جامعة الأمير سلطان
PRINCE SULTAN
UNIVERSITY

WhatsApp Risk Management

Security Risk Management, Governance, and Control

CYS403

Done by:

Lama AlGhzzi 220410092

Dana AlJbreen 218410746

Mishael AlHargan 220410069

Sara AlSadaan 220410793

Reema AlShaibani 219410542

Supervised by:
Dr. Nor Shahida Binti Mohd Jamail

Section:

863

Table of Contents

EXECUTIVE SUMMARY

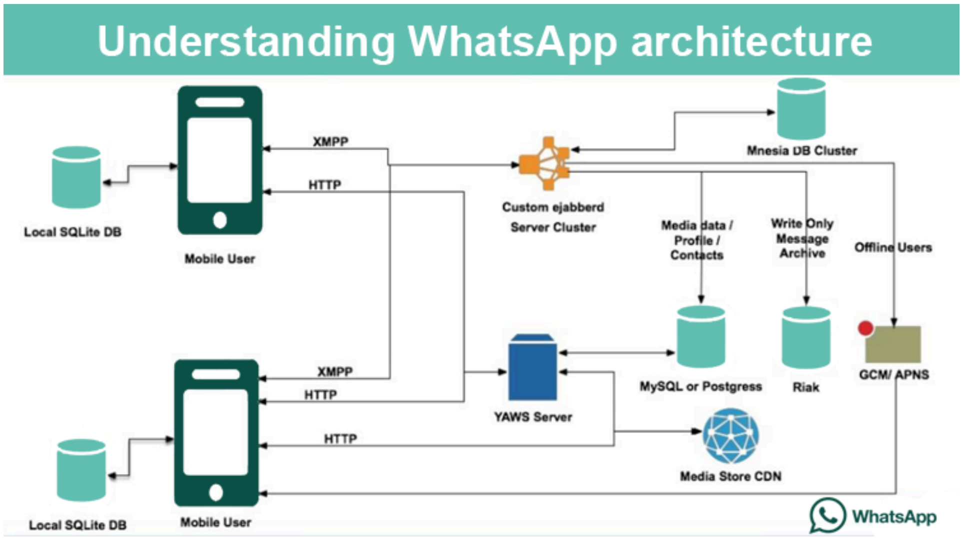
In this project, we talked about WhatsApp and described the security situation of WhatsApp. WhatsApp uses the Signal end-to-end encryption protocol, which ensures secure communication between the client and the server. In addition, we explained the architecture of WhatsApp and created a diagram showing the interaction of the critical assets in WhatsApp. These assets are what help WhatsApp achieve its objectives, so these assets need continuous protection under constant evaluation in order for WhatsApp to continue its operations. However, we have categorized the risks with a risk management plan which is divided into Identification, Assessment and Mitigation & control. To classify risks, we divided risks into different types with examples according to the six components of the information system. To collect potential threats and vulnerabilities in WhatsApp, we chose to reference historical data by using CVE. We also used the STRIDE model to identify threats that may occur to assets. Moreover, we identified the weaknesses, vulnerabilities and strengths of WhatsApp with the risk register and it was the outcome of the risk identification phase. After that, we took the second phase, which is risk assessment. We used a qualitative risk assessment method that relies on observation and judgment. We used NIST SP 800-30 matrices to determine impact and risk probability. In the final phase, we found the potential solutions that were likely to address the issues identified in the first phase. While addressing the risks, we have taken the four countermeasure techniques (risk acceptance, avoidance, mitigation and transfer) into consideration. After that, we prepared a residual risk table based on the residual risk matrix. Finally, we talked about the security guidelines and policies implemented in WhatsApp, and the authentication techniques for login and transactions and confidentiality techniques, and we proposed an enhanced security approach and CIA improvements.

INTRODUCTION

One of the most popular instant messaging applications currently is WhatsApp. WhatsApp is available on many platforms such as MacOS, iOS, Windows and Android. WhatsApp allows users to communicate with each other through text messages, voice and video calls, with features like creating groups, channels, and communities. No one can join groups and communities on WhatsApp except the admins or by sharing the link to join. WhatsApp provides the "Status" feature for sharing texts, photos and videos that stay for 24 hours with the ability to customize viewers. Moreover, WhatsApp provides features like sharing people's live locations, and sharing contacts, documents, and files, since WhatsApp has built-in file-sharing. WhatsApp provides its users the ability to create surveys and share stickers that can be added from outside the application or provided by WhatsApp. In this project, we will analyze the current security situation of WhatsApp and highlight the major security issues that we found. We also aim to propose a risk management plan by identifying, assessing and evaluating potential risks in WhatsApp with recommend the risk control techniques for each of those risks.

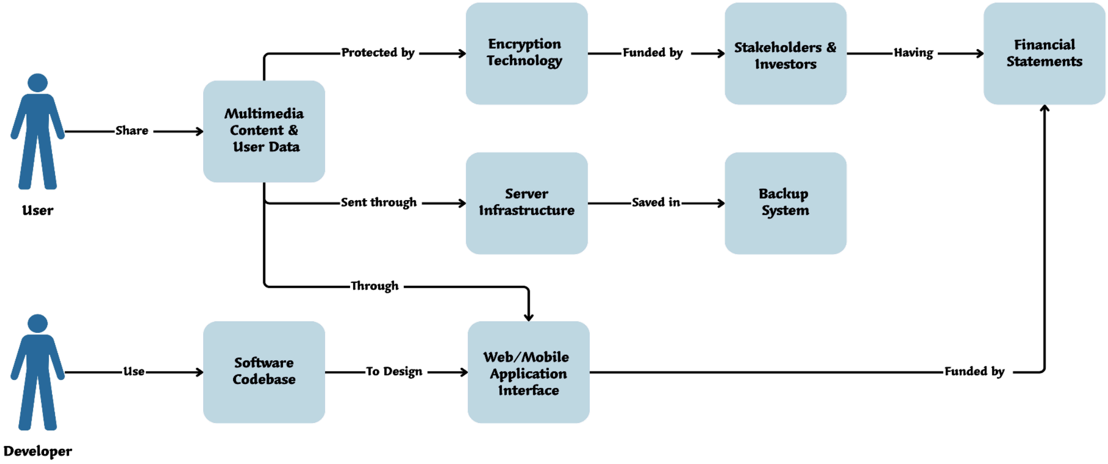
STATE OF ART

WhatsApp offers a secure messaging experience through robust security measures. It relies on end-to-end encryption, safeguarding messages from unauthorized access. Two-step verification provides an extra layer of security to user accounts, enhancing overall safety in communication. Regular updates contribute to addressing potential vulnerabilities, reflecting WhatsApp's commitment to maintaining a secure platform for its users. Regarding communication, WhatsApp employs the Signal Protocol for its end-to-end encryption, which ensures secure communication between the client and server. Strong security features that support the privacy and confidentiality of messages on the platform make this protocol highly regarded. WhatsApp integrated the Signal protocol in its implementation in 2016 to provide encrypted messages and exchange end-to-end encrypted chats to the users and includes security goals, confidentiality, integrity and authenticity [1].



Erlang is used as the main programming language for WhatsApp. WhatsApp uses Ejabberd, an open-source messaging server based on the XMPP protocol. WhatsApp uses the Mnesia database, a distributed database management system built in the Erlang language. Although the simplicity of WhatsApp's interface, its internal architecture is complex and therefore requires a good understanding to achieve security and stability. [2]

A system overview of WhatsApp is shown in the diagram below, which highlights WhatsApp’s critical assets and the interaction between them to achieve the objectives of WhatsApp. The relationships that are shown highlight how important it is to have strong security actions in place to ensure WhatsApp's security and ongoing operation.



RISK MANAGEMENT PLAN:

RISK IDENTIFICATION:

Risk identification is the first step of the risk management plan. We will start by identifying all potential threats and vulnerabilities. To identify all the potential risks related to WhatsApp, we will refer to historical data, which is Common Vulnerabilities and Exposures (CVE).

1. LIST OF IDENTIFIED THREATS:

We have listed the assets that are important to take into consideration in the risk management plan. These assets hold significant value for WhatsApp as they play a crucial role in achieving its objectives, and any threats could detrimentally impact the company. Following the identification of these assets, also prioritization and classification were undertaken. Additionally, we conducted STRIDE threat modeling to identify potential threats to each asset.

Priority level:

- 5: Highest priority - Indicates assets where damage or compromise would lead to extreme monetary loss.
- 4: High priority - Indicates assets where damage or compromise would result in a high level of monetary loss.
- 3: Medium priority - Indicates assets where damage or compromise would lead to a moderate level of monetary loss.
- 2: Low priority - Indicates assets where damage or compromise would result in a relatively low level of monetary loss.
- 1: Lowest priority - Indicates assets where damage or compromise would lead to minimal to no monetary loss.

Classification of information based on confidentiality:

- **Public:** Information that is intended for unrestricted access and dissemination and it poses no risk or harm if disclosed to the public.

- **Internal:** Information restricted to internal use within an organization, its exposure to unauthorized individuals may have minimal impact.
- **Confidential:** Sensitive information requiring protection from unauthorized access, exposure could lead to financial, legal, or reputational damage.
- **Restricted:** Highly sensitive information with a critical impact if disclosed without authorization, it is accessible only to specific authorized individuals or groups.
- **Highly Confidential:** Extremely sensitive information with severe consequences if compromised, access is strictly limited to a select few with specific clearance levels.

Table 1: Identification of the Assets

Categories of the assets	Assets	Description	Priority Level	Relevant CIA	Classification	Personal (P)/ Non-personal (NP)
Software & Technology Assets	**Encryption Technology**	Protecting the privacy and security of multimedia content during transmission and ensuring message privacy and security.	5	CI	Confidential	NP
	Backup System	End-to-End Encryption Protocol: Proprietary encryption	4	A	Internal	P

		technology ensuring message privacy and security.				
	Web Application Interface	The web application interface is accessible via a web browser on any device without having to install a separate application.	3	A	Public	P
	Mobile Application Interface	The mobile application interface is provided by Telegram installed on users' personal devices; it's user-friendly and highlights the app's features.	4	A	Public	P
	Server Infrastructure	The infrastructure	5	CIA	Internal	NP

		supports the storage and transmission of multimedia content across the WhatsApp network.				
Financial Assets	**Financial Statements**	Records detailing the company's financial performance and position.	5	CI	Confidential	NP
User-Related Assets	**Multimedia Content**	These include photos, videos, voice messages, audio files, documents, stickers, and GIFs which are used for communication purposes.	4	CI	Restricted	P
	User Data	These are collected by telegram for improving its services and	5	CI	Confidential	P

		for developing its features while maintaining user privacy and data security.				
Intellectual Property	**Software Codebase**	Unique programming code and innovative features developed by WhatsApp.	2	CI	Internal	NP
Business Relationships	**Stakeholders & Investors**	Entities or individuals invested in or having a stake in the company.	4	C	Public	NP

Table 2: STRIDE threat modeling

Threat Asset	Spoofing	Tampering	Repudiation	Information Disclosure	Denial of service	Elevation of privilege
Encryption Technology	Attackers masquerading as legitimate users to gain unauthorized access to encrypted data or services.	Unauthorized alteration of encrypted data during transmission or storage.	Users deny their involvement in encrypted transactions or communications.	Unauthorized access or exposure of sensitive information through encryption vulnerabilities or weaknesses.	Attackers disrupt or degrade the encryption service, making it unavailable to legitimate users.	Unauthorized escalation of privileges to gain access to encrypted data or manipulate encryption settings.
Backup System	Attackers might spoof or impersonate backup endpoints or services, tricking users into uploading backups	Unauthorized modification of backup data during transmission or storage, altering the integrity of the backups.	Users deny responsibility for specific backup actions or modifications, creating disputes over backup authenticity.	Unauthorized access or exposure of sensitive information contained in backups.	Attackers disrupt backup services or overload servers, rendering backups unavailable.	Unauthorized escalation of privileges to gain unauthorized access or manipulate backup configurations.

	to malicious servers.					
Web Application Interface	Attackers impersonating legitimate users to gain unauthorized access to the web interface, possibly intercepting or manipulating data.	Unauthorized modification of web application data during transmission or at rest, compromising data integrity.	Users denying their actions or transactions within the web interface, causing disputes or accountability issues.	Unauthorized access or exposure of sensitive information presented or stored within the web interface.	Attackers disrupt the availability of the web interface, rendering it unavailable to legitimate users.	Unauthorized escalation of user privileges within the web interface, gaining access to unauthorized features or data.
Mobile Application Interface	Attackers attempting to impersonate legitimate users to gain unauthorized	Unauthorized modification of data within the mobile app, compromising the integrity of user data or	Users denying their actions or transactions within the mobile app interface, causing disputes or accountabilit	Unauthorized access or exposure of sensitive information stored or transmitted through the mobile app.	Attackers disrupt the availability of the mobile app interface, making it unusable	Unauthorized escalation of user privileges within the mobile app interface, gaining access to unauthorized

	access to the mobile app interface, potentially intercepting or manipulating data.	communications.	y issues.		for legitimate users.	functionalities or data.
Server Infrastructure	Attackers attempting to spoof or impersonate legitimate servers within the infrastructure to intercept or manipulate data.	Unauthorized modification of data within servers, compromising the integrity of stored or transmitted information.	Servers denying or being unable to prove actions or transactions performed, leading to disputes or accountability issues.	Unauthorized access or exposure of sensitive information stored or processed by servers.	Attackers disrupting the availability of servers, causing service unavailability for legitimate users.	Unauthorized escalation of privileges within the server infrastructure, allowing access to sensitive functionalities or data.

Financial Statements	Falsification of financial statements or reports by malicious entities, presenting false information as legitimate financial data.	Unauthorized modification or alteration of financial statements, leading to inaccurate or misleading financial records.	Disputes over the authenticity or validity of financial statements, leading to challenges in proving the origin or accuracy of financial data.	Unauthorized access or exposure of sensitive financial information, leading to breaches of confidentiality or regulatory violations.	Disruption of financial systems or processes, rendering them unavailable or non-functional.	Unauthorized escalation of privileges or access to financial systems, potentially compromising financial data.
Multimedia Content	Possibility of attackers spoofing multimedia content (images, videos, audio) to appear as legitimate but containing	Unauthorized modification or alteration of multimedia content during transmission or storage, compromising its integrity.	Users denying sending or receiving specific multimedia content, leading to disputes or accountability issues.	Unauthorized access or exposure of sensitive information within multimedia content.	Attackers disrupting multimedia content services or features, rendering them unavailable to users.	Unauthorized access or manipulation of multimedia content due to elevated privileges or vulnerabilities.

	malicious or altered information.					
User Data	Attackers attempting to spoof or impersonate legitimate users to gain unauthorized access to user data or accounts.	Unauthorized modification or alteration of user data, compromising its integrity or accuracy.	Users denying their actions or transactions within the app, causing disputes or accountability issues regarding user data.	Unauthorized access or exposure of sensitive user information, including personal details or communication content.	Attackers disrupting access to user data or services, rendering them unavailable to legitimate users.	Unauthorized escalation of privileges, allowing access to higher levels of user data or functionalities.
Software Codebase	Malicious actors attempting to insert spoofed or unauthorized code changes into the	Unauthorized modification or alteration of the codebase, introducing vulnerabilities or	Disputes over the origin or authorization of specific code changes, potentially causing accountabilit	Unauthorized access to sensitive information within the codebase, such as hardcoded credentials or	Attackers attempting to disrupt the availability or functionality of the codebase,	Unauthorized access to critical functionalities or administrative controls within the codebase.

	codebase, posing as legitimate contributors.	compromising the integrity of the software.	y issues or challenges in tracking modifications.	proprietary algorithms.	leading to service unavailability or performance issues.	
Stakeholders & Investors	Attempted impersonation of legitimate stakeholders or investors to gain unauthorized access to sensitive information or manipulate decision-making.	Unauthorized modification or alteration of financial or strategic information provided to stakeholders or investors, leading to misinformation or misrepresentation.	Stakeholders or investors denying their involvement or approval of certain decisions or transactions, leading to disputes or lack of accountability.	Unauthorized exposure or leakage of sensitive business strategies, financial data, or plans to competitors or unauthorized entities.	Attempts to disrupt investor meetings, communications, or financial transactions, impacting decision-making or causing interruptions.	Unauthorized access or manipulation of stakeholder or investor-related data, leading to unauthorized decision-making or access to confidential information.

2. CAUSES OF THREATS:

a. WEAKNESSES: [3][4]

- WhatsApp backup is done automatically only once a day, after that the user must make a manual backup.
- WhatsApp allows anonymous voice and video calls without the ability to prevent this.
- WhatsApp Web relies primarily on scanning QR codes for authentication.
- WhatsApp needs an internet connection to send and receive messages.
- WhatsApp backups are stored on third-party cloud services (such as Google Drive or iCloud), which exposes them to vulnerabilities in those platforms.
- Lacks control settings and security in group chat features
- The ability to forward messages to multiple users can result in private information being spread without consent from the sender.
- WhatsApp shares users' information with Facebook

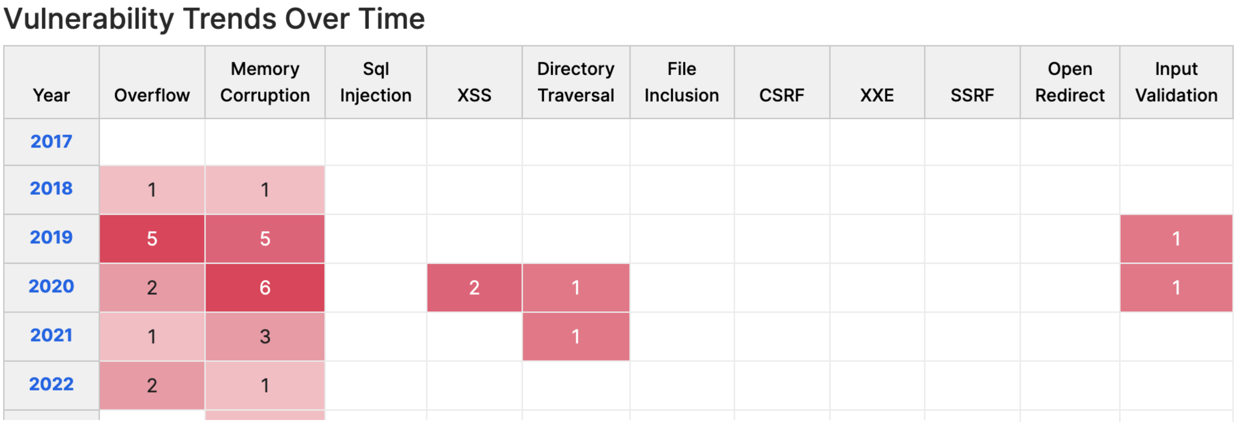
b. VULNERABILITIES

- Overflow
- Memory Corruption
- XSS
- Directory Traversal
- Input Validation

By impact types:

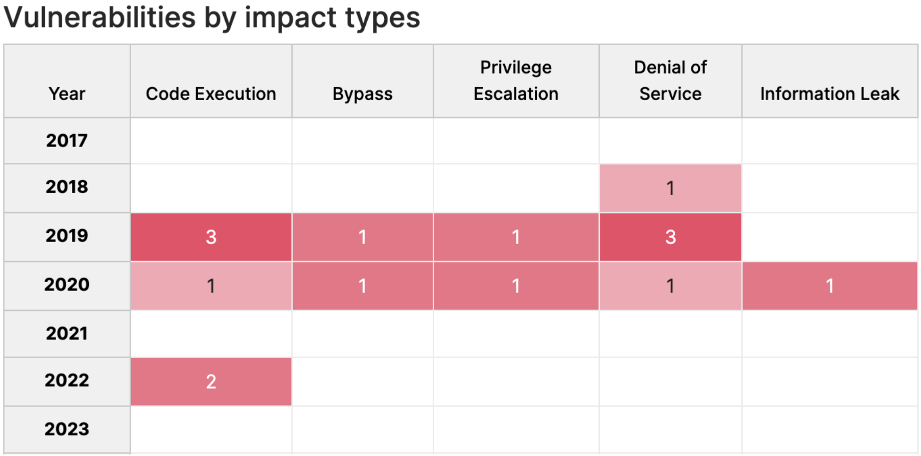
- Code Execution
- Bypass
- Privilege Escalation
- DoS
- Information Leak

The two figures below show the vulnerabilities of WhatsApp over the years [4].



Vulnerability Trends Over Time

Year	Overflow	Memory Corruption	Sql Injection	XSS	Directory Traversal	File Inclusion	CSRF	XXE	SSRF	Open Redirect	Input Validation
2017											
2018	1	1									
2019	5	5									1
2020	2	6		2	1						1
2021	1	3			1						
2022	2	1									



Vulnerabilities by impact types

Year	Code Execution	Bypass	Privilege Escalation	Denial of Service	Information Leak
2017					
2018				1	
2019	3	1	1	3	
2020	1	1	1	1	1
2021					
2022	2				
2023					

3. STRENGTHS:

- Easy to use with a simple user interface
- WhatsApp is a completely free application that provides free calls and chats
- WhatsApp uses a strong encryption system (end-to-end encryption)
- WhatsApp provides frequent system updates to fix issues
- WhatsApp provides the ability to control privacy, such as specifying who can see the status and profile settings
- Provides the feature to undo deleted messages
- It provides self-disappearing images that are displayed only once, which enhances privacy
- Allows admins to reset the invitation link in the groups
- Available on many systems such as macOS, iOS, Android and Windows.

- WhatsApp can use biometric authentication methods to secure access to the app if the device has Face ID or Touch ID

RISK REGISTER:

This is the risk register which is the result of the risk identification phase conducted based on the CVE:

Table 3: Risk Register

	ID	Date Raised	Risk Description	Likelihood	Impact if the risk occurs (CIA)	Severity	Owner	Mitigation Action
1	**CVE-2023-38538**	2023-10-04	An event subsystem race condition caused a heap use-after-free issue in established audio/video calls, which had a very limited chance of causing an unexpected control flow	Medium	C Low I Low A Low	Medium	WhatsApp	-Update to the Latest Version -Avoid answering calls from unknown or untrusted sources

			or app termination.					
2	**CVE-2022-36934**	2022-09-22	Within an established video call, a WhatsApp integer overflow could lead to remote code execution.	High	C High I High A High	Critical	WhatsApp	-Update to the Latest Version -Avoid answering video calls from unknown or untrusted sources
3	**CVE-2021-24035**	2021-06-11	Prior to WhatsApp for Android v2.21.8.13 and WhatsApp Business for Android v2.21.8.13, there was no filename validation	High	C None I High A High	Critical	WhatsApp	-Update to the Latest Version -Avoid opening or extracting files from untrusted

			when unzipping archives, which could have allowed path traversal attacks that overwrote WhatsApp files.					or unknown sources
4	**CVE-2021-24027**	2021-04-06	Prior to WhatsApp for Android v2.21.4.18 and WhatsApp Business for Android v2.21.4.18, there may have been a cache configuration bug that made it possible for a third party with access to the	High	C High I None A None	High	WhatsApp	-Update to the Latest Version -Examine the permissions granted to WhatsApp and WhatsApp Business

			device's external storage to read TLS content that was cached.					
5	**CVE-2021-24026**	2021-04-06	In WhatsApp for Android prior to v2.21.3, WhatsApp Business for Android prior to v2.21.32, WhatsApp for iOS prior to v2.21.32, and WhatsApp Business for iOS prior to v2.21.32, a missing bounds check within the audio decoding pipeline for	High	C High I High A High	Critical	WhatsApp	-Update to the Latest Version -Examine the permissions granted to WhatsApp and WhatsApp Business

			WhatsApp calls could have permitted an out-of-bounds write.					
6	**CVE-2020-20096**	2022-03-23	The user interface in WhatsApp versions iOS 2.19.80 and earlier, as well as Android 2.19.222 and earlier, inadequately displays URI messages. This deficiency leads to URI spoofing through carefully crafted messages.	Medium	C None I High A None	Medium	WhatsApp	-Update to the Latest Version -Users should exercise caution when clicking on links received via WhatsApp

7	**CVE-2020-1910**	2021-02-02	In WhatsApp for Android versions before v2.21.1.13 and WhatsApp Business for Android versions before v2.21.1.13, a lack of bounds check could have permitted out-of-bounds read and write operations. This vulnerability could occur when a user applied particular image filters to a	High	C High I High A High	High	WhatsApp	-Update to the Latest Version -Users should exercise caution when applying image filters

			specially designed image and then sent the modified image.					
8	**CVE-2020-1909**	2020-11-03	In WhatsApp for iOS versions before v2.20.111 and WhatsApp Business for iOS before v2.20.111, a use-after-free issue within a logging library might have led to memory corruption, crashes, and potentially, the execution of	High	C High I High A High	Critical	WhatsApp	-Update to the Latest Version -Users should exercise caution when using animated stickers while holding a video call

			code. This sequence of events could trigger the problem, requiring the receipt of an animated sticker while holding a WhatsApp video call.					
9	**CVE-2020-1908**	2020-11-03	The improper authorization of the Screen Lock function in WhatsApp and WhatsApp Business for iOS versions before v2.20.100 might have allowed Siri to access and interact with the	Medium	C None I High A None	Medium	WhatsApp	-Update to the Latest Version -Users should review the Screen Lock settings within WhatsApp -Disable Siri

			WhatsApp app even when the phone was locked.					Access on the Lock Screen
10	**CVE-2020-1907**	2020-10-06	In WhatsApp for Android versions before v2.20.196.16, WhatsApp Business for Android versions before v2.20.196.12, WhatsApp for iOS before v2.20.90, WhatsApp Business for iOS before v2.20.90, and WhatsApp for Portal	High	C High I High A High	Critical	WhatsApp	-Update to the Latest Version -Avoid opening multimedia content from suspicious messages

			before v173.0.0.29.505, a stack overflow issue could have enabled the execution of arbitrary code. This vulnerability might occur during the parsing of an RTP Extension header content.					
11	**CVE-2020-1906**	2020-10-06	In WhatsApp for Android versions before v2.20.130 and WhatsApp Business for Android versions before	High	C High I High A High	High	WhatsApp	-Update to the Latest Version -Avoid opening videos from suspicious

			v2.20.46, a buffer overflow vulnerability existed. This flaw could be exploited through the processing of improperly formatted local videos containing E-AC-3 audio streams, potentially enabling an out-of-bounds write action.					messages
12	**CVE-2020-1905**	2020-10-06	Before WhatsApp for Android v2.20.185, Media ContentProvider URIs utilized for	Medium	C Low I None A None	Low	WhatsApp	-Update to the Latest Version -Users should be

			launching attachments in other apps were generated in a sequential manner. This flaw could have enabled a potentially malicious third-party app, selected to open the file, to predict the URIs of previously accessed attachments until the app initiating the action was closed.					careful when opening attachment
13	**CVE-2020-1904**	2020-10-06	In WhatsApp for iOS versions before	Medium	C None I High A None	Medium	WhatsApp	-Update to the Latest Version

			v2.20.61 and WhatsApp Business for iOS versions before v2.20.61, a path validation problem existed. This issue could have enabled directory traversal, potentially leading to file overwriting when sending specifically crafted docx, xlsx, and pptx files as message attachments.	🟨	🟥	🟨		-Users should be careful when sending and receiving file attachments

14	**CVE-2020-1903**	2020-10-06	In WhatsApp for iOS versions before v2.20.61 and WhatsApp Business for iOS versions before v2.20.61, there was a potential problem when extracting contents from docx, pptx, and xlsx files. This issue might have caused an out-of-memory denial of service. However, triggering this problem	Medium	C None I None A High	Medium	WhatsApp	-Update to the Latest Version -Users should be careful when opening attachment

			would have required the recipient to actively open the attachment if it was received from a contact not saved in the recipient's WhatsApp contacts.					
15	**CVE-2020-1902**	2020-10-06	In WhatsApp for Android versions ranging from v2.20.108 to v2.20.140, or WhatsApp Business for Android versions from v2.20.35 to v2.20.49, a	High	C High I None A None	High	WhatsApp	-Update to the Latest Version -Users should be careful when interacting with highly forwarded

			scenario occurred where a user conducting a quick search on a widely forwarded message might have inadvertently been directed to the Google service through an insecure plain HTTP connection.					messages
16	**CVE-2020-1901**	2020-10-06	In WhatsApp for iOS versions before v2.20.91.4, the app could freeze when processing a large text message	Medium	C None I None A Low	Medium	WhatsApp	-Update to the Latest Version -Avoid Opening Large Messages

			containing URLs, leading to unresponsiveness or temporary lock-up of the application.					
17	**CVE-2019-3571**	2019-07-16	A flaw in earlier versions of WhatsApp Desktop (before 0.3.3793) enabled malicious clients to send files to users, causing them to be shown with an incorrect file extension.	Medium	C None I Low A None	Medium	WhatsApp	-Update to the Latest Version -Users should be careful when opening attachment

18	**CVE-2020-1894**	2020-09-03	In WhatsApp for Android versions before v2.20.35, WhatsApp Business for Android versions before v2.20.20, WhatsApp for iPhone versions before v2.20.30, and WhatsApp Business for iPhone versions before v2.20.30, there was a vulnerability involving a stack write overflow. Exploiting	High	C High I High A High	High	WhatsApp	-Update to the Latest Version -Avoid interacting with messages that look suspicious

			this flaw might have allowed the execution of arbitrary code when playing a specifically crafted push-to-talk message.					
19	**CVE-2020-1890**	2020-09-03	In WhatsApp for Android versions before v2.20.11 and WhatsApp Business for Android versions before v2.20.2, a problem with URL validation existed. This flaw could have led the recipient of	High	C None I High A None	High	WhatsApp	-Update to the Latest Version -Avoid interacting with stickers that look suspicious

			a sticker message, containing intentionally malformed data, to automatically load an image from a URL controlled by the sender without requiring any user interaction.					
20	**CVE-2019-11928**	2020-09-03	In versions of WhatsApp Desktop preceding v0.3.4932, an input validation problem existed. This flaw could potentially enable	Medium	C Low I Low A None	Medium	WhatsApp	-Update to the Latest Version -Ensure the browser is set up to prevent or notify users of

			cross-site scripting when clicking on a link within a specially crafted live location message.	🟨	🟩	🟨		potentially malicious scripts

RISK CLASSIFICATION:

The following identifies the risks that could lead to system failure, they classified according to the six information systems components:

1- Software -Application- Risk:

- Code vulnerabilities exposing WhatsApp to external threats
- Software bugs causing potential disruptions or data compromise
- Inadequate testing protocols posing risks to WhatsApp's stability
- Software Failures

2- Hardware Risk:

- Physical device threats, including theft or damage impacting WhatsApp access.
- Device hardware failures affecting WhatsApp
- Natural disasters
- Vulnerabilities in the hardware design

3. Network Risk:

- Unauthorized access to WhatsApp messages during transmission

-Interception of messages

- Denial of service attacks

- Vulnerabilities in network protocols and configurations

4. Data Risk:

- Data corruption

-Data breach

- Loss of data

- Accidental exposure of sensitive information

- Unauthorized access to stored sensitive data

5- People Risk:

- Insider threats compromising confidentiality within WhatsApp

- Social engineering attacks exploiting users and posing risks to WhatsApp security

- Unauthorized access to WhatsApp data or systems by individuals

- Risks associated with human errors

6. Procedures Risk:

- Interception of WhatsApp messages during transmission.

- Unauthorized access to WhatsApp communication channels.

-Use of communication protocols with security vulnerabilities.

RISK ASSESSMENT:

The second phase in risk management is risk assessment, which relies on qualitative techniques for evaluating the risk. Qualitative risk assessment involves the evaluation of potential risks based on their impact and likelihood of occurrence.

QUALITATIVE RISK ASSESSMENT:

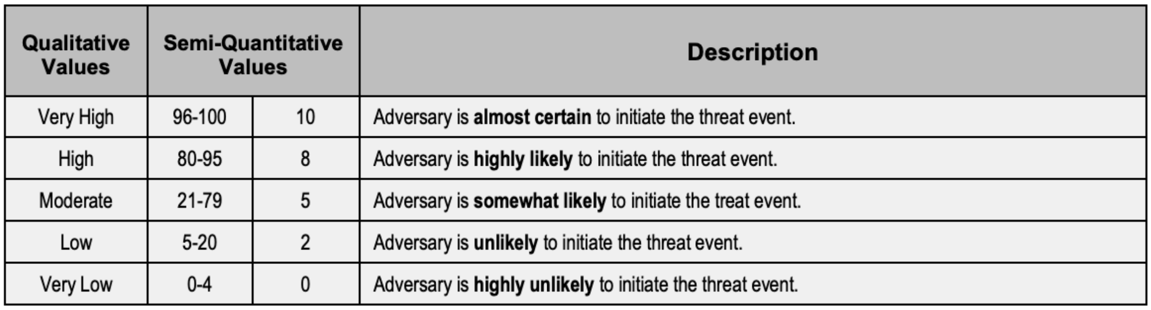
In qualitative risk assessment, the goal is to assign qualitative values to impact and likelihood, providing a subjective but informed understanding of the risks. The impact and likelihood values are then used to categorize risks and prioritize mitigation efforts.

1. Impact:

Is categorized into: low, medium, high etc. These impact levels are used to assess the potential consequences of a risk if it were to occur. Each risk in the register is assigned an impact level based on the severity of its potential effects on the confidentiality, integrity, and availability (CIA) of the system.

The following matrix will be used to determine the impact level:

Table 4: Level of Impact Scale Table [6]



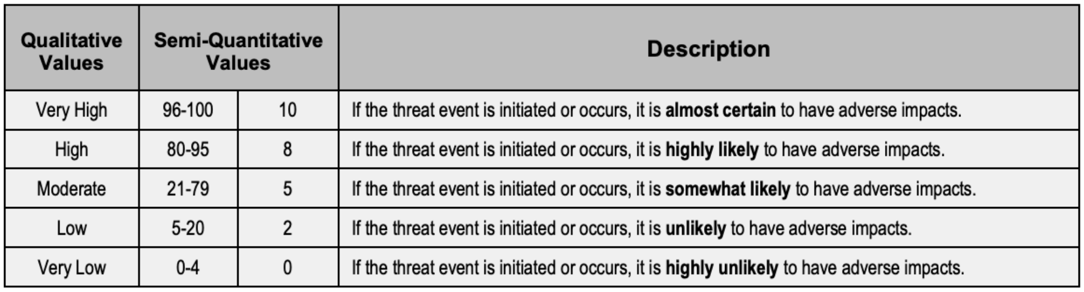
Qualitative Values	Semi-Quantitative Values		Description
Very High	96-100	10	Adversary is **almost certain** to initiate the threat event.
High	80-95	8	Adversary is **highly likely** to initiate the threat event.
Moderate	21-79	5	Adversary is **somewhat likely** to initiate the treat event.
Low	5-20	2	Adversary is **unlikely** to initiate the threat event.
Very Low	0-4	0	Adversary is **highly unlikely** to initiate the threat event.

2. Likelihood/ Probability:

Likelihood or probability is an assessment of how likely it is for a specific risk to materialize. Is categorized into: low, medium, and high. These likelihood levels help determine the probability of a risk event occurring. Each risk is assessed based on its likelihood, considering factors such as historical data, environmental conditions, and system vulnerabilities.

The following matrix will be used to determine the probability level:

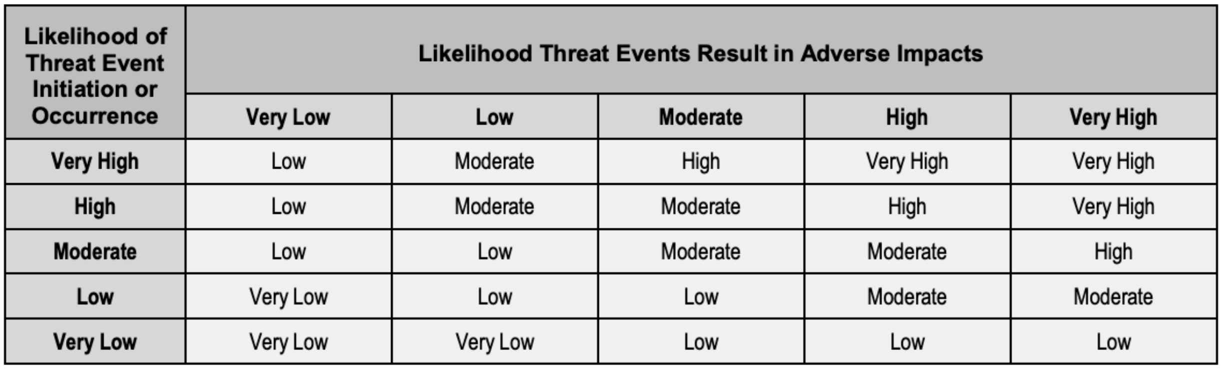
Table 5: Level of Probability Scale Table [6]



Qualitative Values	Semi-Quantitative Values		Description
Very High	96-100	10	If the threat event is initiated or occurs, it is **almost certain** to have adverse impacts.
High	80-95	8	If the threat event is initiated or occurs, it is **highly likely** to have adverse impacts.
Moderate	21-79	5	If the threat event is initiated or occurs, it is **somewhat likely** to have adverse impacts.
Low	5-20	2	If the threat event is initiated or occurs, it is **unlikely** to have adverse impacts.
Very Low	0-4	0	If the threat event is initiated or occurs, it is **highly unlikely** to have adverse impacts.

Thus, we can calculate the risk level from the following (Probability * Impact) matrix:

Table 6: Level of Risk Assessment Table [6]



Likelihood of Threat Event Initiation or Occurrence	Likelihood Threat Events Result in Adverse Impacts				
	Very Low	**Low**	**Moderate**	**High**	**Very High**
Very High	Low	Moderate	High	Very High	Very High
High	Low	Moderate	Moderate	High	Very High
Moderate	Low	Low	Moderate	Moderate	High
Low	Very Low	Low	Low	Moderate	Moderate
Very Low	Very Low	Very Low	Low	Low	Low

Table 7: WhatsApp Risk Assessment Table

Threat Asset	Threats	Vulnerability	Likelihood	Impact	Risk Level	Countermeasures
Encryption Technology	1. Encrypted data/services 2. Unauthorized access or exposure of sensitive information	1. Attackers masquerading as legitimate users 2. Encryption vulnerabilities or weaknesses	High	High	High	1. Implement strong authentication protocols, such as multi-factor authentication, to prevent unauthorized access. 1. Regularly monitor and analyze user behavior for any signs of suspicious activities. 2. Stay updated with the latest encryption standards and best practices. 2. Regularly patch and update encryption software.

Backup System	1. Unauthorized modification of backup data 2. Unauthorized escalation of privileges	1. Inadequate data integrity controls 2. Inadequate access control mechanisms	Medium	High	High	1. Implement data integrity mechanisms, such as checksums or digital signatures, to detect and prevent unauthorized modifications of backup data. 1. Use secure storage systems and encryption to protect the integrity of backup data at rest. 2. Implement strong access control mechanisms, such as privileged access management and least privilege principle. 2. Regularly review and update access control policies and permissions.

Web Application Interface	1. Attackers disrupting the availability of the web interface 2. Unauthorized modification of web application data	1. Lack of robust availability safeguards 2. Inadequate input validation and data integrity controls	Medium	High	High	1. Implement measures to mitigate distributed denial-of-service (DDoS) attacks, such as load balancing and rate limiting. 1. Monitor network traffic and implement intrusion detection and prevention systems. 2. Implement data integrity checks and validation on the server-side. 2. Encrypt sensitive data at rest.
Mobile Application Interface	1. Users denying their actions within the mobileapp interface	1. Insufficient logging and audit trail mechanisms	Low	Medium	Medium	1. Implement comprehensive logging and auditing mechanisms to track user actions and transactions. 1. Ensure logged events are

						tamper-proof and tamper-evident.
Server Infrastructure	1. Theft, vandalism 2. Insider threats	1. Inadequate physical security 2. Weak user access controls	Low	High	Medium	1. Implement physical access controls such as locked server rooms, CCTV surveillance, and entry logs. 1. Use secure server racks and cabinets. 2. Implement strong user access controls, including role-based access and least privilege principles. 2. Educate users about security best practices and policies.
Financial Statements	1. Data breaches 2. Phishing attacks	1. Insufficient encryption 2. User susceptibility to social engineering	Medium	High	High	1. Implement strong encryption protocols for financial statements at rest and in transit. 1. Implement access controls and permissions to

						limit data exposure. 2. Educate employees about phishing attacks and social engineering techniques. 2. Use multi-factor authentication for sensitive financial systems.
Multimedia Content	1. Malware infection	1. Unsafe downloads or malicious files	High	High	Critical	1. Implement strict download and file validation policies. 1. Educate users about safe browsing habits and avoiding suspicious downloads. 1. Use reputable antivirus and antimalware solutions.

User Data	1. Data loss 2. Data leakage	1. Inadequate backup procedures 2. Insecure data transmission	Medium	High	High	1. Regularly backup user data and verify the integrity of backups. 1. Store backups in secure off-site locations. 1. Test backup restoration procedures. 2. Implement secure transmission protocols such as encryption and VPNs. 2. Use secure APIs and enforce data encryption during transit. 2. Regularly monitor network traffic and detect unauthorized data transfers.

Software Codebase	1. Code tampering or modification 2. Insecure configuration	1. Inadequate change management and version control 2. Weak or insecure default configurations	Medium	High	High	1. Utilize secure version control systems and enforce strict change management processes. 1. Implement code signing and integrity checking mechanisms. 2. Follow secure configuration guidelines and best practices. 2. Use secure encryption and authentication algorithms. 2. Regularly test and validate the security of the configuration settings.

Stakeholders & Investors	1. Financial Loss 2. Market Competition	1. Economic downturn, market volatility, fraud, embezzlement, or mismanagement 2. Intense competition, new entrants, or disruptive technologies	High	High	High	1. Implement strong financial controls and auditing mechanisms 1. Stay updated on regulatory and compliance requirements. 2. Conduct market research and analysis to identify trends andcompetitors. 2. Foster strong relationships with customers and stakeholders.

SECURITY POLICIES AND GUIDELINES: [7]-[14]

End-to-End Encryption:

One of WhatsApp's most vigorous security features is its end-to-end encryption(E2EE). WhatsApp encrypts all user-to-user transmission, images, calls, and videos using E2EE. On the other hand, communications are encoded on the sending device and decoded on the receiving one. This infers that the messages can only be decoded and delivered by the intended receiver. In order to preserve E2EE, encryption exits are avoided in WhatsApp which certifies true privacy in group and individual conversations. Voice communications on WhatsApp Messenger feel more organic since users can be sure that no one is hearing in on them. WhatsApp folds and saves a lot of metadata about the messages sent and received by its users; this data can be applied to monitor the location and activities of its users(Carpay & Lontorfos, 2019; Davies et al., 2023; Endeley, 2018).

Privacy settings:

The WhatsApp users have the capability to manage their privacy settings, letting them select who can view their last seen status, profile photo, and status updates. Users have the option to modify the settings for individual contacts or to share this data with all contacts or just some of them. Users are also worried about their privacy due to WhatsApp's data collecting and distributing policies. Some critics claim that WhatsApp shares too much user data with Facebook and folds too much info about its manipulators. Some contend that WhatsApp is vulnerable to backdoors and other security errors and that its end-to-end encryption is unsatisfactory(Dev, Das, & Camp, 2018; Mols & Pridmore, 2021; Terpstra, 2013).

Two-step Verification:

An extra degree of protection is added to a user’s account with two-step verification. It adds another coating of protection against undesirable access by requiring the user to create a PIN. This significant feature lessens the risk of unlawful access, even in situations where authorizations have been hacked(Patidar, Tomar, Pateriya, & Sharma, 2023; Soyemi & Hammed, 2020).

Account Security:

WhatsApp has implemented security actions to protect accounts, such as warning the number of devices that can be linked to an account and providing selections for users to log out of sessions remotely. Using your fingerprint and disappearing messages feature are more secure methods of locking the app than using a password(Rastogi & Hendler, 2017; Tamori, Bhujade, & Sinhal, 2009).

Security Vulnerabilities:

WhatsApp is vulnerable to security errors even with its strong defenses in place. It is possible for backdoors unseen access points into encrypted systems to license illegal access to messages. Furthermore, it may be possible to survey user behavior and assume sensitive information from metadata, which contains details about communications including sender and recipient individualities and timestamps. WhatsApp needs to keep an eye on these possible faintness and take proper actions to keep its security posture complete(Bogos, Mocanu, & Simion, 2023; Mueller, Schrittwieser, Fruehwirt, Kieseberg, & Weippl, 2014).

Cloud security and Messages Backups:

Users of WhatsApp have the possibility to back up their chats to cloud services such as iCloud. Although suitable, customers should be aware of the security configurations of the cloud service they have designated. Although users should be mindful of the privacy rules and security settings of their selected cloud storage provider, WhatsApp does not expose the confidentiality of messages during the backup process. Users can make choices based on their personal security and privacy preferences by being aware of the consequences of cloud backups(Davies et al., 2023).

Metadata and Status Concern:

WhatsApp has addressed doubts about the durability of shared content by introducing capabilities like disappearing messages. Even while these features improve user secrecy, it's important to identify that some metadata is still gathered, such as who chats with whom and when. Users need to comprehend what data the platform might keep around for functional reasons. In order to build confidence and make sure that users are fully aware of the data organization procedures used through the WhatsApp ecosystem, this transparency is crucial(Rastogi & Hendler, 2017).

Data Collection and Sharing:

Numerous user data, such as contacts, phone numbers, usage trends, and metadata are assembled by WhatsApp. Although the facility of fundamental services like message delivery and modified features depends on this data collection, privacy issues are also elevated. Facebook, WhatsApp's parent firm, receives part of this data for publicity purposes. Users and privacy backers have disapproved of this data sharing, claiming that it allows targeted promotion while threatening user privacy(Krisdayanti, Ihsan, & Sevrika, 2023).

Businesses account:

There may be extra security measures and considerations for WhatsApp Business accounts. Corporations that use the WhatsApp Business API have to follow confident rules to protect client communications. WhatsApp's commitment to offering a safe platform to an inclusive range of users is verified by the installation of extra security features for business accounts(Holmes & Nicholls, 1989).

WhatsApp's security measures involve an intricate interplay between user privacy concerns, data collecting, and strong encryption. Although end-to-end encryption offers a robust framework for maintaining message content, user privacy is compromised by the gathering and exchange of additional data. WhatsApp needs to keep trying to find a way to balance protecting user privacy with offering a useful service. WhatsApp can boost its reputation as a safe and private messaging service by fixing possible errors, cultivating data transparency, and giving users more control over their information.

RISK MITIGATION AND CONTROL

To effectively manage risks, WhatsApp should adopt a comprehensive risk strategy that includes proactive measures to identify, assess, and mitigate potential risks. This strategy should focus on minimizing vulnerabilities, protecting user data, and maintaining the integrity and availability of the messaging platform.

RISK STRATEGY:

1- Accept the Risk:

Accept the risk and continue operating

2- Avoid the Risk:

Stop running the program or sharing the data

3- Transfer the Risk:

Use options to compensate for the loss, such as insurance

4- Reduce the Risk:

Implement controls that lessen the impact or lower the likelihood

RISK CONTROL CATEGORIES:

The risk control measures for WhatsApp can be categorized into the following areas:

1. Administrative:

Controls that adapt with the board-approved risk seeking and illuminate employees and workers of management's expectations. Such as training, awareness, and policies and security plans (DRP, IRP, BCP).

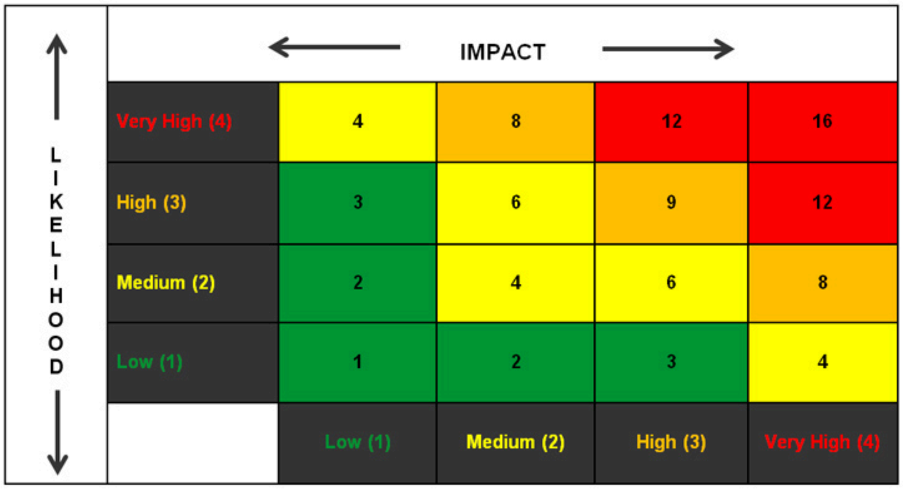
2. Technical:

Software and hardware that prevents unauthorized activities on the system such as firewalls.

3. Physical:

Devices to prevent unauthorized physical access to the system such as locks.

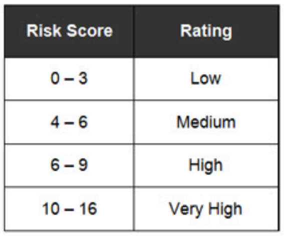
Residual Risk Scoring Matrix:



IMPACT

LIKELIHOOD

Very High (4)	4	8	12	16
High (3)	3	6	9	12
Medium (2)	2	4	6	8
Low (1)	1	2	3	4
	Low (1)	Medium (2)	High (3)	Very High (4)



Risk Score	Rating
0 – 3	Low
4 – 6	Medium
6 – 9	High
10 – 16	Very High

Table 8: Risk Residual Table

Threats	Vulnerability	Risk Level	Risk Control Strategy	Residual Risk	Management Strategy (Countermeasure)	Residual Risk Level
1. Encrypted data/services 2. Unauthorized access or exposure of sensitive information	1. Attackers masquerading as legitimate users 2. Encryption vulnerabilities or weaknesses	High	Risk Mitigation: By implementing strong authentication protocols, monitoring user behavior, staying updated with encryption standards, and regularly patching and updating encryption software, organizations aim to reduce the likelihood and impact	Applicable	1. Implement strong authentication protocols, such as multi-factor authentication, to prevent unauthorized access. 1. Regularly monitor and analyze user behavior for any signs of suspicious activities. 2. Stay updated with the latest encryption standards and best practices. 2. Regularly patch and update encryption software.	Likelihood: High Impact: High Severity: High

			of potential threats.			
1. Unauthorized modification of backup data 2. Unauthorized escalation of privileges	1. Inadequate data integrity controls 2. Inadequate access control mechanisms	High	Risk Mitigation: By implementing the mentioned countermeasures, organizations aim to reduce the likelihood and impact of potential threats to the backup system.	Applicable	1. Implement data integrity mechanisms, such as checksums or digital signatures, to detect and prevent unauthorized modifications of backup data. 1. Use secure storage systems and encryption to protect the integrity of backup data at rest. 2. Implement strong access control mechanisms, such as privileged access management and least privilege principle. 2. Regularly review and update access control policies and permissions.	Likelihood: Medium Impact: High Severity: High

1. Attackers disrupting the availability of the web interface 2. Unauthorized modification of web application data	1. Lack of robust availability safeguards 2. Inadequate input validation and data integrity controls	🟥 High	Risk Mitigation: By implementing the mentioned countermeasures, organizations aim to reduce the likelihood and impact of potential threats to the web application interface.	Applicable	1. Implement measures to mitigate distributed denial-of-service (DDoS) attacks, such as load balancing and rate limiting. 1. Monitor network traffic and implement intrusion detection and prevention systems. 2. Implement data integrity checks and validation on the server-side. 2. Encrypt sensitive data at rest.	Likelihood: Medium Impact: High Severity: High

1. Users denying their actions within the mobile app interface	1. Insufficient logging and audit trail mechanisms	Medium	Risk Mitigation: By Implementing comprehensive logging and auditing mechanisms and ensuring the tamper-proof and tamper-evident nature of logged events, organizations aim to reduce the likelihood and impact of users denying their actions within the mobile app interface.	Applicable	1. Implement comprehensive logging and auditing mechanisms to track user actions and transactions. 1. Ensure logged events are tamper-proof and tamper-evident.	Likelihood: Low Impact: Medium Severity: Medium

1. Theft, vandalism 2. Insider threats	1. Inadequate physical security 2. Weak user access controls	Medium	Risk Mitigation: By implementing the mentioned countermeasures, organizations aim to reduce the likelihood and impact of potential threats to the server infrastructure.	Applicable	1. Implement physical access controls such as locked server rooms, CCTV surveillance, and entry logs. 1. Use secure server racks and cabinets. 2. Implement strong user access controls, including role-based access and least privilege principles. 2. Educate users about security best practices and policies.	Likelihood: Low Impact: Medium Severity: High
1. Data breaches 2. Phishing attacks	1. Insufficient encryption 2. User susceptibility to social engineering	High	Risk Mitigation: By implementing the mentioned countermeasures, organizations aim to reduce the likelihood and impact	Applicable	1. Implement strong encryption protocols for financial statements at rest and in transit. 1. Implement access controls and permissions to limit data exposure. 2. Educate employees about phishing attacks and	Likelihood: Medium Impact: High Severity: High

			of potential threats to the financial statements.		social engineering techniques. 2. Use multi-factor authentication for sensitive financial systems.	
1. Malware infection	1. Unsafe downloads or malicious files	Critical	Risk Mitigation: By implementing the mentioned countermeasures, organizations aim to reduce the likelihood and impact of potential threats to the multimedia content	Applicable	1. Implement strict download and file validation policies. 1. Educate users about safe browsing habits and avoiding suspicious downloads. 1. Use reputable antivirus and antimalware solutions.	Likelihood: High Impact: High Severity: High

1. Data loss 2. Data leakage	1. Inadequate backup procedures 2. Insecure data transmission	High	Risk Mitigation: By implementing the mentioned countermeasures, organizations aim to reduce the likelihood and impact of potential threats to the user data.	Applicable	1. Regularly backup user data and verify the integrity of backups. 1. Store backups in secure off-site locations. 1. Test backup restoration procedures. 2. Implement secure transmission protocols such as encryption and VPNs. 2. Use secure APIs and enforce data encryption during transit. 2. Regularly monitor network traffic and detect unauthorized data transfers.	Likelihood: Medium Impact: High Severity: High

1. Code tampering or modification 2. Insecure configuration	1. Inadequate change management and version control 2. Weak or insecure default configurations	High	Risk Mitigation: By implementing the mentioned countermeasures, organizations aim to reduce the likelihood and impact of potential threats to the software codebase.	Applicable	1. Utilize secure version control systems and enforce strict change management processes. 1. Implement code signing and integrity checking mechanisms. 2. Follow secure configuration guidelines and best practices. 2. Use secure encryption and authentication algorithms. 2. Regularly test and validate the security of the configuration settings.	Likelihood: Medium Impact: High Severity: High

1. Financial Loss 2. Market Competition	1. Economic downturn, market volatility, fraud, embezzlement, or mismanagement 2. Intense competition, new entrants, or disruptive technologies	High	Risk Mitigation: By implementing the mentioned countermeasures, organizations aim to reduce the likelihood and impact of potential threats to stakeholders and investors.	Applicable	1. Implement strong financial controls and auditing mechanisms 1. Stay updated on regulatory and compliance requirements. 2. Conduct market research and analysis to identify trends and competitors. 2. Foster strong relationships with customers and stakeholders.	Likelihood: High Impact: High Severity: High

RISK MONITORING AND REVIEW:

1. Risk identification:

Identify potential risks that could pose a threat to the success of WhatsApp. These risks could include financial aspects, communication issues, network vulnerabilities, user data protection, handling of multimedia content, competition from other messaging apps, and changes in user preferences or behavior.

2. Risk assessment:

Assess the likelihood and impact of each identified risk. For example, there might be a high probability of a security breach, which could result in significant consequences such as loss of user trust and damage to WhatsApp's reputation.

3. Risk tracking:

Continuously monitor and track the identified risks. Stay vigilant to any changes in the risk landscape and ensure appropriate measures are in place to effectively mitigate or manage these risks.

4. Risk evaluation:

Evaluate the effectiveness of risk responses and determine if any new or modified risks have emerged. It may be necessary to adjust the risk response plan to accommodate changes in user preferences or other factors.

5. Risk response planning:

Implement strategies to minimize or eliminate the identified risks. For instance, WhatsApp can conduct user surveys to gather insights into preferences and behavior, and use that information to enhance risk mitigation strategies.

6. Risk communication:

Keep stakeholders, including the WhatsApp team, investors, and users, informed about the risks. Regularly update stakeholders on the status of identified risks and any changes to the risk response plan.

Risk monitoring involves the following activities:

1) Identifying new risks: Continuously identify and evaluate new risks that may arise due to technological advancements, evolving user behavior, or industry developments.

2) Promptly responding to new risks and threats: Stay proactive and respond quickly to emerging risks or threats, implementing appropriate measures to effectively address them.

3) Enhancing existing plans and safeguards: Regularly review and improve risk response plans and safeguards to ensure they remain effective and aligned with the evolving risk landscape.

4) Continuous system upgrades: Keep the WhatsApp system up to date by applying the latest security patches and upgrades, addressing any vulnerabilities and staying protected against emerging risks.

5) Ongoing training for the team and employees: Provide continuous training and education to the WhatsApp team and employees, enhancing their awareness of risks, best practices, and security protocols.

6) Monitoring the impact of implemented countermeasures: Continuously monitor the effects and effectiveness of implemented risk mitigation measures, identifying any unintended consequences or areas for improvement.

AUTHENTICATION TECHNIQUES:

1. Password-based authentication: Users are required to provide their phone number and set a password during the registration process to access their WhatsApp accounts.

2. Two-factor authentication: WhatsApp supports two-factor authentication, where users need to enter a verification code sent via SMS or generated within the app, in addition to their password, to verify their phone number.

3. Session management: WhatsApp maintains user sessions tied to their device and manages authentication throughout the session, ensuring secure access and preventing unauthorized access.

4. End-to-end encryption: All messages, calls, photos, and videos sent through WhatsApp are protected with end-to-end encryption, meaning only the sender and intended recipient can access the content.

5. Transport layer security (TLS): WhatsApp employs TLS protocol to secure data in transit between the user's device and WhatsApp servers, encrypting the communication and verifying the server's identity.

6. Phone number verification: During registration, users must verify their phone number by entering a verification code sent via SMS or phone call.

7. Biometric authentication: WhatsApp allows users to enable biometric authentication on their devices, such as fingerprint or face recognition, to add an extra layer of security when accessing their WhatsApp accounts.

8. Account linking with third-party services: Users can link their WhatsApp accounts with certain third-party services, such as Facebook, to log in using their credentials from the linked service.

9. Account recovery via email: WhatsApp offers an account recovery option via email, allowing users to regain access to their accounts by initiating the recovery process using their registered email address.

10. Account suspension and verification: WhatsApp detects and suspends accounts that violate its terms of service or engage in suspicious activities. Users may need to go through a verification process to regain access to their accounts if they are suspended.

PROPOSED ENHANCED SECURITY APPROACH AND CIA IMPROVEMENT: [16]

Even while WhatsApp usages end-to-end encryption, there are still security problems. These include the incapability to encrypt metadata, limitations on message forwarding controls, and vulnerability to social engineering attacks. To solve these problems and increase user security generally, an upgraded security methodology is suggested. Encoding all media files from beginning to end would guarantee total security during communication. Message metadata, counting sender and recipient characteristics and timestamps, is not encrypted at this time. To protect user privacy and further ambiguous conversation specifics, this data should be encoded. Putting stronger key management procedures in place such as post-quantum coding, would provide ongoing defense against cryptographic outbreaks in the future. Restored User Control Including more sophisticated selections for removing messages, fine-grained message promotion controls, and improved confirmation measures. Greater education and transparency including clearly stated security documents encouraged to find and report vulnerabilities in WhatsApp. By doing this, the platform's overall security attitude would be enhanced and security susceptibilities could be lectured more rapidly.

Improved Security Method Enhances WhatsApp's CIA Triad

There are three key security goals are the prominence of the CIA triad, a basic security model; confidentiality, integrity, and availability.

Confidentially; Encryption for media and metadata from opening to finish guarantees secrecy by limiting access to message content and media files. Advanced key management even if an aggressor manages to obtain the encryption means, they will find it very difficult to decrypt messages thanks to strong key management procedures. Better message forwarding controls and Advanced options for disappearing messages preventing sensitive data from being kept on devices indefinitely.

Integrity; Messages and media files are threatened against handling during transmission and storage by end-to-end encryption. Improved verification procedures are more difficult for illegal users to access accounts and modify data when multi-factor confirmation and biometric verification are used. Independent security audit finds and fixes WhatsApp's system faults, stopping hacks from using them to tamper with data.

Availability; More robust verification procedures lower the possibility of denial-of-service attacks and account appropriation, which can bar honest users from using WhatsApp. Working together with security experts as with cyber security groups and open bug plenty programs aid in the identification and determination of technical issues that could damage service accessibility. Transparency also increased since users may use educational materials and clearer documentation to acquire how to use WhatsApp securely.

In conclusion, by adding more verification layers for integrity, applying strong encryption for confidentiality, and including procedures to maintain service accessibility while actively addressing and avoiding security occurrences, the proposed security approach improves the CIA triad for WhatsApp. The goal of this all-inclusive approach is to give customers access to a safe and reliable communication stage.

CONCLUSION:

WhatsApp, being a widely used messaging application, offers convenience and secure communication to its users. However, it is important to recognize that no digital platform is completely immune to vulnerabilities and security risks. Through the analysis of WhatsApp's current security situation, we have identified several potential risks, including malware attacks, encryption backdoors, account hijacking, and risks associated with third-party apps. To mitigate these vulnerabilities, we have proposed a risk management plan that focuses on various risk control techniques. These techniques include user education, end-to-end encryption, two-factor authentication, regular security updates, app store verification, continuous monitoring, security audits, and penetration testing. By implementing these measures, WhatsApp can enhance its security measures, protect user data, and provide a safer messaging experience for its users. It is crucial for WhatsApp to continuously evaluate and monitor potential risks, adapt security measures to emerging threats, and regularly review its risk mitigation strategies. By maintaining a proactive and comprehensive approach to risk management, WhatsApp can strengthen its security posture, maintain user trust, and ensure the privacy and integrity of user communications. Overall, while no system can be completely risk-free, implementing robust risk mitigation and control measures can significantly enhance the security of WhatsApp and contribute to a safer and more secure messaging environment for its millions of users worldwide.

REFERENCES:

[1] Andries, S., tefania, Miron, A.-D., Cristian, A., & Simion, E. (2022). *A Survey on the Security Protocols Employed by Mobile Messaging Applications*. https://doi.org/https://eprint.iacr.org/2022/088.pdf

[2] Jayathilaka, S. (2018, September 4). Behind the scenes of Chat Applications - Sudaraka Jayathilaka - Medium. Medium. https://sudarakayasindu.medium.com/behind-the-scenes-of-chat-applications-38634f584758

[3] Faife, C. (2022, September 27). WhatsApp discloses critical vulnerability in older app versions. The Verge. https://www.theverge.com/2022/9/27/23374468/whatsapp-bug-video-call-vulnerability-cve

[4] Frew, J. (2023, July 16). Is WhatsApp Safe? 6 Scams, Threats, and Security Risks to Know About. MUO. https://www.makeuseof.com/tag/4-security-threats-whatsapp-users-need-know/

[5] *Whatsapp : Security vulnerabilities, CVES*. Whatsapp : Security vulnerabilities, CVEs. (n.d.). https://www.cvedetails.com/vulnerability-list/vendor_id-19851/Whatsapp.html

[6] National Institute of Standards and Technology. (2012). NIST Special Publication 800-30, Risk Management Guide for Information Technology Systems. https://nvlpubs.nist.gov/nistpubs/legacy/sp/nistspecialpublication800-30r1.pdf

[7] Bogos, C.-E., Mocanu, R., & Simion, E. (2023). A security analysis comparison between Signal, WhatsApp and Telegram. *Cryptology ePrint Archive*.

[8]Carpay, T., & Lontorfos, P. (2019). WhatsApp End-to-End Encryption: Are Our Messages Private? *Retrieved, 2*(05), 2020.

[9]Davies, G. T., Faller, S., Gellert, K., Handirk, T., Hesse, J., Horváth, M., & Jager, T. (2023). *Security analysis of the whatsapp end-to-end encrypted backup protocol.* Paper presented at the Annual International Cryptology Conference.

[10] Dev, J., Das, S., & Camp, L. J. (2018). *Privacy Practices, Preferences, and Compunctions: WhatsApp Users in India.* Paper presented at the HAISA.

[11] Endeley, R. E. (2018). End-to-end encryption in messaging services and national security—case of WhatsApp messenger. *Journal of Information Security, 9*(01), 95.

[12] Holmes, S., & Nicholls, D. (1989). Modelling the accounting information requirements of small businesses. *Accounting and Business Research, 19*(74), 143-150.

[13] Krisdayanti, D. E., Ihsan, M. K., & Sevrika, H. (2023). An Analysis Of Students' Responses To English Teaching Material In Google Classroom And Whatsap At SMAN Muko-Muko. *Jurnal Horizon Pendidikan, 3*(1), 23-36.

[14] Mols, A., & Pridmore, J. (2021). Always available via WhatsApp: Mapping everyday boundary work practices and privacy negotiations. *Mobile Media & Communication, 9*(3), 422-440.

[15] Mueller, R., Schrittwieser, S., Fruehwirt, P., Kieseberg, P., & Weippl, E. (2014). *What's new with whatsapp & co.? revisiting the security of smartphone messaging applications.* Paper presented at the Proceedings of the 16th International Conference on Information Integration and Web-based Applications & Services.

[16] Patidar, P. K., Tomar, D. S., Pateriya, R., & Sharma, Y. K. (2023). *A Threat modeling approach to analyze and mitigate WhatsApp attacks: A Review.* Paper presented at the 2023 IEEE International Students' Conference on Electrical, Electronics and Computer Science (SCEECS).