# Threat Modeling Report

Created on 11/11/2019 2:22:32 PM

Threat Model Name:

Owner:

Reviewer:

Contributors:

Description:

Assumptions:

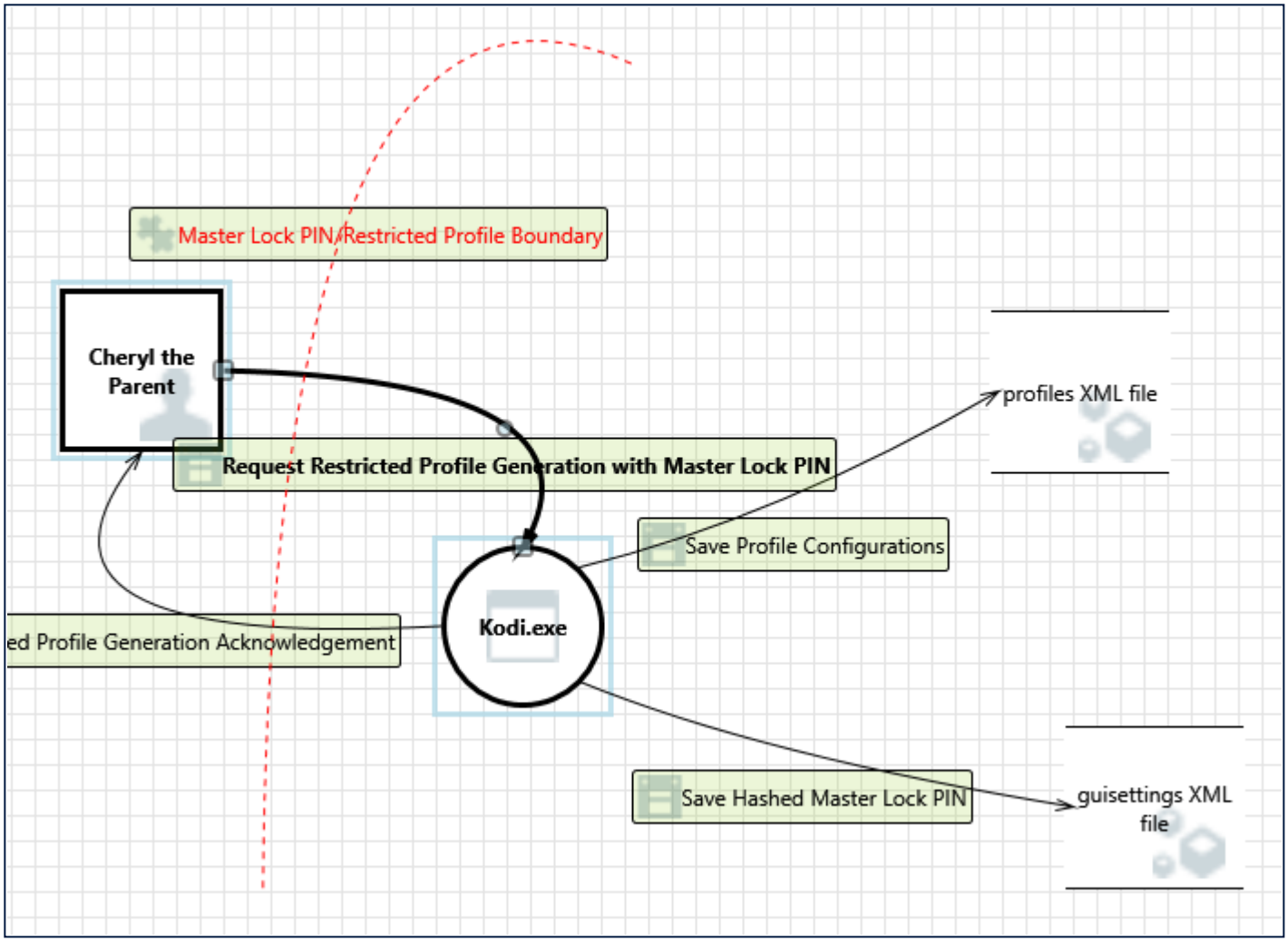
External Dependencies:

## Threat Model Summary:

| | |
|---|---|
| Not Started | 0 |
| Not Applicable | 9 |
| Needs Investigation | 0 |
| Mitigation Implemented | 8 |
| Total | 17 |
| Total Migrated | 0 |

---

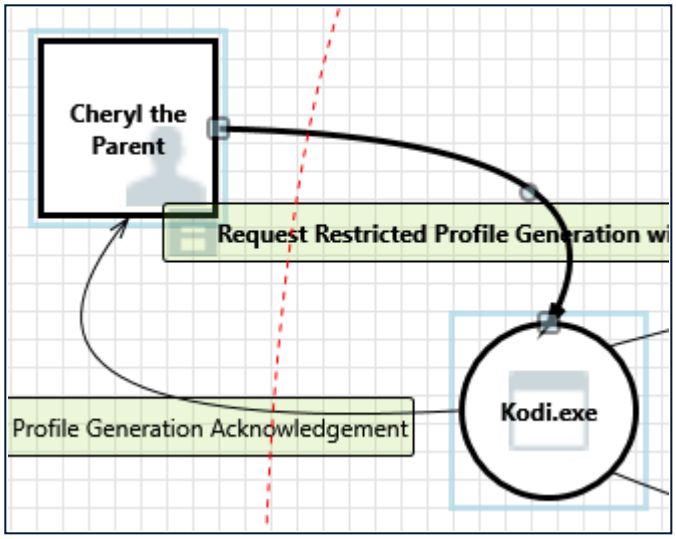
# Diagram:




## Diagram Summary:

| | |
|---|---|
| Not Started | 0 |
| Not Applicable | 9 |
| Needs Investigation | 0 |
| Mitigation Implemented | 8 |
| Total | 17 |
| Total Migrated | 0 |

## Interaction: Request Restricted Profile Generation with Master Lock PIN




1. Elevation Using Impersonation [State: Mitigation Implemented] [Priority: High]

Category: Elevation Of Privilege

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

Justification: The user can set up a Master Lock PIN to mitigate the potential of privilege escalation.

2. Spoofing the Cheryl the Parent External Entity [State: Mitigation Implemented] [Priority: High]

Category: Spoofing

Description: Cheryl the Parent 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: Users may use PIN password to authenticate user profiles.

3. Spoofing the Kodi.exe Process [State: Mitigation Implemented] [Priority: High]

Category: Spoofing

Description: Kodi.exe may be spoofed by an attacker and this may lead to information disclosure by Cheryl the Parent. Consider using a standard authentication mechanism to identify the destination process.

Justification: Master Lock PIN used as authentication mechanism.

4. Potential Lack of Input Validation for Kodi.exe [State: Not Applicable] [Priority: High]

Category: Tampering

Description: Data flowing across Request Restricted Profile Generation with Master Lock PIN may be tampered with by an attacker. This may lead to a denial of service attack against Kodi.exe or an elevation of privilege attack against Kodi.exe or an information disclosure by Kodi.exe. 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.

Justification: External agent would most likely be compromising the hardware, and thus is outside the scope of Kodi.exe

### 5. Potential Data Repudiation by Kodi.exe [State: Mitigation Implemented] [Priority: High]

Category: Repudiation

Description: Kodi.exe 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.

Justification: Kodi software by default generates logs for the user to view.

### 6. Data Flow Sniffing [State: Not Applicable] [Priority: High]

Category: Information Disclosure

Description: Data flowing across Request Restricted Profile Generation with Master Lock PIN 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.

Justification: Entering a PIN to Kodi.exe happens over the hardware and not over a network. If the hardware is compromised and information is disclosed, it is outside the scope of Kodi.

### 7. Potential Process Crash or Stop for Kodi.exe [State: Not Applicable] [Priority: High]

Category: Denial Of Service

Description: Kodi.exe crashes, halts, stops or runs slowly; in all cases violating an availability metric.

Justification: Risk is accepted.

### 8. Data Flow Request Restricted Profile Generation with Master Lock PIN Is Potentially Interrupted [State: Not Applicable] [Priority: High]

Category: Denial Of Service

Description: An external agent interrupts data flowing across a trust boundary in either direction.

Justification: External agent would most likely be compromising the hardware, and thus is outside the scope of Kodi.exe

### 9. Kodi.exe May be Subject to Elevation of Privilege Using Remote Code Execution [State: Mitigation Implemented] [Priority: High]

Category: Elevation Of Privilege

Description: Cheryl the Parent may be able to remotely execute code for Kodi.exe.

Justification: A Master PIN code is implemented to help prevent Elevation of Privilege.

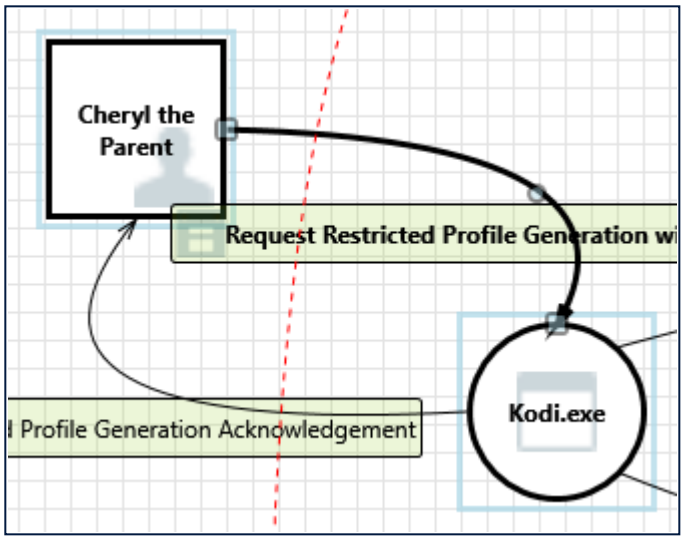
10. Elevation by Changing the Execution Flow in Kodi.exe [State: Mitigation Implemented] [Priority: High]

Category: Elevation Of Privilege

Description: An attacker may pass data into Kodi.exe in order to change the flow of program execution within Kodi.exe to the attacker's choosing.

Justification: Master Lock PIN is implemented to authenticate users.

## Interaction: Restricted Profile Generation Acknowledgement




11. Spoofing of the Cheryl the Parent External Destination Entity [State: Mitigation Implemented] [Priority: High]

Category: Spoofing

Description: Cheryl the Parent may be spoofed by an attacker and this may lead to data being sent to the attacker's target instead of Cheryl the Parent. Consider using a standard authentication mechanism to identify the external entity.

Justification: Master Lock PIN used as authentication mechanism.

12. External Entity Cheryl the Parent Potentially Denies Receiving Data [State: Mitigation Implemented] [Priority: High]

Category: Repudiation

Description: Cheryl the Parent 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.

Justification: Kodi software by default generates logs for the user to view.

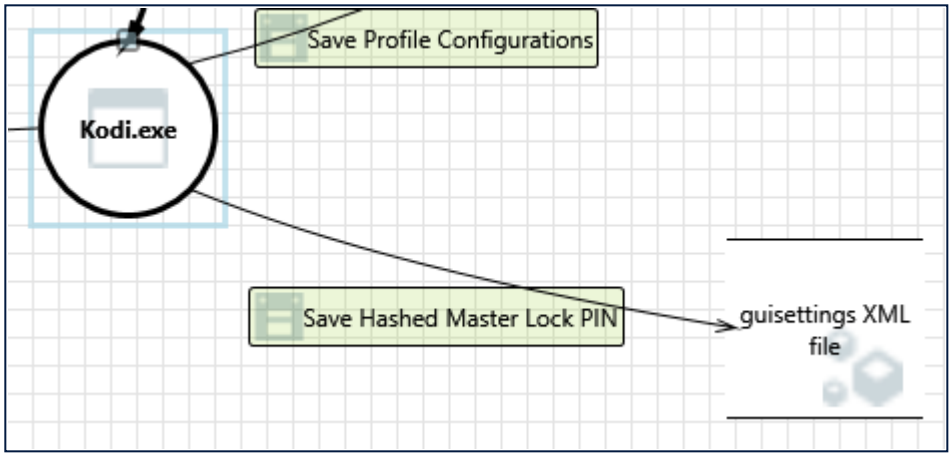
### 13. Data Flow Restricted Profile Generation Acknowledgement Is Potentially Interrupted [State: Not Applicable] [Priority: High]

**Category:** Denial Of Service

**Description:** An external agent interrupts data flowing across a trust boundary in either direction.

**Justification:** External agent would most likely be compromising the hardware, and thus is outside the scope of Kodi.exe

## Interaction: Save Hashed Master Lock PIN




### 14. Potential Excessive Resource Consumption for Kodi.exe or guisettings XML file [State: Not Applicable] [Priority: High]

**Category:** Denial Of Service

**Description:** Does Kodi.exe or guisettings XML file 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:** XML is stored on local hardware and is resource regulated by the operation system.

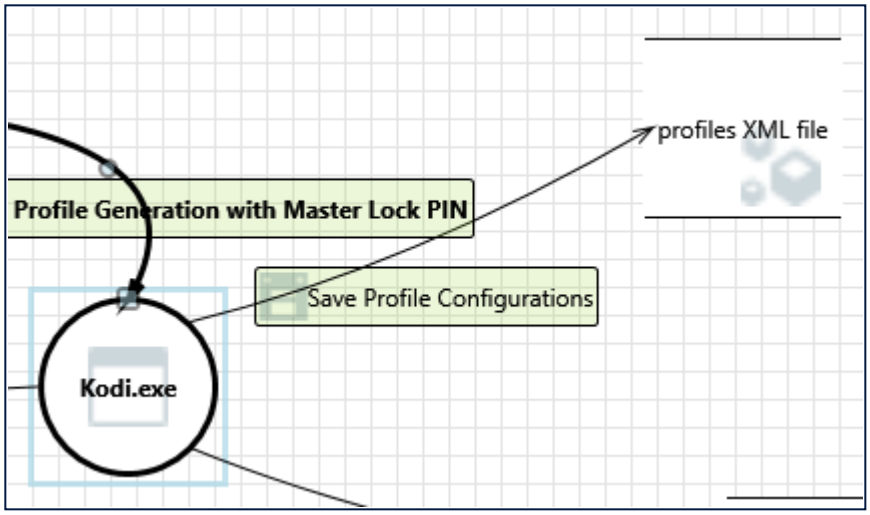
### 15. Spoofing of Destination Data Store guisettings XML file [State: Not Applicable] [Priority: High]

**Category:** Spoofing

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

**Justification:** This file is stored locally on the user's hardware and filesystem. The filesystem is outside the scope of the process.

## Interaction: Save Profile Configurations




16. Potential Excessive Resource Consumption for Kodi.exe or profiles XML file [State: Not Applicable] [Priority: High]

Category: Denial Of Service

Description: Does Kodi.exe or profiles XML file 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: XML is stored on local hardware and is resource regulated by the operation system.

17. Spoofing of Destination Data Store profiles XML file [State: Not Applicable] [Priority: High]

Category: Spoofing

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

Justification: This file is stored locally on the user's hardware and filesystem. The filesystem is outside the scope of the process.