Security Features implemented by UiPath products

1) Communication between robot and Orchestrator is encrypted using the HTTPS protocol (requires an SSL certificate employed by the Orchestrator website)

2) The robot can be connected to Orchestrator only if it is known by Orchestrator.

3) Robot authenticates with machine name and Robot Key

4) Orchestrator never contacts the robot directly. Orchestrator does not try to create a Remote Desktop Session on the robot computer.

5) Robot passwords and credentials that are requested by robots are stored encrypted in the SQL Server database. Encryption algorithm is AES_CBC_256.

6) Users that are defined locally in Orchestrator will login with their username and password. Orchestrator stores an irreversible salted hash of the user's password (because there is no need to decrypt the password). The browser sends the password to Orchestrator, which uses the password + salt to compute the hash which must match the hash that is stored in the DB).

7) Orchestrator supports Windows Integrated Authentication of users. In this case there is no encrypted password or password hash stored in the database.

8) When a robot asks Orchestrator for a password, which is stored encrypted in the SQL database, Orchestrator decrypts the password and sends it as SecureString (not plain string) to the robot. The robot needs to use specific .NET functions to convert the SecureString into a plain text string.

9) In case of an error in the website application, Orchestrator never reveals the real error message to the user (who is using the browser to interact with the application). It uses a customized error page, that states that more details are found in the web application server.

10) The response header of the web application (Orchestrator) does not contain the OS version, the IIS version, the .NET version and the MVC version (an attacker might take advantage of the vulnerabilities of any of such a component).

11) Communication between Orchestrator and SQL Server can be encrypted if necessary, we provide document on how to do this.

https://docs.google.com/document/d/1rqtxs4mecZceU5ZdKh5MEUiztmuJCXuDcacJUq5cj3A

12) Sensitive data should not be stored in the logs. However, access to logged messages stored in SQL Server database is controlled by permission (user's role(s)). For logged messages stored in Elasticsearch, the recommended solution is the X-Pack plugin from Elastic Co.

13) Sensitive data should not be stored in the queue. However, access to the details of a queue item, stored in SQL Server database, is controlled by permission (user's role(s)).

14) Access to the Settings dialog box on the robot machine, where Robot Key and Orchestrator URL can be edited, requires elevated rights.

15) Related to the above, the location of the Robot's settings file is %PROGRAMDATA%\UiPath (in most of the cases expanded into C:\ProgramData\ UiPath). The ProgramData folder is a special (protected) Windows folder. Changing a file in this location requires elevated rights.

16) If a user tries to login to Orchestrator with the correct username but with a bad password, Orchestrator blocks (locks) the account after 5 failed attempts. The account is automatically unlocked after a configurable number of seconds.

17) Starting with 2018.1, access to automation packages on the robot machines is forbidden to regular users. These are the NuGet packages that are downloaded by the robot service and stored locally.