Threat Modeling Report

Created on 11/12/2019 11:58:26 AM

Threat Model Name:

Owner:

Reviewer:

Contributors:

Description:

Assumptions:

External Dependencies:

Threat Model Summary:

Not Started	0
Not Applicable	6
Needs Investigation	1
Mitigation Implemented	3
Total	10
Total Migrated	0

Diagram: Diagram 1

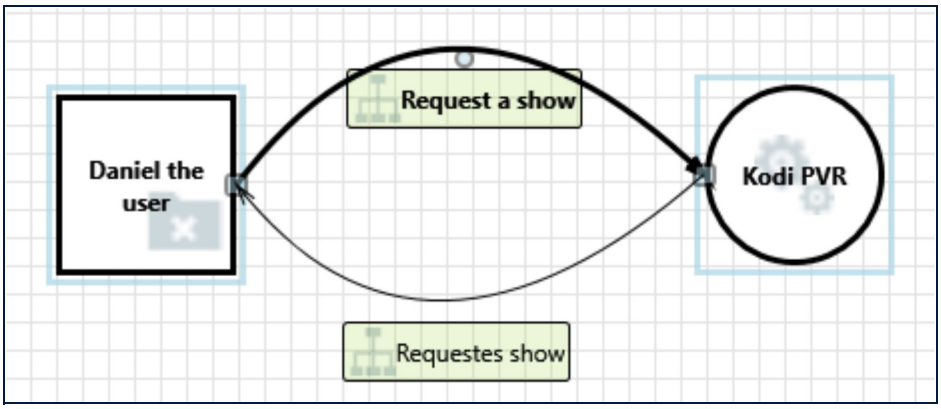
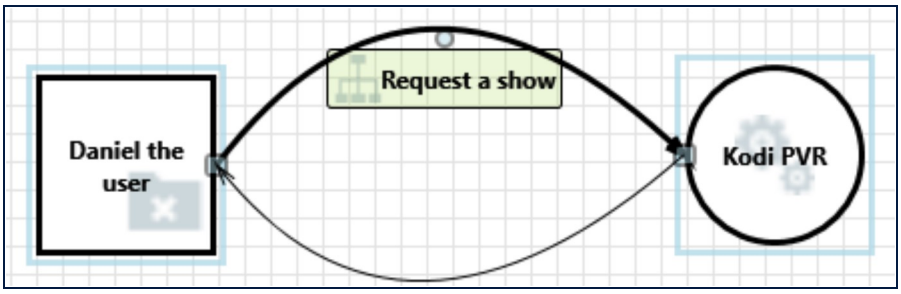


Diagram 1 Diagram Summary:

Not Started	0
Not Applicable	1
Needs Investigation	0
Mitigation Implemented	1
Total	2
Total Migrated	0

Interaction: Request a show



1. Spoofing the Daniel the user External Entity [State: Mitigation Implemented] [Priority: High]

Category:	Spoofing
Description:	Daniel the user may be spoofed by an attacker and this may lead to unauthorized access to Kodi PVR. Consider using a standard authentication mechanism to identify the external entity.
Justification:	Users should use a PIN passcode to be authenticated.

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

Category:	Elevation Of Privilege
Description:	Kodi PVR may be able to impersonate the context of Daniel the user in order to gain additional privilege.
Justification:	Daniel the user would be responsible for setting up the file management on her local storage.

Diagram: Diagram 2

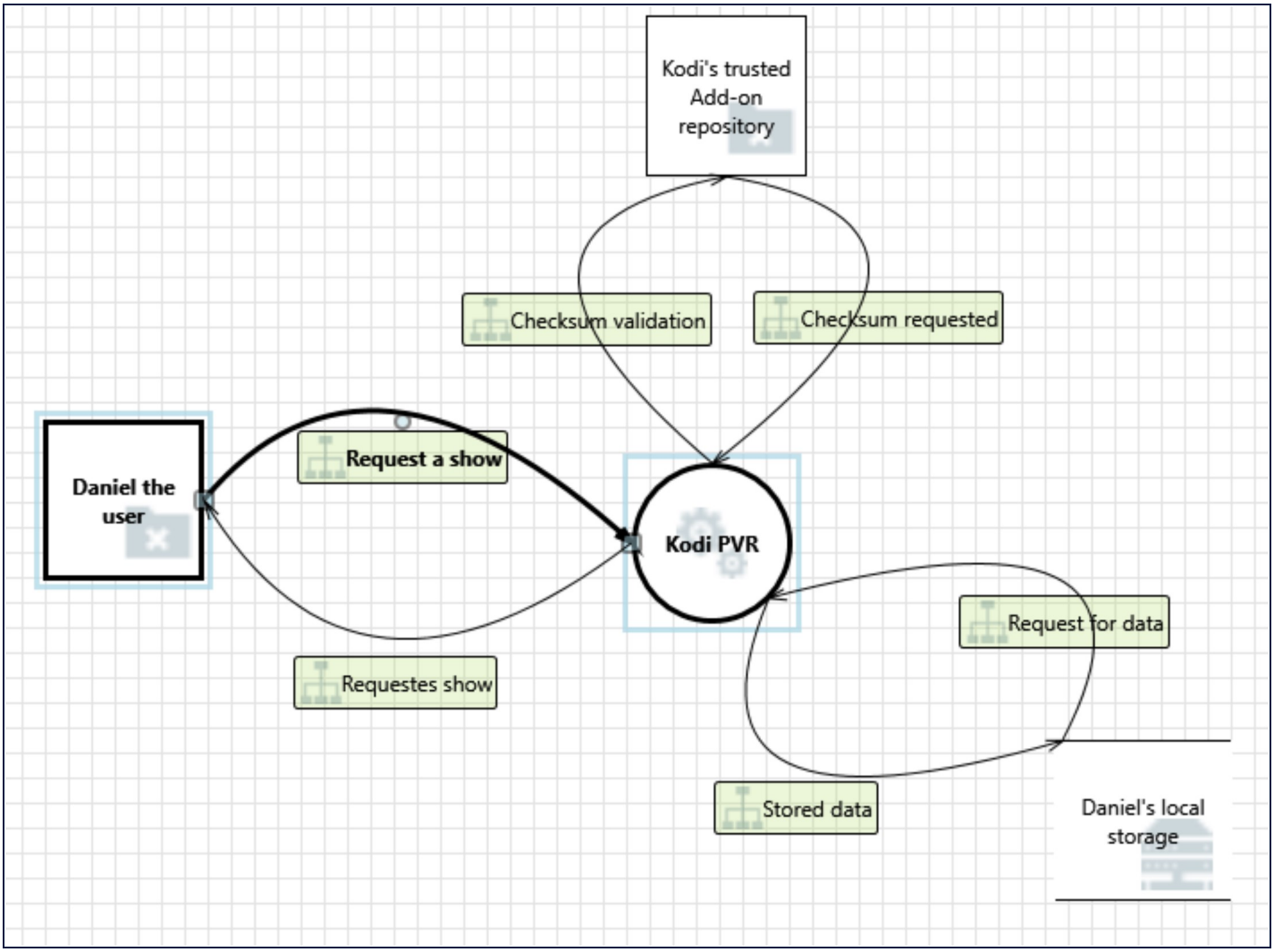
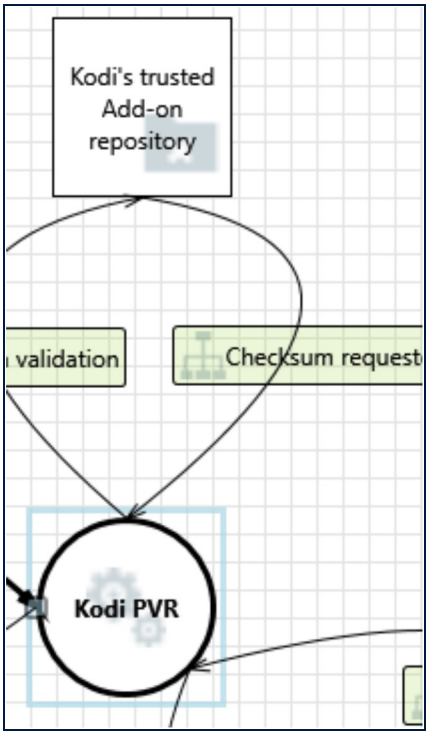


Diagram 2 Diagram Summary:

Not Started	0
Not Applicable	5
Needs Investigation	1
Mitigation Implemented	2
Total	8
Total Migrated	0

Interaction: Checksum requested



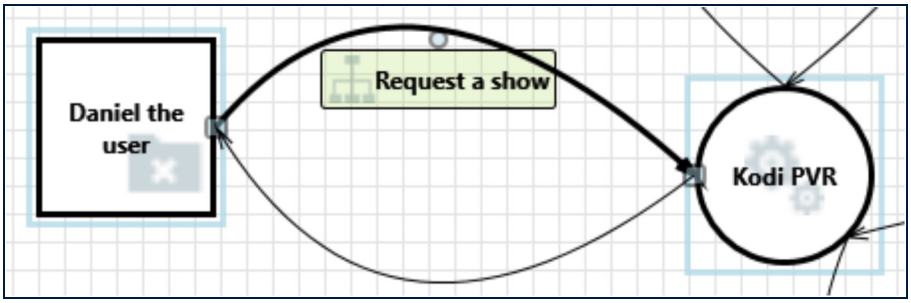
3. Spoofing the Kodi's trusted Add-on repository External Entity [State: Mitigation Implemented] [Priority: High]

Category:	Spoofing
Description:	Kodi's trusted Add-on repository may be spoofed by an attacker and this may lead to unauthorized access to Kodi PVR. Consider using a standard authentication mechanism to identify the external entity.
Justification:	Kodi polles repositories they have deemed trusted.

4. Elevation Using Impersonation [State: Needs Investigation] [Priority: High]

Category:	Elevation Of Privilege
Description:	Kodi PVR may be able to impersonate the context of Kodi's trusted Add-on repository in order to gain additional privilege.
Justification:	Kodi allows repositories to select HTTPS or SSL.

Interaction: Request a show



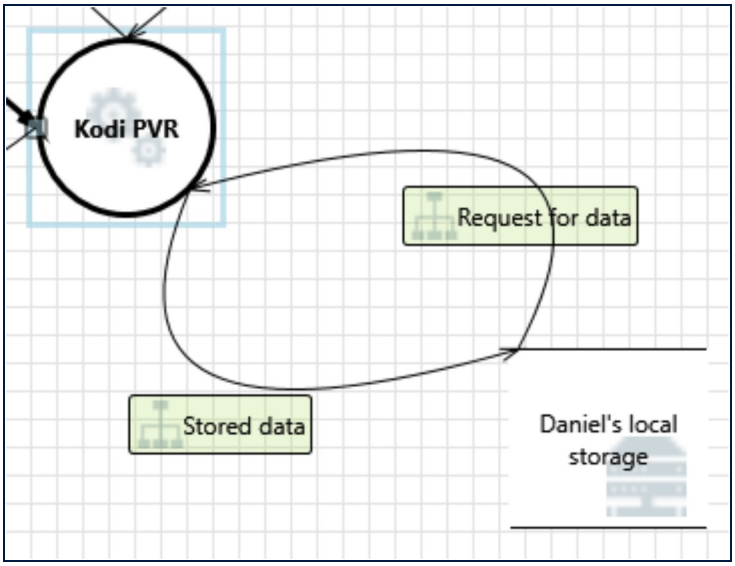
5. Spoofing the Daniel the user External Entity [State: Mitigation Implemented] [Priority: High]

Category:	Spoofing
Description:	Daniel the user may be spoofed by an attacker and this may lead to unauthorized access to Kodi PVR. Consider using a standard authentication mechanism to identify the external entity.
Justification:	Users should use a PIN passcode to be authenticated.

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

Category:	Elevation Of Privilege
Description:	Kodi PVR may be able to impersonate the context of Daniel the user in order to gain additional privilege.
Justification:	Daniel the user would be responsible for setting up the file management on her local storage.

Interaction: Request for data



7. Weak Access Control for a Resource [State: Not Applicable] [Priority: High]

Category: Information Disclosure

Description: Improper data protection of Daniel's local storage can allow an attacker to read information not intended for disclosure. Review authorization settings.

Justification: Daniel the user would be responsible for setting up the file management on her local storage.

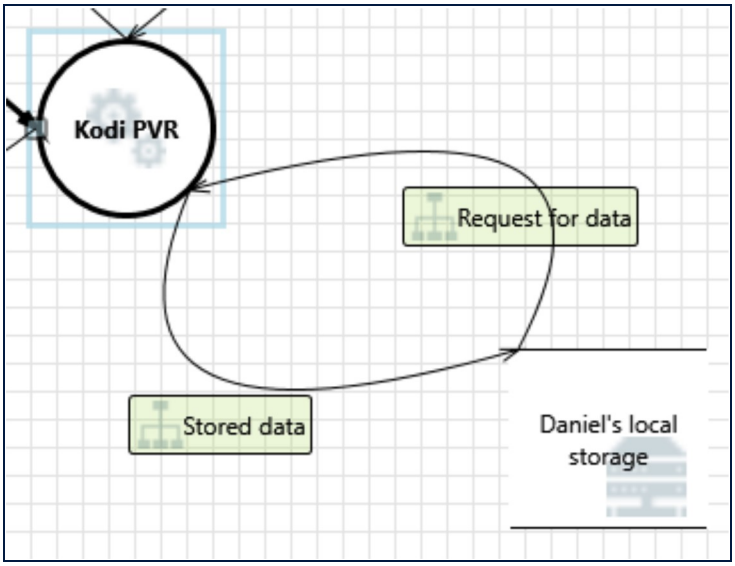
8. Spoofing of Source Data Store Generic Data Store [State: Not Applicable] [Priority: High]

Category: Spoofing

Description: Daniel's local storage may be spoofed by an attacker and this may lead to incorrect data delivered to Kodi PVR. Consider using a standard authentication mechanism to identify the source data store.

Justification: Daniel the user would be responsible for setting up the file management on her local storage.

Interaction: Stored data



9. Spoofing of Destination Data Store Generic Data Store [State: Not Applicable] [Priority: High]

Category: Spoofing

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

Justification: Daniel the user would be responsible for setting up the file management on her local storage.

10. Potential Excessive Resource Consumption for Kodi PVR or Generic Data Store [State: Not

Applicable] [Priority: High]

Category:	Denial Of Service
Description:	Does Kodi PVR or Daniel's local storage 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:	Daniel the user would be responsible for setting up the file management on her local storage.