,

Hochschule für Technik
und Wirtschaft Berlin

University of Applied Sciences

Hochschule für Technik und Wirtschaft Berlin

Fachbereich IV

Professional IT Business and Digitalization

Masters Course M23 IT-Security

Summer 2023

GREEN HEALTH

Sharanya Adiga

GREEN HEALTH

Sharanya Adiga

July 15, 2023

Contents

Chapter 1: Abstract

This case study delves into the critical importance of cybersecurity measures in an Electronic Health Records (EHR) system. EHR systems have become indispensable in modern healthcare as they store and manage sensitive patient information while facilitating seamless data sharing among healthcare providers. However, their increased adoption has made them prime targets for cyberattacks.

The case study focuses on the cybersecurity challenges encountered by a healthcare organization in safeguarding their EHR system. These challenges encompass the potential risks associated with unauthorized access to patient data, data breaches, system vulnerabilities, and the need for secure data sharing among authorized healthcare providers.

To address these challenges, the case study explores the implementation of robust cybersecurity measures. These measures encompass various aspects such as user authentication, access control management, data encryption, network security, incident response, audit and monitoring, and vendor management. Each of these components plays a vital role in establishing a secure EHR system environment.

By implementing stringent cybersecurity measures, the healthcare organization aims to protect patient privacy, maintain the integrity of medical records, and ensure the confidentiality of sensitive data. Moreover, these measures aim to mitigate the risks associated with cyberattacks and unauthorized access attempts, ultimately ensuring the seamless and secure functioning of the EHR system.

The case study serves as a valuable resource for healthcare organizations facing similar challenges, offering insights into effective cybersecurity strategies and emphasizing the importance of proactive measures to safeguard EHR systems.

Chapter 2: Introduction

2.1 System Overview: The system in this case study refers to the Electronic Health Records (EHR) system implemented within a healthcare organization. The goal of the system is to securely store, manage, and share patient health information electronically, improving the efficiency and quality of healthcare services.
The Basic functionalities includes:

- Data Storage: The system securely stores patient health information, ensuring data integrity and confidentiality.
- Data Access and Retrieval: Authorized healthcare providers can access and retrieve patient records from the EHR system, allowing for quick and comprehensive access to relevant medical information.
- Data Sharing and Interoperability: The system enables the secure exchange of patient data between different healthcare providers, promoting seamless coordination and continuity of care.
- Decision Support: The system may provide clinical decision support tools, such as alerts for incident response aiding healthcare providers in making informed decisions.

Different Components and their purposes:

- External Entities:
  Healthcare Providers: Access and utilize the EHR system to provide patient care.
  Patients: Have their health information stored within the EHR system.
  Third-Party Vendors: Provide services or integrations with the EHR system.
- Processes:
  User Authentication: Verifies and authenticates user identities before accessing the EHR system.
  Access Control Management: Manages user permissions and access levels within the EHR system.
  Data Encryption: Applies encryption algorithms to protect sensitive data at rest and in transit.
  Incident Response: Handles cybersecurity incidents, from identification to mitigation.
- Data Stores:
  Electronic Health Records (EHR): Stores patient health information.
  User Accounts and Permissions: Contains user credentials, access privileges, and roles.
  Incident Reports: Stores details of cybersecurity incidents and their resolution.
- Data Flows:
  Patient Data Flow: Represents the flow of patient information within the EHR system, such as data entry, retrieval, and updates.
  User Authentication Flow: Represents the process of user authentication and verification before accessing the EHR system.
  Data Encryption Flow: Illustrates the encryption and decryption of sensitive data within the EHR system.
  Incident Reporting Flow: Depicts the reporting and handling of cybersecurity incidents, including notification and response.

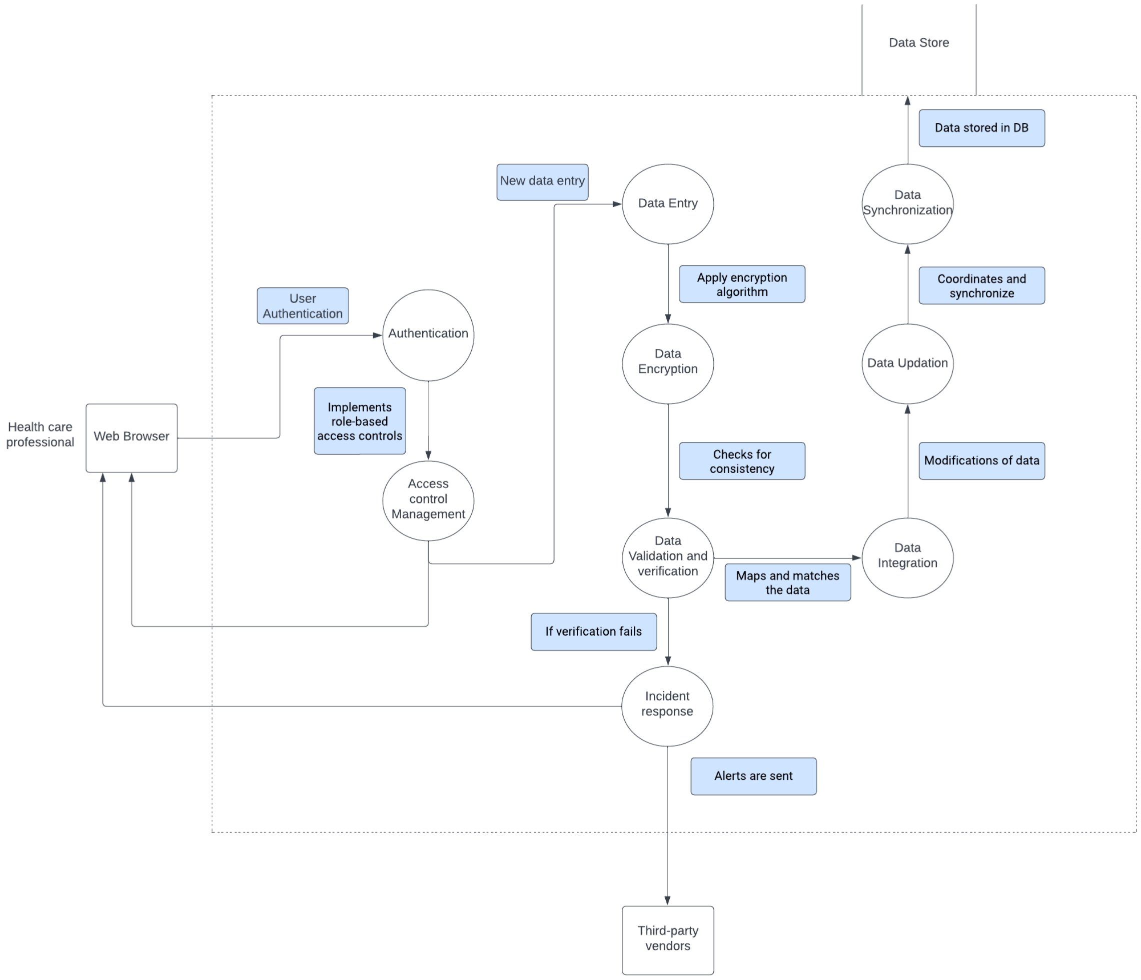


Figure 1: DFD - Green Health

This DFD represents the movement of patient information within the EHR system. It encompasses various activities such as data entry, retrieval, and updates. When a patient's information is entered into the system, it flows through different modules and functionalities, allowing healthcare providers to access and update the data as necessary. This flow ensures that patient data is readily available for authorized users, facilitating efficient healthcare delivery and continuity of care.

The user authentication flow outlines the process by which users are verified and authenticated before accessing the EHR system. When a user attempts to log in, their credentials are validated through authentication mechanisms such as usernames, passwords, and possibly additional factors like biometric data or security tokens. This flow ensures that only authorized individuals can access the system, protecting patient data from unauthorized access and maintaining system security.

The data encryption flow represents the encryption and decryption of sensitive data within the EHR system. When data is transmitted or stored, encryption algorithms are applied to convert the data into an unreadable format using encryption keys. This ensures that even if the data is intercepted, it remains unintelligible to unauthorized entities. The flow encompasses the encryption of data before transmission and its subsequent decryption upon receipt or retrieval. Data encryption provides a vital layer of protection, safeguarding patient information from unauthorized access and maintaining its confidentiality.

The incident reporting flow depicts the reporting and handling of cybersecurity incidents within the EHR system. When a cybersecurity incident occurs, such as a data breach or unauthorized access attempt, it is essential to have a structured process in place to report and respond to the incident. This flow encompasses the notification of relevant parties, including system administrators, security teams, and possibly regulatory authorities. It also involves the steps taken to analyze the incident, mitigate any damage, and implement measures to prevent similar incidents in the future.

Chapter 3: Threat Analysis

The Threat Modeling Tool [Sho14] is used by software architects to identify and mitigate potential security issues.Threat modeling(TM) is the process that improves application and network security by identifying and rating the potential threats and vulnerabilities in the EHR system.We have used STRIDE to analyze threats.

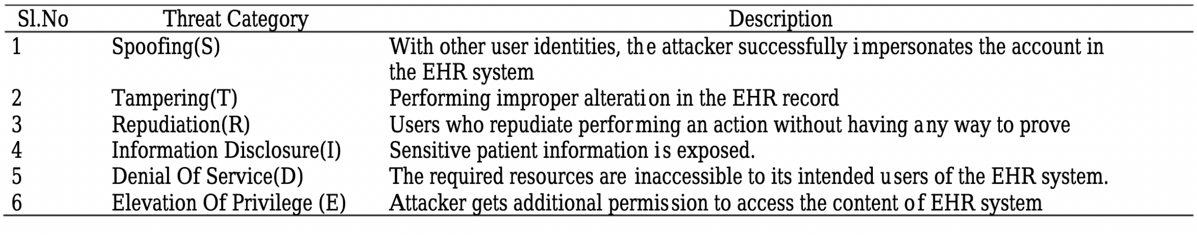
The threat of personnel identity loss or identity sharing, leading to spoofing, poses a high risk to the security of the EHR system. Healthcare providers and system administrators may inadvertently leave their login credentials in public places or intentionally share them with unauthorized individuals. This can enable attackers or malicious insiders to impersonate legitimate users and gain unauthorized access to the EHR system.

TM is especially important during the design phase. TM allows experts to determine the possible threats that could affect the system. The DFD designed for EHR system is given as input to the threat model to identify threats. Identifying threats helps to develop meaningful security model for cloud-based EHR. Threats exist due to weaknesses in design, implementation or configuration. These threats are identified by a systematic review of the system and identifying the intruder access points to eliminate the threats.

Why STRIDE??

The STRIDE model provides a comprehensive coverage of potential threats relevant to the EHR system. This ensures that a wide range of potential threats is considered during the analysis, leaving minimal gaps in threat identification. It also provides a structured framework for analyzing threats, making it easier to understand and apply. It offers a clear categorization of threats, allowing organizations to systematically evaluate each threat category within the context of their EHR system. It can be effectively integrated with other security frameworks and control frameworks, thus enhancing the overall cybersecurity posture of the EHR system and ensures a more holistic approach to risk mitigation.

The possible threat category list [HHS20] for the EHR system is shown below.



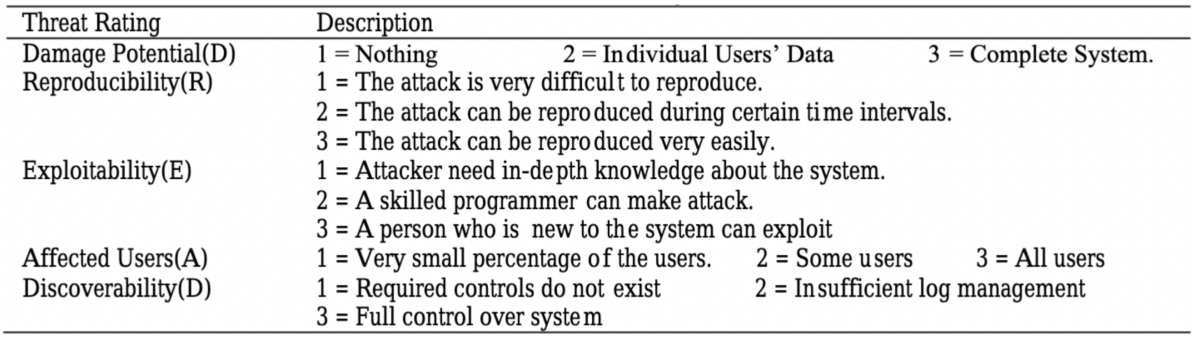
Sl.No	Threat Category	Description
1	Spoofing(S)	With other user identities, the attacker successfully impersonates the account in the EHR system
2	Tampering(T)	Performing improper alteration in the EHR record
3	Repudiation(R)	Users who repudiate performing an action without having any way to prove
4	Information Disclosure(I)	Sensitive patient information is exposed.
5	Denial Of Service(D)	The required resources are inaccessible to its intended users of the EHR system.
6	Elevation Of Privilege (E)	Attacker gets additional permission to access the content of EHR system

Figure 2: Threat list for EHR System

The threats include exposing, altering and/or destroying health information which completely damages the system.

Chapter 4: Risk Analysis

The identified threats are ranked using DREAD. The DREAD is an acronym formed from the first letter of each category of threat namely Damage Potential, Reproducibility, Exploitability, Affected users, Discoverability. The risks are rated over the DREAD scheme with numerical values of 3, 2, and 1. The threat rating scheme is shown below.

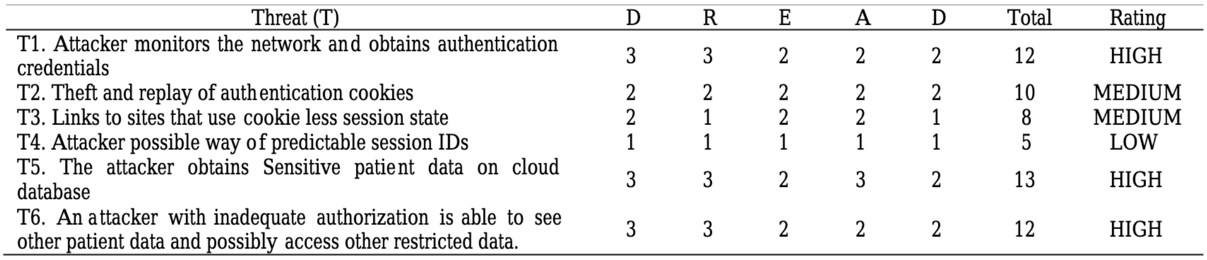


Threat Rating	Description
Damage Potential(D)	1 = Nothing 2 = Individual Users' Data 3 = Complete System.
Reproducibility(R)	1 = The attack is very difficult to reproduce. 2 = The attack can be reproduced during certain time intervals. 3 = The attack can be reproduced very easily.
Exploitability(E)	1 = Attacker need in-depth knowledge about the system. 2 = A skilled programmer can make attack. 3 = A person who is new to the system can exploit
Affected Users(A)	1 = Very small percentage of the users. 2 = Some users 3 = All users
Discoverability(D)	1 = Required controls do not exist 2 = Insufficient log management 3 = Full control over system

Figure 3: Threat rating scheme

The DREAD equation used to compute a risk value, which is the mean of all five categories is Shown as Risk = (D+R+E +A+D) / 5.

The computed risk value is categorized as low (0 to 6), medium (7 to 11) or high (12 to 15) based on the impact the threat possesses to the EHR system. DREAD uses the standard scale for computing High, Medium and Low to rate the threat. When threat is high, it means it needs to be resolved by implementing appropriate countermeasures. The computed risk for the identified threats for the system is shown as:



Threat (T)	D	R	E	A	D	Total	Rating
T1. Attacker monitors the network and obtains authentication credentials	3	3	2	2	2	12	HIGH
T2. Theft and replay of authentication cookies	2	2	2	2	2	10	MEDIUM
T3. Links to sites that use cookie less session state	2	1	2	2	1	8	MEDIUM
T4. Attacker possible way of predictable session IDs	1	1	1	1	1	5	LOW
T5. The attacker obtains Sensitive patient data on cloud database	3	3	2	3	2	13	HIGH
T6. An attacker with inadequate authorization is able to see other patient data and possibly access other restricted data.	3	3	2	2	2	12	HIGH

Figure 4: Risk computation for EHR using DREAD

The result indicated the high possible threats associated with user authentication and authorization whereas theft and replay of authentication cookies and link to the site of those cookies are found with medium threats. The result also indicated that prohibited users can gain unauthorized access to the EHR system by spoofing the login credentials. This threat may lead to the sharing of patient's personal and health-related data in an unauthorized manner that may result in information misuse, information disclosure, and altering information.

Chapter 5:Security Controls - Encryption

Before discussing security Controls some prior assumptions about security are needed. Security assumptions are needed to provide a foundation for designing and implementing security measures within the EHR system. They help establish a baseline understanding of the security posture and set expectations for how the system will operate and protect sensitive data.Security assumptions allow organizations to identify and address potential risks and vulnerabilities this helps to achieve Risk Management. It enables organizations to prioritize security measures, allocate resources appropriately, and establish a roadmap for implementing security controls also helps in decision making.

To enhance the features for the secure access and storage of patient data, Administrative, Physical, and Technical security standards are included in the proposed system. We mainly focus on Authentication and Authorization as security goals and this can be achieved using Cryptography which enables strong authentication mechanisms that verify the identities of communicating parties. Through techniques like public key infrastructure (PKI), and cryptographic protocols like Transport Layer Security (TLS), cryptographic mechanisms can establish trust and authenticate the identities of entities involved in communication, reducing the risk of impersonation or unauthorized access.

The OSI model presentation layer is responsible for communication with regard to authentication. Presentation Layer is the optimal for applying cryptography, reasons being end to end encryption and Data Agnostic, this ensures that the sensitive patient health information remains encrypted throughout transmission, protecting it from unauthorized access or interception [BM13].

5.1 Security Control - Password Security

As the study of EHR databases in the medical field, To alter patients data first need to enter the system. It's important to note that use of password to enter the system would be necessary.To persist passwords in the system here I have used salting technique [GPS20] for authentication of the passwords. Some of the reasons to choose salting techniques or benefits of this technique are increased password complexity,protection against rainbow table attacks, defense against dictionary attacks,unique password hashes,added security in case of Data Breaches.

Passwords serve as a form of authentication, verifying the identity of users before granting access to the system. This helps ensure that only authorized individuals can access the EHR system and mitigates the risk of unauthorized access or data breaches. So while selecting a password it should have some policies. In this study as its crucial it's necessary to have some password policies namely its complexity,expiration and history, Account lockouts. The strength of these passwords can be measured by its length,entropy, character variety,or using password crackers.

Password Complexity: Implementing a password complexity policy is essential to ensure that passwords are sufficiently strong and resistant to guessing attacks. The policy should require a combination of uppercase and lowercase letters, numbers, and special characters.

Enforcing a minimum password length and prohibiting the use of easily guessable or common passwords is also important.

Password Expiration: Regularly expiring passwords reduces the risk of compromised credentials. Implement a password expiration policy that requires users to change their passwords at regular intervals. This practice helps ensure that even if a password is compromised, it becomes less useful over time.

Password History and Reuse: Enforce a password history policy that prevents users from reusing previous passwords. This prevents users from cycling through a set of known passwords and enhances the overall security of the authentication process.

Account Lockouts: Implement account lockout mechanisms to protect against brute-force attacks. If an attacker repeatedly enters incorrect passwords, the account should be temporarily locked or disabled to prevent further login attempts. This control helps mitigate the risk of automated password guessing attacks.

Two-Factor Authentication (2FA): Implementing two-factor authentication adds an extra layer of security to the authentication process. In addition to a password, users are required to provide a second form of verification, such as a unique code generated by a mobile app or received via SMS. This control significantly strengthens the authentication process and reduces the risk of unauthorized access.

Password Storage: Passwords should never be stored in plaintext. Instead, they should be securely hashed and salted using strong cryptographic algorithms. Salting adds random data to the password before hashing, making it more resistant to pre-computed attacks. Hashed passwords are one-way transformations, ensuring that even if the password database is compromised, the original passwords cannot be easily obtained.

Password Education and Training: Provide user education and training on password security best practices. Users should be educated on creating strong passwords, avoiding password reuse, and safeguarding their passwords from unauthorized disclosure. Regular reminders about password security and phishing awareness can significantly enhance the overall security posture.

Multi-Factor Authentication (MFA): Consider implementing multi-factor authentication, which combines something the user knows (password), something the user has (a physical token or mobile device), and/or something the user is (biometric data) for authentication. MFA provides an additional layer of security by requiring multiple forms of verification, making it significantly harder for attackers to gain unauthorized access.

Password Management: Encourage the use of password managers, which securely store and generate unique passwords for each user account. Password managers eliminate the need for users to remember multiple complex passwords and reduce the risk of weak or reused passwords.

Regular Auditing and Monitoring: Implement auditing and monitoring mechanisms to track and detect suspicious activities related to password authentication. This includes monitoring failed login attempts, detecting patterns of brute-force attacks, and regularly reviewing password-related logs for any anomalies or security incidents.

Single Sign-On (SSO) is user authentication service that permits EHR users to access multiple health services after signing in only once [Bel16]. When the user signs in, their identity is recognized and they need not sign in multiple times to access different types of health services. . Implementation of SSO is based on security assertion markup language (SAML). It is an XML based communication protocol for exchanging authentication information between the service provider and identity provider.

The salting technique, which is random data, is used as an additional input to the hash function. Without salting techniques, an intruder can precompute the rainbow tables of common password hashes and easily compare them to a database and see who used which common password. With rainbow table attack output of a hash function is always the same when the input remains the same. To make each hash password unique, random data is added to the input of the hash function. Below figure shows user interaction with the EHR database with salting technique [Sta12].

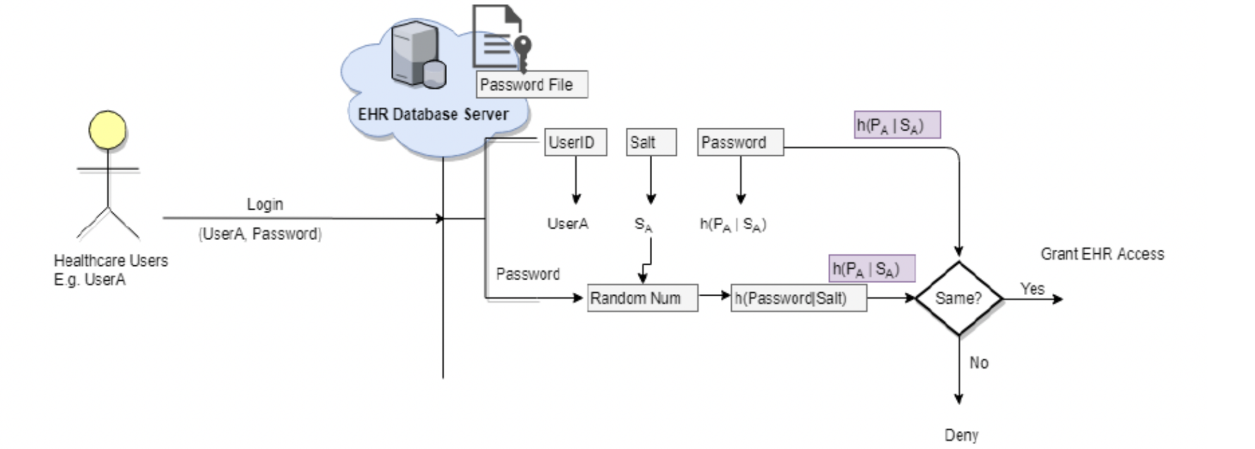


Figure 5: Salting method for authentication

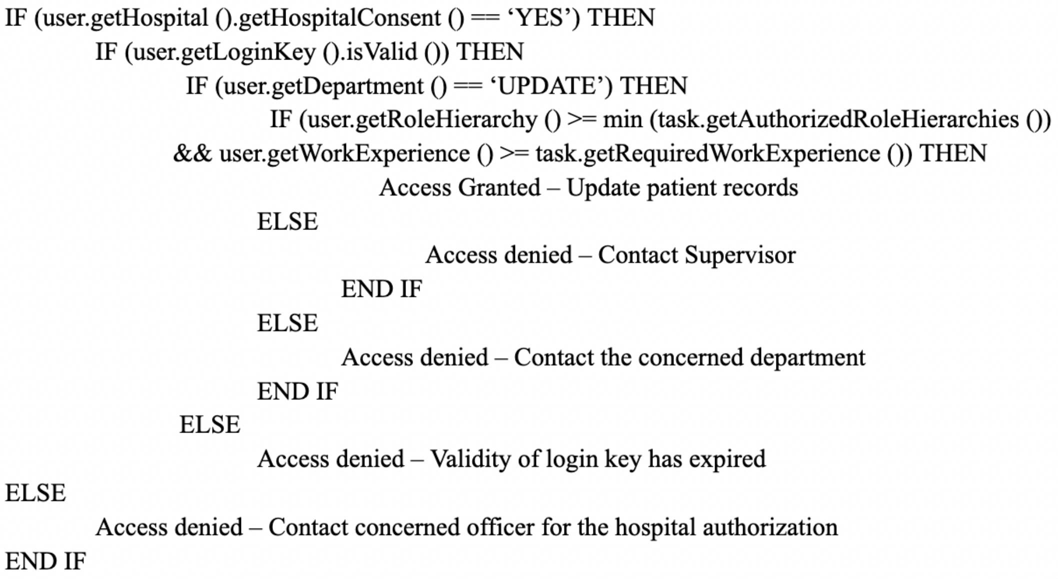
5.2 Security - Access control

The goal of the system is to securely store and manage data after successful authorization granting and denying access for the system is needed. Here an access control mechanism is introduced to enter the patient data into the system. In the system we have access control management as one of the processes where access control can be applied. Here I am using ABAC. When it comes to healthcare organizations, various factors can be considered as attributes. For example here patient data is considered. By using access control the altar of patients' data can be prevented.

Attribute-Based Access Control (ABAC), also known as PBAC defining access policies and authorizing access to resources and data based on certain attributes defined by the organizations [ZZD18][Seo+18]. Attributes can vary from organization to organization [10].

ABAC allows organizations to set a complex set of Boolean logic and conditions to ensure that access is provided if and only if all the conditions have been satisfied. The Pseudocode below shows the workflow of a user who wants to update patients' records.

Pseudocode:



```
IF (user.getHospital ().getHospitalConsent () == 'YES') THEN
        IF (user.getLoginKey ().isValid ()) THEN
                IF (user.getDepartment () == 'UPDATE') THEN
                        IF (user.getRoleHierarchy () >= min (task.getAuthorizedRoleHierarchies ())
               && user.getWorkExperience () >= task.getRequiredWorkExperience ()) THEN
                                  Access Granted – Update patient records
                      ELSE
                                      Access denied – Contact Supervisor
                              END IF
                      ELSE
                              Access denied – Contact the concerned department
                      END IF
               ELSE
                      Access denied – Validity of login key has expired
ELSE
        Access denied – Contact concerned officer for the hospital authorization
END IF
```

Figure 6: Pseudocode to update records

Here to update the records, work attributes like experience,hierarchy of the user are considered.Once a hospital has been authorized, the hospital policies come into play. If a user satisfies all the conditions and policies set by the healthcare organization that they are working in, then they are granted access to that patient's records.

This access control mechanism cannot be used in other components of the system as this component is main and asks for the roles access. Main reasons and benefits to support why I choose ABAC method are dynamic and context-aware access decisions and fine-grained access control where specific attributes are considered along with this access to certain patient records may depend on the user's role. Scalability and flexibility by allowing organizations to easily adapt access control rules by incorporating additional attributes or modifying existing ones. As mentioned above, policy-based enforcement is one of them to be mentioned.

Chapter 6:Network Security

Network security plays a vital role in protecting the EHR system from potential threats and ensuring the confidentiality, integrity, and availability of data. Implementing encryption protocols, such as Transport Layer Security (TLS) or Secure Sockets Layer (SSL), to secure data transmission over the network. Encryption ensures that sensitive information remains protected during transit, reducing the risk of unauthorized interception and data tampering.So by implementing this one can protect the data from getting breached.

SSL enables the authentication of the EHR system to the clients and vice versa. Through the use of digital certificates issued by trusted Certificate Authorities (CAs), SSL verifies the identity of the server, establishing trust and confidence that the clients are communicating with the intended, legitimate EHR system. SSL is often a requirement to comply with privacy and security regulations in the healthcare industry. Regulations such as the Health Insurance Portability and Accountability Act (HIPAA) in the United States or the General Data Protection Regulation (GDPR) in the European Union mandate the use of secure communication protocols like SSL/TLS to protect patient health information during transmission.

The use of SSL/TLS begins with obtaining an SSL certificate from a trusted Certificate Authority (CA) for the EHR system's domain. This certificate serves as proof of the server's identity and authenticity, establishing trust between clients and the system.

Once SSL/TLS is implemented, the communication between clients and the EHR system is protected through encryption. SSL/TLS employs strong cryptographic algorithms to encrypt data, making it unreadable to unauthorized entities. This prevents eavesdropping and unauthorized access to sensitive patient information during transmission.

SSL/TLS also ensures data integrity by employing mechanisms such as digital signatures or message authentication codes (MACs). These mechanisms allow the recipient to verify that the data received has not been tampered with or modified during transit. Any alteration to the data would result in an invalid signature or MAC, alerting the recipient to potential tampering attempts.

Moreover, SSL/TLS provides mutual authentication, allowing both the sides to verify each other's identities. This prevents spoofing attacks and ensures that the client is communicating with the legitimate EHR system. The client verifies the server's identity by validating the SSL certificate, while the server can request client certificates for additional verification.

SSL/TLS also mitigates the risk of data disclosure during transmission. By encrypting data using SSL/TLS, sensitive patient information remains protected even if it is intercepted by unauthorized individuals. This is particularly critical for an EHR system, where the privacy and confidentiality of patient health records must be maintained.

To implement SSL/TLS effectively, we should ensure proper SSL/TLS configuration. This involves selecting the appropriate SSL/TLS protocols and cipher suites, which should align with the latest security recommendations. Regular updates and patching of SSL/TLS libraries and configurations are essential to address any vulnerabilities and maintain a secure network environment.

The research community generally acknowledges the effectiveness and importance of SSL/TLS in providing secure communication channels. However, it is important to note that these protocols are continuously evolving to address emerging threats and vulnerabilities. Additionally, researchers explore emerging technologies like post-quantum cryptography and secure key exchange mechanisms to address future challenges and enhance the security of SSL/TLS.

Most of the apps related to the healthcare field use SSL security [GET22] which is sufficient to prove how this method would be effective.

Conclusion

Healthcare organizations are prime targets for attackers due to the valuable and sensitive information they possess. To ensure secure data sharing among multiple healthcare providers, an Electronic Health Records (EHR) Data Flow Diagram (DFD) is developed. Through the use of threat modeling techniques like STRIDE, potential threats to the EHR system are identified, and the risks they pose are calculated using DREAD. In order to mitigate these threats, a proposed solution includes authentication, authorization, and attribute-based access control to establish a secure EHR system.

The EHR DFD provides a visual representation of how data flows within the system, highlighting the various components and external entities involved. By understanding the flow of data, potential vulnerabilities and attack surfaces can be identified, allowing for targeted security measures to be implemented.

Using the STRIDE threat modeling framework, potential threats are classified into categories such as spoofing, tampering, repudiation, information disclosure, denial of service, and elevation of privilege. This comprehensive analysis helps prioritize the identified threats based on their potential impact on the system.

The DREAD risk assessment model is then applied to quantify the risks associated with the identified threats. By assessing factors such as damage, reproducibility, exploitability, affected users, and discoverability, a numerical score can be assigned to each threat, allowing for prioritization of mitigation efforts.

To mitigate these threats and reduce the associated risks, the proposed solution includes robust authentication mechanisms to verify the identity of users accessing the EHR system. This helps prevent unauthorized access and protects against spoofing attacks.

Authorization ensures that users have the appropriate permissions to access specific EHR data. By implementing proper authorization controls, organizations can prevent unauthorized tampering or disclosure of sensitive information.

Additionally, attribute-based access control (ABAC) is recommended to provide fine-grained access control based on attributes such as user roles, patient consent, and data sensitivity. ABAC enhances security by dynamically enforcing access policies, allowing for more flexible and granular control over data access.

By incorporating authentication, authorization, and attribute-based access control, the proposed solution aims to establish a safe EHR system. These security measures significantly reduce the risk of unauthorized access, data tampering, information disclosure, and other potential threats.

It is important for healthcare organizations to prioritize the implementation of these security measures to protect patient privacy, maintain data integrity, and ensure the secure sharing of healthcare information. By addressing potential threats proactively, organizations can enhance the overall security posture of the EHR system, mitigating risks and safeguarding sensitive patient data.

Acronyms

EHR Electronic Health Record
TMT Threat Modeling tool
TM Threat Modeling
STRIDE Spoofing, Tampering, Repudiation, Information disclosure, Denial of service and Elevation of privilege
DREAD Damage, Reproducibility, Exploitability, Affected users, and Discoverability
PKI Public Key Infrastructure
TLS Transport Layer Security
ABAC Attribute-Based Access Control
PBAC Policy Based Access Control
SSL Secure Sockets Layer
CAs Certificate Authorities
HIPAA Health Insurance Portability and Accountability Act
GDPR General Data Protection Regulation
DFD Data Flow Diagram
SS0 Single Sign-On
SAML Security Assertion Markup Language

References

[Bel16] Victoria Beltran. “Characterization of web single sign-on protocols”. **in***IEEE Communications Magazine*: 54.7 (2016), **pages** 24–30.

[BM13] Arshdeep Bahga **and** Vijay K Madisetti. “A cloud-based approach for interoperable electronic health records (EHRs)”. **in***IEEE Journal of Biomedical and Health Informatics*: 17.5 (2013), **pages** 894–906.

[GET22] GETAPP. *Electronic Medical Records Software with SSL Security*. Last accessed 16 September 2017. 2022. URL: `https://www.getapp.com/healthcare-pharmaceuticals-software/electronic-medical-records/f/ssl-security/`.

[GPS20] Raghavendra Ganiga, Radhika M Pai **and** Rajesh Kumar Sinha. “Security framework for cloud based electronic health record (EHR) system”. **in***International Journal of Electrical and Computer Engineering*: 10.1 (2020), **page** 455.

[HHS20] HHS. *Threat Modeling for Mobile Health Systems*. Last accessed 16 September 2017. 2020. URL: `https://www.hhs.gov/sites/default/files/threat-modeling-mobile-health-systems.pdf`.

[Seo+18] Kwangsoo Seol **andothers**. “Privacy-preserving attribute-based access control model for XML-based electronic health record system”. **in***IEEE Access*: 6 (2018), **pages** 9114–9128.

[Sho14] Adam Shostack. “Threat modeling: Designing for security”. **in**(2014).

[Sta12] William Stallings. *Cryptography and Network Security: Principles and Practice*. 5th. Pearson Education, 2012.

[ZZD18] Yinghui Zhang, Dong Zheng **and** Robert H Deng. “Security and privacy in smart health: Efficient policy-hiding attribute-based access control”. **in***IEEE Internet of Things Journal*: 5.3 (2018), **pages** 2130–2145.

[09] Anitha K. L and T. R. Gopalakrishnan N., “Data storage lock algorithm with cryptographic techniques,
” International Journal of Electrical Computer Engineering, vol. 9, pp. 3843-3849, 2019.

[10] J. Eom, et al., “Patient-controlled attribute- based encryption for secure electronic health records system,” Journal of medical systems, vol. 40, pp. 253, 2016.

[11] F. Alemán, et al., “Security and privacy in electronic health records: A systematic literature review,” Journal of biomedical informatics, vol. 46, pp. 541-562, 2013.