UNIVERSITY OF SOUTHERN BRITTANY
FACULTY OF SCIENCES AND ENGINEERING SCIENCES

Secure Advanced Programming

CSPN

Signal App Evaluation

Advisor: Thibaut Henin

LORIENT/FRANCE, DECEMBER 2022

Member list

No.	Full name	Student ID
1	Paweł Borsukiewicz	e2205101
2	Zakaria Belkadi	e2205119
3	Fares Kechid	e2205111
4	Fatih Durmaz	e2205020
5	Ibrahim Yaghi	e2205106

Contents

1 Introduction

1.1 Product Identification

Producent	Signal Messenger LLC
Version	6.0.4
OS required	Android 4.4 or later
Product's commercial name	Signal
Product's category	Mobile messenger application
Organization URL	https://signal.org/

1.2 Abbreviations

ATH	Authentication
AV	Availability
ATR	Authorization
TOE	Target of Evaluation
INT	Integrity
PBKDF2	Password-based key derivation function
CF	Confidentiality

2 Product and TOE Description

2.1 Product Overview

Signal (fig 1) is a free, privacy-focused messaging and voice talk app that users can use on Apple and Android smartphones, and via desktop. Phone number is needed in order to join. The main features of the app are text or make voice or video calls with friends, either one-on-one or in groups, and use emoji reactions or stickers just like in other apps.

Furthermore, Signal is a secure, free, and open source messaging application that uses end-to-end encryption to securely send and receive all kinds of communications with other Signal users. Using the Internet for all encrypted communication, Signal comes highly recommended by some of the top privacy and security advocates.

Figure 1: Signal Application Overview

2.2 TOE Software Architecture

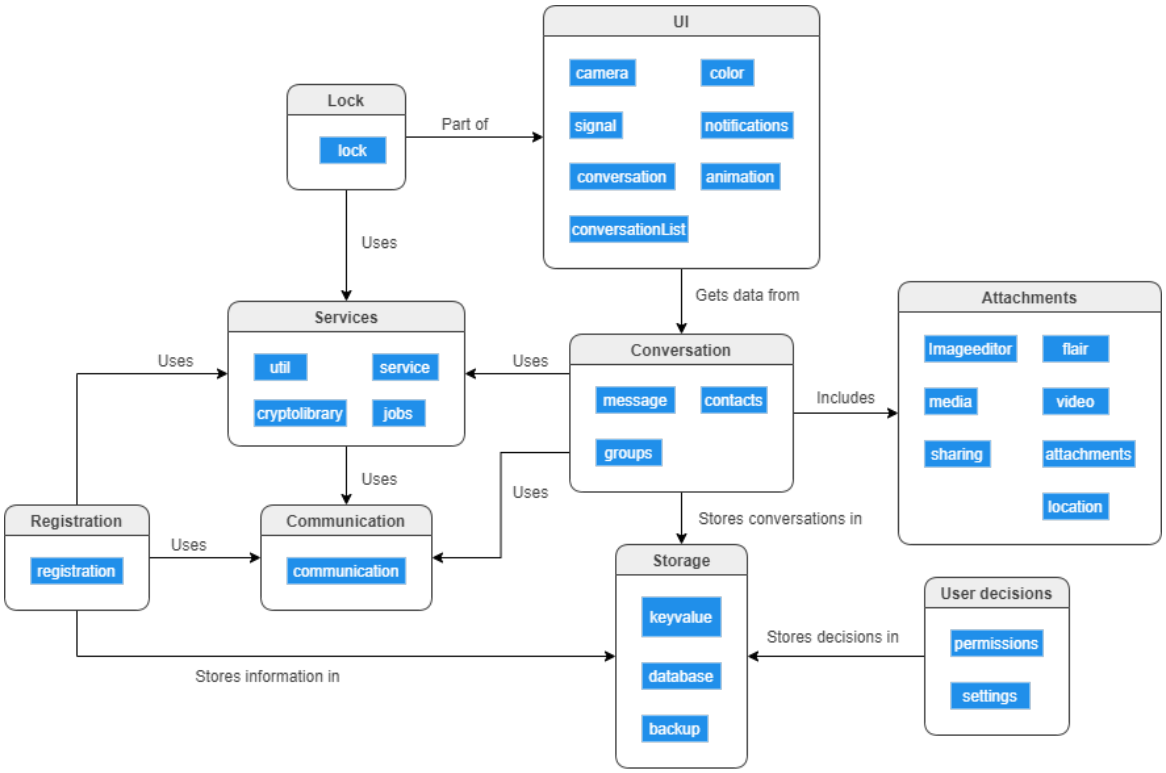

Figure 2: Signal Architecture Overview

The diagram 2 is the result of a high-level decomposition of the android signal app. It regroups sub-components with the same functionalities (blue rectangles) into overall main elements (white rectangles). It also includes relationships between different modules, as represented with arrows in the figure 2.

- **UI**: Which stands for User-interface, is basically what the user is exposed to. This module includes the overall app and what's included in it, such as the conversations and their lists, notification, colors animations, the usage of the camera, etc.
- **Conversation**: This module is one of the most important in the signal app. This is because of two things, the first one being the fact that it includes the main functionality of the app (messaging contacts groups). The second reason is that the whole architecture is centralized around this component, and that almost all other modules have relationships with this part of the architecture.
- **Storage**: This module includes the databases used in the signal servers and key-values that they include. Backups stored in the user's phone are also found in this component.
- **Attachment**: This includes any possible content that can be sent in a message, other than text, such as images, videos, location or even pdf files. User decisions: This module regroups components related to the

user's decision regarding the app's usage of phone resources, such as permissions and settings.

- **Lock**: This component provides the PIN feature, which allows the user to register to the app using his phone number.
- **Service**: As its name suggest, this component contains services that a user can take advantage of such as cryptolibrary, which allows an end-to-end encryption of data.
- **Communication**: This part of the architecture takes care of messaging, whether it's by SMS or video call.
- **Registration**: With the aid of the lock module, this component allows the registration of users.

2.3 TOE Features

Register and Delete Account: Android and iOS devices install Signal using the existing phone number, which must receive insecure SMS or phone calls. The user receives a verification code via SMS. If they are unable to receive SMS, they can request a verification call. The user taps the call button or "I didn't receive a code" button after the timer finishes counting down. Not receiving the verification code means to confirm that:

- Mobile is not connected to the network and cannot receive SMS messages or phone calls.
- Phone number is entered wrong.
- Include any leading zeros in the international phone number.
- Blocked messages from unknown senders.
- Opted out of receiving business or transactional messages from unknown senders by responding "STOP" to them.

To receive the verification code by SMS:

- The user shall call #611# and ask the representative to remove the "Short-code Blacklist" for their account.

To receive the verification code by call:

- The user shall call #632# to turn off Scam Block

After the verification process the user will be asked to create a PIN for their account. This PIN is four digits by default, but they can choose whether to make it an alphanumeric password or to use a longer PIN. This helps the user to recover their profile, settings, contacts, and block list if the user ever loses or switches devices.It supports features like non-phone number based identifiers. A PIN can also serve as a registration lock.

After registration, the user is able to edit the profile. Signal requires only a first name, and it does not need to be the user's real name. Avatars can include nicknames or even emojis.

Delete Account: The user can permanently disable the phone number from being recognized as a Signal user by deleting the account from the registered mobile phone. Deleting a Signal account will delete all the data

associated with it as well. This includes all the chat messages, media, contacts, and associated data. If users sign up again with the same number, they will be starting with a blank slate. If users have any sensitive data in Signal, we recommend that they export it before starting the deletion process.

Edit Profile and Personal Data: User's Signal profile, composed by their name and picture, is shown alongside the user's existing phone number during the communication with other users. Users can either set a profile picture during the initialization or afterwards. Also, they can change their profile picture in Signal anytime from the app's settings menu. Users tap the avatar icon at the top left of the screen to get to the profile picture settings.

Messaging: Through Signal messages, users can send text messages, images, videos, GIFs, voice notes, contacts, location, and stickers. They also have the ability to quote particular messages, use message reactions, send one-time viewable images and videos, and use disappearing messages. For personal data Signal messages app uses end-to-end encryption to keep users' messages private.

Voice message: Users can tap and hold the mic button to record a voice note and release it to send it or slide to the left to cancel it. They also have the option to swipe up to lock the voice to go hands free. When users leave the app while recording a message, they will be presented with a draft when they open the app the next time. Also for the security of voice message it is state of the art end to end encryption keeps user conversations secure. Signal cannot listen to the voice messaging and no one else can either.

Video and voice calling: Users can make both voice and video calls on Signal. Similar to text messages, voice and video calls are private. Users will be prompted to grant the camera and microphone permissions at the first time they make or receive a Signal call. Signal calls, both voice and video, are end-to-end encrypted.

Group Chats and Group Calling: This feature allows users to create a group with other people they select. It also gives access to admin controls, mentions, and group updates. For group calling when one of the group members initiates a call or video call this will send an alert that will appear in the group chat history. When the call starts, users can control their videos, microphone and tap the red phone button to leave the call when they are done.

2.4 Product Usage

The TOE is a mobile application available at Google Play store. After download and installation a user shall create or log into an account using a backup file. In order to create an account the user has to provide their phone number and confirm selection. Subsequently, confirmation code is sent as an SMS message to their device. After entering the code, the user shall follow instructions presented on a screen of their phone to finalize the registration process.

When the user has successfully passed the registration step, they are presented with multiple functionalities. The most basic one is to send messages and files to other users of the application, who can be found using their phone numbers. Chatting feature is extended with phone calls and video calls. All of the data processed by the application is end-to-end encrypted and is not stored on the application servers. As a result, the application has to store all data on the users' devices. Furthermore, users can create group chats to communicate with a higher number of accounts at once.

2.5 Product Environment

TOE is designed as a mobile application running on Android Operating System 4.4 or later.
The TOE environment is composed of:

- All components of users' mobile devices, such as software, hardware or camera, that are necessary for application's proper operation
- Server infrastructure used to transmit data
- Database infrastructure used to store phone numbers of application users
- All other software components that interact with our TOE, including third parties.

3 Security Problem Definition

3.1 Assets

Asset	Sensitivity	Type	Definition
Phone Number	CF, INT,	Business	The phone number is used to provide service to Signal's users. It is the way Signal recognizes the user.
Account Information	CF, ATH, ATR,	Business	Users can add personal information to their profile. This personal information is called Account Information. This information can contain media and textual data.
Message Sending	CF, INT, ATH, ATR, AV	Business	Exchange of messages between parties and groups is in this category.
Message Storing	CF, INT, ATH, ATR	Business	Users can access any received or sent message. Users can also create a backup of their data. Messages are also included in the backup.
Contacts	CF, ATH, ATR, AV	Business	Contact information of the user is used to discover other Signal users in the contacts list.
User Support	CF	Business	When a user contacts the Signal User support, the user shares information with Signal to investigate the issue.
Call receiving and making	CF, ATR, ATH, AV	Business	Users may call their contacts via Signal application. This asset covers delivery and receival of calls.
Calls Storage	CF, ATR, ATH, INT	Business	Users can access the history of calls any time. Users can also create a backup of their data. Call history is also included in the backup.
Server	CF, INT, AV	Support	Execution of requests and instructions on the server.
Pin & Backup Key	CF, INT, ATR, ATH	Support	Backup key is created with a backup request. This key is asked to write down while creating a backup. Pin is another key which helps users recover the account.
Configuration Files of Server	CF, INT, ATH, ATR	Support	Application server configuration files define the available application servers, their configurations, and their contents.
Source Code	INT, ATH, ATR	Support	The application's source code is public and can be accessed by anyone. This source code is the one that is run on servers.

Table 1: Assets explanation

3.2 Subjects

Subject	Definition
S.User	User of SIGNAL on the device, able to: Authenticate on the device using phone number. Validate phone number. Manage App configuration. Send messages. Perform phone calls
S.Signal_servers	Signal Servers are in charge of: Facilitating the discovery of contacts who are also registered Signal users. Automation of exchange of users' public keys.
S.Issuers	The Issuer or its service provider is in charge of: Maintaining centralized servers. Management of S.User data.
S.Merchant	The merchant is the third-party receiving payment through a MobileCoin.

Table 2: Subjects who interact with the TOE

3.3 Security Properties

The Protection of the assets means a security property that we wish to maintain. Details of the security properties depending on the assets given in table 3. Asset - Security property coverage is given in table 4

3.4 Assumptions

Physical security: Physical computer security is the application of physical barriers and control procedures as a preventive measure against threats to resources and confidential information; it refers to the controls and security mechanisms around data processing equipment and storage devices, such as building and office access controls, security cameras, sensors and biometric identity systems, among other measures. Physical security also encompasses the means of remote access implemented to protect the equipment. For signal's architecture, we assume that the servers are protected against unauthorized usage, alongside the user's phone which is the responsibility of its owner.

Users and administrators awareness: Security awareness provides users with the cybersecurity knowledge they need to protect the apps's confidential information from cybercriminals. This field of security is for everyone authorized to access, store, share or modify the signal's data. It is assumed that the administrators as well as users are competent, trustworthy and well trained.

Logs checking: It is assumed that we already have a logging system installed on the signal servers, and that the administrators regularly check those logs to react correspondingly.

Asset	Security property	Security concern
Phone Number	CF, INT, ATH, ATR	The phone number must be confidential, and must be correct for the application to work properly. Only the owner of the account can change his phone number.
Account Information	CF, ATH, ATR,	All the account information is personal and only the account user can change it.
Message Sending	CF, INT,ATH, ATR, AV	In case of any messages disclosure or tampering the company will lose its users and its value. Subsequently, this asset has to work properly without any issues.
Message Storing	CF, INT, ATH, ATR	This asset has similar properties and security concerns with Message Sending.
Contacts	CF, ATH, ATR, AV	Only the user of the account can see the contact list, and it must always be available.
User Support	CF	During the support of the user by the signal employees, confidential information should not be disclosed.
Call receiving and making	CF, ATR, ATH, AV	In a call conversation, the caller and the receiver both must be authenticated.The unavailability of this asset can affect the company's reputation negatively.
Calls Storage	CF, ATR, ATH, INT	Same as call operations, call storage also is very important and must carry out all its security properties.
Server	CF, INT, AV	Servers contain extremely important services such as sessions. Therefore, confidentiality is mandatory as well as availability because if the server is down, the application won't work. All of the services in the server must not be altered by unauthorized users.
Pin & Backup Key	CF, INT, ATR, ATH	Only the owner of the account is authorized to manage Pin and Backup key. Those assets are confidential because by using them, a third party can access other confidential data. These assets should remain the same because any unauthorized modification to them prevents users from using related services.
Configuration Files of Server	CF, INT, ATH, ATR	The configuration files contain the settings of the application. For instance, database files contain credentials which are mandatory in order to connect to the database. Only specific persons are allowed to make changes to these files.
Source Code	INT, ATH, ATR	This asset is the main engine of the app, because the working system of the app is based on its logic. Also this asset contains the app itself. The changes to the source code must be managed by an authorized person.

Table 3: Security properties explanation

	CF	INT	ATH	ATR	AV
Phone Number	+	+	+	+	
Account Information	+		+	+	
Message Sending	+	+	+	+	+
Message Storing	+	+	+	+	
Contacts	+		+	+	+
User Support	+				
Call receiving and making	+		+	+	+
Calls Storage	+	+	+	+	
Server	+	+			+
Pin and Backup Key	+	+	+	+	
Configuration Files of Server	+	+	+	+	
Source Code		+	+	+	

Table 4: Asset - security property coverage

3.5 Threats

Fraudulent modification of message or personal data: Fraudulent modification occurs when personal information is stolen or taken from the Signal system without the owner's knowledge or authorization or when it is done from the user side through phishing or SQL injection. Once the attacker has unauthorized access to all the personal data of a Signal user, he is able to modify that data, send it to the wrong recipient, and lose access to that data.

Unauthorized access of messages and data: Malicious non-authorized users of the TOE authorized to perform certain actions and access certain information gain access to commands or information they are not authorized for. Consequently, attackers had the ability to modify TOE configuration data or log information without authorization. This is when someone gains access to a website, program, server, service or other system of Signal using someone else's account or other methods. For example, if someone kept guessing the password pin for an account that was not theirs until gained access, it is considered unauthorized access.

Unauthenticated Access: Malicious non-authenticated users gain access to the TOE and modify its configuration data without permission.

Personal information Disclosure: This is also known as information leakage, for example if Signal unintentionally reveals sensitive information. Depending on the context, this may leak all kinds of information to a potential attacker, including: Data about users, such as call history, call, and PIN code. This may provide access to source code files via temporary backups and hard-coding API keys, IP addresses, database credentials, and so on in the source code.

Unauthorized Configuration File Access and file Changes: The configuration files contain values for different settings that affect the use of the database and server. Any unauthorized changes to these files can result in invalid authorization and availability issues throughout the server.

Execution on Servers: As part of the threat, attackers implement basic status codes for communication. For example, the server can be interactive; the attacker can send execution commands to the server, which would result in Signal reporting back sensitive information of the clients.

Account Theft, Backup Access: Cyber-attacks of this type can come in three different forms: malware attack, phishing attack, and SQL injection attack. The attacker could, for example, send an urgent email to the Signal user requesting them to click on a specific link to authenticate. The attacker will then be able to access the user account and all of his Signal history as a result of a phishing attack.

DoS Attacks: It occurs when an attacker prevents legitimate Signal users from accessing Signal services. It is typical for attackers to flood web servers, systems, or Signal networks with traffic in order to overwhelm the victim's resources and prevent anyone else from accessing them.

	Phone Number				Account Information			Message Sending				Message Storing			
	CF	INT	ATR, ATH	-	CF	-	ATR, ATH	CF	INT	ATR, ATH	AV	CF	INT	ATR, ATH	-
Fraudulent modification of message or personal data		x							x				x		
Unauthorized access of messages and data	x		x		x		x	x		x		x		x	
Unauthenticated Access	x		x		x		x	x		x		x		x	
Personal information Disclosure	x				x										
Account theft, backup access	x				x			x	x			x	x		
Execution on Servers	x	x							x		x				
DoS Attacks											x				
Configuration file access and file changes											x				

Table 5: Threat assets coverage

	Contacts				User Support			Call receiving and making				Calls Storage			
	CF	-	ATR, ATH	AV	CF	-	-	CF	-	ATH, ATR	AV	CF	INT	ATH, ATR	-
Fraudulent modification of message or personal data													x		
Unauthorized access of messages and data	x		x											x	
Unauthenticated Access	x		x					x		x				x	
Personal information Disclosure					x										
Account theft, backup access					x			x			x				
Execution on Servers				x							x		x		
DoS Attacks				x							x				
Configuration file access and file changes				x							x				

Table 6: Threat assets coverage - Part 2

	Server				Pin and Backup Key				Configuration Files of Server				Source Code			
	CF	INT	-	AV	CF	INT	ATH, ATR	-	CF	INT	ATH, ATR	-	-	INT	ATH, ATR	-
Unauthorized Access					x	x	x		x	x	x			x	x	
Unauthenticated Access					x	x	x		x	x	x			x	x	
Account theft, backup access					x	x										
Execution on Servers	x	x		x					x	x						
DoS Attacks				x												
Configuration file access and file changes	x	x		x					x	x	x					

Table 6: Threat assets coverage - Part 3

4 TOE Security Functions

4.1 Client Side Security Functions

	Integrity Check	Access Control	End-to-End Encryption	Secure Storage	Audit Trail
Fraudulent modification of message or personal data	+	+		+	+
Unauthorized access of messages and data		+	+	+	+
Unauthenticated Access		+	+	+	+
Personal information Disclosure		+	+	+	
Account theft, backup access			+		+

Table 7: Security function - threat coverage Part 1

4.1.1 Integrity Check

Underlying HMAC-SHA256[3], a SHA256-based Hash-Based Message Authentication Code, provides the integrity. TOE presents Integrity Check to the user in a form of safety number[1]. Each one-to-one conversation is linked with a special number that helps to assure that the Man-In-The-Middle attack did not occur. In order to access the number, one shall open a chat with a contact, then tap “Settings” and select the “View security number” option from the settings menu.

Every change of the security number, that is detected by the application, is immediately reported to the user. Such warnings are most frequently displayed when the user switches to a new device or re-installs the TOE, however, they may signify that there has been an attempt to tamper the transferred data. TOE users are advised to verify their safety numbers as in case of its change at the side of the recipient, the user must manually confirm that they still want to send the message.

4.1.2 Access Control

Sensitive data is protected by Signal access control strategy. By using access control gateways, only those whose identities can be verified can access data. Fraudulent modification of message or personal data: Signal follows the General Data Protection Regulations (GDPR) to protect the privacy, unauthorized access, and provide the security of users’ data from modification.

Unauthorized access of messages and data: Among all levels of access control, Mandatory access control is considered to be the most stringent to prevent this threat. Under a MAC environment, access to resource data is controlled by the settings defined by the Signal system administrator. This means access to resource data is controlled by the operating system based on what the system administrator of Signal configured in the settings.

It is not possible for users to change access control of a data resource. MAC uses "security labels" to assign resource data on a system. There are two pieces of information connected to these security labels: classification (high, medium, low) and category (specific department or project – provides "need to know"). Each user account is also assigned classification and category properties. This system provides users access data if both properties match. If a user has high classification but is not part of the category of the object, then the user cannot access the data.[9]

Unauthenticated Access: To prevent unauthenticated access through access control . Signal identifies users by verifying various login credentials, which include the phone number by sending an SMS code and PIN code as a password. If an unauthenticated user wants to login using an existing user phone number this will be impossible because there is an authentication process that should be done before login which is the SMS code that will be sent to that number.

Personal information Disclosure: Signal controls access to non-public information, documents, messages, etc., in order to ensure data confidentiality. Users should grant access to data only to those with a need-to-know basis, based on the principle of least privilege. In this way, personal information will not be disclosed.

4.1.3 Audit trail

Audit trail (or audit log) is a relevant chronological record of the actions, intended to track the events that take place in a system. In a database, it is, most of the time, implemented in order to verify what happened, especially in terms of values before or after the modification. It can be used both for security (who did what), as well as functionally (when was the change made, why was the change to this specific value).

Logging feature, present within the TOE, was implemented using bidirectional websocket protocol as specified in RFC 6455[2]. For that reason, traditional logging of all requests and responses could not be implemented. One event log is created when connection is established and one when it is terminated. Additionally, beyond previously mentioned two logging cases, a series of error logs has been developed to monitor any undesired or erroneous behavior of the TOE. Further, the audit security feature is extended by cloud logging. Parts of the feature are developed using ready-made solutions provided by cloud provider - Google Cloud logging.

4.1.4 End-to-End Encryption

Signal is designed to never collect or store any sensitive information[6]. To support this claim, Signal implements end-to-end encryption in almost every feature. Signal uses RSA for key exchange and AES-GCM for symmetric encryption[4].

End to End encryption covers; sent and received messages, made and received calls. Therefore this function prevents unauthorized access to messages and data. A user needs to have their assigned session key to communicate. A user also needs to have their private key to view their local data. This encryption and viewing operations are done in the background.

If a user wants to create a backup, a private key which is dedicated to backup is created. The backup is encrypted and this private key is used for decryption. Even if an account is stolen, without having this private key, backup cannot be restored[5].

Signal also encrypts the personal data which is stored in the user's device. Even if data of the user is obtained by a third party, the obtained data is encrypted. Therefore this prevents disclosure on the client side.

Signal stores phone numbers on the servers. The phone number of the user is used to authenticate the user. This is also stored in an encrypted way. Therefore, even if a third party obtains the data, it is encrypted. This prevents data disclosure on the server side.

4.1.5 Secure storage

TOE records no data about its users or the conversations taking place within the app. Once the messages are received and decrypted on a user's device, they are stored locally in a SQLite database that is encrypted with SQLCipher. The key to decrypt this database is also stored locally on the user's device and can be accessed if the device is unlocked.

Signal uses a sqlite db file at signal.sqlite for messages and data files, encrypted with the embedded sqlcipher extension, using AES-384 with a randomly generated password that's further whitened by PBKDF2. The key storage depends on the system's version of the key store is: KeyChain in iOS, KeyStore in Android, Credential Manager in Windows, etc. Exported files and histories use the same encryption method with a newly generated key each time.

4.2 Server Side Security Functions

	Access Control	Input Filtering	Firewalls	Load Balancing, Having Independent Servers	Rate Limiting, Throttling
Execution on Servers		+	+		
DoS Attacks	+		+	+	+
Configuration file access and file changes	+				

Table 8: Security function - threat coverage Part 2

4.2.1 Access Control

As already mentioned in the client side security functions, access control is a measure that assures that only the entities authorized to perform a given action can perform it. It is especially important in the context of the direct access to the servers and their configuration files. Only a predefined list of users, Signal employees or contractors, shall be allowed to read and modify the previously mentioned resources. Misconfiguration of the server files can directly lead to DoS or alternatively it may facilitate other attacks taking as an aim disruption of the availability of TOE.

As TOE utilizes Amazon Web Services and Microsoft Azure non-physical servers, access control tools are provided by the cloud provider and shall be implemented by the Issuer. For instance, Microsoft Azure comes

with a role-based access control feature that is a main implementation of this access control security feature. Similarly, Amazon Web Services offer AWS Identity and Access Management functionality that is based on three key components -"“who”, “can access”, ”what”. Firstly, one has to precisely define all the users. Then, all of the resources have to be enumerated and at the end access rights for all combinations of users (or groups of users) and resources have to be decided upon and properly set.

4.2.2 Rate Limiting & Throttling

Rate limiting and throttling are mechanisms that are mainly used to prevent DDoS or DoS attacks. They are both based on setting a limit of requests that can be sent to or that are processed by the server. Rate limiting is implemented at the user level, while throttling is related to the network/server level. When a given threshold of requests is exceeded by the user, their requests are no longer processed by the server until the penalty period passes.

Rate limiting in the TOE is implemented within its REST endpoints utilizing[7] Redis open source data structure store. Additionally, in case of suspiciously excessive activity a user may be prompted to fill captcha to prove that an automated tool is not responsible for sending requests.

API throttling is the process of limiting the number of API requests a user can make in a certain period. An application programming interface (API) functions as a gateway between a user and a software application. The Throttling in the TOE, works this way:

1. A client/user calls an API that interfaces with a web application (Signal).
2. The API throttling logic checks if the current request exceeds the allowed number of API calls.
3. If the request is within limits, the API performs as usual and completes the user's task.
4. If the request exceeds the limit, the API returns an error response to the user.
5. The user will have to wait for a pre-agreed time period, or pay to make any more API calls.

4.2.3 Input Filtering

Execution on Servers: This could be due to SQL injection. SQL injection occurs when a malicious user input is accepted by the application and then used as part of a SQL statement to query the backend database.To change the query structure, an attacker can inject SQL control characters and command keywords (e.g., single quote (’), double quote ("), equal (=), comment (- -), etc.). These control characters are used with common SQL commands (e.g., SELECT, FROM, DELETE, etc.) to gain access, execute or retrieve data elements from a backend database. An input filtering method solves this problem by validating all incoming data and preventing any invalid data from being used by the application. Signal compiles a list of all malicious inputs, then verifies the external input against the compiled list. It then rejects inputs that are unfiltered[8].

4.2.4 Firewalls

A firewall is software and/or hardware that enforces a network security policy which defines what types of communications are allowed on the computer network. It monitors and controls applications and data flows, and decides which rule to apply, based on packet fields.

In order to provide security against several attacks, signal's internal network structure contains a demilitarized zone, which is a real life application of the defense-in-depth strategy. It defines a sub-network containing all public servers requiring different security policies than signal's LAN. These servers are protected by next-generation & web application firewalls, which operate in a stateful manner, meaning that they can apply policies on packets depending on previous data flows. This prevents attacks such as brute force (PIN), since an attacker sends nearly-identical requests to servers, with the only difference being in the PIN. Web application firewalls can also filter incoming data, preventing execution on server (SQL injection), or block data flows, which helps prevent or mitigate DoS attacks.

4.2.5 Load balancing

Load balancing refers to efficiently distributing incoming network traffic across a group of backend servers, also known as a server farm or server pool.

The TOE uses a load balancer who acts as the "traffic cop" sitting in front of its servers and routing client requests across all servers capable of fulfilling those requests in a manner that maximizes speed and capacity utilization and ensures that no one server is overworked, which could degrade performance. If a single server goes down, the load balancer redirects traffic to the remaining online servers. When a new server is added to the server group, the load balancer automatically starts to send requests to it.

4.2.6 Having Independent Servers

As already mentioned, TOE relies on centralized servers that are maintained by Signal Messenger. It offers greater security over decentralized systems because all of the processing is controlled in a central location. In addition, if one terminal breaks down, the user can simply go to another terminal and log in again, and all of their files will still be accessible. Depending on the system, they may even be able to resume their session from the point they were at before, as if nothing had happened.

This type of arrangement does have some disadvantages. The central computer performs the computing functions and controls the remote terminals. This type of system relies totally on the central computer. Should the central computer crash, the entire system will go down.

References

[1] What is a safety number and why do I see that it changed? https://support.signal.org/hc/en-us/articles/360007060632-What-is-a-safety-number-and-why-do-I-see-that-it-changed-. [Online; accessed 22-December-2022].

[2] I. Fette. The WebSocket Protocol. https://www.rfc-editor.org/rfc/rfc6455.html. [Online; accessed 22-December-2022].

[3] Trevor Perrin. The Double Ratchet Algorithm. https://signal.org/docs/specifications/doubleratchet/, 2016. [Online; accessed 22-December-2022].

[4] signal. aesgcm. https://github.com/signalapp/AES-GCM-Provider. [Online; accessed 22-December-2022].

[5] signal. backup. https://support.signal.org/hc/en-us/articles/360007059752-Backup-and-Restore-Messages#:~:text=What%20if%20I%20forget,create%20a%20new%20passphrase. [Online; accessed 22-December-2022].

[6] signal. GDPR. https://support.signal.org/hc/en-us/articles/360007059412-Signal-and-the-General-Data-Protection-Regulation-GDPR-. [Online; accessed 22-December-2022].

[7] signal. rlimit. https://github.com/signalapp/Signal-Server/blob/main/service/src/main/java/org/whispersystems/textsecuregcm/limits/RateLimiter.java. [Online; accessed 22-December-2022].

[8] synopsis. sql. https://www.synopsys.com/glossary/what-is-sql-injection.html. [Online; accessed 22-December-2022].

[9] Robert Townsend. Access Control Models. https://westoahu.hawaii.edu/cyber/best-practices/best-practices-weekly-summaries/access-control/#:~:text=Three%20main%20types%20of%20access,Mandatory%20Access%20Control%20(MAC). [Online; accessed 22-December-2022].