis, 2021). Past examples show that cyber attacks pose a serious threat, particularly in the health sector. For example, a cyber attack on a hospital in Germany resulted in one death (Silomon, 2020). As the ASMIS shifts patient registration, appointment scheduling and contact with the clinic to servers, the servers represent a growing source of danger with regard to the smooth flow of medical treatment. A failure of the server would mean that potential patients would not be able to make an appointment. Existing appointments would also be at risk, as the medical staff would not have any insight into existing appointments and the patient's medical files. In addition to cyber threats, which could result in this and will be discussed in the following, physical dangers also represent a potential threat. Natural disasters such as floods or fires can damage the IT infrastructure, which can impair the web-based system or, in the worst case, fail. Software errors also represent a potential risk. Incorrect configuration of the ASMIS can lead to complications in booking appointments, especially at the beginning, due to appointments that are not saved or that are incorrectly recorded. Medical records cannot be stored properly or they can be difficult to access by medical personnel. A loss of information could make it more difficult to treat the patient or even result in health risks for the patient.

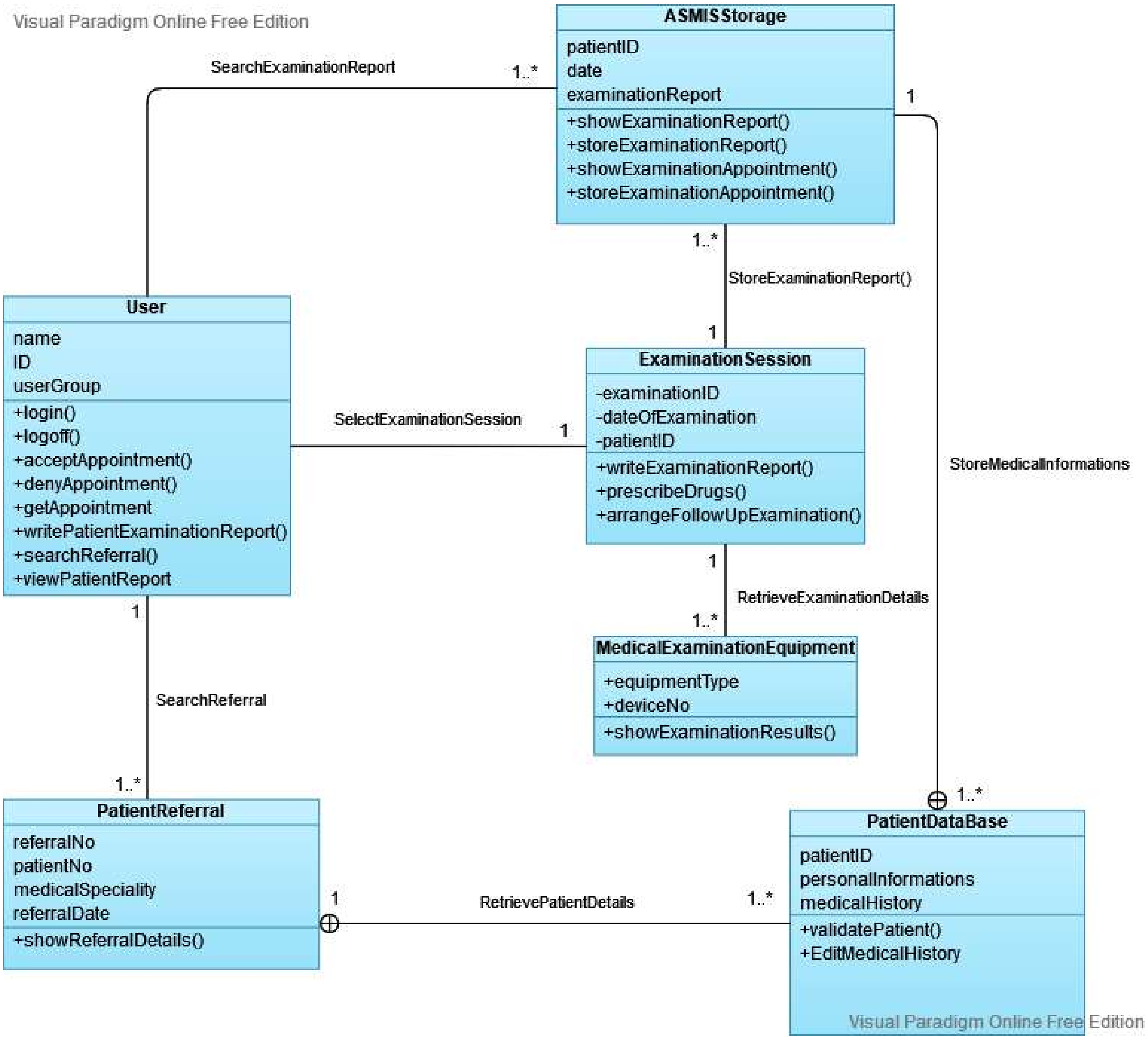
A particularly serious aspect are security problems regarding to data security. The General Data Protection Regulation (GDPR) of the European Union form the framework for the secure handling of the user data collected by companies. Companies under whose definition the clinic falls are obliged to protect the patient's personal data from unauthorized access (The European parliament and the council, 2016). A violation of the regulations can not only result in a loss of patient confidence, but also result in legal repression. In order to protect the ASMIS from cyber threats, these must first be recognized and analyzed. The STRIDE threat model, which was developed by Praerit Garg and Loren Kohnfelder at Microsoft, offers a structured approach, which shows the potential cyber threats (Khan et al.,2017). STRIDE stands for: spoofing, tampering, repudiation, information disclosure, denial of service and elevation of privilege. An example of possible security threats can be seen in the Attack Tree diagram below.


Visual Paradigm Online Free Edition
Unauthorised access to ASMIS
WAN
LAN
Get patient sensitive information
Get admin access to ASMIS
Get admin access to ASMIS
Get medical specialist access to ASMIS
Modify homepage layout and link direction
Modify user accounts database
Modify user account permissions
Fishing patients password
Steal medical specialist password
Brute force medical spcialist password
Expose IP adress
Steal admin password
Brute force admin password
Use vulnerabilities in code
Visual Paradigm Online Free Edition

Attack Tree of the ASMIS

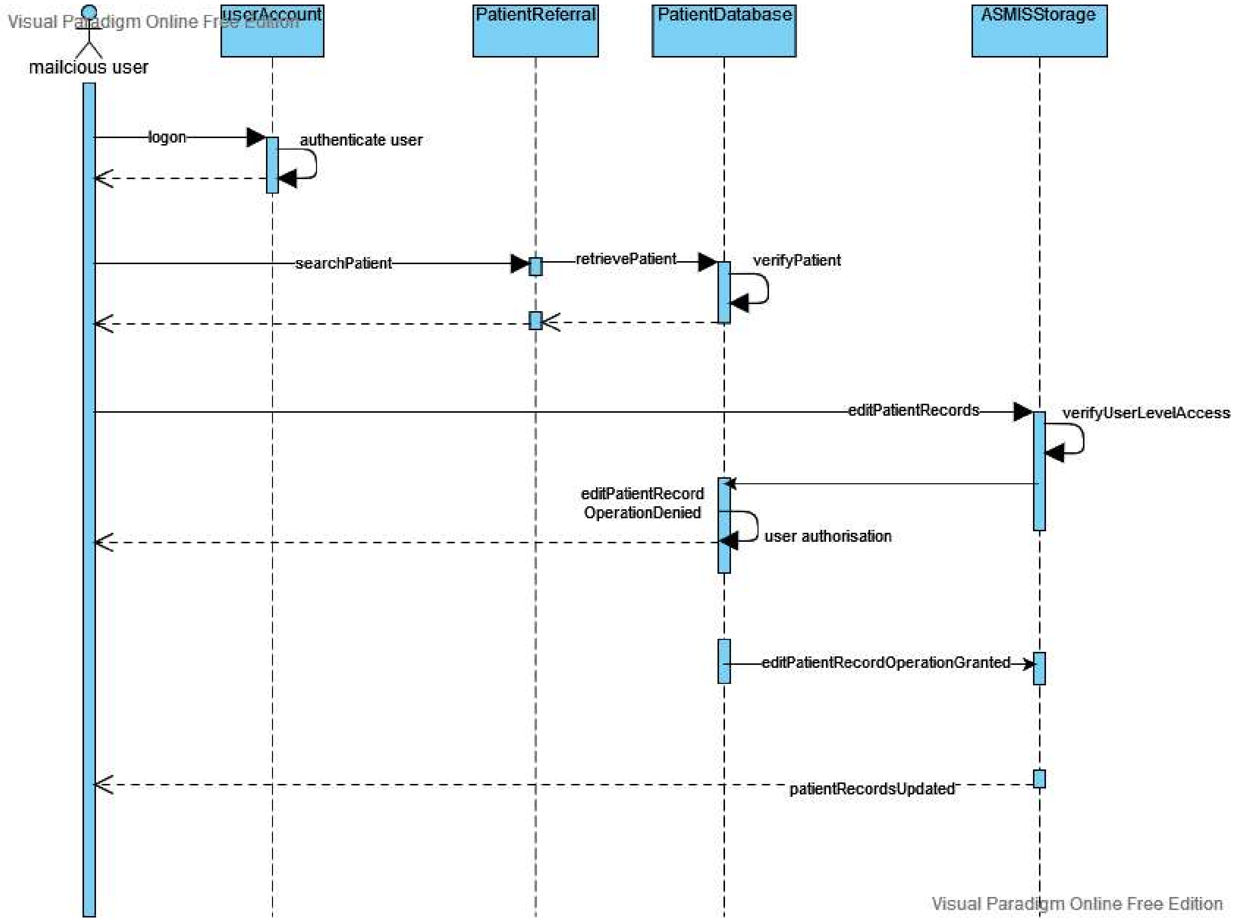
One way of gaining unauthorized access to sensitive patient data is spoofing. Here the access data of patients or the staff who have access to the data are stolen. In addition to local unauthorized access to this data by unguarded and not logged out computers in the clinic, this is done online by forging identities. The attackers try to pretend to be staff of the clinic in order to obtain access data via phishing mails, for example. Should the access data of the ASMIS administrators have been stolen through a phishing attack or other means, or the system is susceptible to a hacker's attack, unauthorized tampering can be carried out in the system, whereby the system becomes faulty or data can also be stolen. Since the communication between the ASMIS and the patient takes place over the Internet, hackers could try to intercept the data transmission in order to gain access to sensitive information of the patients or even their access data. The disclosure of information is therefore another aspect that must be taken into account when setting up an ASMIS. If intruders have found access to the system, there would be a serious risk that they could increase their permissions. In this way, the attackers could gain full access to the system and at the same time withdraw access authorization from the authorized administrators who maintain the system. Figuratively speaking, the clinic could be excluded from its own system. The data could also be encrypted, so that the staff would not have access to the diary and the patient's medical records. That this is a common practice to blackmail hospitals is shown by the ransomware attack known as GandCrab5.3 (Mednic, 2019). Since clinics deal with medical information that can determine the survival of patients, the attackers have a good starting position to blackmail medical facilities with payments. Denial of service (DoS) attacks represent another possibility of disrupting the smooth running of the ASMIS. Here, the servers of the system are flooded with false requests, which means that the patients can no longer connect to the system. Even if the system is protected as optimally as possible, absolute security can never be guaranteed. It must be assumed that a new security hole will be found by hackers for which there is no protection yet. Such attacks, known as zero day exploits, must then be closed by programmers. Until then, the system is vulnerable to attack. The human factor also plays an important role in security. Even an optimally protected system is susceptible to human error. In order to be able to trace interventions and attacks on the system, audits are implemented, which log a harmful intervention so that the source of the weak point can be found. For their part, hackers have an interest in ensuring that these vulnerabilities and their interventions remain undetected. This includes the aspect of the threat of rejection. Without a means of logging and tracking, it becomes much more difficult to detect malicious behavior. For example, a brute force attempt in which the attacker try to gain access to accounts by trying out passwords cannot be differentiated from accidentally entering a patient's password incorrectly.

In order to protect the ASMIS from unauthorized access, structures must be used which only allow the users of the ASMIS to access the respective necessary functions, by a precisely defined user policy. A possible structure of such a system can be seen in the structure model of the ASMIS.



Structure model ASMIS

The users can log in with their user data. However, they do not have the same permissions. While a patient can schedule, promise and cancel a meeting, a receptionist is able to access the patient referral to provide information over the phone or in person. A doctor, on the other hand, also has permission to access the examination session and the ASMIS storage. Furthermore, a doctor is able to access the medical examination equipment in order to obtain data. He can also enter comments on medical information in the patient database. This clear hierarchy of permissions is intended to guarantee that only necessary information is available for the respective users of the ASMIS. An example of use, which should clarify the safety aspects of this structure, is shown in the behavioral model.



Behavioral model ASMIS

If a malicious user tries to gain access to a patient account, the person must first authenticate. If the registration is incorrect, the request will be rejected. However, should the malicious user manage to gain access to the patient account, for example through brute force or successful spoofing, the person only has access to the patient's authorizations. The receptionists are located one authentication level higher. Here, too, a malicious user only needs to gain access if the person can authenticate himself with the necessary authorizations. From this level at the latest, it makes sense to implement a monitoring system that records from which IP address and under which user the access to the data took place, in order to be able to understand from where the cyber attack was carried out in the event of data theft or data manipulation. Using the access log, the weak points in the system can be identified and eliminated in the next step. Access to the ASMIS memory should only be reserved for doctors, as only they need access to the highly sensitive patient data. At this level of the security class, in addition to the general monitoring system, it is advisable to implement a recording system that records repeated failed login attempts and, if necessary, locks the account if too many failed attempts are made. In this way, excessive brute-force attempts by attackers can be repelled. A strict rejection policy is necessary because if the system is successfully accessed, the user has the option of tampering and thus presents massive dangers for the patient.

In order to minimize the damage in a successful tampering in which the data has been maliciously changed or encrypted, a system is recommended that saves backups at regular intervals. In this way, the maliciously manipulated data record can be reset at an earlier point in time (Ayala, 2016). A “honey-pot” server is also a recommended implementation in the ASMIS (Moore, 2016). This is an extra server that is particularly weakly protected in order to get an attacker to access it. The honeypot server contains alleged information that the attacker would like to access, but which is generated generically and does not correspond to the correct data of the ASMIS. There is also tracking software on the server, which enables the attacker to be traced back.

It can be concluded that the ASMIS offers advantages for the clinic and the patients in many respects, by saving personnel and planning possibilities for the needs of future personnel, a bundling of information in a central system and service for the customers. However, the system also provides the basis for potential dangers in terms of data security and its availability. In order to protect the system from malicious interventions, it is advisable to implement a clear hierarchy with regard to user authorizations in order to only allow necessary access by the respective user. Regular backups can reduce the risk of data loss. Finally, a honey-pot server and the recording of accesses to the ASMIS enable weak points to be traced.

References:

Ayala, L. (2016) Cybersecurity for Hospitals and Healthcare Facilities. Fredericksburg: Springer.

Davis, J. (2021) Ransomware Keeps Healthcare in Crosshairs, Triple Extortion Emerges. Health IT Security. Available from: https://healthitsecurity.com/news/ransomware-attacks-surge-102-in-2021-as-triple-extortion-emerges [Accessed: 02.10.2021]

Graham, T., Ali, S., Avdagovska, M. & Ballermann, M. (2020) Effects of a Web-Based Patient Portal on Patient Satisfaction and Missed Appointment Rates: Survey Study. J Med Internet Res 22(5): e17955. Available from: https://www.jmir.org/2020/5/e17955 [Accessed: 29.09.2021]

Khan, R., McLaughlin, K., Laverty, D. & Sezer, S. (2017) STRIDE-based threat modeling for cyber-physical systems. IEEE PES Innovative Smart Grid Technologies Conference Europe (ISGT-Europe). Available from: https://ieeexplore.ieee.org/abstract/document/8260283 [Accessed: 30.09.2021]

Mednic Redaktion (2019) Erpressungstrojaner verschlüsselt Krankenhaus-Daten. mednic. Available from: https://mednic.de/erpressungstrojaner-verschluesselt-krankenhaus-daten/11920 [Accessed: 04.10.2021]

Moore, C. (2016) Detecting Ransomware with Honeypot Techniques. Cybersecurity and Cyberforensics Conference (CCC). Available from: https://ieeexplore.ieee.org/abstract/document/7600214 [Accessed: 04.10.2021]

Silomon J. (2020) The Düsseldorf Cyber Incident. Institute for Peace Research and Security Policy. Available from: https://ifsh.de/en/news-detail/the-duesseldorf-cyber-incident [Accessed: 29.09.2021]

The European parliament and the council (2016) Regulation (EU) 2016/679 of the European parliament and of the council of 27 April 2016. Available from: https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32016R0679 [Accessed: 04.10.2021]