Dragon_DFD

Owner:
Reviewer:
Contributors:
Date Generated: Sun Oct 06 2024

Executive Summary

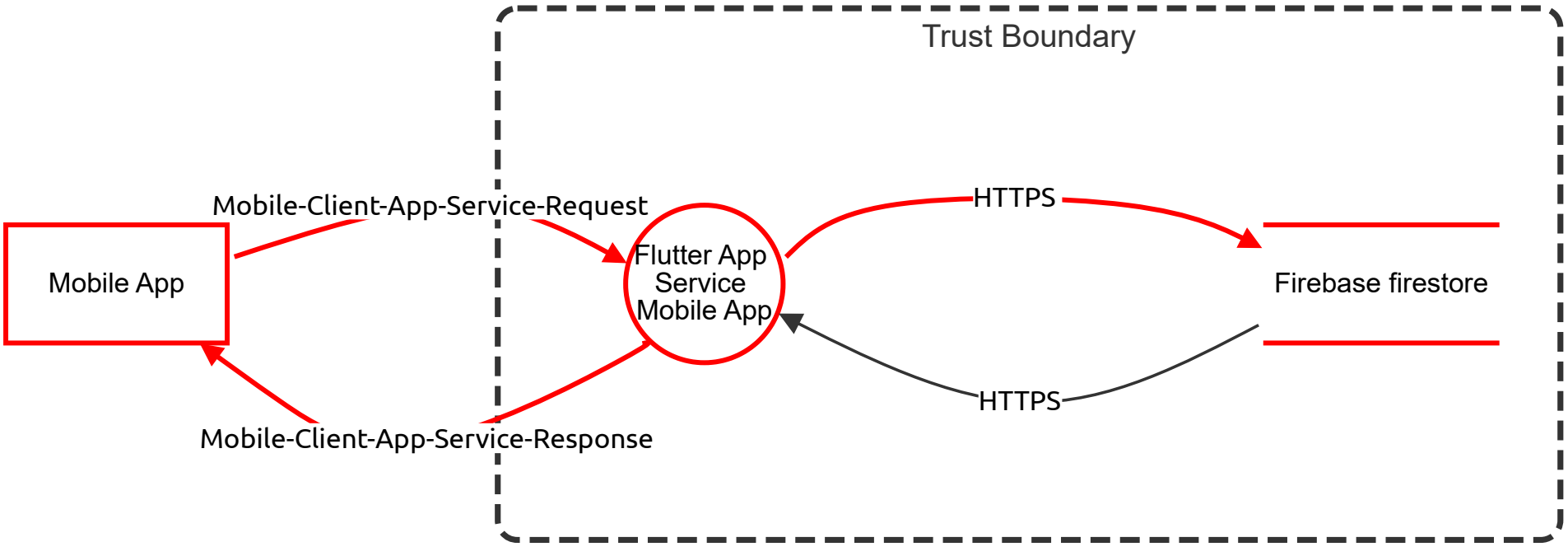
High level system description

Not provided

Summary

Total Threats	10
Total Mitigated	0
Not Mitigated	10
Open / High Priority	9
Open / Medium Priority	1
Open / Low Priority	0
Open / Unknown Priority	0

Sunny_childhood



Sunny_childhood

Mobile App (Actor)

Number	Title	Type	Priority	Status	Score	Description	Mitigations
1	Spoofing of the Mobile Client External Destination Entity	Spoofing	High	Open		Mobile Client may be spoofed by an attacker and this may lead to data being sent to the attacker's target instead of Mobile Client. Consider using a standard authentication mechanism to identify the external entity.	
1	External Entity Mobile Client Potentially Denies Receiving Data	Repudiation	High	Open		Mobile Client 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.	

Flutter App Service Mobile App (Process)

Number	Title	Type	Priority	Status	Score	Description	Mitigations
1	Elevation Using Impersonation	Elevation of privilege	High	Open		Flutter App Service Mobile App may be able to impersonate the context of Mobile Client in order to gain additional privilege.	
1	Spoofing of Destination Data Store Firebase firestore	Spoofing	High	Open		Firebase firestore may be spoofed by an attacker and this may lead to data being written to the attacker's target instead of Firebase firestore. Consider using a standard authentication mechanism to identify the destination data store.	
1	Flutter App Service Mobile App May be Subject to Elevation of Privilege Using Remote Code Execution	Elevation of privilege	High	Open		Mobile Client may be able to remotely execute code for Flutter App Service Mobile App.	
1	Potential Data Repudiation by Flutter App Service Mobile App	Repudiation	High	Open		Flutter App Service Mobile App 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.	

Firebase firestore (Store)

Number	Title	Type	Priority	Status	Score	Description	Mitigations
13	Potential Lack of Input Validation for Flutter App Service Mobile App	Tampering	Medium	Open		Data flowing across Mobile-client-App-Service-Request may be tampered with by an attacker. This may lead to a denial of service attack against Flutter App Service Mobile App or an elevation of privilege attack against Flutter App Service Mobile App or an information disclosure by Flutter App Service Mobile App. 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.	Provide remediation for this threat or a reason if status is N/A

Mobile-Client-App-Service-Request (Data Flow)

Number	Title	Type	Priority	Status	Score	Description	Mitigations
1	Data Flow Sniffing	Information disclosure	High	Open		Data flowing across Mobile-client-App-Service-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.	

HTTPS R (Data Flow)

Number	Title	Type	Priority	Status	Score	Description	Mitigations
1	Potential Excessive Resource Consumption for Flutter App Service Mobile App or Firebase firestore	Denial of service	High	Open		Does Flutter App Service Mobile App or Firebase firestore 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.	

Mobile-Client-App-Service-Response (Data Flow)

Number	Title	Type	Priority	Status	Score	Description	Mitigations
1	Data Flow Mobile-client-App-Service-Response Is Potentially Interrupted	Denial of service	High	Open		An external agent interrupts data flowing across a trust boundary in either direction.	

HTTPS (Data Flow)

Number	Title	Type	Priority	Status	Score	Description	Mitigations