Dragon_DFD

Owner:
Reviewer:
Contributors:
Date Generated: Thu Oct 10 2024

Executive Summary

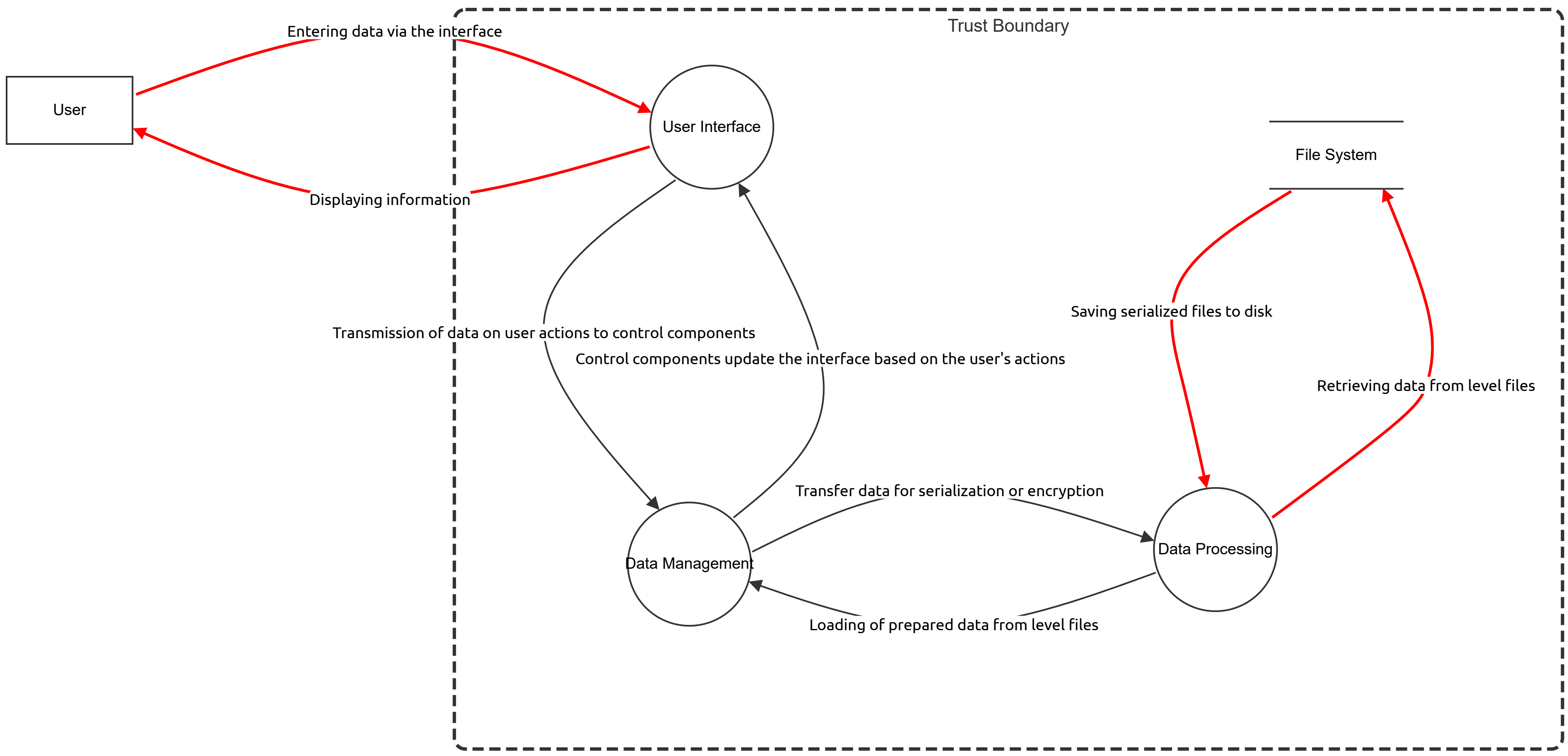
High level system description

Not provided

Summary

Total Threats	10
Total Mitigated	0
Not Mitigated	10
Open / High Priority	4
Open / Medium Priority	5
Open / Low Priority	0
Open / Unknown Priority	0

2D Platformer Game Enginee


Trust Boundary
Entering data via the interface
User
User Interface
Displaying information
File System
Saving serialized files to disk
Transmission of data on user actions to control components
Control components update the interface based on the user's actions
Retrieving data from level files
Transfer data for serialization or encryption
Data Management
Data Processing
Loading of prepared data from level files

2D Platformer Game Enginee

User (Actor)

Number	Title	Type	Priority	Status	Score	Description	Mitigations

Transmission of data on user actions to control components (Data Flow)

Number	Title	Type	Priority	Status	Score	Description	Mitigations

Control components update the interface based on the user's actions (Data Flow)

Number	Title	Type	Priority	Status	Score	Description	Mitigations

Transfer data for serialization or encryption (Data Flow)

Number	Title	Type	Priority	Status	Score	Description	Mitigations

Saving serialized files to disk (Data Flow)

Number	Title	Type	Priority	Status	Score	Description	Mitigations
3	Spoofing of Destination Data Store File System	Information disclosure	High	Open		File System may be spoofed by an attacker and this may lead to data being written to the attacker's target instead of File System. Consider using a standard authentication mechanism to identify the destination data store.	Provide remediation for this threat or a reason if status is N/A
4	Weak Access Control for a Resource	Information disclosure	High	Open		Improper data protection of File System can allow an attacker to read information not intended for disclosure. Review authorization settings.	Provide remediation for this threat or a reason if status is N/A

Retrieving data from level files (Data Flow)

Number	Title	Type	Priority	Status	Score	Description	Mitigations
1	Spoofing of Destination Data Store File System	Information disclosure	High	NotApplicable		File System may be spoofed by an attacker and this may lead to data being written to the attacker's target instead of File System. Consider using a standard authentication mechanism to identify the destination data store.	
2	Potential Excessive Resource Consumption for Data Processing or File System	Denial of service	High	Open		Does Data Processing or File System 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.	Provide remediation for this threat or a reason if status is N/A

Loading of prepared data from level files (Data Flow)

Number	Title	Type	Priority	Status	Score	Description	Mitigations

Displaying information (Data Flow)

Number	Title	Type	Priority	Status	Score	Description	Mitigations
6	External Entity Human User Potentially Denies Receiving Data	Denial of service	High	Open		Human User 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.	Provide remediation for this threat or a reason if status is N/A
7	Data Flow Displaying information Is Potentially Interrupted	Denial of service	Medium	Open		An external agent interrupts data flowing across a trust boundary in either direction.	Provide remediation for this threat or a reason if status is N/A

Entering data via the interface (Data Flow)

Entering data via the interface

Number	Title	Type	Priority	Status	Score	Description	Mitigations
8	Spoofing the User Interface Process	Information disclosure	Medium	Open		User Interface may be spoofed by an attacker and this may lead to information disclosure by Human User. Consider using a standard authentication mechanism to identify the destination process.	Provide remediation for this threat or a reason if status is N/A
9	Potential Process Crash or Stop for User Interface	Denial of service	Medium	Open		User Interface crashes, halts, stops or runs slowly; in all cases violating an availability metric.	Provide remediation for this threat or a reason if status is N/A
10	User Interface May be Subject to Elevation of Privilege Using Remote Code Execution	Tampering	Medium	Open		Human User may be able to remotely execute code for User Interface.	Provide remediation for this threat or a reason if status is N/A
11	Elevation by Changing the Execution Flow in User Interface	Tampering	Medium	Open		An attacker may pass data into User Interface in order to change the flow of program execution within User Interface to the attacker's choosing.	Provide remediation for this threat or a reason if status is N/A

User Interface (Process)

Number	Title	Type	Priority	Status	Score	Description	Mitigations

Data Management (Process)

Number	Title	Type	Priority	Status	Score	Description	Mitigations

Data Processing (Process)

Number	Title	Type	Priority	Status	Score	Description	Mitigations

File System (Store)

Number	Title	Type	Priority	Status	Score	Description	Mitigations