# 0. The purpose of product.

Six sense (It's name of team 6) Special Forces applied A-SQUARE to acquire the COTS messenger applications to assign secret missions to agents.

# 1. Agree on Definitions

|  |  |
| --- | --- |
| message | The mission information transfer from commander to agent |
| COTS | Commercial, off-the-shelf products are packaged or canned software which are then adapted to satisfy the needs of the purchasing organization, rather than the commissioning of custom-made, or bespoke, solutions. |
| leak | Recognition of the message by other than the agent |
| encryption | The technology to protect a message |
| disappearing message | It is that will disappear or automatically get deleted from a chat after sometime. |
| screenshot | Captured image the screen of user |

Example of use case

1. Commander sends a command to an agent
2. The agent checks the message that is encrypted on the network with the device.
3. The message should be automatically deleted right after checking by the agent.

# 2. Identify Security Goal

Any transferred messages for the mission must never be leaked.

# 3. Identify preliminary security requirements

1. COTS application NEVER collect any data from users
2. The transferred message MUST be protected securely
3. Messages MUST be deleted as soon as reading messages or message view is closed from receiver

# 4. Review COTS specifications

Table 1. Comparison of COTS specifications

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
|  | | **WhatsApp** | **Telegram** | **Signal** | **Snapchat** |
| **Collecting data from user** | | Device ID, User ID, Purchase History, Coarse Location, Phone Number, Email Address, Contracts, Payment Info, etc. | Contact Info,  Contacts,  User ID | None | Name, Birthdate, Username, Email address, Phone number |
| **End to end encryption for secure message** | | Default on | Support.  But default off | Default on | Default on |
| **disappearing message** | **Support** | Optional | Optional | Optional | Optional |
| **Time duration** | 7 days | 1 sec to 1 week | 5 second to 1 week | Automatically deletes messages when the sender and receiver has opened and left the chat |
| **When timer start** | Starts simultaneously for sender and receiver after sending message | For sender, the timer starts as soon as the message is sent, while for receiver the time starts when he/she views a message | The timer starts as soon as the message is sent for the sender. For receiver, the time starts when he/she views a message | NA |
| **Screenshot** | Receiver can take screenshots without the sender getting to know | Sender is notified if a receiver takes screenshot of disappearing message. However, this can be bypassed | Impossible | Automatically notifies the user |

Reference: <https://www.gadgetsnow.com/slideshows/disappearing-messages-comes-to-whatsapp-how-it-compares-with-similar-features-of-telegram-signal-and-snapchat/photolist/79081611.cms?picid=79081627>

# 5. Finalize security requirements

Table 2. Whether each app meets requirement or not

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Requirement**  **Number** | **WhatsApp** | **Telegram** | **Signal** | **Snapchat** |
| 1 | does not satisfy | does not satisfy | meets | does not satisfy |
| 2 | meets | meets | meets | meets |
| 3 | does not satisfy | does not satisfy | does not satisfy | does not satisfy |

Recall the 3rd preliminary security requirement. ‘Messages MUST be deleted as soon as reading messages or message view is closed from receiver’. But no one meets this requirement. So we changed the final security requirement to ’Message MUST be deleted within 10sec after reading message from receiver’. So we adjust secure requirement #3.

1. COTS NEVER collect any data from user
2. Message MUST be protected securely end to end
3. **Message MUST be deleted within 10 sec after reading message from receiver**

# 6. Perform tradeoff analysis

Table 3. Whether each app meets requirement or not again with finalized security requirements

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Requirement**  **Number** | **WhatsApp** | **Telegram** | **Signal** | **Snapchat** |
| 1 | does not satisfy | does not satisfy | meets | does not satisfy |
| 2 | meets | meets | meets | meets |
| 3 | does not satisfy | meets | meets | does not satisfy |

As we can see at the Table 3, the Signal COTS satisfies all of finalized security requirement. So we select the Signal messenger app.

Table 4. Perform tradeoff of Signal messenger

|  |  |  |  |
| --- | --- | --- | --- |
| **Requirement**  **Number** | **Final Security Requirements** | **How important** | **Assess how well each product meets** |
| 1 | COTS NEVER collect any data from user | Medium | Meets |
| 2 | Message MUST be protected securely end to end | High | Exceeds |
| 3 | Message MUST be deleted within 10 sec after reading message from receiver | High | Meets |

# 7. Write final product specification

Table 5. Final product specification

|  |  |  |  |
| --- | --- | --- | --- |
|  | | **Our product including Signal** | **Comment** |
| **Collecting data from user** | | None |  |
| **End to end encryption for secure message** | | Always on | On the Signal app, it’s default on. But our product prevent the configuration of the option in Signal |
| **disappearing message** | **Support** | Always on | On the Signal app, it’s optional. Our product prevent the configuration of the option in Signal |
| **Time duration** | 10 seconds | On the Signal app, it’s 5 second to 1 week. Our product fixed it to 10 seconds. |
| **When timer start** | The timer starts as soon as the message is sent for the sender. For receiver, the time starts when he/she views a message |  |
| **Screenshot** | Impossible |  |

The human error can be happened if some options are changed like ‘Time duration’ setting of COTS. To prevent it, we do enforce that the option cannot be changed.