Threat Modeling Report

Created on 11/13/2023 3:25:30 PM

Threat Model Name: Cardea Mobile Agent Threat Model

Owner: Ryan King, Perry Donahue

Reviewer:

Contributors:

Description: Cardea Mobile Agent is a phone app intended for end-users of Cardea. The app is like a digital wallet that holds legal and medical information of the user. The app's data store is the smartphone itself. All data saved by the app is stored on the phone itself; not external servers. The traveler is the end-user. They interact with Cardea Mobile Agent as an app on their phone. The internet boundary is interacting with the Enterprise Issuer Agent. This is a labority, healthcare provider, or state health agency who identifies a Cardea account with a medical release credential via a QR code, and then sends them the lab result.

Assumptions: There are two other external entities of Cardea Mobile Agent: a verifier and a government enterprise agent. The threat boundary created by the verifier is better represented in the verifier DFD diagram by Cole. It was left out of here to avoid a superflous diagram. The government enterprise agent is only used on the Aruba version of Cardea. Aruba is a pacafic island with a different legal jurisdiction that allows this external interactor. The Cardea team does not expect this entity to apply on a larger scale. In a level 2 DFD then this entity would be included. But it was decided that a level 1 DFD conveyed adequate information on threats for the system-of-interest.

External Dependencies: Cardea Mobile Agent is run on end-user smartphones. As such, the performance of the agent depends on the various software and hardware configurations of smartphones. For instance, a smartphone OS may prevent Cardea Mobile Agent from saving files, causing a DoS for the app.

Threat Model Summary:

Not Started	33
Not Applicable	6
Needs Investigation	0
Mitigation Implemented	6
Total	45
Total Migrated	0

Diagram: Diagram 1

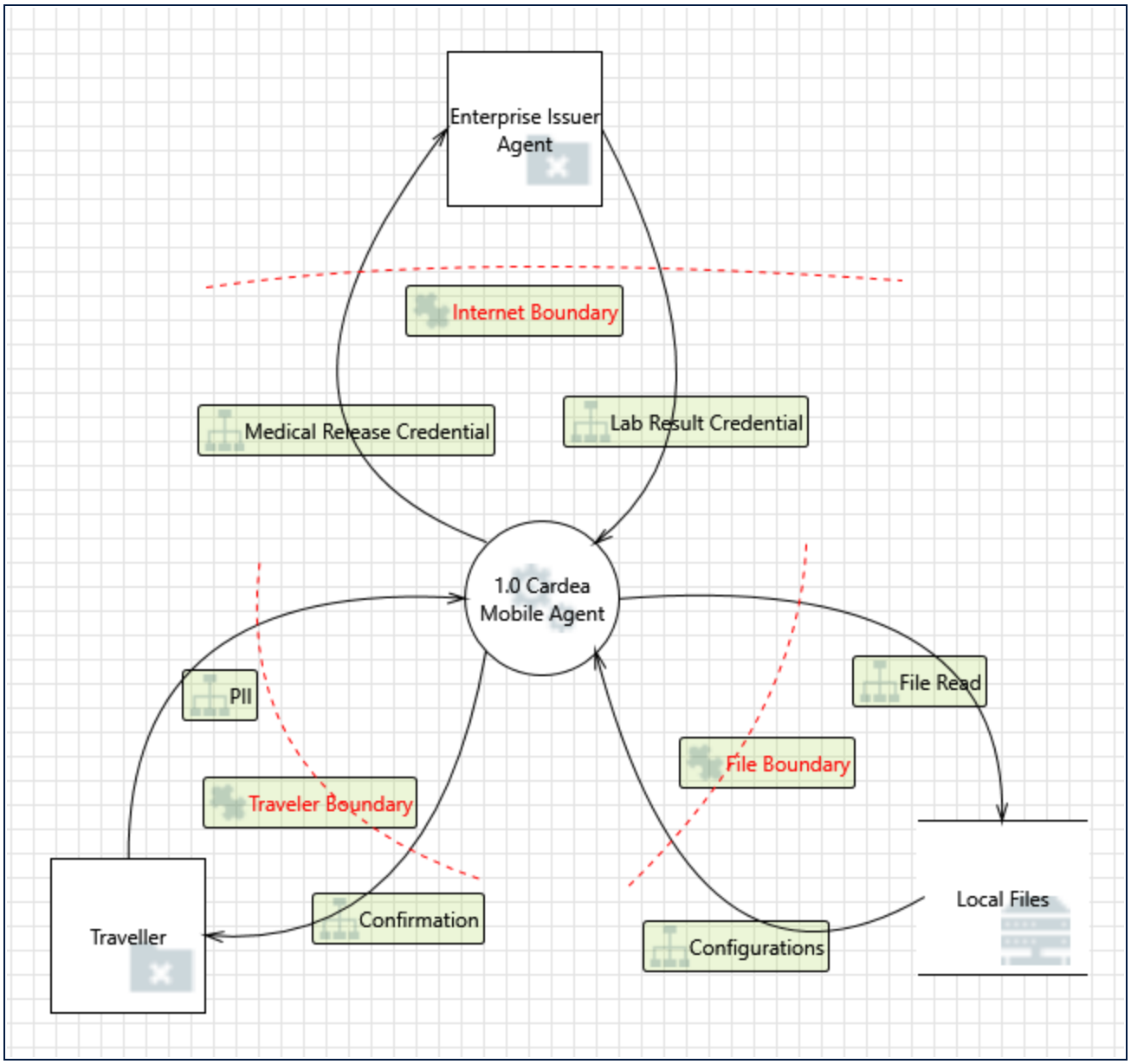
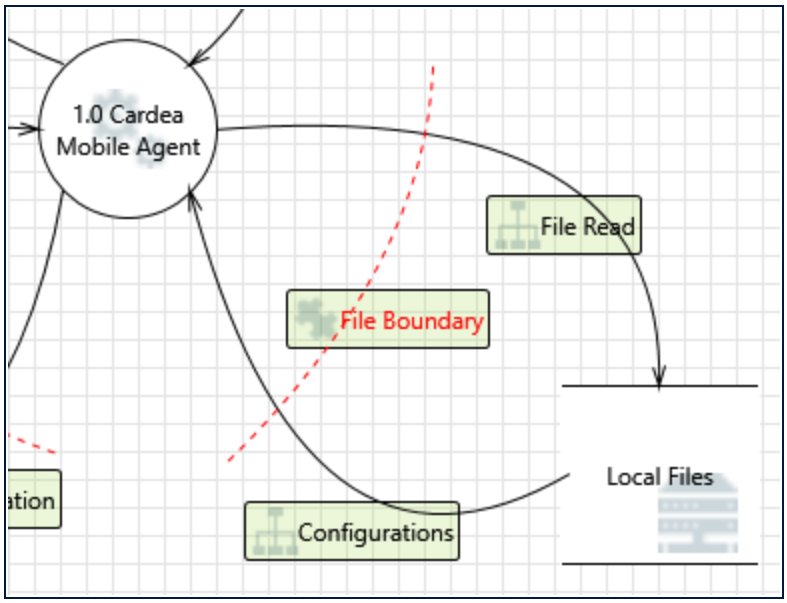


Diagram 1 Diagram Summary:

Not Started	33
Not Applicable	6
Needs Investigation	0
Mitigation Implemented	6
Total	45
Total Migrated	0

Interaction: Configurations



1. Spoofing of Source Data Store Local Files [State: Not Started] [Priority: High]

Category: Spoofing

Description: Local Files may be spoofed by an attacker and this may lead to incorrect data delivered to 1.0 Cardea Mobile Agent. Consider using a standard authentication mechanism to identify the source data store.

Justification: Cardea can push an update to encrypt its local files.

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

Category: Information Disclosure

Description: Improper data protection of Local Files can allow an attacker to read information not intended for disclosure. Review authorization settings.

Justification: Cardea can push an update to encrypt local files.

3. Elevation by Changing the Execution Flow in 1.0 Cardea Mobile Agent [State: Not Started] [Priority: Low]

Category: Elevation Of Privilege

Description: An attacker may pass data into 1.0 Cardea Mobile Agent in order to change the flow of program execution within 1.0 Cardea Mobile Agent to the attacker's choosing. Cardea Mobile Agent can't read local files if they were changed by malware.

Justification: Cardea has no control over third-party software on the smartphone.

4. 1.0 Cardea Mobile Agent May be Subject to Elevation of Privilege Using Remote Code Execution [State: Not Started] [Priority: Medium]

Category: Elevation Of Privilege

Description: Local Files may be able to remotely execute code for 1.0 Cardea Mobile Agent.

Justification: A smartphone must be rooted/jailbroken for Cardea files to be modified.

5. Data Store Inaccessible [State: Not Started] [Priority: Low]

Category: Denial Of Service

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

Justification: Cardea Mobile Agent has no control over third-party software on the phone or OS privileges.

6. Data Flow Configurations Is Potentially Interrupted [State: Not Started] [Priority: Low]

Category: Denial Of Service

Description: An external agent interrupts data flowing across a trust boundary in either direction. Malware or OS privileges may prevent Cardea from saving files.

Justification: Cardea Mobile Agent has no control over third-party software on the phone or OS privileges.

7. Potential Process Crash or Stop for 1.0 Cardea Mobile Agent [State: Not Started] [Priority: Low]

Category: Denial Of Service

Description: 1.0 Cardea Mobile Agent crashes, halts, stops or runs slowly; in all cases violating an availability metric.

Justification: This has no mitigation. Log files would be stored in the same data source as the one that log files are monitoring. At best, local file changes would leave behind artifacts detectable by a logical copy of the phone's hard drive and RAM.

8. Potential Data Repudiation by 1.0 Cardea Mobile Agent [State: Not Started] [Priority: Medium]

Category: Repudiation

Description: 1.0 Cardea Mobile Agent claims that it did not receive data from a source outside the trust boundary. Logging is not a good option since the log files would be stored in the same data source.

Justification: This has no mitigation. Log files would be stored in the same data source as the one that log files are monitoring. At best, local file changes would leave behind artifacts detectable by a logical copy of the phone's hard drive and RAM.

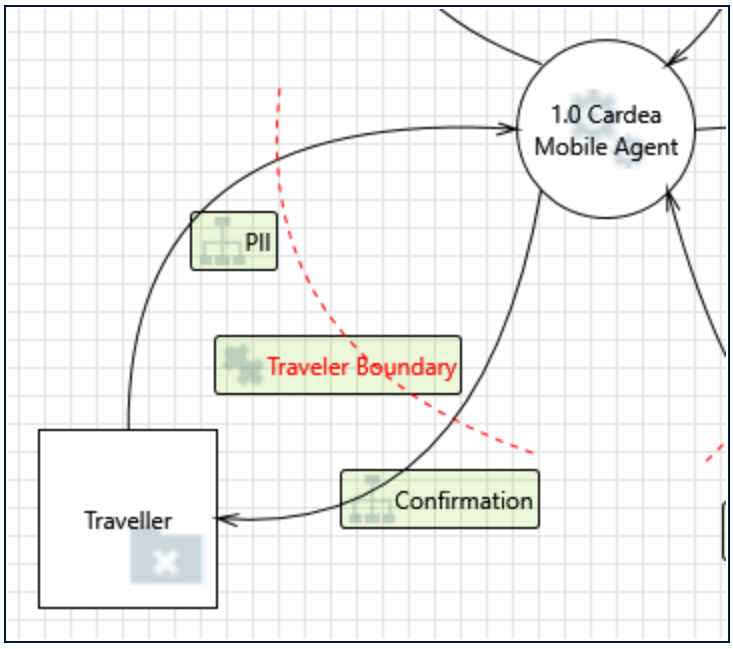
9. Spoofing the 1.0 Cardea Mobile Agent Process [State: Not Started] [Priority: Low]

Category: Spoofing

Description: 1.0 Cardea Mobile Agent may be spoofed by an attacker and this may lead to information disclosure by Local Files. Consider using a standard authentication mechanism to identify the destination process. This is possible if malware performs a masqurade attack on the phone to gain access to its files. Authentication is limited in Cardea's decentralized infrastructure.

Justification: Cardea has no control over third-party software on the smartphone.

Interaction: Confirmation



10. Data Flow Confirmation Is Potentially Interrupted [State: Not Started] [Priority: Low]

Category: Tampering

Description: An external agent prevents the traveler from seeing their information. This is possible if the traveler's friend deletes/denies lab results.

Justification: This requires that the external agent has access to the smartphone in the first place.

11. External Entity Traveller Potentially Denies Receiving Data [State: Not Applicable] [Priority: High]

Category: Repudiation

Description: Traveller 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: N/A

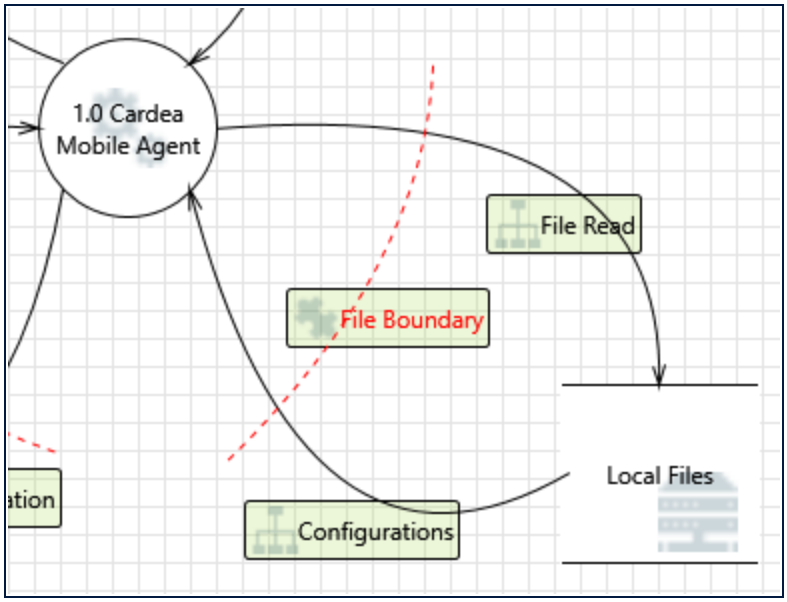
12. Spoofing of the Traveller External Destination Entity [State: Not Applicable] [Priority: High]

Category: Spoofing

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

Justification: N/A

Interaction: File Read



13. Spoofing of Data Store Local Files [State: Not Started] [Priority: High]

Category: Spoofing

Description: Traveler may spoof local files to change their saved lab results. A rooted phone can change a positive COVID test to a negative. This violates the integrity of the test results.

Justification: The phone must be rooted/jailbroken.

14. Potential Excessive Resource Consumption for 1.0 Cardea Mobile Agent or Local Files [State: Not Started] [Priority: Medium]

Category: Denial Of Service

Description: Does 1.0 Cardea Mobile Agent or Local Files 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. Lab results can not be saved to local files if the phone is out of storage.

Justification: Smartphone OS will notify the user if the storage is full or almost full. Also, the user can assign a certain amount of hard drive space to the Cardea Mobile Agent.

15. Impersonating another's account on Cardea Mobile Agent [State: Not Started] [Priority: High]

Category: Spoofing

Description: The phone user can impersonate another's account on Cardea Mobile Agent; and pass-off their friend's information as their own.

Justification: A biometric picture shows the face of the information owner. A verifier can see the biometric picture of the account owner and verify if the impersonater is the account owner.

16. The Local Files Data Store Could Be Corrupted [State: Not Started] [Priority: Low]

Category: Tampering

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

Justification: Lab results can be sanitized for injection code or special characters.

17. OS Denies Local Files Potentially Writing Data [State: Not Started] [Priority: Medium]

Category: Repudiation

Description: The operating system does not grant Cardea Mobile Agent the privileges of saving files. Thus, test results cannot be saved.

Justification: The user can enable the necessary privileges to Cardea Mobile Agent to save files.

18. Data Flow Sniffing [State: Mitigation Implemented] [Priority: Low]

Category: Information Disclosure

Description: Data flowing across File Read 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: According to the Cardea White Paper (p.14), this data flow is encrypted by asymmetric cryptography.

19. Data Flow File Read Is Potentially Interrupted [State: Not Started] [Priority: High]

Category: Information Corruption

Description: An external agent deletes the local files data store. A user with access to the phone can delete the Cardea Mobile Agent, which deletes its local files.

Justification: Smartphones offer password/pin protection.

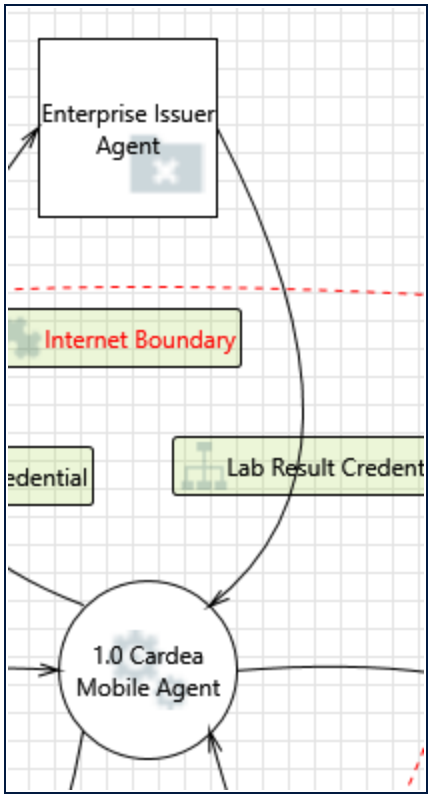
20. Data Store Inaccessible [State: Not Started] [Priority: Low]

Category: Denial Of Service

Description: An external agent prevents access to a data store on the other side of the trust boundary. This can be caused by malware or OS privileges.

Justification: Cardea Mobile Agent has no control over third-party software on the phone or OS privileges.

Interaction: Lab Result Credential



21. Cross Site Request Forgery [State: Not Applicable] [Priority: High]

Category: Elevation Of Privilege

Description: Cross-site request forgery (CSRF or XSRF) is a type of attack in which an attacker forces a user's browser to make a forged request to a vulnerable site by exploiting an existing trust relationship between the browser and the vulnerable web site. In a simple scenario, a user is logged in to web site A using a cookie as a credential. The other browses to web site B. Web site B returns a page with a hidden form that posts to web site A. Since the browser will carry the user's cookie to web site A, web site B now can take any action on web site A, for example, adding an admin to an account. The attack can be used to exploit any requests that the browser automatically authenticates, e.g. by session cookie, integrated authentication, IP whitelisting. The attack can be carried out in many ways such as by luring the victim to a site under control of the attacker, getting the user to click a link in a phishing email, or hacking a reputable web site that the victim will visit. The issue can only be resolved on the server side by requiring that all authenticated state-changing requests include an additional piece of secret payload (canary or CSRF token) which is known only to the legitimate web site and the browser and which is protected in transit through SSL/TLS. See the Forgery Protection property on the flow stencil for a list of mitigations.

Justification: N/A

22. Elevation Using Impersonation [State: Not Applicable] [Priority: High]

Category: Elevation Of Privilege

Description: 1.0 Cardea Mobile Agent may be able to impersonate the context of Enterprise Issuer Agent in order to gain additional privilege.

Justification: N/A

23. Elevation by Changing the Execution Flow in 1.0 Cardea Mobile Agent [State: Not Started] [Priority: Medium]

Category: Elevation Of Privilege

Description: An attacker may pass data into 1.0 Cardea Mobile Agent in order to change the flow of program execution within 1.0 Cardea Mobile Agent to the attacker's choosing.

Justification: Inputs can be sanitized.

24. Enterprise Issuer Agent May be Subject to Elevation of Privilege Using Remote Code Execution [State: Not Started] [Priority: High]

Category: Elevation Of Privilege

Description: 1.0 Cardea Mobile Agent may be able to remotely execute code for Enterprise Issuer Agent.

Justification: Input sanitization.

25. Data Flow Lab Result Credential Is Potentially Interrupted [State: Not Started] [Priority: Medium]

Category: Denial Of Service

Description: An external agent interrupts data flowing across a trust boundary in either direction. An attacker may have incentive to harm travelers by dropping their lab results. Firewall rules may also prevent lab result credentials from reaching the traveler.

Justification: Cardea can push an update to email the traveler notifying of them of their lab result credential being sent. If the traveler does not see such notification on the Cardea Mobile Agent, then they can suspect a DoS.

26. Potential Process Crash or Stop for 1.0 Cardea Mobile Agent [State: Not Started] [Priority: Medium]

Category: Denial Of Service

Description: 1.0 Cardea Mobile Agent crashes, halts, stops or runs slowly; in all cases violating an availability metric. Cardea may have bugs or lack of resources that prevent all lab results from reaching the Cardea Mobile Agent.

Justification: Version control, open-sourced software, staff from Hyperledger Foundation.

27. Data Flow Sniffing [State: Not Started] [Priority: Medium]

Category: Information Disclosure

Description: Data flowing across Lab Result Credential 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: Possible, but this information is protected by asymmetric encryption.

28. Potential Data Repudiation by 1.0 Cardea Mobile Agent [State: Not Started] [Priority: Low]

Category: Repudiation

Description: 1.0 Cardea Mobile Agent 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: Lab results are not constrainted to Cardea. Labs keep a carbon copy of lab results for their user accounts.

29. Potential Lack of Input Validation for 1.0 Cardea Mobile Agent [State: Not Started] [Priority: Medium]

Category: Tampering

Description: Data flowing across Lab Result Credential may be tampered with by an attacker. This may lead to a denial of service attack against 1.0 Cardea Mobile Agent or an elevation of privilege attack against 1.0 Cardea Mobile Agent or an information disclosure by 1.0 Cardea Mobile Agent. 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: Inputs can be sanitized.

30. Spoofing the Enterprise Issuer Agent External Entity [State: Not Started] [Priority: High]

Category: Spoofing

Description: Enterprise Issuer Agent may be spoofed by an attacker and this may lead to unauthorized access to 1.0 Cardea Mobile Agent. The login authorization for Enterprise Issuer Agents have no MFA.

Justification: Enterprise Issuer Agent accounts are username and password protected.

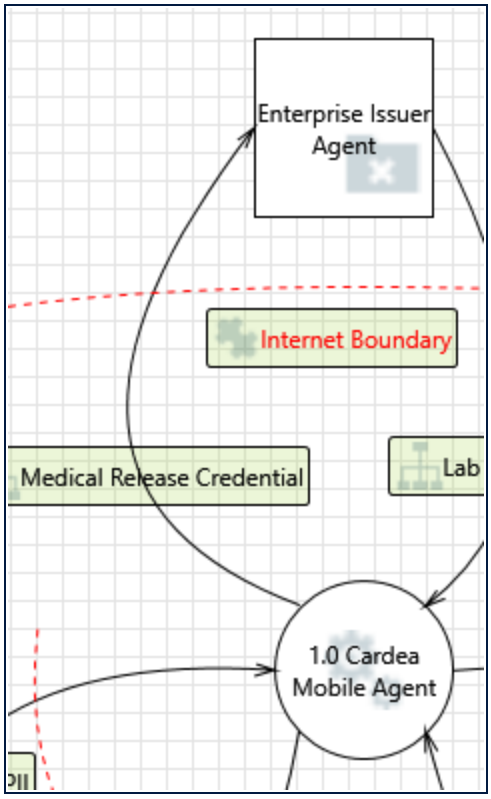
31. Spoofing the 1.0 Cardea Mobile Agent Process [State: Not Started] [Priority: Medium]

Category: Spoofing

Description: 1.0 Cardea Mobile Agent may be spoofed by an attacker and this may lead to information disclosure by Enterprise Issuer Agent. The credentials sent between the Enterprise Issuer Agent and the Cardea Mobile Agent does contain PII, so there is an incentive to capture those credentials. And the authentication is limited by Cardea's decentralized infrastructure.

Justification: Packets sent across the internet boundary are HTTPS encrypted.

Interaction: Medical Release Credential



32. Data Flow Medical Release Credential Is Potentially Interrupted [State: Not Started] [Priority: Medium]

Category: Denial Of Service

Description: An external agent interrupts data flowing across a trust boundary in either direction. This DoS can prevent the traveler from receiving lab test results.

Justification: There is no incentive to preventing a medical release credential from reaching the enterprise issuer agent. There may be an incentive to harm the traveler via dropping their lab test results.

33. External Entity Enterprise Issuer Agent Potentially Denies Receiving Data [State: Not Started] [Priority: Low]

Category: Repudiation

Description: Enterprise Issuer Agent 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: Enterprise Issuer Agent can log whenever they generate a QR code credential for a traveler.

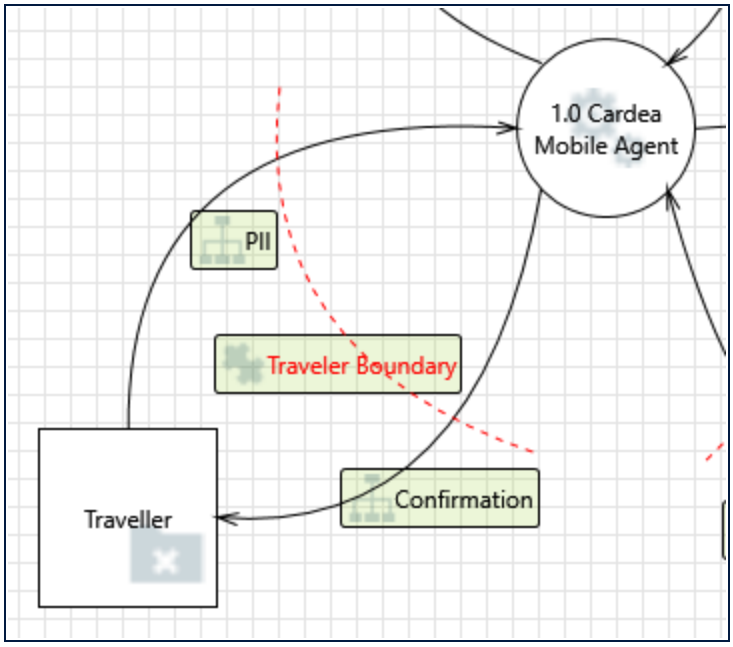
34. Spoofing of the Enterprise Issuer Agent External Destination Entity [State: Mitigation Implemented] [Priority: Low]

Category: Spoofing

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

Justification: According to the Cardea White Paper (p.17), verifier works through a third-party authentication process to confirm the authenticity of the traveler.

Interaction: PII



35. Spoofing the Traveller External Entity [State: Not Started] [Priority: High]

Category: Spoofing

Description: Traveller may be spoofed by an attacker and this may lead to unauthorized access to 1.0 Cardea Mobile Agent. Authentication is limited to Cardea's decentralized infrastructure.

Justification: Smartphones have password/pin protection to protect access to its apps like Cardea Mobile Agent.

36. Cross Site Request Forgery [State: Not Applicable] [Priority: High]

Category: Elevation Of Privilege

Description: Cross-site request forgery (CSRF or XSRF) is a type of attack in which an attacker forces a user's browser to make a forged request to a vulnerable site by exploiting an existing trust relationship between the browser and the vulnerable web site. In a simple scenario, a user is logged in to web site A using a cookie as a credential. The other browses to web site B. Web site B returns a page with a hidden form that posts to web site A. Since the browser will carry the user's cookie to web site A, web site B now can take any action on web site A, for example, adding an admin to an account. The attack can be used to exploit any requests that the browser automatically authenticates, e.g. by session cookie, integrated authentication, IP

whitelisting. The attack can be carried out in many ways such as by luring the victim to a site under control of the attacker, getting the user to click a link in a phishing email, or hacking a reputable web site that the victim will visit. The issue can only be resolved on the server side by requiring that all authenticated state-changing requests include an additional piece of secret payload (canary or CSRF token) which is known only to the legitimate web site and the browser and which is protected in transit through SSL/TLS. See the Forgery Protection property on the flow stencil for a list of mitigations.

Justification: N/A

37. Elevation Using Impersonation [State: Not Applicable] [Priority: High]

Category: Elevation Of Privilege

Description: 1.0 Cardea Mobile Agent may be able to impersonate the context of Traveller in order to gain additional privilege.

Justification: N/A

38. Elevation by Changing the Execution Flow in 1.0 Cardea Mobile Agent [State: Mitigation Implemented] [Priority: Low]

Category: Elevation Of Privilege

Description: An attacker may pass data into 1.0 Cardea Mobile Agent in order to change the flow of program execution within 1.0 Cardea Mobile Agent to the attacker's choosing.

Justification: The traveler already has the highest privileges offered by Cardea Mobile Agent.

39. 1.0 Cardea Mobile Agent May be Subject to Elevation of Privilege Using Remote Code Execution [State: Mitigation Implemented] [Priority: Low]

Category: Elevation Of Privilege

Description: Traveller may be able to remotely execute code for 1.0 Cardea Mobile Agent.

Justification: The traveler already has the highest privileges offered by Cardea Mobile Agent.

40. Data Flow PII Is Potentially Interrupted [State: Not Started] [Priority: Low]

Category: Denial Of Service

Description: An external agent interrupts data flowing across a trust boundary in either direction. This is possible if malware prevents a traveler from using Cardea Mobile Agent.

Justification: Cardea cannot implement controls to prevent third-party software on the traveler's phone.

41. Potential Process Crash or Stop for 1.0 Cardea Mobile Agent [State: Mitigation Implemented] [Priority: Low]

Category: Denial Of Service

Description: 1.0 Cardea Mobile Agent crashes, halts, stops or runs slowly; in all cases violating an availability metric.

Justification: Cardea Mobile Agent is open-sourced. So buggy behavior can be quickly fixed through contributions of the community.

42. Data Flow Sniffing [State: Not Started] [Priority: Low]

Category: Information Disclosure

Description: Data flowing across PII 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. This is possible if malware is on the traveler's phone.

Justification: Cardea has no possible controls for third-party software on the traveler's phone.

43. Potential Data Repudiation by 1.0 Cardea Mobile Agent [State: Mitigation Implemented] [Priority: Low]

Category: Repudiation

Description: 1.0 Cardea Mobile Agent 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: There is real-time confirmation that data is stored and credentials are accepted.

44. Potential Lack of Input Validation for 1.0 Cardea Mobile Agent [State: Not Started] [Priority: Medium]

Category: Tampering

Description: Data flowing across PII may be tampered with by an attacker. This may lead to a denial of service attack against 1.0 Cardea Mobile Agent or an elevation of privilege attack against 1.0 Cardea Mobile Agent or an information disclosure by 1.0 Cardea Mobile Agent. 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: There are niche situations where falsifying PII would benefit the traveler. Also, there is no benefit in exploiting Cardea Mobile Agent, since it is a decentralized application.

45. Spoofing the 1.0 Cardea Mobile Agent Process [State: Not Started] [Priority: High]

Category: Spoofing

Description: 1.0 Cardea Mobile Agent may be spoofed by an attacker and this may lead to information disclosure by Traveller. The traveler may be a friend or family member of the true owner of

Cardea Mobile Agent information. Traveler authentication is limited by Cardea's decentralized infrastructure.

Justification: Having access to someone's smartphone typically means that permission is given to view their information.