Threat Modeling Report

Created on 11/7/2018 10:33:54 PM

Threat Model Name:

Owner:

Reviewer:

Contributors:

Description:

Assumptions:

External Dependencies:

Threat Model Summary:

Not Started	3
Not Applicable	0
Needs Investigation	1
Mitigation Implemented	61
Total	65
Total Migrated	0

Diagram:

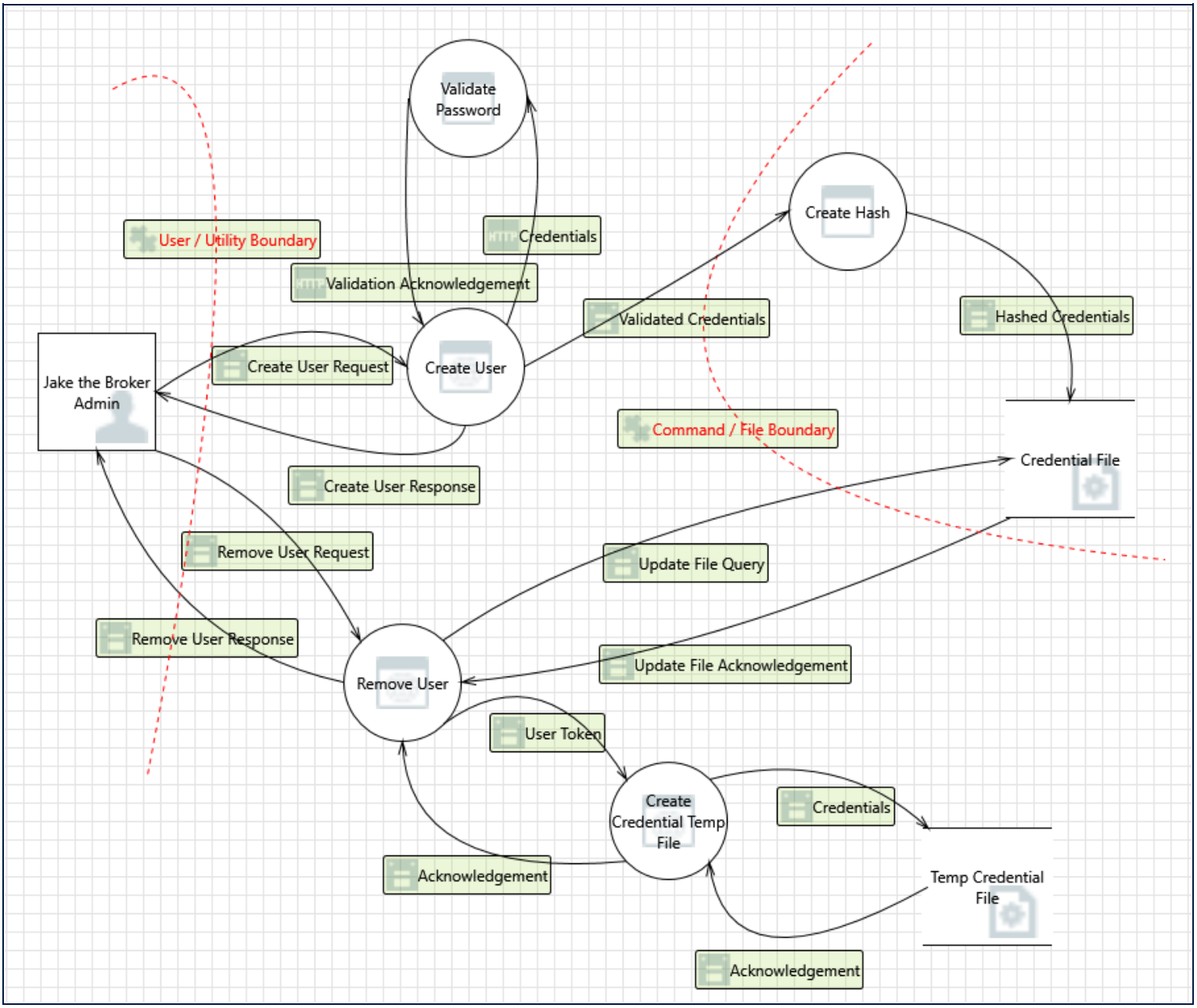
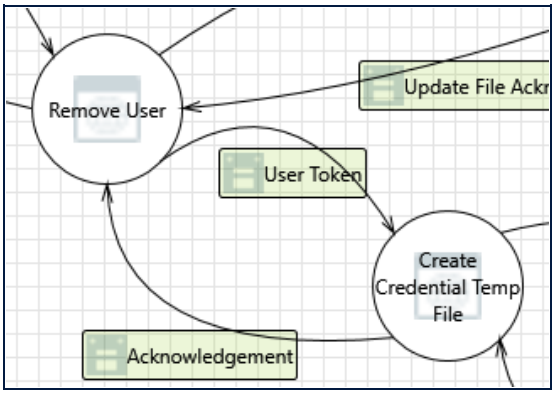


Diagram Summary:

Not Started	3
Not Applicable	0
Needs Investigation	1
Mitigation Implemented	61
Total	65
Total Migrated	0

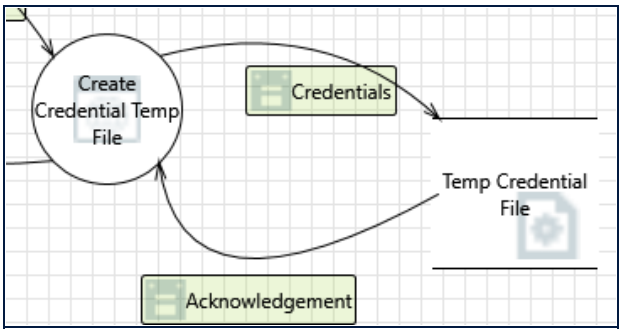
Interaction: Acknowledgement



1. Elevation Using Impersonation [State: Mitigation Implemented] [Priority: High]

Category: Elevation Of Privilege
Description: Remove User may be able to impersonate the context of Create Credential Temp File in order to gain additional privilege.
Justification: Processes use input validation by mosquitto.config on all incoming data and access is verified through ACL

Interaction: Acknowledgement



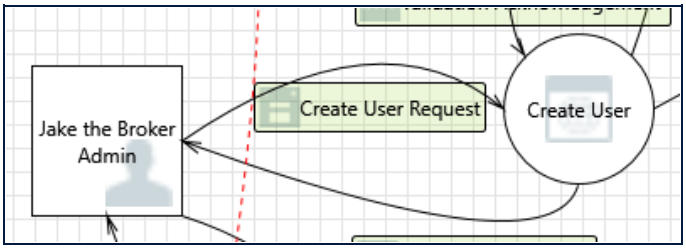
2. Spoofing of Source Data Store Temp Credential File [State: Mitigation Implemented] [Priority: High]

Category: Spoofing
Description: Temp Credential File may be spoofed by an attacker and this may lead to incorrect data delivered to Create Credential Temp File. Consider using a standard authentication mechanism to identify the source data store.
Justification: The system uses authentication mechanisms such input and data source validation to mitigate against spoofing attacks.

3. Weak Access Control for a Resource [State: Mitigation Implemented] [Priority: High]

Category: Information Disclosure
Description: Improper data protection of Temp Credential File can allow an attacker to read information not intended for disclosure. Review authorization settings.
Justification: In order to access data, a process is first authenticated and the ACL validates process before allowing access to Temp Credential File.

Interaction: Create User Request



4. Spoofing the Jake the Broker Admin External Entity [State: Mitigation Implemented] [Priority: High]

Category: Spoofing
Description: Jake the Broker Admin may be spoofed by an attacker and this may lead to unauthorized access to Create User. Consider using a standard authentication mechanism to identify the external entity.
Justification: The system uses authentication mechanisms such as dual factor authenticaion and ACL to mitigate against spoofing attacks. All processes validate users with an ACL

5. Elevation Using Impersonation [State: Mitigation Implemented] [Priority: High]

Category: Elevation Of Privilege
Description: Create User may be able to impersonate the context of Jake the Broker Admin in order to gain additional privilege.
Justification: The access type is controlled using "read", "write" or "readwrite" in ACL, mosquitto.config. Processes use input validation on all incoming data by mosquitto.config.

6. Elevation by Changing the Execution Flow in Create User [State: Mitigation Implemented] [Priority: High]

Category: Elevation Of Privilege
Description: An attacker may pass data into Create User in order to change the flow of program execution within Create User to the attacker's choosing.
Justification: Processes use input validation by mosquitto.config on all incomming data. The access type is controlled using "read", "write" or "readwrite".

7. Create User May be Subject to Elevation of Privilege Using Remote Code Execution [State: Mitigation Implemented] [Priority: High]

Category: Elevation Of Privilege
Description: Jake the Broker Admin may be able to remotely execute code for Create User.
Justification: Processes use input validation by mosquitto.config on all incomming data. The access type is controlled using "read", "write" or "readwrite".

8. Data Flow Create User Request Is Potentially Interrupted [State: Mitigation Implemented] [Priority: High]

Category: Denial Of Service
Description: An external agent interrupts data flowing across a trust boundary in either direction.
Justification: A lack response from the entity not receiving data would result in the process reporting an error and returning an error message.

9. Potential Process Crash or Stop for Create User [State: Mitigation Implemented] [Priority: High]

Category: Denial Of Service
Description: Create User crashes, halts, stops or runs slowly; in all cases violating an availability metric.
Justification: Use disk and processor quotas to prevent excess disk or CPU consumption

10. Data Flow Sniffing [State: Mitigation Implemented] [Priority: High]

Category: Information Disclosure

Description: Data flowing across Create User Request may be sniffed by an attacker. Depending on what type of data an attacker can read, it may be used to attack other parts of the system or simply be a disclosure of information leading to compliance violations. Consider encrypting the data flow.

Justification: In order to access this process a user must be logged in the internal system. All users accessing this process are authenticated and cross referenced within the ACL. This process is not exposed.

11. Potential Data Repudiation by Create User [State: Mitigation Implemented] [Priority: High]

Category: Repudiation

Description: Create User claims that it did not receive data from a source outside the trust boundary. Consider using logging or auditing to record the source, time, and summary of the received data.

Justification: Processes use logging and audit generation mechanism which logs sent and received data.

12. Potential Lack of Input Validation for Create User [State: Mitigation Implemented] [Priority: High]

Category: Tampering

Description: Data flowing across Create User Request may be tampered with by an attacker. This may lead to a denial of service attack against Create User or an elevation of privilege attack against Create User or an information disclosure by Create User. Failure to verify that input is as expected is a root cause of a very large number of exploitable issues. Consider all paths and the way they handle data. Verify that all input is verified for correctness using an approved list input validation approach.

Justification: All processes check the ACL before accepting data. Furthermore, mechanism such as input validation and integrity of data source are in place as well.

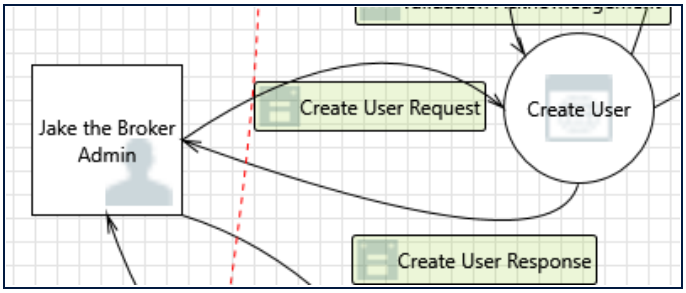
13. Spoofing the Create User Process [State: Mitigation Implemented] [Priority: High]

Category: Spoofing

Description: Create User may be spoofed by an attacker and this may lead to information disclosure by Jake the Broker Admin. Consider using a standard authentication mechanism to identify the destination process.

Justification: The system uses authentication mechanisms such as dual factor authenticaion and ACL to mitigate against spoofing attacks. All processes validate users with an ACL

Interaction: Create User Response



14. Data Flow Create User Response Is Potentially Interrupted [State: Mitigation Implemented] [Priority: High]

Category: Denial Of Service

Description: An external agent interrupts data flowing across a trust boundary in either direction.

Justification: A lack response from the entity not receiving data would result in the process reporting an error and returning an error message.

15. External Entity Jake the Broker Admin Potentially Denies Receiving Data [State: Mitigation Implemented] [Priority: High]

Category: Repudiation

Description: Jake the Broker Admin claims that it did not receive data from a process on the other side of the trust boundary. Consider using logging or auditing to record the source, time, and summary of the received data.

Justification: The system uses logging and audit generation mechanism which logs sent and received data.

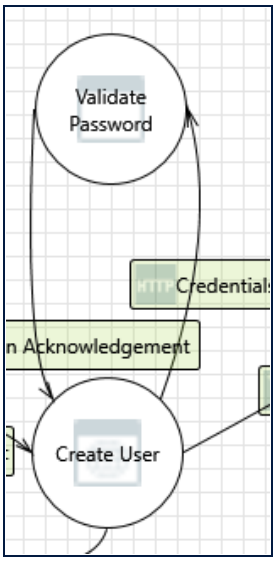
16. Spoofing of the Jake the Broker Admin External Destination Entity [State: Mitigation Implemented] [Priority: High]

Category: Spoofing

Description: Jake the Broker Admin may be spoofed by an attacker and this may lead to data being sent to the attacker's target instead of Jake the Broker Admin. Consider using a standard authentication mechanism to identify the external entity.

Justification: The system uses authentication mechanisms such as dual factor authenticaion and ACL to mitigate against spoofing attacks.

Interaction: Credentials



17. Create User Process Memory Tampered [State: Mitigation Implemented] [Priority: High]

Category: Tampering

Description: If Create User is given access to memory, such as shared memory or pointers, or is given the ability to control what Validate Password executes (for example, passing back a function pointer.), then Create User can tamper with Validate Password. Consider if the function could work with less access to memory, such as passing data rather than pointers. Copy in data provided, and then validate it.

Justification: All processes check the ACL before accepting data. Furthermore, mechanism such as input validation and integrity of data source are in place as well.

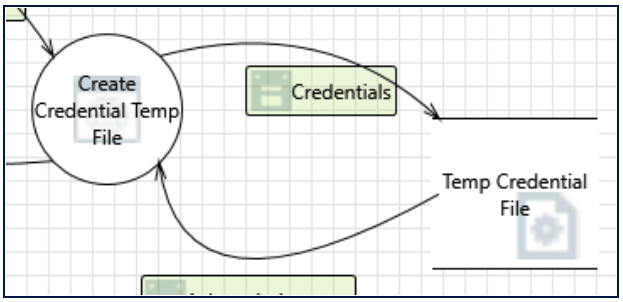
18. Elevation Using Impersonation [State: Mitigation Implemented] [Priority: High]

Category: Elevation Of Privilege

Description: Validate Password may be able to impersonate the context of Create User in order to gain additional privilege.

Justification: Processes use input validation on all incoming data by mosquitto.config.

Interaction: Credentials



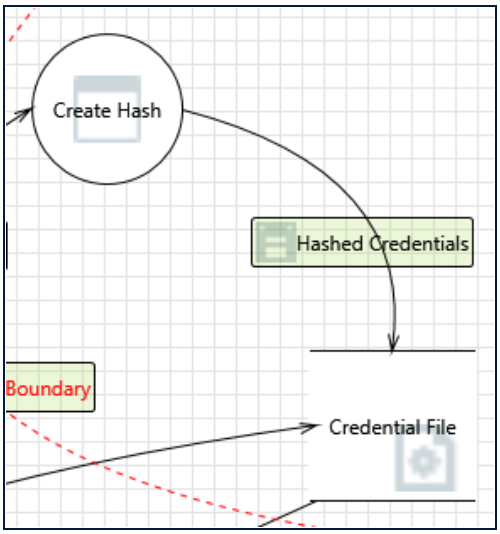
19. Spoofing of Destination Data Store Temp Credential File [State: Mitigation Implemented] [Priority: High]

Category: Spoofing
Description: Temp Credential File may be spoofed by an attacker and this may lead to data being written to the attacker's target instead of Temp Credential File. Consider using a standard authentication mechanism to identify the destination data store.
Justification: The system uses authentication mechanisms such input validation to mitigate against spoofing attacks.

20. Potential Excessive Resource Consumption for Create Temp File or Temp Credential File [State: Mitigation Implemented] [Priority: High]

Category: Denial Of Service
Description: Does Create Credential Temp File or Temp Credential File take explicit steps to control resource consumption? Resource consumption attacks can be hard to deal with, and there are times that it makes sense to let the OS do the job. Be careful that your resource requests don't deadlock, and that they do timeout.
Justification: Separation of users having access to resources. Use disk and processor quotas to prevent excess disk or CPU consumption.

Interaction: Hashed Credentials



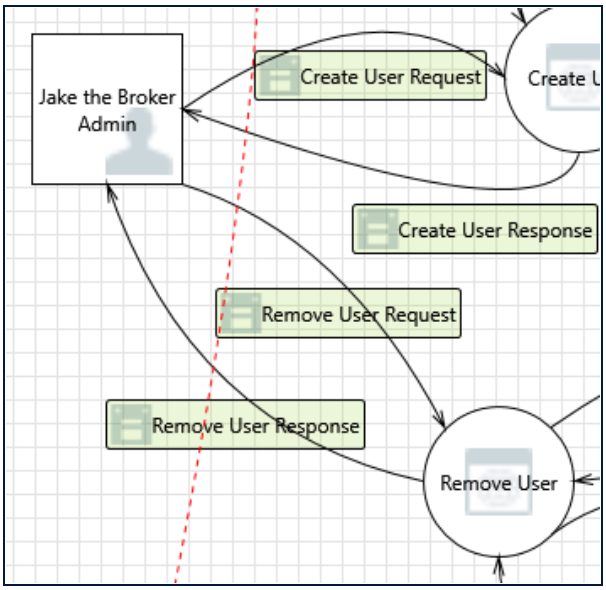
21. Potential Excessive Resource Consumption for Create Hash or Credential File [State: Mitigation Implemented] [Priority: High]

Category: Denial Of Service
Description: Does Create Hash or Credential File take explicit steps to control resource consumption? Resource consumption attacks can be hard to deal with, and there are times that it makes sense to let the OS do the job. Be careful that your resource requests don't deadlock, and that they do timeout.
Justification: Separation of users having access to resources. Use disk and processor quotas to prevent excess disk or CPU consumption.

22. Spoofing of Destination Data Store Credential File [State: Mitigation Implemented] [Priority: High]

Category: Spoofing
Description: Credential File may be spoofed by an attacker and this may lead to data being written to the attacker's target instead of Credential File. Consider using a standard authentication mechanism to identify the destination data store.
Justification: The system uses authentication mechanisms such input validation to mitigate against spoofing attacks.

Interaction: Remove User Request



23. Spoofing the Jake the Broker Admin External Entity [State: Mitigation Implemented] [Priority: High]

Category: Spoofing
Description: Jake the Broker Admin may be spoofed by an attacker and this may lead to unauthorized access to Remove User. Consider using a standard authentication mechanism to identify the external entity.
Justification: The system uses authentication mechanisms such as dual factor authenticaion and ACL to mitigate against spoofing attacks. All processes validate users with an ACL

24. Elevation Using Impersonation [State: Not Started] [Priority: High]

Category: Elevation Of Privilege
Description: Remove User may be able to impersonate the context of Jake the Broker Admin in order to gain additional privilege.
Justification: The access type is controlled using "read", "write" or "readwrite". Processes use input validation on all incoming data by mosquitto.config.

25. Elevation by Changing the Execution Flow in Remove User [State: Mitigation Implemented] [Priority: High]

Category: Elevation Of Privilege
Description: An attacker may pass data into Remove User in order to change the flow of program execution within Remove User to the attacker's choosing.
Justification: Processes use input validation by mosquitto.config on all incomming data. The access type is controlled using "read", "write" or "readwrite".

26. Remove User May be Subject to Elevation of Privilege Using Remote Code Execution [State: Mitigation Implemented] [Priority: High]

Category: Elevation Of Privilege

Description: Jake the Broker Admin may be able to remotely execute code for Remove User.

Justification: The access type is controlled using "read", "write" or "readwrite".

27. Data Flow Remove User Request Is Potentially Interrupted [State: Mitigation Implemented] [Priority: High]

Category: Denial Of Service

Description: An external agent interrupts data flowing across a trust boundary in either direction.

Justification: A lack response from the entity not receiving data would result in the process reporting an error and returning an error message.

28. Potential Process Crash or Stop for Remove User [State: Mitigation Implemented] [Priority: High]

Category: Denial Of Service

Description: Remove User crashes, halts, stops or runs slowly; in all cases violating an availability metric.

Justification: Use disk and processor quotas to prevent excess disk or CPU consumption

29. Data Flow Sniffing [State: Mitigation Implemented] [Priority: High]

Category: Information Disclosure

Description: Data flowing across Remove User Request may be sniffed by an attacker. Depending on what type of data an attacker can read, it may be used to attack other parts of the system or simply be a disclosure of information leading to compliance violations. Consider encrypting the data flow.

Justification: In order to access this process a user must be logged in the internal system. All users accessing this process are authenticated and cross referenced within the ACL. This process is not exposed.

30. Potential Data Repudiation by Remove User [State: Mitigation Implemented] [Priority: High]

Category: Repudiation

Description: Remove User claims that it did not receive data from a source outside the trust boundary. Consider using logging or auditing to record the source, time, and summary of the received data.

Justification: Processes use logging and audit generation mechanism which logs sent and received data.

31. Potential Lack of Input Validation for Remove User [State: Mitigation Implemented] [Priority: High]

Category: Tampering

Description: Data flowing across Remove User Request may be tampered with by an attacker. This may lead to a denial of service attack against Remove User or an elevation of privilege attack against Remove User or an information disclosure by Remove User. Failure to verify that input is as expected is a root cause of a very large number of exploitable issues. Consider all paths and the way they handle data. Verify that all input is verified for correctness using an approved list input validation approach.

Justification: All processes check the ACL before accepting data. Furthermore, mechanism such as input validation and integrity of data source are in place as well.

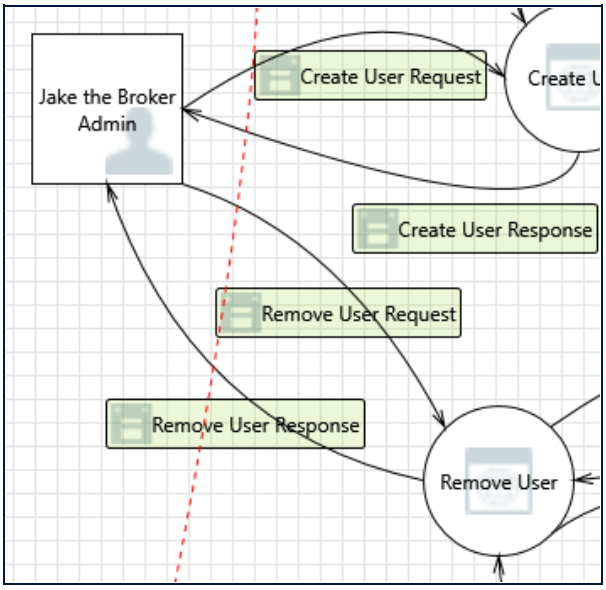
32. Spoofing the Remove User Process [State: Mitigation Implemented] [Priority: High]

Category: Spoofing

Description: Remove User may be spoofed by an attacker and this may lead to information disclosure by Jake the Broker Admin. Consider using a standard authentication mechanism to identify the destination process.

Justification: The system uses authentication mechanisms to mitigate against spoofing attacks

Interaction: Remove User Response



33. Spoofing of the Jake the Broker Admin External Destination Entity [State: Mitigation Implemented] [Priority: High]

Category:	Spoofing
Description:	Jake the Broker Admin may be spoofed by an attacker and this may lead to data being sent to the attacker's target instead of Jake the Broker Admin. Consider using a standard authentication mechanism to identify the external entity.
Justification:	The system uses authentication mechanisms such as dual factor authenticaion and ACL to mitigate against spoofing attacks.

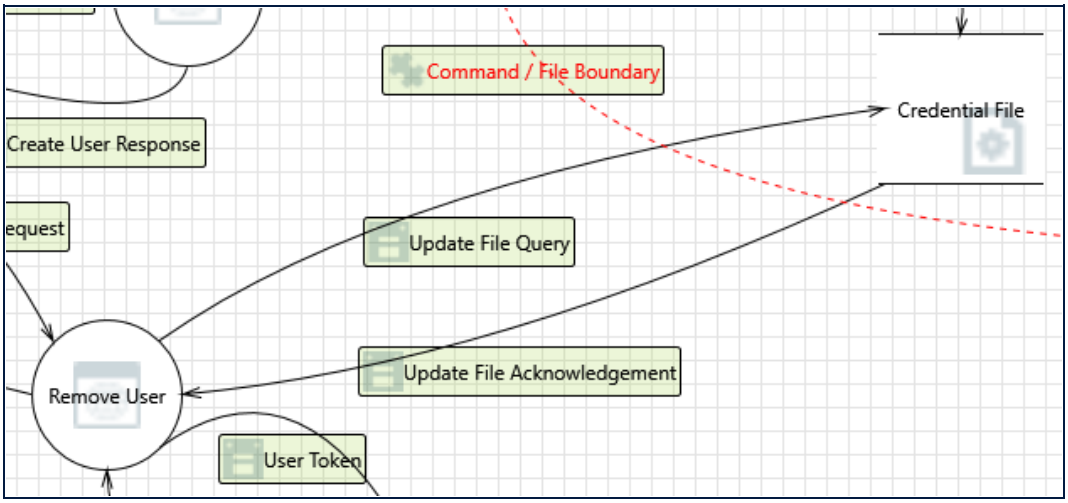
34. External Entity Jake the Broker Admin Potentially Denies Receiving Data [State: Mitigation Implemented] [Priority: High]

Category:	Repudiation
Description:	Jake the Broker Admin claims that it did not receive data from a process on the other side of the trust boundary. Consider using logging or auditing to record the source, time, and summary of the received data.
Justification:	The system uses logging and audit generation mechanism which logs sent and received data.

35. Data Flow Ack Is Potentially Interrupted [State: Mitigation Implemented] [Priority: High]

Category:	Denial Of Service
Description:	An external agent interrupts data flowing across a trust boundary in either direction.
Justification:	A lack response from the entity not receiving data would result in the Remove User process reporting an error and returning an error message.

Interaction: Update File Acknowledgement



36. Spoofing of Source Data Store Credential File [State: Mitigation Implemented] [Priority: High]

Category: Spoofing
Description: Credential File may be spoofed by an attacker and this may lead to incorrect data delivered to Remove User. Consider using a standard authentication mechanism to identify the source data store.
Justification: The system uses authentication mechanisms such input and data source validation to mitigate against spoofing attacks.

37. Weak Access Control for a Resource [State: Not Started] [Priority: High]

Category: Information Disclosure
Description: Improper data protection of Credential File can allow an attacker to read information not intended for disclosure. Review authorization settings.
Justification: In order to access data, a process is first authenticated and the ACL validates process before allowing access to Credential.

38. Spoofing the Remove User Process [State: Mitigation Implemented] [Priority: High]

Category: Spoofing
Description: Remove User may be spoofed by an attacker and this may lead to information disclosure by Credential File. Consider using a standard authentication mechanism to identify the destination process.
Justification: The system uses authentication mechanisms such input and data source validation to mitigate against spoofing attacks.

39. Potential Data Repudiation by Remove User [State: Mitigation Implemented] [Priority: High]

Category: Repudiation
Description: Remove User claims that it did not receive data from a source outside the trust boundary. Consider using logging or auditing to record the source, time, and summary of the received data.
Justification: Processes use logging and audit generation mechanism which logs sent and received data.

40. Potential Process Crash or Stop for Remove User [State: Mitigation Implemented] [Priority: High]

Category: Denial Of Service
Description: Remove User crashes, halts, stops or runs slowly; in all cases violating an availability metric.
Justification: Use disk and processor quotas to prevent excess disk or CPU consumption

41. Data Flow Ack Is Potentially Interrupted [State: Mitigation Implemented] [Priority: High]

Category: Denial Of Service
Description: An external agent interrupts data flowing across a trust boundary in either direction.
Justification: A lack response from the entity not receiving data would result in the process reporting an error and returning an error message.

42. Data Store Inaccessible [State: Mitigation Implemented] [Priority: High]

Category: Denial Of Service
Description: An external agent prevents access to a data store on the other side of the trust boundary.
Justification: A lack response from the entity not receiving data would result in the process reporting an error and returning an error message.

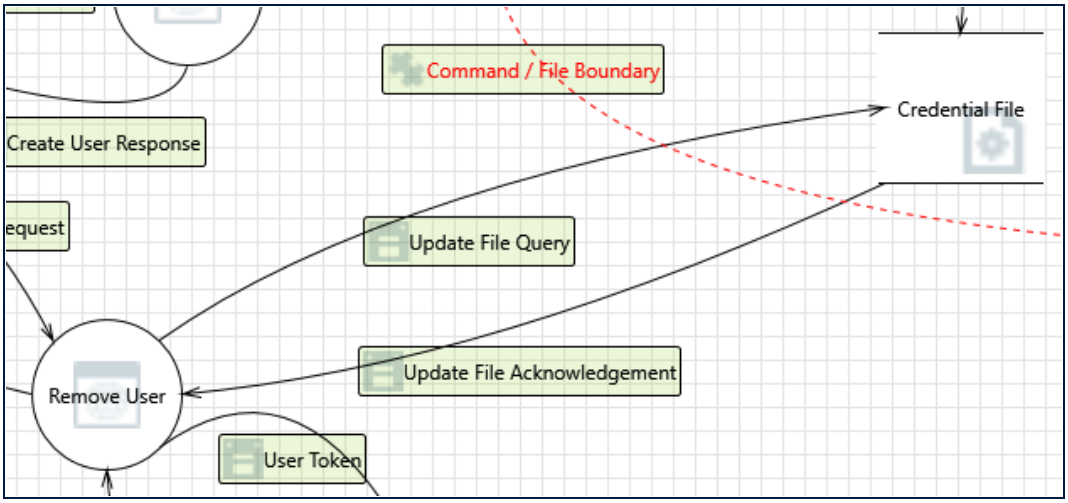
43. Remove User May be Subject to Elevation of Privilege Using Remote Code Execution [State: Mitigation Implemented] [Priority: High]

Category: Elevation Of Privilege
Description: Credential File may be able to remotely execute code for Remove User.
Justification: Processes use input validation on all incoming data by mosquitto.config and access is verified through ACL

44. Elevation by Changing the Execution Flow in Remove User [State: Mitigation Implemented] [Priority: High]

Category: Elevation Of Privilege
Description: An attacker may pass data into Remove User in order to change the flow of program execution within Remove User to the attacker's choosing.
Justification: Processes use input validation on all incoming data by mosquitto.config and access is verified through ACL.

Interaction: Update File Query



45. Spoofing of Destination Data Store Credential File [State: Mitigation Implemented] [Priority: High]

Category: Spoofing
Description: Credential File may be spoofed by an attacker and this may lead to data being written to the attacker's target instead of Credential File. Consider using a standard authentication mechanism to identify the destination data store.
Justification: The system uses authentication mechanisms such input validation to mitigate against spoofing attacks.

46. Potential Excessive Resource Consumption for Remove User or Credential File [State: Mitigation Implemented] [Priority: High]

Category: Denial Of Service

Description: Does Remove User or Credential File take explicit steps to control resource consumption? Resource consumption attacks can be hard to deal with, and there are times that it makes sense to let the OS do the job. Be careful that your resource requests don't deadlock, and that they do timeout.

Justification: Separation of users having access to resources. Use disk and processor quotas to prevent excess disk or CPU consumption.

47. Spoofing the Remove User Process [State: Mitigation Implemented] [Priority: High]

Category: Spoofing

Description: Remove User may be spoofed by an attacker and this may lead to unauthorized access to Credential File. Consider using a standard authentication mechanism to identify the source process.

Justification: The system uses authentication mechanisms such input validation and code integrity to mitigate against spoofing attacks.

48. The Credential File Data Store Could Be Corrupted [State: Mitigation Implemented] [Priority: High]

Category: Tampering

Description: Data flowing across Update File Query may be tampered with by an attacker. This may lead to corruption of Credential File. Ensure the integrity of the data flow to the data store.

Justification: Check the ACL before accepting data. Furthermore, mechanism such as input validation and integrity of data source are in place as well.

49. Data Store Denies Credential File Potentially Writing Data [State: Needs Investigation] [Priority: High]

Category: Repudiation

Description: Credential File claims that it did not write data received from an entity on the other side of the trust boundary. Consider using logging or auditing to record the source, time, and summary of the received data.

Justification: File systems do not support logging and audit generation mechanism.

50. Data Flow Sniffing [State: Mitigation Implemented] [Priority: High]

Category: Information Disclosure

Description: Data flowing across Update File Query may be sniffed by an attacker. Depending on what type of data an attacker can read, it may be used to attack other parts of the system or simply be a disclosure of information leading to compliance violations. Consider encrypting the data flow.

Justification: Credential File validates all input and cross reference the source with the ACL to validate access.

51. Data Flow Update File Query Is Potentially Interrupted [State: Mitigation Implemented] [Priority: High]

Category: Denial Of Service

Description: An external agent interrupts data flowing across a trust boundary in either direction.

Justification: A lack response from the entity not receiving data would result in the process reporting an error and returning an error message.

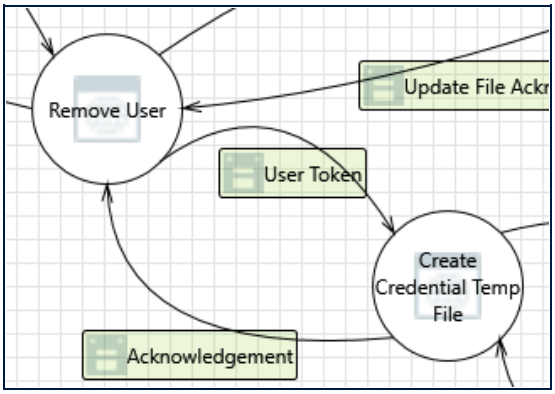
52. Data Store Inaccessible [State: Mitigation Implemented] [Priority: High]

Category: Denial Of Service

Description: An external agent prevents access to a data store on the other side of the trust boundary.

Justification: Requiring authentication using separate user accounts on either side of the trust boundary that are specific to the broker, can prevent external agents from potentially locking or preventing access to the given data store

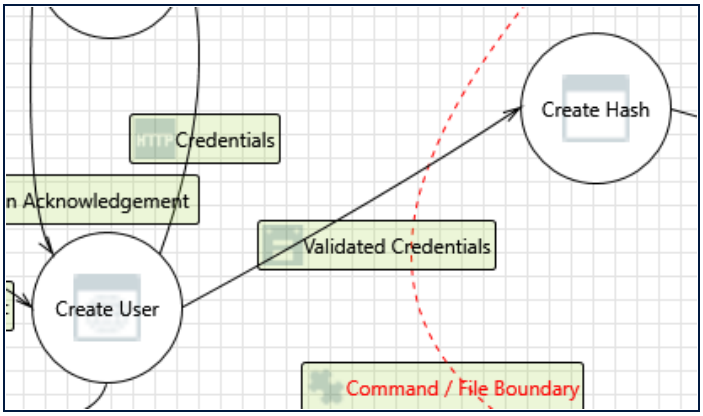
Interaction: User Token



53. Elevation Using Impersonation [State: Mitigation Implemented] [Priority: High]

Category: Elevation Of Privilege
Description: Create Credential Temp File may be able to impersonate the context of Remove User in order to gain additional privilege.
Justification: Processes use input validation on all incoming data by mosquitto.config and access is verified through ACL

Interaction: Validated Credentials



54. Create User Process Memory Tampered [State: Mitigation Implemented] [Priority: High]

Category: Tampering
Description: If Create User is given access to memory, such as shared memory or pointers, or is given the ability to control what Create Hash executes (for example, passing back a function pointer.), then Create User can tamper with Create Hash. Consider if the function could work with less access to memory, such as passing data rather than pointers. Copy in data provided, and then validate it.
Justification: All processes check the ACL before accepting data. Furthermore, mechanism such as input validation and integrity of data source are in place as well.

55. Elevation Using Impersonation [State: Mitigation Implemented] [Priority: High]

Category: Elevation Of Privilege
Description: Create Hash may be able to impersonate the context of Create User in order to gain additional privilege.
Justification: Processes use input validation on all incoming data by mosquitto.config and access is verified through ACL

56. Spoofing the Create User Process [State: Mitigation Implemented] [Priority: High]

Category: Spoofing
Description: Create User may be spoofed by an attacker and this may lead to unauthorized access to Create Hash.

Consider using a standard authentication mechanism to identify the source process.

Justification: The system uses authentication mechanisms such as dual factor authenticaion and ACL to mitigate against spoofing attacks. The trust boundry validates input to Create Hash process

57. Spoofing the Create Hash Process [State: Mitigation Implemented] [Priority: High]

Category: Spoofing

Description: Create Hash may be spoofed by an attacker and this may lead to information disclosure by Create User. Consider using a standard authentication mechanism to identify the destination process.

Justification: The system uses authentication mechanisms such as dual factor authenticaion and ACL to mitigate against spoofing attacks. The trust boundry validates input to Create Hash process

58. Potential Lack of Input Validation for Create Hash [State: Mitigation Implemented] [Priority: High]

Category: Tampering

Description: Data flowing across Validated Credentials may be tampered with by an attacker. This may lead to a denial of service attack against Create Hash or an elevation of privilege attack against Create Hash or an information disclosure by Create Hash. Failure to verify that input is as expected is a root cause of a very large number of exploitable issues. Consider all paths and the way they handle data. Verify that all input is verified for correctness using an approved list input validation approach.

Justification: All processes check the ACL before accepting data. Furthermore, mechanism such as input validation and integrity of data source are in place as well.

59. Potential Data Repudiation by Create Hash [State: Mitigation Implemented] [Priority: High]

Category: Repudiation

Description: Create Hash claims that it did not receive data from a source outside the trust boundary. Consider using logging or auditing to record the source, time, and summary of the received data.

Justification: Processes use logging and audit generation mechanism which logs sent and received data.

60. Data Flow Sniffing [State: Mitigation Implemented] [Priority: High]

Category: Information Disclosure

Description: Data flowing across Validated Credentials may be sniffed by an attacker. Depending on what type of data an attacker can read, it may be used to attack other parts of the system or simply be a disclosure of information leading to compliance violations. Consider encrypting the data flow.

Justification: In order to access this process a user must be logged in the internal system. All users accessing this process are authenticated and cross referenced within the ACL.

61. Potential Process Crash or Stop for Create Hash [State: Mitigation Implemented] [Priority: High]

Category: Denial Of Service

Description: Create Hash crashes, halts, stops or runs slowly; in all cases violating an availability metric.

Justification: Use disk and processor quotas to prevent excess disk or CPU consumption

62. Data Flow Validated Credentials Is Potentially Interrupted [State: Mitigation Implemented] [Priority: High]

Category: Denial Of Service

Description: An external agent interrupts data flowing across a trust boundary in either direction.

Justification: A lack response from the entity not receiving data would result in the process reporting an error and returning an error message.

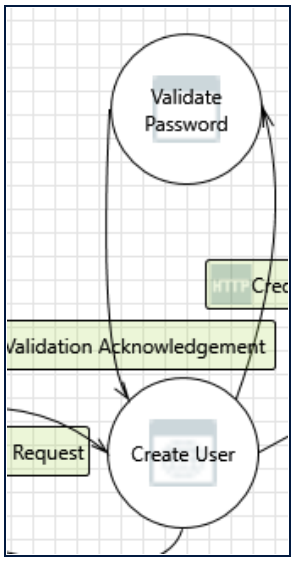
63. Create Hash May be Subject to Elevation of Privilege Using Remote Code Execution [State: Mitigation Implemented] [Priority: High]

Category: Elevation Of Privilege
Description: Create User may be able to remotely execute code for Create Hash.
Justification: Processes use input validation by mosquitto.config on all incoming data and access is verified through ACL

64. Elevation by Changing the Execution Flow in Create Hash [State: Mitigation Implemented] [Priority: High]

Category: Elevation Of Privilege
Description: An attacker may pass data into Create Hash in order to change the flow of program execution within Create Hash to the attacker's choosing.
Justification: Processes use input validation by mosquitto.config on all incomming data. The access type is controlled using "read", "write" or "readwrite".

Interaction: Validation Acknowledgement



65. Elevation Using Impersonation [State: Not Started] [Priority: High]

Category: Elevation Of Privilege
Description: Create User may be able to impersonate the context of Validate Password in order to gain additional privilege.
Justification: Processes use input validation on all incoming data by mosquitto.config.