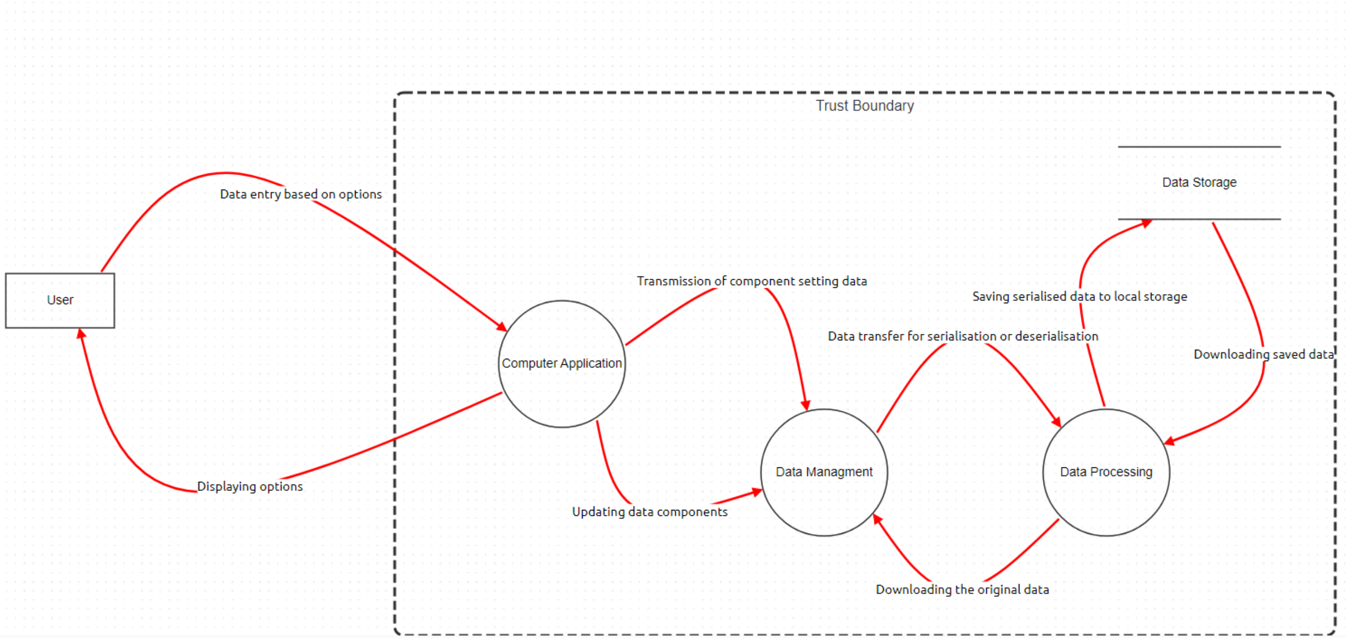
Report on the Data Flow Diagram and Associated Threats

Overview of the Diagram


Trust Boundary
Data Storage
Data entry based on options
User
Transmission of component setting data
Saving serialised data to local storage
Computer Application
Data transfer for serialisation or deserialisation
Downloading saved data
Data Managment
Data Processing
Displaying options
Updating data components
Downloading the original data

The diagram illustrates the data flow between the User, Computer Application, Data Management, Data Processing, and Data Storage. It outlines the various interactions and data transfers occurring within the system, delineating a trust boundary that indicates where data security measures should be enforced. The red connections in the diagram signify critical interactions that are subject to potential security threats, as analyzed through the STRIDE threat modeling framework.

Description of Threats

The following threats have been identified based on the connections in the diagram:

Data transfer for serialization or deserialization

Threat: Elevation of Privilege

Description: Data Processing may impersonate Data Management to gain additional privileges.

Transmission of component setting data

Threat: Information Disclosure

Description: Improper protection of Data Storage could allow unauthorized access to sensitive information.

Transmission of component setting data

Threat: Spoofing

Description: Data Storage may be spoofed, leading to incorrect data being processed. Implementing strong authentication can mitigate this risk.

Downloading saved data

Threat: Elevation of Privilege

Description: Data Management may impersonate Computer Application to gain additional privileges.

Data entry based on options

Threat: Spoofing

Description: An attacker may spoof the Computer Application, leading to information disclosure by the Human User.

Data entry based on options

Threat: Spoofing

Description: An attacker may impersonate the Human User, allowing unauthorized access to Computer Application.

Data entry based on options

Threat: Tampering

Description: Data input may be tampered with, leading to denial of service or privilege escalation attacks. Input validation is crucial for mitigating this risk.

Data entry based on options

Threat: Denial of Service

Description: An external agent may interrupt data flow across the trust boundary, causing service disruptions.

Data entry based on options

Threat: Elevation of Privilege

Description: Computer Application may impersonate the Human User to gain additional privileges.

Data entry based on options

Threat: Elevation of Privilege

Description: The Human User may execute remote code for Computer Application, potentially compromising security.

Displaying options

Threat: Tampering

Description: An attacker could read or modify data transmitted over an authenticated data flow, compromising data integrity.

Updating data components

Threat: Elevation of Privilege

Description: Computer Application may impersonate Data Management to gain additional privileges.

Downloading the original data

Threat: Elevation of Privilege

Description: Data Management may impersonate Data Processing to gain additional privileges.

Saving serialized data to local storage

Threat: Denial of Service

Description: Lack of resource management may lead to Denial of Service (DoS) attacks, causing performance degradation or system unavailability.

Conclusion

The diagram effectively outlines the interactions within the system, but the identified threats underscore the importance of implementing robust security measures. Regular reviews of data protection mechanisms, input validation processes, and user authentication methods are essential to mitigate the identified risks and ensure the integrity and confidentiality of the data throughout its lifecycle.