PRAUDYOGIKEE

Anonybox

A DEEP JOURNEY INTO ANONYBOX'S TECHNOLOGY

MORAD ABDELRASHEED MOKHTAR ALI GILL

JUNE 28, 2020

COMPREHENSIVE TECHNOLOGY MADE BY A 15-YEARS-OLD TEENAGER TO ESTABLISH ANONYBOX.

1ST JSNCP.

JSNCP, AKA "Java Secure Network Communication Protocol", is a protocol, whereby data could be transferred between two endpoints. The features of this Protocol are as following:

- A workaround for writeUTF(): You can send Data Bigger than 64KB using Buffer Technology. DATA_BUFFER_CONST is responsible for the Data Size per packet. Actual Packet Size is DATA_BUFFER_CONST + 6 bytes "A link whereby the read() function knows that the next packet is appended to the existing one".
- Uses AES-256: It uses AES-256 with CBC mode and PKCS5 Padding with IV customization.
- IV Customization Can be used to exchange IVs between client and server "TBD".

This JSNCP is a crucial component for Anonybox since it's used to receive and/or send packets.
Note for non-java-programmers: writeUTF() is the implemented function to pass the data through connection, and read() function is to read the data from the stream.

IV EXCHANGING? , WHAT IS IT?

Anonybox uses IV Exchanging to Increase Security Level, The process goes as follow:
1- Client Requests a random IV from the server,
2- Server generates the random IV and sets the Default IV to the generated IV,
3- Server sends the IV to the Client under AES-256 Encryption,
4- Client receives the IV and sets the Default IV to the generated IV, and
5- Client sends a TEST Message to the Server: If the two IVs are identical, Server will reply with a confirmation message

WHAT ABOUT THE ENCRYPTION KEY?

Anonybox doesn't use Diffie-Hellman Key Exchanging Algorithm *at the moment*, even though it's required by the client to know the Encryption Key. The process goes as follows:
1- Client Connects to the server,
2- Client Sends a TEST message with All-Zeroed IV "till the client receives the new IV" to the server, and
3- If the two Encryption Keys are identical, Server will reply with s confirmation message

* = TBD

ENCRYPTION KEY ISN'T THE SAME !

Yes, the Input Encryption Key isn't the accurate one. Instead, it takes first 16 bytes of the Encoded-SHA1-Key and then adjust it to work!

1ST ANONYBOX API.

I, personally, prefer to call it ”Anonybox Utilities” as it considers as a bunch of tools rather than a complete API.
JSNCP is included in the API, along with other utilities ”functions”, to grease the wheels and simplify the code.
It includes:
1- JSNCP,
2- Read Files ”A shortcut for like 4 lines lol”,
3- Generate Random Strings of length 20 chars, and
4- Generate Random IV of a size of 16 bytes 5- Decrypt/Encrypt Data.

ABOUT THE API'S CONSTANTS.

Till June 28, 2020, Two Constants Exist:
1- EMPTY_IV that contains All-Zeroed IV,
2- DATA_BUFFER_CONST that is the amount of data ”in bytes” included in one packet ”Return to Page 2 to the features of JSNCP”. It’s a required value by the JSNCP.

FUTURE PLANS.

1- Convert Read Files Function into Secured Read Files Function **
2- Make a secure Write on Files Function **
3- Add Diffie-Hellman Key Exchanging Algorithm 4- Improve GUI

** = Using AES-256 CBC PKCS5 Encryption with All-Zeroed IV and Encryption File "will be generated out of another Encryption key the user will enter on first time only and the user must save it for later for further usage except he deleted all files and he started to fresh again"

SECURITY?

A filter is added to filter all special characters out that could be used in many vulnerabilities such as:
1- RCE
2- Buffer Overflow

HASHMAPSTORE.

It's a feature that takes users' and admins' DB files and translates them into A HashMap.
EDelimiter is the Element Delimiter, or we can call it one Key and Value
KVDelimiter is the Key-Value Delimiter, or we can say it's the delimiter in every element that splits the Key and Value, so HashMapStore can identify them separately.

WRITEDATA FUNCTION.

It inserts data in DB files. If there are existing queries, a delimiter will be prefixed to the input text; otherwise, the text will remain the same.

WRITEFILE FUNCTION.

Write on file... That's it!
Why I did that? I'm kind of lazy, and if I wrote around 5 lines each time, the code would be huge.

READFILE FUNCTION.

Read a file... That's it!
Why I did that? I'm freaking lazy, and I also have to replace the zero-content with 'NOTHING'.
Why? Well, When a Mailbox is empty, the ReadFile() would return null that won't send the message and/or not displayed properly.

3RD ANONYBOX

Apparently, Anonybox depends on many components, such as JSNCP and Anonybox API and HashMapStore. Furthermore, a firewall will be implemented. The firewall rules are as follow:
1- Block >64KB Packets
2- Filter all special characters from any input and/or data that it sent through port 1111 Official port for Anonybox" except [.] and [@] and [-] and [,] and [(] and [)] and [!] and [?] and the space character and \n and [:]
3- Limit processing speed to a specific speed like 150 p/s "packets per second"

COMMANDS

user [user] -> enter the username
pass [pass] -> Enter the Password
IVGENERATE -> Generate an IV
TEST -> Test connection " I/O "
For User
mail -> view mailbox
compose [content],[dest] -> Send [content] to [dest]
logout -> Logout
change password [oldpass],[newpass] -> Change the password from [oldpass] to [newpass]
change username [olduser],[newuser] -> Change the username from [olduser] to [newuser]

For Admin

create user [user],[pass] -> Create a user of credentials [user] and [pass] delete user [user], [pass] -> Delete a user of credentials [user] and [pass]

ANONYBOX IN NUMBERS

63 is the number of Anonybox API usages all over the application.
238 is the number of lines in Client side
15 is the number of lines in Firewall code
202 is the number of lines in Anonybox API
472 is the number of lines in Server side
174 is the number of lines in Starter page
1101 is the number of lines of code to make this project