Threat Modeling Report

Created on 11/10/2019 1:36:14 PM

Threat Model Name:

Owner:

Reviewer:

Contributors:

Description:

Assumptions:

External Dependencies:

Threat Model Summary:

Not Started	0
Not Applicable	6
Needs Investigation	0
Mitigation Implemented	4
Total	10
Total Migrated	0

Diagram: Diagram 1

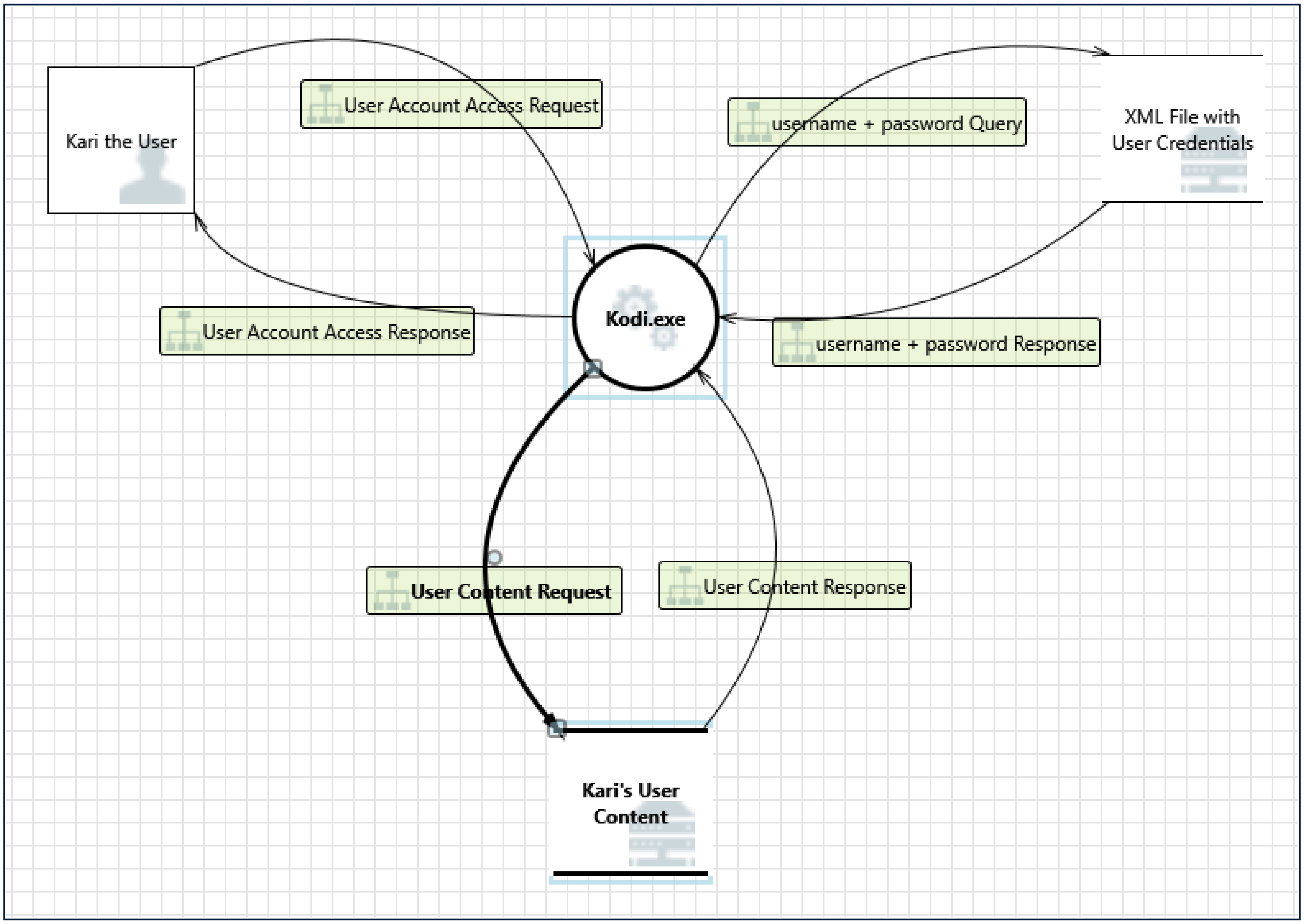
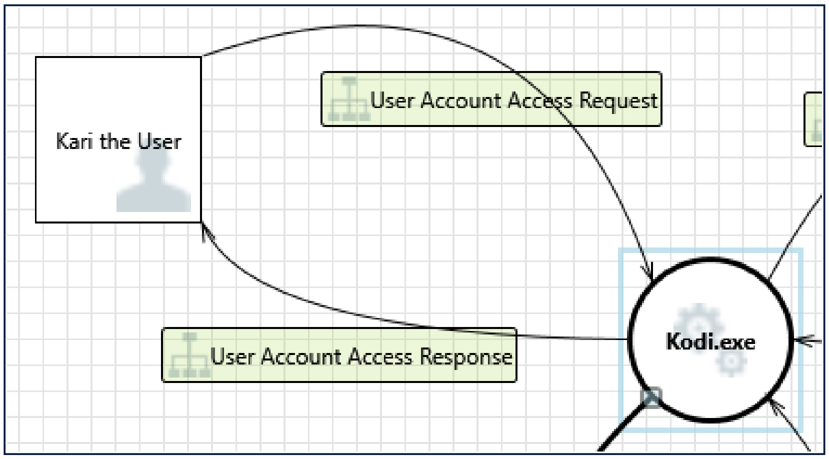

Kari the User
User Account Access Request
username + password Query
XML File with User Credentials
Kodi.exe
User Account Access Response
username + password Response
User Content Request
User Content Response
Kari's User Content

Diagram 1 Diagram Summary:

Not Started	0
Not Applicable	6
Needs Investigation	0
Mitigation Implemented	4
Total	10
Total Migrated	0

Interaction: User Account Access Request



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

Category: Elevation Of Privilege

Description: Kodi.exe may be able to impersonate the context of Kari the User in order to gain additional privilege.

Justification: User account information is stored on the user&#39;s local hardware and the risk of elevation of privilege is accepted

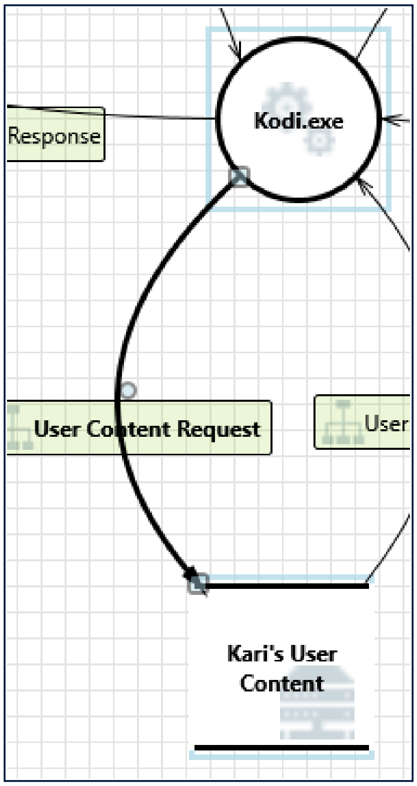
2. Spoofing the Kari the User External Entity [State: Mitigation Implemented] [Priority: High]

Category: Spoofing

Description: Kari the User may be spoofed by an attacker and this may lead to unauthorized access to Kodi.exe. Consider using a standard authentication mechanism to identify the external entity.

Justification: Profile PINs can be activated and implemented to produce an authentication method.

Interaction: User Content Request



3. Potential Excessive Resource Consumption for Kodi.exe or Kari's User Content [State: Not Applicable] [Priority: High]

Category: Denial Of Service

Description: Does Kodi.exe or Kari's User Content 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: Files and executable are stored on user&#39;s hardware and filesystem therefor resource consumption should be implemented by the user&#39;s OS. This is out of scope for the process.

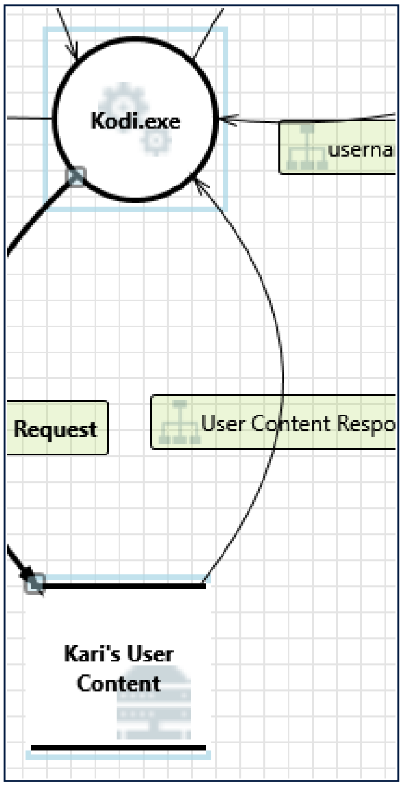
4. Spoofing of Destination Data Store Kari's User Content [State: Not Applicable] [Priority: High]

Category: Spoofing

Description: Kari's User Content may be spoofed by an attacker and this may lead to data being written to the attacker's target instead of Kari's User Content. Consider using a standard authentication mechanism to identify the destination data store.

Justification: The file is stored locally on the user&#39;s hardware and filesystem. The hardware and filesystem are outside of the scope of the process

Interaction: User Content Response



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

Category: Information Disclosure

Description: Improper data protection of Kari's User Content can allow an attacker to read information not intended for disclosure. Review authorization settings.

Justification: Notify user that data is stored insecurely to and implement their own data protection.

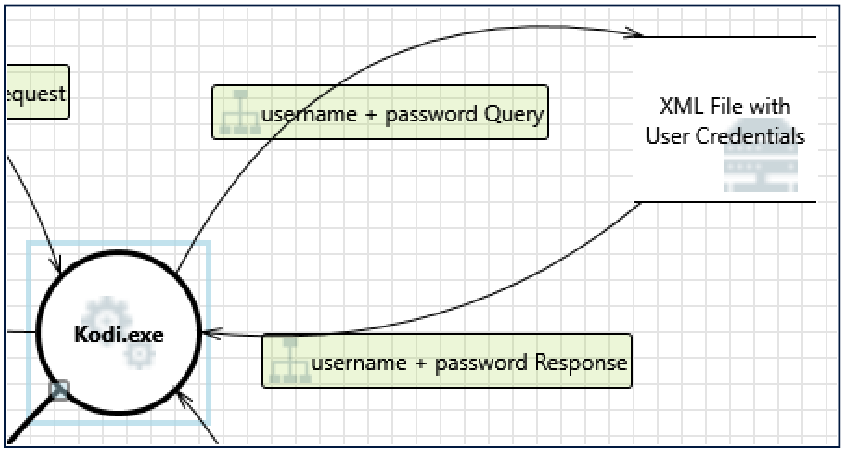
6. Spoofing of Source Data Store Kari's User Content [State: Not Applicable] [Priority: High]

Category: Spoofing

Description: Kari's User Content may be spoofed by an attacker and this may lead to incorrect data delivered to Kodi.exe. Consider using a standard authentication mechanism to identify the source data store.

Justification: The file is stored locally on the user&#39;s hardware and filesystem. The hardware and filesystem are outside of the scope of the process

Interaction: username + password Query



7. Potential Excessive Resource Consumption for Kodi.exe or User Credentials File [State: Not Applicable] [Priority: High]

Category: Denial Of Service

Description: Does Kodi.exe or XML File with User Credentials 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: Files and executable are stored on user&#39;s hardware and filesystem therefor resource consumption should be implemented by the user&#39;s OS.

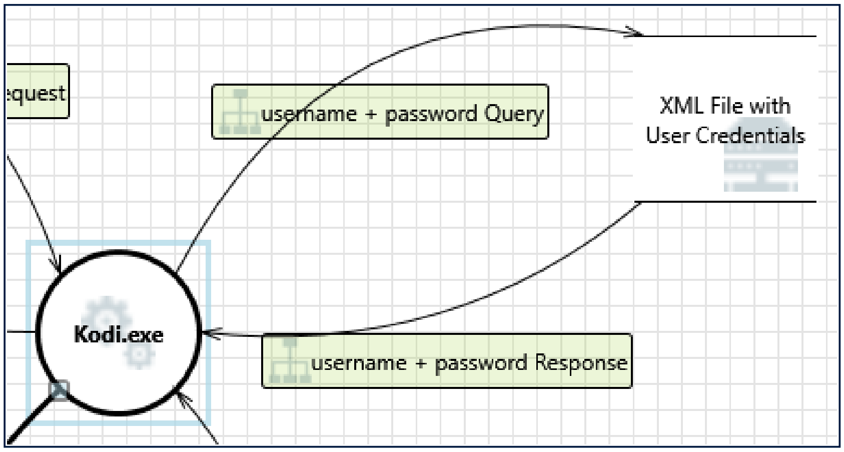
8. Spoofing of Destination Data Store User Credentials File [State: Mitigation Implemented] [Priority: High]

Category: Spoofing

Description: XML File with User Credentials may be spoofed by an attacker and this may lead to data being written to the attacker's target instead of XML File with User Credentials. Consider using a standard authentication mechanism to identify the destination data store.

Justification: Profile PINs can be activated and implemented to produce an authentication method.

Interaction: username + password Response



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

Category: Information Disclosure

Description: Improper data protection of XML File with User Credentials can allow an attacker to read information not intended for disclosure. Review authorization settings.

Justification: Notify user that usernames and passwords are stored in plaintext and to implement their own data protection or secondary authentication

10. Spoofing of Source Data Store User Credentials File [State: Not Applicable] [Priority: High]

Category: Spoofing

Description: XML File with User Credentials may be spoofed by an attacker and this may lead to incorrect data delivered to Kodi.exe. Consider using a standard authentication mechanism to identify the source data store.

Justification: The XML file is stored locally on the user&#39;s hardware and filesystem. The hardware and filesystem are outside of the scope of the process