Designing a methodology to evaluate the security of an instant-messaging system

1. Research question overview

The purpose of this report is to formulate a method and methodology to answer the research question: *We want to develop a secure instant-messaging system. How can we evaluate its security?* The research question itself is broad since the terms *secure* and *instant-messaging system* are not clearly defined. To better answer the given research question we therefore formulate several subquestions that together will bring an answer to the overall research question. The subquestions will focus on confidentiality, integrity and availability (CIA triad) to define the security of the instant-messaging system.

Derived Subquestions:

The following sub-questions were derived to enable accurate evaluation of the system:

1. *What are key security attributes (such as confidentiality, integrity, availability) that should be evaluated in instant-messaging systems?*

2. *What are the potential vulnerabilities in an instant-messaging system?*

3. *What methods can be used to assess the system's resistance to common cybersecurity threats, such as data breaches and malware?*

4. *What measures can be used to evaluate the strength and reliability of the system's encryption protocols?*

5. *What methods can be used to evaluate user authentication and data privacy?*

2. Methodology

To address our research question, and derived subquestions, about the security of secure instant-messaging systems we will engage in both theoretical evaluations and extensive literature review.

2.1 Key security features evaluation

In order to identify relevant key security features to evaluate the system we would need to conduct a systematic literature review and utilize databases such as IEEE Xplore, Scopus and Web of Science. Our primary focus is on terms like "instant messaging security", "communication security attributes" and similar phrases. Our research will also cover the useability aspect of these security features and explore how they combine with user needs and preference. If necessary, we would also potentially use terms like "secure messaging

protocols", "encryption in instant messaging" and "privacy in digital communication" to capture a wider range of material.

To further refine the search process, we plan to utilize a combination of keywords and boolean operators. For example "instant messaging AND security" to narrow down articles focusing on addressing security in instant messaging.

We will focus on peer-reviewed articles and conference papers, and exclude non-peer-reviewed sources. Given the rapidly evolving nature of technology we will also limit our search to studies published within the last five years, the most relevant and up-to-date information, unless seminal.

2.2 Vulnerability assessment

To identify possible vulnerabilities in the system, we will conduct a non-systematic literature review. The review should source a wide range of publications to ensure that different viewpoints and insights are considered. Relevant keywords would be terms such as "messaging system vulnerabilities", "security threats in messaging apps" and "exploiting messaging apps" .

The goal is to gather and analyze a diverse collection of articles and technical reports that specifically discuss vulnerabilities and security threats to instant-messaging systems. This approach ensures an overall understanding of potential security weaknesses.

Our focus will be segmented into several areas:

- **System exploit:** We will delve into common system exploits and vulnerabilities that could impact the security of our system. This requires an investigation of vulnerabilities related to software components, network protocols, and user interactions with the system.

- **Known vulnerabilities:** Our assessment will include an exploration of known vulnerabilities in similar systems as ours. By studying vulnerabilities that have been previously identified and addressed, we can expect the potential issues in our system.

- **Case studies:** We will analyze real-world case studies of security breaches in instant messaging systems. This will provide insights into the types of vulnerabilities that can lead to security incidents which enable us to address these concerns effectively.

Additionally, we will evaluate the context and environment in which these vulnerabilities are discussed to get a better understanding of the security challenges. To further refine the search process, similar utilizations mentioned for the previous subquestion's method will be employed, as well as the previously mentioned databases.

2.3 Cybersecurity threats assessment

We will design and conduct penetration testing to evaluate the security of the system using established tools such as Metasploit. The testing will begin with reconnaissance and controlled exploitation to assess the system's security status. Throughout this process, the aim is to identify any security weaknesses and the system's ability to detect and mitigate threats.

The testing will cover both the application and network layers of the instant-messaging system. The objective is to identify potential security weaknesses across the system. Therefore, the focus will be on evaluating vulnerabilities in the software, data transmission security and server robustness.

- **Software vulnerability analysis:** Evaluating the software for any exploitable weaknesses that could be leveraged by potential attackers.

- **Data transmission security:** Assessing the integrity and confidentiality of data as it traverses the network to ensure that communication channels are secure.

- **Server robustness:** Examining the server to withstand various cyber-attacks to ensure the stability and reliability of the system.

All testing will comply with legal requirements and ethical standards. E.g. ethical hacking principles such as anonymizing data used in simulation and informing users of any potential impact, as well as ensuring all testing is authorized and does not harm the system or its users.

The testing will cover the vulnerabilities found in the earlier part of the study, i.e. the results from subquestion 2.

2.4 Encryption protocol

To evaluate the strength and reliability of the system's encryption protocols we will conduct cryptographic analysis. Our cryptographic analysis will include:

- **Key length evaluation:** We will assess the length of cryptographic keys used, as key length is an important factor in determining the strength of encryption. In general, longer keys have higher security which make them more resistant to brute force attacks.

- **Algorithm robustness:** This involves their complexity and resistance to known vulnerabilities.

- **Resistance to common cryptographic attacks:** This includes simulating threats like brute force attacks where the attacker tries to decode encrypted data by trying all possible combinations, and side-channel attacks, which exploit physical or logical vulnerabilities in the encryption process.

The focus will also be on the practical implementation of these protocols within the system, ensuring they are applied correctly. Finally, benchmarking the encryption protocols against standards, such as those set by National Institute of Standards and Technology (NIST) or the International Organization for Standardization (ISO/IEC), will be an important part of our analysis. This comparison ensures that the encryption methodologies comply with global best practices.

2.5 User authentication and data privacy

The evaluation of user authentication and data privacy in the system would include:

- **Strength of authentication protocols:** We will analyze the authentication protocols implemented in the system. This involves evaluating the security features of these protocols such as two-factor authentication, biometric verification and the strength of password.

- **Penetration testing on the authentication systems:** Doing penetration testing on our authentication mechanisms helps identify vulnerabilities. These tests will simulate attack scenarios to determine the system's resilience against unauthorized breaches.

Additionally, assessment would also be made regarding the system's approach to user consent and data control. This will include:

- **Review of privacy policies:** We will consider the privacy policies and ensure it is transparent and user-friendly. We will also verify that these policies adequately inform users about how their data is used, stored and protected.

- **Data handling and protection:** This includes reviewing data encryption methods, data storage practices. We aim to be sure that all measures are in place to protect user data.

To uphold ethical data handling and legal compliance, our evaluation will cover:

- **User consent and data control:** We will ensure that the system design includes clear mechanisms for users to understand and manage their data preferences.

- **Legal standards:** Compliance with legal standards such as the General Data Protection Regulation (GDPR) will be an important part of our assessment. This includes assessing how the system's design can prevent misuse by e.g. external entities and ensure users rights are protected.

3. Discussion

3.1 Key security features evaluation

The databases Web of Science, Scopus and IEEE Xplore are used for retrieving information because they index scientific publications i.e. refereed journal articles and conference

papers. Web of Science and Scopus are citation databases, and citations can be helpful for finding relevant publications with a high impact. These databases allow for the tracking of how frequently a paper is cited, which indicates its relevance in the field. Additionally, using a combination of keywords and boolean operators in the search increases the chances of finding relevant articles. Moreover, focusing on more recent publications is also important in this rapidly evolving field.

A potential limitation is that the search terms and keywords might inadvertently omit some relevant studies that use different terminology. Furthermore, only focusing on more recent studies might exclude some significant earlier works.

3.2 Vulnerability assessment

A non-systematic literature review for identifying vulnerabilities is appropriate since it offers flexibility to cover a diverse set of perspectives. This approach allows an exploration of various aspects of security challenges in instant-messaging systems. By identifying a broad area of vulnerabilities, by for example ranking them based on number of occurrences, a general view of the biggest threats can be mapped. Furthermore, considering the context in which the security challenges are discussed, e.g. technical environments and user behavior, offers a better understanding of the potential vulnerabilities.

Since a non-systematic literature review is less structured and less comprehensive than a systematic review, it may potentially miss key studies. It may also not be as convincing to others since the selection of sources is not transparently documented. Additionally, while real-world case studies offer practical insights, it is not necessary that they completely represent theoretical vulnerabilities.

By providing an answer to this subquestion we bring into attention the instant-messaging systems capabilities in all aspects of the CIA triad. Identifying vulnerabilities can address problems in all three aspects as a vulnerability can affect one or several of them.

3.3 Cybersecurity threats assessment

Penetration testing, including ethical hacking principles, was selected as it provides a real world simulation of threats, allowing us to evaluate the system’s strength in a dynamic environment. This method is effective for assessing the security of the instant-messaging system, ensuring a comprehensive understanding of potential security weaknesses. To maintain ethical standards during the testing process, we anonymize the data used in simulations and ensure that no identifiable user information is at risk.

Additionally, by conducting tests on potential vulnerabilities identified earlier in the study (results form subquestion 2) we can target the most relevant security concerns. However, it is important to be aware of its limitations in predicting future threats or identifying every possible security issue.

By providing an answer to this subquestion we bring into attention the instant-messaging systems capabilities to address confidentiality. This is by identifying how the system remains operational and resistant to threats that could disrupt service.

3.4 Encryption protocol

When examining the encryption protocol, it's important to look at key lengths, algorithm strength, and resistance against attacks. However, it is also important to consider how the protocol is actually used in practice. It is important to maintain a balance between its level of security and how fast it is, i.e. its performance. Benchmarking against recognized standards like NIST or ISO/IEC adds an extra layer of validation which ensures that the encryption meets the accepted industry benchmarks.

However, there are limitations to this kind of analysis. Threats are constantly evolving, and it can be difficult to replicate real-world attacks.

By providing an answer to this subquestion we bring into attention the instant-messaging systems capabilities to address integrity. This is as encryption protocols are crucial in ensuring that messages are not altered or compromised during transmission.

3.5 User authentication and data privacy

The evaluation of user authentication and data privacy involves an analysis of authentication protocols, privacy policy reviews, and penetration tests. This helps to ensure robust user identity protection, prevents unauthorized access, and verifies compliance with legal standards.

This approach ensures a good understanding of the user consent, data control, and overall ethical data handling. Furthermore, the inclusion of penetration tests on the authentication systems provides insights into the robustness of user authentication mechanisms.

By providing an answer to this subquestion we bring into attention the instant-messaging systems capabilities in all aspects of the CIA triad. By examining user authentication and data privacy we include we target confidentiality, integrity and availability together.

3.6 Ethical aspects

Ethical aspects related to the methodology focuses on responsible and legally compliant research practices. This included e.g. anonymization of user data in simulations, informed consent and transparency and ethical handling of user data. This involves assessing the system’s approach to user consent and data control. Users should be aware of how their data is used and handled. An additional ethical aspect considered when evaluating the system is the balance between user friendliness and security. Even though the system must protect sensitive data, it shouldn’t be too difficult for the user to use the system. Another relevant aspect is the risk of misuse. E.g. the government should not be able to spy on user’s conversations, and therefore a high level of confidentiality must be ensured. However, it is also important to consider measures against criminals exploiting this high level of confidentiality. Therefore, it is worth considering implementing a controlled access point for legal enforcement.

4. Conclusion

In conclusion, our methodological approach to evaluating the security of an instant-messaging system has tried to answer the main research question by navigating a complex terrain of key security attributes, vulnerabilities, cybersecurity threats, encryption protocols, and user authentication.

Through a systematic literature review, we identify and assess key security features, drawing on reputable databases to ensure the reliability and relevance of our findings. The non-systematic literature review for vulnerabilities allows us to explore diverse perspectives, providing a comprehensive understanding of potential security challenges. By including penetration testing, guided by ethical hacking principles, we get offered a real-world simulation of threats, ensuring a dynamic assessment of the system's strength. By also focusing on cryptographic analysis, practical implementation, and benchmarking against industry standards adds robust layers to the evaluation of encryption protocols. The multifaceted approach to user authentication and data privacy underscores our commitment to holistic understanding and ethical data handling.

While limitations exist, such as potential omissions in search terms and the exclusion of earlier works, our findings will weave a comprehensive narrative that effectively answers the research question.

Acknowledgements

We have used generative language models (AI) for language questions.