eYSIP2016

Robot State Collector

Security Document

Amanpreet Singh
Amit Raushan
Shubham Gupta
Duration of Internship: 10/06/2016 – 24/07/2016

List of all the Security Features

- **Authentication:** Only the users with valid login credentials can send the data collected by the GUI to the servers.
- **Data Integrity:** To check if any modifications have been made to the text file containing the data in between the time of file generation and sending that file to the server, we first generate the checksum on the client side while creating the file. This checksum is the first thing to be sent to the server. Once the collected data is sent to the server another checksum is generated, this time at the server side. These two generated checksums can be matched to verify the Data Integrity.
- **Confidentiality:** The State data is encrypted using AES, which is a symmetric key encryption algorithm. The 128 bit key of this symmetric key encryption is generated randomly at the client side and is encrypted using 1024 bit public key of RSA, which is a asymmetric key encryption algorithm. The corresponding Private key is already available at the server side and hence we can recover the AES key. Now this AES key can be used to decrypt the data.

Steps followed to maintain all the Security Features

1. State Information is collected and then encrypted before storing it on the disk.
2. Login credentials are verified by the server.
3. Checksum of the encrypted file is sent to the server. This checksum was calculated as soon as the file was written to the disk.
4. Then the randomly generated encrypted AES symmetric key is sent using Public Key.
5. The data encrypted with shared key is sent to the server.
6. The checksum is generated for the received data at the server side. Only if this checksum matches with the checksum recieved in step 3, further process takes place.
7. Server decrypts the recieved encrypted shared key using its Private Key.
8. The State Data is obtained by decrypting the recieved data using this shared key.